WSM User Guide

Installation and management of workshop systems

Version: 1.4.0
Date: 26.02.2008

Table of contents

1 General remarks

These instructions describe how to use Workshop System Management (WSM) as well as how to set up and use the Integrated Service Information Server (ISIS) system with the associated new-generation devices (Integrated Service Information Display (ISID), Integrated Communication Optical Module (ICOM) and Integrated Service Access Point (ISAP)) from BMW AG.

Knowledge of the information contained in this User Guide and technically proper implementation of the instructions given here are prerequisites for a successful commissioning.

For the sake of clarity, this User Guide does not contain all details and cannot cover every conceivable commissioning and operation scenario.

By the same token, the content of the illustrations described here may deviate slightly from the content actually displayed.

1.1 Target audience of the WSM user guide

This User Guide is addressed primarily to the system administrator or users in the workshop who are responsible for configuring the network and managing the individual devices in the workshop network.

1.2 Explanation of the symbols used

Throughout the document, two different symbols are used to draw the reader's attention to certain topics.

⚠	These **notes** must be read carefully, since problems can occur if they are ignored.
ℹ	The areas marked with this symbol provide the user with additional **information.**

2 First steps

2.1 Workshop System Management tasks

Workshop System Management (WSM) is used to perform the following tasks:

- Software updates of the system components
- Device Management (adding, setting up, starting, configuring, terminating)
- Monitoring of the system components
- Providing an information interface for support

A convenient web front end is available as a user interface.

The WSM start page is opened either via the ISIS Launcher (see chapter 4.1.1) on the workshop PC or directly by entering the ISIS IP in the browser.

2.2 Components supported in the workshop network

2.2.1 Integrated Service Information Server (ISIS)

The **I**ntegrated **S**ervice **I**nformation **S**erver (ISIS) is the intelligent server system for the workshop of the future. The ISIS consists of two top-quality servers in a lockable rack (see Fig. 1).

ℹ	**Information:** The term "ISIS" used here and throughout the rest of the documentation refers to the Integrated Service Information Server.

It forms the basis for modern processes in dealerships. ISIS is a critical component of the new systems for further optimization of service consultation and the workshop area. The new generation of diagnostic and programming systems made available with ICOM and ISID is also based on the new platform.

In addition, the electronic parts catalogue (EPC) as well as the new systems for the processes in service consultation and the workshop area are integrated on the server. These are installed quickly and simply on the ISIS by means of a DVD and are updated by means of online updates. This means that all the necessary data is available locally on the ISIS at the dealership.

WSM, which is launched via PCs at the dealership, displays the most important parameters of the server and the associated applications. On the basis of this data, possible malfunctions such as defective fans or disk failures can be detected at an early stage and total failures can be prevented.

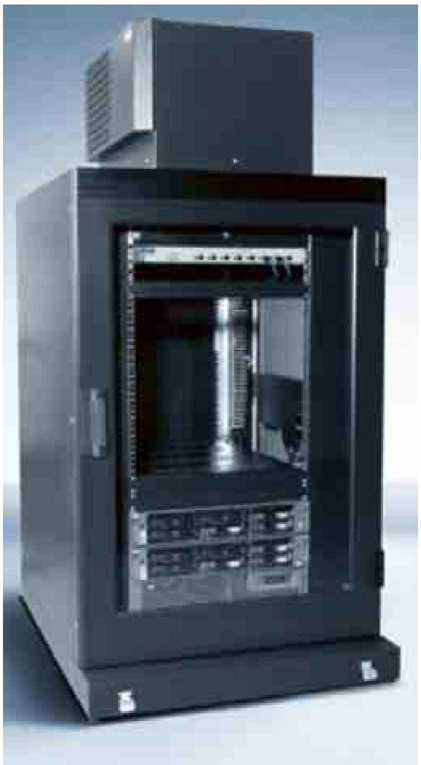


Fig. 1: ISIS (Integrated Service Information Server)

By default, 2 server plug-in modules are always used in a combination, which is referred to throughout the rest of this documentation as an ISIS. This ensures basic security in the event of a failure of one plug-in module.

2.2.2 Uninterruptible power supply (UPS)

The uninterruptible power supply (UPS) is a device in the ISIS rack that ensures the continued running of the applications for a few minutes after a malfunction incident, thus guaranteeing a proper shutdown procedure (see Fig. 2).

Fig. 2: Uninterruptible power supply (UPS)

2.2.3 Integrated Service Information Display (ISID)

The **I**ntegrated **S**ervice **I**nformation **D**isplay (ISID) is a powerful display and operating unit for the workshop. Fig. 3 It is intended for use in the workshop as well as in vehicle reception.

The ISID is a keyboardless control unit. It is operated by touch-screen.

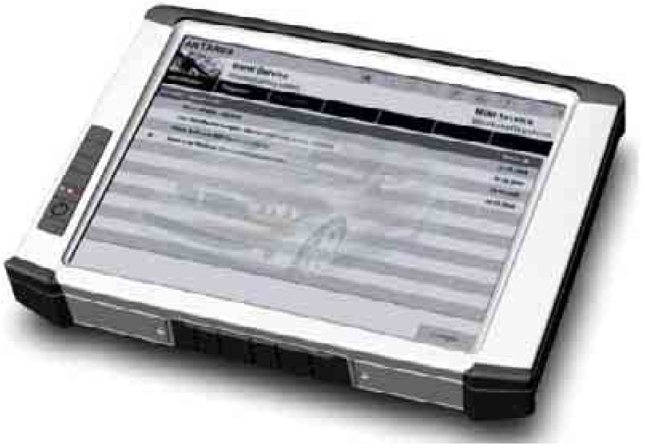


Fig. 3: Integrated Service Information Display (ISID)

ℹ	**Information:** The term "ISID" used here and throughout this documentation refers to the Integrated Service Information Display.

2.2.4 Integrated Communication Optical Module (ICOM)

The **I**ntegrated **C**ommunication **O**ptical **M**odule (ICOM) is a powerful vehicle interface for worldwide use in the BMW Group dealers association. It is intended for use in the workshop as well as in the service department for service consultation, diagnostic and vehicle programming processes.

The ICOM consists of the following components:

- ICOM A

  The ICOM A (see Fig. 4) is an "intelligent" OBD (on-board diagnosis) plug that is mainly used as a protocol converter for communication between a tester (workshop network) and the vehicle control units and/or the vehicle protocols.

  It is used for programming and for diagnosis.

  Communication between the ICOM and workshop network can occur via LAN and WLAN.

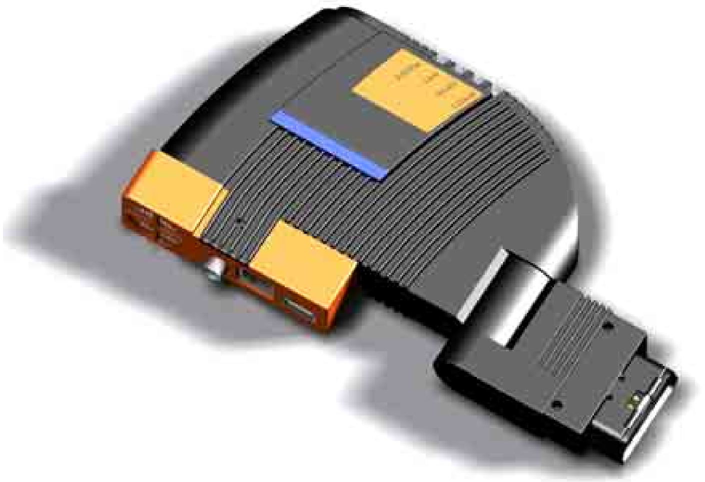


Fig. 4: Integrated Communication Optical Module A (ICOM A)

- ICOM B

  If required, the ICOM B (see Fig. 5) establishes the MOST (Media Oriented System Transport) access to the vehicle. This is an extension of the ICOM A and it is connected to the ICOM A via a standard USB (Universal Series Bus).

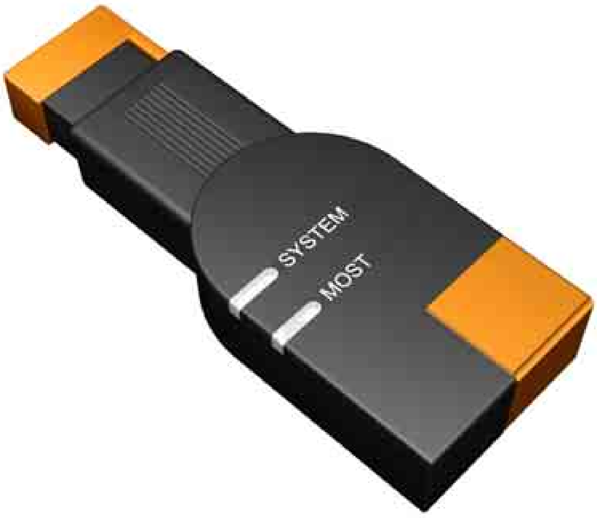


Fig. 5: Integrated Communication Optical Module B (ICOM B)

- ICOM C

  The ICOM C (see Fig. 6) is an adapter for the connection between an OBD plug and a diagnosis circular connector. It enables connection of the ICOM to older vehicles.

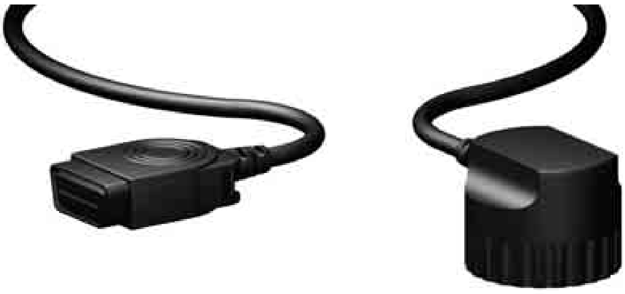


Fig. 6: Integrated Communication Optical Module C (ICOM C)

ℹ	**Information 1:** ICOM B and C are managed via the ICOM A and are not independent components in the WSM. ICOM B and C are thus not firmly assigned to any particular ICOM A, which means they can be used with any ICOM A.

ℹ	**Information 2:** The term "ICOM" used here and throughout this documentation refers to the **I**ntegrated **C**ommunication **O**ptical **M**odule.

2.2.5 Integrated Measurement Interface Box (IMIB)

The **I**ntegrated **M**easurement technology **I**nterface **B**ox (IMIB) provides measurement technology as a network function within the framework of the Integrated Service Technical Application (ISTA) (see Fig. 7). This measuring system enables rapid input and processing of the data as well as flexible use for testing signal sensors, cables and electronic components of the vehicles. In addition, the IMIB can also be used as a portable digital multimeter (DMM).

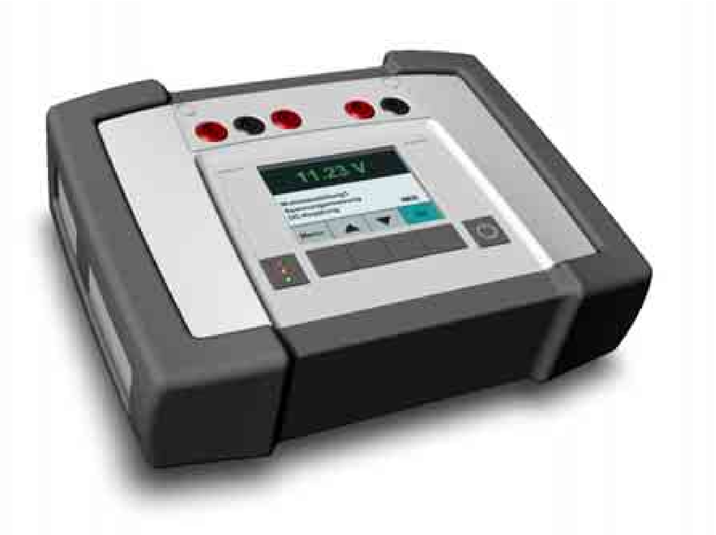


Fig. 7: Integrated Measurement Interface Box (IMIB)

i	**Information:** The IMIB is a new generation device. At the time of this printing, is not yet being delivered. This will take place at a later time.

2.2.6 Integrated Service Access Point (ISAP)

The **I**ntegrated **S**ervice **A**ccess **P**oint (ISAP) is a powerful device for connecting all diagnosis and programming systems to the ISIS via wireless LAN (see Fig. 8). The radio standard used complies with specification 802.11n, draft 2.0. The ISAP is able to transmit and receive in the 2.4 GHz or 5 GHz radio frequency band in compliance with national legislation and guidelines.

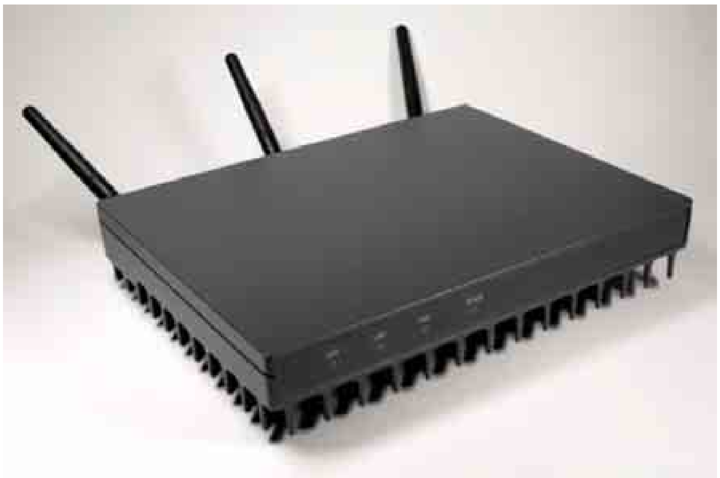


Fig. 8: Integrated Service Access Point (ISAP)

ℹ	**Information:** The term "ISAP" used here and throughout this documentation refers to the Integrated Service Access Point.

2.3 Requirements for commissioning

2.3.1 LAN workshop network, DHCP and router configuration

The following two sections will explain the two possible variants of a workshop network. The devices communicate via LAN and not via WLAN.

2.3.1.1 Dealer's network has no IP sub-networks

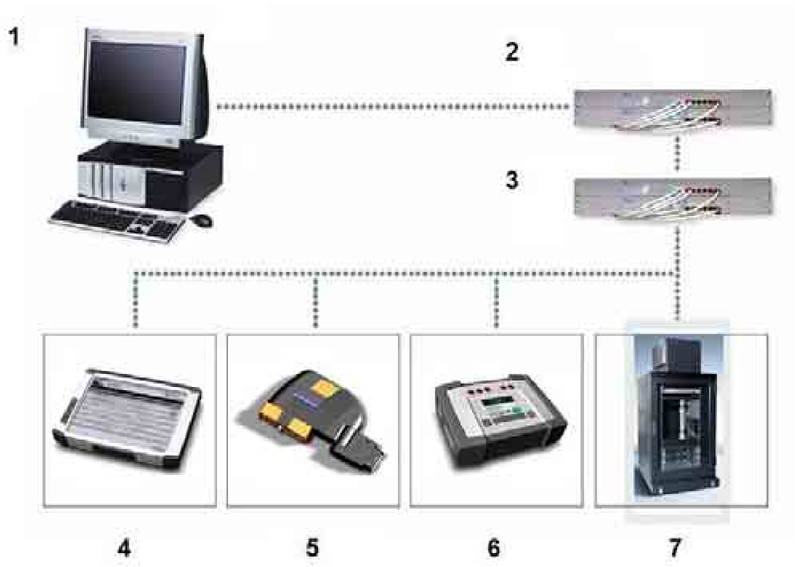


Fig. 9: Dealer's network without sub-networks

Legend (Fig. 9):

Network with workshop PC (1), layer-2 switch (2), ISIS gigabit switch (3), ISID (4), ICOM (5), IMIB (6) and ISIS in the rack in an appropriate room (7)

The dealer computer network is free of IP subnets, i.e. there is only one IP network. The IP addresses of the connected devices consequently differ, for example, only in the last IP octet (i.e. with an IP XXX.XXX.XXX.YYY in the area YYY).

The connected devices (e.g. ISID) are located in the ISIS broadcast domain[1] and can thus be connected to any LAN socket for initial or new installation.

[1] A broadcast domain is a logical group of computers in a local network in which a broadcast reaches all domain members.

Note:

If you are not yet operating a DHCP server in your workshop network, use the DHCP server integrated into the ISIS for the new workshop devices. The DHCP server on the ISIS only "operates" workshop devices from this one IP network.

Also make sure that the default gateway is always specified.

2.3.1.2 Dealer's network has a number of IP sub-networks

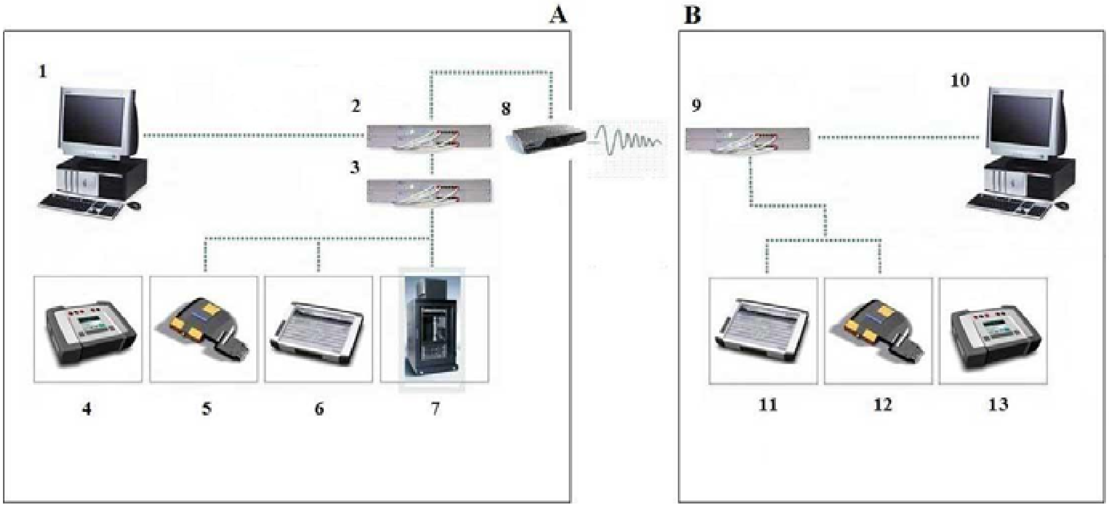


Fig. 10: Dealer's network with two sub-networks

Legend (Fig. 10):

Subnet with workshop PC (1), layer-2 switch (2), ISIS gigabit switch (3), IMIB (4), ICOM (5), ISID (6), ISIS in the rack in an appropriate room (7) and a router (8) that has been configured accordingly

Subnet B with switch (9), workshop PC (10), ISID (11), ICOM (12) and IMIB (13)

The dealer's computer network has its own IP subnets, i.e. there is a subnet in which an ISIS is located, and at least one other subnet in which there is no ISIS. The IP addresses of the connected devices, for example, differ in more than the last IP octet (i.e. with an IP XXX.XXX.XXX.YYY in the areas YYY and XXX).

The connected devices (e.g. ISID) are **not** located in the ISIS broadcast domain and can thus be connected to the network in two different ways for the initial or new installation (according to the spatial circumstances).

Connection variant 1 – no configuration of forwarding addresses:

In this case, the device (e.g. ISID) must be connected to the ISIS in the subnet. This can be achieved by connecting the device to the gigabit switch of ISIS directly or to the gigabit switch of the ISIS via a connected layer-2 switch.

Connection variant 2 – configuration of forwarding addresses:

In this case, the forwarding addresses to the routers (see Fig. 10) that separate the IP subnet of the ISID from the IP subnet of the ISIS must be configured accordingly. Then the device (e.g. ISID) must be connected to any LAN socket in the IP subnet where the router is configured.

⚠	**Note:** If you are not yet operating a DHCP server in your workshop network, use the DHCP server integrated into the ISIS for the new workshop devices. The DHCP server on the ISIS only "operates" workshop devices from the same IP network, i.e. in other subnets, you have to provide a separate DHCP server (a separate DHCP server for each subnet). It is also important to make sure that the default gateway is always specified.

2.3.2 WLAN workshop network, DHCP and router configuration

ℹ	**Information:** One ISAP or a number of ISAPs can be used for each ISIS cluster in the workshops. The number of ISAPs required must be decided in each individual case. As a rule, this depends on what areas of the workshop are to be covered by WLAN functionality.

⚠	**Note:** Each WLAN (Wireless LAN) has a configurable SSID (Service Set Identifier) to identify the radio network. It functions as the name of the network.

2.3.2.1 Workshop network with only one ISAP

In this case, a single ISAP provides the wireless connection of ISID, IMIB and ICOM to the workshop LAN of an ISIS cluster of the dealer (see Fig. 11).

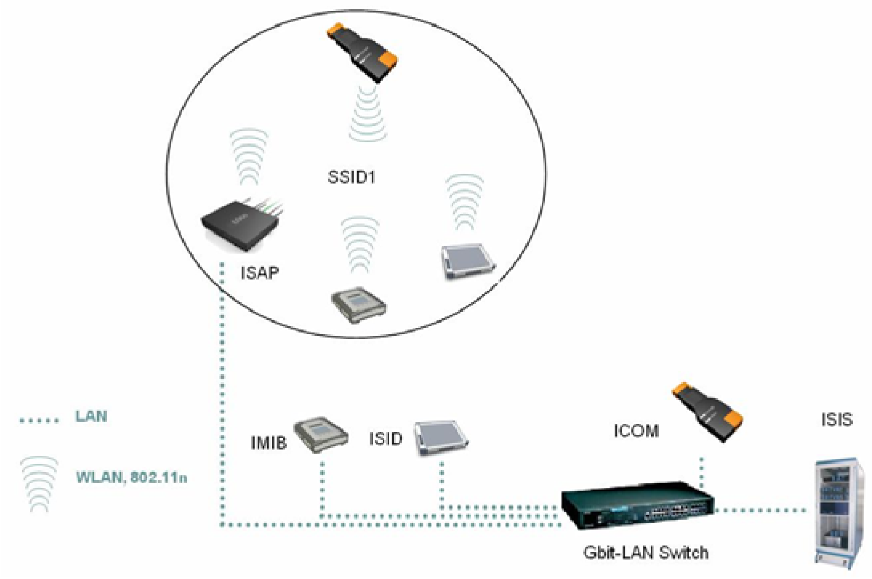


Fig. 11: Workshop network with one ISAP

2.3.2.2 Workshop network with a number of ISAPs

A number of ISAPs can be installed in the workshop. Here, a distinction is drawn as to whether the ISAPs are connected to a joint ISIS cluster or different ISIS clusters.

If the ISAPs are connected to and configured on a shared ISIS cluster, the corresponding overlap of the WLAN radio cells means that the ISID and IMIB devices can be moved between the radio cells of the ISAPs. In this case, a so-called roaming takes place (see Fig. 12).

If the ISAPs are connected to and configured on different ISIS clusters, then the ISID and IMIB devices cannot be moved between each of the radio cells because the radio networks for each ISIS cluster have different network IDs (SSIDs) (see Fig. 13).

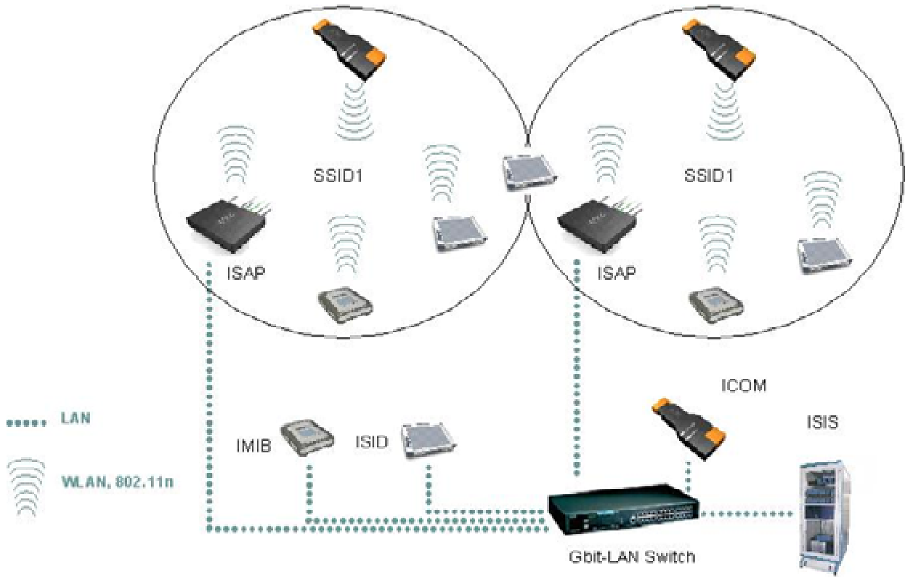


Fig. 12: Roaming in the workshop network with a number of ISAPs

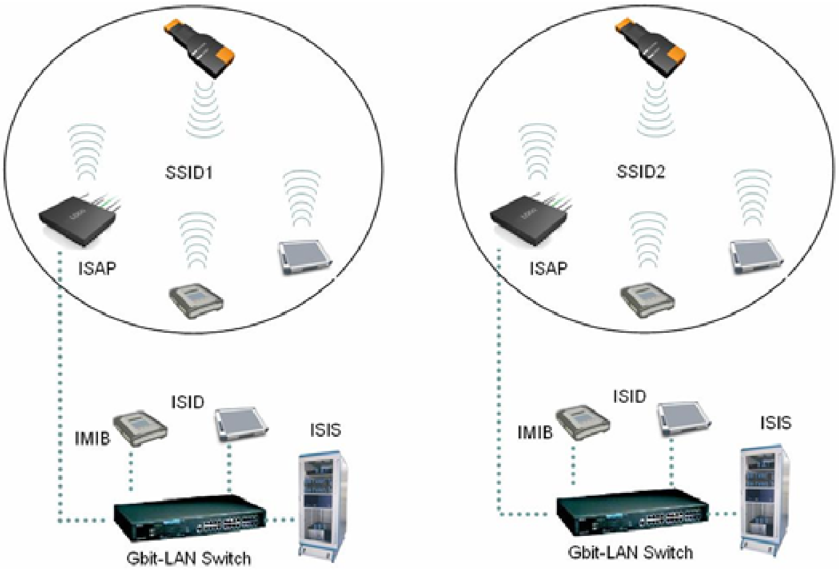


Fig. 13: Workshop network with two ISIS clusters and two ISAPs

2.3.3 Internet connection

Operation without an Internet connection is possible in principle but is not recommended because without an Internet connection, important online systems are unavailable. The consequences of absence of an Internet connection are:

- Software and data updates are not possible online: they are only possible after waiting several days for the corresponding DVD to arrive by mail.
- No access to the portals of the BMW Group, which results in a restricted function of ISPA (Integrated Service Process Application) and ISTA (Integrated Service Technical Application).

The Internet connection permits the dealer to use the necessary central services offered by the BMW Group.

2.3.4 Workshop / service PC

The following requirements must be met for commissioning the devices or using the WSM via the workshop PC:

- Windows XP Professional with Service Pack 2
- MS Internet Explorer, Version 6.0 or later
- The browser settings must enable cookies so that the ISIS can be registered from the workshop PC.

2.4 Layout of the Web interface of the WSM

The Web interface of the WSM is divided into various areas for different information (see Fig. 14). These are explained in the following subsections.

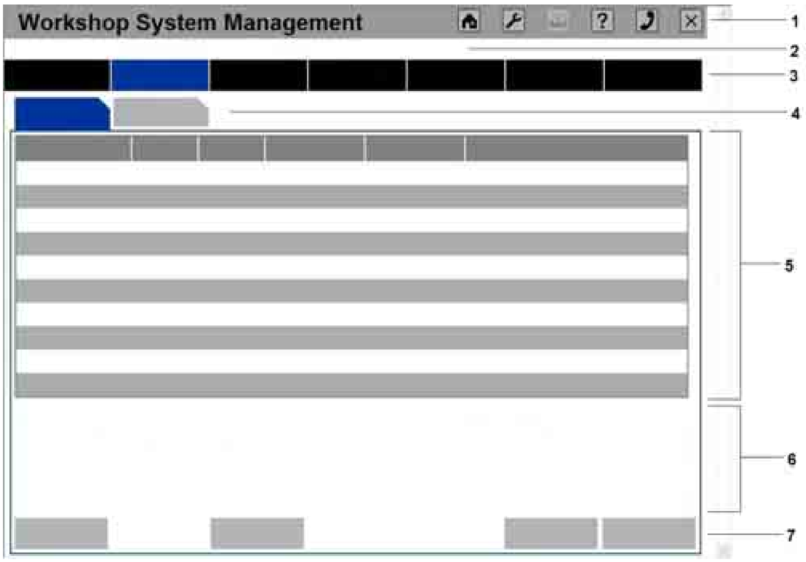


Fig. 14: Layout of the Web interface

Legend (Fig. 14):

Web page with toolbar (1), information line (2), menu (main and submenu) (3), tab bar (4), workspace (5), information area (6) and button bar (7)

2.4.1 Icon bar

The icon bar (see Fig. 14, item (1)) is visible in all screens. A short explanation of the icons and their function is provided in the following table. Detailed information is given in chapter 5.1.1.

Icon	Name	Meaning
⌂	Start page	Opens the start page
🔧	WSM settings	Used for making language settings and setting the brand of the WSM
🖶	Print	Prints the device information
?	Help	Help (this User Guide and system information)
☎	Support request	Opens the page for managing support requests (callbacks)
✕	Close	Closes the WSM – provided on certain devices

ℹ	**Information:** Since each of the symbols appears in all dialog boxes, the user can change the language setting, print the device information, access help for the present dialog box, close the window, and reach the start page from any screen.

2.4.2 Header (information line)

The header (see Fig. 14, item (2)) contains details about the selected device.

The information line does not always appear and does not always contain the corresponding details. The displays only appear if a device has been selected for which information is required or changes are to be made.

The following device information can be found in the information line:

- Device type
- Serial number
- Host name

2.4.3 Navigation (menus)

You can navigate to the individual functions of the workshop system via

(1) the main menu (first line),

(2) the submenu (second line), and

(3) the tab bar (third line).

A selected menu item or tab is highlighted in color to ensure orientation. The base color is determined by the dealer brand color. The brand is set on the 'Administration' screen (see chapter 5.1.1.2).

2.4.4 Menus and tab bar

The menu contains a main menu (see Fig. 14, item (3)) and possibly a number of submenus.

In the same way as the main menu, the active submenu is highlighted with the corresponding brand color to assist orientation.

The tab bar (see Fig. 14, item (4)) determines the individual screens of each menu that contain the corresponding information.

2.4.5 Workspace

The workspace (see Fig. 14, item (5)) can be divided into various parts and can contain information as well as input options.

2.4.6 Information area

General or additional information, e.g. the time or available updates, appears in the information area (see Fig. 14, item (6)).

2.4.7 Button bar (command line):

Depending on the workspace, the button bar contains buttons that might also be 'grayed out' if certain functions are not available.

2.4.8 Possibilities for text input (virtual keyboard)

In various screens, it can be necessary to enter text or characters.

In general, this can be done using the PC keyboard. In addition, the so-called "virtual keyboard" can be displayed (see Fig. 15). This is possible by clicking the "Display keyboard" button.

Only the buttons that represent a valid input in each function step are enabled on the virtual keyboard. Non-permitted characters cannot be selected on the virtual keyboard.

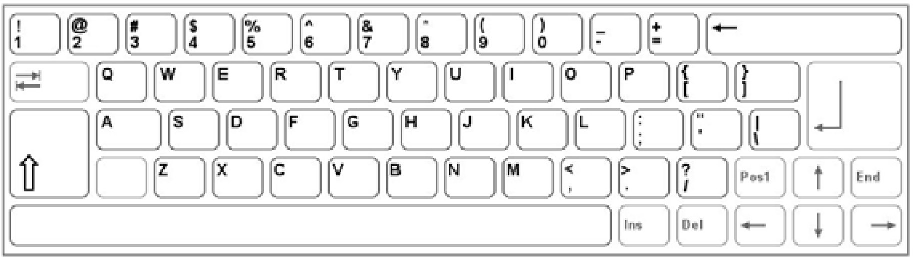

! 1 @ 2 # 3 $ 4 % 5 ^ 6 & 7 * 8 (9) 0 _ - + =
Q W E R T Y U I O P { [}]
A S D F G H J K L : ; " ' | \
Z X C V B N M < , > . ? /
Pos1
End
Ins
Del

Fig. 15: Virtual keyboard

3 Commissioning / new installation of the individual devices

⚠	**Note:** Please make sure that the corresponding requirements (described in chapter 2.3) have been met before commissioning.

3.1 Integrated Service Information Server (ISIS)

⚠	**Note:** Please bear in mind that both the complete installation and the registration must be successfully concluded in order for the ISIS, the new generation devices (ISID, ICOM, IMIB), and the applications to be used to the full extent.

3.1.1 Requirements for commissioning / new installation

Before you start commissioning the ISIS, check whether the following conditions have been met:

- There is a connection to the workshop network
- For online dealers: there is a connection to the Internet (this is not required for offline dealers)
- The latest version of the DVD installation medium is available
- The access data (user name and password) of the responsible BMW dealer portal is available (nor required for offline dealers or independent dealers)
- A pen and notepaper are available for noting down configurations and IP addresses as needed
- 17 static and 5 dynamic IP addresses must be available for the ISIS (advanced Details can be found in the "ISIS Cookbook"[2])
- A commercially available PC (with installed browser) is necessary for configuration of the ISIS
- The ISIS Connectivity Checker Tool[3] must have been run successfully to check the Internet connection and login data for the dealer portal.

[2] The ISIS Cookbook provides assistance in preparation of the technical infrastructure and can be found on Servolution and/or is distributed via the Market Community.

[3] The ISIS Connectivity Checker Tool (ICC Tool) checks, among other things, the usability of IP addresses for the ISIS. It can be found on Servolution and/or is distributed via the Market Community.

⚠	**Note:** Please check whether the UPS is switched on. If it is not, switch it on as described in the following point.

- If the **uninterruptible p**ower **s**upply (UPS) located in the ISIS rack has not already been switched on, then it must be switched on using the button (1) (see Fig. 16).

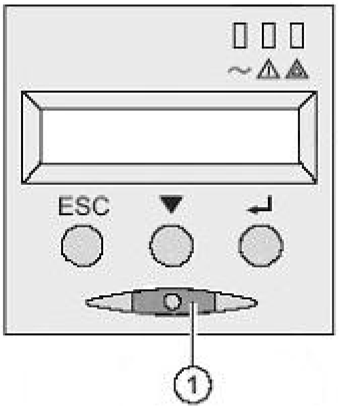


Fig. 16: UPS operating section

3.1.2 Installation process

When installing 2 ISISs, it is possible to run these largely in parallel. The time sequence is shown in the following diagram (see Fig. 17).

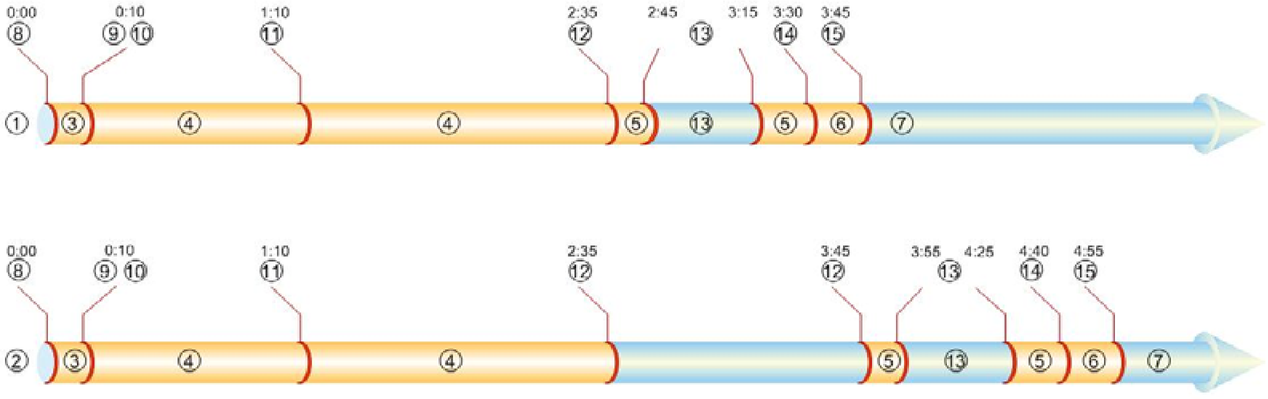


Fig. 17: Time sequence of the ISIS installation

Legend (Fig. 17**):**

ISIS1 master (1), ISIS2 slave (2), Wiping (3), Installation (4), Configuration (5), Registration (6), Normal operation (7), Inserting the WIPE CD (8), Ejecting the WIPE CD (9), Inserting the ISIS DVD (10), Ejecting the ISIS DVD (11), Display of the temporary IP address (12), Restarting the ISIS and changing the IP address (13), Starting the registration (14) and Ending the registration (15); Time sequentially indicated in hour:minute format

3.1.3 Selection of the installation type

The ISIS is delivered in a preinstalled state. However, if a new installation of a server plug-in module is required because there is a new full version or due to a complete system failure, two variants are possible for the new installation. These are explained in the following two subsections.

3.1.3.1 Installation of a new base DVD with adoption of the configuration

⚠	**Note:** In the case of a new installation of ISIS, please note that the first server plug-in module must be configured with the second server plug-in module switched off. For the subsequent new installation of the second server plug-in module, the first server plug-in module that has already been installed and configured must be left on.

ℹ	**Information:** It is not necessary to register the ISIS after the installation because the data is adopted.

ISIS is already switched on:

- Insert the base DVD (see Fig. 18) and close the DVD drive

Fig. 18: Inserting the base DVD in the ISIS DVD drive

- Restart the ISIS via the WSM by selecting the device in the "System Overview" in the "Overview" tab and clicking the "Restart Device" button (more detailed information on restarting can be found in chapter 5.1.6)
- Continue with the steps from chapter 3.1.4

ISIS is switched off:

- Switch on ISIS by pressing the button (1) (see Fig. 19)

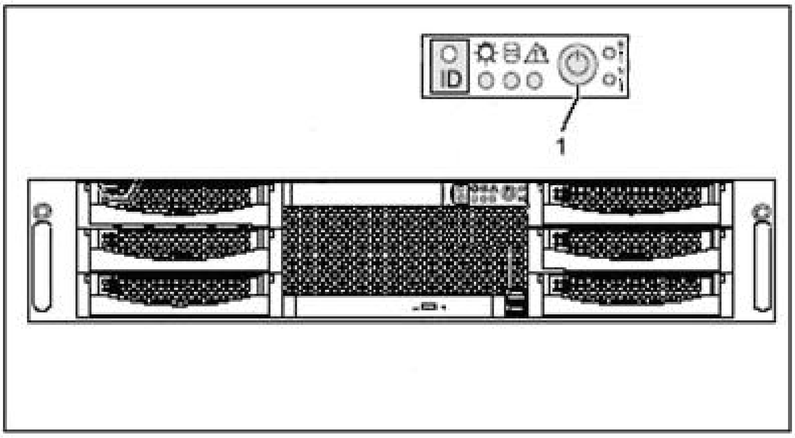


Fig. 19: Front of the ISIS

- Insert the base DVD into the DVD drive (see Fig. 18) and close the drive again
- Switch off the server by pressing the button (1) (see Fig. 19) for at least 3 seconds.
- Switch on the server again by pressing the button (1) (see Fig. 19)
- Continue with the steps from chapter 3.1.4

3.1.3.2 Installation of a new base DVD without adopting the configuration by means of Wipe CD

If the present configuration of the ISIS is not to be used any longer, a so-called Wipe CD is used. This enables automated removal of all components of the system used to date.

⚠	**Note 1:** Before an ISIS is wiped, it must be unregistered according to the steps from chapter 5.1.3.7 to enable a renewed registration after the new installation.

⚠	**Note 2:** If a Wipe CD is used, **all the data** (including the database backups) on the hard drive of the ISIS is **deleted.** Please make sure that you really want to do this. We therefore recommend you make a data backup on an external share beforehand.

⚠	**Note 3:** Wiping must be carried out on both server plug-in modules.

If the hard drive of an ISIS system must be deleted (e.g. the installation of a base DVD can require this), then proceed according to the following steps, depending on state of the ISIS (switched on or switched off):

ISIS is switched on:

- Insert the Wipe CD (as shown in Fig. 18) and close the DVD drive
- Restart the ISIS via the WSM by selecting the device in the "System Overview" in the "Overview" tab and clicking the "Restart Device" button (more detailed information can be found in chapter 5.1.6)

ISIS is switched off:

- Switch on ISIS by pressing the button (1) (see Fig. 20)

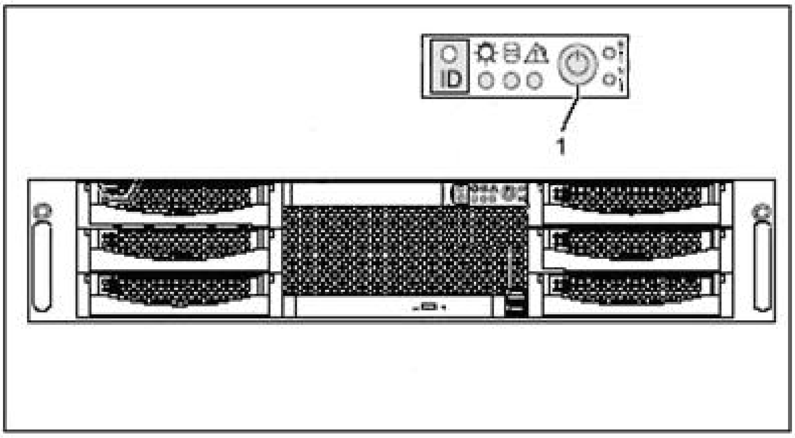


Fig. 20: Front of the ISIS

- Insert the Wipe CD into the DVD drive (as shown in Fig. 18) and close the DVD drive.
- Switch off the server by pressing the button (1) (see Fig. 20) for at least 3 seconds.
- Switch on the server again by pressing the button (1) (see Fig. 20)

Remaining procedure:

After a few seconds, the software of the Wipe CD is executed automatically. Wiping takes about 10 minutes. The CD is then ejected automatically and the prompt "Insert ISIS DVD" appears on the ISIS display.

The contents of the hard drive have now been deleted and the server can be reinstalled from the base DVD.

Proceed as follows:

- Insert the base DVD into the DVD drive and close the DVD drive.

The new installation is described in the following chapter.

3.1.4 Installation of the ISIS

⚠	**Note 1:** Please bear in mind that the complete installation of an ISIS without applications up to achievement of the configuration can take approx. 145 minutes.

⚠	**Note 2:** When configuring the first server plug-in module, it is important to make sure that the second server plug-in module is switched off or is still in the installation phase. For the subsequent configuration of the second server plug-in module, the first server plug-in module that has already been installed and is online must be left on.

ℹ	**Information:** In the course of the installation, the server is automatically restarted several times.

To install an ISIS, perform the following steps:

- If the ISIS display is not visible, then proceed as follows:

  Lightly pressing against the front (3) (see Fig. 21) move the display outwards slightly.
  Then carefully pull the display out gradually until you are able to fold it downwards. The angle between the display and ISIS front should be set in such a way that the output can be read without difficulty.

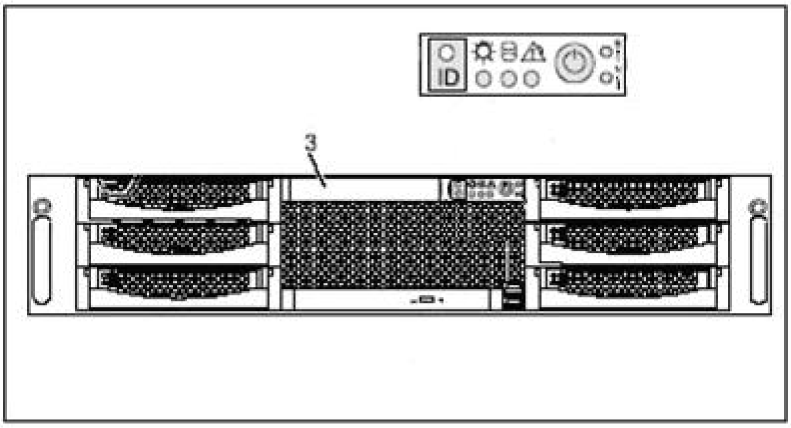


Fig. 21: ISIS front

- The data is copied onto the hard drive within about 60 minutes.
- When this time has elapsed, the DVD is automatically ejected.
- The DVD must be removed from the drive and the drive must be closed. Then the server installs the software and generates other text outputs on the small display (see chapter 10). This can take approx. 85 minutes.
- As soon as the server remains switched off, the basic installation is finished.
- Now the server has to be switched on again. Wait until the server has completely powered up (the word 'SETUP' appears on the display, followed by the IP address of the server).

3.1.5 Reading off and noting down the ISIS IP address

- As soon as an IP address appears on the display of the ISIS (see Fig. 22), it should be noted down.

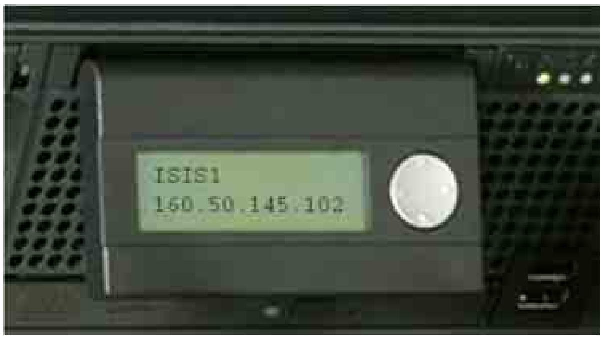


Fig. 22: Reading the ISIS IP

- If the IP address of the ISIS starts with 169[4], continue with the instructions in chapter 3.1.6. Otherwise, skip directly to the steps in chapter 3.1.7.

[4] The ISIS expects the IP address of an external DHCP server. If no address of DHCP server is available, then the ISIS automatically receives an address from the range of the "IP autoconfiguration", which starts with 169.

3.1.6 Configuration of the workshop PC for subsequent ISIS configuration

If the IP address of the ISIS starts with 169 (this is the case if no DHCP server is configured in the workshop network) or if an error has occurred during activation of the browser (see chapter 3.1.7), then perform the following steps:

- Access the Control Panel of the workshop PC

  On a Windows computer, click "Start" and then on "Control Panel" (see Fig. 23).

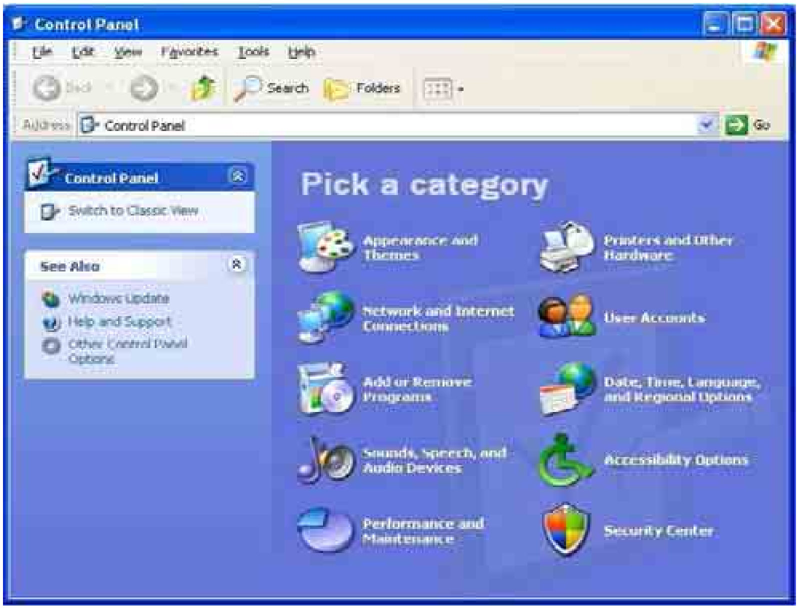


Fig. 23: Windows Control Panel of the workshop PC

- Selection of the network environment

  Selecting "Network and Internet Connections" and then "Network Connections" takes the user to the corresponding list of them.

- Open the properties of the network connection for the local network (LAN)

  Right-clicking the symbol for the local network (see Fig. 24) and selecting the entry "Properties" opens the dialog box for setting the general properties of the LAN connection (see Fig. 25).

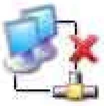
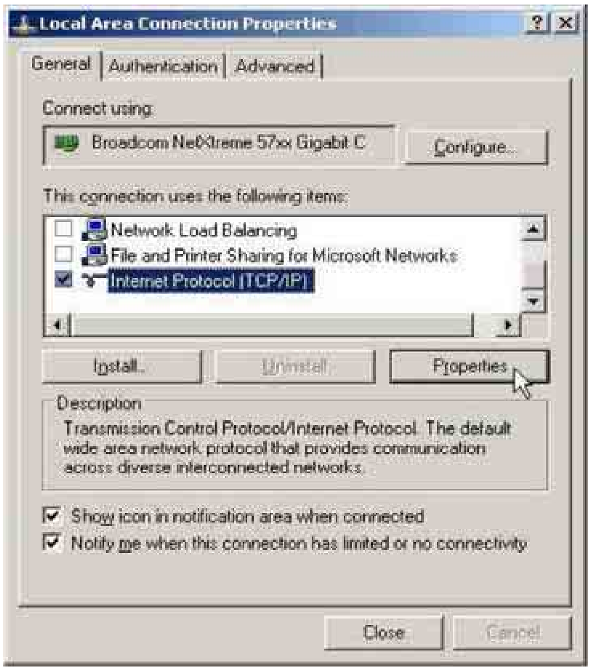


Fig. 24: LAN (Local Area Network)



Local Area Connection Properties

General | Authentication | Advanced

Connect using:

Broadcom NetXtreme 57xx Gigabit C — Configure...

This connection uses the following items:

□ Network Load Balancing
□ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Install... | Uninstall | Properties

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

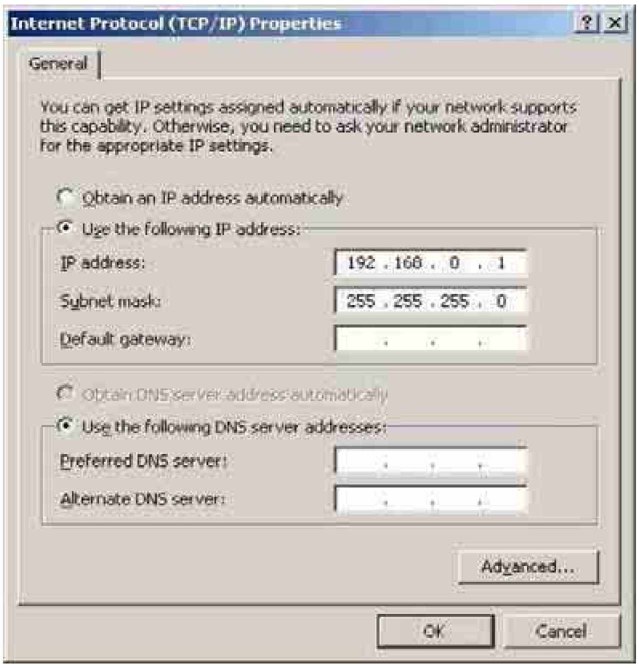
☑ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

Close | Cancel

Fig. 25: LAN properties of the workshop PC

- Open the properties of the TCP/IP protocol

  Selecting the "Internet Protocol (TCP/IP)" entry and clicking the "Properties" option opens the "Properties of Internet Protocol (TCP/IP)" dialog box (see Fig. 26).



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 0 . 1
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

Advanced...

OK | Cancel

Fig. 26: TCP/IP properties of the workshop PC

- Write down the values already configured in the dialog boxes. The values will be used accordingly at a later time (see chapter 3.1.9).
- Select the DHCP mode in the TCP/IP protocol by selecting "Obtain an IP address automatically" (see Fig. 26).
- The selection is confirmed by clicking "OK" and the opened dialog box is closed by clicking "Close".
- Please make sure that no check mark has been placed next to “Use Proxy Server for LAN (…)” in Internet Explorer at Extras -> Internet Options -> Connections -> Settings.

3.1.7 Accessing the ISIS setup program

The network board of the PC must be connected to the switch with a patch cable.

Start a browser on the workshop PC. In the address line, enter the IP address that appeared on the display of the ISIS and was noted down (see Fig. 27).

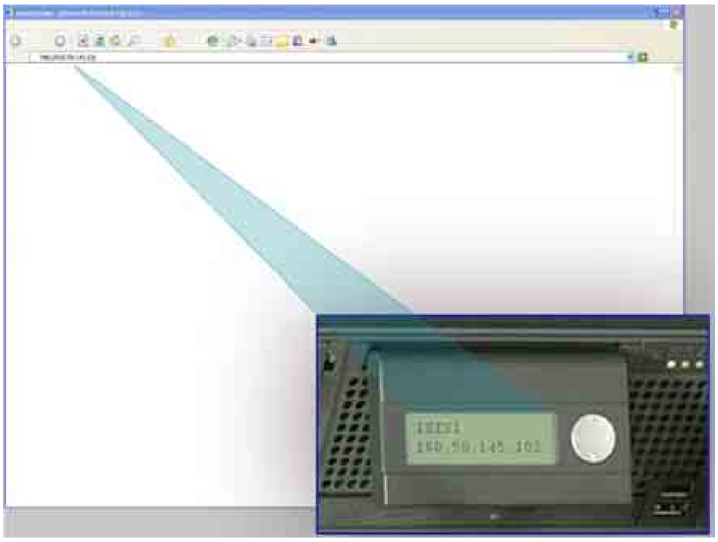


Fig. 27: Accessing the ISIS setup program

If the entered URL is confirmed, then the first dialog box of the WSM configuration wizard for setting up the system appears and you can proceed immediately to the steps of the following chapter.

But if an error message appears, first check to make sure that the correct IP address was entered. If it was entered correctly and the error message still appears, then check the steps from chapter 3.1.6 once again.

3.1.8 Configuration of the ISIS (part 1)

ℹ	**Information:** The ISIS is configured using the WSM Configuration Wizard.

The WSM configuration wizard can be terminated at any time by clicking the "Close" icon. This deletes all of the settings that have been entered up to this point and when the WSM configuration wizard is restarted the first dialog box is displayed again.

Selecting the "Help" function displays this WSM User Guide.

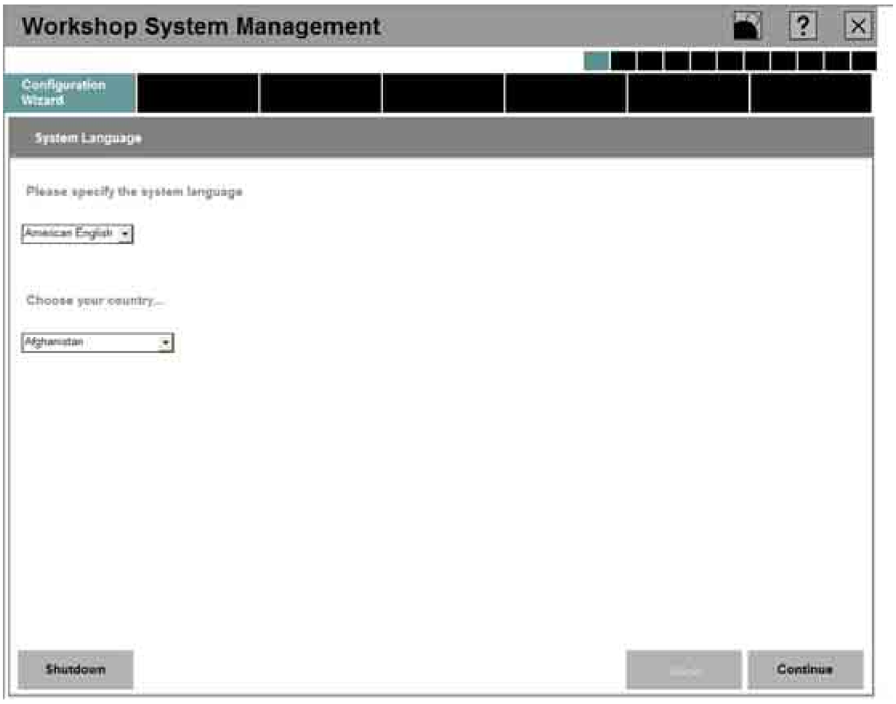
The "Master-slave mode" display allows you check the mode of the ISIS that is currently being configured. It cannot be selected and is thus only used for information purposes.

Icon	Name	Meaning
	Master-slave mode	Indicates that the ISIS is in the master[5] mode.
	Master-slave mode	Indicates that the ISIS is in the slave mode[6].
?	Help	Indicates this WSM User Guide.
☒	Close	Terminates the WSM Configuration Wizard.

[5] The first installed ISIS is referred to as the master. This is indicated by (P) or *.

[6] The second installed ISIS is referred to as the slave. This is indicated by (S). On configuration, the slave automatically adopts the settings of the master.

3.1.8.1 Setting the language and country (startup page of the WSM Configuration Wizard)



Please specify the system language

American English

Choose your country...

Afghanistan

Fig. 28: Configuration of the language and country

In the present dialog box (see Fig. 28), the desired system language is selected for the WSM on the ISIS. To set the relevant language, click the small arrow and select the corresponding language from the specified list.

It is also necessary to select the corresponding country in which the dealer is located.

Clicking the "Continue" button saves the language and the user is then taken to the subsequent dialog boxes. These are displayed in the selected language.

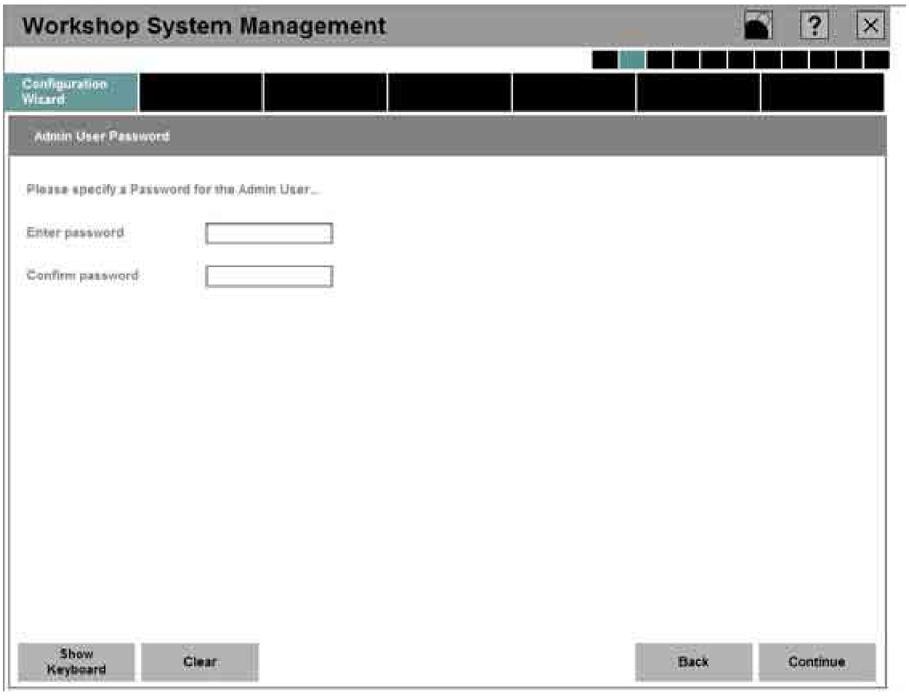
⚠	**Note:** These settings are mandatory in order to carry out a successful online registration.

ℹ	**Information:** Setting the language and country automatically specifies the format for the date and time.

3.1.8.2 Setting the password for the Web interface

Information:

To avoid later confusion, the same password should be set for ISIS1 and ISIS2.



Admin User Password

Please specify a Password for the Admin User...

Enter password

Confirm password

Fig. 29: Configuration of the password

There are two reasons for setting an administrator password (see Fig. 29):

First, to safeguard the system against unauthorized changes to the configuration and second, to enable the subsequent setup of workshop PCs and other workshop devices. This password is requested for accesses to protected areas and can also be changed later (see chapter 5.1.17).

The password must consist of at least eight characters (in upper and lower case letters) and should contain both letters and numbers. German 'umlauts' such as ä, ö, ü or special characters such as $ or § not permitted.

The password must be entered in the upper input field. Repetition of the password in the lower input field confirms the intended password.

Clicking the "Back" button takes the user to the previous screen. In this case, the password is not saved.

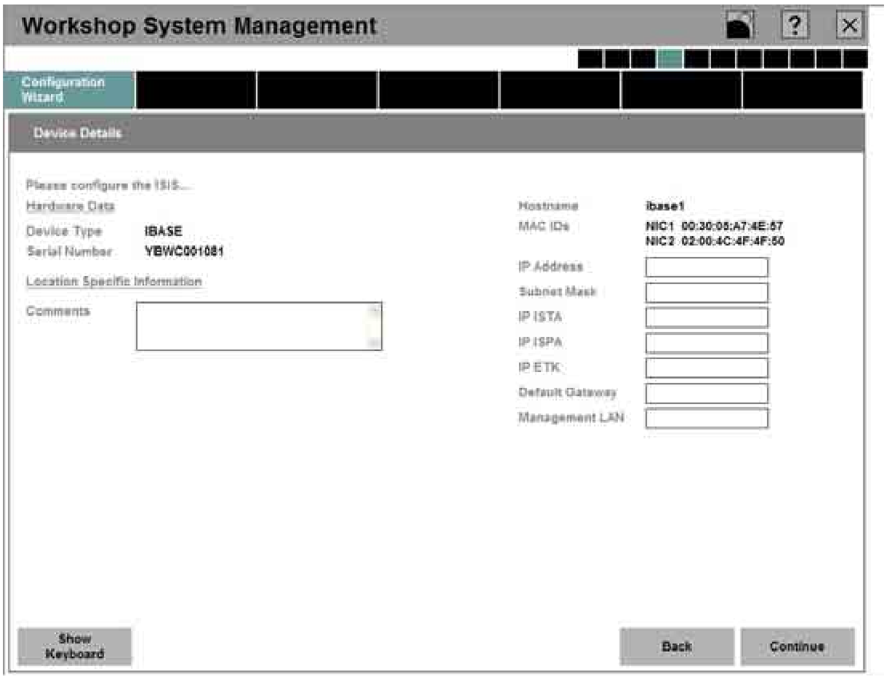
If the user is satisfied with the password entry, the next screen is reached by clicking the "Continue" button.

Click the "Clear" button to delete a password that has already been entered.

Information:

The WSM can also be used by normal users because read access to certain areas is also possible without a password.

3.1.8.3 Configuration of the IP addresses of the device



Please configure the ISIS...

Hardware Data

Device Type IBASE
Serial Number YBWC001081

Location Specific Information

Comments

Hostname ibase1
MAC IDs NIC1 00:30:05:A7:4E:57
NIC2 02:00:4C:4F:4F:50

IP Address
Subnet Mask
IP ISTA
IP ISPA
IP ETK
Default Gateway
Management LAN

Fig. 30: Configuration of the IP addresses of the device

This dialog box (see Fig. 30) contains important device information and also has input fields to specify certain device information and data.

The following device details are determined and displayed automatically by the system as user information:

- *Hardware data* - device type and serial number
- *Host name* (assigned by the system)
- *MAC IDs* (hardware network data)

The following data should be specified in the input fields specifically designed for the purpose:

- *Comments* – The user has the option of writing a legend in his or her own words, e.g. to draw attention to problems.
- *IP addresses* – IP addresses must be assigned both to the host and the applications ISTA, ISPA and EPC. The subnet mask, the default gateway, and the management LAN also receive an IP address in the course of entries.[7]

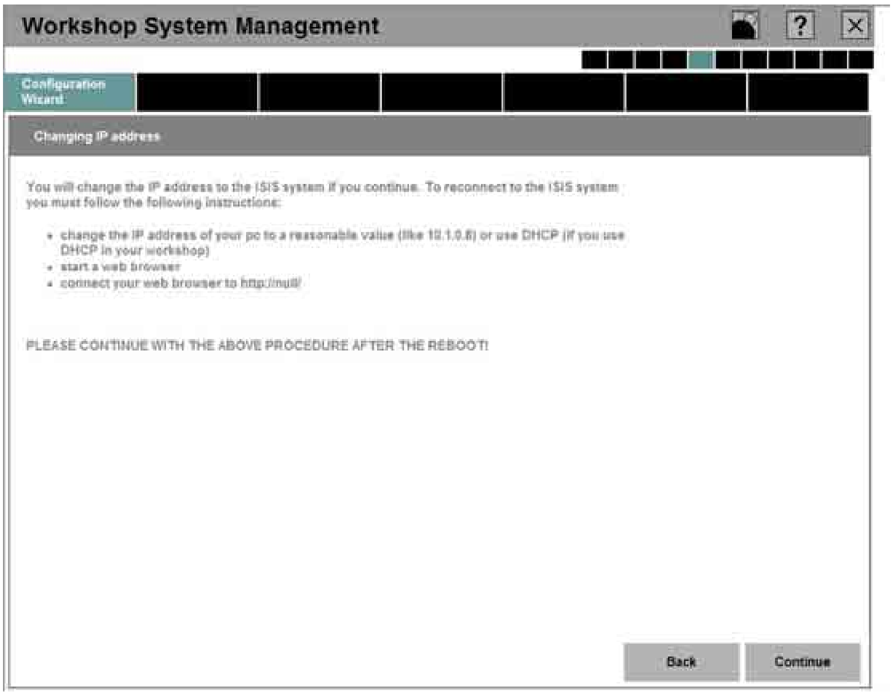
  The "ISIS Cookbook" provides support for selection of the IP addresses.

[7] A network board in the ISIS for technical support on site at the dealer.

⚠	**Note 1:** Please note that five IP addresses not yet used in the network are to be used for each server plug-in module. The network mask and the default gateway are taken from the specifications for a valid network configuration of the computer network. In case of doubt, contact the service provider or person responsible for IT at the dealership.

⚠	**Note 2:** Changing IP addresses after the fact has repercussions on the new generation devices in other subnets. Communication across subnet borders is no longer assured as a matter of course. In the worst case scenario, the devices in the reconfigured ISIS network must be briefly logged on to the ISIS.

Clicking the "Back" button takes the user to the previous screen; clicking "Continue" opens the following dialog box (see Fig. 31).



You will change the IP address to the ISIS system if you continue. To reconnect to the ISIS system you must follow the following instructions:

- change the IP address of your pc to a reasonable value (like 10.1.0.8) or use DHCP (if you use DHCP in your workshop)
- start a web browser
- connect your web browser to http://null/

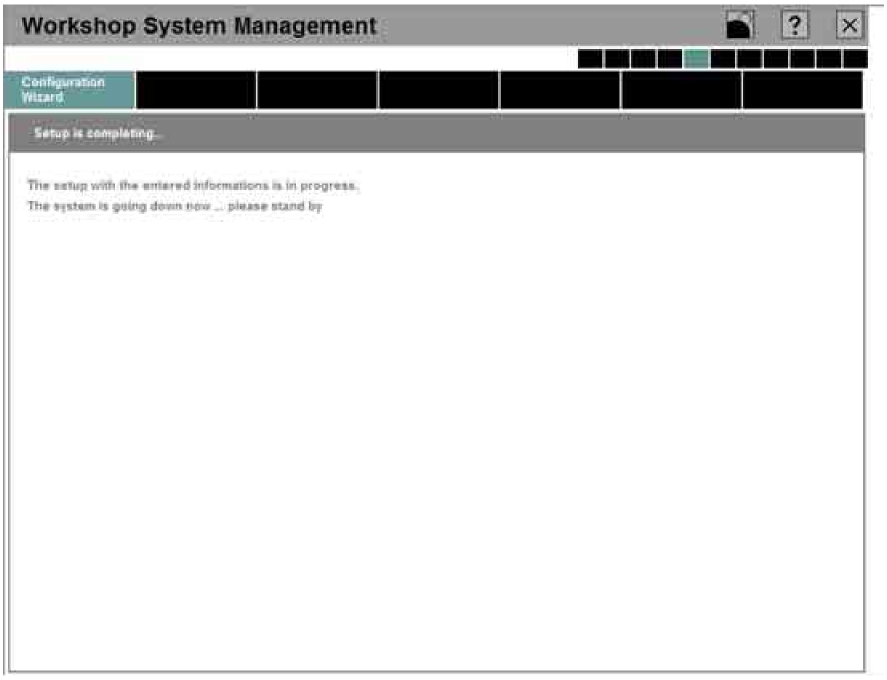
PLEASE CONTINUE WITH THE ABOVE PROCEDURE AFTER THE REBOOT!

Fig. 31: Confirmation of the network configuration

In this dialog box (see Fig. 31), the other steps to be carried out next are listed.

Clicking the "Continue" button opens the following dialog box (see Fig. 32), thus concluding the first part of the ISIS configuration. The ISIS is integrated into the network environment.

ℹ	**Information:** It can take up to 30 minutes for the server to finish the configuration process. During this time, no operations need to be carried out the ISIS. After the subsequent new start, the new IP of the ISIS can be seen on the display.



Setup is completing...

The setup with the entered informations is in progress.
The system is going down now ... please stand by

Fig. 32: End of the configuration (part 1)

3.1.9 Recovery of the original workshop PC configuration

If the workshop PC configuration was changed in the course of commissioning and installing the ISIS (i.e. the steps in chapter 3.1.6 were carried out), then these settings must be reset.

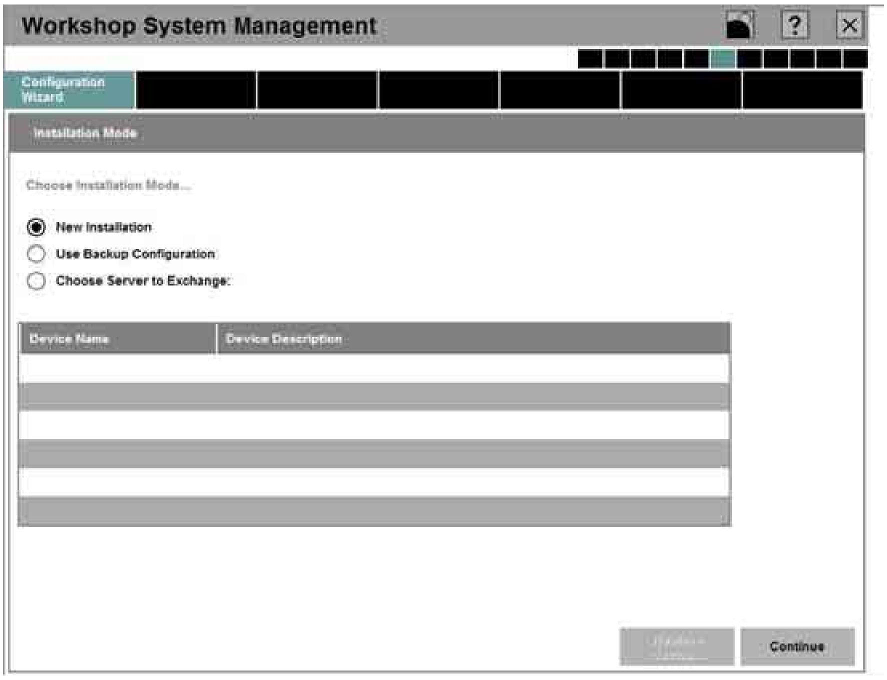
To do so, items 1-7 from chapter 3.1.6 must be repeated. In the dialog box (see Fig. 26), switch from the DHCP mode to the original setting and once again enter the values fixed in advance in writing (see item 5 in chapter 3.1.6).

3.1.10 Configuration of the ISIS (part 2)

⚠	**Note:** Wait until the new IP address appears in the display of the ISIS before you begin this part of the configuration.

To continue configuration of the ISIS, open a browser and enter the IP set for the ISIS in chapter 3.1.8.3 in the address line of the browser. Then the following dialog box appears (see Fig. 33).

3.1.10.1 Selection of the installation mode



Installation Mode

Choose Installation Mode...

● New Installation
○ Use Backup Configuration
○ Choose Server to Exchange:

Device Name	Device Description

Fig. 33: Selection of the installation mode

The installation mode is set based on this dialog box (see Fig. 33). There are three possibilities here:

- <New Installation>
  This mode is selected if this is an initial installation.

- <Use Backup Configuration>
  This mode is selected for two reasons:
  - First, if settings that have already been made are to be adopted, e.g. after a server failure
  - Second, if the hard disk content is not to be deleted under any circumstances in the case of a new installation (Wipe CD has not been used – see chapter 3.1.3.1).

- <Choose Server to Exchange>
  This mode is selected if defective hardware is replaced with new hardware (mainboard or entire plug-in module). It is important here that it is necessary to switch off the server hardware to be replaced. Selecting the server to be replaced means that the new server is installed in the identical fashion.

Clicking the "Continue" button takes the user to the next screen.

ℹ	**Information:** The configuration saved by the user and the server exchange cannot currently be selected.

3.1.10.2 Configuration of the network

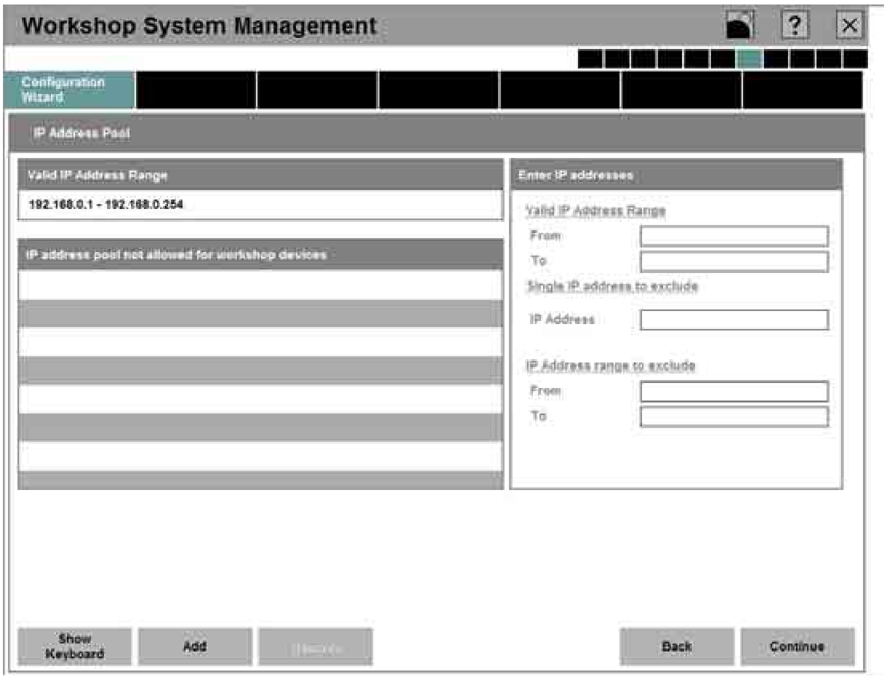
Note:

When using DHCP, make sure that no IP address is assigned more than once. The DHCP server be notified of which IP addresses are explicitly excluded and which IP address ranges are to be permitted or excluded so as to prevent IP conflicts with manually assigned IP addresses.

No entries are required here during installation of the second ISIS.

Information:

If the ISIS is not used as the DHCP server, the 2 screens "IP Address Pool" (see Fig. 34) and "DHCP" (see Fig. 35) can be skipped without input by clicking "Continue".



Workshop System Management

IP Address Pool

Valid IP Address Range: 192.168.0.1 - 192.168.0.254

IP address pool not allowed for workshop devices

Enter IP addresses

Valid IP Address Range
From
To

Single IP address to exclude
IP Address

IP Address range to exclude
From
To

Fig. 34: Configuration of the IP addresses

In this dialog box (see Fig. 34), the impermissible IP addresses can be set or unusable IP address ranges can be specified.

On the basis of the previously entered addresses for the ISIS, a proposal for the valid IP address range is calculated automatically. This range cannot be changed directly by the user; it can only be changed by the exclusion of IP addresses.

There are 2 different possibilities for entering corresponding IP addresses:

- Individual IP address Individual IP address that must not be used
- IP address range Start and end address of the non-permitted IP range

Since the IP addresses specified for the two ISIS systems are not automatically excluded, these 17 addresses (11 IP addresses for the ISIS and 6 IP addresses for the applications) still have to be manually excluded via "IP Address Range" (from - to, since this is a consecutive range).

If the addresses 192.168.0.10 – 192.168.0.26 are used for the ISIS, for example, then the address in the field "From" must be 192.168.0.10 and the address in the field "To" must be 192.168.0.26.

Clicking the "Add" button adds the entered addresses to the IP address pool. This can be repeated any number of times for various inputs. When doing so, make sure that the IP address of the gateway is not listed as excluded.

If an IP address or address range is to be removed from the list, then the entry must be highlighted and can be deleted from the list by clicking the "Remove" button.

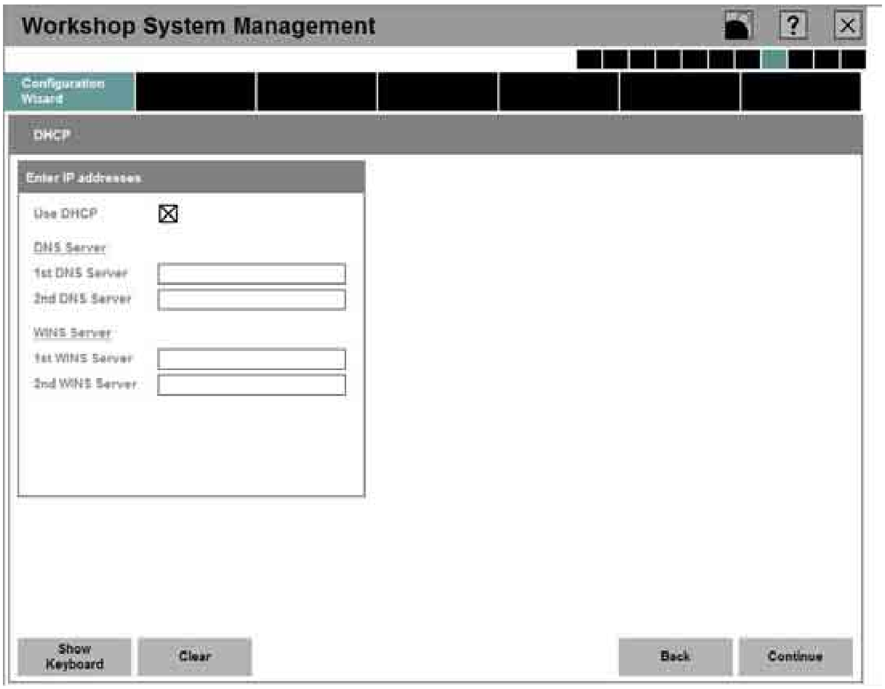
To enter the next dialog box, simply click the "Continue" button or click the "Back" button to go back to the previous screen.

3.1.10.3 Configuration of the DHCP system (dynamic IP allocation)

⚠	**Note 1:** A DHCP server is a necessary precondition for integration of the new generation devices (ISID, ICOM, ISAP) into the workshop network! This configuration is not required for installation of the second ISIS. Click "Next" without making any settings.

⚠	**Note 2:** Please also follow the instructions on how to use DHCP in the chapter 2.3.1.

Configuration:



Workshop System Management

Configuration Wizard

DHCP

Enter IP addresses

Use DHCP ☒

DNS Server

1st DNS Server

2nd DNS Server

WINS Server

1st WINS Server

2nd WINS Server

Fig. 35: Configuration of the automatic IP allocation

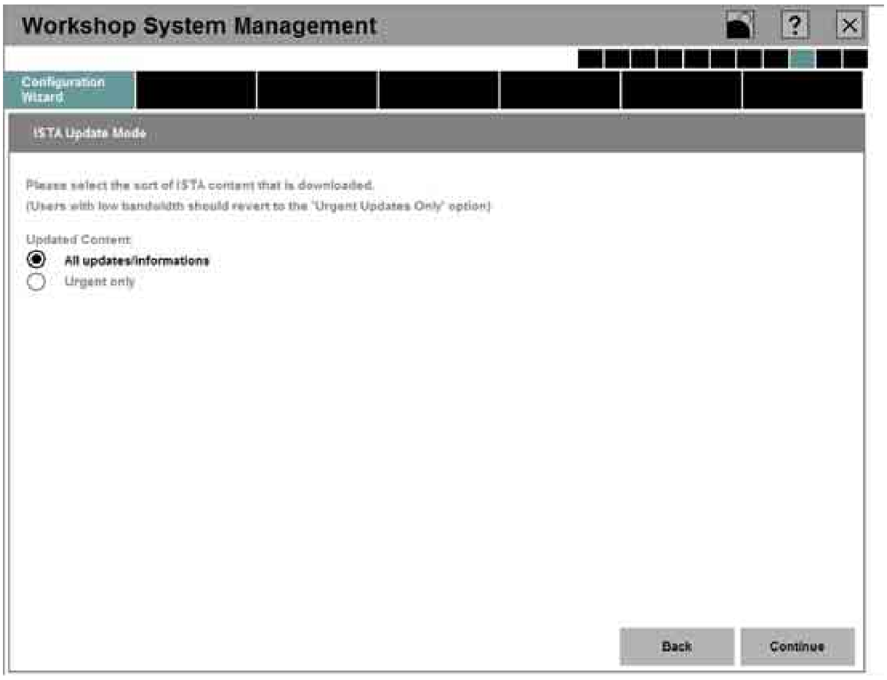
Selecting "Use DHCP" (see Fig. 35) activates the ISIS DHCP server. However, it is only permissible to activate the dynamic address assignment if no other DHCP server (e.g. Windows 2000/2003 server, ISDN or DSL router) is active within the network (the subnet).

Under DNS Server, two different servers can be specified for the **D**omain **N**ame **S**ystem and under WINS Server two different servers can be specified for the **W**indows **I**nternet **N**aming **S**ystem.

Clicking the "Back" or "Continue" buttons takes the user to the previous or next screen.

3.1.10.4 Configuration of the update mode

The Update mode defines the amount of data to be downloaded for the applications via online update.



Please select the sort of ISTA content that is downloaded.
(Users with low bandwidth should revert to the 'Urgent Updates Only' option)

Updated Content:
● All updates/informations
○ Urgent only

Fig. 36: Configuration of the update mode

In this dialog box (see Fig. 36), the type and scope of the services to be used must be specified. If you are interested in obtaining all of the updates and information relating to ISTA online, click "All Updates/Information". But if you only want access to urgent information and updates that are essential for operation of the ISIS, then select "Only urgent updates/information".

i	**Information:** Currently, only the entry "All Updates/Information" can be selected.

To move to the previous or next screen, click the "Back" or "Continue" button.

3.1.11 Registration of the ISIS

!	**Note 1:** For the registration, please also take into account the remarks on the type of registration in chapters 5.1.3.1, 5.1.3.2, and 5.1.3.3.

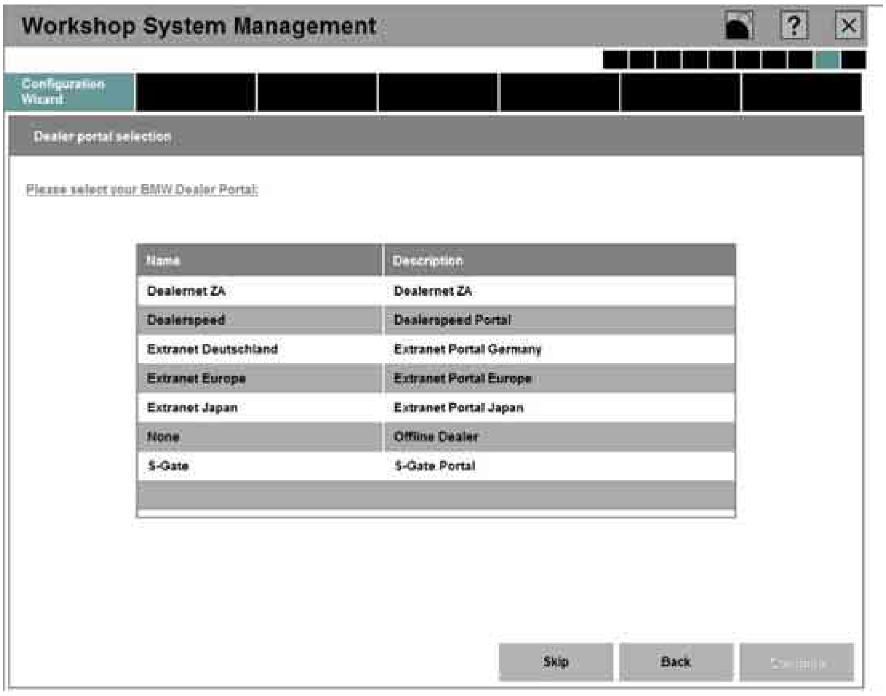
!	**Note 2:** The registration can be skipped during the configuration by clicking the "Skip" button (see Fig. 37). But please remember that the registration must then be carried out at a later time. Otherwise, the ISIS can only be used to a limited extent.

After configuration of the first ISIS has been carried out, the next step involves the online or offline registration (see chapter 3.1.11.1) of this ISIS at the BMW Group.

Internet access is required for the online registration procedure. The authorized dealer must have this access so that the registration data can be exchanged between the dealer and BMW via the Internet.

If no Internet access is available, then an offline registration (see chapter 3.1.11.2) must be made via fax using a registration form.

Selection of a dealer portal:



Please select your BMW Dealer Portal:

Name	Description
Dealernet ZA	Dealernet ZA
Dealerspeed	Dealerspeed Portal
Extranet Deutschland	Extranet Portal Germany
Extranet Europe	Extranet Portal Europe
Extranet Japan	Extranet Portal Japan
None	Offline Dealer
S-Gate	S-Gate Portal

Fig. 37: Selection of a portal

In a first step (see Fig. 37) click to select the BMW dealer portal responsible for the user region.

⚠	**Note:** For an offline dealer, select the portal "None" and run the offline registration (see chapter 3.1.11.2).

Clicking the "Continue" button takes the user to the next screen.

3.1.11.1 Online registration

Note 1:

This type of registration can only be carried out if an Internet connection and a dealer portal login are available.

Note 2:

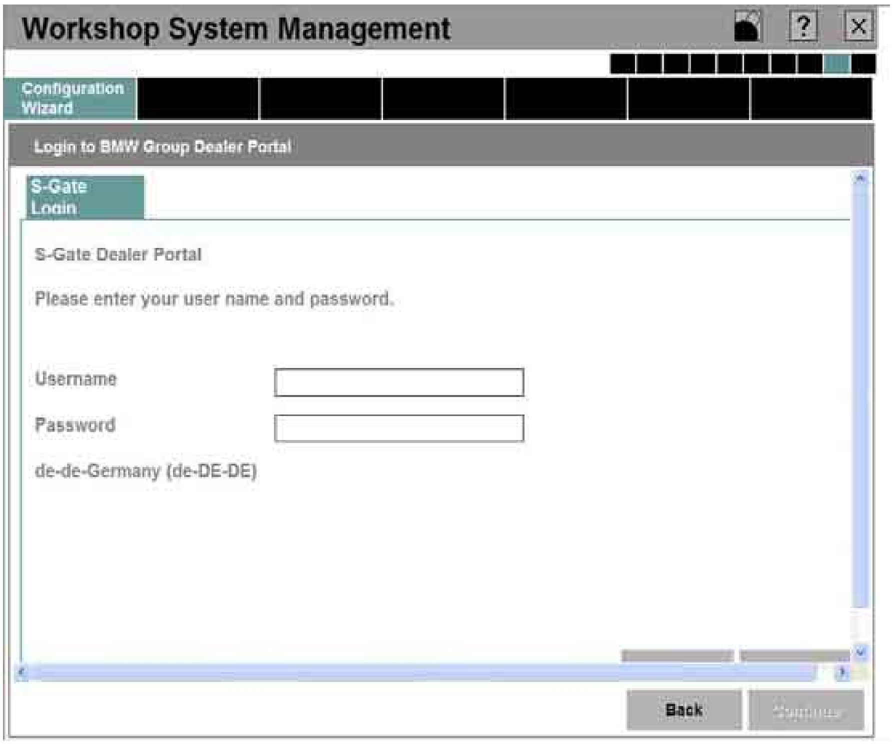
Before the online registration, check whether the password is still valid.

Information:

In the rest of this guide, a dealer who has made this type of registration is also referred to as an "online dealer" and all of the new generation devices that are registered for this ISIS are also registered online.

Login to the dealer portal:

The following procedure is described as an example for the dealer portal "S-Gate". All other dealer portals offer the same or similar screens for completion.



S-Gate Dealer Portal

Please enter your user name and password.

Username

Password

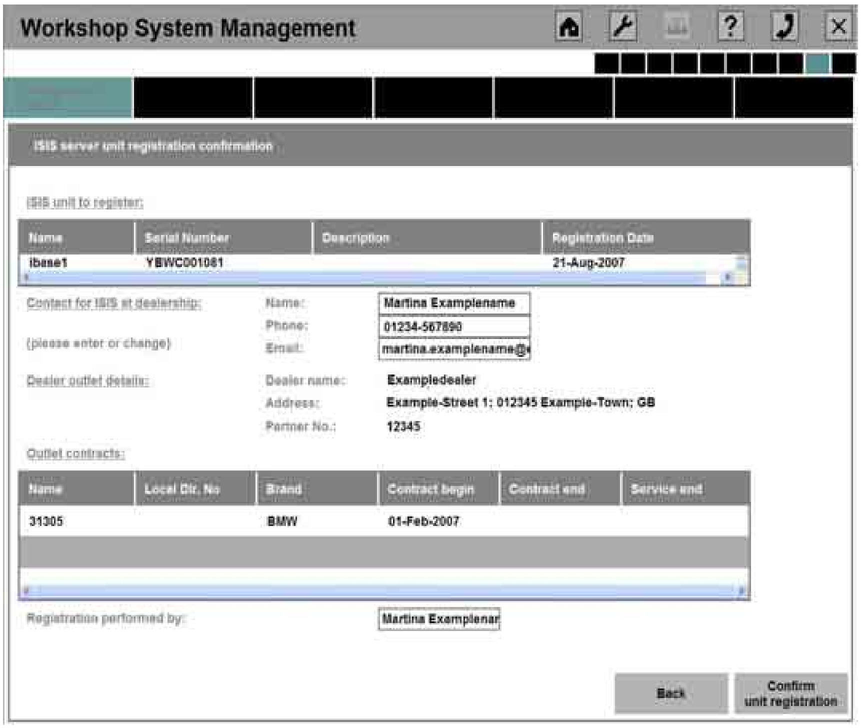
de-de-Germany (de-DE-DE)

Fig. 38: Login at the portal

To log into the selected dealer portal, the user must enter a user name and password for the corresponding dealer portal (see Fig. 38; here, the "S-Gate" portal is used as an example). When the "Login" button is clicked, the input data is checked.

As soon as the check is without errors, the user is taken to the screen for the input of dealer information (see Fig. 39).

Display and specification of dealer data (registration acknowledgement):



[redacted]

ISIS server unit registration confirmation

ISIS unit to register:

Name	Serial Number	Description	Registration Date
ibase1	YBWC001081		21-Aug-2007

Contact for ISIS at dealership:
(please enter or change)
Name: Martina Examplename
Phone: 01234-567890
Email: martina.examplename@e

Dealer outlet details:
Dealer name: Exampledealer
Address: Example-Street 1; 012345 Example-Town; GB
Partner No.: 12345

Outlet contracts:

Name	Local Dlr. No	Brand	Contract begin	Contract end	Service end
31305		BMW	01-Feb-2007		

Registration performed by: Martina Examplenar

Fig. 39: Registration acknowledgement

The ISIS server data is automatically generated in the first line of the dialog box for registration acknowledgement (see Fig. 39):

- Server name
- Serial number of the server
- Description of the server
- Day of registration

Contact person:

In the next section, supplementary data with regard to the contact person at the authorized dealership who is responsible for the ISIS must be entered. This involves the following details:

- Name
- Phone
- E-mail address

Authorized dealer:

The dealer data is determined automatically in the section "Dealership details" by the portal login and in the corresponding positions of the dialog box. This is the dealer name, the dealer address and the BMW partner number.

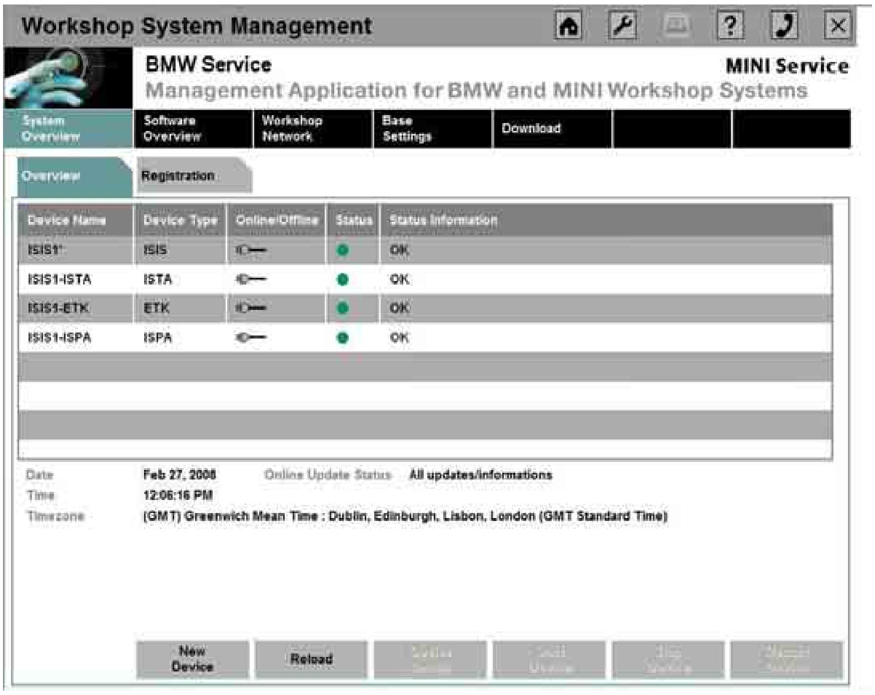
Contract data:

The system displayed the contract data of the dealer.

In the bottom field, the portal user name is inserted automatically as the person for completion of the registration.

Clicking the "Confirm Registration" button initiates a check of the entered data and carries out the registration.

After successful registration, the start page of the WSM is displayed (see Fig. 40).



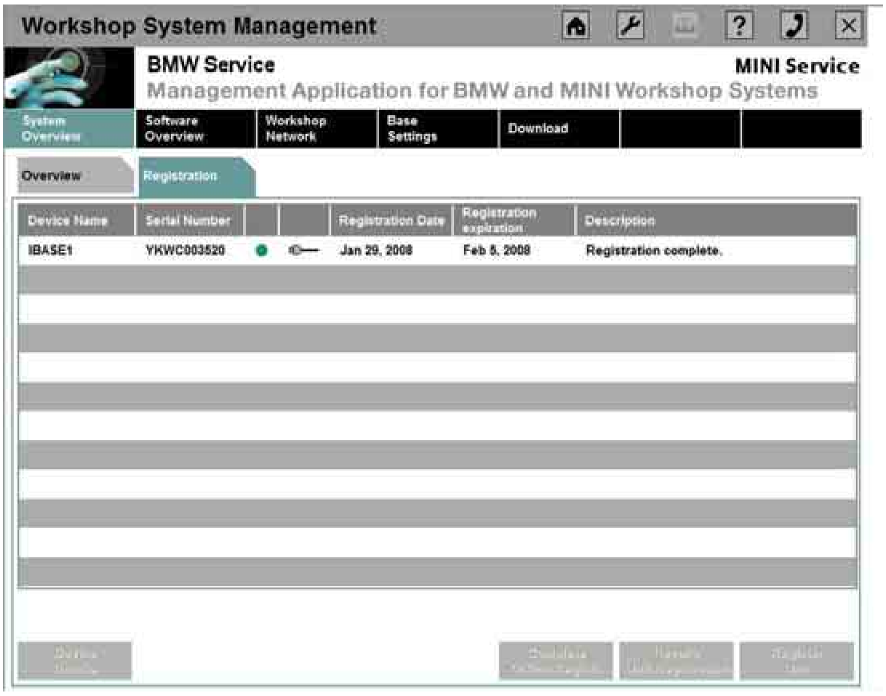
Device Name	Device Type	Online/Offline	Status	Status Information
ISIS1*	ISIS	⊸	●	OK
ISIS1-ISTA	ISTA	⊸	●	OK
ISIS1-ETK	ETK	⊸	●	OK
ISIS1-ISPA	ISPA	⊸	●	OK

Date Feb 27, 2008 Online Update Status All updates/informations
Time 12:06:16 PM
Timezone (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London (GMT Standard Time)

Fig. 40: System overview after ISIS configuration and registration

Completion of the online registration:

To check whether the registration was successful, the registration overview in the "System Overview" menu at the "Registration" tab can be used. A green dot (see Fig. 41) should now appear after the ISIS that has just been installed and registered.



Device Name	Serial Number			Registration Date	Registration expiration	Description
IBASE1	YKWC003520	●		Jan 29, 2008	Feb 5, 2008	Registration complete.

Fig. 41: Registration overview

After successful completion of the online registration process, the server plug-in module has been installed, configured and registered and is now enabled for use.

Note:

In order to be able to use the ISIS and above all its applications to the full extent, continue with the instructions in chapter 4.

For configuration and registration of the second server plug-in module, follow the instructions from chapter 3.1.8 in the same way for the ISIS2.

Note:

During configuration and registration of the ISIS2, the ISIS1 must remain switched on.

3.1.11.2 Offline registration (part 1) – generating the registration fax

Information 1:

Please bear in mind that the offline registration per fax can usually only be completed successfully after 2 working days.

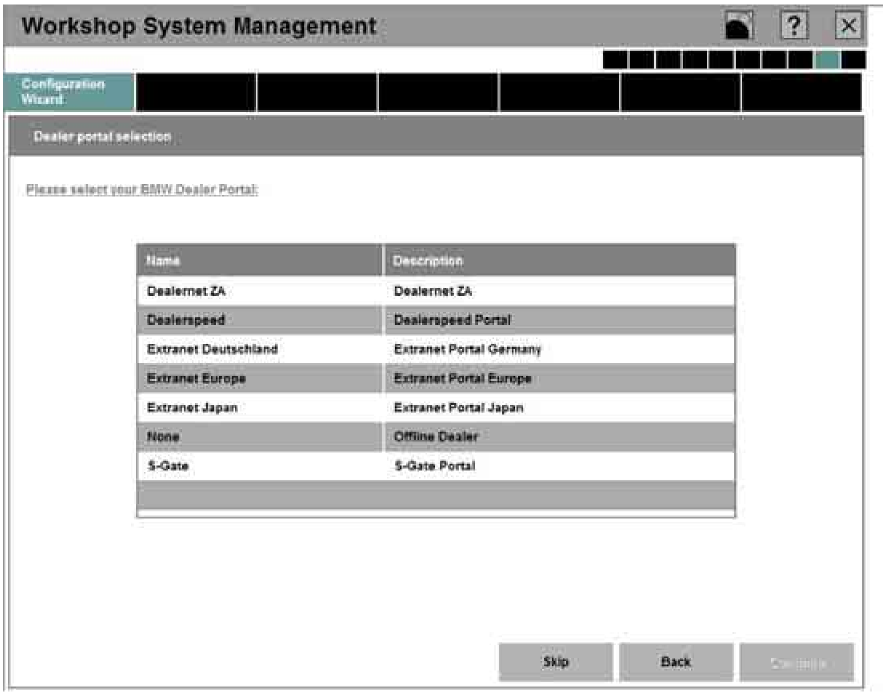
Information 2:

In the rest of this guide, a dealer who has made this type of registration is also referred to as an "offline dealer" and all of the new generation devices that are registered for this ISIS are also registered offline.

Note:

ISIS online functions (e.g. online update and others) are not available in the case of an offline registration.

If the authorized dealer does not have Internet access, it is possible to register the ISIS offline.



Dealer portal selection

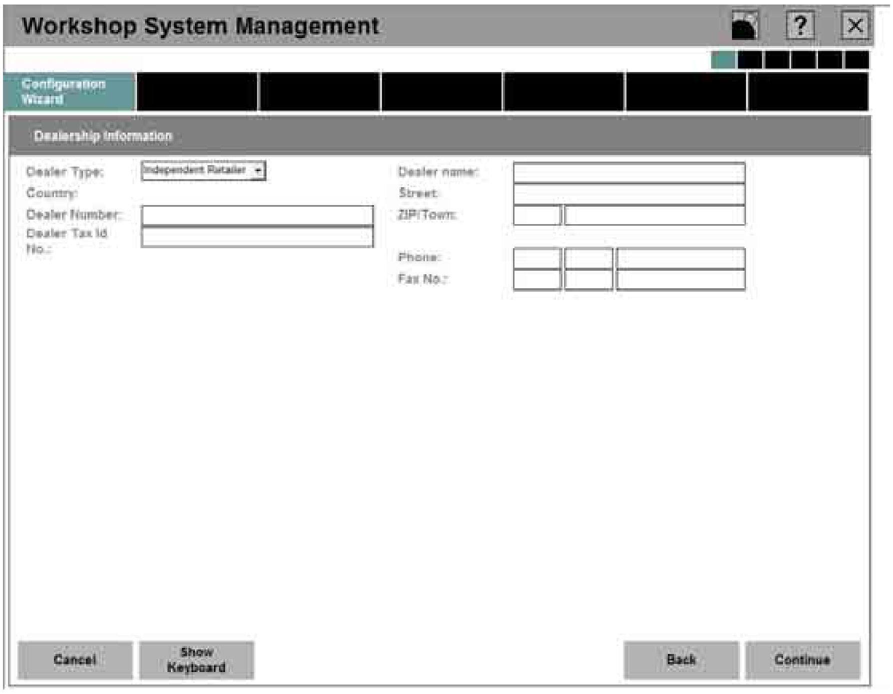
Please select your BMW Dealer Portal:

Name	Description
Dealernet ZA	Dealernet ZA
Dealerspeed	Dealerspeed Portal
Extranet Deutschland	Extranet Portal Germany
Extranet Europe	Extranet Portal Europe
Extranet Japan	Extranet Portal Japan
None	Offline Dealer
S-Gate	S-Gate Portal

Fig. 42: Selection of the offline registration

In this dialog box (see Fig. 42), select as portal "None - Offline Dealer".

Entering the dealer data:



Dealer Type: Independent Retailer

Fig. 43: Entering the dealer data

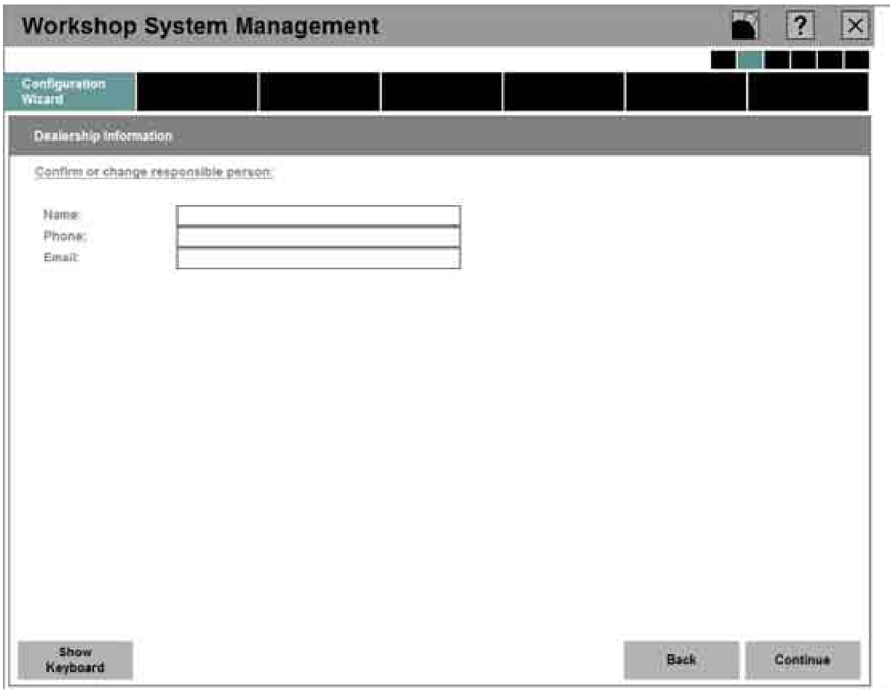
Exact entry of the dealer data is required on this screen (see Fig. 43).

The user is asked to enter the following data in the fields specifically designed for the purpose:

- Selection of the dealer type (independent dealer or partner dealer)
- Dealer number according to dealer contract
- Dealer name
- Street
- Zip/Town
- Country selection
- Phone
- Fax number
- Dealer Tax ID number

To move on to the previous or next screen, click the "Back" or "Continue" button respectively.

Specifying the contact person:



Dealership information

Confirm or change responsible person:

Name:
Phone:
Email:

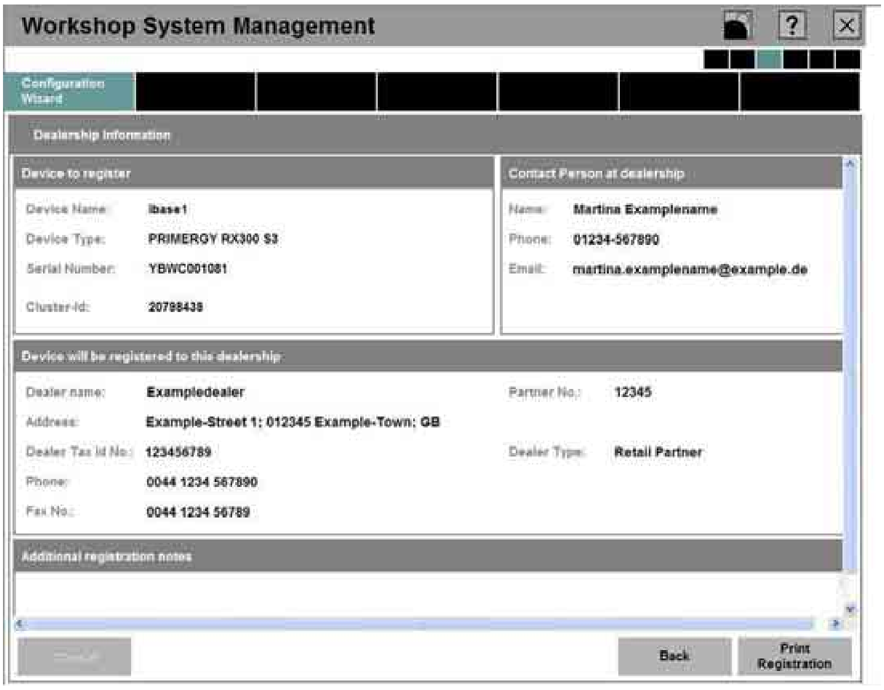
Fig. 44: Specifying the contact person

The present dialog box (see Fig. 44) can be used to provide precise details about the employee responsible for the ISIS in the company. These can also be changed again at a later time. Regardless of whether this is an initial entry or a later change, the input fields must be completed accordingly:

- Last name
- First name
- Telephone
- e-mail

To switch to the previous or next screen, click the "Back" or "Continue".

Confirmation of the details and printing the registration:



Dealership Information

Device to register

Device Name: ibase1

Device Type: PRIMERGY RX300 S3

Serial Number: YBWC001081

Cluster-Id: 20798438

Contact Person at dealership

Name: Martina Examplename

Phone: 01234-567890

Email: martina.examplename@example.de

Device will be registered to this dealership

Dealer name: Exampledealer

Partner No.: 12345

Address: Example-Street 1; 012345 Example-Town; GB

Dealer Tax Id No.: 123456789

Dealer Type: Retail Partner

Phone: 0044 1234 567890

Fax No.: 0044 1234 56789

Additional registration notes

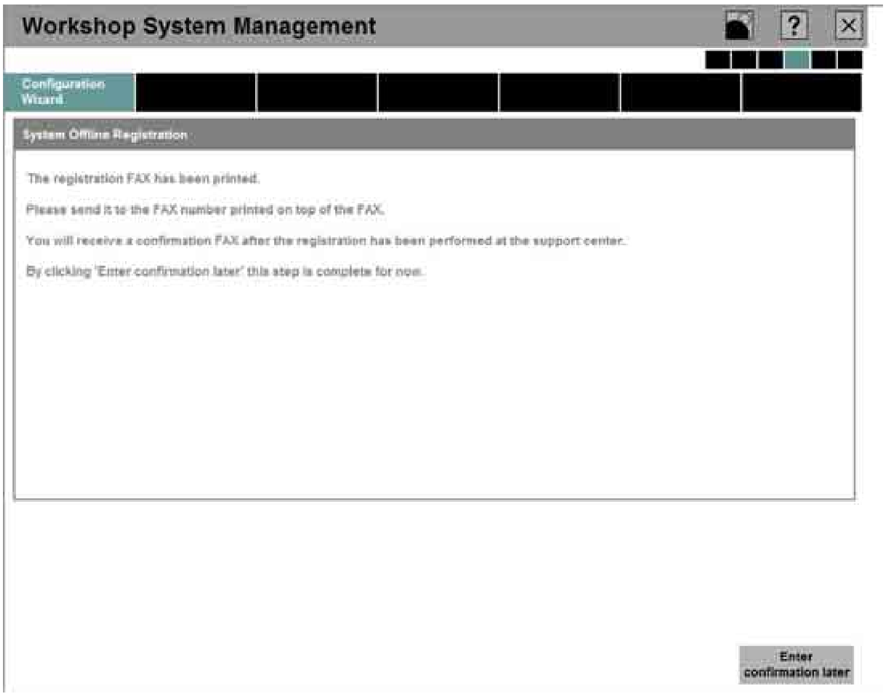
Fig. 45: Confirmation of the details and printing the registration

The system now generates the data specified by the user and summarizes it as follows (see Fig. 45):

- Dealer type
- Dealer number
- Dealer address
- Telephone and fax numbers
- Dealer Tax ID number
- Contact person
- Designation of the ISIS server unit

If you agree to the confirmed details, the following dialog box (see Fig. 46) appears and the form is printed by clicking the "Print registration" button.

Sending the fax:



System Offline Registration

The registration FAX has been printed.

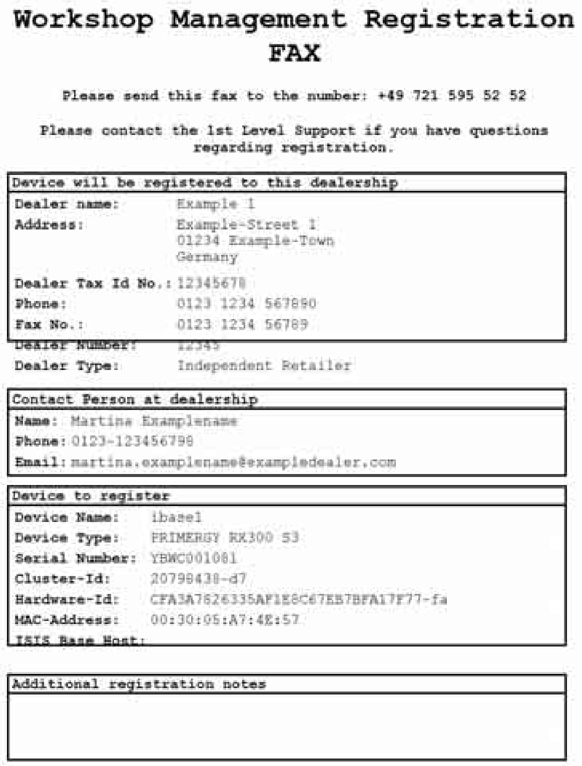
Please send it to the FAX number printed on top of the FAX.

You will receive a confirmation FAX after the registration has been performed at the support center.

By clicking 'Enter confirmation later' this step is complete for now.

Fig. 46: Prompt for printing the registration

The printed form (see Fig. 47) must then be sent to fax number shown in the top right of the fax.



Workshop Management Registration
FAX

Please send this fax to the number: +49 721 595 52 52

Please contact the 1st Level Support if you have questions
regarding registration.

Device will be registered to this dealership

Dealer name:	Example 1
Address:	Example-Street 1 01234 Example-Town Germany
Dealer Tax Id No.:	12345678
Phone:	0123 1234 567890
Fax No.:	0123 1234 56789
Dealer Number:	12345
Dealer Type:	Independent Retailer

Contact Person at dealership

Name:	Martina Examplename
Phone:	0123-123456790
Email:	martina.examplename@exampledealer.com

Device to register

Device Name:	ibase1
Device Type:	PRIMERGY RX300 S3
Serial Number:	YBWC001081
Cluster-Id:	20798438-d7
Hardware-Id:	CFA3A7626335AF1E8C67EB7BFA17F77-fa
MAC-Address:	00:30:05:A7:4E:57
ISIS Base Host:	

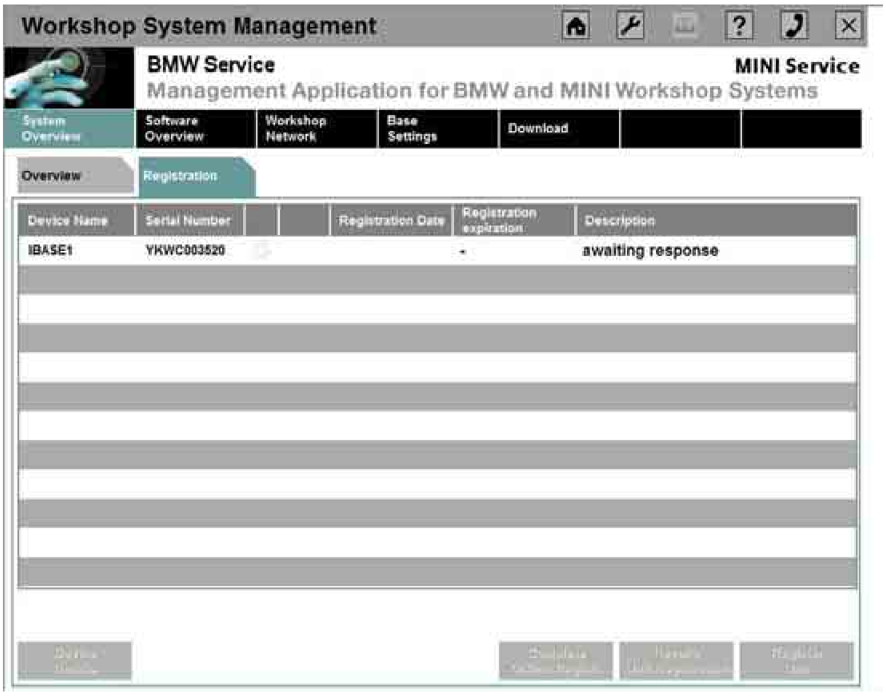
Additional registration notes

Fig. 47: Registration fax

Clicking the "Confirm later" button (see Fig. 46) takes you to the start page (System Overview) of the WSM.

Completion of the offline registration (part 1):

This concludes the first part of the offline registration. In the WSM, a white dot appears in the System Overview in the 'Registration' tab (see also chapter 5.1.3). This indicates that the first part of the offline registration has been carried out (see Fig. 48).



Device Name	Serial Number			Registration Date	Registration expiration	Description
IBASE1	YKWC003520				-	awaiting response

Fig. 48: Completion of the offline registration (part 1):

The user will receive a reply fax from BMW AG within one working day. You can then continue with the steps from the following chapter (see chapter 3.1.11.3).

3.1.11.3 Offline registration (part 2) – reply fax for the registration received

The second part of the offline registration of the ISIS takes place in the same way as the procedure described in chapter 5.1.3.6.

Note:

In order to be able to make full use of the ISIS and above all its applications, continue with the instructions in chapter 5.1.3.6 after the registration.

For configuration and registration of the second server plug-in module,, follow the instructions from chapter 3.1.8 in the same way for the ISIS2.

Note:

During configuration and registration of the ISIS2, the ISIS1 must remain switched on.

3.1.12 Installation of the applications

The installation of the applications (ISTA, ISPA and EPC) is implemented via the WSM. The exact procedure is described in chapter 4.

Information:

After registration is complete, the first ISIS is ready for operation. The second ISIS must then be started and the installation carried out according to the steps in Chapter 3.1.4, following the special instructions for installation of the second ISIS.

3.2 Integrated Service Information Display (ISID)

The ISID is not delivered in a preinstalled state, which means that commissioning involves installation. This installation is executed via the ISIS.

Note 1:

The commissioning and initial installation of an ISID takes place via the ISIS; it is therefore necessary to make sure that an ISIS has already been successfully commissioned and registered.

Note 2:

If you wish to commission a number of ISIDs, it is advisable to install the ISIDs in succession.

3.2.1 Important requirements

For commissioning, the following conditions must be met:

- For the initial installation, a DHCP server must be present in the workshop network. This can be implemented via the ISIS or another DHCP server in the workshop network. This DHCP server ensures that the ISID is automatically supplied with an IP address.
- There must be an image on the ISIS, previously loaded onto the ISIS from the supplied DVD (see chapter 5.1.4.1).

Note:

If there are a number of ISIS subnets in the workshop network, then the ISID for commissioning must be in the same subnet as the ISIS. Only after commissioning can the ISID also be used in other subnets.

Specific information for other details on networking in the workshop can be found in chapter 2.3.1 or through your market.

3.2.2 Sequence for commissioning

Commissioning requires execution of a number of steps on the ISID as well as in the WSM on the ISIS. Registration of the device is carried out after completion of the steps.

Note:

Please bear in mind that an installation without applications can take up to 90 minutes and an installation with applications can take up to 180 minutes.

Information:

No additional devices are required for the initial installation (keyboard etc.).
However, if you have a USB mouse or USB keyboard, these can be used.

3.2.2.1 Reading off and noting down the LAN MAC address

The MAC address of the ISID is the hardware address and its purpose is to uniquely identify the ISID in the network. It is required for the WSM to integrate the ISID.

To read off the MAC address, disconnect the operating unit from the docking station. The MAC address of the LAN adapter is located on the back; please note it down (see Fig. 49, LAN: 00-01-A9-00-20-00).

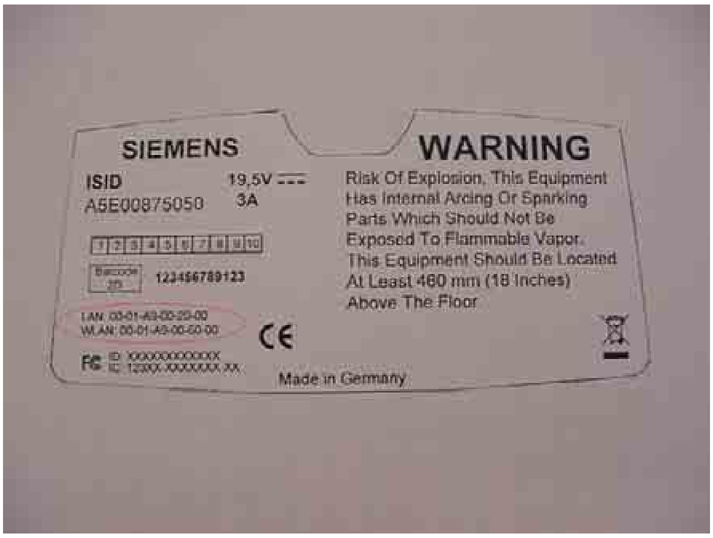
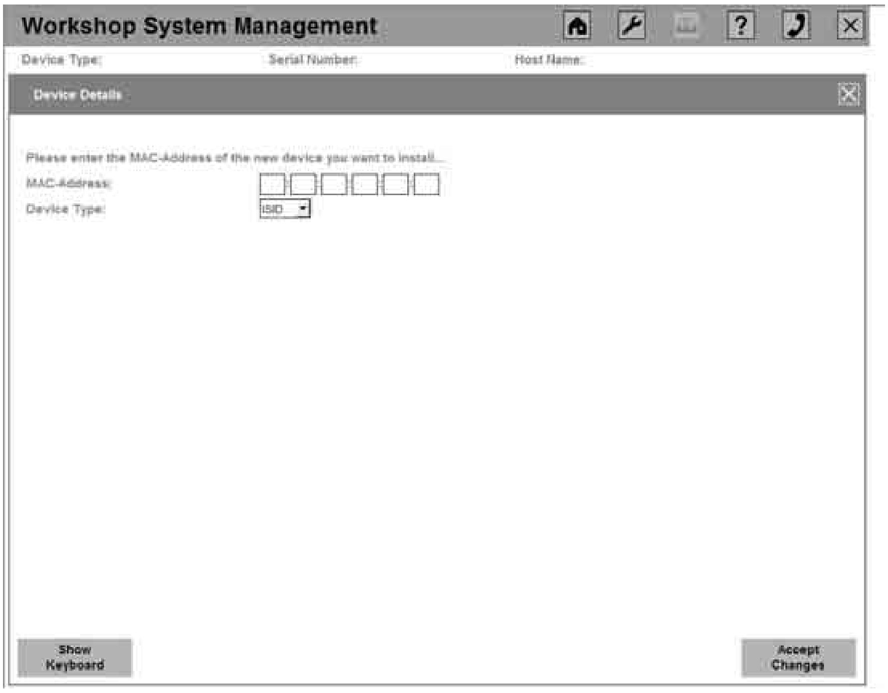


Fig. 49: Reading off the ISID LAN MAC address

3.2.2.2 Setting up ISID as a new device in the WSM

- The workshop PC is used to start the WSM of the ISIS on which the ISID is to be commissioned.
- In the WSM, click the "New device" button on the start page.
- In the dialog box that follows (see Fig. 50), enter the MAC address of the device (which you noted down before) and select the device type "ISID".
- Confirm the input by clicking the "Apply" button. The ISID is now configured automatically and the server plug-in modules are synchronized. This takes around 20 minutes. This sets up the ISID as a new device in the WSM.



Workshop System Management

Device Type:
Serial Number:
Host Name:

Device Details

Please enter the MAC-Address of the new device you want to install...

MAC-Address: □□□□□□

Device Type: ISID

Fig. 50: Setting up a new ISID in the WSM

3.2.2.3 Connecting ISID to the network

After the requirements for the ISIS have been met, the ISID installation can be prepared.

⚠	**Note:** Please follow the instructions from chapter 2.3.1.

Information:

The ISID can be installed when it is docked or undocked.

However, it is advisable for the operating unit to be docked for the new installation of the ISID and supplied with voltage via the external power supply so that the installation is not aborted due to a dead battery.

- Connecting the ISID to the active workshop network by means of LAN

  For a docked operating unit, this is done via the docking station (see Fig. 51).
  For an undocked operating unit, it is done directly via the operating unit itself (see Fig. 52).

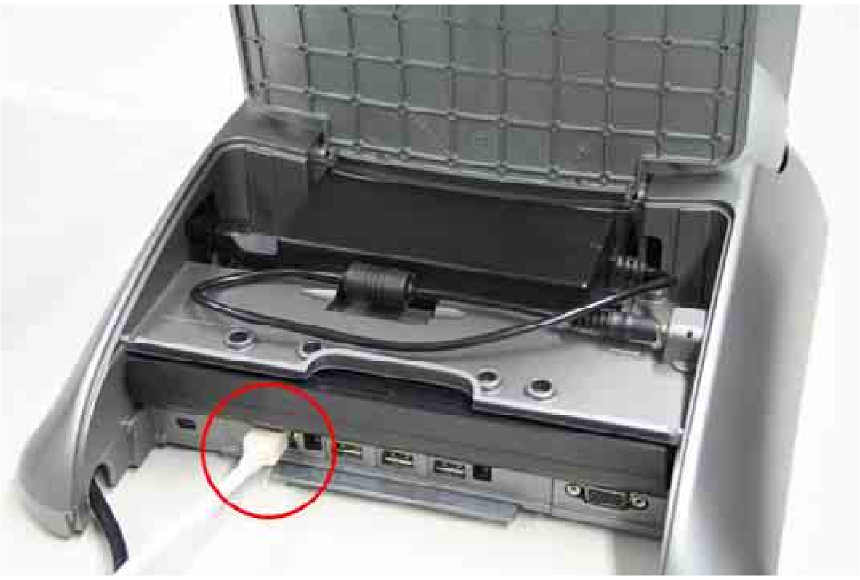


Fig. 51: Connecting the ISID to the workshop network via the docking station

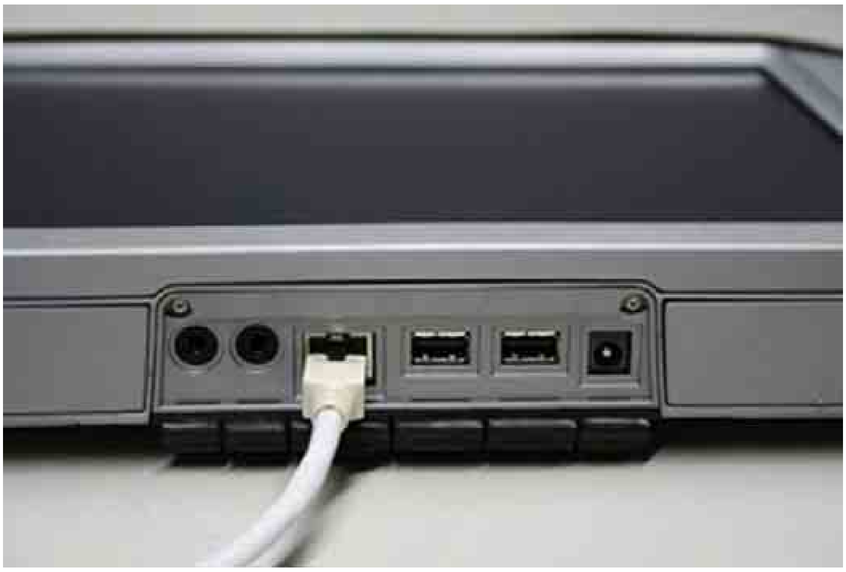


Fig. 52: Connecting the ISID to the workshop network without docking station

!	**Note:** For the initial installation, only the wired network (LAN) is operational. The purpose of the two LEDs directly on the LAN connecting socket is to monitor the functioning of the network.

3.2.3 Switching on the ISID for installation

!	**Note:** The ISID must **not** be physically moved during the installation.

- Start the ISID by pressing the on/off button (29) on the front of the operating unit (see Fig. 53). The LEDs (see Fig. 53: LED area (25) surrounding the LEDs (26), (27) and (28)) flash briefly in succession.

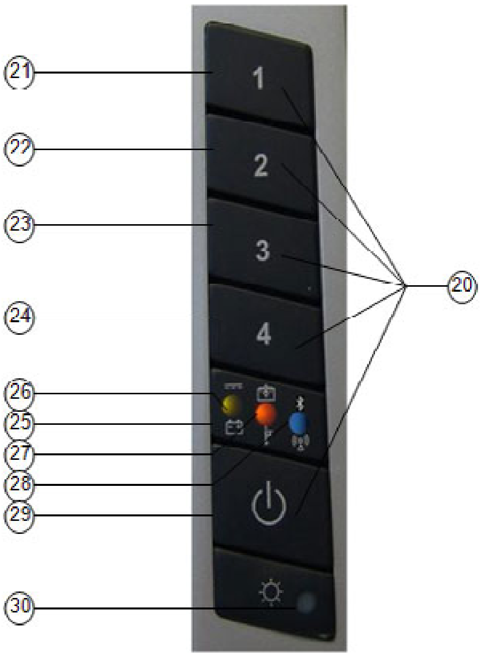


Fig. 53: Device buttons of the ISID operating unit

Information:

The operating unit has 5 device buttons (see Fig. 53: (20)) - buttons 1, 2, 3 and 4 and the on/off button.

Depending on the operation status (switching on or normal operation), buttons 1-4 are assigned different functions.

On/off button (29): With the operating unit switched off: starts the operating unit

Button functions after switching on:

Button 1 (21): Pressed simultaneously with button 4: initial / new installation

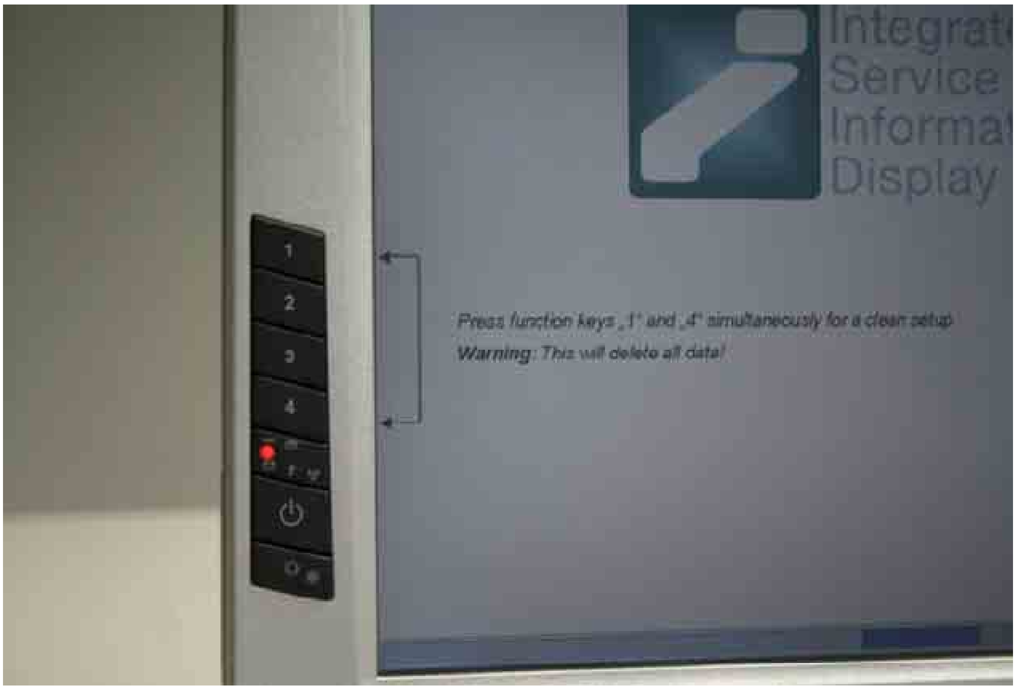
Button 2 (22): starts the self-test of hard disk and main memory

(more detailed information in the ISID User Guide)

Button 3 (23): not used

Button 4 (24): Pressed simultaneously with button 1: initial / new installation

- As soon as the prompt for setup (see Fig. 54) appears after switching on, simultaneously press device buttons 1 and 4 (see Fig. 53) buttons (21) and (24)).



Press function keys „1" and „4" simultaneously for a clean setup
Warning: This will delete all data!

Fig. 54: Prompt for setup when starting the ISID

Information:

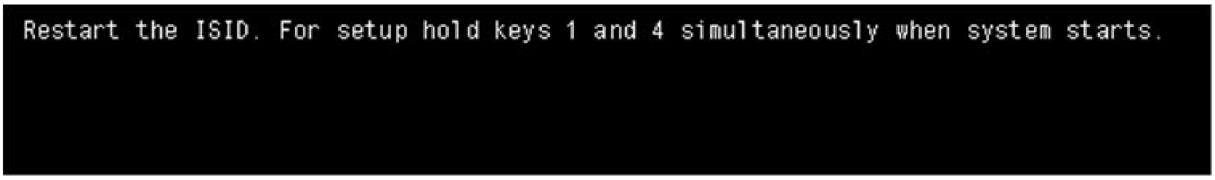
This prompt (see Fig. 54) only appears for a few moments. When performing an **initial installation,** if you do not press the corresponding button combination in time, an error message appears (see Fig. 55) since at this point there is not yet an operating system on the ISID.

In this case, proceed as follows:

- Switch the ISID off by pressing the on/off button (29) (see Fig. 53) for approx. 5 seconds.
- Restart the ISID by pressing the on/off button (29) (see Fig. 53).
- Press buttons 1 and 4 (see Fig. 53 buttons (21) and (24)) simultaneously as soon as the prompt (see Fig. 54) appears on the display.

If the button combination is not pressed in time during a new installation, the ISID starts normally and displays the WSM user interface once the boot-up process has concluded.

In this case, shut down the ISID via the WSM in a controlled manner, restart it (instructions can be found in chapter 6.7), and when the prompt is displayed (see Fig. 54), press buttons 1 and 4 simultaneously.



```
Restart the ISID. For setup hold keys 1 and 4 simultaneously when system starts.
```

Fig. 55: Error message with lack of operating system

Note:

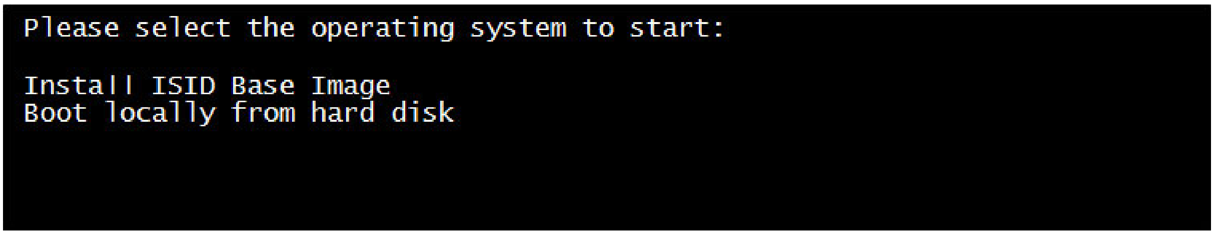
If an ISID is not installed with the new base system available on the ISIS, the ISID goes into the temporary offline mode. This is necessary because otherwise, the co-operation between the software of ISIS and ISID is no longer assured.

It can only be returned to the infrastructure mode when the new installation has been carried out with the current base system.

The new installation can then be initiated by means of a new start with a button combination.

3.2.4 Selection of the boot menu

After switching on the ISID for the image installation, a selection menu (boot menu) appears (see Fig. 56) with two possible selections.



```
Please select the operating system to start:

Install ISID Base Image
Boot locally from hard disk
```

Fig. 56: ISID boot menu

Select "Install ISID Base Image" for the image installation.

A selection can be made by pressing buttons 1 and 2 on the front of the operating unit (see Fig. 53 buttons (21) and (22)). Press button 4 (see Fig. 53 button (24)) to confirm the selection.

Once "Install ISID Base Image" is selected, the installation occurs automatically. No other user input is required.

ℹ	**Information:** If a new installation is inadvertently initiated by pressing buttons 1 and 4 (see Fig. 53 buttons (21) and (24)), this can be canceled either by selecting the option "Boot locally from hard disk" in the boot menu (see Fig. 56) or by disconnecting the LAN cable and then switching off the ISID.

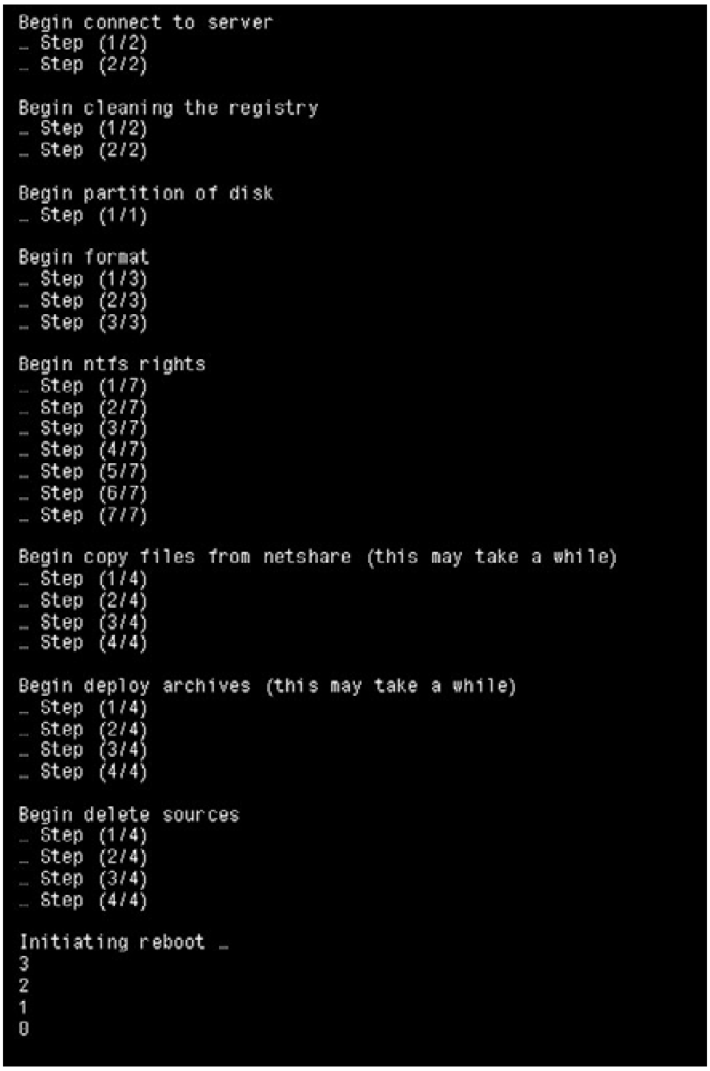
3.2.5 Installation

Note:

In the course of the installation, the ISID is restarted automatically several times.

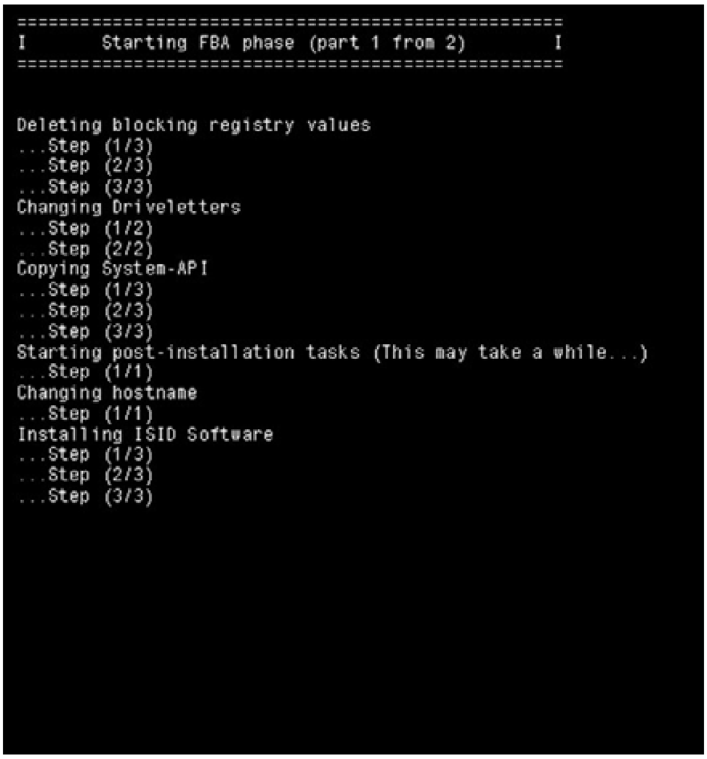
At this point, make sure **NOT** to press the corresponding button combination for initial / new installation.

The installation is carried out in three phases (according to Fig. 57, Fig. 58, and Fig. 59).



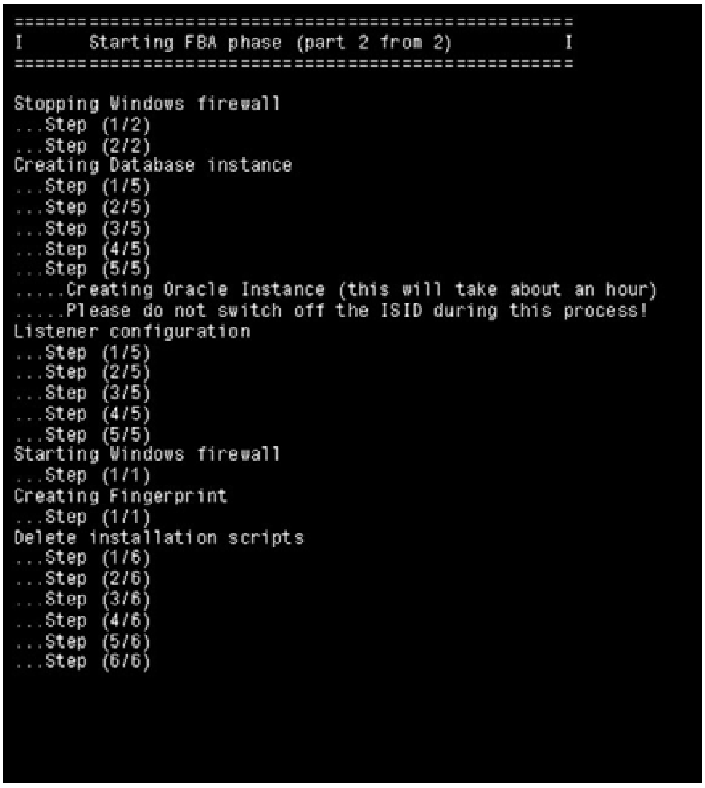
```
Begin connect to server
… Step (1/2)
… Step (2/2)

Begin cleaning the registry
… Step (1/2)
… Step (2/2)

Begin partition of disk
… Step (1/1)

Begin format
… Step (1/3)
… Step (2/3)
… Step (3/3)

Begin ntfs rights
… Step (1/7)
… Step (2/7)
… Step (3/7)
… Step (4/7)
… Step (5/7)
… Step (6/7)
… Step (7/7)

Begin copy files from netshare (this may take a while)
… Step (1/4)
… Step (2/4)
… Step (3/4)
… Step (4/4)

Begin deploy archives (this may take a while)
… Step (1/4)
… Step (2/4)
… Step (3/4)
… Step (4/4)

Begin delete sources
… Step (1/4)
… Step (2/4)
… Step (3/4)
… Step (4/4)

Initiating reboot …
3
2
1
0
```

Fig. 57: ISID installation phase 1



```
====================================================
I       Starting FBA phase (part 1 from 2)         I
====================================================


Deleting blocking registry values
...Step (1/3)
...Step (2/3)
...Step (3/3)
Changing Driveletters
...Step (1/2)
...Step (2/2)
Copying System-API
...Step (1/3)
...Step (2/3)
...Step (3/3)
Starting post-installation tasks (This may take a while...)
...Step (1/1)
Changing hostname
...Step (1/1)
Installing ISID Software
...Step (1/3)
...Step (2/3)
...Step (3/3)
```

Fig. 58: ISID installation phase 2



```
=====================================================
I      Starting FBA phase (part 2 from 2)           I
=====================================================

Stopping Windows firewall
...Step (1/2)
...Step (2/2)
Creating Database instance
...Step (1/5)
...Step (2/5)
...Step (3/5)
...Step (4/5)
...Step (5/5)
.....Creating Oracle Instance (this will take about an hour)
.....Please do not switch off the ISID during this process!
Listener configuration
...Step (1/5)
...Step (2/5)
...Step (3/5)
...Step (4/5)
...Step (5/5)
Starting Windows firewall
...Step (1/1)
Creating Fingerprint
...Step (1/1)
Delete installation scripts
...Step (1/6)
...Step (2/6)
...Step (3/6)
...Step (4/6)
...Step (5/6)
...Step (6/6)
```

Fig. 59: ISID installation phase 3

After successful installation, the WSM configuration wizard is started. The configuration can be carried out according to the following chapter.

3.2.6 Configuration of the ISID

The configuration of the ISID is carried out using the WSM configuration wizard described below.

3.2.6.1 Calibrating the touch-screen

Note:

The calibration is started automatically immediately after the new installation of the ISID. If the calibration is not carried out within 10 seconds, the calibration can be restarted on the next screen (dialog box for configuration of the WSM).

Because the operating unit is delivered without an operating system and thus without calibration data, calibration is required after the initial installation.

The calibration is carried out as follows:

- A circle (see Fig. 60) appears in the top-left corner, adjacent to which is the word "TOUCH" (see Fig. 61).

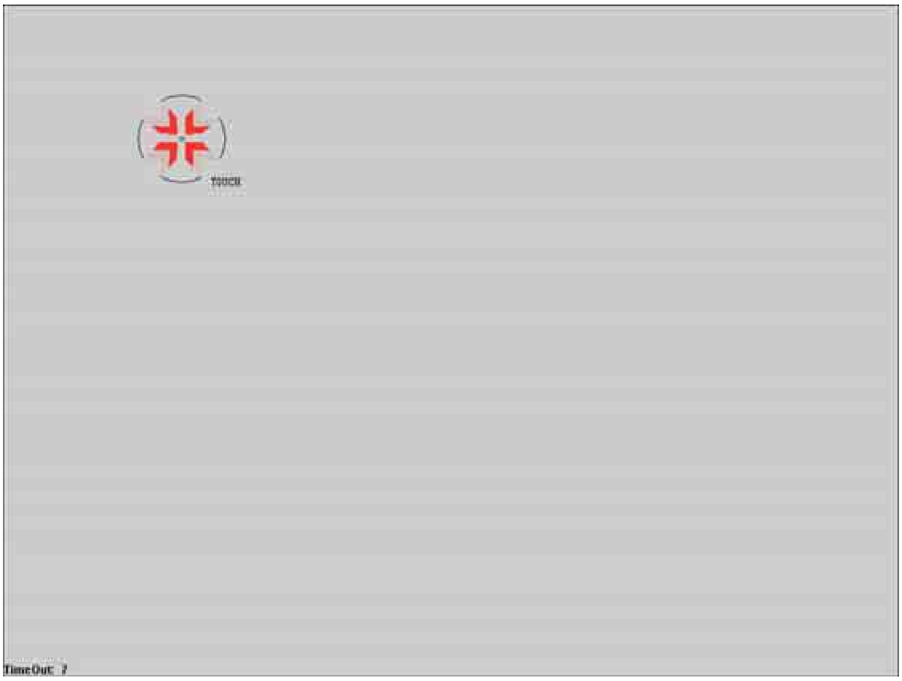


Fig. 60: Calibration of the ISID

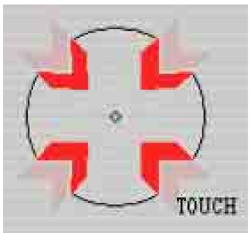


Fig. 61: Touch symbol during ISID calibration

- Now use the touchpen to touch the display in the centre of the circle.

  The circle becomes smaller the longer the centre of the circle is touched with the pen, during which time, the word "HOLD" is displayed beside the circle (see Fig. 62).

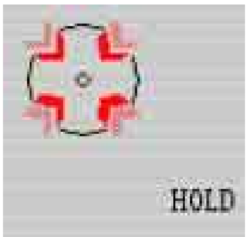


Fig. 62: Hold symbol for ISID calibration

- Hold down the selected point until the circle has almost disappeared and the word "RELEASE" appears beside it (see Fig. 63).

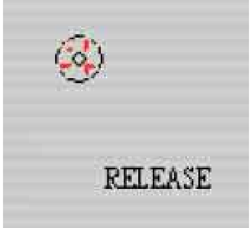


Fig. 63: Release symbol for ISID calibration

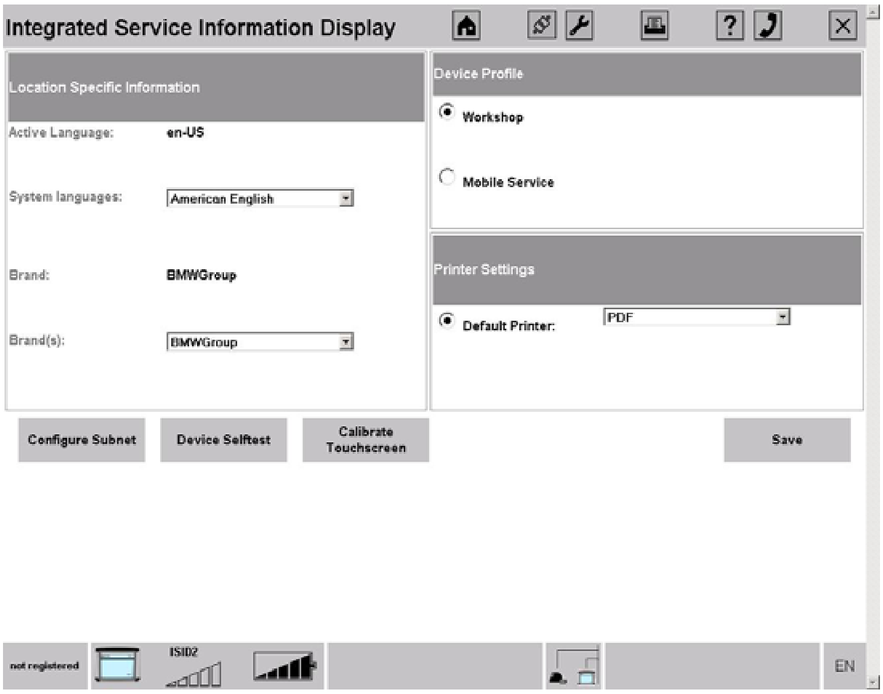
- Repeat this operation for the remaining corners (top right, bottom right and bottom left).

i	**Information:** If it was not possible to run the calibration in good time or if the setting did not run as desired, there the calibration can be restarted in the next screen (see Fig. 64) by clicking the "Calibrate touch-screen" button.

3.2.6.2 Settings for the WSM

Information:

If the calibration is not run within 10 seconds, in the next dialog box (see Fig. 64) selecting the "Calibrate touch-screen" button starts a new attempt at calibration.



Location Specific Information

Active Language: en-US

System languages: American English

Brand: BMWGroup

Brand(s): BMWGroup

Device Profile

● Workshop

○ Mobile Service

Printer Settings

● Default Printer: PDF

Fig. 64: Settings of the WSM on the ISID

Setting the language:

In this dialog box (see Fig. 64), the desired system language for the WSM on the ISID is selected on the upper left-hand side. To set the relevant language, click the small arrow and select the corresponding language.

Setting the brand – determining the color assignment of the WSM:

If the dealer sells a number of brands, each ISID can be configured to conform with the brands (same as color allocation of the WSM of the ISIS). The corresponding brand can be selected on the lower left-hand side of the screen (see Fig. 64) by clicking the small arrow next to the field.

Setting the profile:

Since the ISID can be used both within the workshop network and for Mobile Service, you can set the purpose of the ISID in the configuration in the upper area of the right-hand side of the dialog box (see Fig. 64).

Here, two profiles that set the scope of the installed applications are distinguished:

- "Workshop” profile
- "Mobile Service” profile

After completion of the initial installation, the application "Workshop System Management" is already installed.

In the "Workshop" profile, the ISTA application is installed.

For the "Mobile Service” profile, the additional application ELOS is installed.

⚠	**Note:** Only when the applications have been set up on the ISIS (see chapter 4) can they also be installed on the ISID.

Setting the printer:

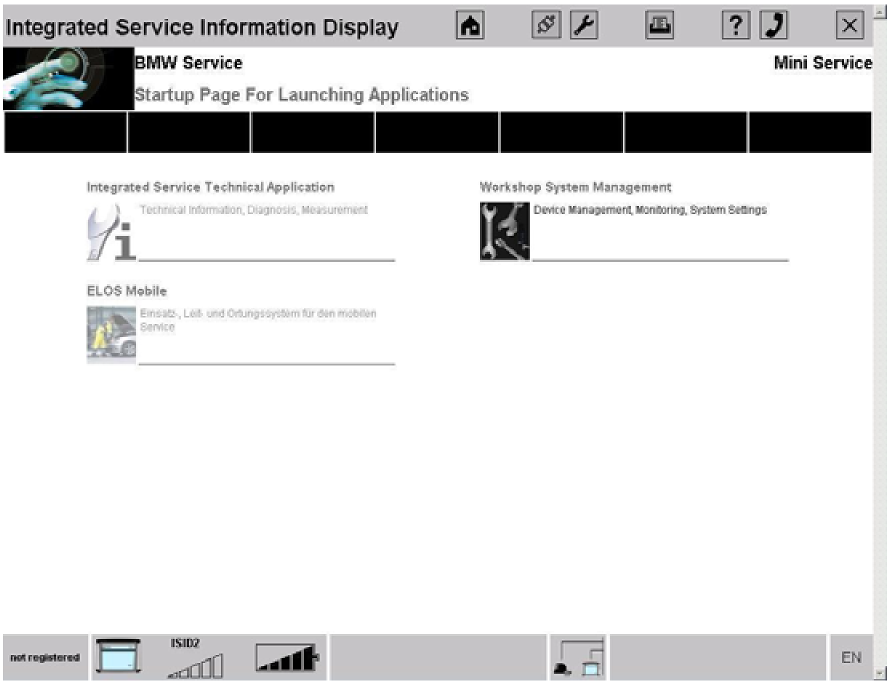
The printer responsible for print output can be selected on the lower right-hand side of the screen (see Fig. 64) when the ISID is in the infrastructure mode.

⚠	**Note 1:** A local printer (USB printer) is only possible for Mobile Service.

⚠	**Note 2:** The current version supports saving the print jobs as pdf files. These are transferred automatically onto the ISIS and can be opened there using the Acrobat Reader of the workshop PC and printed out on the printer installed there.

Selecting the "Continue" button saves the settings and the corresponding applications are installed in the background according to the selected profile.

The Jumpgate (see Fig. 65) appears.



Integrated Service Information Display

BMW Service

Mini Service

Startup Page For Launching Applications

Integrated Service Technical Application

Technical Information, Diagnosis, Measurement

Workshop System Management

Device Management, Monitoring, System Settings

ELOS Mobile

Einsatz-, Leit- und Ortungssystem für den mobilen Service

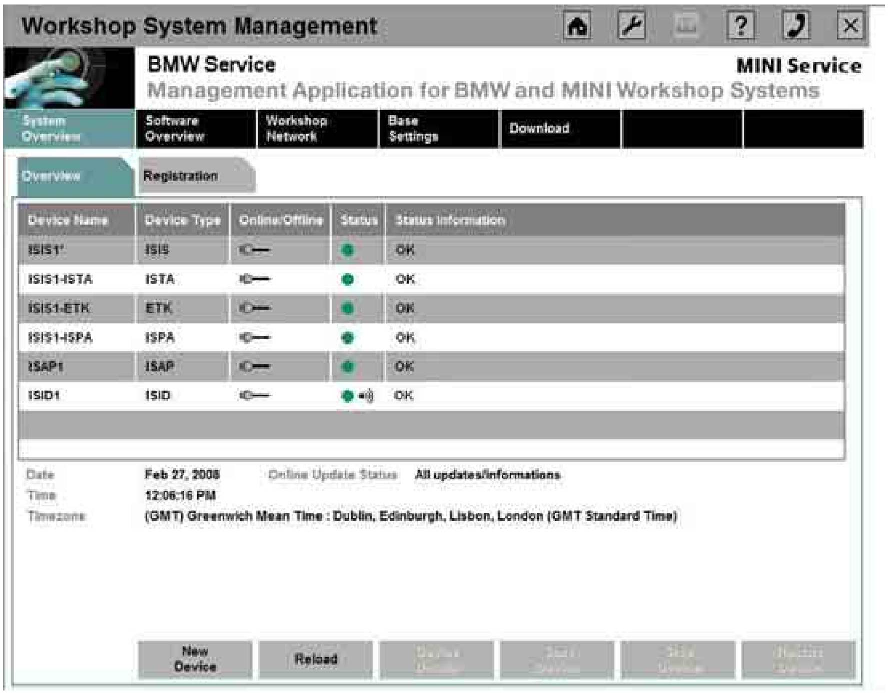
Fig. 65: Jumpgate

Note:

Until the registration has been carried out, the applications in the Jumpgate are 'grayed out' and cannot be started.

3.2.6.3 Registration of the ISID

The ISID is registered according to the steps in chapter 5.1.3.4 for online registration or according to the steps in the chapters 5.1.3.5 and 5.1.3.6 for offline registration.



Device Name	Device Type	Online/Offline	Status	Status Information
ISIS1'	ISIS	🔌	●	OK
ISIS1-ISTA	ISTA	🔌	●	OK
ISIS1-ETK	ETK	🔌	●	OK
ISIS1-ISPA	ISPA	🔌	●	OK
ISAP1	ISAP	🔌	●	OK
ISID1	ISID	🔌	● 🔊	OK

Date Feb 27, 2008 Online Update Status All updates/informations
Time 12:06:16 PM
Timezone (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London (GMT Standard Time)

Fig. 66: ISID in the WSM System Overview

The WLAN symbol (see Fig. 67) directly beside the status message indicates that the ISID supports WLAN.

Fig. 67: WLAN symbol

3.2.6.4 Installation of the applications

The applications are installed automatically after completion of the configuration wizard.

3.3 Integrated Communication Optical Module (ICOM)

Note:

The commissioning and initial installation of an ICOM takes place via the ISIS; it is therefore necessary for one ISIS to have already been successfully commissioned and registered.

Information:

The delivered ICOM is already preinstalled, which means that an initial installation is **not** necessary.

3.3.1 Important precondition

For commissioning, the following condition must be met:

- For commissioning, a DHCP server must be present in the workshop network. This can be implemented via the ISIS or via another DHCP server in the workshop network. This DHCP server ensures that the ICOM is automatically supplied with an IP address.

Note:

If there are a number of ISIS subnets in the workshop network, then the ICOM for commissioning must be in the same subnet as the ISIS. Only after commissioning can the ICOM also be used in other subnets.

Specific information for other details on networking in the workshop can be found in chapter 2.3.1 or through your market.

3.3.2 Sequence for commissioning

Commissioning requires execution of a number of steps on the ICOM as well as in the WSM on the ISIS. Registration of the device is carried out after completion of the steps.

3.3.2.1 Reading off and noting down the LAN MAC address

The MAC address of the ICOM is the hardware address and its purpose is to uniquely identify the ICOM in the network. It is required for the WSM to integrate the ICOM.

The MAC address is located on the back of the ICOM (see Fig. 68); please note it down.

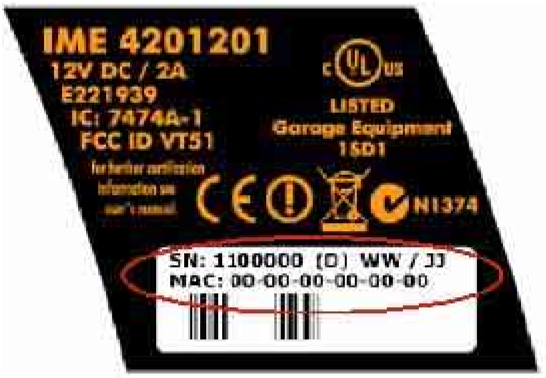
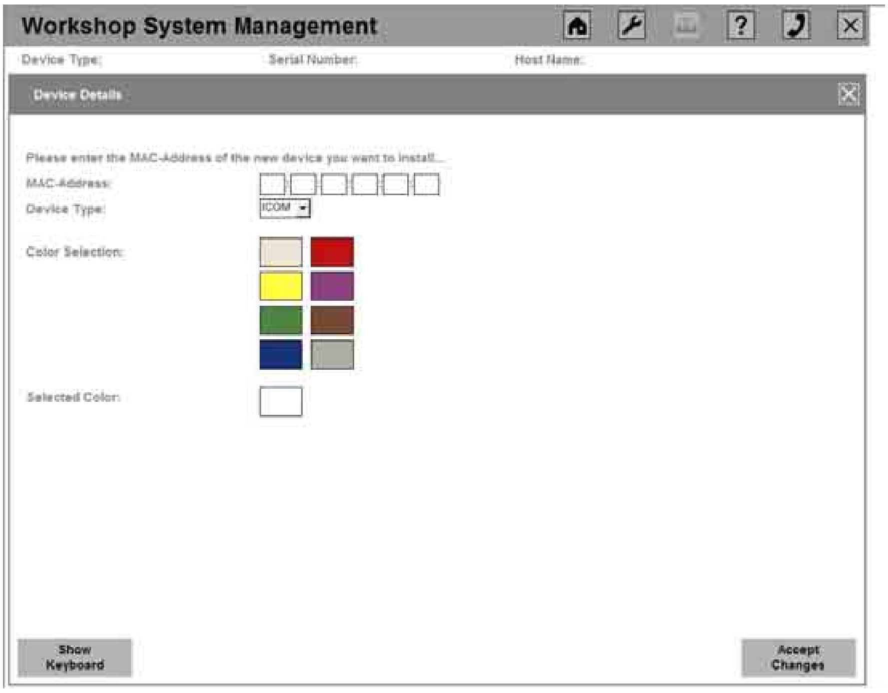


Fig. 68: Reading off the ICOM LAN MAC address

3.3.2.2 Setting up ICOM as a new device in the WSM

- The workshop PC is used to start the WSM of the ISIS on which the ICOM is to be commissioned.
- In the WSM, click the "New device" button on the start page.
- In the dialog box that follows (see Fig. 69), enter the MAC address of the device (which you noted down before) and select the device type "ICOM".
- For an ICOM, a color can also be selected from the list. The color should be selected in accordance with the attached color marking to prevent confusion between the devices.
- Confirm the input by clicking the "Apply" button. This sets up the ICOM as a new device in the WSM.



Device Type: Serial Number: Host Name:

Please enter the MAC-Address of the new device you want to install...

MAC-Address: □□□□□□

Device Type: ICOM

Color Selection:

Selected Color: □

Fig. 69: Setting up a new ICOM in the WSM

3.3.2.3 Connecting ICOM to the network

- Connect the ICOM to the workshop network via LAN (see Fig. 70).

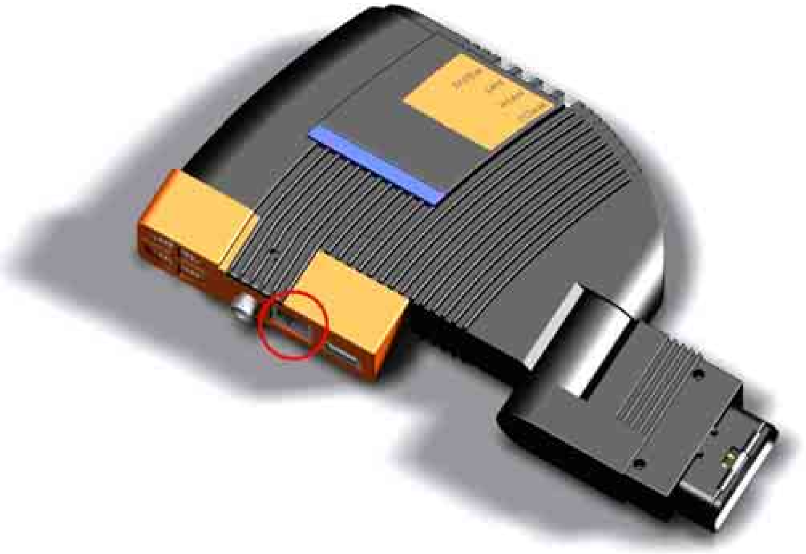


Fig. 70: Connecting the ICOM to the workshop network

- Connect the ICOM to the vehicle via the OBD plug (see Fig. 71) to establish the power supply for the ICOM.

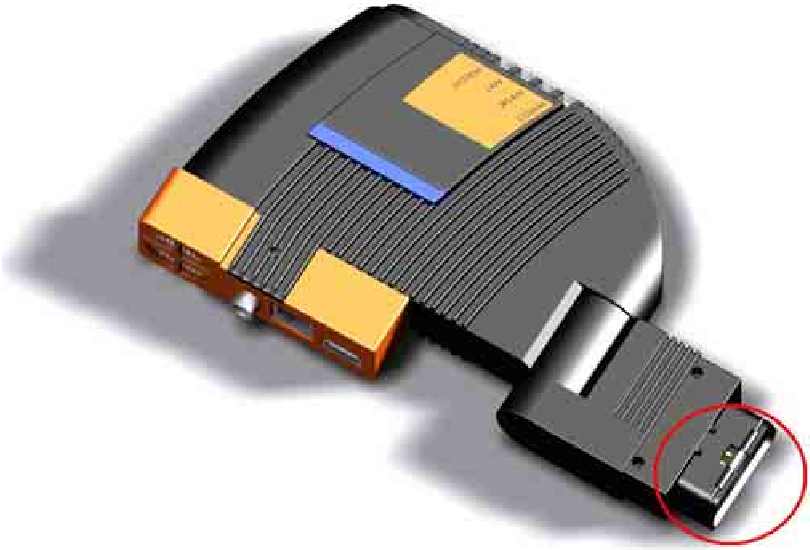
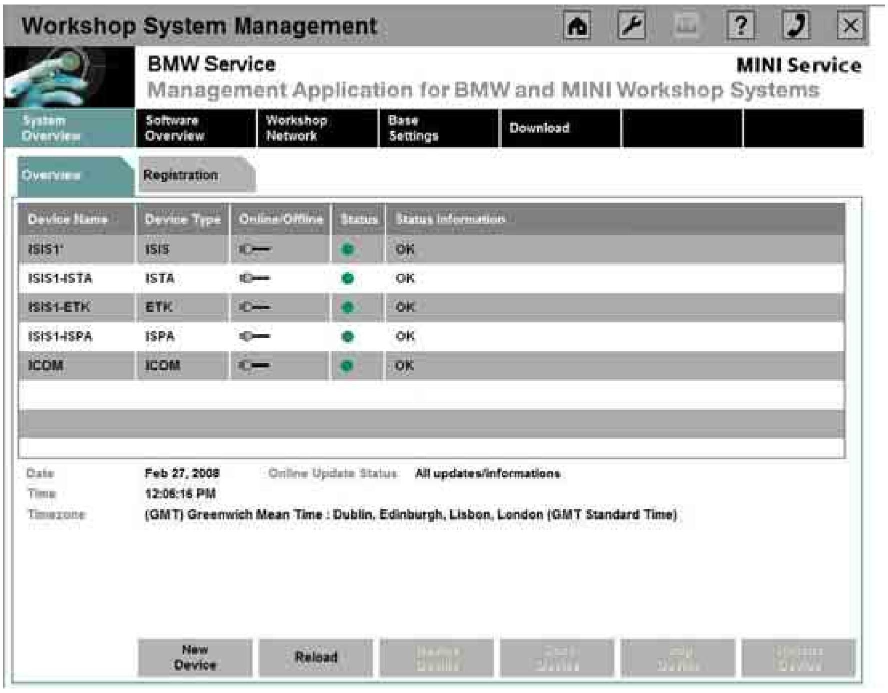


Fig. 71: Connecting the ICOM to the vehicle

- The ICOM is listed as a device in the System Overview (see Fig. 72).



Device Name	Device Type	Online/Offline	Status	Status Information
ISIS1'	ISIS	🔌	●	OK
ISIS1-ISTA	ISTA	🔌	●	OK
ISIS1-ETK	ETK	🔌	●	OK
ISIS1-ISPA	ISPA	🔌	●	OK
ICOM	ICOM	🔌	●	OK

Date Feb 27, 2008 Online Update Status All updates/informations
Time 12:08:16 PM
Timezone (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London (GMT Standard Time)

Fig. 72: ICOM in the WSM System Overview after starting the ICOM

3.3.3 Registration of the ICOM

The ICOM is registered according to the steps in chapter 5.1.3.4 for online registration or according to the steps in the chapters 5.1.3.5 and 5.1.3.6 for offline registration.

3.4 Integrated Service Access Point (ISAP)

Information:

The appropriate software is already installed on the delivered ISAP, which means that an initial installation is **not** necessary. However, the ISAP must be initially configured for deployment in the workshop network.

3.4.1 Important requirements

For commissioning, the following condition must be met:

- For commissioning, a DHCP server must be present in the workshop network. This can be implemented via the ISIS or via another DHCP server in the workshop network. This DHCP server ensures that the ISAP is automatically supplied with a required IP address.

Note:

If there are a number of ISIS subnets in the workshop network, check which network the ISAP is to be commissioned in and connect it to the ISIS that functions as the server for this network. Specific information for other details on networking in the workshop can be found in chapter 2.3.1 or through your market.

Note:

The ISAP is usually commissioned and operated in the same LAN segment as the corresponding ISIS. However, two other scenarios are also possible:

- The ISAP is first connected in the LAN segment of the ISIS and successfully configured with the steps described in the following sections. Then, the ISAP can be mounted in its final installation position and also connected to a LAN segment that does not contain the ISIS.
- Because of its installation position, the ISAP is commissioned and operated on a different LAN segment than that of the ISIS, using the steps described in the following sections. For this to occur, ISAP and ISIS must be able to exchange the multicast packages required by the Service Location Protocol (SLP). This means deployment and corresponding configuration of routers with multicast capability between the LAN subnets.

3.4.2 Sequence for commissioning

3.4.2.1 Reading off and noting down the LAN MAC address

The MAC address of LAN interface of the ISAP is a specific hardware address and its purpose is to uniquely identify the ISAP in the network. It is also required so that the WSM can identify and integrate the ISAP.

The MAC address of the LAN interface is located on the back of the ISAP. This must be noted down before the ISAP is installed and connected to the power supply and LAN in step 3.4.2.3.

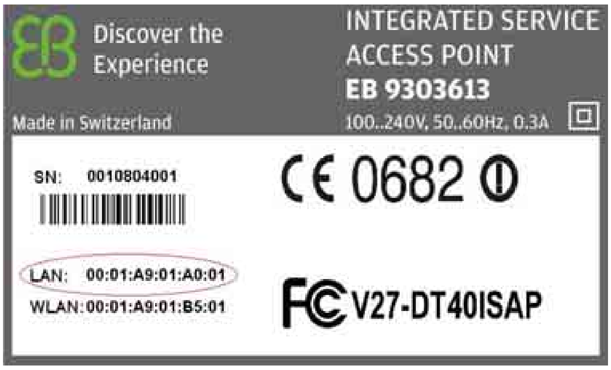


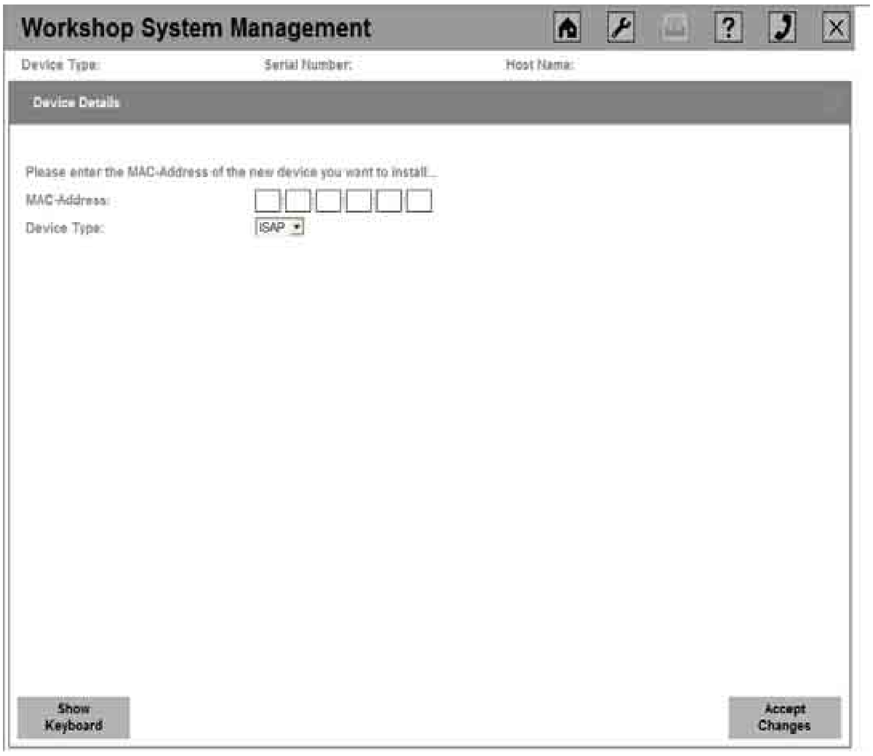
Fig. 73: Reading off the ISAP LAN MAC address

3.4.2.2 Setting up ISAP as a new device in the WSM

Please note:

This step must be performed before connection of the ISAP to the power supply and LAN. If the ISAP has already been connected to the power supply and LAN, disconnect the ISAP from both and, after completing the steps described in this section, briefly interrupt the power supply to restart the ISAP so that it can be recognized by the WSM.

- The WSM console of the ISIS cluster on which the ISAP is to be commissioned is accessed via the ISID or the workshop PC.
- In the System Overview, clicking the "New Device" button takes you to the screen for inputting the previously noted MAC address of the LAN interface of the ISAP.
- Select "ISAP" as device type, enter the MAC address, and click the "Apply" button (see Fig. 74). This meets the requirements for the ISAP to be recognized as a new device when it is connected to the workshop LAN.



Device Type:
Serial Number:
Host Name:

Please enter the MAC-Address of the new device you want to install...

MAC-Address: □□□□□□

Device Type: ISAP

Fig. 74: Selection of ISAP device type and input of the ISAP MAC address

3.4.2.3 Installing ISAP and connection to the network

- The ISAP should now be installed according to the guidelines in the ISAP User Guide. Bear in mind that compliance with these guidelines with regard to the installation position of the ISAP is critical to the later performance of the WLAN network.
- The ISAP is connected to the LAN subnet of the corresponding ISIS cluster.
- Do not connect the ISAP to the power supply until it has been connected to the LAN.
This sequence is necessary for proper powering up of the ISAP.

⚠	**Please note:** For initial configuration, the ISAP must be connected to the same LAN segment as the ISIS cluster. After completion of the initial configuration and a successful test of the WLAN functionality, the ISAP can also be connected to and operated on another LAN segment.

3.4.3 Registration of the ISAP

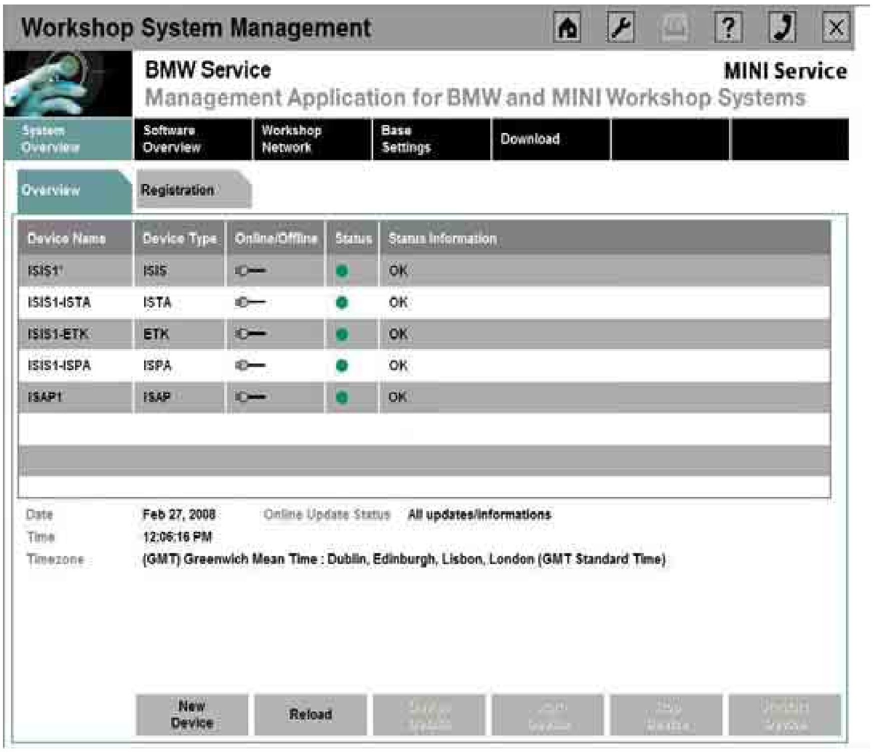
⚠	**Note:** The ISAP is registered according to the steps in chapter 5.1.3.4 for online registration or according to the steps in the chapters 5.1.3.5 and 5.1.3.6 for offline registration.

3.4.4 Update of the ISAP

ℹ	**Information:** If an update is available on the ISIS at the time that the ISAP is switched on, then it is automatically installed on the ISAP.

3.4.5 Standard configuration in the WSM

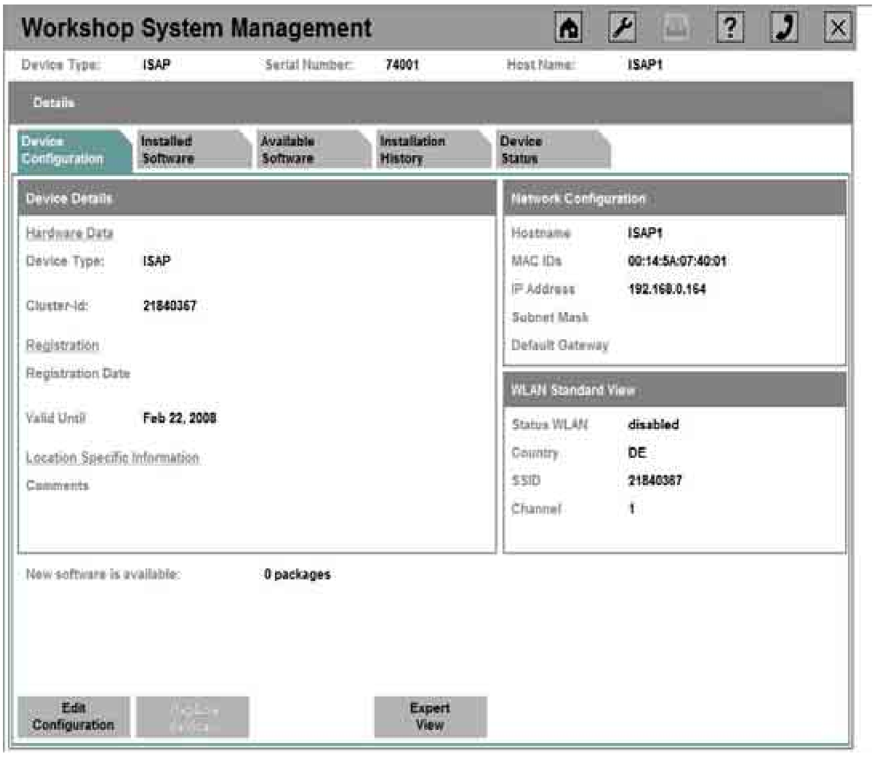
- Once the MAC address of the ISAP has been declared in the WSM and the ISAP has been connected to the LAN and power supply, WSM automatically recognizes the presence of a new ISAP device in the workshop network. The new device is listed in the WSM System Overview.
- In the System Overview, select the ISAP to be configured. "Device Details" takes the user to the standard view of the ISAP.
- When the "Edit Configuration" button is clicked, the user is prompted to enter the WSM administrator password, which activates the configuration mode.
- Within the framework of the initial configuration, a dialog box appears in a new window, prompting the user to restart the ISIS. For the rest of the configuration of the ISAP, the prompt must be confirmed by clicking "Yes".
- After restarting the ISIS, the ISAP is once again in the "Online" status (see Fig. 75). Clicking the "Device Details" button takes the user to the device configuration view of the ISAP (see Fig. 76).



Device Name	Device Type	Online/Offline	Status	Status Information
ISIS1'	ISIS	⊸	●	OK
ISIS1-ISTA	ISTA	⊸	●	OK
ISIS1-ETK	ETK	⊸	●	OK
ISIS1-ISPA	ISPA	⊸	●	OK
ISAP1	ISAP	⊸	●	OK

Date Feb 27, 2008 Online Update Status All updates/informations
Time 12:06:16 PM
Timezone (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London (GMT Standard Time)

Fig. 75: ISAP in the WSM System Overview after starting the ISIS



Device Type: ISAP Serial Number: 74001 Host Name: ISAP1

Device Details

Hardware Data
Device Type: ISAP
Cluster-Id: 21840367
Registration
Registration Date
Valid Until Feb 22, 2008
Location Specific Information
Comments

Network Configuration

Hostname ISAP1
MAC IDs 00:14:5A:07:40:01
IP Address 192.168.0.164
Subnet Mask
Default Gateway

WLAN Standard View

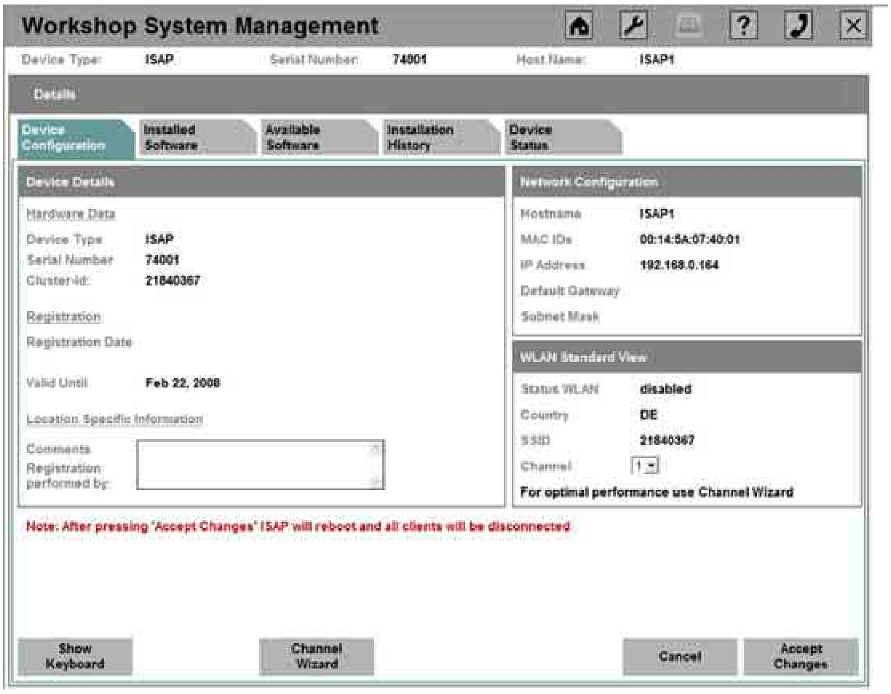
Status WLAN disabled
Country DE
SSID 21840367
Channel 1

New software is available: 0 packages

Fig. 76: View of the device configuration of the ISAP during initial configuration

- When the "Edit Configuration" button is clicked, the user is prompted to enter the WSM administrator password, which activates the configuration mode. This mode enables editing of the "Comments" field and selection of a suitable WLAN radio channel ("Channel" field) (see Fig. 77).

⚠	**Note:** Initially, setting the radio channel is only possible manually on initial installation of the ISAP. The reason for this is that the ISAP is delivered with the WLAN interface disabled. The WLAN interface is only enabled after completion of the initial installation and the "WLAN Status" in the WSM console is set to "enabled". From this point on, the "Channel Wizard" should be used to optimize the setting of the radio channel (see chapter 3.4.6).



Workshop System Management

Device Type: ISAP
Serial Number: 74001
Host Name: ISAP1

Details

Device Details

Hardware Data

Device Type: ISAP
Serial Number: 74001
Cluster-id: 21840367

Registration

Registration Date

Valid Until: Feb 22, 2008

Location Specific Information

Comments
Registration performed by:

Network Configuration

Hostname: ISAP1
MAC IDs: 00:14:5A:07:40:01
IP Address: 192.168.0.164
Default Gateway
Subnet Mask

WLAN Standard View

Status WLAN: disabled
Country: DE
SSID: 21840367
Channel: 1

For optimal performance use Channel Wizard

Note: After pressing 'Accept Changes' ISAP will reboot and all clients will be disconnected

Fig. 77: Editing the device configuration

- After the "Apply" button has been clicked, the new configuration is saved on the ISAP and the ISAP automatically reboots. After completion of the reboot (duration approx. 1 minute), the ISAP is ready for operation, but the display in the WSM System Overview only changes into the "OK" status after a delay of up to 1 minute. You can then start activating the WLAN functionality of the new generation devices in the workshop.

⚠	**Note:** If there are a number of WLAN networks, it is advisable to use the Channel Wizard (see next chapter).

3.4.6 Channel Wizard

The Channel Wizard helps you find the radio channel required for optimal performance of the WLAN radio network in the workshop. If you suspect that there are other WLAN radio networks in the immediate vicinity of the workshop that could disrupt the WLAN radio network, it is advisable to use the "Channel Wizard". It detects the interference from neighboring WLAN networks and suggests a radio channel that has the lowest level of interference and therefore promises the best performance.

The Channel Wizard can only be used after completion of the initial configuration of the ISAP, when the "Status WLAN" has the value "enabled".

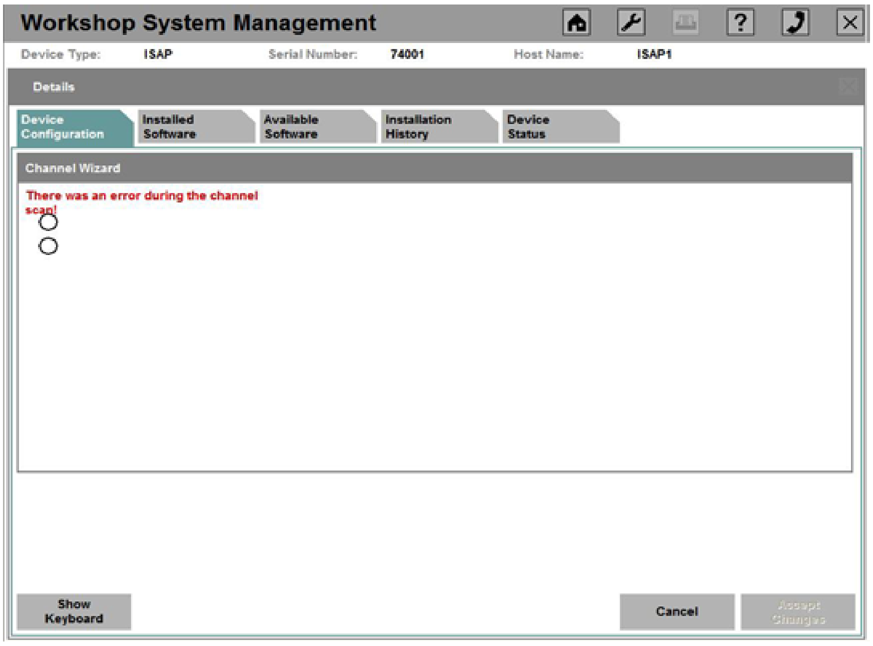
Use the following steps to find and set the optimal WLAN radio channel:

- Highlight the relevant ISAP in the WSM System Overview, select the "Device Details" menu and then the "Edit Configuration" tab, and click the "Channel Wizard" button
- The ISAP then scans all WLAN radio channels and checks whether the radio channels are occupied by other WLAN radio networks. This process can take up to 90 seconds.

ℹ	**Information:** During the scan operation, the current display does not change. On completion of the scan operation, a new view is set up.

- The scan operation also determines the strength of the received signals of the neighboring WLAN radio networks. On the basis of these measurements, the ISAP determines a recommendation that can be adopted by the user. To do so, click the radio button of the recommendation and then click the "Apply" button (see Fig. 78).
- When configuring the ISAP, if you know that the WLAN radio channel proposed by the Channel Wizard should not be selected, a list of other WLAN radio channel recommendations, sorted in descending order, is available, i.e. the table entry with no. 1 is the WLAN radio channel with the least interference, entry no. 2 is the WLAN radio channel with the second-lowest amount of interference, etc.

  However, it is not possible to adopt a WLAN radio channel directly from the list in this view. The user must note the relevant value, exit from the Channel Wizard by clicking "Cancel" and select the value for the WLAN radio channel in the configuration view.



Device Type: ISAP
Serial Number: 74001
Host Name: ISAP1

There was an error during the channel scan!

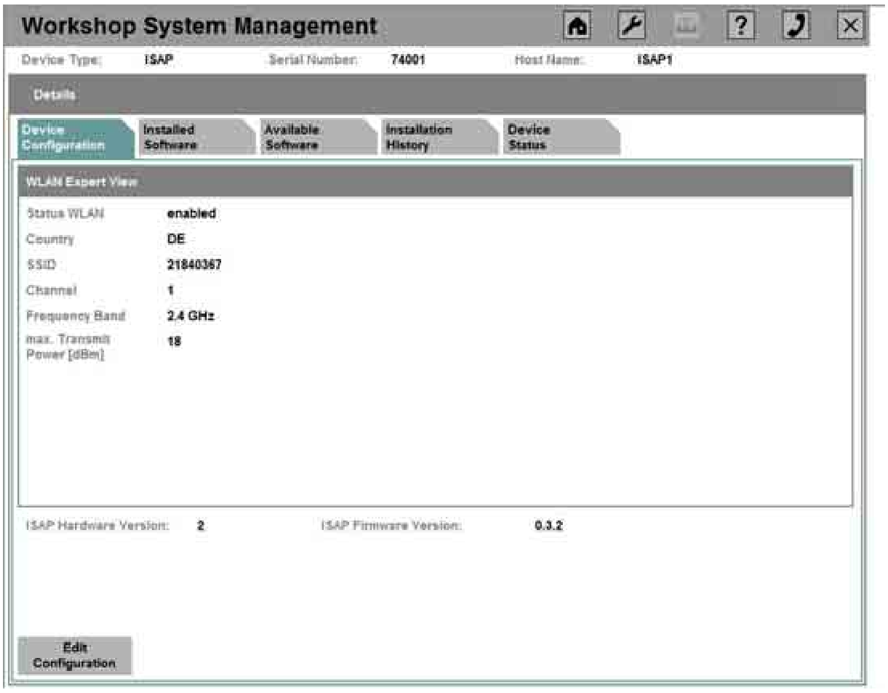
○
○

Fig. 78: Result and recommendation of the Channel Wizard

3.4.7 Expert configuration in the WSM

The steps described in section 3.4.4 commission the ISAP in a very simple manner, subsequently providing the desired WLAN functionality in the workshop. With this configuration, the ISAP transmits on a radio channel in the 24 GHz band.

The existence of WLAN radio networks or deployment of more than one ISAP can make it necessary under certain circumstances to operate the ISAP in the 5 GHz band. The switch from the default 2.4 GHz band into the 5 GHz band and selection of a corresponding WLAN radio channel from this band take place in the "Expert View".



Device Type: ISAP
Serial Number: 74001
Host Name: ISAP1

Status WLAN	enabled
Country	DE
SSID	21840367
Channel	1
Frequency Band	2.4 GHz
max. Transmit Power [dBm]	18

ISAP Hardware Version: 2
ISAP Firmware Version: 0.3.2

Fig. 79: Expert View of the device configuration of the ISAP

To support optimized selection of a WLAN radio channel, it is advisable to use the "Channel Wizard" in the "Expert View" to measure the existing usage of the 2.4 GHz and 5 GHz bands and to obtain a recommendation for a radio channel from the ISAP. Using it takes the user through a procedure analogous to the one described in section 3.4.6.

4 Installation of the ISIS software on the workshop PC

So that a workshop PC can be used in conjunction with an ISIS, the corresponding software is delivered with the ISIS. This software runs on any standard PC equipped with the operating system Windows XP (with Service Pack 2 or later).

⚠	**Note 1:** To install the packages on the workshop PC, the corresponding applications must already have been installed on the ISIS.

⚠	**Note 2:** Administrator rights are required for installation of the applications on the workshop PC.

4.1 Installation of the ISIS Launcher on the workshop PC

⚠	**Note:** The ISIS Launcher must be installed on the workshop PC in order to use ISTA, EPC, and ISPA on this PC.

To install the client software, the IP of an ISIS must be entered in the browser (see Fig. 80). The WSM System Overview is displayed. Selecting the "Software Overview" menu and the "Client Installer" tab opens a dialog box (see Fig. 81) that displays the available software packages.

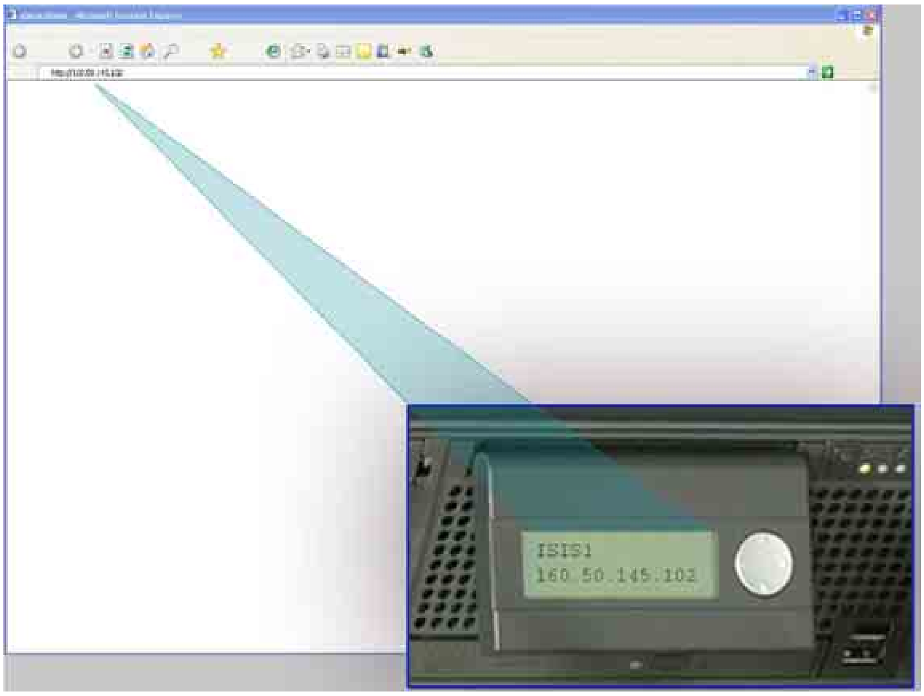
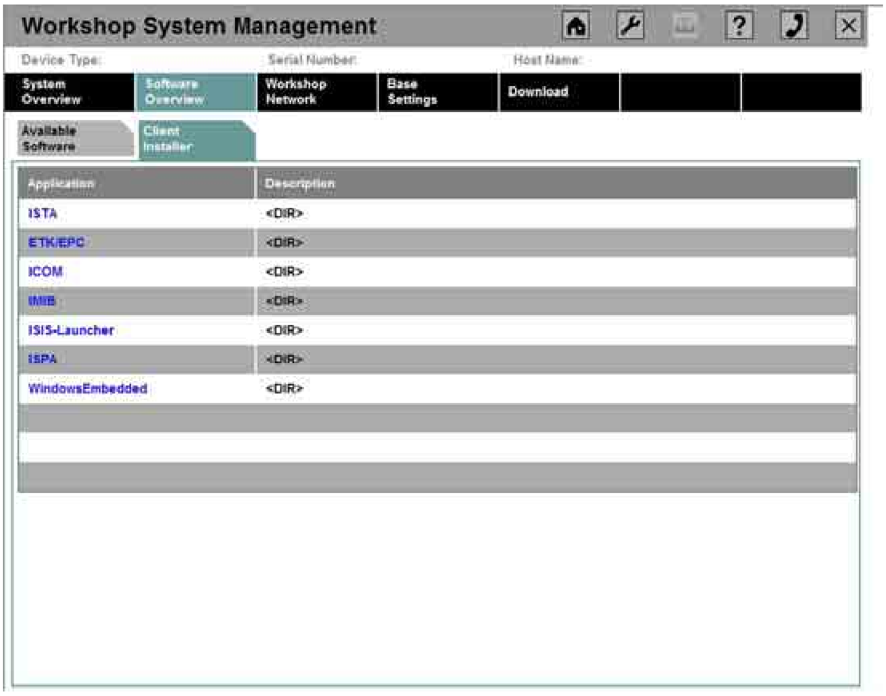


Fig. 80: Input of the ISIS IP into the browser



Application	Description
ISTA	<DIR>
ETK/EPC	<DIR>
ICOM	<DIR>
IMIB	<DIR>
ISIS-Launcher	<DIR>
ISPA	<DIR>
WindowsEmbedded	<DIR>

Fig. 81: Software for the workshop PC

Selecting the package and clicking the "Save" button as confirmation in the pop-up window that appears downloads the software package onto the workshop PC. It can then be started from the corresponding memory location.

Clicking the "Run" button in the pop-up window that appears triggers immediate initialization of the installation process without downloading the package.

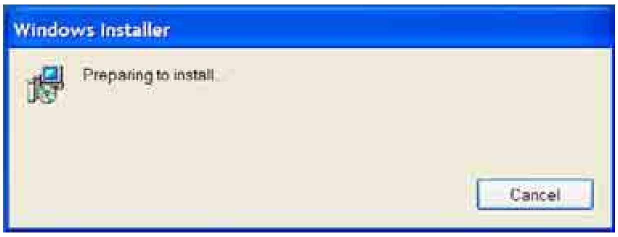
In a first step, the ISIS Launcher must be installed on the workshop PC and then started. The ISIS Launcher prepares the PC to use the ISIS software (e.g. ISTA, ISPA or EPC).

To do so, perform the following steps after downloading the package:

Step 1:

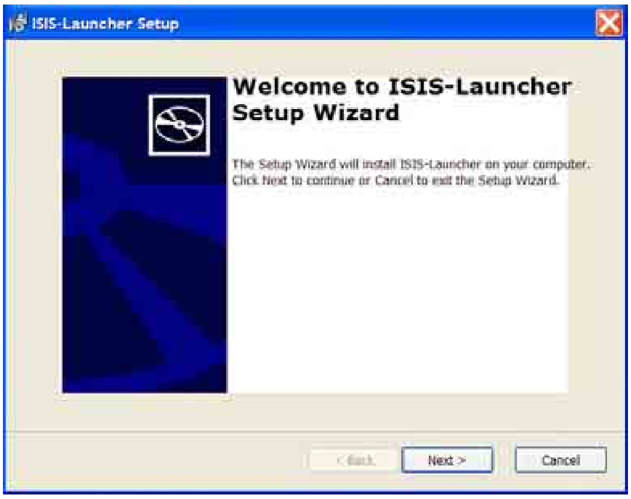
Starting the installer via the icon from Fig. 82 or the "Run" button in the pop-up window initializes the installation process (see Fig. 83). Then the setup wizard is started and the following prompt (see Fig. 84) appears.

Fig. 82: Installer for the ISIS Launcher



Preparing to install...

Fig. 83: Preparation for installation of the ISIS Launcher



Welcome to ISIS-Launcher Setup Wizard

The Setup Wizard will install ISIS-Launcher on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

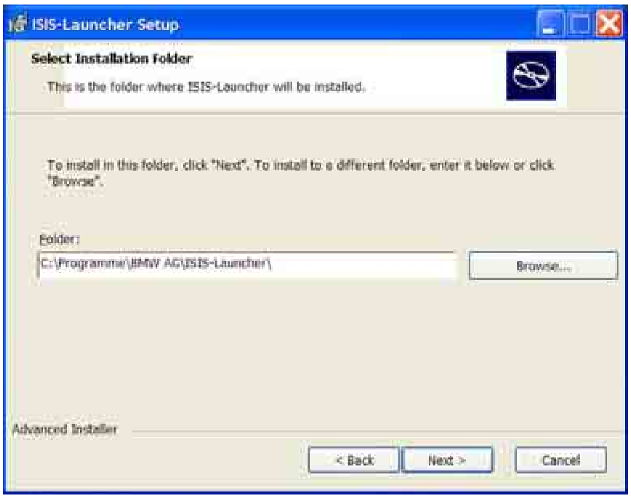
Fig. 84: ISIS Launcher setup – step 1

Clicking the "Next" button takes the user to the next dialog box (see Fig. 85).

The installation can be cancelled by clicking the "Cancel" button.

Step 2:

In the window that follows, select the directory in which the ISIS Launcher is to be installed (see Fig. 85).


ISIS-Launcher Setup

Select Installation Folder

This is the folder where ISIS-Launcher will be installed.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder:
C:\Programme\BMW AG\ISIS-Launcher\

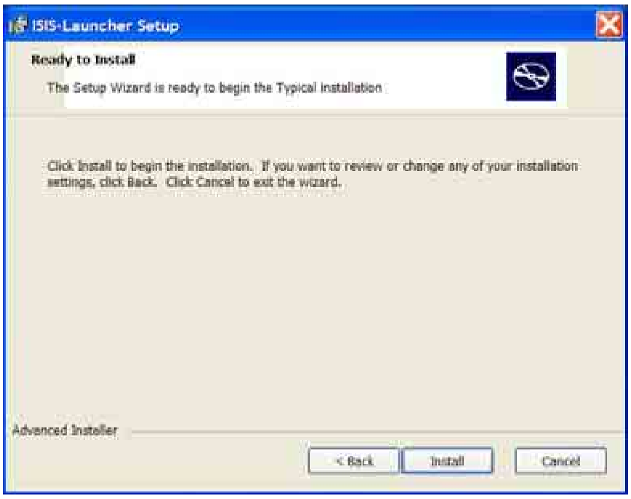
Fig. 85: ISIS Launcher setup – step 2

Clicking "Next" confirms the input and opens the next dialog box (see Fig. 86).

The installation can be cancelled by clicking the "Cancel" button.

Step 3:

The installation of the software package is started by clicking the "Install" button (see Fig. 86).


ISIS-Launcher Setup

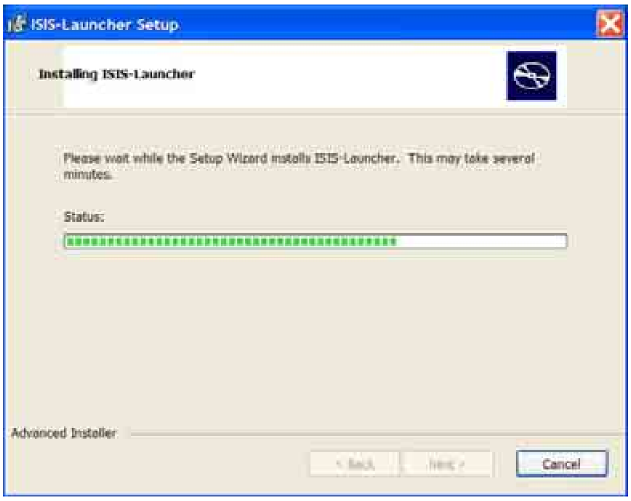
Ready to Install

The Setup Wizard is ready to begin the Typical installation

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Fig. 86: ISIS Launcher setup – step 3

During the installation, the following progress bar appears (see Fig. 87).



Installing ISIS-Launcher

Please wait while the Setup Wizard installs ISIS-Launcher. This may take several minutes.

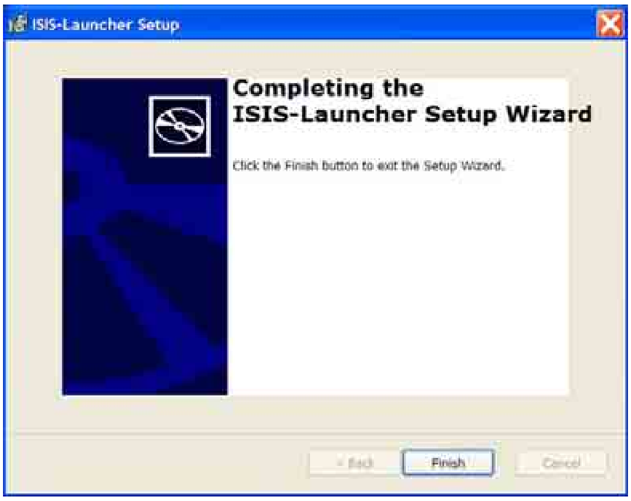
Status:

Advanced Installer

Fig. 87: ISIS Launcher setup – step 3

Step 4:

To conclude the installation, click the "Finish" button in the next window (see Fig. 88).



Completing the ISIS-Launcher Setup Wizard

Click the Finish button to exit the Setup Wizard.

Fig. 88: ISIS Launcher setup – step 4

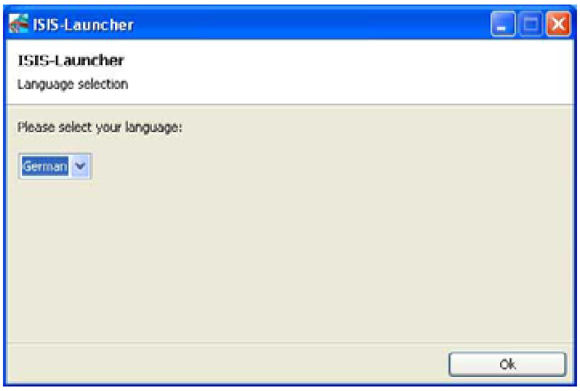
4.1.1 Initial start of the ISIS Launcher

After the installation, the ISIS Launcher starts automatically. If this does not occur, the ISIS Launcher can be started manually using the Windows start menu.

Language selection for the ISIS Launcher:

> **Note:**
>
> If an ISIS Launcher was already installed on the workshop PC, the prompt for the language setting is no longer displayed and the language of the previously installed ISIS Launcher is used.

First, a prompt appears for the language selection (see Fig. 89); in this case, though, there is only a choice between German and English.



ISIS-Launcher

ISIS-Launcher
Language selection

Please select your language:

German

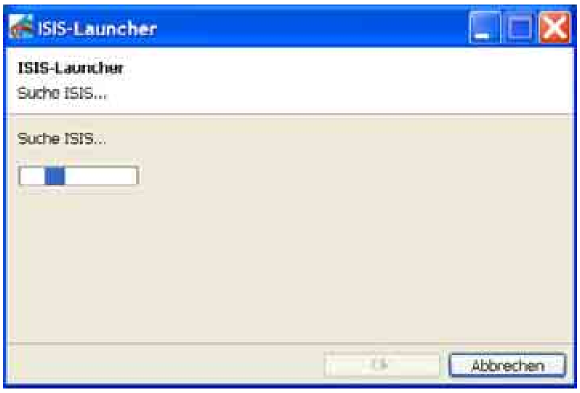
Fig. 89: Language selection for the ISIS Launcher

Clicking the "OK" button starts the automatic search for an ISIS (see Fig. 90).

The ISIS Launcher can be terminated during the next steps by clicking "Cancel".

Searching for an ISIS:

First, an automatic search is run for an ISIS (see Fig. 90).



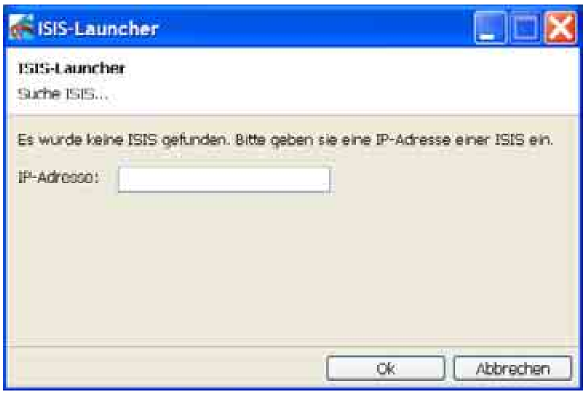
ISIS-Launcher

ISIS-Launcher
Suche ISIS...

Suche ISIS...

Fig. 90: Automatic search for an ISIS

If the ISIS Launcher does not find the ISIS automatically in the course of the initial start, the Launcher starts an IP query (see Fig. 91).



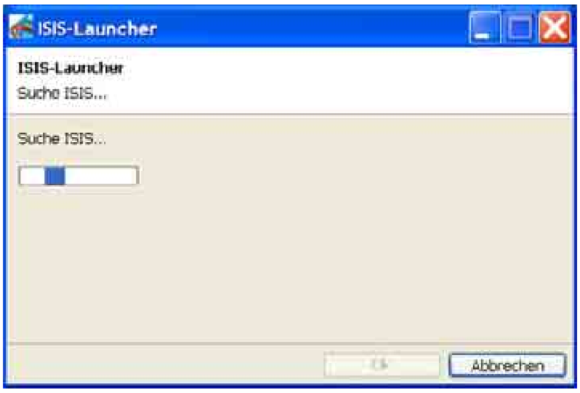
ISIS-Launcher
Suche ISIS...

Es wurde keine ISIS gefunden. Bitte geben sie eine IP-Adresse einer ISIS ein.

IP-Adresse:

Fig. 91: Starting an IP query

Enter the IP address of the ISIS in the free field for "IP address" and then confirm this by clicking "OK".



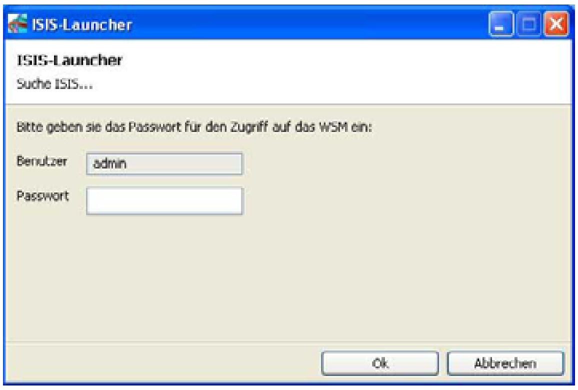
ISIS-Launcher
Suche ISIS...

Suche ISIS...

Fig. 92: Search for the ISIS

If the ISIS Launcher has received the corresponding IP address, its starts the search for the ISIS (see Fig. 92). If the search is successful, the next dialog box appears (see Fig. 93).

If no ISIS is found, the dialog box from Fig. 91 is displayed again.



ISIS-Launcher

ISIS-Launcher
Suche ISIS...

Bitte geben sie das Passwort für den Zugriff auf das WSM ein:

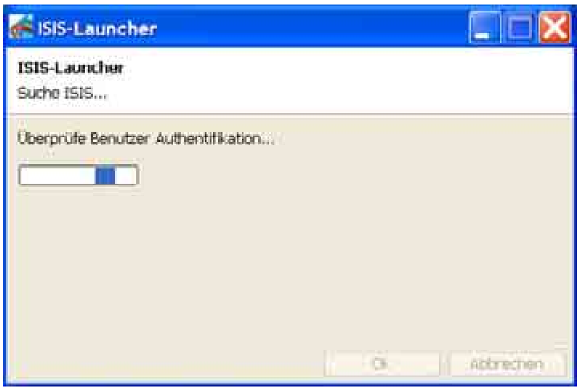
Benutzer: admin

Passwort:

Fig. 93: Starting a user query for the password

For authorization of the access, the expression "admin" is a fixed default setting in the user line. The password is the password established during installation (see chapter 3.1.8.2) or the password changed at a later point (see chapter 5.1.17).

i	**Information:** The password query only appears when the Launcher is started for the first time or if the WSM password has been changed.



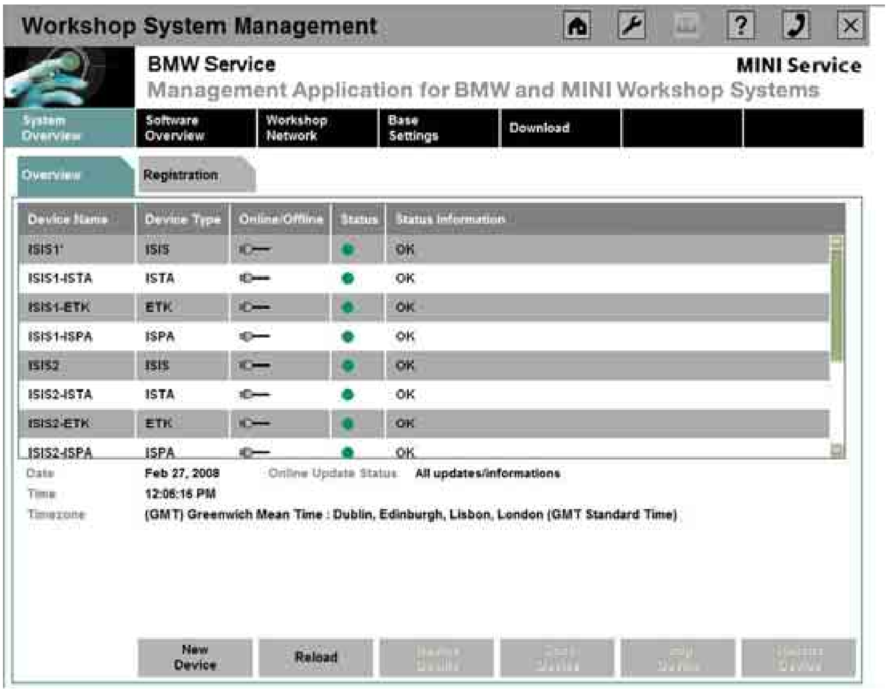
ISIS-Launcher

ISIS-Launcher
Suche ISIS...

Überprüfe Benutzer Authentifikation...

Fig. 94: Check of authorization

After a successful check of the user authorization (see Fig. 94), the ISIS Launcher starts the WSM System Overview in a Web browser (see Fig. 95). The workshop PC is thus prepared for use together with the ISIS.



Device Name	Device Type	Online/Offline	Status	Status Information
ISIS1'	ISIS		●	OK
ISIS1-ISTA	ISTA		●	OK
ISIS1-ETK	ETK		●	OK
ISIS1-ISPA	ISPA		●	OK
ISIS2	ISIS		●	OK
ISIS2-ISTA	ISTA		●	OK
ISIS2-ETK	ETK		●	OK
ISIS2-ISPA	ISPA		●	OK

Date Feb 27, 2008 Online Update Status All updates/informations
Time 12:08:16 PM
Timezone (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London (GMT Standard Time)

Fig. 95: Display after connection of the ISIS Launcher to an ISIS

4.1.2 Status messages in the notification field

The symbol in the notification field of the task bar can be used to monitor the current status of the ISISs (see Fig. 96).

The status symbol can be activated via the entry "Launcher Notification" in the Windows start menu. After the first start, the status symbol opens automatically every time the workshop PC is started.

Depending on the status of the ISIS, information is shown in a speech balloon in the notification field, e.g. "No Connection to ISIS" (see Fig. 96).

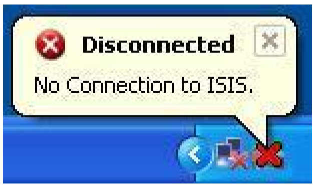

Disconnected
No Connection to ISIS.

Fig. 96: Message ISIS Disconnect

More information on problems that occur can be found in the "Device Details".

Possible statuses of the ISIS indicated by a status symbol:

Symbol	Condition
🌐	The ISIS can be reached and there are no problems.
!	A problem has occurred, but the ISIS is able to continue working.
❗	A problem has occurred that restricts the functionality of the ISIS.
❌	The ISIS cannot be reached.

4.1.3 Update of the ISIS Launcher

If a new version of the ISIS Launcher is available, this is downloaded automatically to the workshop PC and installed the next time the PC is started.

4.2 Software package ISTA for the workshop PC

⚠	**Note:** The ISIS Launcher must be installed on the workshop PC in order to use ISTA on this PC.

To install the ISTA client, open the ISTA installation package in the WSM menu "Software Overview" under the tab "Client Installer" (see Fig. 81). More information is given in the documentation for the ISTA application.

4.3 Software package ISPA for the workshop PC

⚠	**Note:** The ISIS Launcher must be installed on the workshop PC in order to use ISPA on this PC.

To install the ISPA client, open the ISPA installation package in the WSM menu "Software Overview" under the tab "Client Installer" (see Fig. 81). More information is given in the documentation for the ISPA application.

4.4 Software package EPC for the workshop PC

⚠	**Note:** The ISIS Launcher must be installed on the workshop PC in order to use EPC on this PC.

To install the EPC client, open the EPC installation package in the WSM menu "Software Overview" under the tab "Client Installer" (see Fig. 81). More information is given in the documentation for the EPC application.

5 Using the WSM

5.1 Overview

5.1.1 General functions in the WSM

This chapter describes the general functions behind the icons in the icon bar. Since this bar appears on each individual screen of the Web interface, the following functions can be activated from each screen within the WSM.

5.1.1.1 Start page

Clicking the 'Home' icon (see Fig. 97) in the icon bar opens the start page of the WSM.

Fig. 97: Home icon

The start page shows the menu items "System Overview", "Software Overview", "Workshop Network", "Base Settings" and "Download", which are explained below:

- The menu item "System Overview" shows all new generation workshop devices that are enabled or disabled in the workshop environment.
- The menu item "Software Overview" is used to manage the software of the ISIS, the software systems ISTA, ISPA and EPC, as well as the data of the new hardware generation.
- The menu item "Workshop Network" is used to administer the automatic IP management for the new device hardware generation.
- The menu item "Base Settings" is used to configure dealer data, etc..
- The menu item "Download" makes documents created on the ISID available for downloading.

5.1.1.2 Administration - setting the WSM language and the brand

Clicking the 'wrench' icon (see Fig. 98) in the icon bar opens the 'Administration' screen (see Fig. 99) of the WSM.

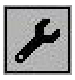
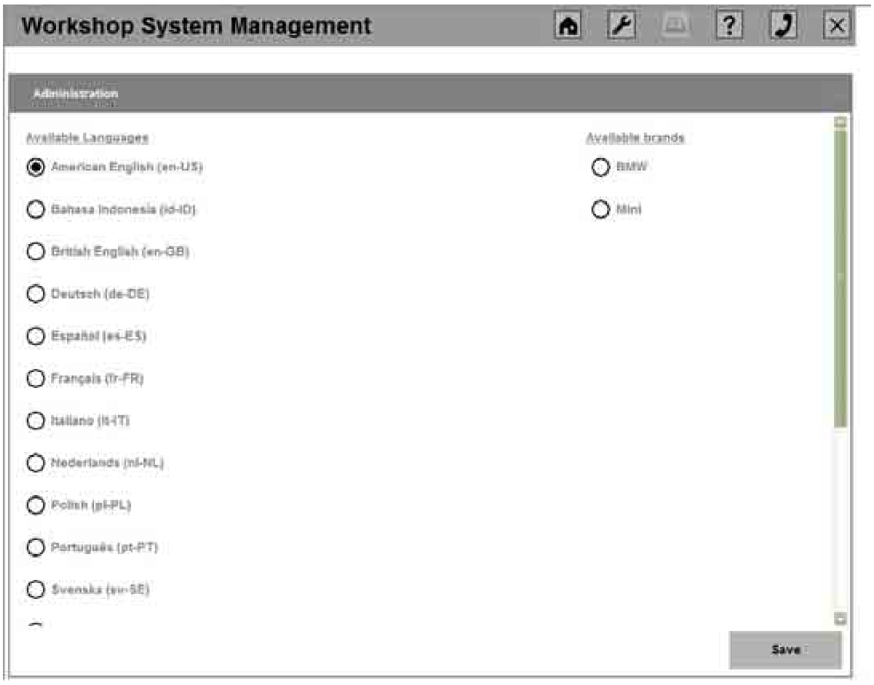


Fig. 98: 'Wrench' icon



Workshop System Management

Administration

Available Languages

● American English (en-US)

○ Bahasa Indonesia (id-ID)

○ British English (en-GB)

○ Deutsch (de-DE)

○ Español (es-ES)

○ Français (fr-FR)

○ Italiano (it-IT)

○ Nederlands (nl-NL)

○ Polish (pl-PL)

○ Português (pt-PT)

○ Svenska (sv-SE)

Available brands

○ BMW

○ Mini

Fig. 99: Administration – setting the language and brand

On the 'Administration' screen, you can specify the language of the WSM user interface and the brand, thus setting the color assignment of the active menus in the WSM.

Select the language on the left-hand side by clicking the corresponding radio button to the left of the relevant language.

On the right-hand side, the list of brands available to this dealer is displayed according to the dealer data. Selecting the relevant brand sets the color assignment of the active menu.

Clicking the "Save" button adopts the changes.

5.1.1.3 Printing

ℹ	**Information:** This icon (see Fig. 100) can be used to print all the completed WSM configurations. This function is unavailable at the moment.

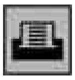


Fig. 100: Printer icon

5.1.1.4 Help - WSM User Guide and system information

Clicking the question mark icon (see Fig. 101) in the icon bar opens the Help screen (see Fig. 102) with the tabs "Index" and "System Information" of the WSM.

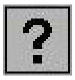
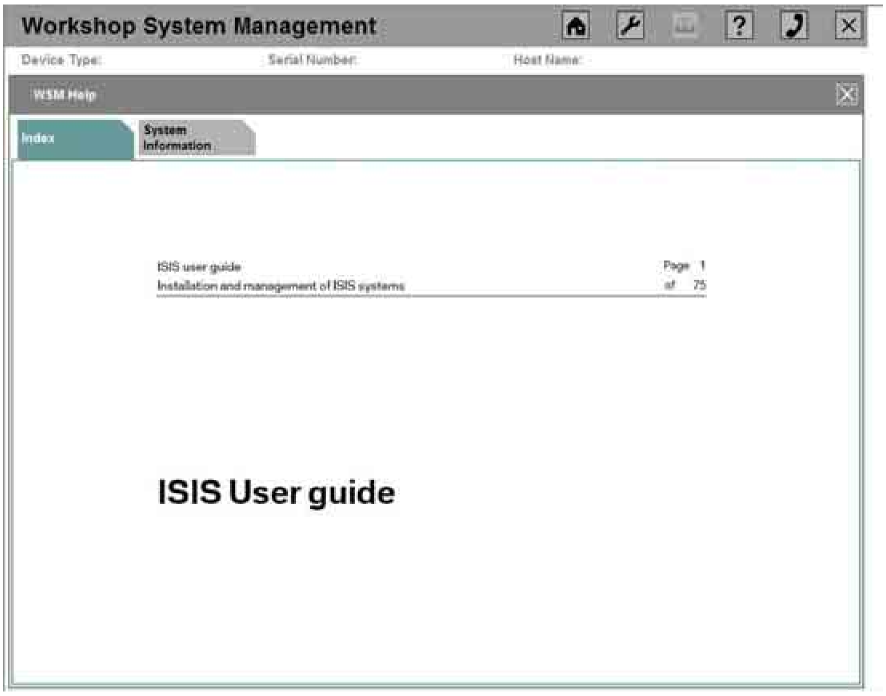


Fig. 101: Question mark icon



ISIS user guide
Installation and management of ISIS systems
Page 1
of 75

ISIS User guide

Fig. 102: WSM help (User Guide)

This User Guide can be found in PDF format under the "Index" tab (see Fig. 102) and the installed WSM version appears under the "System Information" tab.

5.1.1.5 Callback

Clicking the telephone receiver icon (see Fig. 103) in the icon bar opens the start page to enter a callback, i.e. a query to BMW support, or displays an overview of existing callbacks (see Fig. 104).

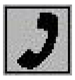
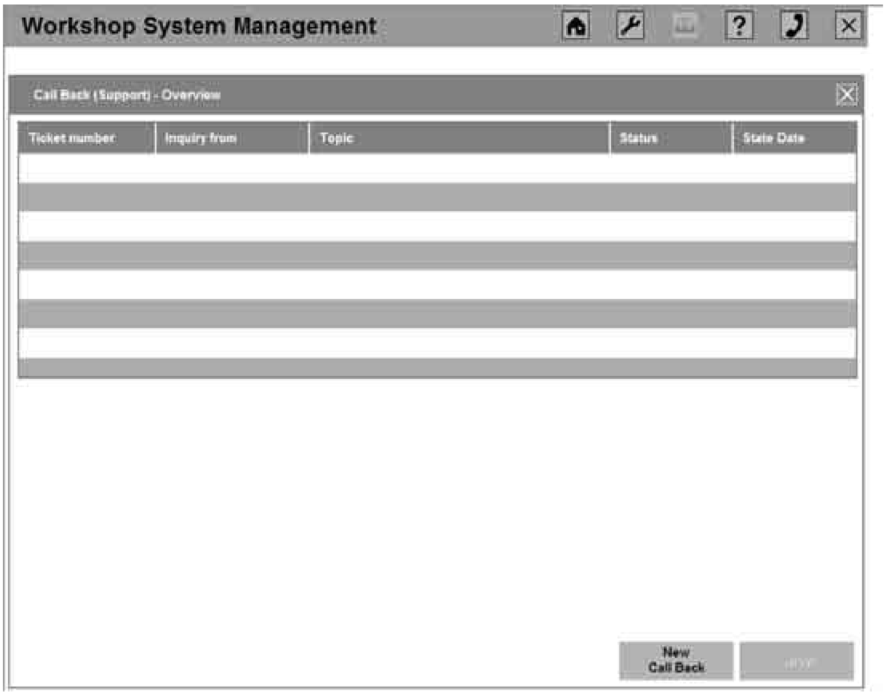


Fig. 103: Telephone receiver icon



Ticket number	Inquiry from	Topic	Status	State Date

Fig. 104: Callback start page

More detailed information on the procedure for entering a callback is given in section 8.5.

5.1.1.6 Closing the WSM

Clicking the "X" icon (see Fig. 105) in the icon bar closes the current WSM session and closes the browser.

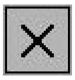


Fig. 105: X icon

To start a new WSM session, either start the ISIS Launcher or enter the IP address of the ISIS in the browser.

ℹ	**Information:** Clicking the "X" icon in the WSM on the ISID opens the start page of the ISID (Jumpgate).

5.1.2 Adding and removing devices in the WSM

All the devices that can be used in the workshop are listed in the WSM "System Overview".

To keep this overview up to date, it is necessary for all new devices to be recorded in the WSM and for all devices that are no longer used in the workshop to be removed from the "System Overview".

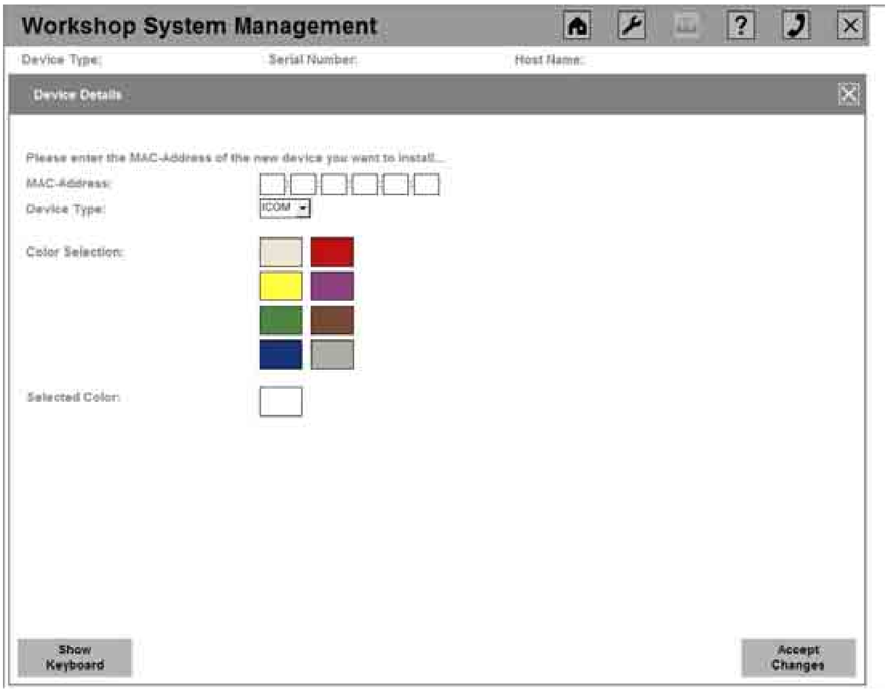
5.1.2.1 Adding devices to the WSM

Note:

In this context, follow the instructions in the chapters on commissioning the individual devices (for ISID chapter 3.2, for ICOM chapter 3.3, and for ISAP chapter 3.4).

As a general principle, adding devices to the WSM works as follows:

- In the WSM, click the "New device" button on the start page.
- In the dialog box that follows (see Fig. 106), enter the MAC address of the device (which you noted down before) and select the device type ("ISID", "ICOM", or "ISAP".



Workshop System Management

Device Type: Serial Number: Host Name:

Device Details

Please enter the MAC-Address of the new device you want to install...

MAC-Address: □ □ □ □ □ □

Device Type: ICOM

Color Selection:

Selected Color: □

Fig. 106: Adding a new device to the WSM

- For an ICOM, an additional color can be selected to make it easier, among other things, to assign it to a color marking.

- Confirm the input by clicking the "Apply" button. This sets up a new device.

5.1.2.2 Removing devices from the WSM

Information:

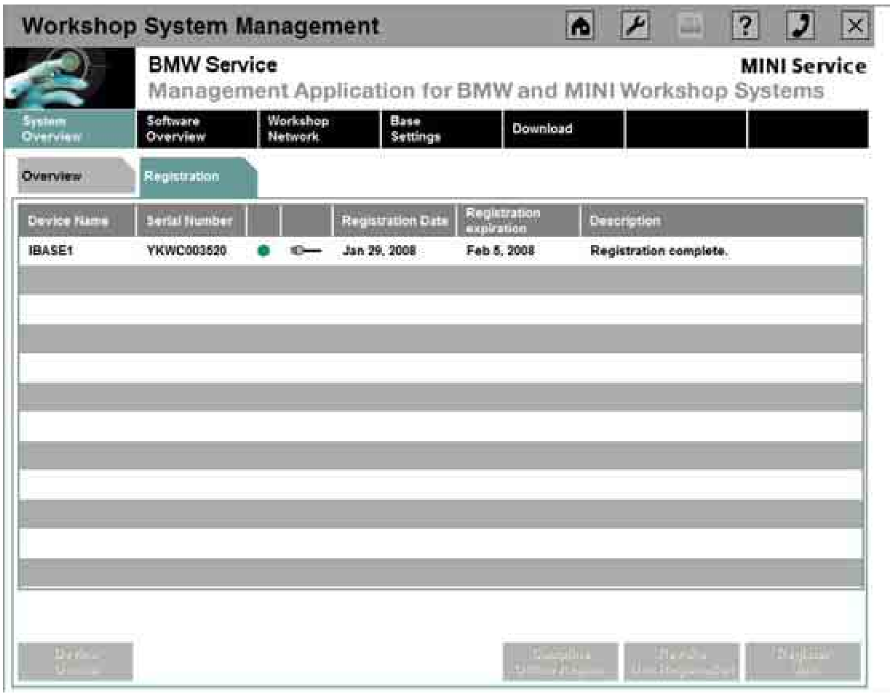
At the time of this printing, it is not yet possible to remove devices from the WSM overview.

5.1.3 Registration of devices

Note:

The maximum number of registered servers for one dealer is normally two server plug-in modules.

The current status of the registration of the individual devices is shown in the "System Overview" in the "Registration" tab (see Fig. 107).



Device Name	Serial Number			Registration Date	Registration expiration	Description
IBASE1	YKWC003520	●	⊸	Jan 29, 2008	Feb 5, 2008	Registration complete.

Fig. 107: Registration overview

This overview also provides the following information:

- Device and its serial number
- Registration status

Symbol	Meaning

🔴	"unregistered" Either no registration has been carried out for this device, the (temporary) registration of the device has expired, the device is already registered at another dealer (another sales partner no.), or a technical error has occurred during registration.
🟡	"not online" The online connection to the central BMW server is either missing or disconnected.
🟢	"registered" A registration of the device has been carried out successfully.
⚪	"still open" A registration fax has been created and sent, but the second part of the offline registration has not yet been carried out.

- Registration date and end of the registration
- Description of the registration status, for example if the second part of the offline registration has not yet been carried out

There are two different types of registration with regard to the Internet connection of the dealer:

- Online registration for dealers that are connected to the BMW Group via the Internet
- Offline dealers (also independent dealers) that are not connected to the BMW Group via the Internet

5.1.3.1 Purpose of registration

The registration promotes user support and the tracking of devices in the event of theft. Without registration (or before the registration has been successfully concluded), the device can only be used to run the WSM, i.e. applications cannot be used without a valid registration.

A device that is already registered cannot be registered again in another ISIS network (e.g. at another dealer).

5.1.3.2 Types of dealer and their registration options

Internet access is required for the online registration procedure. The authorized dealer must have this access so that the registration data can be exchanged via Internet between the dealer and BMW.

If no Internet access is available, then an offline registration can be made via fax using a registration form.

Authorized dealers with Internet connection and access to the BMW portal

Authorized dealers who have an Internet connection and a BMW portal login account can carry out the registration online by selecting the corresponding portal from a list.

Authorized dealers with Internet connection but no access to the BMW portal

Authorized dealers with an Internet connection but no BMW portal login account can, if they wish to use the online functions, request a portal login account (e.g. S-Gate) from their distribution company on delivery of the ISIS. That portal can be used for online registration but not for accessing any other BMW online application. If a defined portal access account is not requested, the offline registration alternative must be used.

Authorized dealer without Internet connection:

The registration must be carried out as an offline registration.

As soon as the dealer is granted access to the BMW dealer portal, the offline registration can be switched at any time to an online registration.

Independent dealer:

An independent dealer must carry out an offline registration.

5.1.3.3 Effect of the ISIS registration on the registration of other devices

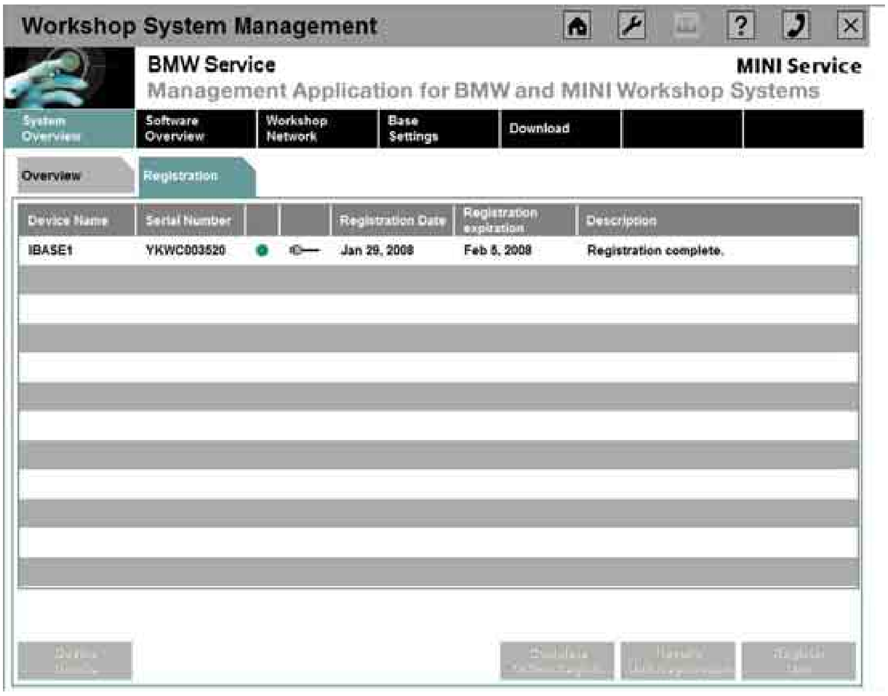
Registering new generation devices (ISID, ICOM, ISAP) requires prior registration of the relevant ISIS ("online" or "offline") and thus also the availability of dealer master data on the ISIS. A valid registration of the ISIS is required for registration of an ISID or ICOM.

ℹ	**Information:** In the case of an online dealer who has registered the ISIS online, the registrations of the other devices are also carried out online. In the case of an offline dealer, a registration fax must be sent for every additional device registration.

5.1.3.4 Carrying out the online registration

ℹ	**Information:** The procedure described below should also be followed if the registration was skipped in the configuration wizard on registration of the ISIS.

⚠	**Note:** Please make sure that you have selected the corresponding dealer portal (corresponding chapter 5.1.13) and contact person (corresponding chapter 5.1.8).



Device Name	Serial Number			Registration Date	Registration expiration	Description
IBASE1	YKWC003520	●		Jan 29, 2008	Feb 5, 2008	Registration complete.

Fig. 108: Registration overview

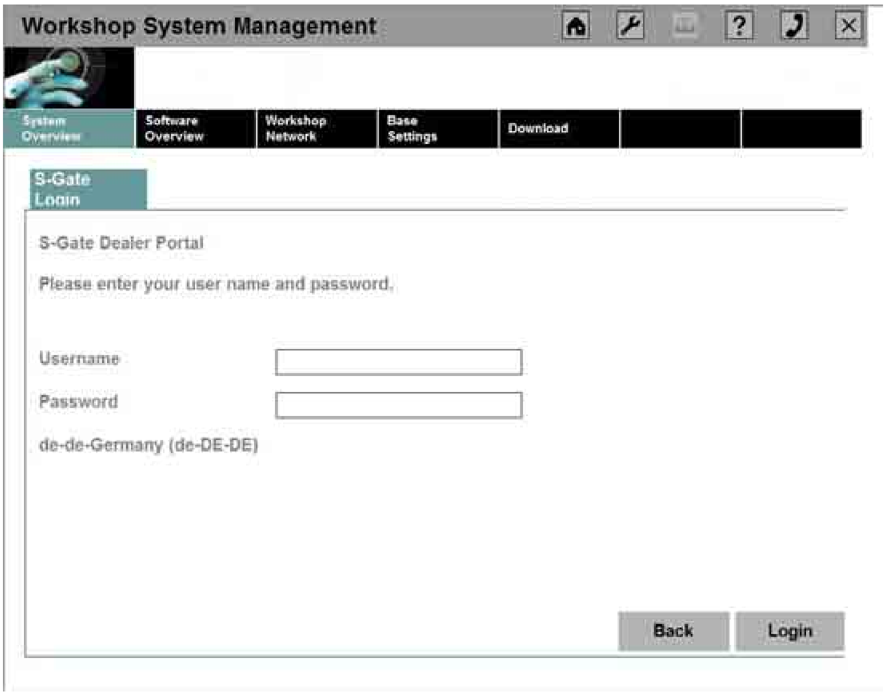
Selecting the "Registration" tab in the "System Overview" displays all devices that can be registered or have already been registered (see Fig. 108).

To register a device, select it and then click the "Register device" button.

Note:

Registering the devices ICOM, ISID and ISAP no longer requires the portal login because registration of the devices only takes place on the ISIS.

A screen appears that queries the dealer portal access data (see Fig. 109, demonstrated here with an S-Gate access as an example).



S-Gate Dealer Portal

Please enter your user name and password.

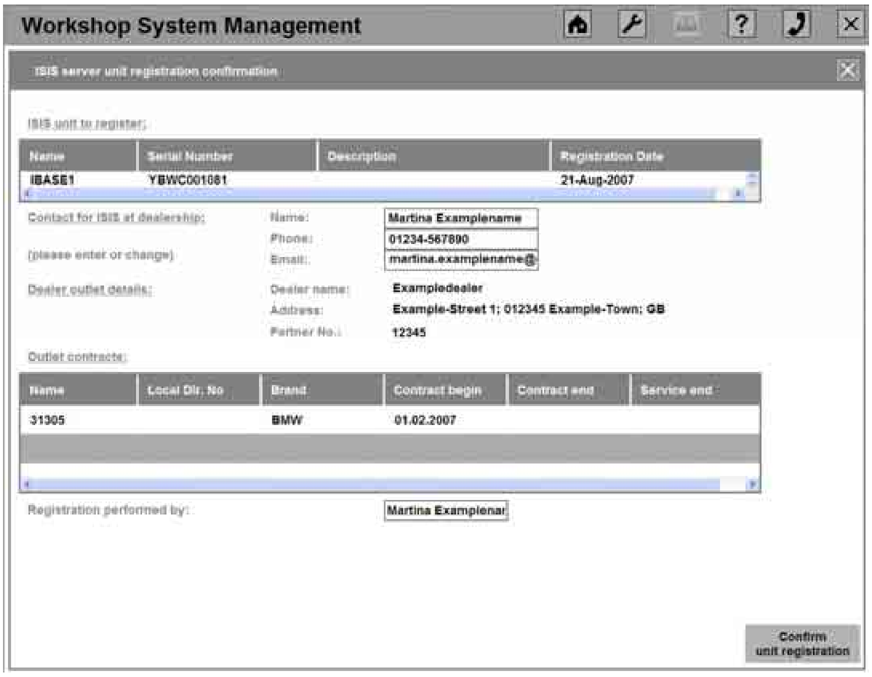
Username

Password

de-de-Germany (de-DE-DE)

Fig. 109: Online registration: Query of dealer portal access data

After successful input and subsequent check of the input data, the screen for registration of the selected device (see Fig. 110) is displayed.


Workshop System Management
ISIS server unit registration confirmation
Confirm unit registration

ISIS unit to register:

Name	Serial Number	Description	Registration Date
IBASE1	YBWC001081		21-Aug-2007

Contact for ISIS at dealership: Name: Martina Examplename

(please enter or change) Phone: 01234-567890

Email: martina.examplename@

Dealer outlet details: Dealer name: Exampledealer

Address: Example-Street 1; 012345 Example-Town; GB

Partner No.: 12345

Outlet contracts:

Name	Local Dir. No	Brand	Contract begin	Contract end	Service end
31305		BMW	01.02.2007		

Registration performed by: Martina Examplenar

Fig. 110: Carrying out the online registration

The following data is entered automatically in the corresponding fields in the screen shown above (see Fig. 110):

- Device to be registered (name, serial number, description and registration date)
- Dealership branch details (dealership branch, address and partner number)
- Existing contracts with the dealership branch

The following fields for the contact person responsible in the dealer company are to be completed:

- Name
- Phone
- E-mail address

Clicking the "Confirm Registration" button initiates a check of the entered data and carries out the registration. To confirm the success of the process, you can look in the "System Overview" under the "Registration" tab to see whether the status has been set to green.

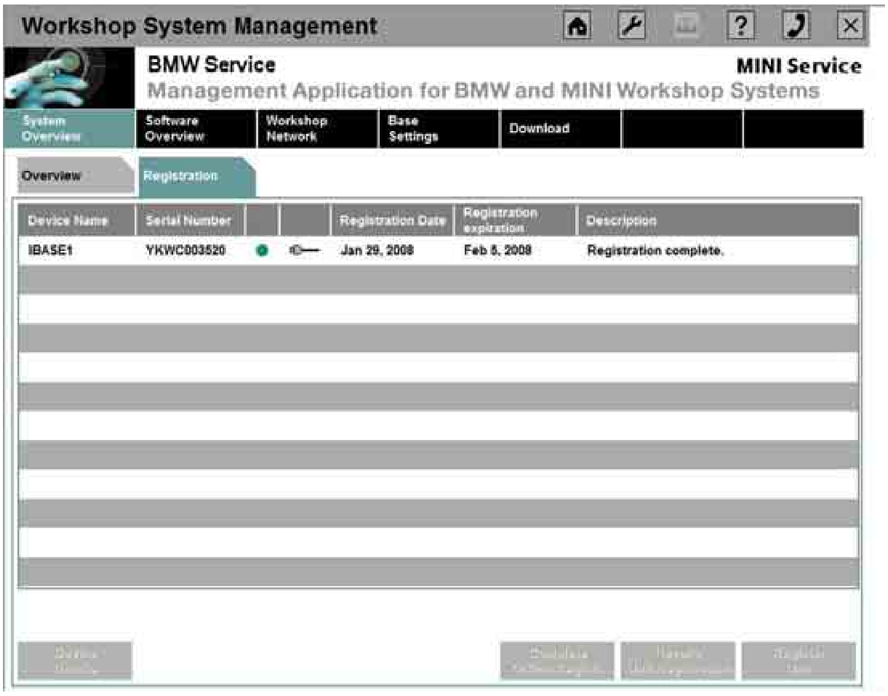
If you need to cancel the registration, select the "X" in the second line.

5.1.3.5 Carrying out the offline registration (part 1) – generating the registration fax

ℹ	**Information 1:** The procedure described below should also be followed if the registration was skipped in the configuration wizard on registration of the ISIS.

ℹ	**Information 2:** A registration fax must be created and sent to the BMW Group for each device that is to be registered.

⚠	**Note:** Please make sure that you have selected the corresponding BMW portal "None" (configuration, see chapter 5.1.13) and contact person (see chapter 5.1.8) to carry out an offline registration.

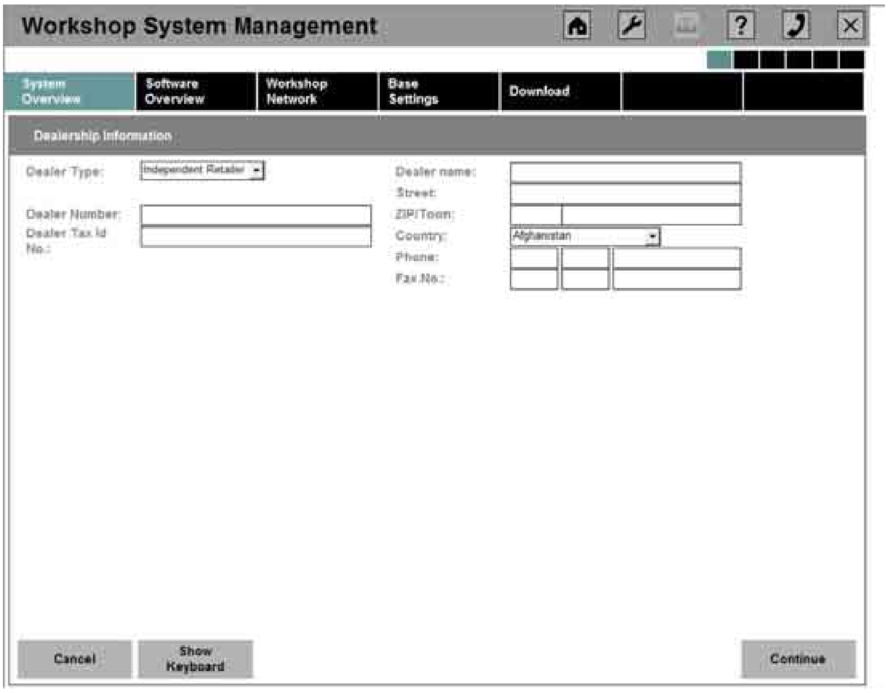


Device Name	Serial Number			Registration Date	Registration expiration	Description
IBASE1	YKWC003520	●		Jan 29, 2008	Feb 5, 2008	Registration complete.

Fig. 111: Registration overview

Selecting the "Registration" tab in the "System Overview" displays all the devices that can be registered or have already been registered (see Fig. 111).

To register a device, select it and then click the "Register device" button.



Dealer Type: Independent Retailer

Dealer Number:

Dealer Tax Id No.:

Dealer name:

Street:

ZIP/Town:

Country: Afghanistan

Phone:

Fax No.:

Fig. 112: Offline registration: Dealer information

Provide details on the dealership in the screen (see Fig. 112).

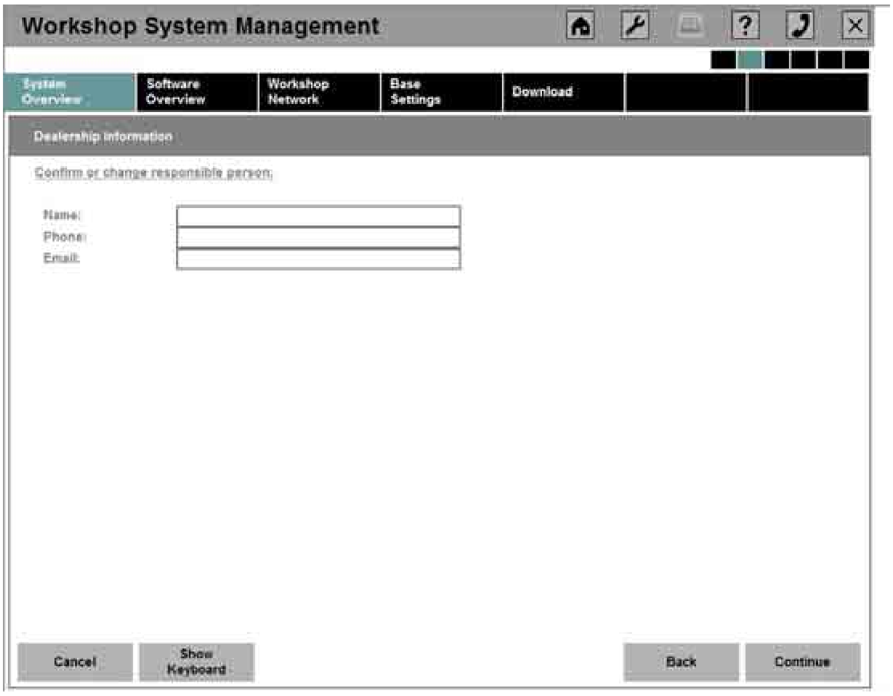
In a first step, the dealer type is designated. Here, it is possible to choose between "Independent dealer" and "Partner dealer" by clicking the small arrow to the right of the selection field.

The following input is required:

- Dealer number
- VAT ID no.
- Dealership branch
- Address of the dealer (full address and postal code)
- Country of the dealer headquarters (Here, too, select by clicking the small arrow to the right of the selection field)
- Telephone number and fax number; make sure to enter the country code in the first of the three input fields

Creation of the registration fax can be aborted by clicking the "Cancel" button.

Clicking the "Continue" button takes the user to the screen for inputting the contact person at the dealership (see Fig. 113). This is where to check or enter information on the name, telephone number and e-mail address of the contact person.



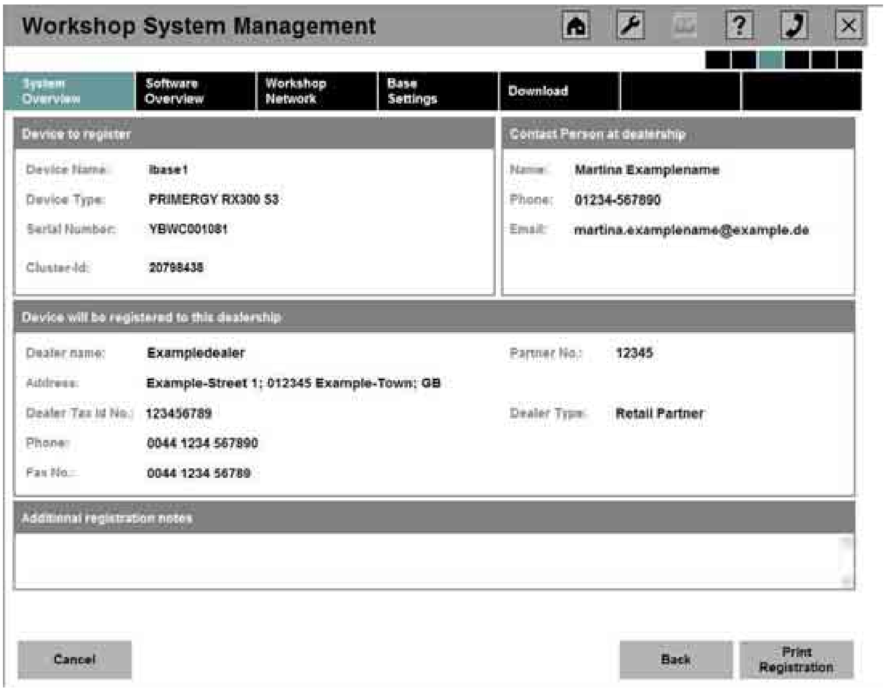
Confirm or change responsible person:

Name:
Phone:
Email:

Fig. 113: Offline registration: Dealer point of contact

Clicking the “Continue” button brings up a summary of the data entered for the registration fax (see Fig. 114).

Clicking the "Back" button takes the user to the previous screen; the "Cancel" button cancels the registration.



Device to register

Device Name:	ibase1
Device Type:	PRIMERGY RX300 S3
Serial Number:	YBWC001081
Cluster-Id:	20798438

Contact Person at dealership

Name:	Martina Examplename
Phone:	01234-567890
Email:	martina.examplename@example.de

Device will be registered to this dealership

Dealer name:	Exampledealer	Partner No.:	12345
Address:	Example-Street 1; 012345 Example-Town; GB		
Dealer Tax Id No.:	123456789	Dealer Type:	Retail Partner
Phone:	0044 1234 567890		
Fax No.:	0044 1234 56789		

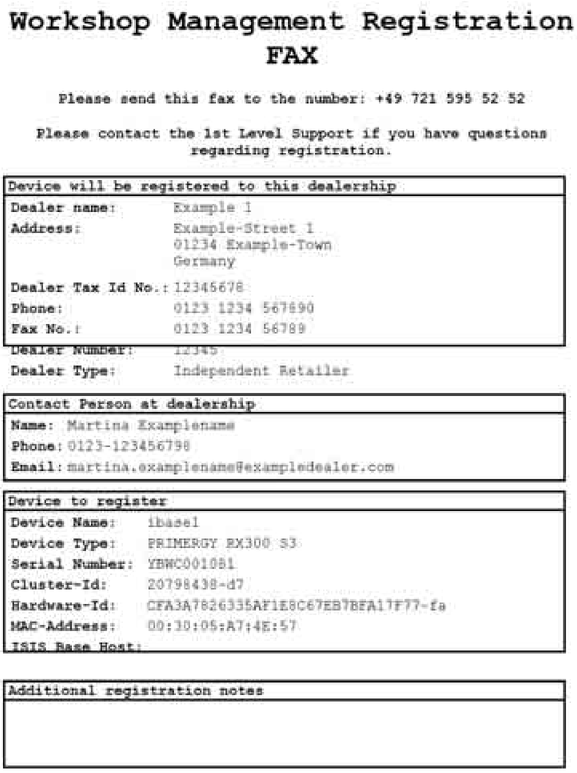
Additional registration notes

Fig. 114: Offline registration: Summary

In this dialog box (see Fig. 114), additional registration notes can be added in the lower area by clicking the field and entering the corresponding input directly.

Here, too, clicking the "Back" button takes the user to the previous screen and the registration procedure can be terminated by clicking "Cancel".

Clicking the "Print Registration" button sends the registration fax to the printer (see Fig. 115). The following prompt then appears (see Fig. 116) in the WSM.



Workshop Management Registration
FAX

Please send this fax to the number: +49 721 595 52 52

Please contact the 1st Level Support if you have questions regarding registration.

Device will be registered to this dealership

Dealer name: Example 1
Address: Example-Street 1
01234 Example-Town
Germany
Dealer Tax Id No.: 12345678
Phone: 0123 1234 567890
Fax No.: 0123 1234 56789
Dealer Number: 12345
Dealer Type: Independent Retailer

Contact Person at dealership

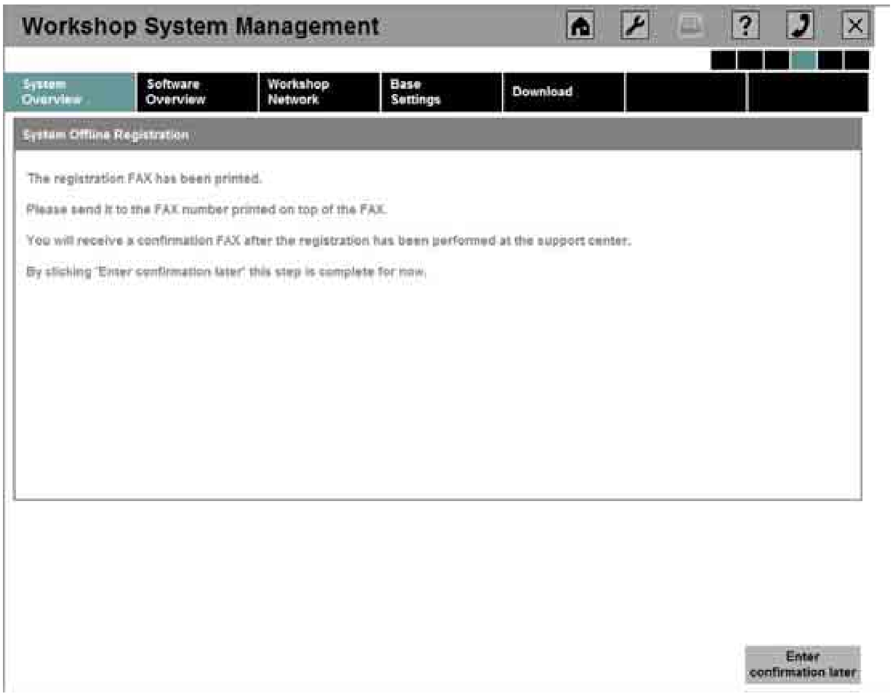
Name: Martina Examplename
Phone: 0123-123456798
Email: martina.examplename@exampledealer.com

Device to register

Device Name: ibasel
Device Type: PRIMERGY RX300 S3
Serial Number: YBWC001081
Cluster-Id: 20798438-d7
Hardware-Id: CFA3A7826335AF1E8C67EB7BFA17F77-fa
MAC-Address: 00:30:05:A7:4E:57
ISIS Base Host:

Additional registration notes

Fig. 115: Registration fax



The registration FAX has been printed.

Please send it to the FAX number printed on top of the FAX.

You will receive a confirmation FAX after the registration has been performed at the support center.

By clicking 'Enter confirmation later' this step is complete for now.

Fig. 116: Offline registration: Prompt for fax printing

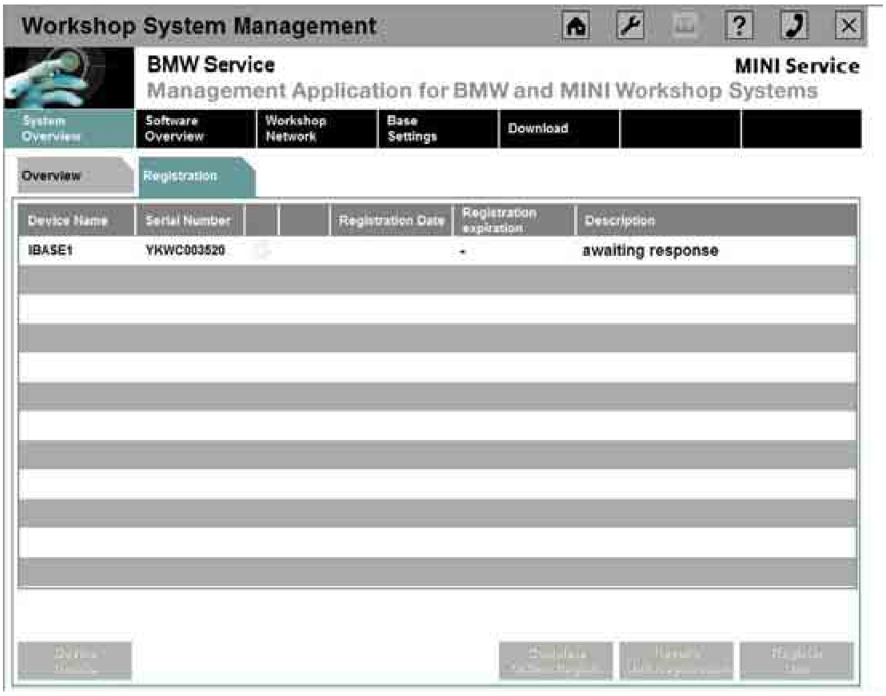
Note:

Within one working day of sending the fax of the registration printout, the user will receive a reply fax from the BMW Group.

The reply fax contains the data the user requires to complete the registration (according to the steps in the next chapter).

5.1.3.6 Carrying out an offline registration (part 2) – reply fax for the registration received

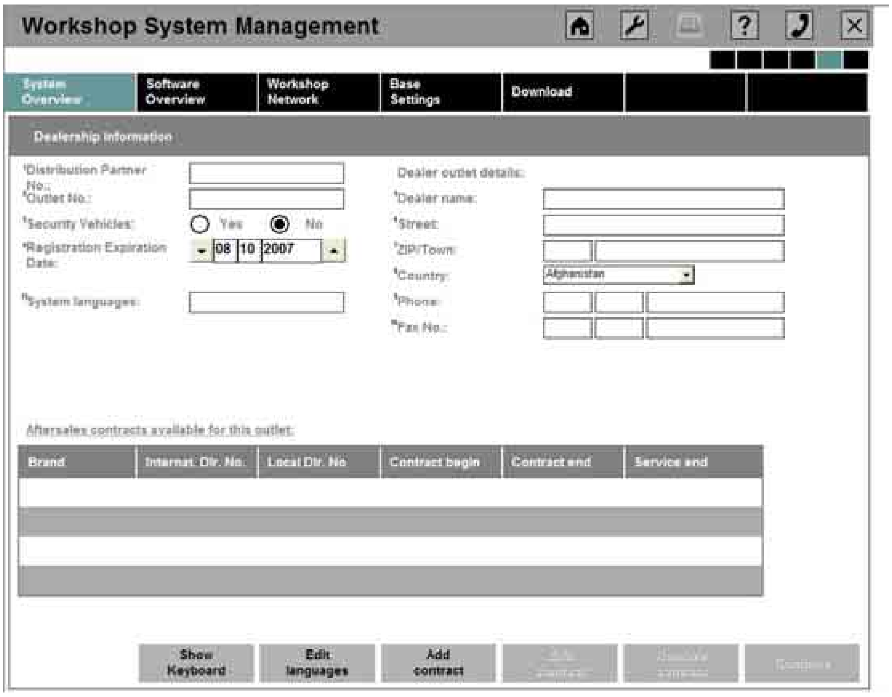
To be able to complete the offline registration, open the "System Overview" in the WSM, click on the "Registration" tab (see Fig. 117), and select the corresponding device.



Device Name	Serial Number			Registration Date	Registration expiration	Description
IBASE1	YKWC003520				-	awaiting response

Fig. 117: Starting the offline registration (part 2)

Clicking the "Complete offline registration" button takes the user to the following dialog box (see Fig. 118), where the corresponding data of the confirmation fax must be entered.



Dealership information

*Distribution Partner No.:
*Outlet No.:
*Security Vehicles: ○ Yes ● No
*Registration Expiration Date: 08 10 2007
**System languages:

Dealer outlet details:
*Dealer name:
*Street:
*ZIP/Town:
*Country: Afghanistan
*Phone:
**Fax No.:

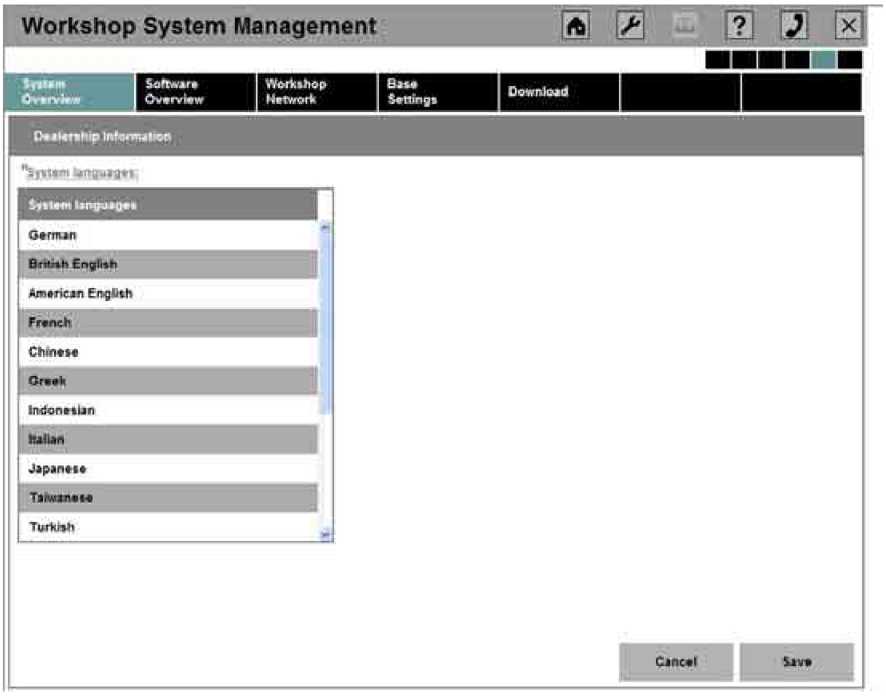
Aftersales contracts available for this outlet:

Brand	Internat. Dlr. No.	Local Dlr. No	Contract begin	Contract end	Service end

Fig. 118: Offline registration: Enter dealer information

Selection of the system language:

Select the system language by clicking the "Edit system languages " button (see Fig. 118), then selecting the corresponding language from the list (see Fig. 119), and adopting it by clicking "Save".



Dealership information

**System languages:

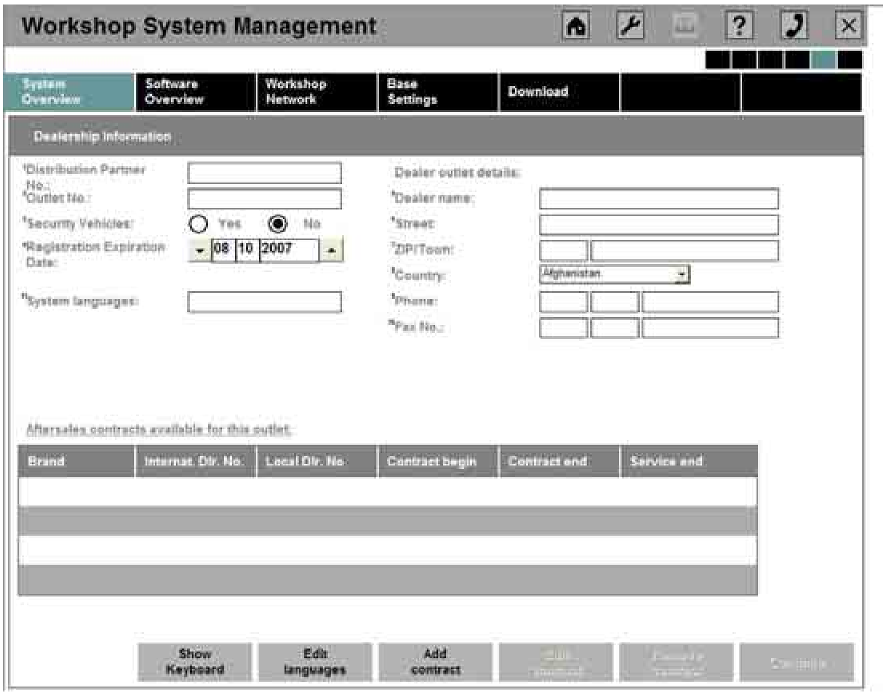
System languages
German
British English
American English
French
Chinese
Greek
Indonesian
Italian
Japanese
Taiwanese
Turkish

Fig. 119: Offline registration: System language

Entering the data from the confirmation fax:

Note:

The data must be entered correctly and completely; the registration cannot be carried out successfully without it.



Dealership information

*Distribution Partner No.:
*Outlet No.:
*Security Vehicles: ○ Yes ● No
*Registration Expiration Date: 08 10 2007
**System languages:

Dealer outlet details:
*Dealer name:
*Street:
*ZIP/Town:
*Country: Afghanistan
*Phone:
**Fax No.:

Aftersales contracts available for this outlet

Brand	Internat. Dlr. No.	Local Dlr. No	Contract begin	Contract end	Service end

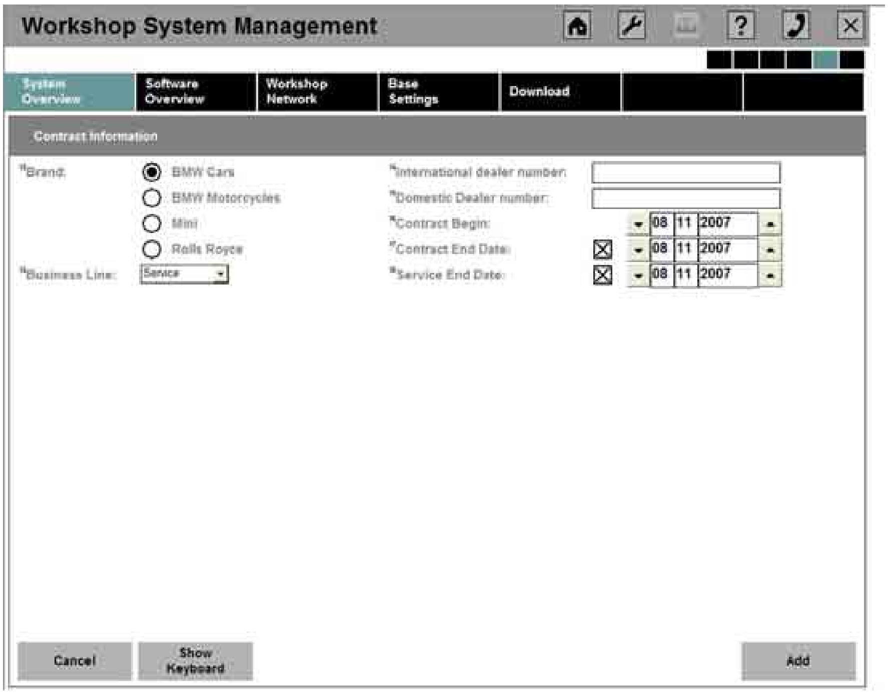
Fig. 120: Offline registration: Data input

The first part of the data of the reply fax must be entered into the above dialog box (see Fig. 120) as follows:

- BMW partner number of the dealer (distribution partner number)
- Outlet number
- Security vehicle selection
- Registration expiration date
- Location name (dealership branch)
- Street
- ZIP/Town
- Country selection
- Phone
- Fax number

Entering the contract data:

The corresponding contract data can be selected by clicking the "Add Contract" button (see Fig. 120) in the dialog box that appears (see Fig. 121).



Contract Information

*Brand: ● BMW Cars ○ BMW Motorcycles ○ Mini ○ Rolls Royce

*Business Line: Service

*International dealer number:

*Domestic Dealer number:

*Contract Begin: 08 11 2007

*Contract End Date: ☒ 08 11 2007

*Service End Date: ☒ 08 11 2007

Fig. 121: Entering the contract data

The second part of the data of the BMW reply fax must be entered in this dialog box (see Fig. 121).

The input fields are to be completed for those brands of cars for which the partner company has concluded service contracts. If the user company works with BMW, Mini, and Rolls-Royce, complete all three subsections of the dialog box by entering the contract data for each individual brand. If services are only offered for one (of three) or two (of three) brands of cars, only these sections are to be edited; the following details are of interest:

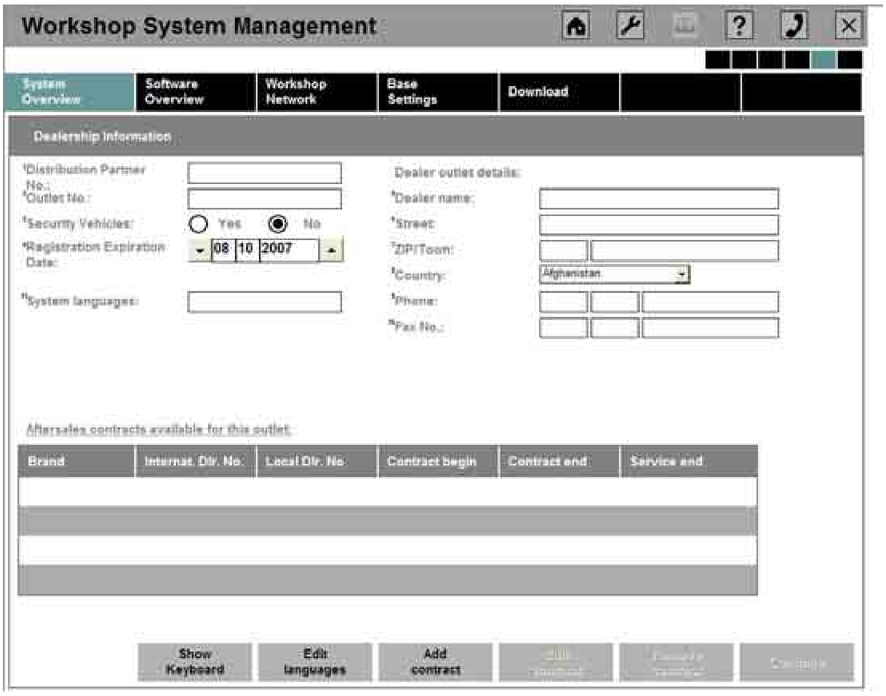
- International dealer number
- Domestic dealer number
- Start of the dealer contract
- Expiration of the dealer contract
- Expiration of the service agreements specified in the contract

If the no expiration date for dealer contracts or service agreements is specified in the confirmation fax, these entry fields can be hidden by clicking the checkboxes to the left of the contract end date and service end date in the dialog box (see Fig. 121).

The business line (Service or Vehicle Sales) is specified by clicking the arrow beside the selection field and selecting the corresponding line of business.

Click "Add" to confirm the input for the contracts.

The following dialog box (see Fig. 122) now contains the summarized details of the contract.



Dealership Information

*Distribution Partner No.:
*Outlet No.:
*Security Vehicles: ○ Yes ● No
*Registration Expiration Date: 08 10 2007
*System languages:

Dealer outlet details:
*Dealer name:
*Street:
*ZIP/Town:
*Country: Afghanistan
*Phone:
*Fax No.:

Aftersales contracts available for this outlet:

Brand	Internat. Dlr. No.	Local Dlr. No	Contract begin	Contract end	Service end

Fig. 122: Offline registration: Contract added

Note:

In the case of a contract for a number of brands, bear in mind that you have to perform the steps from this section "Entering the contract data" for all these brands.

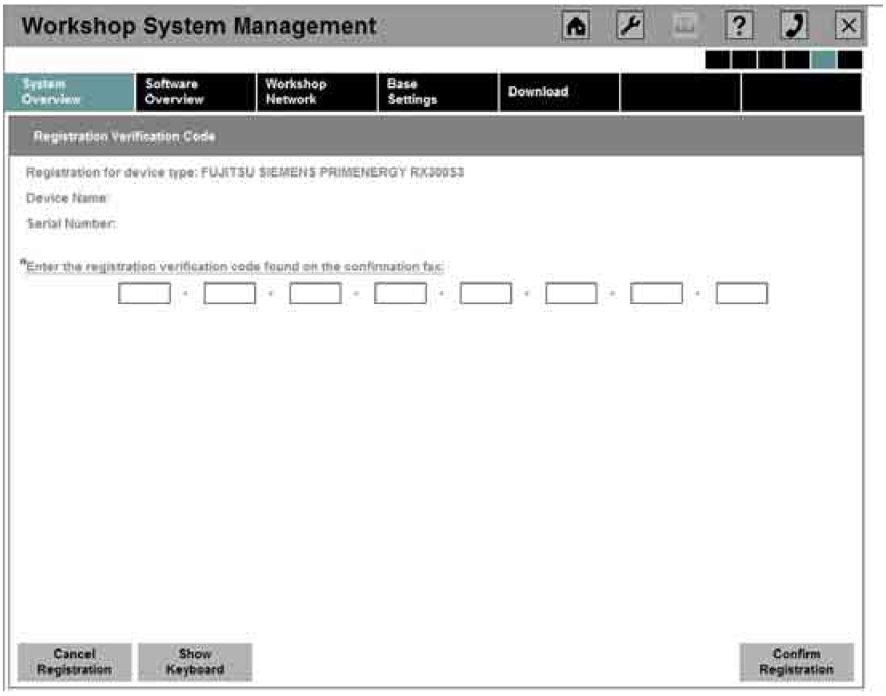
If other contracts are to be added, click "Add Contract" to do so.

If changes to existing contracts are required, select the corresponding contract and then click the "Edit Contract" button . The following screen corresponds to the one in Fig. 121.

A contract can be deleted by selecting it and then clicking "Remove Contract".

Clicking “Continue” confirms the data entered from the confirmation fax.

Confirmation of the registration data by entering the check code:



Registration Verification Code

Registration for device type: FUJITSU SIEMENS PRIMENERGY RX300S3

Device Name:

Serial Number:

*Enter the registration verification code found on the confirmation fax:

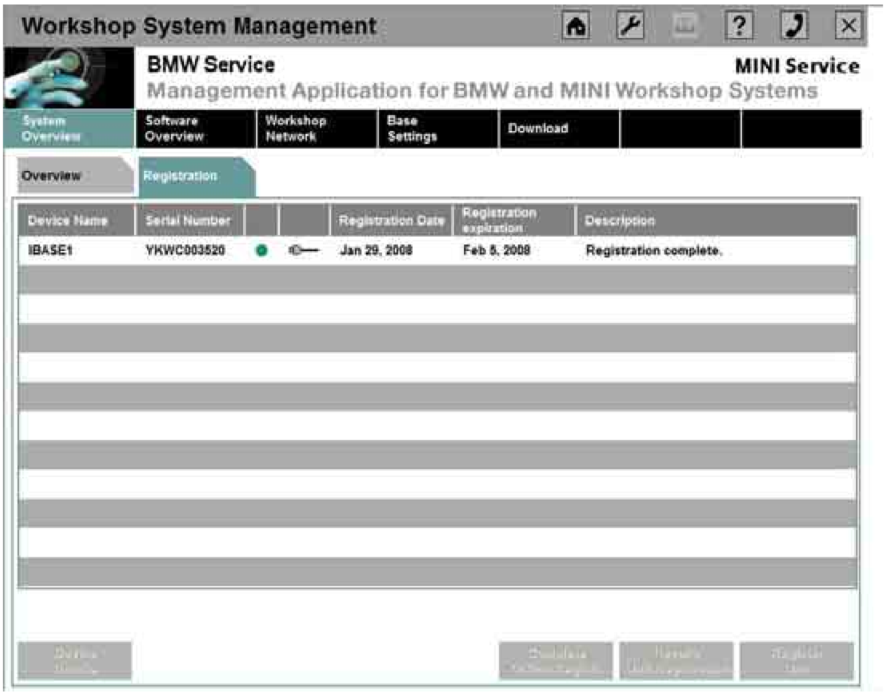
Fig. 123: Input of the check code

The check code assigned by the BMW Group, which is also included in the reply fax, must be entered in the provided field in order to complete the offline registration procedure (see Fig. 123). This check code ensures that the entries are correct. Click the "Confirm Registration" button to finish.

After successful registration, the start page of the WSM is displayed.

Completion of the offline registration:

Use the registration overview in the "System Overview" menu under the "Registration" tab to confirm that the registration was successful. A green dot (see Fig. 124) should now appear to the right of the ISIS that has just been registered.



Device Name	Serial Number			Registration Date	Registration expiration	Description
IBASE1	YKWC003520	●		Jan 29, 2008	Feb 5, 2008	Registration complete.

Fig. 124: Registration overview

After successful completion of the offline registration process, the corresponding device has been installed and registered and is now enabled for use.

5.1.3.7 Unregistration

Information 1:

A device can only be unregistered if a registration for this device has already been carried out successfully.

Information 2:

The unregistration of a device can only take place in the home network in which the registration of the device was carried out.

Need for unregistering the ISIS:

When an ISIS is replaced, it must be unregistered because one dealer can only register a certain number of servers. This is the only way to assure the registration of a new server.

An ISIS must also be unregistered if a new installation is carried out using the Wipe CD. This is important for enabling re-registration of the ISIS after the new installation.

Need for unregistering ICOM, ISID, and ISAP:

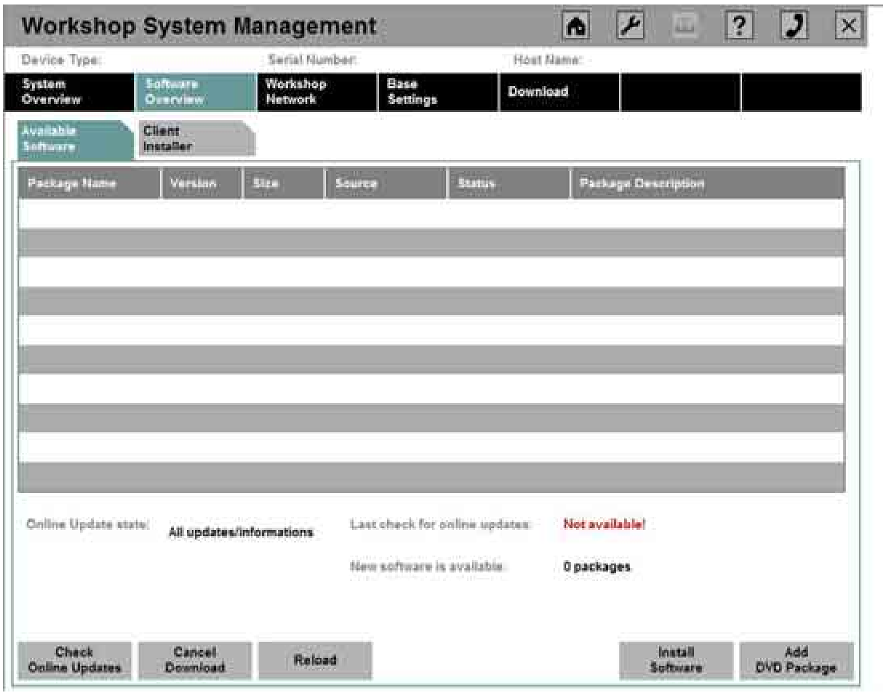
The primary purpose of unregistering ICOM, ISID, and ISAP is for data maintenance on the ISIS if this device is no longer used in the workshop (e.g.: defective device).

The online unregistration is carried out in the "System Overview" under the "Registration" tab by selecting the device to be unregistered and then clicking the "Undo Registration" button (see Fig. 124).

The offline unregistration takes place via First Level Support.

5.1.4 Software installation and update

For software installation or an update, open the "Software Overview" (see Fig. 125).



Device Type:
Serial Number:
Host Name:

Package Name	Version	Size	Source	Status	Package Description

Online Update state: All updates/informations

Last check for online updates: Not available!

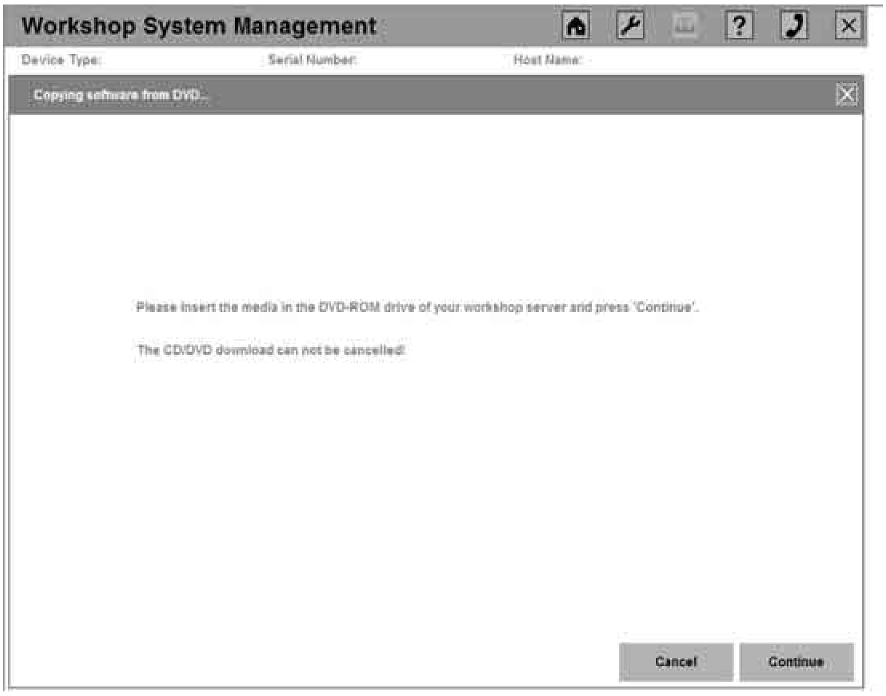
New software is available: 0 packages

Fig. 125: Software Overview

All software installations and update packages for the ISIS, ISID, ICOM and ISAP are loaded from this screen. There are two different possible procedures; these are explained in the following two chapters.

5.1.4.1 Loading the software onto the ISIS via DVD

Once the "Add DVD Package" button in the "Software Overview" (see Fig. 125) has been clicked, the corresponding DVD drawer opens on the ISIS and the system prompts you to insert the disc (see Fig. 126). The DVD must be inserted into the drive and the drive must be closed.



Please insert the media in the DVD-ROM drive of your workshop server and press 'Continue'.

The CD/DVD download can not be cancelled!

Fig. 126: Prompt to insert a CD / DVD

The process can be aborted by pressing "Cancel". Otherwise, the user clicks the "Continue" button.

A list of the software packages is displayed and clicking the "Download" button copies all of the listed packages onto the ISIS.

This starts the copying process and a corresponding message is displayed on the screen.

During the download, the process can be aborted by clicking "Cancel Download".

After successful completion, the system displays the packages available for installation in the "Software Overview".

5.1.4.2 Online download of the software onto the ISIS

ℹ	**Information 1:** Only online dealers can download software since it requires an online connection.

ℹ	**Information 2:** The download of packages is carried out automatically in the maintenance period (configuration according to chapter 5.1.9). This chapter describes the procedure for a manual download.

In the "Software Overview", clicking the "Find Online Updates" button initiates a search for online updates and the available packages are subsequently listed.

All the software packages available for download are displayed. Use the right-hand scrollbar to view the list of all packages.

The information area displays information about how many packages can be downloaded and the amount of data to be transferred.

The transfer operation can be terminated by clicking "Cancel" or initiated by clicking the "Download" button.

The next dialog box can be used to observe the download status.

Click "Cancel download" to interrupt the download operation. This can then be restarted at any time. Sections that have already be loaded are retained.

After successful termination of the download operation, the "Software Overview" dialog box appears; it now lists the packages to be installed.

The installation of the packages can then be continued as described in the next chapter.

5.1.4.3 Installing software packages on the ISIS

Information:

The installation of packages is usually carried out automatically in the maintenance period (configuration according to chapter 5.1.9).

Note:

Software packages can also be installed manually, as described in this chapter.

Please note:

During the entire installation operation, the ISIS is not available. This can lead to restrictions in the functionality of the applications and devices (ISID and ICOM).

The manual installation is started via the Software Overview by clicking the "Install Package" button.

After displaying a message that the installation has been started, the program switches to the "System Overview". The status is shown in yellow to the right of each server plug-in module and the installation indicator "Software Installed" appears in "Status Information". Here, the applications are in the offline mode (plug icon crossed out).

The software is installed on the ISIS in accordance with the installation process. If software has been loaded for the devices ISID, ICOM, and ISAP, then the corresponding steps from the next two subchapters (5.1.4.4 and 5.1.4.5) must be performed.

5.1.4.4 Software installation and update of the ISID

Note 1:

Before the software installation or update can be started, the packages must be loaded onto or downloaded onto the ISIS (see chapter 5.1.4.1 or 5.1.4.2) and then installed on the ISIS (see chapter 5.1.4.3).

Note 2:

To be able to run an installation or update on the ISID, make sure that the ISID is connected in the workshop network. The corresponding ISIS must also be available.

When updating the ISID, there is a difference between updating individual applications that are on the ISID and updating the base system (new image installation).

Update of individual applications on the ISID:

A check for available updates takes place:

- On switching on the ISID
- Every 4 hours if the ISID is switched on and in the infrastructure mode
- On switching off the ISID
- On switching from the temporary offline mode into the infrastructure mode
- During the initial installation if the configuration was carried out

In general, all the updates are required to continue use. The ISTA program is an exception to this because it takes a long time to update.

Note 1:

ELOS can only be installed if the "Mobile Service" profile is set on the ISID.

If an update is available, a corresponding message is issued and you are asked whether the update should be carried out now.

Note 2:

If you decline the update, the ISID switches into the temporary offline mode. This means the ISID is no longer connected to the ISIS.

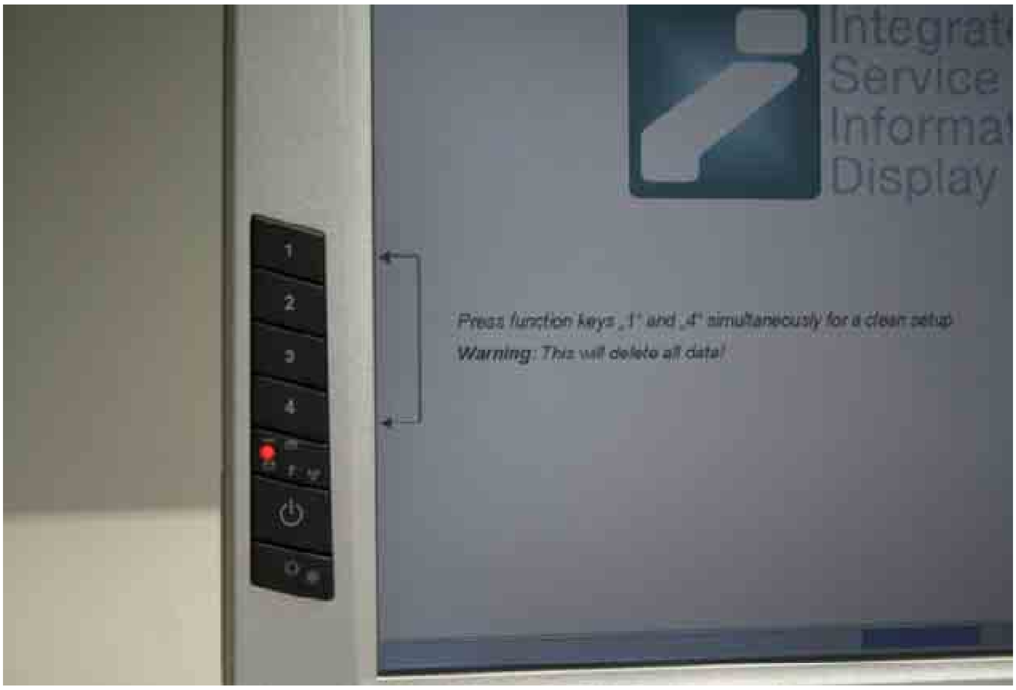
Only when you have agreed to the update is the ISID switched back into the infrastructure mode and the update carried out immediately.

Information:

While the ISID is being updated, a corresponding message appears in the WSM in the "System Overview".

Image new installation:

Here, when the ISID is switched on, the prompt (see Fig. 127) for a new image is displayed. You can then proceed in the same way as for a new installation of an ISID (see chapter 3.2.3 and later).



Press function keys „1" and „4" simultaneously for a clean setup
Warning: This will delete all data!

Fig. 127: ISID prompt to press the button combination

Information:

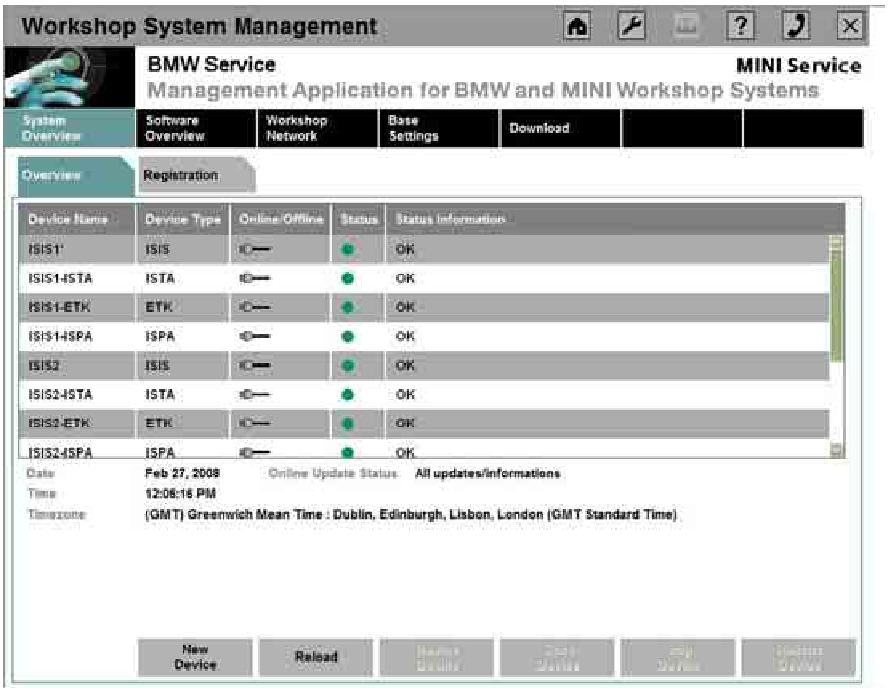
A renewed registration and configuration of the ISID is not required because the old settings have been stored on the ISIS and are adopted automatically after the new installation.

5.1.4.5 Update of the ICOM

Information:

If an update is available on the ISIS at the time that the ICOM is switched on, then it is automatically installed on the ICOM. The LEDs of the ICOM flash red in sequence.

5.1.5 Displaying and editing device configurations



Device Name	Device Type	Online/Offline	Status	Status Information
ISIS1'	ISIS	🔌	●	OK
ISIS1-ISTA	ISTA	🔌	●	OK
ISIS1-ETK	ETK	🔌	●	OK
ISIS1-ISPA	ISPA	🔌	●	OK
ISIS2	ISIS	🔌	●	OK
ISIS2-ISTA	ISTA	🔌	●	OK
ISIS2-ETK	ETK	🔌	●	OK
ISIS2-ISPA	ISPA	🔌	●	OK

Date Feb 27, 2008 Online Update Status All updates/informations
Time 12:08:16 PM
Timezone (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London (GMT Standard Time)

Fig. 128: System Overview

The main menu item "System Overview" (see Fig. 128) shows all enabled or disabled new generation workshop devices. Applications such as ISTA, EPC, or ISPA that are installed on the corresponding ISIS are also listed here.

In this overview, the applications are treated as separate physical devices.

The submenu item "Overview" provides a list of all devices in the workshop network and also describes the device name, the device type, whether the device is currently online or offline, as well as the device status.

The entries "Online" (plug icon, see Fig. 129) or "Offline" (crossed-out plug icon, see Fig. 130) indicate the current mode of the corresponding device.

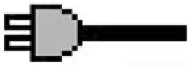


Fig. 129: Online mode

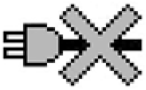


Fig. 130: Offline mode

The footer is located below the device list. It provides the following information:

- Date, time, time zone
- Online update status (to indicate the update method)

If a problem or error occurs, the status of each device is displayed in the "System Overview" after the relevant device name.

The following symbols are used for the corresponding status:

Symbol	Meaning
○	"no status present" Non-defined status or standard status with the device switched off.
🟢	"everything OK" There are no problems.
🟡	"uncritical problem" A problem has occurred, but the device is able to continue working.
🔴	"Critical system error" A problem that restricts the functionality of the device has occurred.

If a status has been set, e.g., to yellow, the "Device Details" provide more detailed information on what problem has occurred.

If the WLAN symbol (see Fig. 131) is shown directly beside the status message, WLAN is available for this device.

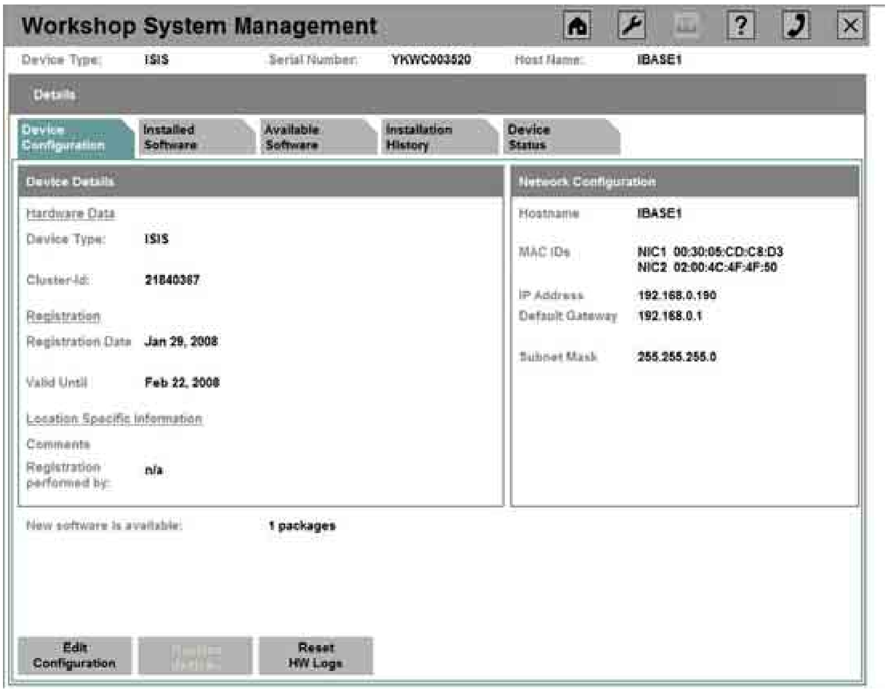
Fig. 131: WLAN symbol

Further information regarding the software version and configuration of each selected device is also displayed.

i	**Information:** The input fields and configurable values differ depending on the selected device. More information is provided in the following 5 chapters.

5.1.5.1 ISIS - Displaying and changing the device configuration

Selecting the ISIS in the "System Overview" and clicking the "Device Details″ button opens a dialog box for the device configuration (see Fig. 132).



Device Type: ISIS Serial Number: YKWC003520 Host Name: IBASE1

Hardware Data

Device Type: ISIS

Cluster-Id: 21840387

Registration

Registration Date Jan 29, 2008

Valid Until Feb 22, 2008

Location Specific Information

Comments

Registration performed by: n/a

Hostname IBASE1

MAC IDs NIC1 00:30:05:CD:C8:D3
NIC2 02:00:4C:4F:4F:50

IP Address 192.168.0.190

Default Gateway 192.168.0.1

Subnet Mask 255.255.255.0

New software is available: 1 packages

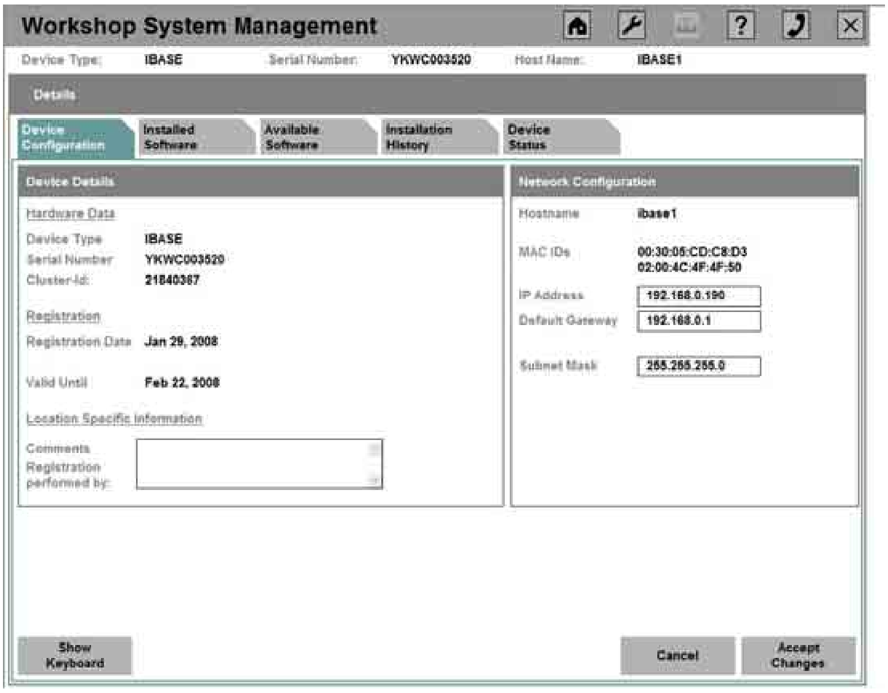
Fig. 132: Displaying the device configuration of the ISIS

The following details can be added or changed by clicking the "Edit configuration" button (see Fig. 133):

- A comment assigned by the dealer, e.g. with regard to the location in the workshop and the employee of the company who carried out the registration
- IP configuration of the device (IP address, default gateway, subnet mask)

i	**Note:** When changing the IP configuration, it is important to make sure that the IP of the ISIS is changed first and only after this, the IPs of the applications.

The purpose of the "Reset HW Logs" button is to delete existing log files. Log files contain automatically created logs of certain actions by processes on the ISIS. These files enable tracking of any errors. For this reason, this button should only be pressed if technical support instructs you to do so or if a technician does so when performing work on the system.



Device Type: IBASE
Serial Number: YKWC003520
Host Name: IBASE1

Device Details

Hardware Data

Device Type IBASE
Serial Number YKWC003520
Cluster-Id: 21840367

Registration

Registration Date Jan 29, 2008

Valid Until Feb 22, 2008

Location Specific Information

Comments
Registration performed by:

Network Configuration

Hostname ibase1

MAC IDs 00:30:05:CD:C8:D3
02:00:4C:4F:4F:50

IP Address 192.168.0.190
Default Gateway 192.168.0.1

Subnet Mask 255.255.255.0

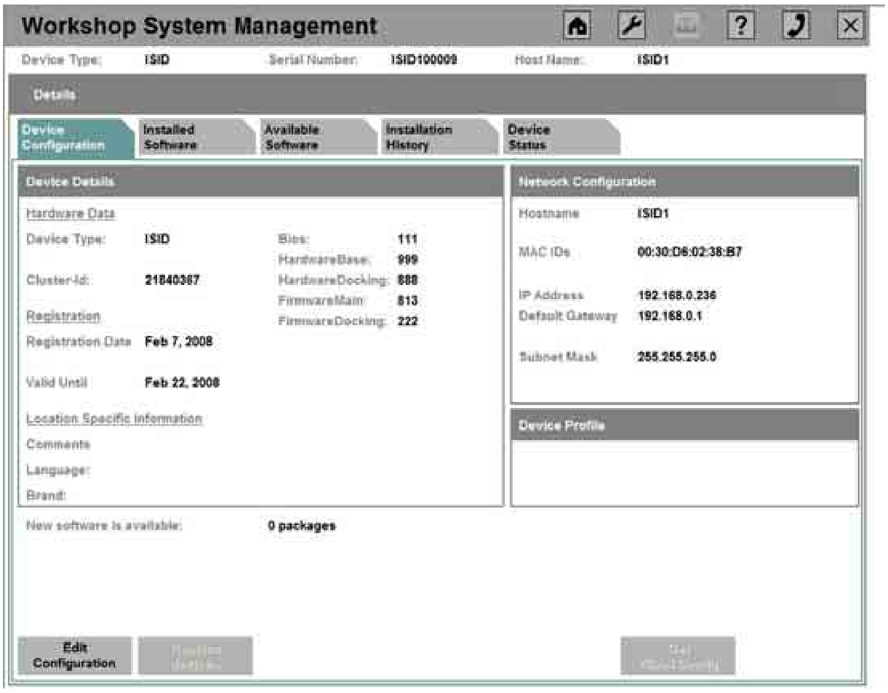
Fig. 133: Editing the device configuration of the ISIS

The inputs are saved by clicking "Apply" and rejected by clicking "Cancel".

The "Device Details" menu can be closed by clicking the "X" icon in the third line.

5.1.5.2 ISID - Displaying and changing the device configuration

Selecting the ISID in the "System Overview" and clicking the "Device Details″ button opens a dialog box for the device configuration (see Fig. 134).



Device Type: ISID Serial Number: ISID100009 Host Name: ISID1

Device Details

Hardware Data

Device Type: ISID

Cluster-Id: 21840367

Bios: 111
HardwareBase: 999
HardwareDocking: 888
FirmwareMain: 813
FirmwareDocking: 222

Registration

Registration Date Feb 7, 2008

Valid Until Feb 22, 2008

Location Specific Information

Comments

Language:

Brand:

Network Configuration

Hostname ISID1

MAC IDs 00:30:D6:02:38:B7

IP Address 192.168.0.236
Default Gateway 192.168.0.1

Subnet Mask 255.255.255.0

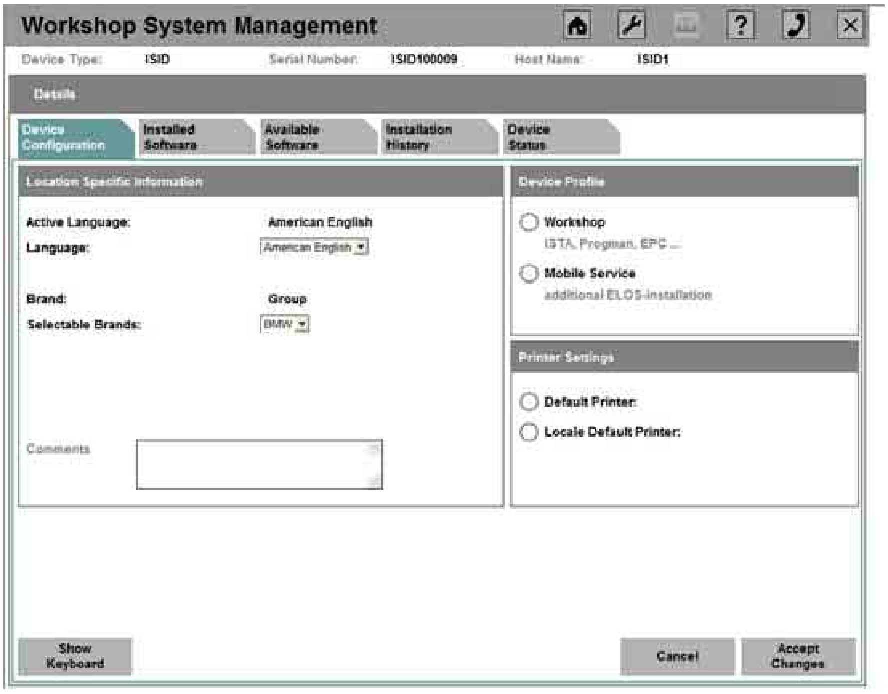
Device Profile

New software is available: 0 packages

Fig. 134: Displaying the device configuration of the ISID

The following details can be added or changed by clicking the "Edit configuration" button (see Fig. 135):

- The active language of the ISID
- A certain brand for which the ISID was configured
- A comment assigned by the dealer, e.g. with regard to the location in the workshop



Device Type: ISID Serial Number: ISID100009 Host Name: ISID1

Location Specific Information

Active Language: American English
Language: American English

Brand: Group
Selectable Brands: BMW

Comments

Device Profile

○ Workshop
ISTA, Progman, EPC ...

○ Mobile Service
additional ELOS-installation

Printer Settings

○ Default Printer:

○ Locale Default Printer:

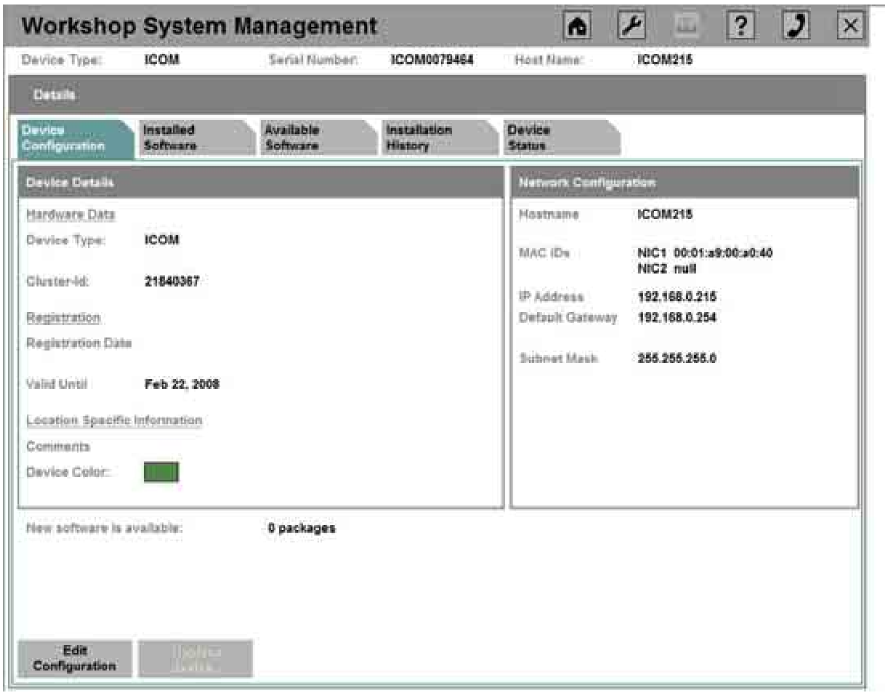
Fig. 135: Editing the device configuration of the ISID

The inputs are saved by clicking "Apply" and rejected by clicking "Cancel".

The "Device Details" menu can be closed by clicking the "X" icon in the third line.

5.1.5.3 ICOM - Displaying and changing the device configuration

Selecting the ICOM in the "System Overview" and clicking the "Device Details" button opens a dialog box for the device configuration (see Fig. 136).



Device Type: ICOM
Serial Number: ICOM0079464
Host Name: ICOM215

Device Type: ICOM
Cluster-Id: 21840367
Registration Date
Valid Until Feb 22, 2008
Comments
Device Color: 🟩

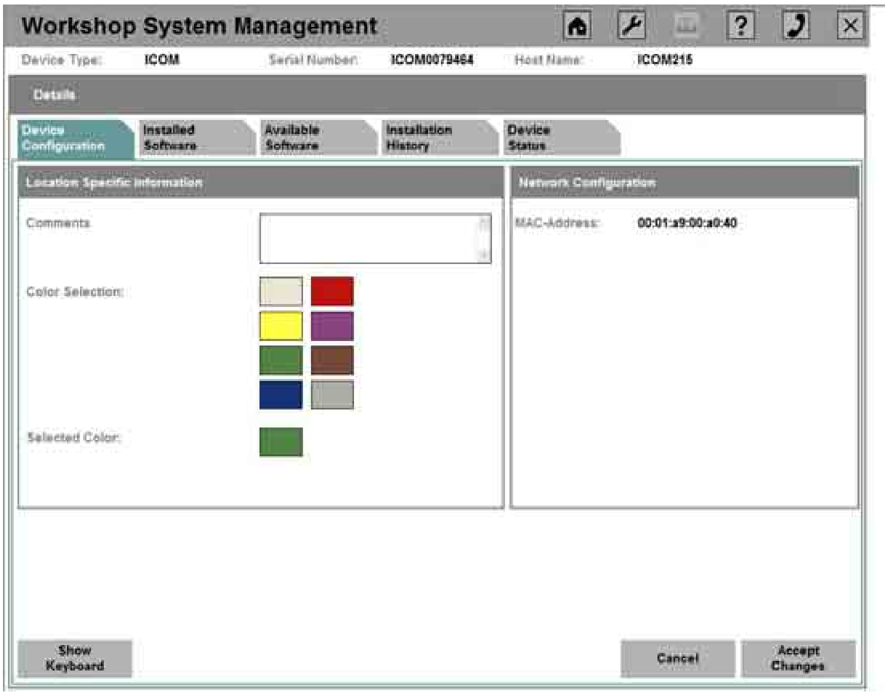
Hostname ICOM215
MAC IDs NIC1 00:01:a9:00:a0:40
NIC2 null
IP Address 192.168.0.215
Default Gateway 192.168.0.254
Subnet Mask 255.255.255.0

New software is available: 0 packages

Fig. 136: Displaying the device configuration of the ICOM

The following details can be added or changed by clicking the "Edit configuration" button (see Fig. 137):

- A comment assigned by the dealer, e.g. with regard to the location in the workshop
- Change in color to facilitate assignment of the color-coded devices



Device Type: ICOM
Serial Number: ICOM0079464
Host Name: ICOM215

Comments:

Color Selection:

Selected Color:

MAC-Address: 00:01:a9:00:a0:40

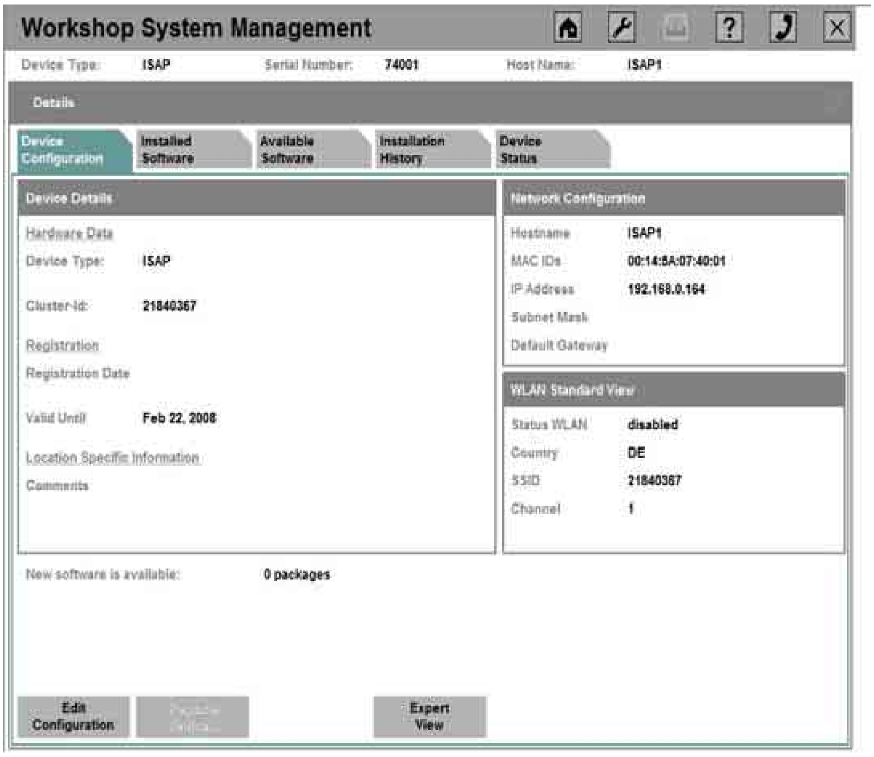
Fig. 137: Editing the device configuration of the ICOM

The inputs are saved by clicking "Apply" and rejected by clicking "Cancel".

The "Device Details" menu can be closed by clicking the "X" icon in the third line.

5.1.5.4 ISAP - Displaying and changing the device configuration

Selecting the ISAP in the "System Overview" and clicking the "Device Details″ button opens a dialog box for the device configuration (see Fig. 138).



Device Type: ISAP
Serial Number: 74001
Host Name: ISAP1

Device Details

Hardware Data
Device Type: ISAP
Cluster-Id: 21840367
Registration
Registration Date
Valid Until Feb 22, 2008
Location Specific Information
Comments

Network Configuration

Hostname ISAP1
MAC IDs 00:14:5A:07:40:01
IP Address 192.168.0.164
Subnet Mask
Default Gateway

WLAN Standard View

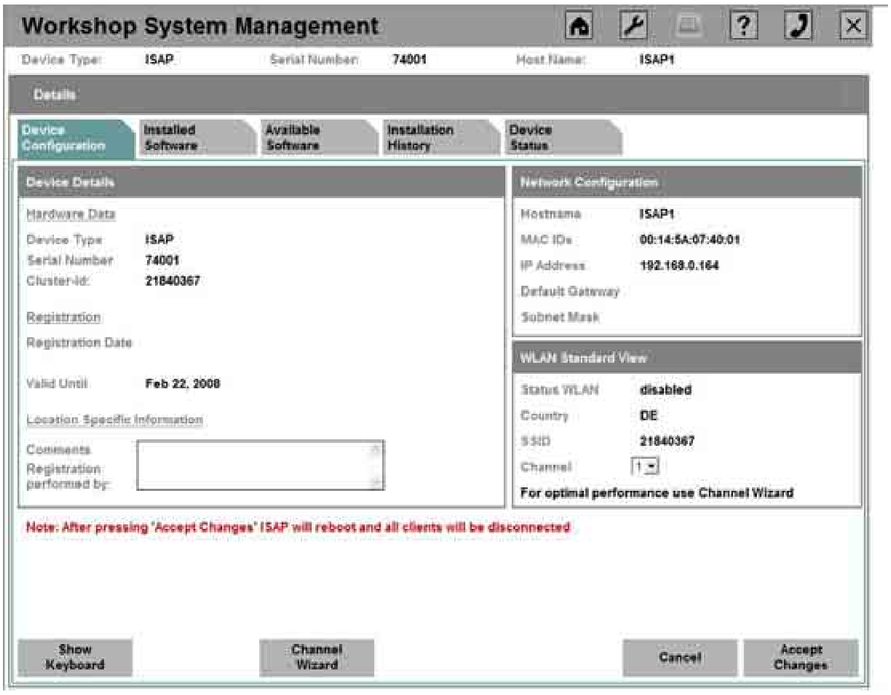
Status WLAN disabled
Country DE
SSID 21840367
Channel 1

New software is available: 0 packages

Fig. 138: Displaying the device configuration of the ISAP

The following details can be added or changed by clicking the "Edit configuration" button (see Fig. 139):

- A comment assigned by the dealer, e.g. with regard to the location in the workshop and the employee of the company who carried out the registration
- Channel over which the ISAP is to transmit and receive (see chapter 3.5.5)



Device Type: ISAP
Serial Number: 74001
Host Name: ISAP1

Device Details

Hardware Data
Device Type ISAP
Serial Number 74001
Cluster-Id: 21840367
Registration
Registration Date
Valid Until Feb 22, 2008
Location Specific Information
Comments
Registration performed by:

Network Configuration

Hostname ISAP1
MAC IDs 00:14:5A:07:40:01
IP Address 192.168.0.164
Default Gateway
Subnet Mask

WLAN Standard View

Status WLAN disabled
Country DE
SSID 21840367
Channel 1
For optimal performance use Channel Wizard

Note: After pressing 'Accept Changes' ISAP will reboot and all clients will be disconnected

Fig. 139: Editing the device configuration of the ISAP

The inputs are saved by clicking "Apply" and rejected by clicking "Cancel".

The "Device Details" menu can be closed by clicking the "X" icon in the third line.

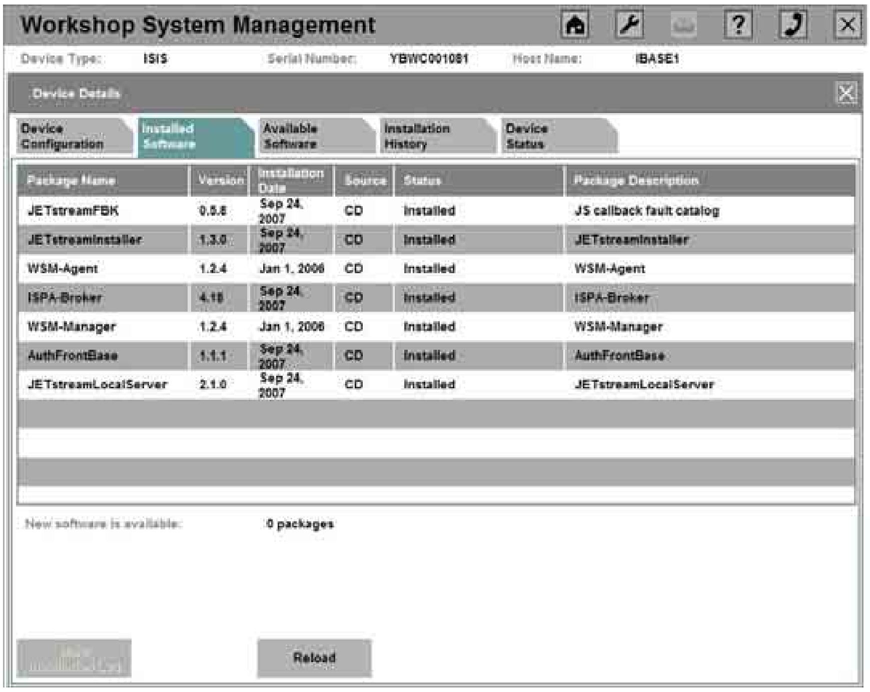
Expert configuration in the WSM:

If a WLAN radio network already exists or a number of ISAPs are to be deployed, it may be necessary to operate the ISAP in another band. This change can be made in the "Expert View".

By default, the 2.4 GHz band is set for the ISAP. This view can be used to switch to the 5 GHz band and to select a corresponding WLAN radio channel from this band.

To support optimized selection of a WLAN radio channel, it is advisable to use the "Channel Wizard" in the "Expert View" to measure the present use of the 5 GHz band and to obtain a recommendation for a radio channel from the ISAP. Using it takes the user through a procedure analogous to the one described in section 3.4.6.

5.1.5.5 Overview of the currently installed software of a device



Device Type: ISIS
Serial Number: YBWC001081
Host Name: IBASE1

Package Name	Version	Installation Date	Source	Status	Package Description
JETstreamFBK	0.5.8	Sep 24, 2007	CD	Installed	JS callback fault catalog
JETstreamInstaller	1.3.0	Sep 24, 2007	CD	Installed	JETstreamInstaller
WSM-Agent	1.2.4	Jan 1, 2006	CD	Installed	WSM-Agent
ISPA-Broker	4.18	Sep 24, 2007	CD	Installed	ISPA-Broker
WSM-Manager	1.2.4	Jan 1, 2006	CD	Installed	WSM-Manager
AuthFrontBase	1.1.1	Sep 24, 2007	CD	Installed	AuthFrontBase
JETstreamLocalServer	2.1.0	Sep 24, 2007	CD	Installed	JETstreamLocalServer

New software is available: 0 packages

Fig. 140: Overview of the currently installed software of a device

Highlighting a device in the "System Overview", then clicking "Device Details" and selecting the "Installed Software" tab opens the above dialog box (see Fig. 140), containing the following information in the overview:

- Package name of the currently installed software package
- Version information of the current software

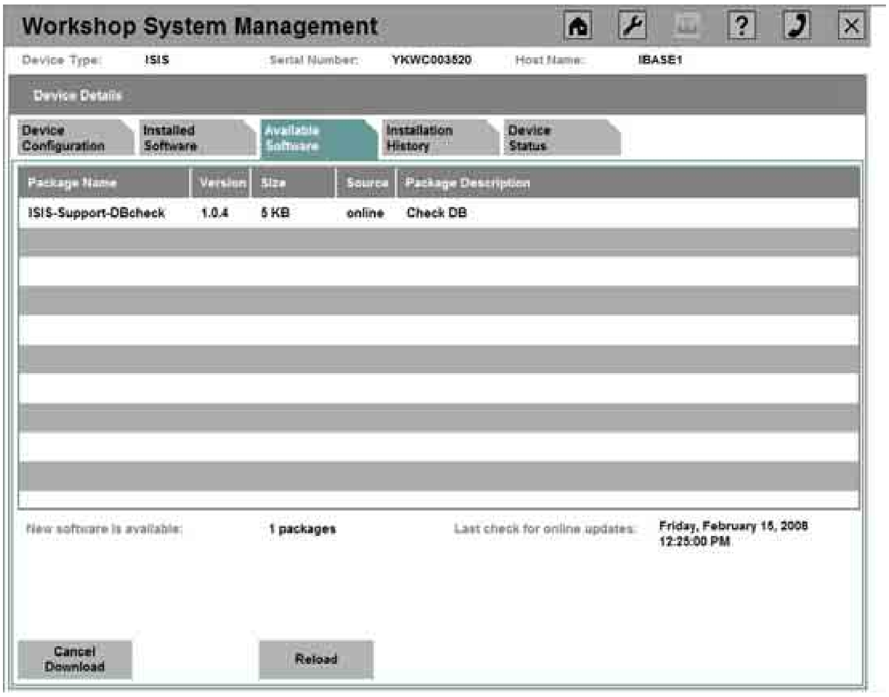
- Date and time of installation
- Source of the package (online or from DVD)
- Package description; what this package involves

If the software package is selected and then the "Show Installation Log" button is clicked, a detailed list with recorded information for the log file of the installation appears.

Other details are provided in the information area:

- Information regarding whether new software packages are available for the currently selected device

5.1.5.6 Overview of available software for a device



Workshop System Management

Device Type: ISIS   Serial Number: YKWC003520   Host Name: IBASE1

Device Details

Package Name	Version	Size	Source	Package Description
ISIS-Support-DBcheck	1.0.4	5 KB	online	Check DB

New software is available: 1 packages

Last check for online updates: Friday, February 15, 2008 12:25:00 PM

Fig. 141: Overview of available software for a device

Selecting a device in the "System Overview", then clicking "Device Details" and selecting the "Available Software" tab opens the above dialog box (see Fig. 141).

The list contains all the available packages with:

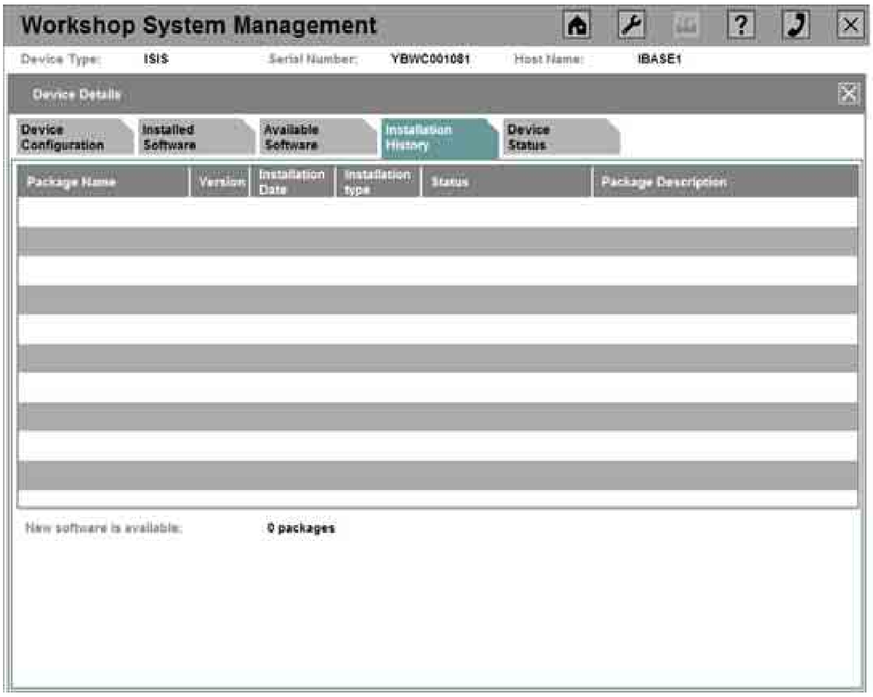
- The corresponding name
- Version information
- Size of the package
- The source of supply

- Package description; precisely which software is involved

Other details are provided in the information area:

- Information regarding how many more-recent versions are available
- Time when the last update query was carried out

5.1.5.7 Installation history of a device



Device Type: ISIS Serial Number: YBWC001081 Host Name: IBASE1

Package Name	Version	Installation Date	Installation type	Status	Package Description

New software is available: 0 packages

Fig. 142: Installation history of a device

Selecting a device in the "System Overview", then clicking "Device Details" and selecting the "Installation History" tab opens the above dialog box (see Fig. 142), containing the following information on all packages installed to date:

- Names of all the software packages ever installed on this device
- Version information
- Date of the installation
- Source of the package (online or from DVD)
- Package description; what this package involves

Other details are provided in the information area:

- Information regarding whether more-recent versions are available

5.1.6 Switching off and restarting the devices (including applications)

Note:

It is important to make sure that the ISIS is not switched off using the on / off button on the front of the ISIS; instead, the steps from this chapter are carried out. Otherwise, an uncontrolled shutdown can damage the system (e.g. the database). In the worst-case scenario, this may require reinstallation of the ISIS.

To either switch a device off or restart it, select the corresponding device in the "System Overview" under the "Overview" tab. Click the "Stop Device" or "Restart Device" button to trigger the desired action.

It must be noted here that a device can only be switched off or restarted if the device is already switched on and connected to the workshop network, i.e. a plug icon (see Fig. 143) appears after the device.

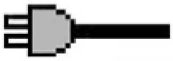


Fig. 143: Plug icon in the System Overview

5.1.7 Displaying dealer data

The overview of the dealer data is displayed automatically when you select the main menu "Base Settings".

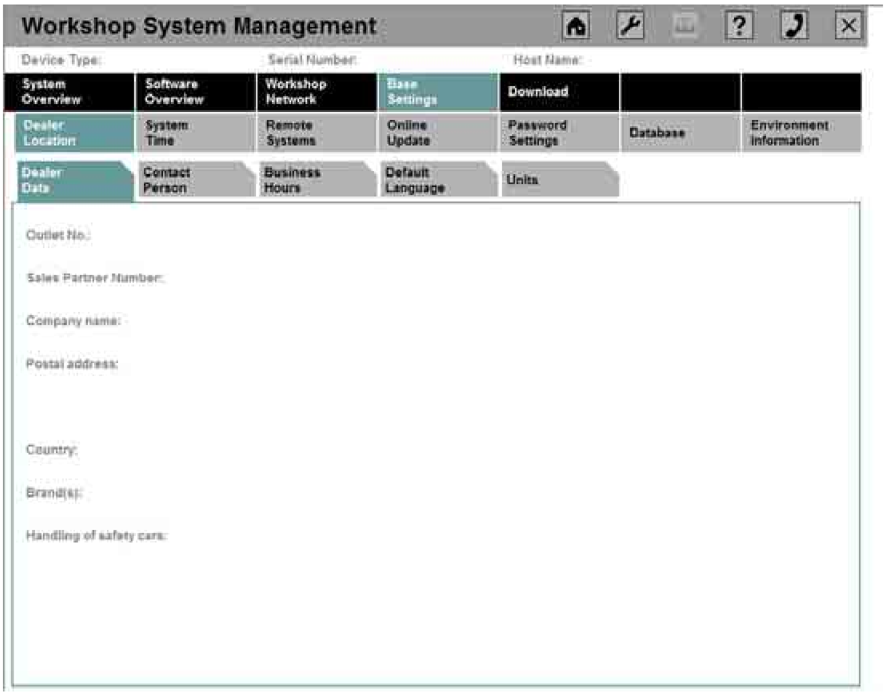


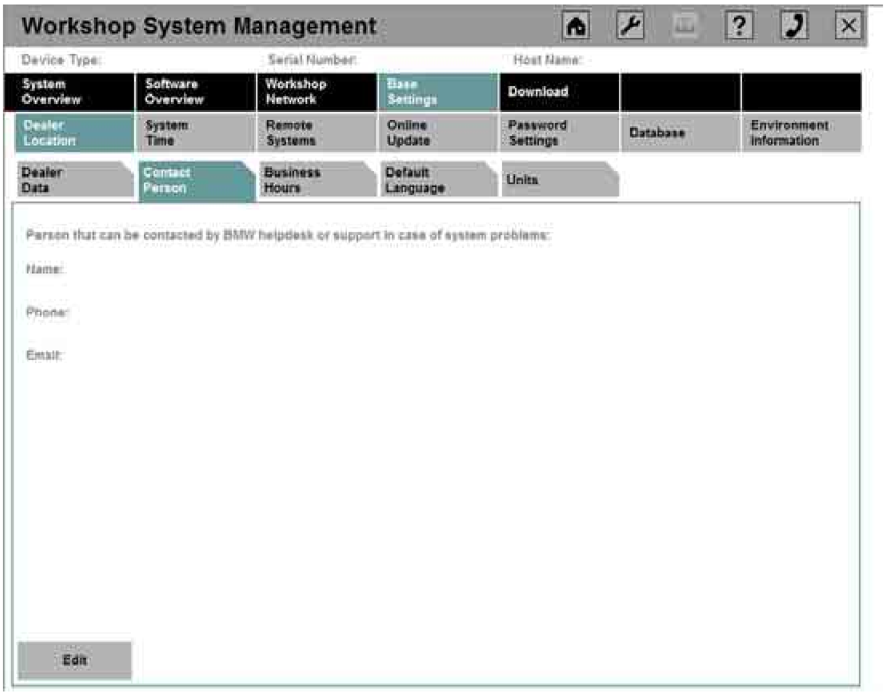
Fig. 144: Display of the dealer data

If the device has been successfully registered, the dealer data that were used to register the ISIS can be viewed here (see Fig. 144):

- Outlet number
- Sales partner number (VPN)
- Company name and the postal address of the dealer location as well as the corresponding country
- Brand(s) for which the dealer has concluded sales agreements.
- Permission for security vehicles

5.1.8 Specifying / changing the contact person

Open the "Base Settings" menu, then the "Dealer Settings" submenu, and then the "Contact Person" tab to view the settings for the contact person.



Person that can be contacted by BMW helpdesk or support in case of system problems:

Name:

Phone:

Email:

Fig. 145: Data of the contact person

The present dialog box (see Fig. 145) shows the data with regard to the contact person of the dealership. This contact person is also the contact person responsible for the workshop devices.

If the user clicks "Edit", a dialog box appears in which the data for the contact person responsible can be changed.

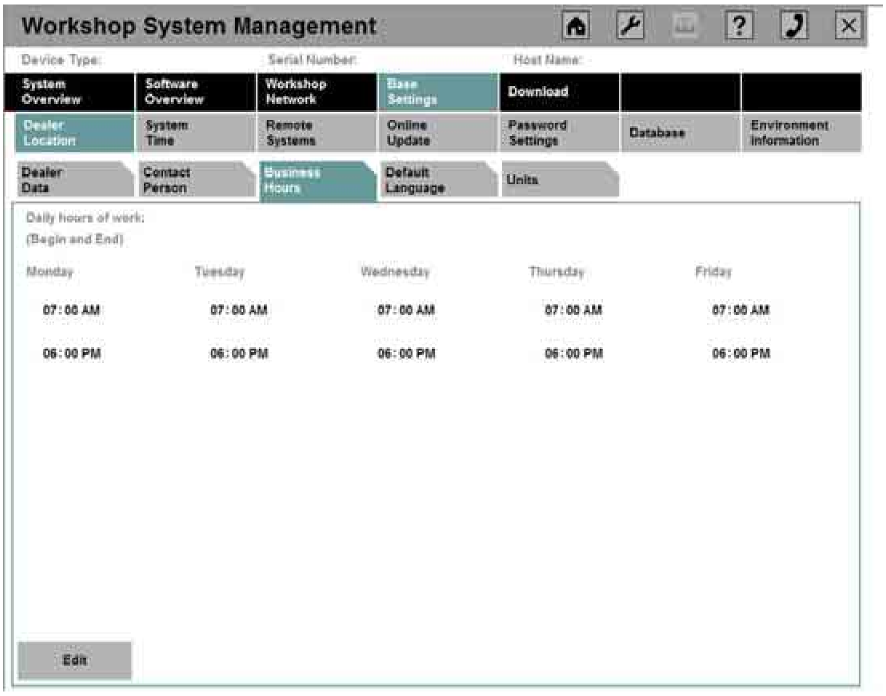
The name, telephone number, and e-mail address must be specified for the contact person.

Clicking the "Save" button saves the entered information.

Clicking "Cancel" takes the user back to the previous dialog box.

5.1.9 Specifying and changing the business hours / maintenance period of the dealer

The settings for the business hours are shown in the "Base Settings" menu, in the "Dealer Settings" submenu, under the "Business Hours" tab.



Daily hours of work:
(Begin and End)

Monday	Tuesday	Wednesday	Thursday	Friday
07 : 00 AM	07 : 00 AM	07 : 00 AM	07 : 00 AM	07 : 00 AM
06 : 00 PM	06 : 00 PM	06 : 00 PM	06 : 00 PM	06 : 00 PM

Fig. 146: Business hours of the dealer

This dialog box is for entering the business hours of the dealer (see Fig. 146).

Note:

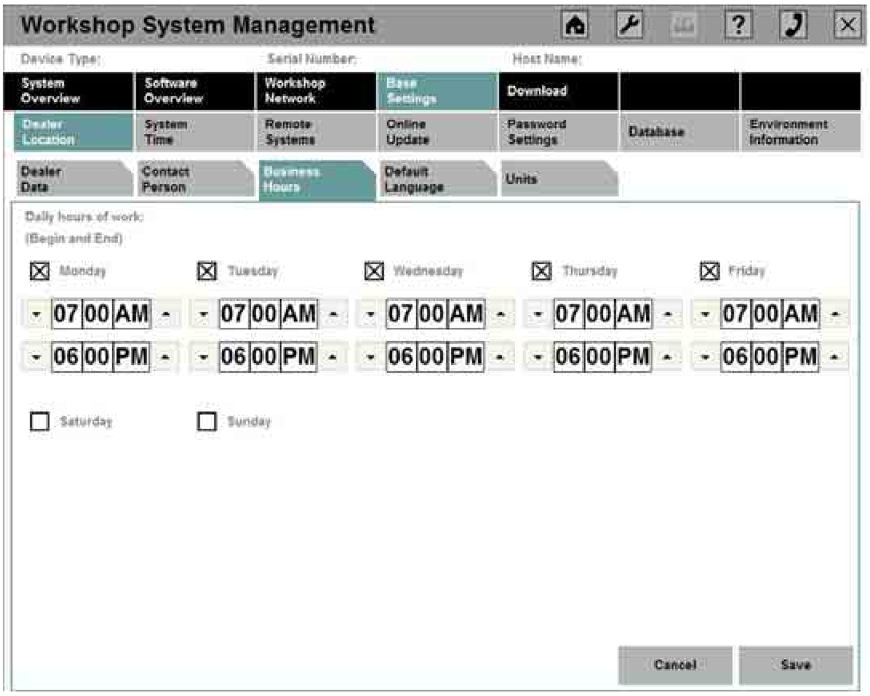
The working time should not exceed 20 hours per day, leaving a time window of at least 4 hours for online updates as well as certain maintenance processes. During these inactive periods, the ISIS cannot be used or only to a limited extent.

If you wish to make changes, go to "Edit", select the corresponding field to edit in the next dialog box (see Fig. 147) and click the adjacent arrow buttons to raise or lower the number.

In addition, days can be configured in such a way that the maintenance period can be extended to the entire day. The other settings for such non-working days are hidden by clicking the X next to the day.

To make hidden days accessible again for setting business hours, click in the box next to the day to insert an X.

All of the entries are adopted and activated by clicking "Save".



Daily hours of work:
(Begin and End)

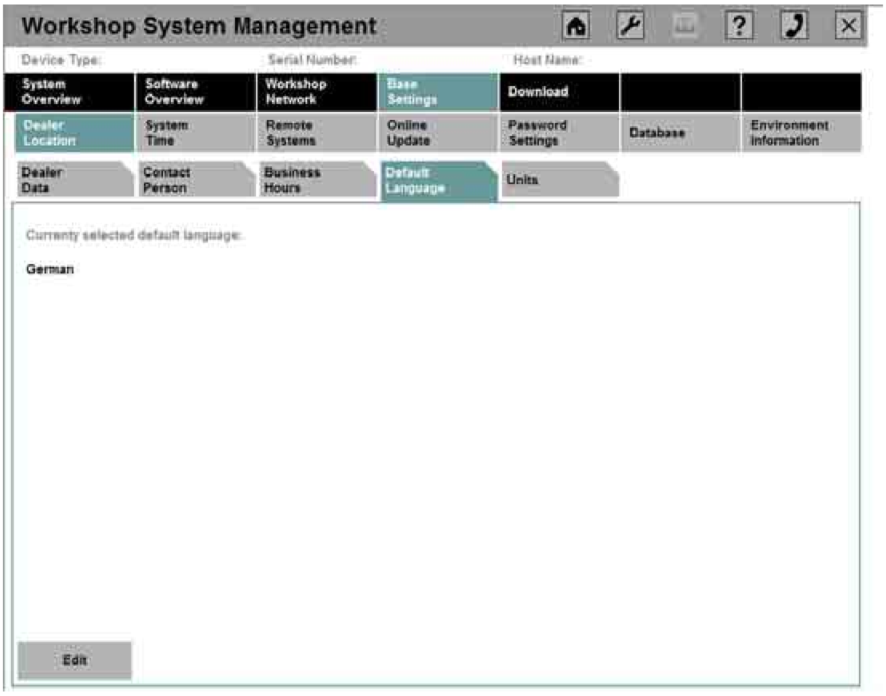
☒ Monday	☒ Tuesday	☒ Wednesday	☒ Thursday	☒ Friday
07 00 AM	07 00 AM	07 00 AM	07 00 AM	07 00 AM
06 00 PM	06 00 PM	06 00 PM	06 00 PM	06 00 PM

□ Saturday □ Sunday

Fig. 147: Editing the dealer business hours

5.1.10 Changing the default language of the dealer

The settings for the default language can be viewed and edited by opening the "Base Settings" menu, then the "Dealer Settings" submenu, and then clicking the "Default Language" tab (see Fig. 148).



Currenty selected default language:
German

Fig. 148: Default language

The languages available for selection are based on the circumstances of the market.

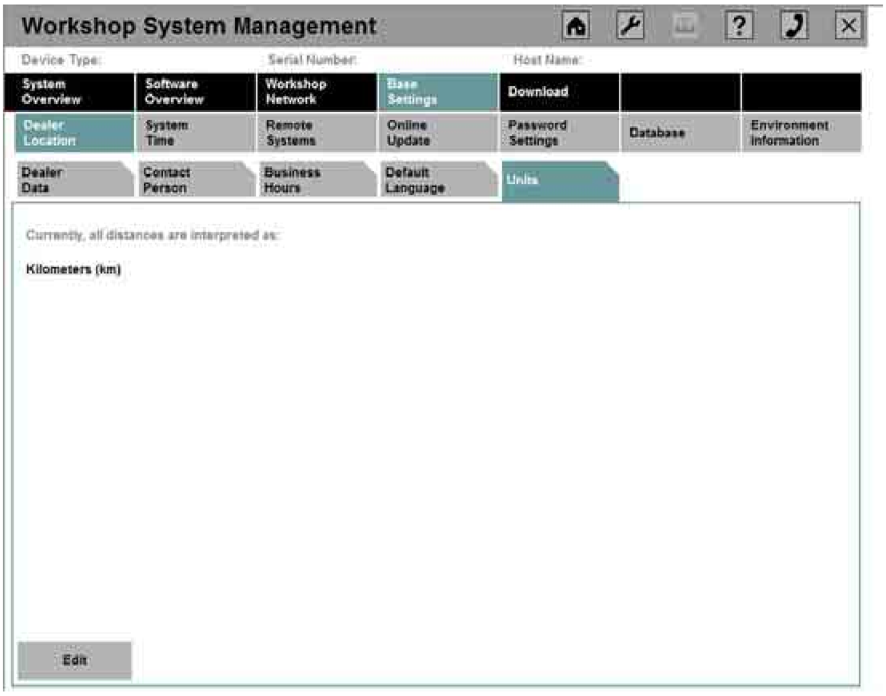
Once it has been set, the language can be changed by clicking "Edit", selecting the appropriate language in the next dialog box, and confirming this by clicking "Save".

Information:

Certain applications are geared to the system language set in the WSM.

5.1.11 Configuring units

The settings for units of distance are shown in the "Base Settings" menu, in the "Dealer Settings" submenu, under the "Units" tab (see Fig. 149).



Currently, all distances are interpreted as:

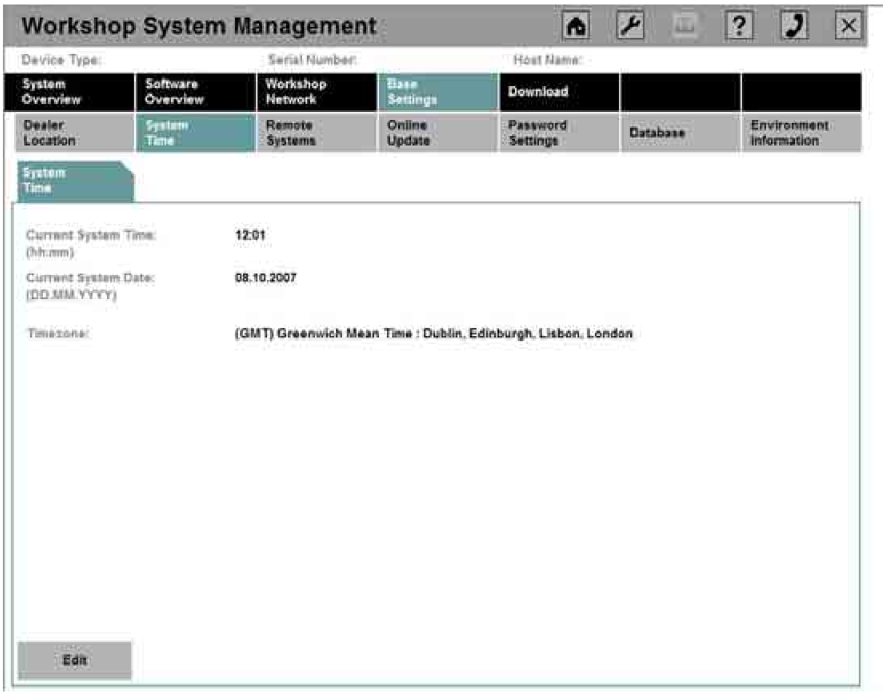
Kilometers (km)

Fig. 149: Metric units

Once the units have been set, they can be changed by clicking "Edit" and then choosing between kilometers and miles.
The selection is confirmed by clicking "Save".

5.1.12 Setting the system time

The "Base Settings" menu, in the "System Time" submenu provides the "System Time" tab (see Fig. 150) that lists the system’s time settings.



Current System Time: (hh:mm) 12:01

Current System Date: (DD.MM.YYYY) 08.10.2007

Timezone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

Fig. 150: System time

The settings can be changed by clicking the "Edit" button.

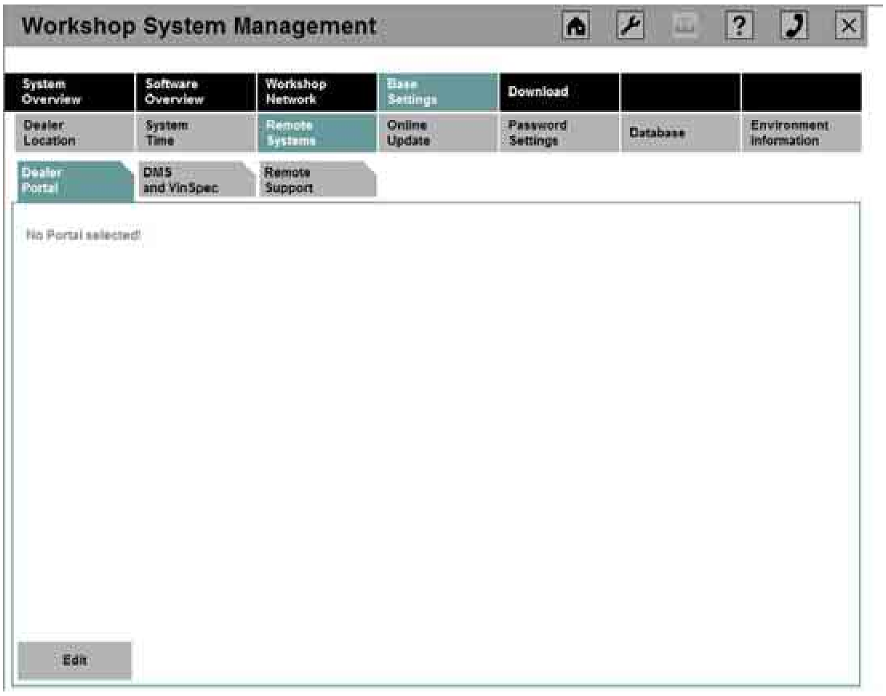
In the case of offline servers, the system time of the ISIS and the workshop devices is set at the ISIS itself. To do so, the time, date, and time zone applicable to the dealer must be entered.

If the ISIS is a system that is connected online, only the time zone can be set.

Abort the input by clicking “Cancel”. Confirm the entry by clicking "Save".

5.1.13 Selecting the BMW dealer portal

The setting of the portal via which the registration is to be completed is shown in the "Base Settings" menu, in the "Remote Systems" submenu, under the "Dealer Portal" tab (see Fig. 151).



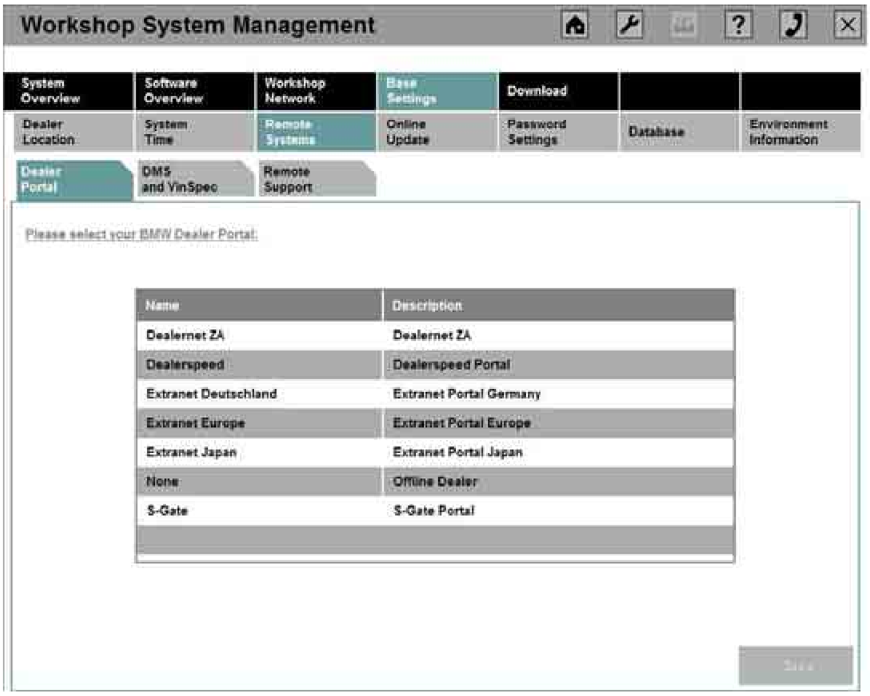
No Portal selected!

Fig. 151: Display of the dealer portal used

If you wish to change the portal setting, click "Edit" and then select a portal from the list (see Fig. 152). Click "Save" to confirm.

Note:

For an offline dealer, it make sure that the portal <None> is selected here.



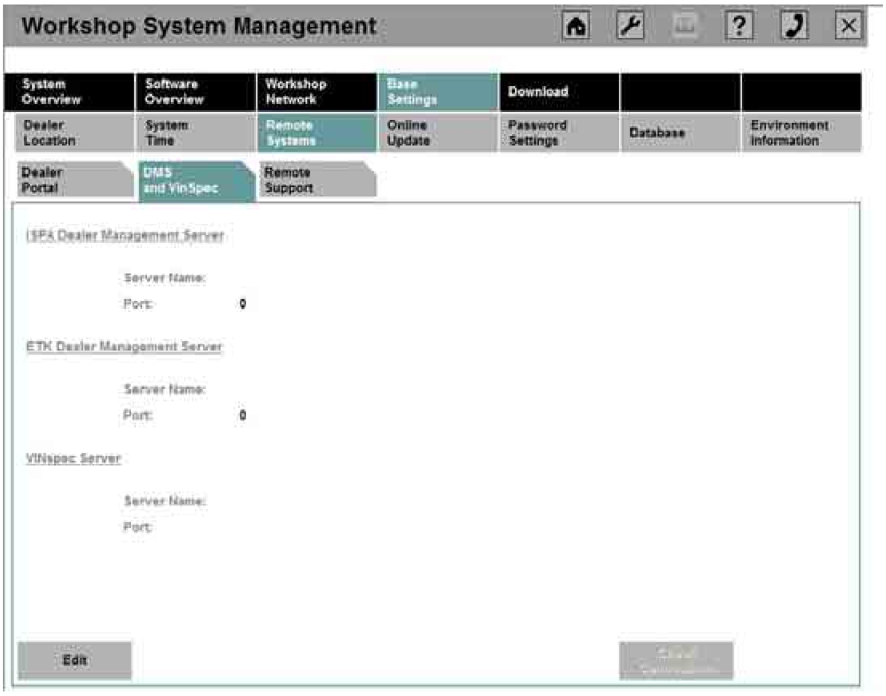
Please select your BMW Dealer Portal:

Name	Description
Dealernet ZA	Dealernet ZA
Dealerspeed	Dealerspeed Portal
Extranet Deutschland	Extranet Portal Germany
Extranet Europe	Extranet Portal Europe
Extranet Japan	Extranet Portal Japan
None	Offline Dealer
S-Gate	S-Gate Portal

Fig. 152: Selection of a dealer portal

5.1.14 Configuring DMS and VINSpec systems

The menu "Base Settings", in the "Remote Systems" submenu, contains the "DMS and VINSpec" tab (see Fig. 153), which lists the settings of the addresses of the Dealer Management Systems for the applications ISPA and EPC, as well as the entry of the address of the VINSpec server.



ISPA Dealer Management Server

Server Name:
Port: 0

ETK Dealer Management Server

Server Name:
Port: 0

VINspec Server

Server Name:
Port:

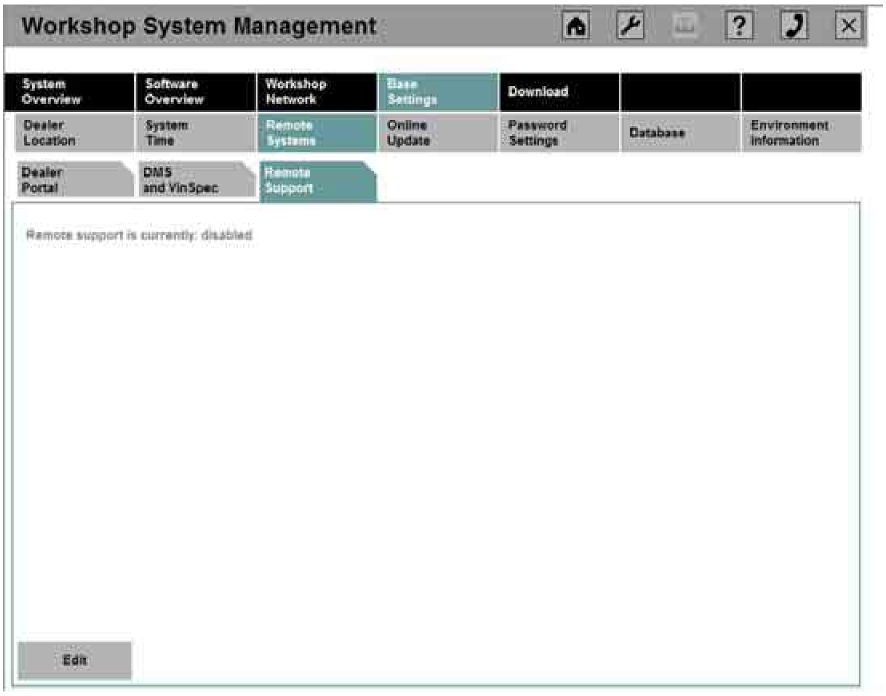
Fig. 153: Configuration of DMS and VINSpec systems

Changes can be made to the configuration by clicking "Edit" and specifying the corresponding server name and corresponding port.

The connections can be tested by clicking "Test Connection" and then the settings can be adopted by clicking "Save".

5.1.15 Activating and deactivating remote support

The setting for remote support is shown in the "Base Settings" menu, in the "Remote Systems" submenu, under the "Remote Support" tab (see Fig. 154).



Remote support is currently: disabled

Fig. 154: Settings for remote support

You can enable or disable remote support by clicking the "Edit" button.

Only if the remote support has been enabled can remote desktop connections to the ISIS be set up so that support can provide assistance with problems.

Information:

By default, remote support is disabled.

Note:

Enabling remote support permits various accesses to the ISIS (by means of remote desktop connections). Please make sure that you really want to do this.

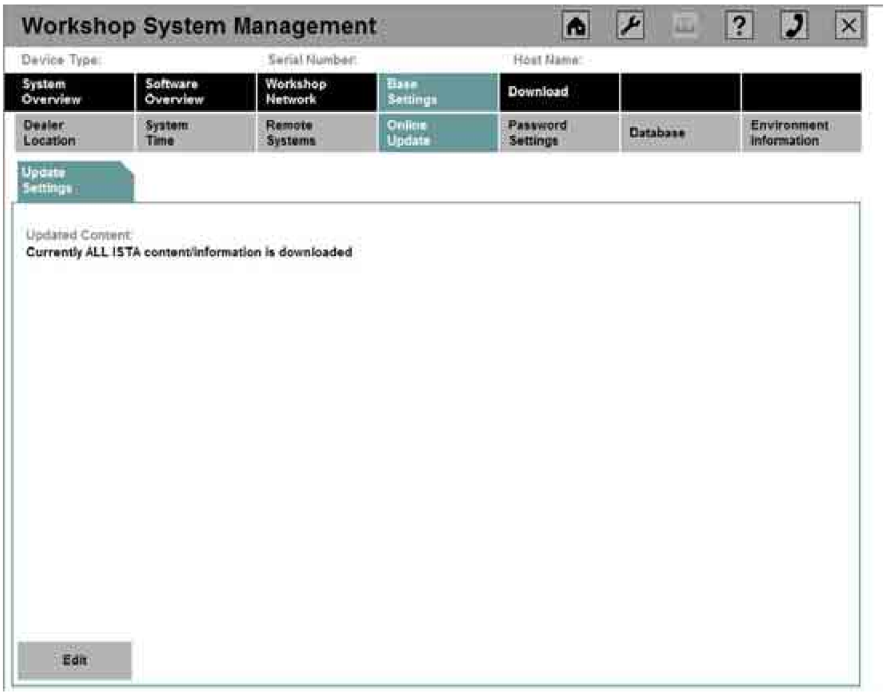
The change can be enabled by clicking "Save".

5.1.16 Setting the online update mode

To view the setting for the online update mode, open the main menu "Base Settings" and the submenu "Online Update" (see Fig. 155).

Information:

Currently, no change to the update mode can be made.



Device Type:

Serial Number:

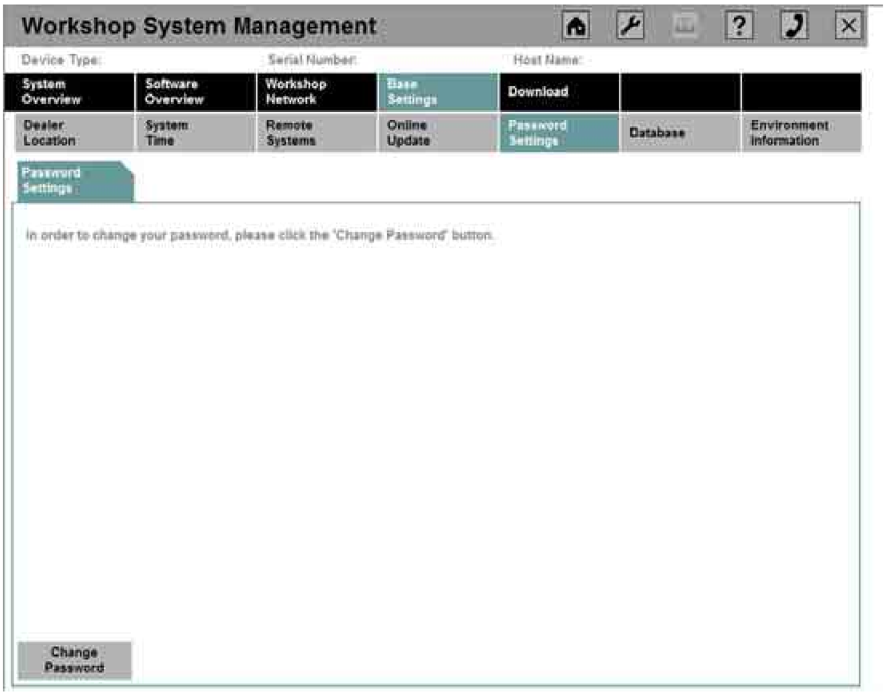
Host Name:

Updated Content:
Currently ALL ISTA content/information is downloaded

Fig. 155: Online update mode

5.1.17 Changing the WSM password

A change to the WSM password can be made in the main menu "Base Settings", in the submenu "Password Settings".

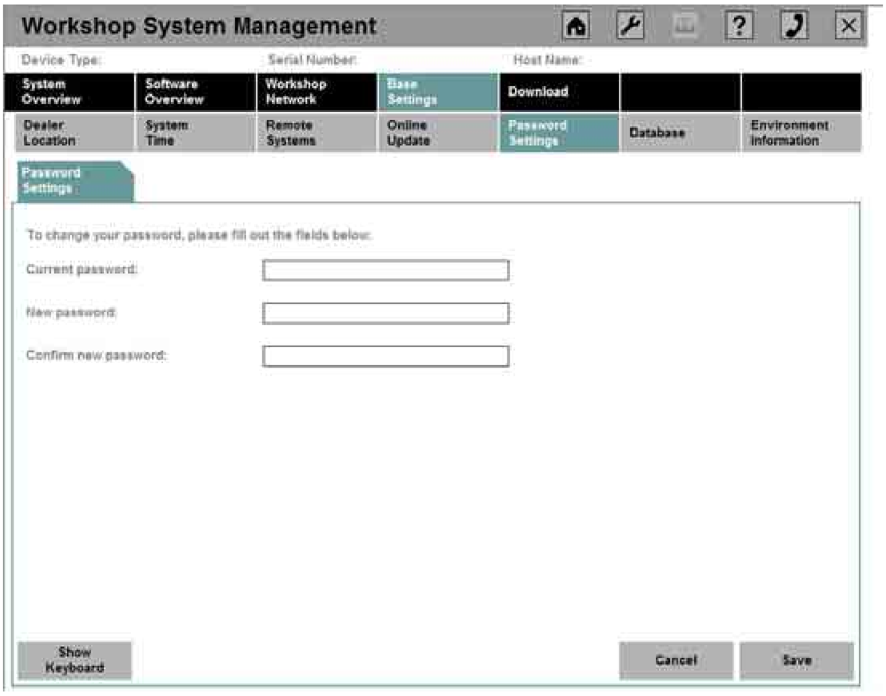


In order to change your password, please click the 'Change Password' button.

Fig. 156: Changing the password

The purpose of the password is to secure access to protected areas in the WSM and it should only be known to the person responsible for IT in the workshop in order to prevent unauthorized changes to the system.

The password is set for the first time during the installation (see chapter 3.1.8.2) and can be changed in the present dialog box (see Fig. 156) by clicking "Change Password".



Workshop System Management

Device Type:

Serial Number:

Host Name:

To change your password, please fill out the fields below:

Current password:

New password:

Confirm new password:

Fig. 157: Entering a new password

To change the password (see Fig. 157), first enter the current password and then the new password twice.

⚠	**Note:** Make sure that the password has at least eight characters and is composed of letters and numbers.

The new password is confirmed by clicking "Save" or rejected by clicking "Cancel".

If the user happens to forget the password, a password with limited validity can be requested from support. This password can be used to enter protected areas and set a new password.

5.1.18 Data backup

By default, data backup is carried out for all data.

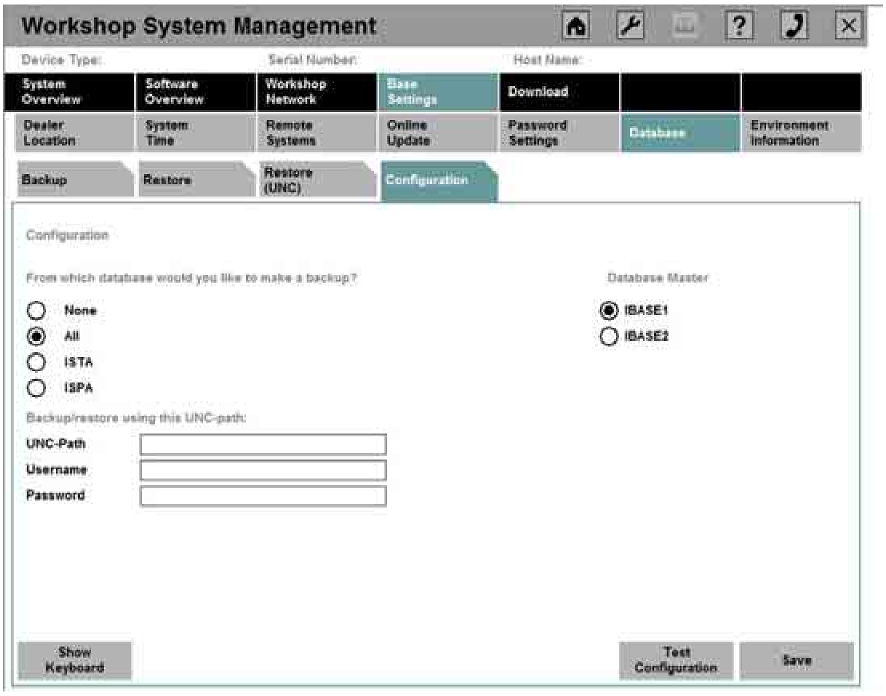
If adaptations to the configuration of the data backup are required, continue with the next sub-chapter. Otherwise, this chapter can be skipped.

5.1.18.1 Configuration of the data backup

The data backup is configured under the "Configuration" tab in the main menu "Base Settings", in the submenu "Database" (see Fig. 158).

i	**Information:** As a general principle, the data is backed up on both server plug-in modules. The number of data backups on the ISIS is a fixed number preset by the ISIS system.

It is also possible to save the data on an external share. A corresponding UNC path must be specified.



Configuration

From which database would you like to make a backup?

○ None
● All
○ ISTA
○ ISPA

Database Master

● IBASE1
○ IBASE2

Backup/restore using this UNC-path:

UNC-Path
Username
Password

Fig. 158: Configuration of the data backup

In the upper section of the dialog box (see Fig. 158), select which data is to be saved. On the right-hand side, select the active database which is to be backed up on both server plug-in modules . This is important in the event of an error so that the current data are correspondingly available.

⚠	**Note:** Please bear in mind that if the option "none" has been selected, it might not be possible to restore data in the event of a server failure.

For configuration of the UNC path in the lower part of the dialog box, please note the following:

Access to the external system requires a UNC[8] path, consisting of the computer name and share name.

For a corresponding authorization to access the share, a user name must be specified, consisting of the computer name\user or domain[9]\user. If required, the person responsible for IT at the company can provide information about both possibilities.

In addition, the corresponding password for access to the share must be specified.

The configuration can be tested by clicking "Test Configuration" and subsequently adopted by clicking "Save".

5.1.18.2 Running a data backup

General information on data backup:

To prevent data on the ISIS from being lost, it should be backed up regularly. For data backup, the following functions are provided:

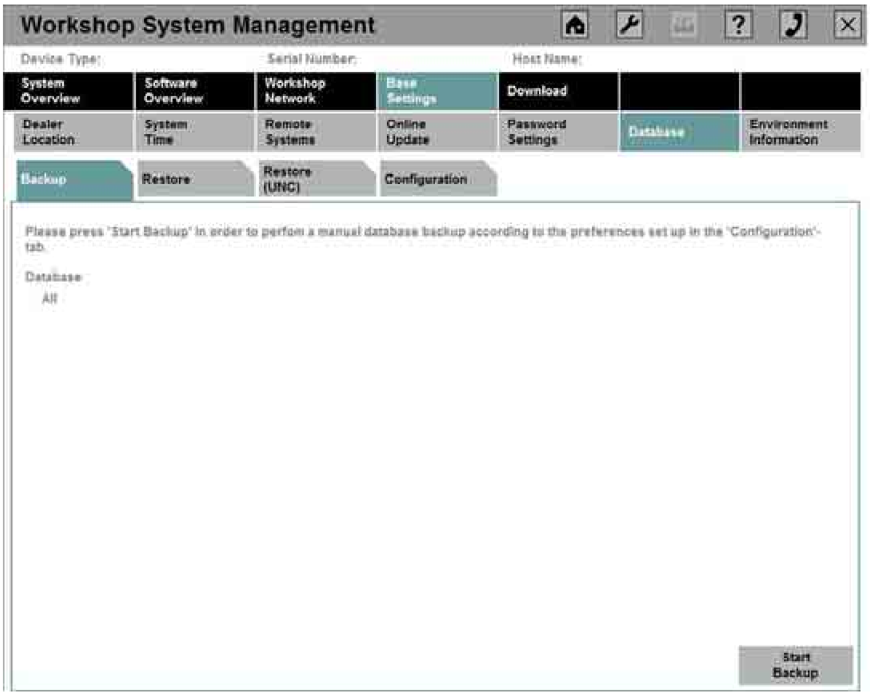
- Regular automated internal backup (daily at 12 noon and 12 midnight)
- Distributed data backups across all server plug-in modules to ensure a corresponding redundancy in the event of a failure
- Storage of data backups on external systems (by UNC path)

In addition to the automatic backup, it is also possible to start a manual backup.

The manual data backup is activated (see Fig. 159) via the main menu "Base Settings", in the submenu "Database" and is carried out based on the configuration (see chapter 5.1.18.1).

[8] UNC stands for *Uniform Naming Convention* and is regarded as the standard if a user wishes to reach shared resources in a computer network. If the UNC path is selected, there is no need for a connection with assignment of a drive letter. The format of such a path under Windows is: \\servername\sharename\path.

[9] In the Microsoft operating systems, a domain is a closed, trustworthy administrative structure and is not to be confused with the principle of a work group. Within a domain, users are not administered on the individual PC, rather centrally on one or a number of server systems.



Please press 'Start Backup' in order to perfom a manual database backup according to the preferences set up in the 'Configuration'-tab.

Database
All

Fig. 159: Running a data backup

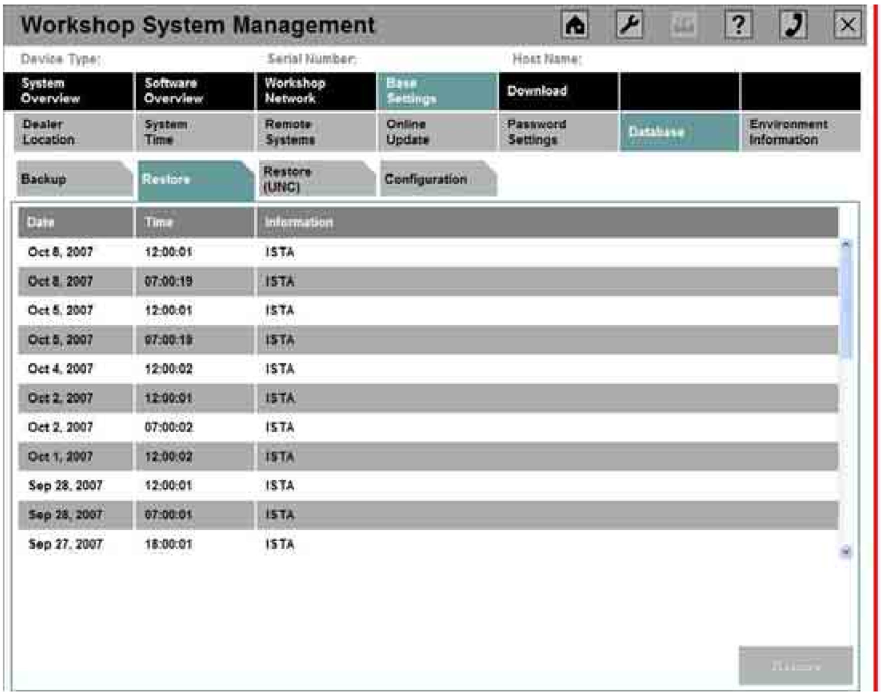
To create a backup, click the "Start Backup" button. The backup is then made available for data recovery (see chapter 5.1.19).

While the backup is being created, a corresponding message is displayed in the information area.

5.1.19 Running data recovery

The "Base Settings" menu item, in the "Database" submenu, under the "Restore" or "Restore (UNC)" tab lists the available ISTA and ISPA data backups.

Depending on the configuration, not only the local data backup of the ISIS (can be found in the "Restore" tab) but also the backup via an external share (to be found under the "Restore (UNC)" tab) can be used for data recovery.



Date	Time	Information
Oct 8, 2007	12:00:01	ISTA
Oct 8, 2007	07:00:19	ISTA
Oct 5, 2007	12:00:01	ISTA
Oct 5, 2007	07:00:19	ISTA
Oct 4, 2007	12:00:02	ISTA
Oct 2, 2007	12:00:01	ISTA
Oct 2, 2007	07:00:02	ISTA
Oct 1, 2007	12:00:02	ISTA
Sep 28, 2007	12:00:01	ISTA
Sep 28, 2007	07:00:01	ISTA
Sep 27, 2007	18:00:01	ISTA

Fig. 160: Recovery of the data

To trigger data recovery, select the desired backup in the corresponding dialog box
(in this case, by clicking "Restore" as an example; see Fig. 160) and click the "Load" button.

Use the scrollbar to view the entire list of the backup.

⚠	**Note 1:** When a data recovery has been started, the currently active database is overwritten with the data from the backup. Depending on which backup has been selected, there can be a loss of data between the current status and the selected backup.

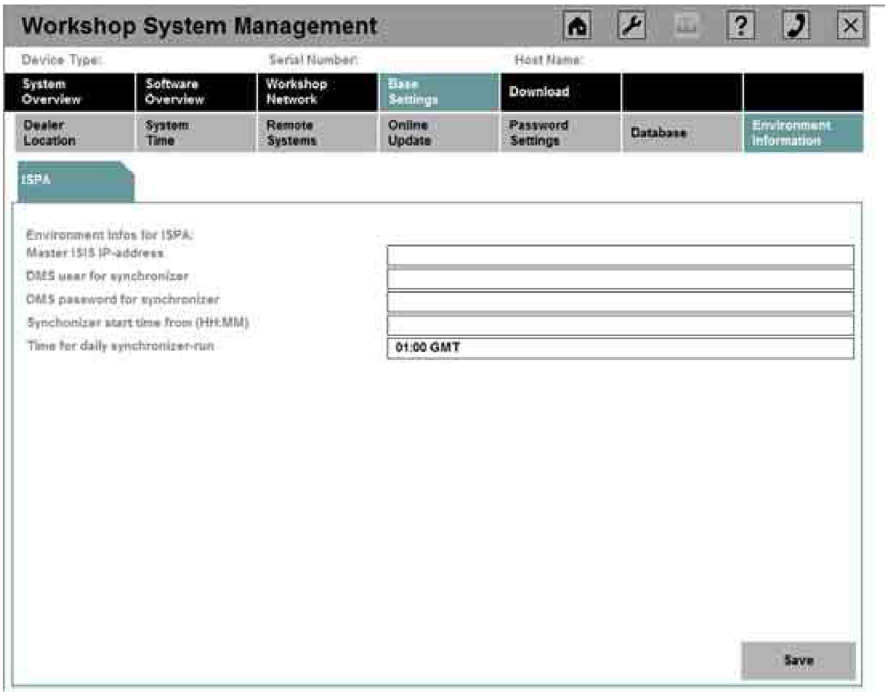
⚠	**Note 2:** It is crucial to remember that no ISIS applications (EPC, ISTA or ISPA) should be run on any of the workshop PCs during the data recovery. Otherwise, the active application is terminated abruptly at the time of the data recovery. Any data entered up to that point are lost.

5.1.20 Specifying environment information

Some applications (e.g. ISPA) require application-specific settings that can be made in the "Base Settings" main menu, in the "Environment Information" submenu (see Fig. 161).

Information:

More information on the various settings can be found in the User's Manuals of the individual applications.



Environment infos for ISPA:
Master ISIS IP-address
DMS user for synchronizer
DMS password for synchronizer
Synchonizer start time from (HH:MM)
Time for daily synchronizer-run 01:00 GMT

Fig. 161: Specifying environment information

The settings can be adopted by clicking the "Save" button.

5.1.21 ISIS DHCP configuration

The ISIS-DHCP configuration includes specifying an address pool from which the IP addresses for the DHCP service can be selected and enabling or disabling the DHCP service.

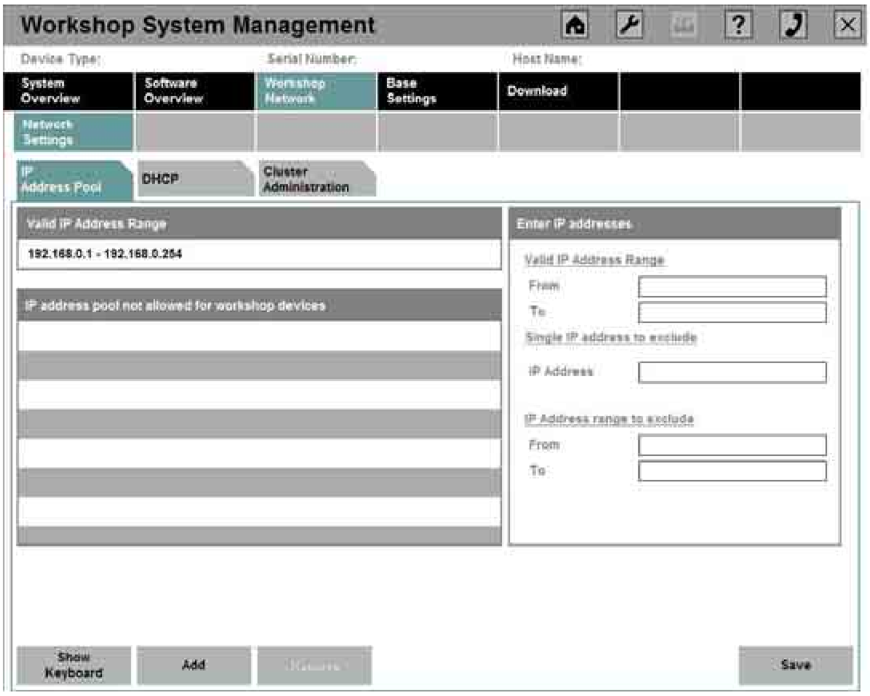
5.1.21.1 Specifying the IP address pool

The overview in the "Workshop Network" menu (submenu "Network Settings", tab "IP Address Pool") is used to display and configure the IP address pool.

If the DHCP server is to be used via the ISIS, a corresponding IP address pool must be made available for the devices to obtain the corresponding IP addresses.

The valid IP address range as well as non-permitted IP addresses and ranges for workshop devices are displayed in the screen.

The configuration can be changed by clicking the "Edit" button (see Fig. 162).



Device Type:
Serial Number:
Host Name:

Valid IP Address Range
192.168.0.1 - 192.168.0.254

IP address pool not allowed for workshop devices

Enter IP addresses

Valid IP Address Range
From
To

Single IP address to exclude
IP Address

IP Address range to exclude
From
To

Fig. 162: Editing the IP address pool

Here, the valid IP address range can be changed and IPs and IP address ranges can be excluded from the valid range.

⚠	**Note:** If static IP addresses have already been allocated in the workshop network, these have to be excluded individually from the possible address range in order to prevent IP address conflicts.

The inputs are adopted into the list on the left-hand side by clicking "Add".

Other IP inputs can be made in the same way.

To remove a non-permitted IP address or a non-permitted IP address range from the left-hand list, select the IP address or address range and then click the "Remove" button.

The complete configuration can be adopted and activated by clicking "Save". The user is then automatically returned to the overview that contains the new configuration.

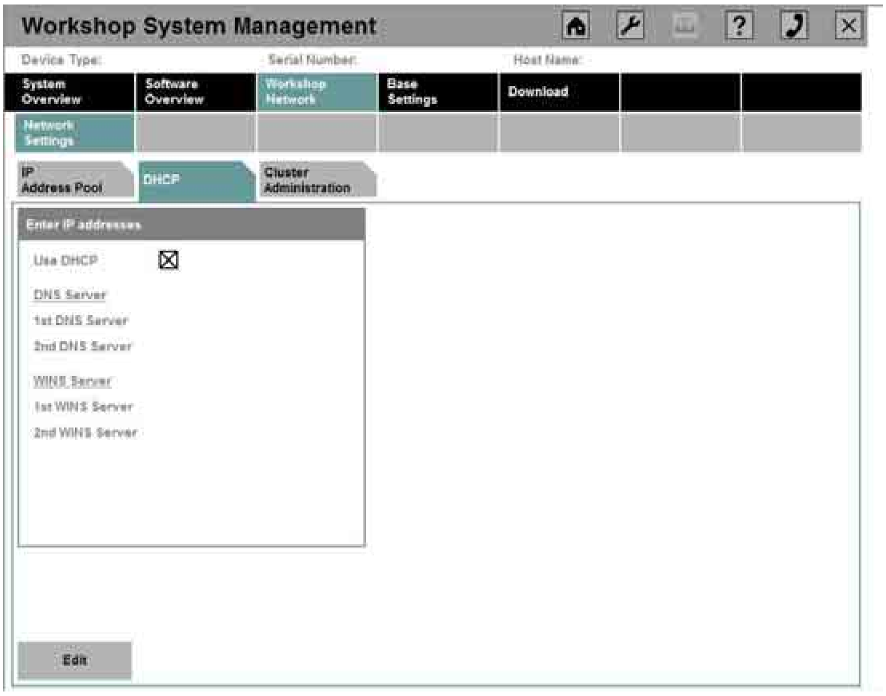
To enable the DHCP server, proceed according to the steps in the next chapter.

5.1.21.2 Enabling and disabling DHCP

Note:

Please follow the instructions from chapter 2.3.1.

Other DHCP settings, including the enabling and disabling of the DHCP server of the ISIS, can be made in the main menu "Workshop Network" (in the submenu "Network Settings"), under the tab "DHCP" (see Fig. 163).



Use DHCP ☒

DNS Server
1st DNS Server
2nd DNS Server

WINS Server
1st WINS Server
2nd WINS Server

Fig. 163: DHCP settings

The configuration can be changed by clicking "Edit".

Selecting "Use DHCP" enables the ISIS DHCP server.

Note:

The dynamic address assignment may only be enabled if no other DHCP server (e.g. Windows 2000/2003 server, ISDN, or DSL router) is active within the network.

In addition, DNS[10] and WINS[11] servers can be configured in this screen.

[10] The **Domain Name System** (**DNS**) has the task, among others, of converting Internet addresses into the corresponding IP address.

[11] The **Windows Internet Name Service (WINS)** is a system for the dynamic resolution of NetBIOS names. WINS works in a similar manner to DNS. If a new device goes on the network, it registers its name automatically with the WINS server, which means that manual intervention is not necessary. Furthermore, not only the NetBIOS name but also the name of the domain and the names of the logged in users and user groups are registered.

Thereafter, the settings can be adopted by clicking "Save".

5.1.22 Cluster administration

The ISIS clusters known to the system can be found via the menu item "Workshop Network", in the submenu "Network Settings", under the tab "Cluster Administration".

In order to use the database on another ISIS cluster (this can be the case, for example, when various subsidiary dealership branches want to use the database of the main dealership), one cluster must make the other cluster aware of the database.

The "Cluster Administration" screen contains a list of the various cluster addresses with the following information:

- Cluster ID
- Cluster IP
- Current status of reachability
- Number of attempts if the cluster is not reached

Information:

Approx. 180 attempts are made to reach a cluster. However, if no connection can be set up, the cluster is automatically removed from the list.

Editing the cluster administration settings:

If you wish to make your own cluster known to other clusters, select "Edit" to make the corresponding settings in the dialog box that follows (see Fig. 164).

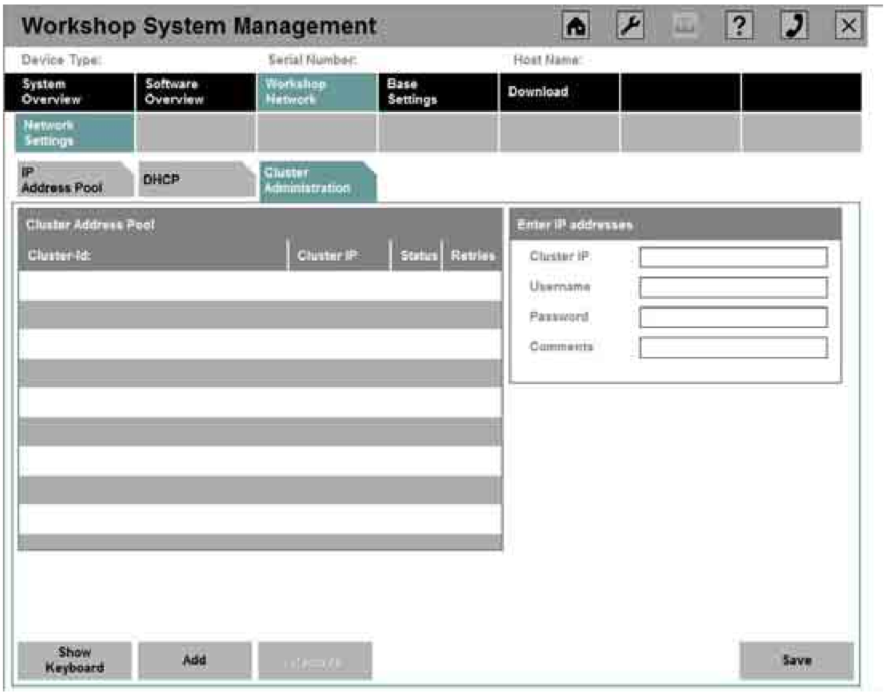


Fig. 164: Editing the cluster administration settings

On the right-hand side of the screen (see Fig. 164), the cluster IP, the corresponding user name with password and an additional comment can be specified for each cluster. After the inputs have been checked, they are included in the list on the left by clicking "Add".

This operation can be repeated for any number of clusters.

Existing clusters can be deleted from the list by selecting them in the left-hand overview and then clicking the "Remove" button.

To adopt the changes you have made, click the "Save" button.

Note:

Other configurations are required in each of the applications (ISPA and ISTA).

5.1.23 Displaying and downloading stored PDF files

In the main menu "Download" (see Fig. 165), documents created on the ISID (by means of a PDF printer driver, see chapter 6.4) are provided for downloading.

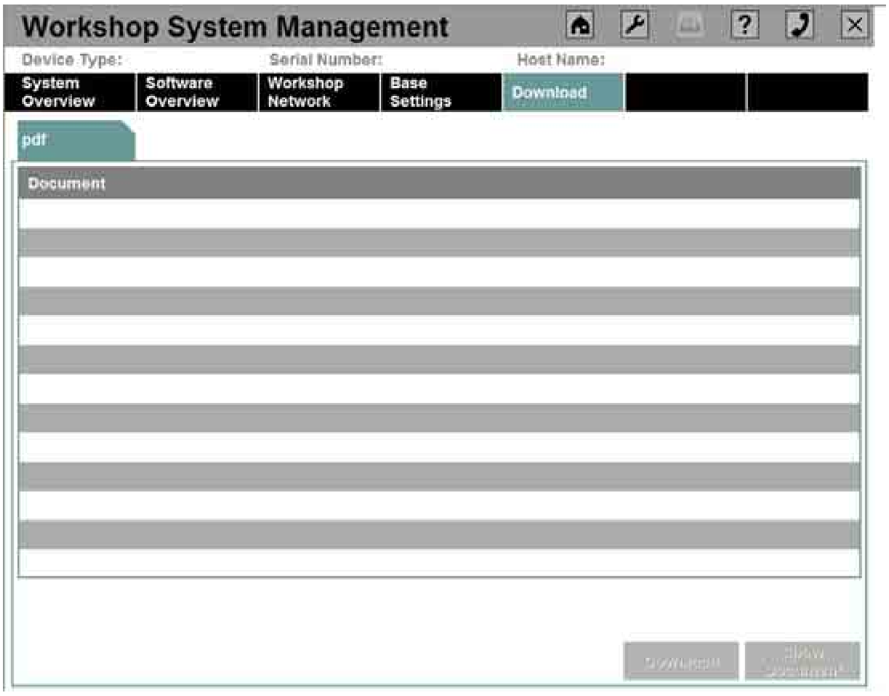


Fig. 165: Downloading documents

The corresponding document can be selected and subsequently displayed in the overview ("Display Document" button) or downloaded onto the workshop PC ("Download" button).

Note:

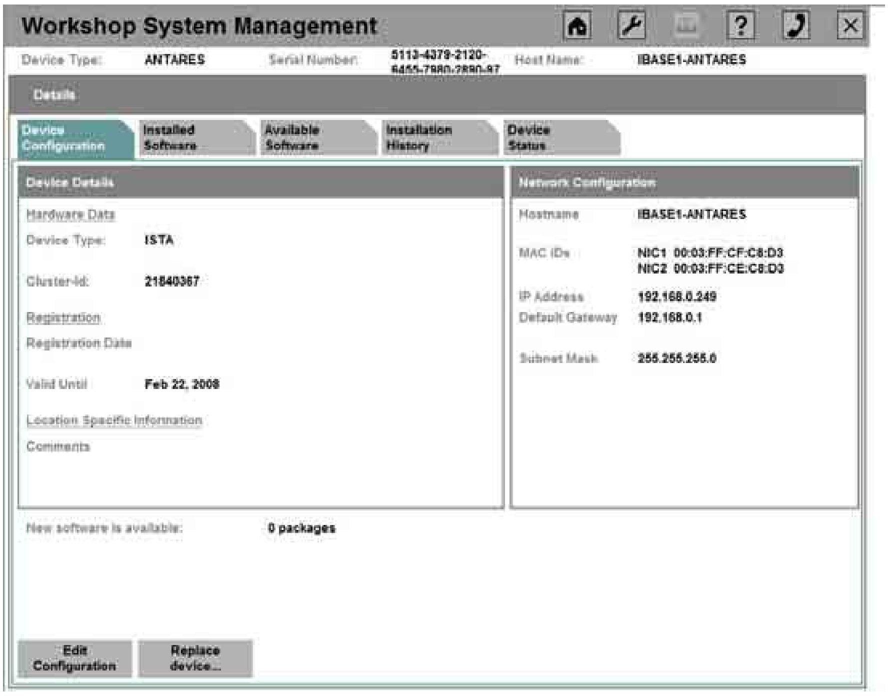
The documents are deleted one after the other as soon as the directory in which the documents have been stored exceeds a certain size. The delete operation starts with the oldest file. For this reason, all important documents should be downloaded as soon as they become available.

5.1.24 Reinstalling applications (EPC, ISTA, ISPA)

The WSM provides a simple possibility to reinstall the applications used.

Select the corresponding application in the System Overview and then click the "Device Details" button.

In the dialog box that appears (see Fig. 166), the details of the device are listed and the application can be uninstalled by clicking the "Replace Device" button. The application is then installed anew in the next maintenance period.



Device Type: ANTARES Serial Number: 5113-4379-2120-6455-7880-2890-97 Host Name: IBASE1-ANTARES

Hardware Data
Device Type: ISTA
Cluster-Id: 21840367
Registration
Registration Date
Valid Until Feb 22, 2008
Location Specific Information
Comments

Hostname IBASE1-ANTARES
MAC IDs NIC1 00:03:FF:CF:C8:D3
NIC2 00:03:FF:CE:C8:D3
IP Address 192.168.0.249
Default Gateway 192.168.0.1
Subnet Mask 255.255.255.0

New software is available: 0 packages

Fig. 166: Reinstalling applications

6 Special features of the WSM on the ISID

This chapter describes only the different or additional functions of the WSM on the ISID.

6.1 Start page of the ISID

The start page of the ISID is also referred to as 'Jumpgate' (see Fig. 167).

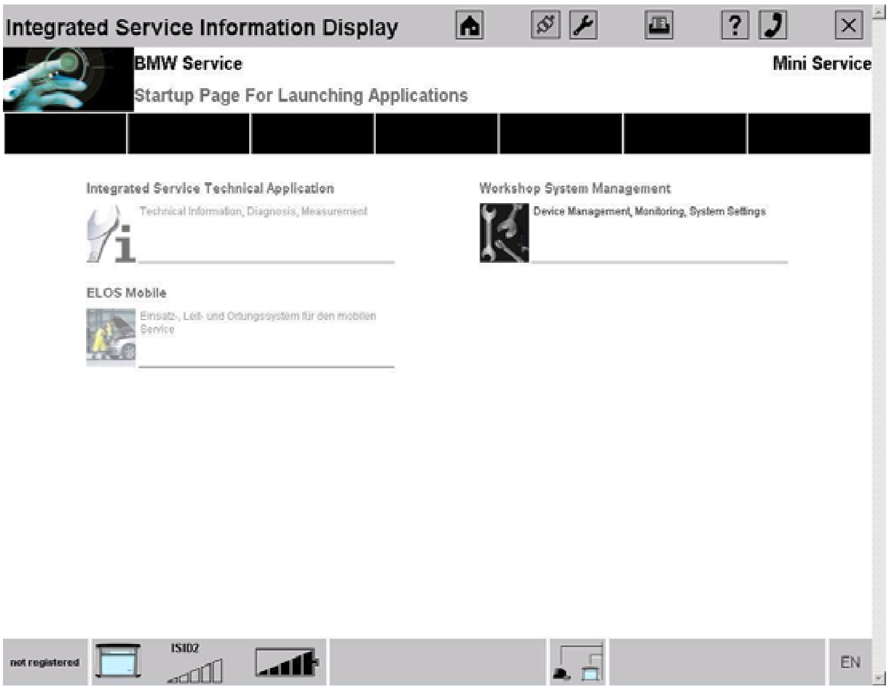

Integrated Service Information Display
BMW Service
Mini Service
Startup Page For Launching Applications
Integrated Service Technical Application
Technical Information, Diagnosis, Measurement
Workshop System Management
Device Management, Monitoring, System Settings
ELOS Mobile
Einsatz-, Leit- und Ortungssystem für den mobilen Service
not registered
ISID2
EN

Fig. 167: Jumpgate

The various applications (such as WSM, ISTA, and ELOS) can be started from this start page.

6.1.1 Icon bar on the start page of the ISID

The icon bar on the startup page of the ISID has a design similar to that of the icon bar in the WSM. The meanings of the individual icons are given in the following table.

Icon	Name	Meaning
🏠	WSM start page	Opens the WSM start page
🔌 🔌	Connection mode change	Displays the current mode of the ISID
🔧	WSM settings on the ISID	Making various settings for the WSM
🖶	Print	Prints the device information
?	Help	Help (this User Guide and system information)
☎	Callback (support request)	Opens the page for managing support requests (callbacks)
✕	Close	Shutdown of the ISID

6.1.2 Status bars on the ISID

The status bar contains various items of information regarding the status of the ISID.

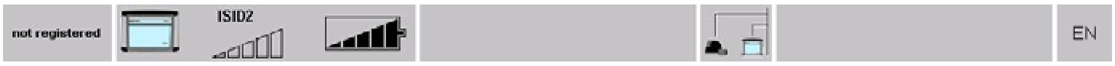


Fig. 168: ISID status bar

The meanings of the individual displays are given in the following table:

Display	Name	Meaning
🔋	Battery	Display of the current battery status
🖧	Connection mode	Display of the mode the ISID is in
📶	Connection quality	Display of the connection quality of the WLAN connection
ISID2	Name of the ISID	Display of the ISID name analogous to the display in the WSM System Overview
EN	Language	Set language of the ISID

6.2 Changing the connection (infrastructure mode, temporary offline mode, or WLAN)

The display for changing the connection mode on the start page of the ISID (see plug icon in Fig. 167) is indicated by 2 different icons (see Fig. 169 and Fig. 170)

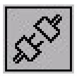


Fig. 169: ISID is in the temporary offline mode

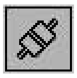
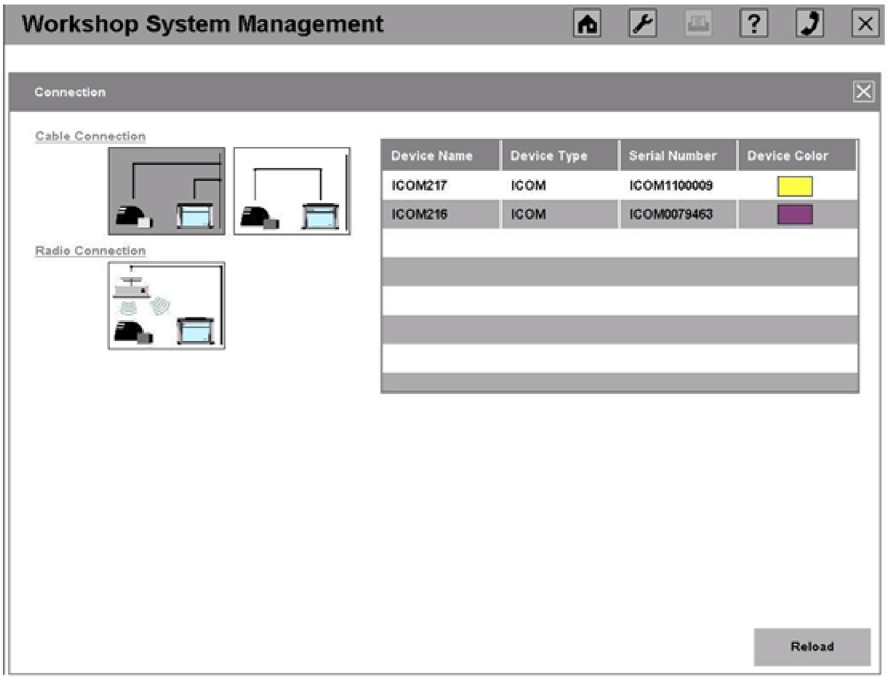


Fig. 170: ISID is in the infrastructure mode

If you wish to change the connection type and also specify which devices are to be adopted into the new mode, select the corresponding icon (see Fig. 169 or Fig. 170) in the toolbar.

A dialog box for selecting the connection type (Fig. 171) appears, listing the available connection types on the left-hand side. The devices that are available depending on the selected connection type are listed on the right-hand side of the dialog box.



Device Name	Device Type	Serial Number	Device Color
ICOM217	ICOM	ICOM1100009	🟨
ICOM216	ICOM	ICOM0079463	🟪

Fig. 171: Changing the connection

Selecting the connection type

A total of four different connection types are available for selection:

- LAN cable connection via switch (infrastructure mode)
- LAN cable direct connection (temporary offline mode)
- WLAN connection via Access Point
- Direct radio connection (not yet available)

i	Information: The connection via Access Point can only be selected if the ISID has already been configured for WLAN

Selecting the devices to be adopted into the new mode

Depending on which mode the ISID is in, the available devices are shown on the right-hand side of the dialog box.

In the case of a mode change, select the corresponding devices to be adopted into the new mode from the right-hand table and set the new mode.

Changing the connection type

After selecting the device that is also to be adopted into the new mode and specifying the new mode, a dialog box opens, asking whether the connection type is to be changed. Confirmation by clicking "OK" starts the connection change.

Remaining procedure the sample switch from the infrastructure mode into the temporary offline mode

After confirmation by clicking "OK", a new dialog box opens. At this point, the ICOM must be directly connected to the ISID. If this has been done correctly, various services start up on the ISID and the connection type has been changed successfully.

After switching into the temporary offline mode, the corresponding symbol appears in the status bar (see Fig. 172). The number of days on which the ISID can remain in the temporary offline mode is displayed beside the 'Connect' symbol. The duration is restricted to a maximum of 11 days, because among other things, no updates can be run if there is no connection between the ISIDs and the ISIS.

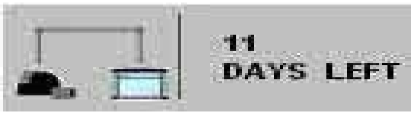
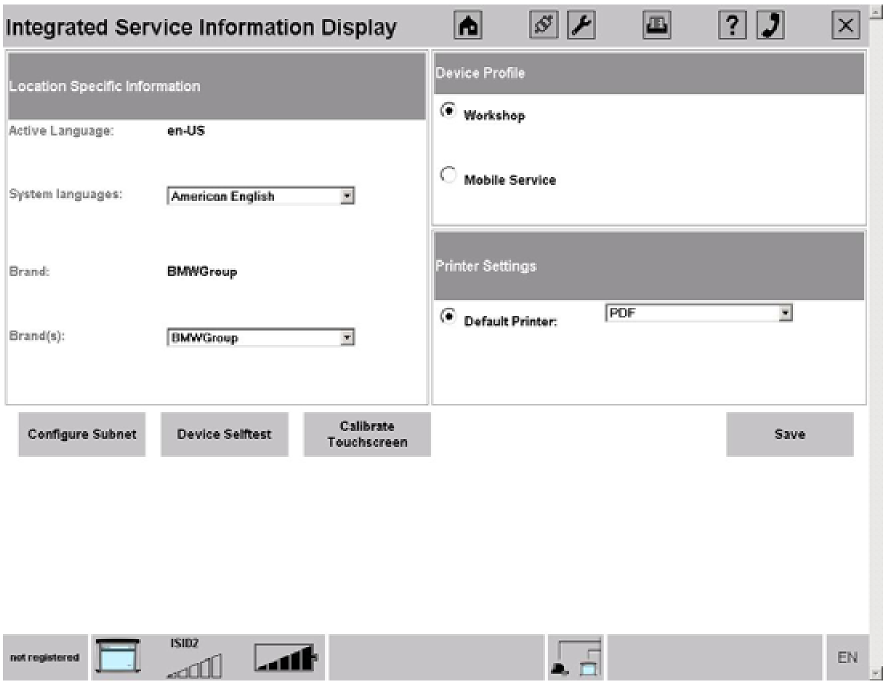


Fig. 172: Display of the temporary offline mode

i	**Information:** If the ISID is in the temporary offline mode and it is connected to the infrastructure, the status of the ISID switches automatically to the infrastructure mode. The ICOM remains in the relevant connection type. To change the connection type, the ICOM must be connected accordingly (infrastructure or offline) and restarted beforehand.

6.3 Administration of the ISID

Various settings (see Fig. 173) can be configured on the ISID via the start page of the ISID and by selecting the 'wrench' icon. These are explained in the following subchapters.



Integrated Service Information Display

Location Specific Information

Active Language: en-US

System languages: American English

Brand: BMWGroup

Brand(s): BMWGroup

Device Profile

● Workshop

○ Mobile Service

Printer Settings

● Default Printer: PDF

Fig. 173: Settings on the ISID

6.3.1 Setting the system language

The system language for the applications can be set in the top left-hand corner of the dialog box that appears via the start page of the ISID and by selecting the 'wrench' icon (see Fig. 173). Selecting the small arrow to the right of the selection field displays the entire list, enabling selection of the corresponding language.

The procedure is completed by clicking "Continue” to confirm the inputs.

6.3.2 Setting the brand - setting the color assignment of the WSM

The brand can be set in the top left-hand corner of the dialog box that appears via the start page of the ISID and by selecting the 'wrench' icon (see Fig. 173). Selecting the small arrow to the right of the selection field displays the entire list, enabling selection of the corresponding brand from all of the brands available to the dealer.

The procedure is completed by clicking "Continue" to confirm the inputs.

6.3.3 Setting the profile

The device profile for the applications can be set in the top right-hand corner of the dialog box that appears via the start page of the ISID and by selecting the 'wrench' icon (see Fig. 173). Either the "Workshop" profile or the "Mobile Service" profile can be set.

The procedure is completed by clicking "Continue" to confirm the inputs.

6.3.4 Setting the printer

Via the start page of the ISID and by selecting the 'wrench' icon, the printer responsible for print output can be selected on the lower right-hand side of the screen that appears (see Fig. 173) when the ISID is in the infrastructure mode.

The procedure is completed by clicking "Continue"" to confirm the inputs.

6.3.5 Calibrating the touch-screen

The necessary cycle for renewing the calibration data depends heavily on the environmental conditions in daily use (e.g. temperature, humidity). However, calibration of the touch-screen once a year should be adequate.

If the point you press on the touchscreen is different from the point perceived by the program, then it is time to calibrate the screen.

The calibration can be started from the WSM by selecting the 'wrench' icon on the startup page of the ISID and clicking the "Calibrate Touch-screen" button in the dialog box that appears.

The calibration takes place in accordance with the steps from chapter 3.2.6.1.

After completion of the calibration, the "Administration" screen is displayed again.

6.4 Printing

The printer functionality differs according to the profile in which the ISID is running.

In the Mobile Service profile, a USB printer can be connected to the ISID, and this can be used to print the current document.

In the Infrastructure mode, documents can also be printed on the printers configured on the ISIS. To do so, the document is transferred to the ISIS and then output on the configured printer.

In addition, PDF files can be created by means of a PDF printer driver. These are then transferred to the ISIS and displayed in the main menu "Download", from which they can be downloaded to the workshop PC (see chapter 5.1.23).

⚠	**Note:** It is unfortunately not possible to specify a name for the document.

6.5 Help

The help is operated in the same way as the help of the WSM on the ISIS (see chapter 5.1.1.4).

6.6 Callback

⚠	**Note:** The callback function is only enabled when the ISID is in the infrastructure mode.

The callback mechanism is operated in the same way as it is used on the ISIS (see chapter 8.5).

6.7 Switching off the ISID

Clicking the "Close" icon switches off the ISID.

6.8 Communication beyond subnet boundaries

⚠	**Note:** The home ISIS is the ISIS on which the ISID was commissioned.

For communication of an ISID beyond subnet boundaries, the following three variants are possible:

ISID is connected to its home ISIS:

In this case, no user interaction is necessary because the ISID automatically connects to its home ISIS.

ISID cannot connect to its home ISIS:

The ISID is located e.g. in another subnet. The ISID attempts to find its home ISIS, but is unable to reach it.

In this case, a pop-up opens on the start page of the ISID. Enter the IP address of the new ISIS and then click the "Repeat" button.

Manual change to the set IP:

In this case, click the 'wrench' icon in the Jumpgate. On the Administration page, click the "Configure Subnet" button, then enter the desired IP address into the menu that appears (see Fig. 174) and click "Repeat".

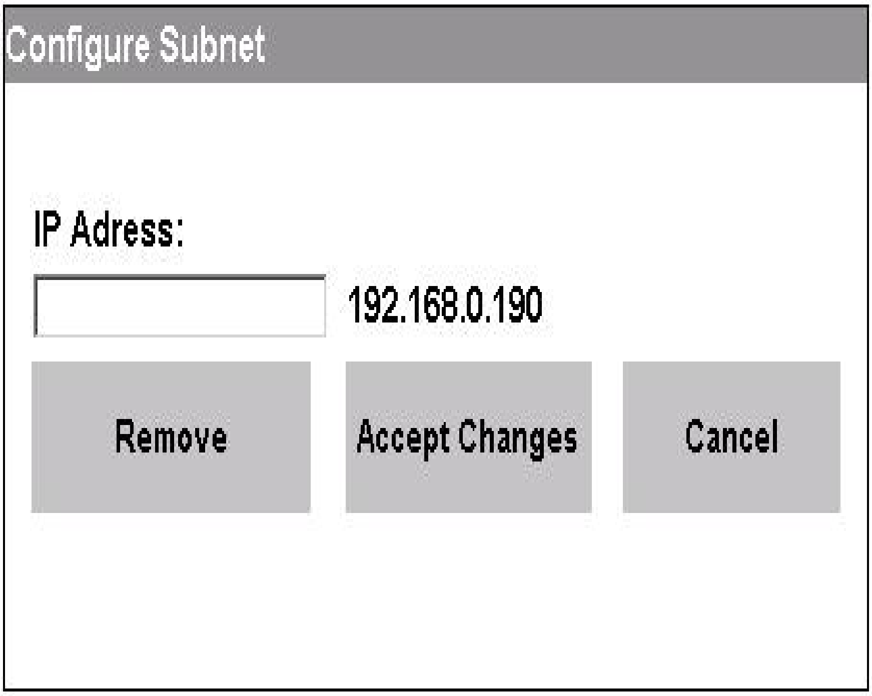


Fig. 174: Changing the IP address of the ISID

If the ISID is in the home network but outside of the set subnet, a pop-up window appears. The IP address for the new subnet must be entered in this window.

7 Special features of the ICOM

7.1 Communication beyond subnet boundaries

⚠	**Note:** The home ISIS is the ISIS on which the ICOM was commissioned.

To communicate beyond subnet boundaries, the ICOM must be in the subnet of its home ISIS when it is registered. The ICOM saves the IP address of its home ISIS. If the ICOM enters another subnet, it searches for a new ISIS. If this is not successful, it reconnects to the home ISIS.

If the ICOM does not find an ISIS, it should be restarted. If this does not help, operate the ICOM in the home network once again. If this also fails, open a callback ticket.

8 Troubleshooting

8.1 Self-help for problems – symptoms / causes

8.1.1 Commissioning and installing ISIS

Symptom	Possible cause	Solution
Wipe of the ISIS is not carried out.	This might involve an incorrect Wipe CD or the CD is not legible.	Please check whether you are using the correct Wipe CD and, if applicable, insert the correct CD. If the CD is correct but cannot be read → Open a callback ticket.
The installation DVD is ejected before data could be copied from the DVD.	This might involve an incorrect DVD or the DVD is not legible.	Please check whether you are using the correct DVD and, if applicable, insert the correct DVD. If the DVD is correct but cannot be read → Open a callback ticket.
Installation aborts at a certain point with an error before an IP is displayed on the ISIS.	Errors occurred during the installation.	Try to run the installation again. If the error recurs → Open a callback ticket and specify the error code.
Configuration of the ISIS could not be completed.	The entered data may contain errors or else not all of the commissioning and configuration instructions were followed.	Check all of your entries and follow the instructions for commissioning and configuration of the ISIS. If the error occurs again → Open a callback ticket.
Once you have completed setup, one or a number of VMs with the name "BMW ..." go online.		A restart of the server from the WSM remedies this problem.
After setup, the second ISIS is in a different cluster to that of the first ISIS.	Brief interruption of the connection from ISIS1 to ISIS2 during registration	Unregister the second ISIS, then reboot (from the WSM). Once it is online again and all indicators are green, it can be re-registered.
ISIS1 and ISIS2 are not synchronized after setup.		Shut down the ISIS2 via WSM, then reboot the ISIS1 via the WSM. Once the first ISIS has rebooted (ISIS1 and all its VMs are green in the WSM), switch on the second ISIS again.

8.1.2 Commissioning and installing ISID

Symptom	Possible cause	Solution
During installation procedure: 1st phase		
Error message: "connection to server failed" "cannot access installation sources"	No connection to the server	Please check the LAN connection: Check the cable and plug connections; if the error occurs again during a new installation → Open a callback ticket.
Error message: "partitioning of disk failed"	Hard disk error	Restart the installation. If the error occurs again → Open a callback ticket.
Error message: "setting of NTFS rights failed"	Hard disk error	Restart the installation. If the error occurs again → Open a callback ticket.
Error message: "copy files to local disk failed"	Installation source not installed on server ISIS or hard disk error	Reinstall the RAM boot image and restart the ISID installation. If the error occurs again → Open a callback ticket.
Error message: "deploy files to local disk failed"	Installed files on the ISIS are corrupt or hard disk error	Reinstall the RAM boot image on the ISIS and restart the ISID installation. If the error occurs again → Open a callback ticket.
Error message: "deletion of installation sources failed"; The ISID system may nevertheless remain usable	Hard disk error	Open a callback ticket.
Error message: "installation aborted"	Follow any additional instructions!	If the error occurs during a renewed installation attempt → Open a callback ticket.
During installation procedure: 2nd phase		
Error message: "Deployment process did not end successfully Please repeat deployment process Installation aborted. Please switch off the ISID now"	Follow any additional instructions!	In the first phase of the installation, problems that prevent another installation occurred. The installation must be restarted from the beginning, i.e. new start of the ISID with button combination 1+4
Error message: "Could not create logging directory Installation aborted. Please switch off the ISID now"	Hardware might be defective.	There were problems accessing the hard disk. The installation must be restarted, i.e. new start of the ISID with button combination

Symptom	Possible cause	Solution
		1+4
Error message: "Could not create Logfile Installation aborted. Please switch off the ISID now"	Hardware might be defective.	There were problems accessing the hard disk. The installation must be restarted, i.e. new start of the ISID with button combination 1+4
Error message: "Could not change drive letter Installation aborted. Please switch off the ISID now"	Hardware might be defective.	There were problems accessing the hard disk. The installation must be restarted, i.e. new start of the ISID with button combination 1+4
Error message: "Could not copy the System-API Installation aborted. Please switch off the ISID now"	Hardware might be defective.	There were problems accessing the hard disk. The installation must be restarted, i.e. new start of the ISID with button combination 1+4
Error message: "Copying of config file failed. Installation aborted. The system cannot find the file specified."	Configuration file could not be copied from the ISIS to the ISID or this file does not exist	Open a callback ticket.
Error message: "Could not apply post-installation tasks Installation aborted. Please switch off the ISID now"	Hardware might be defective.	There were problems accessing the hard disk. The installation must be restarted, i.e. new start of the ISID with button combination 1+4
Error message: "Could not apply new hostname Installation aborted. Please switch off the ISID now"	Hardware might be defective.	There were problems accessing the hard disk. The installation must be restarted, i.e. new start of the ISID with button combination 1+4
Error message: "Installation of WSM failed Installation aborted. Please switch off the ISID now"	Hardware might be defective.	There were problems accessing the hard disk. The installation must be restarted, i.e. new start of the ISID with button combination 1+4
Error message: "Installation of IVM failed Installation aborted. Please switch off the ISID now"	Hardware might be defective.	There were problems accessing the hard disk. The installation must be restarted, i.e. new start of the

Symptom	Possible cause	Solution
		ISID with button combination 1+4
Error message: "Installation of JetStream failed Installation aborted. Please switch off the ISID now”	Hardware might be defective.	There were problems accessing the hard disk. The installation must be restarted, i.e. new start of the ISID with button combination 1+4
During installation procedure: 3rd phase		
Error message: "Errors occurred in FBA phase (part 1) Installation aborted. Please switch off ISID now"	The installation script in the 2nd phase of the installation was not terminated properly.	The installation cannot be continued and must be restarted, i.e. new start of the ISID with button combination 1+4
On starting the ISID		
Error message: "Restart the ISID. Hold buttons 1 and 4 simultaneously when system starts."	No operating system	Install the ISID (see chapter 3.2.3).
Operating unit does not start, screen remains black, no LED lights up	Battery is dead	Charge battery or switch to external power supply. If the error symptom remains: →Open a callback ticket.

8.1.3 Registration problems

Symptom	Possible cause	Solution
ISIS registration cannot be carried out.	The corresponding dealer portal has not be correctly selected or the access data to the portal is incorrect.	Please check whether the right portal is set (for offline dealers, the portal "None"). If necessary, also check to make sure your access data for the corresponding portal are correct. If you are still unable to carry out the registration → Open a callback ticket.
Offline registration cannot be carried using of the registration fax.	An error might have occurred during data entry.	Please check that all of the entered data correctly matches the data from the registration fax.

Symptom	Possible cause	Solution
		If you are still unable to carry out the registration → Open a callback ticket.
Registration of ISID or ICOM is not carried out	The device might already be registered for another dealer.	Open a callback ticket.

8.1.4 Communication beyond subnet boundaries, ICOM

Symptom	Possible cause	Solution
When using the ICOM in another subnet, no ISIS is found.	There are problems with the software and/or hardware of the ICOM or there are network problems.	Restart the ICOM. If this does not help, operate the ICOM in the subnet itself. If no ISIS is found here either, open a callback ticket.

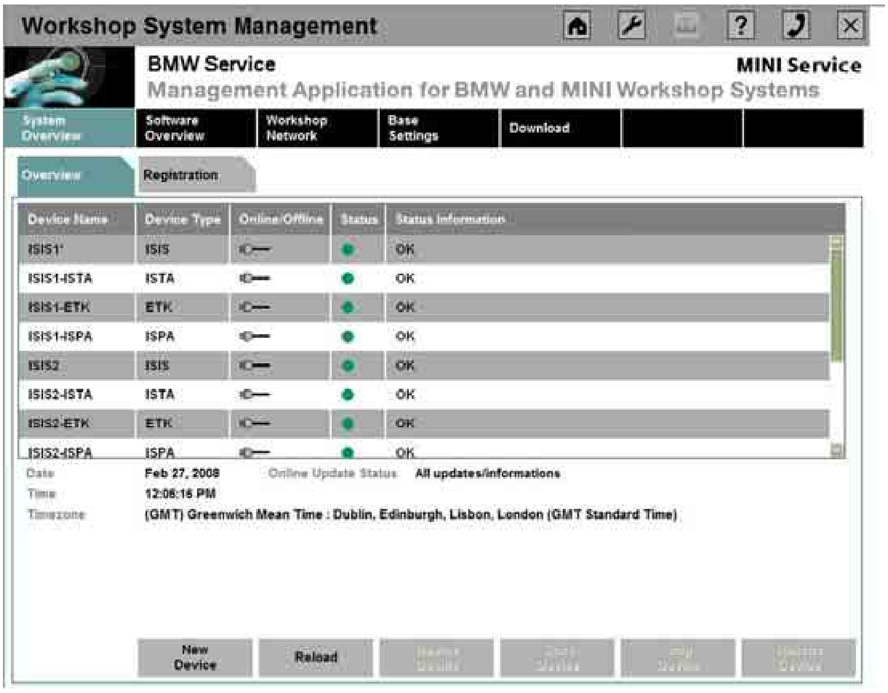
8.1.5 Using WSM

Symptom	Possible cause	Solution
WSM message "UPS not available".	Cabling, communication problem	In such cases, the PrimusHit solution EN3013 should be used (request via 1st Level).
Device was added to the WSM, but cannot be used	ISIS-DHCP range is exhausted	Extend the DHCP range. If the error persists → Open a callback ticket.
WSM password is no longer valid after new installation	The password might have been set to the password "admin" after the new installation of the WSM	Assign a new password by using the password "admin" as the old password.
WSM password is not accepted	The WSM password has been forgotten.	Open a callback ticket. You are provided with a newly generated system password that is valid as the old password for specifying a new password. Bear in mind that the generated password is only valid for a certain time span.
Message in the WSM "Local server unavailable"		Restart the server. If the error is still displayed →

Symptom	Possible cause	Solution
		Open a callback ticket.
Callback could not be sent.	Problems with the language templates or routing table	Set the language to English and submit the callback once again. You can then reset the language to your national language. If this does not help, contact 1st Level Support (possible suspicion: the routing tables could be incorrect).
Callback could not be created.	JetStream local server is not started.	Restart the master server via the WSM.
USV beeps and indicates that there is no power.	Power connection has been disconnected.	Check all power connections of the ISIS.
USV beeps and indicates that there is no power.	Power failure in the server room.	If everything is correctly cabled, there is a defective fuse or power failure. In this case, the server (as of V1100) automatically powers down to prevent damage to the ISIS. Once the power supply has been restored, the server restarts.
No network connection to the ISIS present.	Network cable has been disconnected.	Check the cabling of the ISIS to see whether a network cable has been inadvertently unplugged.
Backup via UNC path does not save anything on the client computer.	UNC path data is incorrect.	Check whether the data specified in the UNC configuration is correct. Also check specifically whether the specified IP address is correct (via DHCP, the IP address may change from time to time).
A VM is displayed as offline in WSM.		Select the VM and click the "Start Device" button. If this does not help, contact 1st Level Support.

8.2 System status / check device status

The system status can be viewed in the "System Overview" (see Fig. 175). All the devices of the workshop network are listed here and the status of the individual devices is displayed in the corresponding column. If an error occurs, brief information on the problem is provided in the "Status Information" column.

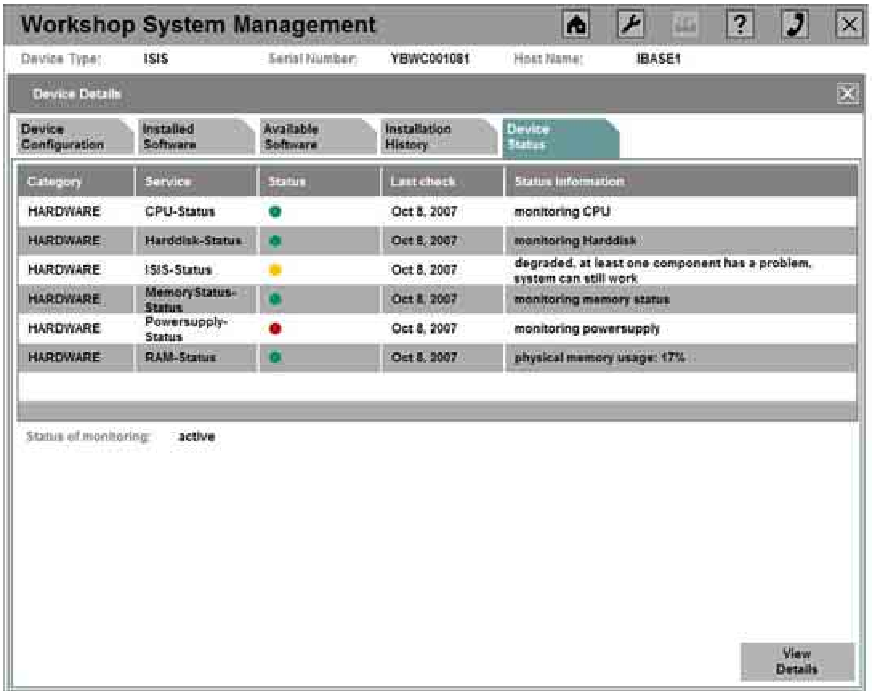


Device Name	Device Type	Online/Offline	Status	Status Information
ISIS1'	ISIS		●	OK
ISIS1-ISTA	ISTA		●	OK
ISIS1-ETK	ETK		●	OK
ISIS1-ISPA	ISPA		●	OK
ISIS2	ISIS		●	OK
ISIS2-ISTA	ISTA		●	OK
ISIS2-ETK	ETK		●	OK
ISIS2-ISPA	ISPA		●	OK

Date Feb 27, 2008 Online Update Status All updates/informations
Time 12:08:16 PM
Timezone (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London (GMT Standard Time)

Fig. 175: Viewing the system status

Selecting the device in the "System Overview" and clicking accordingly on "Device Details" opens the Device Overview. Clicking the "Device Status" displays the detailed status of the device.



Device Type: ISIS Serial Number: YBWC001081 Host Name: IBASE1

Category	Service	Status	Last check	Status information
HARDWARE	CPU-Status	●	Oct 8, 2007	monitoring CPU
HARDWARE	Harddisk-Status	●	Oct 8, 2007	monitoring Harddisk
HARDWARE	ISIS-Status	●	Oct 8, 2007	degraded, at least one component has a problem, system can still work
HARDWARE	MemoryStatus-Status	●	Oct 8, 2007	monitoring memory status
HARDWARE	Powersupply-Status	●	Oct 8, 2007	monitoring powersupply
HARDWARE	RAM-Status	●	Oct 8, 2007	physical memory usage: 17%

Status of monitoring: active

Fig. 176: Device status information

Information:

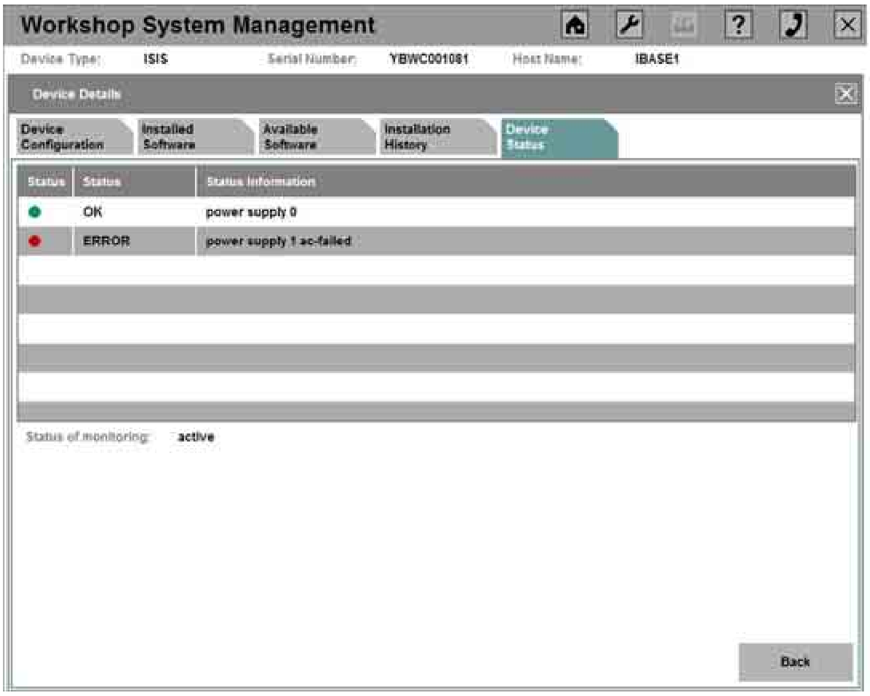
In ISID and ICOM, the screens differ slightly from the screen used in ISIS.

The dialog box is divided into the following subitems (see Fig. 176):

- Category – describes the service categories available.
- Service – indicates the service to be checked.
- Status – assumes one of the three status colors (green, yellow, red).
- Last check – indicates the time that the last check was carried out.
- Status information – generates a brief written message in English regarding the check result.

The current monitoring status (active or inactive) is specified in the information area.

If the user wishes to see detailed information about a test result, *Details* can be accessed by clicking the corresponding line (see Fig. 177).



Workshop System Management

Device Type: ISIS Serial Number: YBWC001081 Host Name: IBASE1

Device Details

Status	Status	Status Information
●	OK	power supply 0
●	ERROR	power supply 1 ac-failed

Status of monitoring: active

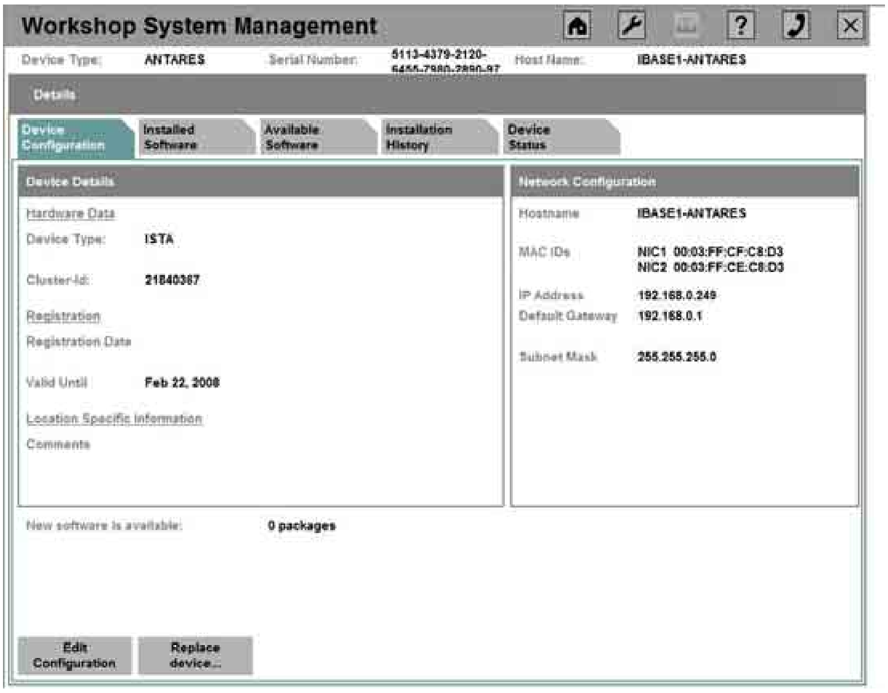
Fig. 177: Details on the device status

Clicking the "Back" button closes the current dialog box.

8.3 Reinstalling applications

In the WSM, it is possible to remove and reinstall applications (ISTA, ISPA, EPC). This procedure is necessary, for example, if errors occur during the installation or if the applications no longer start.

Selecting the desired application in the "System Overview" menu (see Fig. 128) and clicking the "Device Details" button opens the "Device Configuration" dialog box (see Fig. 178).



Device Type: ANTARES
Serial Number: 5113-4379-2120-6455-7980-2890-97
Host Name: IBASE1-ANTARES

Hardware Data

Device Type: ISTA

Cluster-Id: 21840367

Registration

Registration Date

Valid Until Feb 22, 2008

Location Specific Information

Comments

Hostname IBASE1-ANTARES

MAC IDs NIC1 00:03:FF:CF:C8:D3
NIC2 00:03:FF:CE:C8:D3

IP Address 192.168.0.249

Default Gateway 192.168.0.1

Subnet Mask 255.255.255.0

New software is available: 0 packages

Fig. 178: Replacing applications

The displayed application can now be uninstalled. To do so, first click the button "Replace Device..." and then click "OK" in the pop-up window that follows.

After successful uninstallation, the application is automatically reinstalled in the next maintenance period.

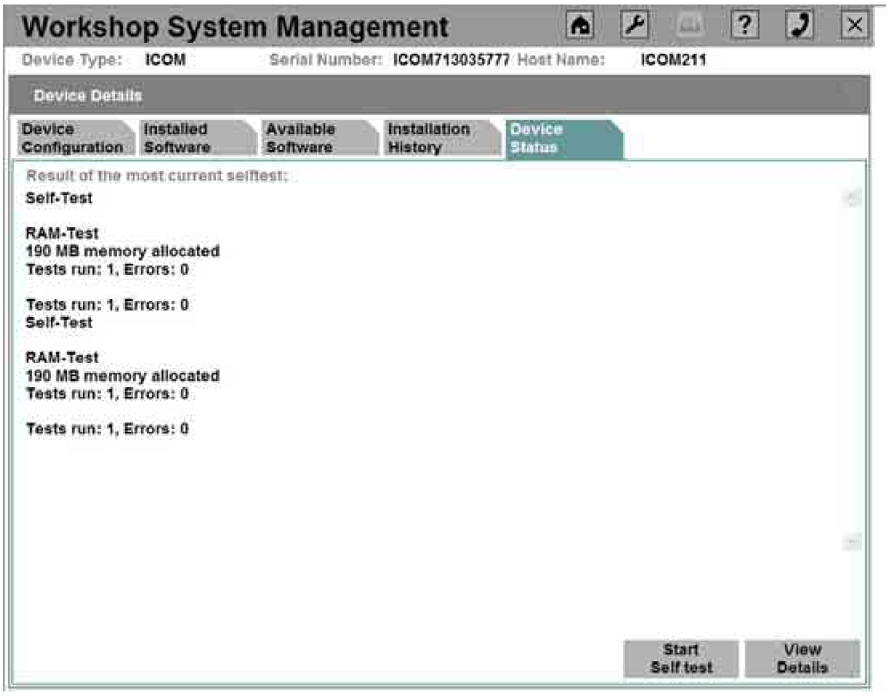
The manual installation is started via the "Software Overview" by clicking the "Install Package" button.

After displaying a message that the installation has been started, the program switches to the System Overview. The status is shown in yellow after each server plug-in module and the installation indicator "Software Installed" appears at "Status Information". Here, the applications are in the offline mode (plug icon crossed out).

8.4 Running a self-test of a device

If problems with a device (e.g. ISID, ICOM or ISAP) are detected, i.e. an error (yellow or red) is displayed in the status field, a self-test of the device can be carried out to obtain more detailed information on the problem that has occurred.

The self-test can be started by opening the "System Overview", selecting the corresponding device, clicking the "Device Details" button, "Device Status" tab and then clicking the "Start Self-test" button (see Fig. 179).



Device Type: ICOM Serial Number: ICOM713035777 Host Name: ICOM211

Result of the most current selftest:

```
Self-Test

RAM-Test
190 MB memory allocated
Tests run: 1, Errors: 0

Tests run: 1, Errors: 0
Self-Test

RAM-Test
190 MB memory allocated
Tests run: 1, Errors: 0

Tests run: 1, Errors: 0
```

Fig. 179: Display of the device status after running a self-test

During the self-test, an activity indicator appears.

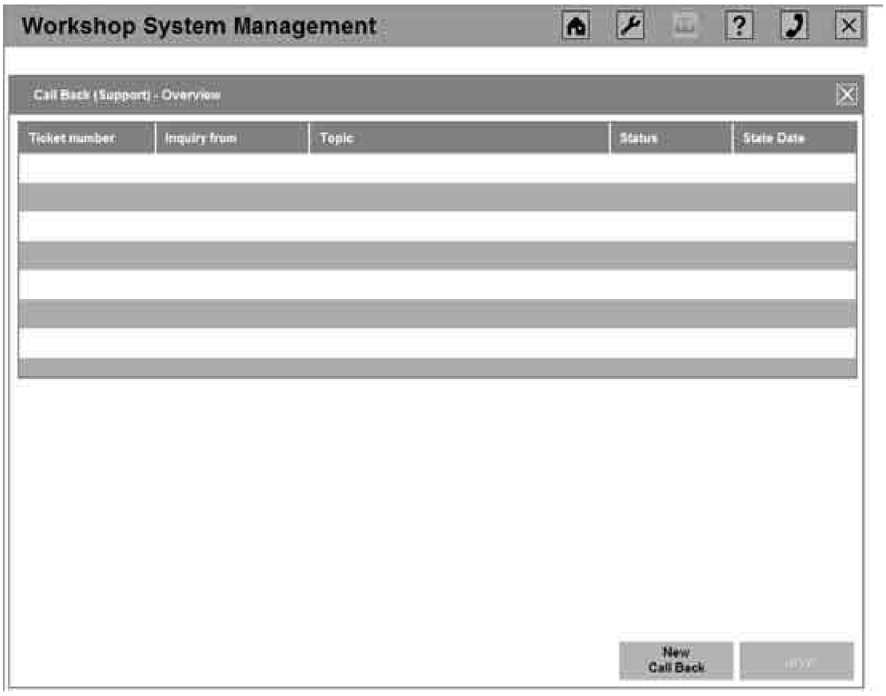
After a short time, the result of the self-test is displayed in the device status overview.

i	**Information:** For an ICOM, a log file is created and its content is then displayed.

8.5 Support request / sending a callback

The malfunction notification for the ISIS generally takes place via the callback mechanism of the Workshop System Management. The malfunction notifications are then forwarded automatically to the appropriate support office and processed there.

The telephone receiver icon in the icon bar at the top right takes the user to the Callback system (see Fig. 180) that is used for administering, writing, and sending support requests.



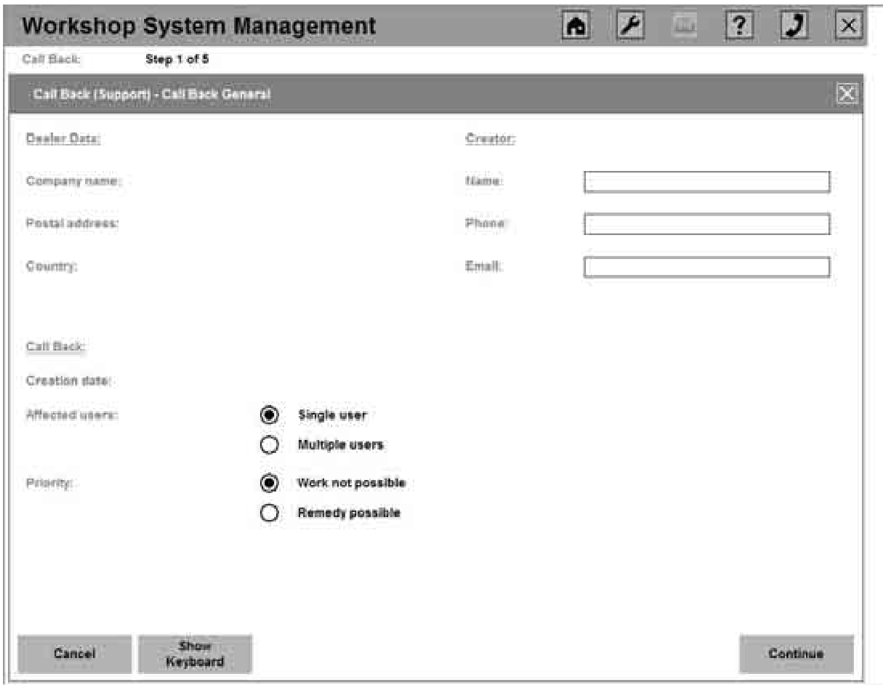
Workshop System Management

Call Back (Support) - Overview

Ticket number	Inquiry from	Topic	Status	State Date

Fig. 180: Overview of callback

Clicking the "New Callback" button brings up the next dialog box (see Fig. 181).



Workshop System Management

Call Back: Step 1 of 5

Call Back (Support) - Call Back General

Dealer Data:

Company name:

Postal address:

Country:

Creator:

Name:

Phone:

Email:

Call Back:

Creation date:

Affected users: ● Single user ○ Multiple users

Priority: ● Work not possible ○ Remedy possible

Fig. 181: Opening a callback

In Step 1, first the general dealer data (company name, postal address and country) is generated automatically, as is the creation date of the callback.

With regard to callback data, the following details must be specified:

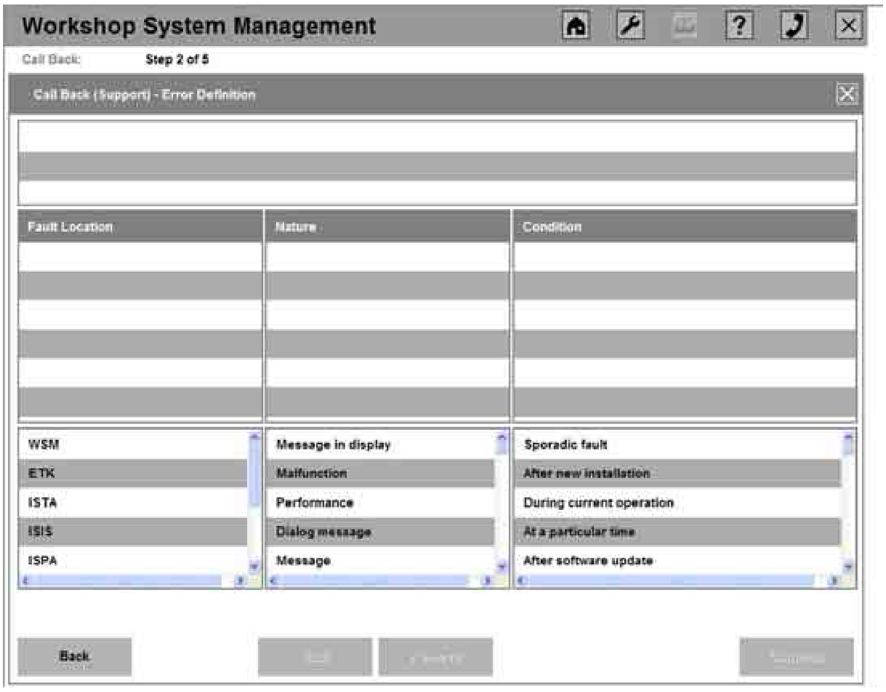
- Under Affected users, the user must specify whether a single user or multiple users is/are affected.
- Under Priority, the user must absolutely indicate whether the error that has occurred has halted work processes or whether a workaround would permit work to continue – at least temporarily.

In the right-hand column, the input fields are to be completed as follows:

- Name of the person responsible for ISIS
- Phone number of the person responsible for ISIS
- E-mail address of the person responsible for ISIS (optional)

Clicking the "Cancel" button aborts the support request.

Clicking the "Continue" button takes the user to the next dialog box (see Fig. 182).



Workshop System Management

Call Back: Step 2 of 5

Call Back (Support) - Error Definition

Fault Location	Nature	Condition
WSM	Message in display	Sporadic fault
ETK	Malfunction	After new installation
ISTA	Performance	During current operation
ISIS	Dialog message	At a particular time
ISPA	Message	After software update

Fig. 182: Selection of the error definition

In step 2, the user can simplify the description of the error by compiling the corresponding error variants from an error pattern system.

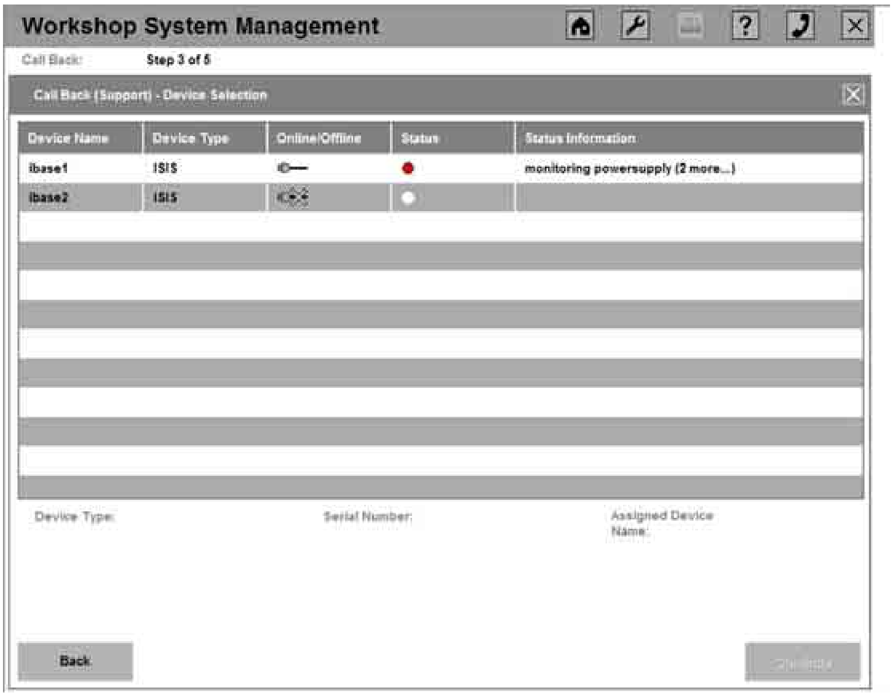
Selecting the corresponding specifications consisting of error location, error type and general condition adopts these into the middle area.

Once the error profile has been clearly described, it is added to the callback by clicking the "Add" button.

Other error profiles can also be added to the callback in this way.

If the description of the added error profile is not completely correct, it can be removed from the callback list by selecting it and then clicking "Remove".

Once all the error profiles have been included in the top list, click "Continue" to proceed.



Workshop System Management

Call Back: Step 3 of 5

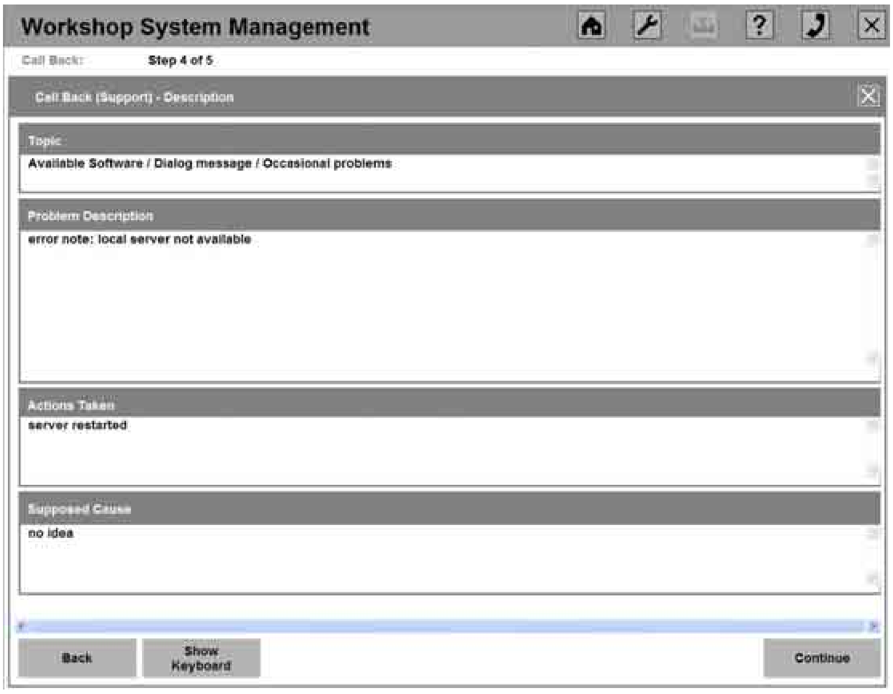
Call Back (Support) - Device Selection

Device Name	Device Type	Online/Offline	Status	Status Information
ibase1	ISIS		●	monitoring powersupply (2 more...)
ibase2	ISIS		○	

Device Type: Serial Number: Assigned Device Name:

Fig. 183: Selection of the device

In step 3 (see Fig. 183), the malfunctioning device is selected from the available devices and adopted into step 4 by clicking "Continue". The device type, serial number, and device name of the selected device are confirmed in the information area.



Workshop System Management

Call Back: Step 4 of 5

Call Back (Support) - Description

Topic:
Available Software / Dialog message / Occasional problems

Problem Description
error note: local server not available

Actions Taken
server restarted

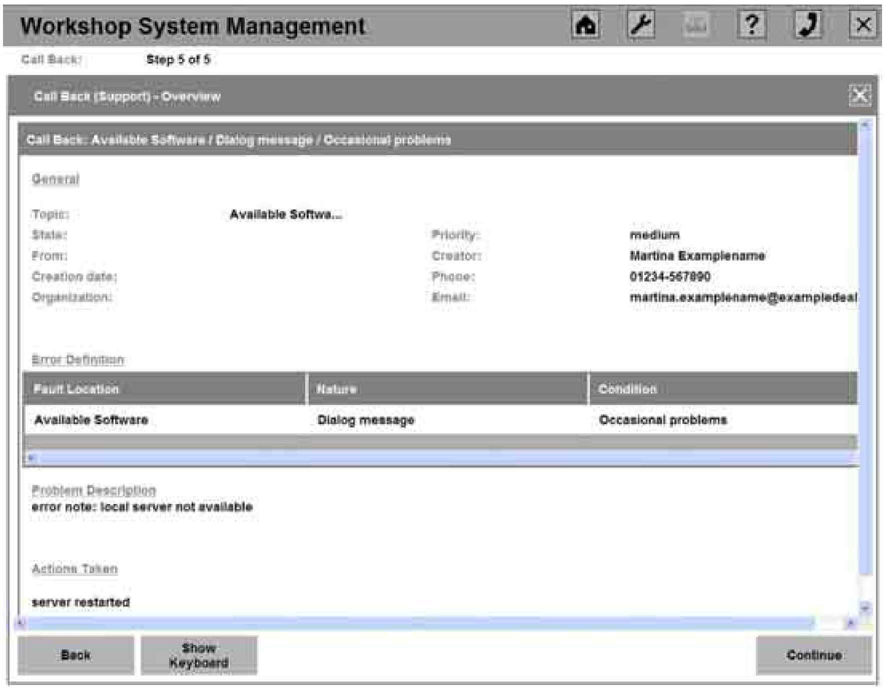
Supposed Cause
no idea

Fig. 184: Input of other information (description)

In step 4, a variety of additional information can be entered to specify the error that has occurred even before the return call comes in. The user must complete the entire dialog box:

- Topic – the already generated error profile is shown here.
- Problem Description – the user explains the problem in the form of key words.
- Actions Taken – the user lists the countermeasures already carried out.
- Suspected Cause – the user - where possible - indicates potential error causes.

Clicking the "Continue" button takes the user to step 5 of the support request. Clicking the "Back" button takes the user to the previous dialog box.



Call Back: Step 5 of 5

Call Back (Support) - Overview

Call Back: Available Software / Dialog message / Occasional problems

General

Topic: Available Softwa...
State:
From:
Creation date:
Organization:
Priority: medium
Creator: Martina Examplename
Phone: 01234-567890
Email: martina.examplename@exampledeal

Error Definition

Fault Location	Nature	Condition
Available Software	Dialog message	Occasional problems

Problem Description
error note: local server not available

Actions Taken

server restarted

Fig. 185: Summary of the callback

In the last step (see Fig. 185), the entries made for the callback are summarized once again.

If you need to re-edit a previous step, click "Back".

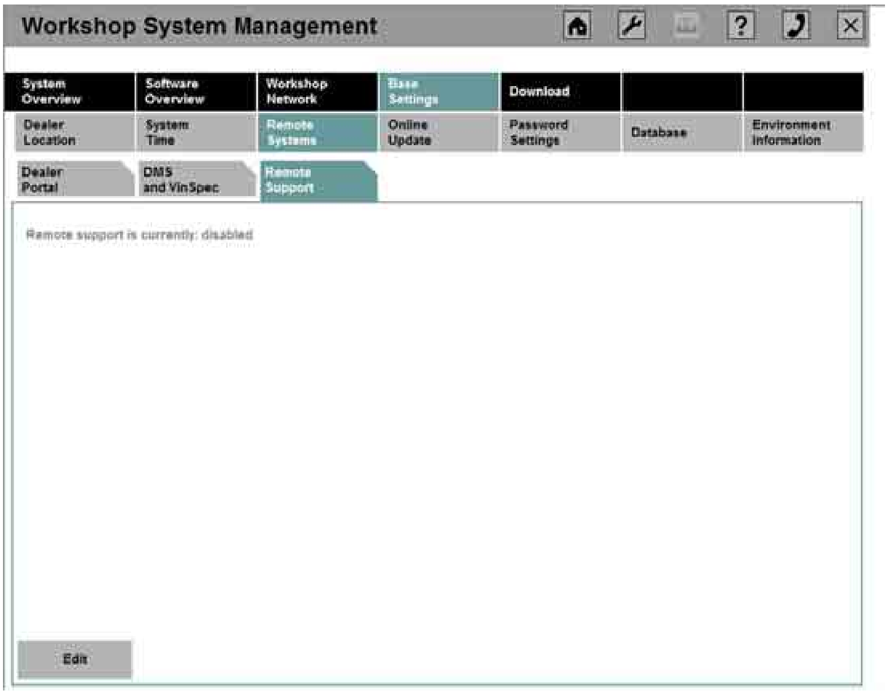
Selecting the "Continue" button confirms all of the entries and sends the callback.

Subsequently, a message appears indicating whether the callback was sent successfully or an error has occurred.

8.6 Enabling remote support

On the ISIS, it is possible to enable access for support (remote support).

Via the WSM, from the ISIS or ISID, open the "Base Settings" menu, then the "Remote Systems" submenu and the "Remote Support" tab. A dialog box opens, displaying the current status (see Fig. 186).



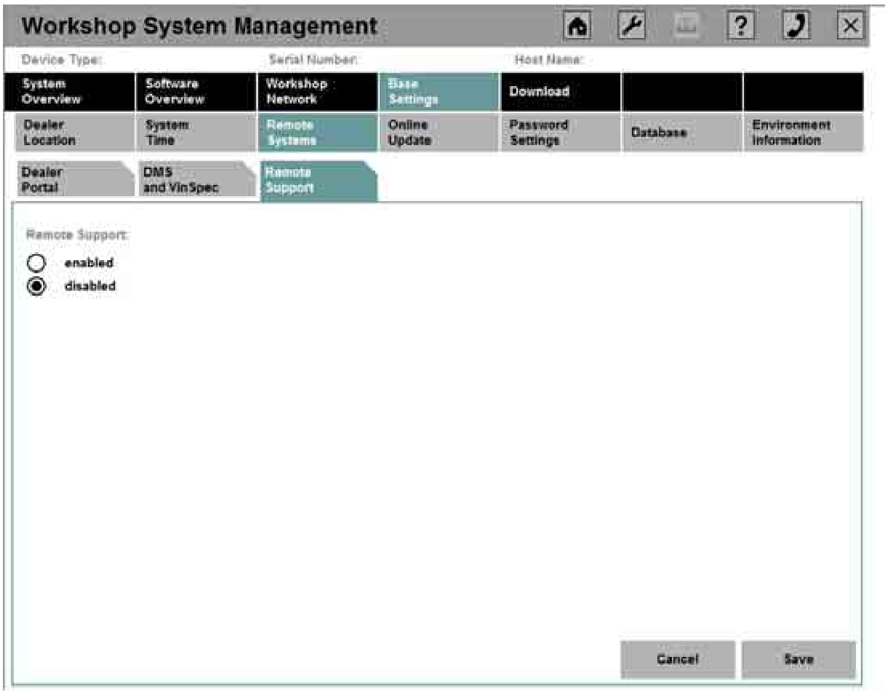
Remote support is currently: disabled

Fig. 186: Display of the remote support

By default, remote support is disabled.
This status can be changed by clicking the "Edit" button (see Fig. 187).

Note:

Enabling remote support permits various accesses to the ISIS (by means of remote desktop connections). Please make sure that you really want to do this.

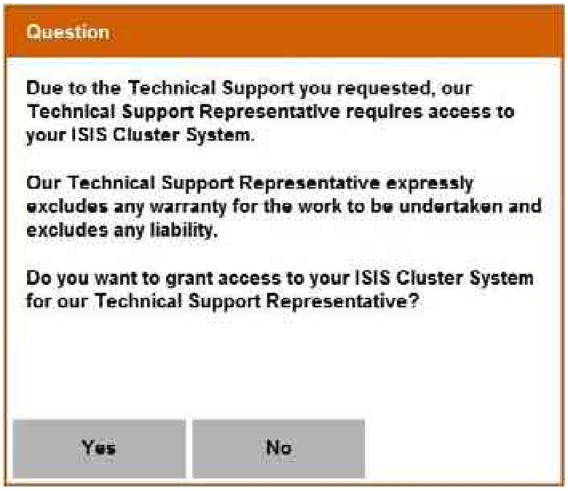


Remote Support:
○ enabled
● disabled

Fig. 187: Editing remote support

The input is adopted by clicking "Save" and rejected by clicking "Cancel".

After you click the "Save" button, a prompt asks whether support access really should be permitted (see Fig. 188). If this prompt is confirmed by clicking "Yes", remote desktop connections to the ISIS can be set up.



Due to the Technical Support you requested, our Technical Support Representative requires access to your ISIS Cluster System.

Our Technical Support Representative expressly excludes any warranty for the work to be undertaken and excludes any liability.

Do you want to grant access to your ISIS Cluster System for our Technical Support Representative?

Fig. 188: Dialog box for the remote enable

8.7 Service phone numbers

Malfunction notifications are generally sent via the callback mechanism of the WSM.

If the WSM is unavailable, worldwide service phone numbers can be used for these emergencies.

The current telephone and fax numbers can be found in the document **"Service addresses for ISIS/ITOOLS – information on the current use of service addresses".**

9 Glossary

BMW AG	**B**ayerische **M**otoren **W**erke AG
Broadcast	A broadcast is a circular message in a computer network, i.e. a message in which data packages are transferred from one point to all participants in a network.
Broadcast domain	A broadcast domain is a logical group of computers in a local network with the feature that a broadcast reaches all domain participants.
Bus	Wired system for the interchange of data and/or energy between potentially more than two participants
Callback	Particular type of BMW support in which requests are sent to the BMW Group via the Internet
CD	**C**ompact **D**isk
Cluster	also ISIS cluster An ISIS system in a subnet, consisting of at least 2 servers.
DHCP	**D**ynamic **H**ost **C**onfiguration **P**rotocol DHCP is used to replace the statically assigned IP addresses with an automatic assignment mechanism, thus reducing errors in the device setup to a minimum.
DMM	**Digital multimeter**
DMS	**D**ealer **M**anagement **S**ystem
DNS	**D**omain **N**ame **S**ystem The main task of the DNS is to convert Internet addresses into the corresponding IP address.
Domain	A domain is a closed, reliable administrative structure.
DVD	**D**igital **V**ersatile **D**isk
ELOS	Deployment guidance and locating system
EPC	**E**lectronic **P**arts **C**atalogue
New generation devices	ISID, ICOM, IMIB and ISAP
Home network	The ISIS network in which a new generation device was first registered
ICC Tool	Among other things, the **I**SIS **C**onnectivity **C**hecker **Tool** checks the usability of IP addresses for the ISIS. It can be found on Servolution and/or is distributed via the Market Community.
ICOM	**I**ntegrated **C**ommunication **O**ptical **M**odule
IP address	**I**nternet-**P**rotocol address (address according to the Internet protocol)
IMIB	**I**ntegrated **M**easurement **I**nterface **B**ox
ISAP	**I**ntegrated **S**ervice **A**ccess **P**oint

ISID	**I**ntegrated **S**ervice **I**nformation **D**isplay
ISIS	**I**ntegrated **S**ervice **I**nformation **S**erver, designation for all the servers in the ISIS rack with the various server plug-in modules
ISIS Cookbook	The ISIS Cookbook provides assistance in preparation of the technical infrastructure and can be found on Servolution and/or is distributed via the Market Community.
ISPA	**I**ntegrated **S**ervice **P**rocesses **A**pplication
ISTA	**I**ntegrated **S**ervice **T**echnical **A**pplication
LAN	**L**ocal **A**rea **N**etwork
LED	**L**ight **E**mitting **D**iode
MAC address	**M**edia **A**ccess **C**ontrol address
Management LAN	A network board in the ISIS for technical support on site at the dealer.
Master	Master refers the ISIS installed first. Indicated by (P) or *
MOST	**M**edia **O**riented **S**ystems **T**ransport Serial bus system to transmit audio and video, voice and data signals
OBD	**O**n-**B**oard **D**iagnosis Diagnosis system integrated into motor vehicles
Offline dealer	Dealers where the workshop network is not connected to the Internet and where, consequently, the ISIS and all new generation devices have been registered offline.
Online dealer	Dealers where the workshop network is connected to the Internet and where, consequently, the ISIS as well as all new generation devices have been registered online.
Slave	The second installed ISIS is referred to as the slave. This is indicated by (S). It adopts its configuration settings from the master.
SLP Service	**S**ervice **L**ocation **P**rotocol **Service -** This local service notifies other devices as to which services are offered by the device.
SSID	**S**ervice **S**et **Id**entifier SSID identifies a radio network based on IEEE 802.11.
UNC	**U**niform **N**aming **C**onvention UNC is the standard when a user wishes to reach enabled resources in a computer network.
USB	**U**niversal **S**erial **B**us
UPS	**Uninterruptible** **P**ower **S**upply
VINSpec	**V**ehicle **I**dentification **N**umber **Spec**ification
VP number	Sales Partner Number
WINS	**W**indows **I**nternet **N**ame **S**ervice WINS is a system for the dynamic resolution of NetBIOS names; works in a manner

	similar to that of DNS and is also dynamic.
WLAN	**W**ireless **LAN**

10 Overview of displayed messages during the ISIS installation

Message	Meaning	Remark
2-regSETREG-1	Start Set Registry Keys	
2-regSETREG-3	Error Set Registry Keys --	
2-regSETREG-2	End Set Registry Keys	
2-ntwRENLAN-1	Start Rename LAN Connections	
2-ntwCHGEXT-1	Start Change External Connection Names	
2-ntwCHGEXT-3	Error Change External Connection Names --	
2-ntwCHGEXT-2	End Change External Connection Names	
2-ntwCHGINT-1	Start Change Internal Connection Names	
2-ntwCHGINT-3	Error Change Internal Connection Names --	
2-ntwCHGINT-2	End Change Internal Connection Names	
2-ntwRENLAN-2	End Rename LAN Connections	
2-ntwCFGIPA-1	Start Configure IP Address Loopback Adapter	
2-ntwCFGIPA-3	Error Configure IP Address Loopback Adapter --	
2-ntwCFGIPA-2	End Configure IP Address Loopback Adapter	
2-vhdINSMOU-1	Start Installation Mounting Tool	
2-vhdCOPVHD-1	Start File copy VHDMount	
2-vhdCOPVHD-3	Error File copy VHDMount --	
2-vhdCOPVHD-2	End File copy VHDMount	
2-vhdINSVHD-1	Start Installation VHD Mount	
2-vhdINSVHD-3	Error Installation VHD Mount --	
2-vhdINSVHD-2	End Installation VHD Mount	
2-vhdINSMOU-2	End Installation Mounting Tool	
2-sfwINSVUD-1	Start Installation Microsoft Updates in Virtual Server	Duration: 40 min
2-vhdINSVSR-1	Start Installation Virtual Server	
2-vhdINSVSR-3	Error Installation Virtual Server --	
2-vhdINSVSR-2	End Installation Virtual Server	
2-sfwINS749-1	Start Installation Update Package MS07-049 KB937986 in Virtual Server	
2-sfwINS749-3	Error Installation Update Package MS07-049 KB937986 in Virtual Server --	

Message	Meaning	Remark
2-sfwINS749-2	End Installation Update Package MS07-049 KB937986 in Virtual Server	
2-sfwINSVUD-2	End Installation Microsoft Updates in Virtual Server	
2-sfwINSVMP-1	Start Installation VMRCplus	
2-sfwINSVMP-3	Error Installation VMRCplus --	
2-sfwINSVMP-2	End Installation VMRCplus	
2-vhdCREVNC-1	Start Create Virtual Networks	
2-vhdCREVNC-3	Error Create Virtual Networks --	
2-vhdCREVNC-2	End Create Virtual Networks	
2-vhdENAVRM-1	Start Enable VMRC	
2-vhdENAVRM-3	Error Enable VMRC --	
2-vhdENAVRM-2	End Enable VMRC	
2-vhdCOPISO-1	Start Copying ISO and VFD File	
2-vhdCOPISO-3	Error copy ISO and VFD File --	
2-vhdCOPISO-2	End Copying ISO and VFD File	
2-regSETTMD-1	Start Set Time Settings including Daylight Savings	
2-regSETTIM-1	Start Set Time Settings	
2-regSETTIM-3	Error Set Time Settings --	
2-regSETTIM-2	End Set Time Settings	
2-regSETDTS-1	Start Set Daylight Savings	
2-regSETDTS-3	Error Set Daylight Savings --	
2-regSETDTS-2	End Set Daylight Savings	
2-regSETTMD-2	End Set Time Settings including Daylight Savings	
2-sfwINSRES-1	Start Installation Remote Support	
2-sfwINSCert-1	Start Installation Remote Support Certificates	
2-sfwINSCert-3	Error Installation Remote Support Certificates --	
2-sfwINSCert-2	End Installation Remote Support Certificates	
2-sfwINSCli-1	Start Installation IAG Client	
2-sfwINSCli-3	Error Installation IAG Client --	
2-sfwINSCli-2	End Installation IAG Client	
2-sfwCOPIAG-1	Copy IAG Hosts File	
2-sfwCOPIAG-3	Error Copy IAG Hosts File --	
2-sfwCOPIAG-2	End Copy IAG Hosts File	

Message	Meaning	Remark
2-sfwDELCRT-1	Start Delete Old Certificates	
2-sfwDELCRT-3	Error Delete Old Certificates --	
2-sfwDELCRT-2	End Delete Old Certificates	
2-sfwINSRES-2	End Installation Remote Support	
2-regSETSCP-1	Start Set Script Links	
2-regSETSCP-3	Error Set Script Links --	
2-regSETSCP-2	End Set Script Links	
2-ntwCFGDHC-1	Start Configure DHCP Service	
2-ntwCFGDHC-3	Error Configure DHCP Service --	
2-ntwCFGDHC-2	End Configure DHCP Service	
2-sysDELPOS-1	Start Delete POSIX subsystem	
2-sysDELPOS-3	Error Delete POSIX subsystem --	
2-sysDELPOS-2	End Delete POSIX subsystem	
2-secINSTPL-1	Start Installation Security Template, Set Registry & ACLs	
2-secCHGGUI-1	Start Change GUID in XML	
2-secCHGGUI-3	Error Change GUID in XML --	
2-secCHGGUI-2	End Change GUID in XML	
2-secSETTPL-1	Start Installation SecurityTemplate	
2-secSETTPL-3	Error Installation Security Template --	
2-secSETTPL-2	End Installation Security Template	
2-secCOPSCW-1	Start Copy SCW LogFile	
2-secCOPSCW-3	Error Copy SCW LogFile --	
2-secCOPSCW-2	End Copy SCW LogFile	
2-secFSCSCD-1	Start Security Settings in Registry for Host	
2-secSETREG-3	Error Security Settings in Registry for Host--	
2-secSETREG-2	Start Security Settings in Registry for Host	
2-secSETSAC-1	Start Set Security ACLs	
2-secSETSAC-3	Error Set Security ACLs --	
2-secSETSAC-2	End Set Security ACLs	
2-secINSTPL-2	End Installation Security Template, Set Registry & ACLs	
2-sfwINSCRB-1	Start Installation and Configuration Remote Boot Server	
2-sfwINSRBS-1	Start Installation Remote Boot Server	
2-sfwINSRBS-3	Error Installation Remote Boot Server --	

Message	Meaning	Remark
2-sfwINSRBS-2	End Installation Remote Boot Server	
2-sfwCOPRBS-1	Start Copy Remote Boot Server Files	
2-sfwCOPRBS-3	Error Copy Remote Boot Server Files--	
2-sfwCOPRBS-2	End Copy Remote Boot Server Files	
2-sfwCFGRBS-1	Start Configuration Remote Boot Server	
2-sfwCFGRBS-3	Error Configuration Remote Boot Server --	
2-rsfwCFGRBS-2	End Configuration Remote Boot Server	
2-sfwINSCRB-2	End Installation and Configuration Remote Boot Server	
2-sfwINSKIW-1	Start Installation KIWI Syslog	
2-sfwINSKII-1	Start Installation KIWI Syslog Daemon	
2-sfwINSKII-3	Error Installation KIWI Syslog --	
2-sfwINSKII-2	End Installation KIWI Syslog	
2-sfwINSKIC-1	Start Copy LoadNewSetting File and Remove Shortcut	
2-sfwINSKIC-3	Error copy LoadNewSetting File and Remove Shortcut --	
2-sfwINSKIC-2	End Copy LoadNewSetting File and Remove Shortcut	
2-sfwINSKIW-2	End Installation KIWI Syslog	
2-sfwINSFR-1	Start Install FreeRadius	
2-sfwINSFR-3	Error Installation FreeRadius --	
2-sfwINSFR-2	End Installation FreeRadius	
2-sfwINSPDF-1	Start Installation FreePDF	
2-sfwINSPDF-3	Error Installation FreePDF--	
2-sfwINSPDF-2	End Installation FreePDF	
2-oraINSSRV-1	Start Installation Oracle Server & Patches	
2-oraINSORA-1	Start Installation Oracle Server	
2-oraINSORA-3	Error Installation Oracle Server --	
2-oraINSORA-2	End Installation Oracle Server	
2-oraINSPAT-1	Start Installation Oracle Patches	
2-oraINSPAT-3	Error Installation Oracle Patches --	
2-oraINSPAT-2	End Installation Oracle Patches	
2-oraCREDBA-1	Start Create Databases	
2-oraCREDBA-3	Error Create Databases --	
2-oraCREDBA-2	End Create Databases	
2-oraINSPA2-1	Start Installation Oracle Patches	

Message	Meaning	Remark
2-oraINSPA2-3	Error Installation Oracle Patches --	
2-oraINSPA2-2	End Installation Oracle Patches	
2-oraINSSRV-2	End Installation Oracle Server & Patches	
2-sfwINSWSM-1	Start Installation WSM Manager	
2-sfwINSWSM-3	Error Installation WSM Manager --	
2-sfwINSWSM-2	End Installation WSM Manager	
2-sfwCOPLAN-1	Start Copy ISIS Launcher	
2-sfwCOPLAN-3	Error Copy ISIS Launcher --	
2-sfwCOPLAN-2	End Copy ISIS Launcher	
2-sfwINSIVM-1	Start Installation IVM Manager	
2-sfwINSIVM-3	Error Installation IVM Manager --	
2-sfwINSIVM-2	End Installation IVM Manager	
2-sfwINSJET-1	Start Installation JetStream	
2-sfwINSJLO-1	Start Installation JetStream Localserver	
2-sfwINSJLO-3	Error Installation JetStream Localserver --	
2-sfwINSJLO-2	End Installation JetStream Localserver	
2-sfwINSJFC-1	Start Installation JetStream CallbackFaultCatalog	
2-sfwINSJFC-3	Error Installation JetStream CallbackFaultCatalog --	
2-sfwINSJFC-2	End Installation JetStream CallbackFaultCatalog	
2-sfwINSJINS-1	Start Installation JetStream Installer	
2-sfwINSJINS-3	Error Installation JetStream Installer --	
2-sfwINSJINS-2	End Installation JetStream Installer	
2-sfwINSAUF-1	Start Installation Authentication Frontend	
2-sfwINSAUF-3	Error Installation Authentication Frontend --	
2-sfwINSAUF-2	End Installation Authentication Frontend	
2-sfwINSAFC-1	Start Installation Authentication Frontend Config	
2-sfwINSAFC-3	Error Installation Authentication Frontend Config --	
2-sfwINSAFC-2	End Installation Authentication Frontend Config	
2-sfwCOPJFP-1	Start Copy JetStream Fingerprints	
2-sfwCOPJFP-3	Error Copy JetStream Fingerprints --	
2-sfwCOPJFP-2	End Copy JetStream Fingerprints	
2-sfwINSJET-2	End Installation JetStream	
2-sfwINSSCO-1	Start Installation SCore Broker	

Message	Meaning	Remark
2-sfwINSSCO-3	Error Installation SCore Broker --	
2-sfwINSSCO-2	End Installation SCore Broker	
2-secINSSEC-1	Start Installation Final Security Template	
2-secINSSEC-3	Error Installation Security Template --	
2-secINSSEC-2	End Installation Security Template	
2-ntwCFGWSM-1	Start Configure WSM Services	
2-ntwCFGWMM-1	Start Configure WSM Manager Service	
2-ntwCFGWMM-3	Error Configure WSM Manager Services --	
2-ntwCFGWMM-2	End Configure Services	
2-ntwCFGWMA-1	Start Configure WSM Agent Service	
2-ntwCFGWMA-3	Error Configure WSM Agent Service --	
2-ntwCFGWMA-2	End Configure WSM Agent Service	
2-ntwCFGWMS-1	Start Configure WSM SLP Service	
2-ntwCFGWMS-3	Error Configure WSM SLP Service --	
2-ntwCFGWMS-2	End Configure WSM SLP Service	
2-ntwCFGWSM-2	End Configure WSM Services	
2-sfwINSUPD-1	Start Installation Microsoft Updates	
2-sfwINSMRT-1	Start Installation Malware Removal Tool	
2-sfwINSMRT-3	Error Installation Malware Removal Tool --	
2-sfwINSMRT-2	End Installation Malware Removal Tool	
2-sfwINS742-1	Start Installation Update Package MS07-042 KB936181	
2-sfwINS742-3	Error Installation Update Package MS07-042 KB936181 --	
2-sfwINS742-2	End Installation Update Package MS07-042 KB936181	
2-sfwINS779-1	Start Installation Update Package MS07-042 KB933579	
2-sfwINS779-3	Error Installation Update Package MS07-042 KB933579 --	
2-sfwINS779-2	End Installation Update Package MS07-042 KB933579	
2-sfwINS678-1	Start Installation Update Package MS06-078 KB925398-v2	
2-sfwINS678-3	Error Installation Update Package MS06-078 KB925398-v2 --	
2-sfwINS678-2	End Installation Update Package MS06-078 KB925398-v2	
2-sfwINSUPD-2	End Installation Microsoft Updates	
2-hskCOPLOG-1	Start Copy Log Files	
2-hskCOPLOG-3	Error Copy Log files --	
2-hskCOPLOG-2	End Copy Log files	

Message	Meaning	Remark
2-hskDELAFF-1	Start Delete AfterSetup Files and Folders	
2-hskDELFLC-1	Start Delete Folders	
2-hskDELFLC-3	Error Delete Folders --	
2-hskDELFLC-3	End Delete Folders	
2-hskDELVBS-1	Start Delete AfterSetup Files	
2-hskDELVBS-3	Error Delete AfterSetup Files --	
2-hskDELVBS-2	End Delete AfterSetup Files	
2-hskDELAFF-2	End Delete AfterSetup Files and Folders	
2-sysLOG2ND-2	Script finished - Reboot will be initiated	
	--- Reboot ---	
	Part WSM	
	--- Shutdown ---	

11 List of illustrations