Release Notes

System Software 7.8.7

Version 1.1

Purpose

This document describes new features, changes, and solved problems of **System Software 7.8.7.**

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 7.8.7 carefully to avoid problems when updating or using the software.

1.1 Applicability

System Software 7.8.7 is available only for the following devices and cannot be used on other devices:

- **R230a, R230aw, R232b, R232aw, R232bw,**
- **TR200aw, TR200bw,**
- **R1200, R1200w, R1200wu,**
- **R3000, R3000w, R3400, R3800,**
- **R4100, R4300,**
- **W1002, W1002n, 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 and Downgrade

Take note of the following indications regarding the update and the possibilities of a downgrade.

You can carry out an update or downgrade using the **Funkwerk Configuration Interface** (FCI) or - if desired - using the SNMP shell and the Setup tool.

1.2.1 Preparation and update with the FCI

The update of the system software with the Funkwerk Configuration Interface uses a BLUP (bintec Large Update) so as to update all necessary modules intelligently. All those elements are updated that are newer in the BLUP than on your gateway.

Attention!

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

To prepare and carry out an update to **System Software 7.8.7** with the **Funkwerk Configuration Interface**, proceed as follows:

1. For the update you will need the file *bl7807.xxx, where you device is encoded in the file extension xxx*.
   Ensure that the file that you need for the update is available on your PC.
   If the file is not available on your PC, enter www.funkwerk-ec.com in your browser.
   The Funkwerk homepage will open. You will find the required file in the download area for your gateway. Save it on your PC.
2. Backup the current boot configuration.
   Export the current boot configuration using the ***MAINTENANCE*** ➜ ***SOFTWARE & CONFIGURATION*** menu on the **Funkwerk Configuration Interface**. To do this, select:
   ACTION = *Export configuration*
   CURRENT FILE NAME IN FLASH = *boot*
   INCLUDE CERTIFICATES AND KEYS = Enabled
   CONFIGURATION ENCRYPTION = Disabled
   Confirm with **Go**. The window *Opening <name of gateway>.cf* will open. Leave the selection *Save to diskette/hard disk* and click **OK** to save the configuration to your PC.
   The file *<Name of gateway.cf>* is saved, the *Downloads* window shows the saved file.
3. Carry out the update to **System Software 7.8.7** via the ***MAINTENANCE*** ➜ ***SOFTWARE & CONFIGURATION*** menu.

To do this, select:
ACTION = *Update system software*
SOURCE = *Local File*
FILENAME = bl7807.xxx
Confirm with **Go**.
The message "System request. Please stand by. Your request is being processed." or "System 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 "System - Maintenance. Success. Operation completed successfully. The system must be restarted."
Click **Reboot**.
You will see the message "System - Reboot. Rebooting. Please wait. This takes approximately 40 seconds." The device will start and the browser window will open.

You can log into your device and configure it.

1.2.2 Downgrade with the FCI

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

1. Replace the current boot configuration with the previous backup version.
   Import the backup boot configuration via the ***MAINTENANCE*** ➜ ***SOFTWARE & CONFIGURATION*** menu.
   To do this, select:
   ACTION = *Import configuration*
   CONFIGURATION ENCRYPTION = Disabled
   FILENAME = *<Name of device>.cf*
   Confirm with **Go**. The message "System request. Please stand by. Your request is being processed." or "System maintenance. Please stand by. Operation in progress." shows that the selected system software is being uploaded to the device. When the upload procedure is finished, you will see the message "System - Maintenance. Success. Operation completed successfully. The system must be restarted."
   Click **Reboot**.
   You will see the message "System - Reboot. Rebooting. Please wait. This

takes approximately 40 seconds." The device will start and the browser window will open. Log into your device.

2. Carry out the downgrade to the required software version via the ***MAINTENANCE*** ➜ ***SOFTWARE & CONFIGURATION*** menu.
   To do this, select:
   ACTION = *Update system software*
   SOURCE = *Local File*
   FILENAME = *bl7802.rey* (example)
   Confirm with **Go**.
   The message "System request. Please stand by. Your request is being processed." or "System maintenance. Please stand by. Operation in progress." shows that the selected system software is being uploaded to the device. When the upload procedure is finished, you will see the message "System - Maintenance. Success. Operation completed successfully. The system must be restarted."
   Click **Reboot**.
   You will see the message "System - Reboot. Rebooting. Please wait. This takes approximately 40 seconds." The device will start with the previously backed up boot configuration and the old version of the system software. The browser window will open.

You can log into your device and configure it.

2 New Functions

System Software 7.8.7 includes a number of new functions that significantly extend the performance compared with the previous version of the system software:

2.1 Dime Manager available

In System Software 7.8.7 you can use the new Dime Manager tool to locate, configure and manage Funkwerk devices within the network.

Detailed information on the Dime Manager can be found in the Dime Manager documentation.

2.2 New Discovery Protocol

System Software 7.8.7 includes the new Discovery protocol SNMP Multicast.

The Dime Manager uses this protocol to locate Funkwerk devices within the network.

2.3 Software update and file transfer extended

In **System Software 7.8.7** you can use HTTP(S) and web server authentication for a software update or for the transfer of configuration files.

The standard format is used for the URL encoding:

http[s]://[<User Name>:<Password>@] <Host> [:<Port>]/<Path>/<File>

tftp://<Server>/<File>

You can use this information in the command line when updating and transferring a configuration file and in the corresponding field on the system maintenance page under *http://<IP address of your gateway>/maint*.

Note

Please note that the URL in the command line must be divided into two parts (*hosturl* and *file*) to define the file format (see example below).

You can only use the full URL in the new file format for system maintenance *and in the FCI (under* ***MAINTENANCE*** ➜ ***SOFTWARE & CONFIGURATION***).

Software update

The following shows examples for entries, if a software update is carried out with the *update* command:

update http://server:8080/download/R232bw_bl7802.sx6

update https://server/download/R232bw_bl7802.sx6

update http://user:secret@server/download/R232bw_bl7802.sx6.

Configuration

Configuration files can exist in two different formats: the old unencrypted format and the new CSV format (see **Release Notes Systemsoftware 7.5.1**).

Note

Note that you should only use the new CSV format, as the file used in this format is smaller, can be encrypted if necessary and guarantees better compatibility between the various system software versions.

If you want to transfer the configuration files to a web server, which has the HTTP extension WEBDAV (PUT method), you must enter the following:

cmd=put_all hosturl="http://<Server>/<Path>" file="<config>.cf" (for the old format).

cmd=put_all hosturl="http://<Server>/<Path>" file:"<config>.cf" (for the new CSV format, if to be used unencrypted)

cmd=put_all hosturl="http://<Server>/<Path>" file="<pwd>:<config>.cf" (for the new CSV format, if the data is to be encrypted with a password)

(<config> means that you must enter the name of the desired configuration file here without brackets.)

If you want to download configuration files from a web server, you must enter the following:

cmd=get_all hosturl="http://<Server>/<Path>" file="<config>.cf" (recognises old and new formats automatically)

cmd=get_all hosturl="http://<Server>/<Path>" file="<pwd>:<config>.cf" (downloads an encrypted file).

2.4 New UMTS card (only R1200wu)

With System Software 7.8.7 the R1200wu device now supports the card type OPTION GE0421, for example the Mobile Connect Card Vodafone E3730 card.

Note

A up-to-date list of supported UMTS cards can be found on the Internet at www.funkwerk-ec.com under **R1200wu** in the ***PRODUCTS*** area.

2.5 ADSL - ANNEX M added (only R200)

In **System Software 7.8.7** the new option *ANNEX M* is available in the ***ADSL MODE*** field in the FCI menu ***PHYSICAL INTERFACES*** ➜ ***ADSL MODEM*** ➜ ***ADSL CONFIGURATION***.

2.6 WLAN - Debugging

In **System Software 7.8.7** debugging information can be queried for the WLAN subsystem. The new variables *DebugType* and *DebugLevel* have been implemented in MIB table ***WLANGLOBAL*** for this purpose.

2.7 WLAN - New messages

In **System Software 7.8.7** new messages are displayed in the FCI menu ***WIRELESS LAN*** ➜ ***WLANx*** ➜ ***BRIDGE LINKS*** ➜ ***AUTO CONFIG ICON***.

If you click the **Start Auto Config** button, the following message is displayed "Warning! Do only start the auto configuration mechanism if AP is in Bridge operation and Bridge Link itself is deactivated.".

During the configuration process, different messages are displayed depending on the operation band and the phase of the configuration process.

For 2.4 GHz the message "Phase 1: Auto configuration process is running, it can take 30 to 90 seconds." or "Phase 2: Link finding process is running, it can take 30 to 90 seconds." is displayed. For 5 GHz the message "Phase 1: Auto configuration process is running, it can take 30 to 180 seconds." or "Phase 2: Link finding process is running, it can take 30 to 180 seconds." is displayed.

2.8 WLAN - New Max. Clients field

In **System Software 7.8.7** the new field ***MAX. CLIENTS*** has been added in the FCI menu ***WIRELESS LAN*** ➜ ***WLANX*** ➜ ***VIRTUAL SERVICE SETS*** ➜ **Icon to change an entry / New** and in the setup tool menu ***WLAN*** ➜ ***VSS CONFIGURATION*** ➜ **ADD/EDIT** for the maximum number of clients. The default value is *32*. The maximum value depends on the number of wireless networks: if there is one wireless network the value is *256*, if there are two the value is *128*, ..., if there are four the value is *32* and so on.

2.9 Multicast packets available on all interfaces

In **System Software 7.8.7** multicast packets can be received on all interfaces that provide an IP address.

2.10 Multicast - New MIB table igmpInterfaceOperTable

The new MIB table ***IGMPINTERFACEOPERTABLE*** makes it possible to view the interfaces on which IGMP is currently being used.

2.11 IPSec - Extended Authentication (XAuth) available

System Software 7.8.7 now offers Extended Authentication for IPSec (XAuth), an additional authentication method for IPSec tunnel users.

The gateway can take on two different roles when using XAuth as it can act as a server or as a client:

- As a server the gateway requires a proof of authorisation.

- As a client the gateway provides proof of authorisation.

In server mode multiple users can obtain authentication via XAuth, e.g. users of Apple iPhones. Authorisation is verified either on the basis of a list or via a Radius Server. If using a one time password (OTP), the password check can be carried out by a token server (e.g. SecOVID from Kobil), which is installed behind the Radius Server.

If a company's headquarters is connected to several branches via IPSec, several peers can be configured. A specific user can then use the IPSec tunnel over various peers depending on the assignment of various profiles. This is useful, for example, if an employee works alternately in different branches, if each peer represents a branch and if the employee wishes to have on-site access to the tunnel.

XAuth is carried out once IPSec IKE (Phase 1) has been completed successfully and before IKE (Phase 2) begins.

If XAuth is used together with IKE Config Mode, the transactions for XAuth are carried out before the transactions for IKE Config Mode.

XAuth Server

If you wish to configure your gateway as a XAuth server, you can allow authentication via a Radius Server or locally.

XAuth Server with authentication via RADIUS

If you wish to use a Radius Server, you must configure this for XAuth.

1. To do this, select ***System Management*** ➜ ***Remote Authentication*** ➜ ***RADIUS*** ➜ **New** in the FCI menu.
2. Select ***Authentication Type*** = *XAUTH*.
3. Enter the required group name for the Radius Server in the ***Group Description New*** field.
4. Click **Advanced Settings**.
5. Change and add the remaining settings for the Radius Server as desired and click **OK**.
   The Radius Server for XAuth is created.

Create a corresponding profile.

1. To do this, select ***VPN*** ➜ ***IPSec*** ➜ ***XAUTH Profiles*** ➜ **New**.
2. Enter a ***Description*** for the XAuth profile.

3. Select ***ROLE*** = *Server*.
4. Select ***MODE*** = *RADIUS*, select the desired RADIUS server in the ***RADIUS SERVER GROUP ID*** field and click **OK**.
   The profile is created with Radius Server.

Create an IPSec Peer for XAuth.

1. To do this, select ***VPN*** ➜ ***IPSEC*** ➜ ***IPSEC-PEERS*** ➜ **New**.
2. Enter a ***DESCRIPTION*** for the peer.
3. Click **Advanced Settings**.
4. Select the desired profile in the ***XAUTH PROFILE*** field.
5. Change and add the remaining settings for the IPSec peer as desired and click **OK**.
   The IPSec Peer is created.

XAuth Server with local authentication

If you wish to obtain authentication locally via group assignment, you can define an XAuth profile with the respective user group.

1. To do this, select ***VPN*** ➜ ***IPSEC*** ➜ ***XAUTH PROFILES*** ➜ **New**.
2. Enter a ***DESCRIPTION*** for the XAuth profile.
3. Select ***ROLE*** = *Server*.
4. Select ***MODE*** = *Local*.
5. For ***USERS*** enter a user name in the ***NAME*** field and a password in the ***PASSWORD*** field.
6. Add further users by clicking the Add button and define ***NAME*** and ***PASSWORD*** for each.
7. Click the **OK** button.
   The XAuth profile is added with the defined user group.

Create an IPSec Peer for XAuth.

1. To do this, select ***VPN*** ➜ ***IPSEC*** ➜ ***IPSEC-PEERS*** ➜ **New**.
2. Enter a ***DESCRIPTION*** for the peer.
3. Click **Advanced Settings**.
4. Select the desired profile in the ***XAUTH PROFILE*** field.

5. Change and add the remaining settings for the IPSec peer as desired and click **OK**.
   The IPSec Peer is created.

XAuth Client If you wish to configure your gateway as a XAuth Client proceed as follows:

Create a profile for XAuth in client mode.

1. To do this, select ***VPN*** ➜ ***IPSec*** ➜ ***XAUTH Profiles*** ➜ **New**.
2. Enter a ***Description*** for the XAuth profile.
3. Select ***Role*** = *Client*.
4. Enter the required user name in the ***Name*** field.
5. Enter the password for the user and click **OK**.
   The profile is created.

Create an IPSec Peer for XAuth.

1. To do this, select ***VPN*** ➜ ***IPSec*** ➜ ***IPSec-Peers*** ➜ **New**.
2. Enter a ***Description*** for the peer.
3. Click **Advanced Settings**.
4. Select the desired profile in the ***XAUTH Profile*** field.
5. Change and add the remaining settings for the IPSec peer as desired and click **OK**.
   The IPSec Peer is created.

2.12 IPSec - Dynamic Peer and IKE Config Mode

In **System Software 7.8.7** "Dynamic Peer Mode" can be used together with IKE Config Mode.

2.13 IPSec - Dynamic Peer and XAUTH

In **System Software 7.8.7** "Dynamic Peer Mode" can be used together with XAUTH.

3 Changes

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

3.1 Group Description field changed

The *None* option has been removed from the list of options in the ***GROUP DESCRIPTION*** field in the FCI menu ***SYSTEM MANAGEMENT*** ➜ ***REMOTE AUTHENTICATION*** ➜ ***RADIUS*** and the *New* option has been added. If you select *New*, you must enter a name in the adjacent field.

3.2 WLAN fields added (only W1002n)

From **System Software 7.8.7** the setting options for the **W1002n** device have been added with standard 802.11n in the FCI menus ***WIRELESS LAN*** and ***MONITORING*** ➜ ***WLAN***.

3.3 WLAN fields changed (only W1002n)

A small number of changes have been made in the FCI for the new device **W1002n**:

The order of the options in the ***Operation Band*** field has been changed for the settings ***Operation Mode*** = *Access Point* and ***Operation Mode*** = *Bridge* in the FCI menu ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Radio Settings***. In the same menu the option *5 and 2.4 GHz*, which is not supported by Ralink Chipset, has been removed from the ***Operation Band*** field for the setting ***Operation Mode*** = *Access Client*.

In the same menu the field ***Secondary Channel*** has been renamed ***Used Secondary Channel***. In devices with only one WLAN module the ***Wireless LAN*** ➜ ***WLAN2*** menu was displayed; it has been renamed ***Wireless LAN*** ➜ ***WLAN***. The **Connect** button has been renamed **Start Auto Config** in the ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Bridge Links*** ➜ ***Auto Config*** menu.

3.4 WLAN client roaming parameter removed

If the field ***Operation Mode*** = *Access Client* was set in the FCI menu ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Radio Settings*** ➜ ***Icon to change an entry*** , the following fields were displayed in the FCI menu ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Radio Settings*** ➜ ***Icon to change an entry*** ➜ ***Advanced Settings***: ***Association Advantage***, ***RSSI Advantage***, ***Weight of Age***, ***Weight of Penalty*** and ***Penalty Value***. These fields have been removed.

3.5 WLAN column Signal-to-Noise Ratio removed

The ***SNR*** (signal-to-noise ratio) column has been removed for the setting ***Operation Mode*** = *Access Client* under ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Client***

Link ➜ **Symbol Scan** ➜ **Scan** in the FCI menu ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Radio Settings*** ➜ **Icon to change an entry**, as it is impossible to calculate the signal-to-noise ratio correctly. The Ralink firmware for 802.11n does not support any noise level for scan results.

3.6 WLAN bandwidth setting added

The option ***Bandwidth*** = *40 MHz* has been added for ***Operation Band*** = *5.8 GHz Outdoor* in the FCI menu ***Wireless LAN*** ➜ ***WLAN*** ➜ ***Icon to change an entry*** ➜ ***Radio Settings***.

3.7 Web filter field changed (only R200)

The ***Enable Web Filter*** field has been renamed ***Web Filter Status*** in the FCI menu ***Local Services*** ➜ ***Web Filter*** ➜ ***Global Settings***. You can enable or disable the ***Web Filter Status*** field.

3.8 RADIUS Server group configuration simplified

The MIB variable ***GroupDescr*** has been added to the MIB table ***radiusServerTable*** to make it easier to reach a group of RADIUS servers that have been grouped together with the ***GroupId*** variable.

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 or property in question, you can ignore the problem mentioned.

The following problems have been solved in System Software 7.8.7

4.1 Access change prompted error message

(ID 11470)

In the FCI menu ***System Management*** ➜ ***Administrative Access*** ➜ ***Access*** an error message sometimes appeared when changing the current selection for any interface.

The problem has been solved.

4.2 Problems with bridge link configuration (only W1002n)

(ID 11424)

Various problems occurred with the automatic configuration of a WDS bridge link in the 5 GHz band.

The problems have been solved.

4.3 Bridge link automatic configuration incorrect (only W1002n)

(ID 11622)

The automatic configuration consists of two phases: the actual configuration process and establishing the connection.

If an automatic configuration was started and if the ***Operation Mode*** = *Bridge* field was set in the FCI menu ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Radio Settings*** ➜ ***Icon to change an entry***, the **Start Auto Config** button was available after the first phase in the ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Bridge Links*** ➜ ***Auto Config Icon*** menu. If the user clicked the button during the second phase, errors occurred and the configuration could not be completed.

The problem has been solved.

4.4 Help page not displayed

(ID n/a)

When configuring a MAC bridge, the corresponding online help page was not displayed.

The problem has been solved.

4.5 ISDN Login language not available (only R1xxx/R3xxx/R4xxx)

(ID 9794)

If the value *ISDN Login* was selected in the ***SERVICE*** field in the FCI menu ***PHYSICAL INTERFACES*** ➜ ***ISDN PORTS*** ➜ ***MSN CONFIGURATION*** ➜ **New**, the default setting ***BEARER SERVICE*** = *Data + Voice* was applied although *Voice* was not available for incoming connections.

The problem has been solved.

4.6 WLAN packets not passed (only W1002n)

(ID 11531)

If the ***SECURITY MODE*** = *WPA-PSK* or ***SECURITY MODE*** = *WPA Enterprise* setting was set for an access point **W1002n**, the clients can be registered and authenticated successfully after rebooting the access point (AP), but no sessions could be initiated from the LAN behind the AP. Broadcast and multicast packets, which have been sent by the AP, were ignored by the clients.

The problem has been solved.

4.7 WLAN incorrect display

(ID 11146)

The value *1* was displayed in the ***ACTION*** field whilst setting up the bridge in ***OPERATION MODE*** = *Bridge* in the ***WIRELESS LAN*** ➜ ***WLANX*** ➜ ***BRIDGE LINKS*** menu in the FCI menu ***WIRELESS LAN*** ➜ ***WLANX*** ➜ ***RADIO SETTINGS*** ➜ **Icon to change an entry**.

The problem has been solved; a red arrow is displayed instead.

4.8 WLAN ad-hoc mode incorrect setting options

(ID 11427)

If the ***Operation Mode*** = *Access Client* field was set in the FCI menu ***Wireless LAN ➜ WLANx ➜ Radio Settings***, superfluous setting options were displayed in the ***Wireless LAN ➜ WLANx ➜ Client Link*** menu. The ***Security Mode*** = *WPA-PSK* field could be set and different options could be selected in the ***WPA Mode*** field.

The problem has been solved, the above settings have been removed from the FCI.

4.9 WLAN wireless mode - different descriptions

(ID n/a)

Different texts were displayed in the ***Wireless Mode*** field in devices with and without 802.11n in the FCI menu ***Wireless LAN ➜ WLANx ➜ Radio Settings***.

The problem has been solved; the texts are now the same.

4.10 WLAN incorrect channel displayed (only W1002n)

(ID 11425)

If the field ***Operation Mode*** = *Access Point* was set in the FCI menu ***Wireless LAN ➜ WLANx ➜ Radio Settings ➜ Icon to change an entry***, the configure channel was displayed instead of the channel currently being used in the ***Channel in Use*** column in the ***Wireless LAN ➜ WLANx ➜ Radio Settings*** menu.

The problem has been solved.

4.11 IPSec peers incorrect display

(ID 11637)

All IPSec peers were displayed, even those not configured manually, in the FCI menu ***VPN ➜ IPSec ➜ IPSec Peers***.

The problem has been solved, only peers that can be configured manually are displayed.

4.12 IPSec phase-2 bundles do not transmit local network

(ID 11409)

Local network not transmitted with IPSec phase-2 bundles, if no local IP address was configured on the router.

The problem has been solved.

4.13 Firewall - QoS incorrect display

(ID 11863)

The assignment of filter rules to interfaces displayed in the FCI menu ***Firewall*** ➜ ***Policies*** ➜ ***QoS*** does not match the configured assignment.

The problem has been solved.

4.14 VoIP - Media Gateway - Registrar field missing

(ID 11758)

The ***Registrar*** field was not displayed in the FCI menu ***VoIP*** ➜ ***Media Gateway*** ➜ ***SIP Accounts*** ➜ **New**.

The problem has been solved.

4.15 VoIP incorrect display

(ID 11726)

The columns for the fields in the FCI menu ***VoIP*** ➜ ***Media Gateway*** ➜ ***Extensions*** ➜ **New** ➜ **Advanced Settings** were displayed wider than in the ***Basic Parameters*** area.

The problem has been solved, the display on the page has uniform widths in all areas.

4.16 VoIP ISDN trunks missing

(ID n/a)

FCI menu ***VoIP*** ➜ ***Media Gateway*** ➜ ***ISDN Trunks*** missing.

The problem has been solved, the menu is displayed.

4.17 VoIP - No display

(ID n/a)

No values were displayed in the ***Associated Line*** column in the FCI menu ***VoIP*** ➜ ***Media Gateway*** ➜ ***Call Translation***.

The problem has been solved.

4.18 VoIP - SIP accounts incorrect display

(ID n/a)

The ***External Address*** column was displayed for SIP accounts with disabled trunk mode in the FCI menu ***VoIP*** ➜ ***Media Gateway*** ➜ ***Call Translation***.

The problem has been solved.

4.19 VoIP - Trunk setting options not displayed

(ID n/a)

If the field ***TRUNK MODUS*** = *gw-trunk* was set in the FCI menu ***VOIP*** ➜ ***MEDIA GATEWAY*** ➜ ***SIP ACCOUNTS*** ➜ **New**, the ***TRUNK SETTINGS*** menu was not displayed.

The problem has been solved.

4.20 VoIP provider not displayed

(ID n/a)

In the FCI menu ***VOIP*** ➜ ***MEDIA GATEWAY*** ➜ ***CALL ROUTING*** the VoIP providers with ***TRUNK MODE*** = *gw-trunk* set in the ***VOIP*** ➜ ***MEDIA GATEWAY*** ➜ ***SIP ACCOUNTS*** ➜ **New** menu were not displayed.

The problem has been solved.

4.21 VoIP selection incomplete

(ID n/a)

If the field ***TRUNK MODUS*** = *Client* was set in the FCI menu ***VOIP*** ➜ ***MEDIA GATEWAY*** ➜ ***SIP ACCOUNTS*** ➜ **New**, the *Display only* option was not displayed in the list in the ***SIP HEADER FIELD(S) FOR CALLER ADDRESS*** field.

The problem has been solved.

4.22 VoIP - Incorrect display

(ID n/a)

No values were displayed in the ***Subscriber Number*** and ***Called Line*** columns in the FCI menu ***VoIP*** ➜ ***Media Gateway*** ➜ ***CLID Translation***.

The problem has been solved.

4.23 IP/MAC Binding restricted

(ID 11756)

In the FCI menu ***Local Services*** ➜ ***DHCP Server*** ➜ ***IP/MAC Binding*** it was not possible to assign two different MAC addresses to the same IP address. An error message appeared.

The problem has been solved. You can now assign the same IP address twice in order to connect a laptop via LAN and via WLAN for example.

4.24 E-mail Alert - Subsystem missing

(ID 11554)

The *WLAN* option was missing in the list under ***Subsystem*** **Add** in the FCI menu ***External Reporting*** ➜ ***E-mail Alert*** ➜ ***E-mail Alert Recipient*** ➜ **New**.

The problem has been solved; the list has been expanded.

4.25 Setup Tool - Multicast - Stacktrace for IGMP

(ID 11508)

If for VDSL (Very High Speed Digital Subscriber Line) the field ***STATUS*** = *enabled* in the setup tool menu ***IP*** ➜ ***MULTICAST*** and the field ***STATUS*** = *up* in the ***IP*** ➜ ***MULTICAST*** ➜ ***IGMP*** menu and if ***MODE*** = *v3only* was set and two entries were created with **ADD** and one of these entries was then changed, saving these settings resulted in a panic followed by stacktrace and reboot.

The problem has been solved.

4.26 Setup Tool - IPSec - Incorrect input mask for Block Time field

(ID 11840)

A value of up to four digits could be entered in the ***BLOCK TIME*** field in the setup tool menu ***IPSEC*** ➜ ***IKE (PHASE 1)*** ➜ **Edit** ➜ **Add**, although the value range for this field *-1* to *86400*. In the FCI the input options were correct.

The problem has been solved.