Wx002-, WIx040-, WIx065-Series

Release Notes

System Software 7.6.1

Version 1.0

Purpose

This document describes new features, changes, and solved problems of **System Software 7.6.1.**

Liability

While every effort has been made to ensure the accuracy of all information in this manual, Funkwerk Enterprise Communications GmbH cannot assume liability to any party for any loss or damage caused by errors or omissions or by statements of any kind in this document and is only liable within the scope of its terms of sale and delivery.

The information in this manual is subject to change without notice. Additional information and changes can be found at www.funkwerk-ec.com.

As multiprotocol gateways, Bintec gateways set up WAN connections in accordance with the system configuration. To prevent unintentional charges accumulating, the operation of the product should be carefully monitored. Funkwerk Enterprise Communications GmbH accepts no liability for loss of data, unintentional connection costs and damages resulting from unsupervised operation of the product.

Trademarks

Bintec and the Bintec logo are registered trademarks of Funkwerk Enterprise Communications GmbH.

Other product names and trademarks mentioned are usually the property of the respective companies and manufacturers.

Copyright

Guidelines and standards

Bintec gateways comply with the following guidelines and standards:

R&TTE Directive 1999/5/EG

CE marking for all EU countries and Switzerland

You will find detailed information in the Declarations of Conformity at www.funkwerk-ec.com.

How to reach Funkwerk Enterprise Communications GmbH

Funkwerk Enterprise Communications GmbH Suedwestpark 94 D-90449 Nuremberg Germany Telephone: +49 180 300 9191 0 Fax: +49 180 300 9193 0 Internet: www.funkwerk-ec.com	Funkwerk Enterprise Communications 6 Avenue de la Grande Lande - CS 20102 33173 Gradignan cedex France Telephone: +33 (0)1 61 37 32 76 Fax: +33 (0)1 61 38 15 51 Internet: www.funkwerk-ec.com

1 Important Information

Please read the following information about System software 7.6.1 carefully to avoid problems when updating or using the software.

1.1 Applicability

System software 7.6.1 is available only for the following devices and cannot be used on other devices:

- **W1002**
- **W2002**
- **WI1040**
- **WI2040**
- **WI3040**
- **WI1065**
- **WI2065**
- **WI3065**

Note

Please note that new features, changes or the solution of a problem are only available on your device if the menu described is shown.

1.2 Update

In the **W1002** and **W2002** devices, where you run them with ACE, from **System software 7.6.1**, the operating system is changed to BOSS. Devices in the **WI** series are already shipped with the BOSS operating system.

Configurations set up or saved with **System software 7.6.1** are therefore incompatible with earlier versions of our System software that were set up under ACE.

Note

Note that, during an update, the configuration of your device will be lost.

The following table gives an overview of the available updates and update-mechanisms:

Device	Software currently run	New software	Mechanism
Wx002	ACE	7.6.1 Downgrade to ACE possible	**ComPoint Manager** and FCI or console
	7.5.1	7.6.1 Downgrade to ACE possible	Console or FCI
WIx040	7.5.1	7.6.1 Downgrade to ACE not possible	Console or FCI
WIx060	7.5.1	7.6.1 Downgrade to ACE not possible	Console or FCI

1.2.1 Preparation and update (W1002 and W2002)

When updating to System software 7.6.1, the operating system is, where appropriate, automatically changed from ACE to BOSS.

Note

If you already run **System software 7.5.1** on your device, proceed with your update as described for devices in the **WI** series (see “Preparation and update (WI series)” on page 14).

Carry out the update as follows:

Update preparation

1. For the update you will need, for the device **W1002**, the file *W1002_boss_s7601b01,afw* or, for the device **W2002**, the file *W2002_boss_s7601b01,afw* (the beta number (...*b01*) may be different).
   In addition, you will need the file W1002_Blup_LED_SCHEME.w1p or W2002_Blup_LED_SCHEME.w2p, as appropriate, to enable the LEDs of the device following the update.
   Ensure that the program **ComPoint Manager** from Artem and the files that you need for the update are available on your PC.
   If the program and/or the two files are not available on your PC, enter www.funkwerk-ec.com in your browser.
   The Funkwerk homepage will open. In the download-area for your device you will find the required program and files.
2. Install the program on your computer.
   Alternatively, you can load the program from the CD-ROM delivered with your access point.
3. Save the two files on your PC.
4. Ensure that the access point on which you wish to make the update is in the same network as the PC on which the **ComPoint Manager** program is installed.
5. Start the **ComPoint Manager**.
   The **ComPoint Manager** discovers the access points installed on the network and shows them as a list in its main window.
6. If the device on which you wish to make the update does not yet have an IP address, assign it an IP address in your network in the **ComPoint Manager** under ***CONFIGURATION*** ➜ ***IP SETTINGS***.
7. In the window that follows, enter the password for the user Admin if this has not been entered in the **ComPoint Manager** under ***TOOLS*** ➜ ***PASSWORD***.

Boot configuration backup

Back up the current boot configuration for any later downgrade. Proceed as follows:

1. In the **ComPoint Manager**, select in the list the device for which you wish to backup the boot configuration.
2. In the **ComPoint Manager**, select ***Configuration*** ➜ ***Save configuration***.
3. If asked to do so, enter the password.
   The ***Save as*** window will open.
4. Select the desired folder, the filename can remain unchanged. Click on **Save**.
   You will see the message "Device configuration successfully saved."
5. Confirm with **OK**.
   The configuration will now be found in the selected folder.

Carrying out the update

Carry out the update as a firmware upgrade with the **ComPoint Manager**.

Attention!

The result of interrupted updating operations could be that your access point no longer boots. Do not turn your access point off during the update!

1. In the main window of the **ComPoint Managers**, click on the device in the list for which you wish to carry out the update.
2. Select ***Configuration*** ➜ ***Load firmware***.
3. Click on **Select software**.
4. Click on **Browse**, select the folder containing the files and click on **OK**.
   The desired file(s) will be shown.
5. Depending on the device, select the desired firmware, i.e. *W1002_boss_s7601b01,afw* for **W1002** or *W2002_boss_s7601b01,afw* for **W2002**, click on **OK** and then click on **Upload firmware**.
   The **ComPoint Manager** will check whether the selected firmware is suitable for the device and, if so, upload it.

In accordance with the BOSS-standard, the serial interface will automatically be set to Baudrate 9600, 8-bit data, no parity, 1 stop bit, no handshake.
You will see the message "Reboot to activate newly loaded firmware."

6. Select the option "Reboot now (recommended)" and click on **OK**.
   The device will reboot.

Note

The device will reboot with the new software and the default-IP address *192.168.0.252* but with no configuration. The LEDs will not be enabled.

After the update from ACE to BOSS, you can use only the following functions of the **ComPoint Manager**:

- *Discovery Server*
- *IP configuration*

Under BOSS, all other configuration options are accessed with the **Funkwerk Configuration Interface**.

Enabling the LEDs

To enable operation of the LEDs, you must upload the file W1002_Blup_LED_SCHEME.w1p or W2002_Blup_LED_SCHEME.w2p, according to the device.

1. Ensure that your PC is on the same network as the access point on which you wish to enable the LEDs. If necessary, assign a suitable second IP address to your PC in the network settings.
2. Enter the default-IP address of your device *192.168.0.252* in a browser.
   The browser window will open.
3. Log into your device with the username *admin* and the password *funkwerk* and click on **Login**.
   The Status-page of the **Funkwerk Configuration Interface** will open.
4. Make sure that the language setting is *English*.
5. Click on ***MAINTENANCE*** ➜ ***SOFTWARE UPDATE***.
6. In the ***UPDATE MECHANISM*** field, select the value *Local file* and click on the **Browse** button.
7. Click on the desired filename, e.g. *W1002_Blup_LED_SCHEME.w1p* and then on **Open**.

8. Now click on **Go**.
   The message "Router Maintenance. Please stand by. Operation in progress." shows that the selected file is being uploaded to the device. When the upload procedure is finished, you will see the message "Router maintenance. Success. Operation completed successfully. The router must be restarted."
9. Click on **Reboot**.
   The device will start with the LEDs lit. The browser window will open.

You can log into your device and configure it.

Downgrade

In the event of a downgrade, the operating system is automatically changed from BOSS to ACE.

For this procedure, you will need, according to the device, the file *W1002_ace_6_15,w1p* or *W2002_ace_6_15,w2p,* which you will find under www.funkwerk-ec.com (see “Update preparation” on page 9).

Note

Note that, during a downgrade, the configuration of your device will be lost. After a downgrade, you will only be able to use the configuration that you backed up before the update.

Attention!

The result of interrupted downgrade operations could be that your access point no longer boots. Do not turn your access point off during the downgrade!

Downgrading

If you wish to carry out a downgrade from **System software 7.6.1**, proceed as follows:

1. Enter the IP address of your device in a browser.
   The browser window will open.
2. Log into your device with your username and password and click on **Login**.
3. Make sure that the language setting is *English*.
4. Click on ***Maintenance*** ➜ ***Software update***.

5. In the ***UPDATE MECHANISM*** field, select the value *Local file* and click on the **Browse** button.
6. Click on the desired filename, e.g. *W1002_ace_6_15,w1p* and then on **Open**.
7. Click on **Go**.
   The process will take a few minutes, during which you will see the message "Router maintenance. Please stand by. Operation in progress." The message "Router-Maintenance. Success. Operation completed successfully. The router must be restarted" shows that the upload process has finished.
8. Click on **Reboot**.
   This can take a few minutes. The device will start with the Status LED showing green.

Note

With the **ComPoint Manager**, you can discover the access point. The device can no longer be reached with the browser.

Configuration upload

After the downgrade to ACE, you can upload to your device the configuration that you hopefully backed up before the update to BOSS.

1. Start the **ComPoint Manager**.
   The **ComPoint Manager** will open. It discovers the access points installed on the network and shows them as a list in its main window.
2. In the **ComPoint Manager**, under ***CONFIGURATION*** ➜ ***IP SETTINGS*** assign an IP address in your network range to your device.
3. In the list, select the device to which you wish to upload the backup configuration.
4. In the **ComPoint Manager**, select ***CONFIGURATION*** ➜ ***UPLOAD CONFIGURATION***.
5. When asked, enter the password for the user Admin.
   The window ***OPEN...*** will open.
6. Select the desired file. Click on **Open**.
   You will see the message "Upload configuration (version *x.xx*) to the device (version *x.xx*) and reboot?"

7. If the two version numbers are the same, proceed with these settings with **Yes**.
   The configuration will be uploaded to the device.
   You will see the message "Configuration successfully uploaded."
8. Click on **OK**.
   You can use the configuration in your device.

1.2.2 Preparation and update (WI series)

Devices in the WI series are already shipped with System software 7.5.1 so that configuration and maintenance via the Funkwerk Configuration Interface is available, making it simple to update the software. This makes an update possible in two ways.

Update preparation

1. For the update, you will need, for devices of the **WI** series, the file *bl7601b04,iny* (the beta number (...*b04*...) may be different).
   Ensure that the program **ComPoint Manager** from Artem and the file that you need for the update are available on your PC.
   If the program and/or the file are not available on your PC, enter www.funkwerk-ec.com in your browser.
   The Funkwerk homepage will open. In the download-area for your device you will find the required program and files.
2. Install the program on your computer.
   Alternatively, you can load the program from the CD-ROM delivered with your access point.
3. Save the two files on your PC.
4. Ensure that the access point on which you wish to make the update is in the same network as the PC on which the **ComPoint Manager** program is installed.
5. Start the **ComPoint Manager**.
   The **ComPoint Manager** discovers the access points installed on the network and shows them as a list in its main window.
6. If the device on which you wish to make the update does not yet have an IP address, assign it an IP address in your network in the **ComPoint Manager** under ***CONFIGURATION*** ➜ ***IP SETTINGS***.

7. In the window that follows, enter the password for the user Admin if this has not been entered in the **ComPoint Manager** under ***Tools*** ➜ ***Password***.


Note

You can now use the following functions of the **ComPoint Manager**:

- *Discovery Server*
- *IP configuration*

Under BOSS, all other configuration options are accessed with the **Funkwerk Configuration Interface**.

Update via the Funkwerk Configuration Interface

The simplest way to carry out an update is via the **Funkwerk Configuration Interface**, using the ***Maintenance*** ➜ ***Software & Configuration*** menu.

If you wish to carry out an update, proceed as follows:

1. Backup the current boot configuration using the ***Maintenance*** ➜ ***Software & Configuration*** menu:
   a) Under ***Action***, select *Export Configuration*.
   b) Leave all other settings and click on the **Go** button.
   c) To save the file on your PC, follow the instructions in your browser.
2. Stay in the ***Maintenance*** ➜ ***Software & configuration*** menu.
3. In the ***Action*** field, select *Update System Software*.
4. As ***Source*** for the update, select *Current software from Funkwerk server*. The system file is on the official funkwerk update server.
5. Click on the **Go** button. Your request will be processed.
   The process takes a few minutes. The message "System maintenance. Success. Operation completed successfully. The system must be restarted" shows that the process has finished.
6. Click on **Reboot**.
   The device will start; you can log into your device.

Other possibilities for carrying out the update:

1. As ***Source*** for the update, select *Local file* (default value). The system file is stored locally on your PC. For the update, you need, for devices of the **WI** series, the file *INY\Blup\bl7601b04,iny*, which you will find under www.funkwerk-ec.com.

2. Enter the path and name of the file or select the file with **Browse...** via the explorer/finder.
3. Click on the **Go** button. Your request will be processed.
   The process takes a few minutes. The message "System maintenance. Success. Operation completed successfully. The system must be restarted" shows that the process has finished.
4. When the process is finished, click on **Reboot**.
   The device will start and you can log into your device.

Alternatively, under ***SOURCE***, you can select *HTTP server*. You enter the ***URL*** of the update server from which the software file is loaded here.

Update via the command line

To prepare and carry out an update to **System software 7.6.1**, proceed as follows:

1. Backup the current boot configuration. Use one of the following possibilities:
   a) In the SNMP shell, enter `cmd=save path=boot.alt`. This backs up the current boot configuration in the flash ROM of your access point under the name "boot.alt".
   b) On a computer on your LAN, start a TFTP server and export the current boot configuration using the ***CONFIGURATION MANAGEMENT*** menu of the Setup tool. To do this, select:
   - ***OPERATION*** = *put (FLASH -> TFTP)*
   - ***TFTP SERVER IP ADDRESS*** = *<IP-address of the TFTP servers on the LAN>*
   - ***TFTP FILE NAME*** = *boot.alt*
   - ***NAME IN FLASH*** = *boot*
2. Carry out the update to **System software 7.6.1** with the BLUP (Bintec Large Update) named above to update all necessary modules.
   The update using the BLUP runs as follows:

```
wi3040:> update <IP address of the TFTP server>
/INY/Blup/bl7601b04,iny
Starting TFTP File Transfer ....................................
..................... (139320+4887788 Bytes)
List of files in this update (len 4887788):
  Version    Length  Name
7.6.1.400   4048577  Boss
7.6.1.400    774792  webpages.ez
7.6.1.400    182462  text_ger.ez

*** Don't power-off while the update takes place ***

Perform update (y or n)?
```

Here, the software modules contained in the BLUP are listed:

- BOSS - the operating system itself
- webpages.ez - the HTML configuration interface
- text_ger.ez - the German localisation of the HTML interface.

If you confirm with *y*, all those elements are updated that are newer in the BLUP than on your access point. When updating to **System software 7.6.1** this will, as a rule, be all three modules.

The update then takes place for all modules concerned:

```
Updating Boss
Erasing Flash ROM
.............................................................OK
Writing Flash ROM
.............................................................OK
Verifying Flash ROM
.............................................................OK

Software update successfully finished

Updating webpages.ez

Perform Flash ROM update
Update Flash ROM ............ OK
Verify Flash ROM ............ OK

File update successfully finished

Updating text_ger.ez

Perform Flash ROM update
Update Flash ROM . OK
Verify Flash ROM . OK

File update successfully finished

Rebooting... (y or n) [n] ?
```

After the reboot, you have the new software version available. You can access it using a supported Web browser under the IP address of the access point. If you have deleted the boot configuration, the access point will again have the default address *192.168.0.252*.

Downgrade If you wish to carry out a downgrade, proceed as follows:

1. Replace the current boot configuration with the previous backup version. Use one of the following possibilities:
   a) In the SNMP shell, enter `cmd=move path=boot.alt pathnew=boot`. This overwrites the current boot configuration with the previous backup version. The configuration named "boot.alt" is thereby deleted from the flash ROM (if you want to keep this in the flash, use `cmd=copy` instead of `cmd=move`).
   b) On a computer on your LAN, start a TFTP server and import the current boot configuration using the ***CONFIGURATION MANAGEMENT*** menu of the Setup tool. To do this, select:
   - ***OPERATION*** = get (TFTP -> FLASH)
   - ***TFTP SERVER IP ADDRESS*** = *<IP-address of the TFTP servers on the LAN>*
   - ***TFTP FILE NAME*** = *boot.alt*
   - ***NAME IN FLASH*** = *boot*
2. Carry out the downgrade to the desired software version.
3. Reboot the access point. The device will start with the previously backed up boot configuration and the old version of the system software.

2 New Features

System software 7.6.1 includes a number of new functions that significantly extend the performance compared with System software 7.5.1:

2.1 SFP Slot Support

The devices **funkwerk WI1040**, **WI2040**, **WI3040**, **WI1065**, **WI2065** and **WI3065** have a slot for a fiber optic module, also known as an SFP-module (from the "SFP-MSA" standard - Small Form Factor Pluggable Multi-Sourcing Agreement). This slot can accommodate modules operating at 100 Mbit/s, full duplex. Gigabit modules are not supported.

An inserted SFP module is automatically recognized and enabled during the boot up process. You can insert the module in the running device (hot-pluggable), it will not, however, be enabled until the next reboot.

The recognition procedure also checks the module for operability.

In the event of a fault, you will see the following message in the console:
SFP module not suitable for device, disabling SFP support
The manufacturer and type number are also shown.

Funkwerk Configuration Interface

The SFP module is configured like any other Ethernet Interface.

You will find the Ethernet interface configuration in the **Funkwerk Configuration Interface** under ***PHYSICAL INTERFACES*** ➜ ***ETHERNET PORTS***

Attention!

Either of the two Ethernet ports, *en1-0* or *en1-1*, can be freely assigned as SFP port and is this bound to it by switch.

2.2 Simple Network Time Protocol server

System software 7.6.1 supports the SNTP server function.

Previously, time requests sent by a client to the access point remained unanswered. With the SNTP server function, the access point has an internal time server and can send an answer to such client requests (time settings and other options).

Funkwerk Configuration Interface

You can configure the SNTP server function via the **Funkwerk Configuration Interface**, in the ***System management*** ➜ ***Global settings*** ➜ ***Date and time*** menu, in the ***Internal Time Server*** field.

Parameter	Value
Internal Time Server	Select whether the internal time server is to be used. The function is activated with *Enabled*. Time requests from a client will be answered with the current system time. This is given as GMT, without offset. The default state of the function is Disabled. Time requests from a client are not answered. This is the same behavior as in previous software versions.

Table 2-1: Additional field in the ***System management*** ➜ ***Global settings*** ➜ ***Date and time*** menu

2.3 Temperature measurement

The devices **funkwerk WI1040**, **WI2040**, **WI3040**, **WI1065**, **WI2065** and **WI3065** are fitted with a temperature sensor. This is located on the main board, under the first WLAN card.

Function

The sensor measures the current temperature. Its measurement range is from -55 to +125 °C with an accuracy of less than 1 °C.

In addition, the minimum and maximum temperatures reached are shown, together with the times at which they were reached. On rebooting the device, these values are cleared and refilled.

By default, lower and upper limits are set for the temperature; overstepping these sets an alert-variable and generates a syslog-message. The values are updated every 10 seconds.

Funkwerk Configuration Interface

The current, minimum and maximum temperatures are shown in the **Funkwerk Configuration Interface**, in the ***System management*** ➜ ***Status*** menu, in the ***Temperature*** field.

You can configure the temperature limits in the **Funkwerk Configuration Interface**, in the ***Local services*** ➜ ***Surveillance*** ➜ ***Temperature*** menu. You can link the overstepping of a limit value with an action.

You can edit the existing values or click on the **New** button and configure new limit values and actions.

The menu contains the following fields:

Parameter	Value
Trigger	Enter here the temperature limit value (min/max). Possible values: ■ *Temperature above* ■ *Temperature below*

Parameter	Value
Action	Select the desired action. Possible values: ■ *Enable* (default value) ■ *Deactivating*
Interface	Select the interface via which the action is to be carried out. Possible values: ■ *Relay* (default value): The overstepping of the limit is coupled with the relay (see also “Alarm relay” on page 22). ■ <*Interface*>: On overstepping the temperature limit, the selected interface is turned off.

Table 2-2: Fields in the ***LOCAL SERVICES*** ➜ ***SURVEILLANCE*** ➜ ***TEMPERATURE*** ➜ ***NEW*** menu

2.4 Alarm relay

The devices **funkwerk WI1040**, **WI2040**, **WI3040**, **WI1065**, **WI2065** and **WI3065** are fitted with a relay. The rest (i.e. normal/unexcited/fault) state of the contacts is open.

Function You can choose whether the relay is manually controlled or used as an alarm relay, coupled with the red error LED. When manually controlled, the state of the relay is set during booting when the configuration is loaded.

Funkwerk Configuration Interface The relay is configured in the **Funkwerk Configuration Interface** under ***PHYSICAL INTERFACES*** ➜ ***RELAY*** ➜ ***RELAY CONFIGURATION***.

The menu contains the following fields:

Parameter	Value
Port mode	Possible values: ■ *Off* (default value): The relay is manually set to always open. ■ *On*: The relay is manually set to always closed. ■ *Alarm relay*: The relay is automatically coupled with the red error LED.

Table 2-3: Field in the ***PHYSICAL INTERFACES*** ➜ ***RELAY*** menu

2.5 WLAN - encryption possibilities extended

In System software 7.6.1, the encryption possibilities have been extended. The *WPA MODE* *WPA and WPA 2* is now available with AES or TKIP encryption or with both encryption methods.

2.6 Update command extended

In System software 7.6.1, the update command has an additional -q option to define the inactive mode in the scheduler without outputing the Syslog messages.

3 Changes

The following changes have been made in our system software to improve its performance and usability:

3.1 Setup Tool - WAN - Delay after Connection Failure

Formerly, in the *WAN Partner* ➜ ADD ➜ *Advanced Settings* menu, the *Delay after Connection Failure (sec)* = *300* field was set by default. From System software 7.6.1 BETA 5, this field is set depending on the *Layer 1 Protocol* field. For *Layer 1 Protocol* = *PPP over Ethernet (PPPoE)*, *PPP over PPTP*, *PPP over L2TP (LNS mode)*, *PPP over L2TP (LAC mode)* **or** *PPP over ATM (PPPoA)*, ***Delay after Connection Failure (sec)*** = *60* **by default. For all other values, *Delay after Connection Failure (sec)*** = *300* **as previously.**

3.2 External IP address

In the *Routing* ➜ *NAT* ➜ *Port Forwarding* menu, the designation of the *IP Address* field has been changed to *External IP Address*.

3.3 Headings and String IDs

Colons have been removed from headings For *E-Mail Notification Server* and *E-Mail Notification Recipient*, String IDs were added for the translation process.

3.4 Standard interfaces

In the *System Administration* ➜ *Administrative Access* ➜ *Access* menu, it is no longer possible to delete standard interfaces, i.e. those interfaces that were not set up via the Add button will always be shown.

4 Problems solved

Not all devices listed in chapter “Important Information” on page 7 were affected by the following problems. If your device does not have the menu of proerty in question, you can ignore the problem mentioned.

The following problems have been solved in System software 7.6.1:

4.1 Stacktrace in raw mode

(ID n/a)

In raw mode, pressing the tab key resulted in a stacktrace.

The problem has been solved.

4.2 Stacktrace with memory problems

(ID 8856)

The growth of the MIB table, ***apDiscSetTable***, was unlimited. This could lead to a full memory and stacktrace.

The problem has been solved.

4.3 Stacktrace during XMODEM transfer

(ID 9322)

In a timeout of an XMODEM transfer (e.g. when backing up the configuration), a stacktrace could be performed without panic and without a reboot.

The problem has been solved.

4.4 Panic and stacktrace when ACL mode enabled

(ID 8776)

Enabling ACL mode caused panic and a stacktrace.

The problem has been solved.

4.5 Incorrect display of the start page

(ID n/a)

Despite the non-existence of an access authorisation, the log-in screen of the Funkwerk Configuration Interface is displayed.

The problems have been solved; in the ***Security*** ➜ ***Local Services Access Control*** ➜ ***ADD*** menu, the ***HTTPS*** value was added in the *Service* field.

The problem has been solved.

4.6 Import of a configuration file failed

(ID 9303)

The import of configuration files in the "old" format (no CSV format) failed and destroyed the boot configuration, because the HTTP import function did not recognise the two different formats.

The problem has been solved.

4.7 Funkwerk Discovery Server faulty

(ID 8892)

If a number of addresses were assigned to a single interface, the Discovery Server did not work correctly.

The problem has been solved.

4.8 Incorrect display of the *BIBOADMCONFIGDIRTABLE* table

(ID 9926)

After the booting, the ***BIBOADMCONFIGDIRTABLE*** table did not display all data; however, all the data was correctly saved.

The problem has been solved.

4.9 Problems with the input/output link of the debug command

(ID n/a)

An input/output link (pipe) of the *debug* command with another command led to misbehaviour.

For example, when calling *debug all* | *grep XXX*, no filtering was performed and all of the lines were always output.

The *debug* command thus wrote incorrectly via the default error output instead of the default output.

The problem has been solved.

4.10 HTTP daemon crashed

(ID 9974)

In the event of a large number of simultaneous queries, the HTTP daemon crashed.

The problem has been solved; the number of simultaneously possible queries has been limited.

4.11 HTTPS connection problems

(ID 8900)

When configuring via HTTPS, it could happen that the connection was lost or that although the connection was kept alive, the browser could display no data.

The problem has been solved.

4.12 SNTP server - wrong Destination Port

(ID 10062)

With the use of the SNTP server function, the router always used destination port 123 for its response, which was incorrect.

The problem has been solved.

4.13 VLAN - Maximum number of VLANs not possible

(ID 8932)

In the ***LAN*** ➜ ***VLAN*** ➜ ***VLANs*** menu only 31 instead of 32 entries could be made.

The problem has been solved.

4.14 Bridge link configuration

(ID 9671)

In a bridge link configuration, the "Remote Link" status did not work. If the bridge link remote configuration was deactivated, it became active again after rebooting the device.

The problem has been solved.

4.15 Bridge - Test did not work

(ID n/a)

The test to see if more than one interface was set to *New Bridge Group* status did not work.

The problem has been solved.

4.16 RADIUS - Problems with WLAN client authentication

(ID 9118)

If, during a WLAN authentication via RADIUS, the first RADIUS server was not reachable, no request was sent to the second RADIUS server.

The problem has been solved.

4.17 LAN routes problem

(ID 9380)

A new LAN route was mistakenly linked via the default route to a WAN interface.

The problem has been solved.

4.18 WLAN - incorrect operation band can be set in the FCI

(ID 7836)

In the ***WIRELESS LAN*** ➜ ***WLAN1*** menu, for ***OPERATION BAND*** = *5 GHz*, the ***WIRELESS MODE*** field was shown.

The problem has been solved, for ***OPERATION BAND*** = *5 GHz*, the ***WIRELESS MODE*** field is no longer shown. The wireless mode setting is fixed at 802.11a.

4.19 WLAN - client mode could not be disabled

(ID 8819)

If the client mode was enabled on a wireless module, it could no longer be disabled.

This problem has been solved.

4.20 WLAN - stacktrace

(ID 9783)

After a WLAN configuration, a stacktrace started.

The problem has been solved.

4.21 WLAN - connection problems to WI1040

(ID 9826)

It could occur that no cableless connection could be established to a WI1040.

The problem has been solved.

4.22 WLAN - data loss

(ID n/a)

It could occur that, after the first configuration on a WLAN bridge link, many data packets were lost.

The problem has been solved.

4.23 WLAN - problems with bridge link

(ID n/a)

Various problems occurred with bridge links:

Multiple bridge links on the same radio module were not represented correctly. On scanning, not all links were correctly recognised; the links of switched-off radio modules appeared in the list of links. It could occur that the automatic configuration was performed, but the bridge did not work.

The problems have been solved.

4.24 WLAN - status LED did not work

(ID n/a)

In bridge mode (a.k.a. WDS only), the WLAN status LED did not work. It flashed regardless of whether the bridge status was *up* or *down*.

The problem has been solved.

4.25 WLAN - bridge link connection

(ID n/a)

If the radio mode of *Bridge* (a.k.a. WDS only) was switched to *off*, the MIB variable ***OperStatus*** in the MIB table ***wlanWDSTable*** incorrectly retained the *true* value.

The problem has been solved.

4.26 WLAN - authentication problems

(ID 9908)

In WLAN client mode, connections with WEP encryption were not authenticated.

The problem has been solved.

4.27 WLAN - sporadic crash

(ID 9975)

On scanning the bridge link, a crash could occur.

The problem has been solved.

4.28 WLAN - lack of checking

(ID 9906)

In the ***Wireless LAN ➜ WLAN1 ➜ Wireless networks (VSS)*** menu, no error checking was carried out on the security settings entered.

The problem has been solved.

4.29 WLAN - MAC address

(ID 9064)

In the ***Wireless LAN ➜ WLAN1 ➜ Wireless networks (VSS)*** menu, a client could continue to access the VSS, even after its ***MAC address*** had been overwritten.

The problem has been solved.

4.30 WDS links were not shown

(ID 8528)

If, in the ***Wireless LAN ➜ WLAN1*** menu, under ***Radio settings*** the operation mode was set to *Access point* or *Bridge* and confirmed with **OK**, automatically configured WDS/Bridge links were not shown.

The problem has been solved.

4.31 Multicast - problems with multicast applications

(ID n/a)

Running multiple multicast applications simultaneously, problems could occur.

The problems have been solved.

4.32 Multicast - icorrect entries in the MIB tables *IGMPCACHETABLE* and *IGMPSRCLISTTABLE*

(ID n/a)

In the MIB tables ***IGMPCACHETABLE*** and ***IGMPSRCLISTTABLE***, values were incorrectly saved although the MIB variables in these tables should have been write-protected.

The problems have been solved.

4.33 Octet string with zeroes incorrectly processed

(ID n/a)

The content of an octet string was accepted as a string. If the octet string included a zero, it was only accepted up to the zero (end of string).

The problem has been solved, octet strings can noe include zeroes as valid values.

4.34 FCI - stacktrace when routing/bridging

(ID 9613)

In the ***SYSTEM ADMINISTRATION*** ➜ ***INTERFACE MODE / BRIDGE GROUPS*** ➜ ***INTERFACES*** menu, changing the ***MODE / BRIDGE GROUP*** field from Routing to Bridging or from Bridging to Routing triggered a panic followed by a stacktrace.

The problem has been solved.

4.35 FCI - exception / stacktrace with port forwarding

(ID 9655)

In the ***Routing*** ➜ ***NAT*** ➜ ***Port Forwarding*** menu, the ***Interface*** = *none* setting triggered an exception or a stacktrace and could no longer be reached via the FCI.

The problem has been solved.

4.36 FCI - date and time not correct

(ID 9124)

If, in the ***System management*** ➜ ***Global settings*** ➜ ***Date and Time*** menu, New date and New time were set, the values were not applied.

The problem has been solved.

4.37 FCI - incorrect interface selection

(ID n/a)

In the ***LAN*** ➜ ***IP Configuration*** ➜ ***New*** menu, in the ***Based on Ethernet Interface*** field, Bridges and WLAN routing were incorrectly included in the available selection.

The problem has been solved.

4.38 FCI - no hexadecimal input for the WEP key

(ID 9679)

In the ***Wireless LAN ➜ WLAN1 ➜ WLAN1 ➜ Wireless Networks (SSID) ➜ New*** menu, in the ***WEP keys 1-4*** field, it was not possible to enter a hexadecimal value.

The problem has been solved.

4.39 FCI - incorrect page layout

(ID 9625)

In the ***Routing ➜ Routes ➜ IP Routes*** menu, the page layout was not correct.

The problem has been solved.

4.40 FCI - problems with external IP address

(ID 9289)

In the ***Routing ➜ NAT ➜ Port Forwarding*** menu, if the ***External IP Address*** field was changed, problems occurred with entires in the MIB table ***ipNatOutTable***.

The problems have been solved.

4.41 FCI - load management could be incorrectly configured

(ID 9790)

In the ***Routing*** ➜ ***Load Sharing*** ➜ ***Load Sharing Groups*** ➜ ***New*** ➜ ***Add*** menu, with a number of interfaces in the sum, a load share of more than 100 % could be configured.

The problem has been solved: the load share sum is checked and an error message is output if it exceeds 100 %.

4.42 FCI - filter rules and QoS - incorrect warning

(ID 9901)

In the ***Firewall*** ➜ ***Policies*** ➜ ***Filter Rules*** menu, if rules with ***Use QoS*** = *enabled* were defined, in the ***Firewall*** ➜ ***Policies*** ➜ ***QoS*** menu, QoS interfaces were set up waren and one of these interfaces was deleted, the message "Warning: changes not supported by the Setup Tool!" appeared in error.

The problem has been solved.

4.43 FCI - incorrect QoS queue

(ID 10011)

An FTP data session did not use the same QoS queue as the control session.

The problem has been solved.

4.44 FCI - WDS link did not work

(ID 9869)

A WDS link with ***Security Mode*** = *WEP 104* did not work.

The problem has been solved.

4.45 FCI - DNS test did not work

(ID 9978)

In the ***Maintenance*** ➜ ***Diagnostics*** ➜ ***DNS test*** menu, the DNS test did not work. After clicking on the **Go** button, nothing was indicated.

The problem has been solved.

4.46 FCI - display problems

(ID 9985, ID 9795, ID 10050, ID 9784, ID 9786, ID 10048, ID 9672, ID 9600, ID 9910)

In the ***Physical Interfaces*** ➜ ***Ethernet Ports*** menu, the SFP port was not shown.

In the ***Routing*** ➜ ***Routes*** ➜ ***IP Routes*** menu, when using Firefox V2, the IP address and the netmask were shown outside the columns if the values included the full 12 digits.

In the ***WAN*** ➜ ***Real-time Jitter Control*** menu, the bridge group interfaces were shown in error.

In the ***VPN*** ➜ ***PPTP*** ➜ ***PPTP Tunnel*** ➜ ***New*** menu, with the ***IP Address Mode*** = *Provide IP Address* setting, the ***Default Route*** and ***Create NAT Policy*** fields were incorrectly shown as enabled.

In the ***VPN ➜ PPTP ➜ PPTP Tunnel ➜ New ➜ Advanced Settings*** menu, under ***PPTP Callback***, if the ***Callback*** field was not enabled, further possible setting were nevertheless shown.

In the ***VPN ➜ PPTP ➜ PPTP Tunnel ➜ New*** menu, the ***Prioritise TCP-ACK Packets*** field was shown in error.

In the ***Monitoring ➜ WLAN ➜ WDS*** and ***Monitoring ➜ WLAN ➜ Bridge-Links*** menus, the respective WDS interfaces and WLAN bridges were not shown correctly.

In the ***Monitoring ➜ WLAN ➜ Bridge-Links*** menu, only the first bridge link was shown, the second was missing.

In the ***Monitoring ➜ IPSec ➜ IPSec Tunnel*** menu, the IP address was shown inconsistently in the list.

The problems have been solved, these items are now shown correctly.

4.47 FCI - filter problems

(ID 9778, ID 9776, ID 9654, ID 9924, ID 9780, ID n/a)

In the ***Routing ➜ Routes ➜ IP Routes*** menu, the ***Interface*** filter did not work correctly.

In the ***WAN ➜ Internet + Dialup ➜ PPoE*** menu, the entries could not be filtered because the ***Filter in*** field was empty.

In the ***Firewall ➜ Policies ➜ Filter Rules*** menu, the filters for the ***Action***, ***Data Traffic Ppriority*** and ***Policy Enabled*** columns did not work correctly.

In the ***PBX ➜ Connection Data ➜ Single Connections*** menu, the ***Direction*** filter did not work correctly.

In the ***Monitoring ➜ Internal Log ➜ System Messages*** menu, the ***Subsystem*** and ***Level*** filter functions were swapped.

In tables, it could happen that the entries were incorrectly filtered.

The problems have been solved.