Wx002-, WIx040-, WIx065-Series

Release Notes

System Software 7.8.2

Version 1.0

Purpose

This document describes new features, changes, and solved problems of **System Software 7.8.2.**

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

1.1 Applicability

System Software 7.8.2 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 7.8.2**, 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 7.8.2** 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	7.8.2 Downgrade to ACE possible	**ComPoint Manager** or console
	7.6.2	7.8.2 Downgrade to ACE possible	Console or FCI

1.2.1 Preparation and update (W1002 and W2002)

When updating to System Software 7.8.2, the operating system is, where appropriate, automatically changed from ACE to BOSS.

Note

If you already run **System Software 7.5.1** or higher on your device, proceed with your update as described for devices in the **WI** series (see “Preparation and update (WI series)” on page 15).

Carry out the update as follows:

Update preparation

1. For the update you will need, for the device **W1002**, the file *W1002_boss_s7802.afw* or, for the device **W2002**, the file *W2002_boss_s7802.afw*.
   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 **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 the device in the list for which you wish to carry out the update.
2. Select ***CONFIGURATION*** ➜ ***LOAD FIRMWARE***.
3. Click **Select software**.
4. Click **Browse**, select the folder containing the files and click **OK**.
   The desired file(s) will be shown.
5. Depending on the device, select the desired firmware, i.e. *W1002_boss_s7802.afw* for **W1002** or *W2002_boss_s7802.afw* for **W2002**, click **OK** and then click **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 **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 **Login**.
   The status page of the **Funkwerk Configuration Interface** will open.
4. Make sure that the language setting is *English*.
5. Click ***Maintenance*** ➜ ***Software & Configuration***.
6. In the ***Action*** field, select *Update System Software*.
7. In the ***Source*** field, select the value *Local File* and click the **Browse** button.
8. Click the desired filename, e.g. *W1002_Blup_LED_SCHEME.w1p* and then **Open**.
9. Now click **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."
10. Click **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_18.w1p* or *W2002_ace_6_18.w2p,* which you will find under www.funkwerk-ec.com (see “Update preparation” on page 10).

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 7.8.2** , 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 **Login**.
3. Make sure that the language setting is *English*.
4. Click ***Maintenance*** ➜ ***Software & Configuration***.
5. In the ***Action*** field, select *Update System Software*.
6. In the ***Source*** field, select the value *Local File* and click the **Browse** button.
7. Click the desired filename, e.g. *W1002_ace_6_18.w1p* and then **Open**.
8. Click **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.

9. Click **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 **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 **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 7.6.2 so that configuration and maintenance via the Funkwerk Configuration In-

terface is available, making it simple to update the software. This makes an update possible in two ways.

Update preparation

1. For the update, you need, for devices of the **WI** series, the file *bl7802.iny*. 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 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 **Go**. 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 **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\bl7802.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 file browser.
3. Click **Go**. 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 **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

If appropriate, proceed as follows to prepare and carry out an update to **System Software 7.8.2**:

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 Set-up 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 7.8.2** 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/bl7802.iny
Starting TFTP File Transfer .....................................
..................... (139320+4887788 Bytes)
List of files in this update (len 4887788):
  Version    Length  Name
7.8.2.000   4048577  Boss
7.8.2.000    774792  webpages.ez
7.8.2.000    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 7.8.2** 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 Functions

System Software 7.8.2 includes a number of new functions that significantly extend the performance compared with System Software 7.6.2:

2.1 Funkwerk Configuration Interface - Overview

A number of new functions are now available for devices in the Wx002, WIx040 and WIx065 series. The table below shows the name of the respective function, the path to where you can find the function in the Funkwerk Configuration Interface and a short description. Detailed information can be found in the Help section for your device if not included in these Release Notes.

Function	Path / Comment
NAT	In the ***ROUTING*** ➜ ***NAT*** menu you can use Network Address Translation (NAT) to translate the source and destination addresses for IP packets.
RIP	In the ***ROUTING*** ➜ ***RIP*** menu you can determine how the routing information between several devices is exchanged dynamically.
Load Balancing	In the ***ROUTING*** ➜ ***LOAD BALANCING*** menu you can distribute the data traffic on various interfaces and use load balancing to organise these within a group of interfaces according to various criteria.
Multicast	In the ***ROUTING*** ➜ ***MULTICAST*** you can define the communication from a sender to several recipients.
Internet + Dialup	In the ***WAN*** ➜ ***INTERNET + DIALUP*** menu, you can set up internet access and dialup connections.
Real Time Jitter Control	You can optimise the quality of telephone calls over the Internet in the ***WAN*** ➜ ***REAL TIME JITTER CONTROL*** menu.
IPSec	In the ***VPN*** ➜ ***IPSEC*** menu you can setup secure connection between two localities (VPN) so that sensitive company information can be transmitted over an insecure medium such as the internet.
L2TP	In the ***VPN*** ➜ ***L2TP*** menu you can use the layer 2 tunnel protocol (L2TP) to enable PPP connections to be tunnelled via a UDP connection.

Function	Path / Comment
GRE	In the ***VPN*** ➜ ***GRE*** menu you can used the Generic Routing Encapsulation (GRE) protocol to encapsulate other protocols and to transport these over the internet protocol using tunnels (see page 39).
Certificates	In the ***VPN*** ➜ ***CERTIFICATES*** menu you can view existing certificates and request or import additional certificates as required.
Policies	In the ***FIREWALL*** ➜ ***POLICIES*** menu you can display, change and add new filter rules. In the ***FIREWALL*** ➜ ***POLICIES*** ➜ ***QOS*** menu you can distribute bandwidths as required using the Quality of Service (QoS) function and reserve these for specific applications.
Addresses	In the ***FIREWALL*** ➜ ***ADDRESSES*** menu you can display addresses that have already been configured, set up additional addresses and compile addresses into groups.
Services	In the ***FIREWALL*** ➜ ***SERVICES*** menu you can display all available addresses, set up new services and compile services into groups.
DynDNS Client	In the ***LOCAL SERVICES*** ➜ ***DYNDNS CLIENT*** menu you can ensure that your device can always be located using the dynamic IP address.
E-mail Alert	In the ***EXTERNAL REPORTING*** ➜ ***E-MAIL ALERT*** menu the gateway administrator can be notified of specific events via E-mail (see page 41).
Monitoring IPSec	In the ***MONITORING*** ➜ ***IPSEC*** menu you can display all of the configured IPSec tunnels and statistical values for all IPSec connections.
Monitoring Bridges	In the ***MONITORING*** ➜ ***BRIDGES*** menu, the current values of the configured bridges are shown.

2.2 Serial over IP (SoIP; only WIx040 and WIx065 series)

In System Software 7.8.2 the devices funkwerk WI1040, WI2040, WI3040, WI1065, WI2065 and WI3065 come with the Serial over IP (SoIP) function. The serial interface can now be operated as a console or as a data interface. In data interface mode, the data for the serial interface can be transmitted over an IP infrastructure (Serial over IP).

Funkwerk Configuration Interface

You can configure the Serial over IP function in the FCI menu ***PHYSICAL INTERFACES*** ➜ ***SERIAL PORT*** ➜ ***SERIAL PORT***.

Parameter	Value
Port mode	Select in which mode the serial interface is to be used. Possible values: ■ *Configuration* (default value): The serial interface is used as a console. This is the same behaviour as in previous software versions. ■ *Data port*: The serial interface is operated as a data interface, Serial over IP is used.

Parameter	Value
Baud rate	Only for ***PORT MODE*** = *Data port*. Select which baud rate should be used. Make sure that the remote terminal is suitable for the selected baud rate. Possible values: ■ *300* ■ *600* ■ *1200* ■ *2400* ■ *4800* ■ *9600*: (default value) ■ *19200* ■ *57600* ■ *115200.*
Data bits	Only for ***PORT MODE*** = *Data port*. Select how many data bits should be sent in sequence for traffic data. Possible values: ■ *8* (default value): Eight data bits are sent in sequence. ■ *7*: Seven data bits are sent in sequence.

Parameter	Value
Parity	Only for ***PORT MODE*** = *Data port*. Select whether or not a parity bit should be used to identify transmission errors. Possible values: ■ *None* (default value): No parity bit is used. ■ *Even*: An even number of "1" bits is used to identify transmission errors. ■ *Odd*: An uneven number of "1" bits is used to identify transmission errors.
Stop bits	Only for ***PORT MODE*** = *Data port*. Stop bits terminate the data transmission of a transmission unit. Choose whether a stop bit should be used or whether two stop bits should be used. Possible values: ■ *1* (default value) ■ *2.*
Handshake	Only for ***PORT MODE*** = *Data port*. Choose how the recipient can continue the data transmission so that no data is lost, if no other data can be processed. Possible values: ■ None: The recipient is unable to continue the data transmission. ■ *RTS/CTS*: The hardware handshake used controls the data flow over the RTS and CTS lines. ■ *XON/XOFF*: If the software handshake is used, the recipient sends special signs to the sender to control the data flow.

Parameter	Value
Mode	Only for ***PORT MODE*** = *Data port*. Select the mode in which the gateway should process IP data packets. Possible values: ■ *Server* (default value): The gateway waits for incoming TCP connections. ■ *Client*: The gateway actively sets up a TCP connection. ■ *UDP*: The gateway sends and receives UDP packets.
Local IP Address	Only for ***PORT MODE*** = *Data port*. For ***MODE*** = *Server* Enter the IP address of the client logging in. If ***LOCAL IP ADDRESS*** = *0.0.0.0*, any client can log in.
Local Port	Only for ***PORT MODE*** = *Data port*. Enter the port for the ***LOCAL IP ADDRESS***.
Remote IP	Only for ***PORT MODE*** = *Data port*. For ***MODE*** = *Client* Enter the IP address of the server at which your gateway should log in as a client.
Port number	Only for ***PORT MODE*** = *Data port*. Enter the port for the ***REMOTE IP***.

Parameter	Value
Byte number	Only for ***PORT MODE*** = *Data port*. Before an IP packet is sent, there is a delay until the specific number of bytes has been received. The function is activated with *Enabled*. The function is enabled by default. Possible values: *1* .. *1460*. Default value: *128*.
Timeout	Only for ***PORT MODE*** = *Data port*. Before an IP packet is sent, there is a delay until the specified time in ms has passed since the last character was received. The function is activated with *Enabled*. The function is enabled by default. Possible values: *0* .. *65535*. Default value: *0*.
Inter-ByteGap	Only for ***PORT MODE*** = *Data port*. Before an IP packet is sent, there is a delay until the specified time in ms has passed since the first character was received. The function is activated with *Enabled*. The function is disabled by default. Possible values: *0* .. *65535*. Default value: *100*.
Delete serial RX buffer	Only for ***PORT MODE*** = *Data port*. Click the **Delete** button to clear the receive buffer.
Delete serial TX buffer	Only for ***PORT MODE*** = *Data port*. Click the **Delete** button to clear the send buffer.

Table 2-1: Fields in the ***PHYSICAL INTERFACES*** ➜ ***SERIAL PORT*** ➜ ***SERIAL PORT*** menu

2.3 ISAKMP Configuration Method (IKE Config Mode)

System Software 7.8.2 now offers the ISAKMP Configuration Method (IKE Config Mode for short) that allows you to connect a mobile PC workstation (Secure IPSec Client) to the head office over VPN. The IP address and, if required, other data such as the domain and server parameters for DNS and WINS are sent to the client by the VPN gateway on request. This method allows a dynamic IP address to be assigned from the internal address range for the head office.

IKE Config Mode can be operated by extending the IPSec configuration. Data is transmitted from the gateway to the client in IPSec according to IKE (Phase 1) and is therefore protected by encryption.

Note

Note that IKE Config Mode is only available for IPSec peers with a virtual interface.

Proceed as follows to use IKE Config Mode.

1. Create at least one IP address range. To do this, select the FCI menu options ***VPN*** ➜ ***IPSec*** ➜ ***IP Pools*** and click **Add**. Enter the ***IP Pool Name*** and the ***IP Pool Range*** for the current IP address range. Click **Add** to create additional IP address ranges. Save the created IP address range with **OK**. The created IP address ranges are available.
2. Select IKE Config Mode and assign your chosen IP address range. To do this, select the FCI menu options ***VPN*** ➜ ***IPSec*** ➜ ***IPSec Peers*** and click **New**. Select ***IP address assignment*** = *IKE Config Mode*. Select ***IP Assignment Pool*** = *<Your chosen pool>*. Save with **OK**.

IKE Config Mode configuration is complete and a secure IPSec client can now dial into the gateway.

2.4 Layer 2.5 Bridge

In System Software 7.8.2 you can realise bridging for devices behind access clients with the Layer 2.5 Bridge function. In wildcard mode you cannot define how Unicast non-IP frames or non-ARP frames are processed.

To use the layer 2.5 bridge function, you must carry out configuration steps in several FCI menus.

1. Select the FCI menu ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Radio Settings*** and click the icon to change an entry.
2. Select ***enabled*** in the *Wireless Module* field.

The menu is displayed.

3. Set ***Operation Mode*** to *Access Client* and save the settings with **OK**.
4. Select the menu options ***System Management*** ➜ ***Interface Mode / Bridge Groups*** ➜ ***Interfaces***.

The additional interface *sta1-0* is displayed.

5. For interface sta1-0 select ***Mode / Bridge Group*** = *br0 (<IP Address>)* and ***Configuration Interface*** = *en1-0* and save the settings with **OK**.
6. Click the **Save Configuration** button to save all of the configuration settings.

You can use the Layer 2.5 Bridge.

Wildcard mode

To configure the wildcard mode, you must carry out additional configuration steps.

7. In the ***System Management*** ➜ ***Interface Mode / Bridge Groups*** ➜ ***Interfaces*** menu click the icon to change an entry in the row for interface sta1-0.

The layer 2.5 options menu opens. ***sta1-0*** is displayed as the *Interface*.

8. Select a ***Wildcard mode***.
   Three options are available:
   If you choose the *Static* setting you must also enter the MAC address of a device that is connected over IP. Each packet without IP and without ARP is forwarded to this device. This occurs even when the device is no longer

connected. If ***Transparent MAC Address*** is *enabled* the wildcard MAC address is used in addition to the WLAN MAC address to establish the connection to the access point.
If you choose the *first* setting the MAC address of the first non-IP unicast frame or non-ARP unicast frame, which occurs on any of the Ethernet interfaces, is used as the wildcard MAC address. This wildcard MAC address can only be reset by rebooting the device or by selecting another wildcard mode.
If you choose the *last* setting the internal WLAN MAC address is used to establish a connection to the access point. As soon as a non-IP unicast frame or non-ARP unicast frame appears, it is forwarded to the MAC address from which the last non-IP unicast frame or non-ARP unicast frame was received on the Ethernet interface of the device. This wildcard MAC address is renewed with each non-IP unicast frame or non-ARP unicast frame.

2.5 Fast Roaming for WLAN Client Mode

System Software 7.8.2 now offers a so-called fast roaming for WLAN client mode, i.e. roaming for fast moving clients. This function can be used to transmit data from a client installed in an underground station to access points in the underground tunnel. In this scenario the roaming of the client from one access point to another occurs quickly due to the high speed of the underground train.

You can configure fast roaming for WLAN client mode in the FCI menu ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Radio Settings***.

1. Click the icon to change an entry to open the menu.
2. Select ***enabled*** in the *Wireless Module* field to show the full menu.
3. Select ***Operation Mode*** = *Access Client* You can also modify the default settings for the remaining fields if required.
4. Define the parameters for client fast roaming in the ***Advanced Settings*** menu.

The FCI menu ***Wireless LAN ➜ WLANx ➜ Radio Settings ➜ Icon to change an entry ➜ Advanced Settings*** contains the following fields when ***Operation Mode*** is set to *Access Client*:

Parameter	Value
Scan Channels	When *All* is selected the device scans all of the channels for available wireless networks. This field is set to *All* by default. If *All* is disabled, you can define the channels to be used for the search in the ***Selected Channels*** field.
Selected Channels	Only if *All* is enabled in the ***Scan Channels*** field. If you have saved the setting ***Operation Mode*** = *Access Client* with **OK**, you will see all of the channels that are currently selected here. You can define the channels on which the device should search for available wireless networks. You can delete channels that are already selected. If not all channels are selected, you can click **Add** to add any missing channels.

Parameter	Value
Roaming Profile	Here you can select the conditions under which roaming will occur. To do this, you can either use a predefined profile that contains fixed values for all parameters or you can define all of the parameters yourself. Each AP known to the client is evaluated using this parameter and is assigned a number. The client connects to the AP with the highest number. Possible values: ■ *Fast Roaming*: If the data rate is 26 Mbps or less, roaming is carried out as soon as an access point with a higher data rate becomes available. ■ *Normal Roaming* (default value): If the data rate is approx. 18 Mbps or less, roaming is carried out as soon as an access point with a higher data rate becomes available. ■ *Slow Roaming*: If the data rate is approx. 6 Mbps or less, roaming is carried out as soon as an access point with a higher data rate becomes available. ■ *No Roaming*: Roaming is only carried out if the connected to the access point is interrupted. ■ *Custom Roaming*: You can define the roaming parameters according to your needs.

Parameter	Value
Scan Threshold	You can only change the value for ***ROAMING PROFILE*** = *Custom Roaming*; for all other ***ROAMING PROFILE*** settings a fixed value is assigned. Enter the threshold value in dBm above which a search should be triggered for available wireless networks. The default value is *-70* dBm.
Scan Interval	You can only change the value for ***ROAMING PROFILE*** = *Custom Roaming*; for all other ***ROAMING PROFILE*** settings a fixed value is assigned. Enter the time interval in milliseconds at which a search should be triggered for available wireless networks. The default value is *5000* ms.
Channel Sweep	You can only change the value for ***ROAMING PROFILE*** = *Custom Roaming*; for all other ***ROAMING PROFILE*** settings a fixed value is assigned. Enter the number of frequencies that should be used for the search. The default value is *2*. The value *0* disables the search. The value -1 uses all available frequencies for the search.

Parameter	Value
Min. Time Period for Active Scan	You can only change the value for ***ROAMING PROFILE*** = *Custom Roaming*; for all other ***ROAMING PROFILE*** settings a fixed value is assigned. Enter the shortest interval that should be used when carrying out active scanning for a frequency. (Active scanning means that the client actively searches for access points in its range.) The default value is *10* ms.
Max. Time Period for Active Scan	You can only change the value for ***ROAMING PROFILE*** = *Custom Roaming*; for all other ***ROAMING PROFILE*** settings a fixed value is assigned. Enter the longest interval that should be used when carrying out active scanning for a frequency. (Active scanning means that the client actively searches for access points in its range.) The default value is *40* ms.
Min. Time Period for Passive Scan	You can only change the value for ***ROAMING PROFILE*** = *Custom Roaming*; for all other ***ROAMING PROFILE*** settings a fixed value is assigned. Enter the shortest interval that should be used when carrying out passive scanning for a frequency. (During passive scanning the client receives and evaluates the signals send by all of the access points.) The default value is *20* ms.

Parameter	Value
Max. Time Period for Passive Scan	You can only change the value for ***ROAMING PROFILE*** = *Custom Roaming*; for all other ***ROAMING PROFILE*** settings a fixed value is assigned. Enter the longest interval that should be used when carrying out passive scanning for a frequency. (During passive scanning the client receives and evaluates the signals send by all of the access points.) The default value is *120* ms.
Association Advantage	You can only change the value for ***ROAMING PROFILE*** = *Custom Roaming*; for all other ***ROAMING PROFILE*** settings a fixed value is assigned. This parameter is a measure of how important it is that roaming occurs on a client. The higher the value, the higher the probability that no roaming will occur and that the client will remain at the current access point. The default value is *10*.
RSSI Advantage	You can only change the value for ***ROAMING PROFILE*** = *Custom Roaming*; for all other ***ROAMING PROFILE*** settings a fixed value is assigned. This parameter is a measure of to what extent the signal strength is taken into account when making a roaming decision. The higher the value, the sooner roaming occurs. The default value is *10*.

Parameter	Value
Weight of Age	You can only change the value for ***ROAMING PROFILE*** = *Custom Roaming*; for all other ***ROAMING PROFILE*** settings a fixed value is assigned. This parameter is a measure of to what extent the time period is taken into account when making a roaming decision if the client already "knows" the AP. The higher the value, the more likely it is that the client will access a known AP during roaming. The default value is *5*.
Weight of Penalty	You can only change the value for ***ROAMING PROFILE*** = *Custom Roaming*; for all other ***ROAMING PROFILE*** settings a fixed value is assigned. With this parameter you can also influence the roaming decision. The value indicates to what extent the value of the ***PENALTY VALUE*** influences the roaming decision. The default value is *10.*
Penalty Value	You can only change the value for ***ROAMING PROFILE*** = *Custom Roaming*; for all other ***ROAMING PROFILE*** settings a fixed value is assigned. With this parameter you can also influence the roaming decision. The higher the value, the greater the influence on the roaming decision. The default value is *50.*

Table 2-2: Fields in the ***WIRELESS LAN*** ➜ ***WLANx*** ➜ ***RADIO SETTINGS*** ➜ ***ICON TO CHANGE AN ENTRY*** ➜ ***ADVANCED SETTINGS*** menu

2.6 GRE

In System Software 7.8.2 the GRE function is available in the FCI. In the *VPN* ➜ *GRE* menu you can used the Generic Routing Encapsulation (GRE) protocol to encapsulate other protocols and to transport these over the internet protocol using tunnels.

The ***VPN*** ➜ ***GRE*** ➜ ***GRE TUNNELS*** ➜ ***NEW*** menu contains the following fields:

Parameter	Value
Description	Enter a description for the GRE tunnel.
Local GRE IP Address	Enter the source IP address of the GRE packets to the GRE partner. If no IP address is given (this corresponds to IP address 0.0.0.0), the source IP address of the GRE packets is selected automatically from one of the addresses of the interface via which the GRE partner is reached.
Remote GRE IP Address	Enter the destination IP address of the host or network to which the packets are to be sent through the GRE tunnel.
Default Route	If you enable the ***DEFAULT ROUTE***, all data is automatically routed to a single connection. The function is disabled by default.
Local IP Address	Enter the IP address to be used as the source address for this GRE connection.

Parameter	Value
Route Entries	Define other routing entries for this connection partner. Add a new entry with **Add**. ***REMOTE IP ADDRESS***: IP address of the destination host or network. ***NETMASK***: Netmask of ***REMOTE IP ADDRESS***. If no entry is made, your device uses a default netmask. ***METRIC***: The lower the value, the higher the priority of the route (possible values *0*... *15*). The default value is *1*.
MTU	Enter the maximum packet size (Maximum Transfer Unit, MTU) in bytes that is allowed for the GRE connection between the partners. Possible values are *1* to *8192*. The default value is *1500*.
Use Key	Enable the key input for the GRE connection, which makes it possible to distinguish between several parallel GRE connections between two GRE partners (see RFC 1701). The function is activated with *Enabled*. The function is disabled by default.
Key Value	Only for ***USE KEY*** = *enabled*. Enter the GRE connection key. Possible values are *0* to *2147483647*. The default value is *0*.

Table 2-3: Fields in the ***VPN*** ➜ ***GRE*** ➜ ***GRE TUNNELS*** ➜ ***NEW*** menu

2.7 E-mail alert

In System Software 7.8.2 the E-mail alert function is available in the FCI. The gateway administrator can be notified of certain events that are displayed by syslog messages via E-mail.

You can configure the E-mail alert function in the FCI menu ***External Reporting*** ➜ ***E-mail Alert***.

The ***External Reporting*** ➜ ***E-mail Alert*** ➜ ***E-mail Alert Server*** ➜ ***Basic Parameters*** menu contains the following fields:

Parameter	Value
Alert service	Here you can enable and disable the function. The function is enabled by default.
Sender's E-mail Address	Enter the E-mail address to be displayed in the sender field of the E-mail.
Maximum number of messages per minute	Here you can limit the number of outgoing E-mails per minute. Possible values are *1* to *15*. The default value is *6*.

Table 2-4: Fields in the ***External Reporting*** ➜ ***E-mail Alert*** ➜ ***E-mail Alert Server*** ➜ ***Basic Parameters*** menu

The ***External Reporting*** ➜ ***E-mail Alert*** ➜ ***E-mail Alert Server*** ➜ ***SMTP Settings*** menu contains the following fields:

Parameter	Value
SMTP Server	Enter the address (IP address or valid DNS name) of the mail server to be used for sending the E-mails. The entry is limited to 40 characters.

Parameter	Value
SMTP Authentication	Select whether or not authentication should be used between the client and server and if so, which protocol should be used. Possible values: ■ *None* (default value): No authentication should be used. ■ *ESMTP*: Extended SMTP with Authentication should be used. ■ *SMTP after POP*: POP (Post Office Protocol) with Authentication should be used first, following by SMTP with the same authentication.
User name	Only for ***SMTP AUTHENTICATION*** = *ESMTP* or ***SMTP AUTHENTICATION*** = *SMTP after POP*. Enter the user name of the client for authentication.
Password	Only for ***SMTP AUTHENTICATION*** = *ESMTP* or ***SMTP AUTHENTICATION*** = *SMTP after POP*. Enter the password of the client for authentication.
POP3 Server	Only for ***SMTP AUTHENTICATION*** = *SMTP after POP*. Enter the address (IP address or valid DNS name) of the POP3 server to be used for downloading the E-mails. Appropriate POP3 server software must be installed so that the mailserver can answer the requests via POP3.

Parameter	Value
POP3 Timeout	Only for ***SMTP AUTHENTICATION*** = *SMTP after POP*. Select the period of time after which authentication will expire. After this time, E-mails cannot be sent. The possible values are *60* to *3600* seconds, the default value is *600*.

Table 2-5: Fields in the ***EXTERNAL REPORTING*** ➜ ***E-MAIL ALERT*** ➜ ***E-MAIL ALERT SERVER*** ➜ ***SMTP SETTINGS*** menu

The ***EXTERNAL REPORTING*** ➜ ***E-MAIL ALERT*** ➜ ***E-MAIL ALERT RECIPIENT*** ➜ ***NEW*** ➜ ***ADD/EDIT E-MAIL RECIPIENT*** menu contains the following fields:

Parameter	Value
Recipient	Enter the recipient's E-mail address here.
Matching String	Enter the string that must occur in a syslog message for an E-mail to be sent. Bear in mind that without the use of wildcards (e.g. "*"), only those strings that correspond exactly to the entry fulfil the condition. The string entered therefore usually contains wildcards. To be informed of all syslog messages of the selected level, just enter "*".

Parameter	Value
Severity	Here you select the syslog level at which the string entered in the ***MATCHING STRING*** field must occur to trigger an E-mail alert. Possible values: ■ *Emergency* (default value) ■ *Alert* ■ *Critical* ■ *Error* ■ *Warning* ■ *Alert* ■ *Information* ■ *Debug.*
Message Timeout	Enter the maximum number of seconds the gateway must wait after a relevant event before it sends an E-mail. Possible values are *0* to *86400*. The value *0* disables the timeout.
Number of Messages	Here you enter the number of syslog messages that must be reached before an E-mail can be sent for this case. If ***MESSAGE TIMEOUT*** is configured, the E-mail is sent when this expires, even if the ***NUMBER OF MESSAGES*** has not been reached.

Parameter	Value
Message Compression	Here you can select whether the E-mail message text is to be shortened. The E-mail then contains the syslog message only once plus the number of relevant events. Enable or disable the function. The function is enabled by default.

Table 2-6: Fields in the ***External Reporting*** ➜ ***E-mail Alert*** ➜ ***E-mail Recipient*** ➜ ***New*** ➜ ***Add/Edit E-mail Recipient*** menu

The ***External Reporting*** ➜ ***E-mail Alert*** ➜ ***E-mail Recipient*** ➜ ***New*** ➜ ***Monitored Subsystems*** menu contains the following fields:

Parameter	Value
Subsystem	Here you select the subsystems to be monitored. Add a new system with **Add**.

Table 2-7: Fields in the ***External Reporting*** ➜ ***E-mail Alert*** ➜ ***E-mail Recipient*** ➜ ***New*** ➜ ***Monitored Subsystems*** menu

2.8 SSH Client

In **System Software 7.8.2** the SSH (Secure Shell) Client function is available. This allows you to set up a secure connection from your gateway to a remote computer or to a second gateway and, for example, to output the command line of the remote computer on your gateway or to check the configuration of the second gateway.

To dial into a remote computer or a second gateway, enter the command line *ssh <User Name Gateway>@<IP address of the remote computer or IP address of the second gateway>*.

2.9 IGMP Host for local applications

System Software 7.8.2 supports IGMP for local multicast applications; i.e. local applications (e.g. Access Point Discovery Daemon) log in to specific multicast groups using IGMP reports and so can receive multicast packets. This may be necessary for switches that use IGMP snooping.

For this mode you do not need to manually enable IGMP for each application on the corresponding interface as you can simply use the automated function provided: As soon as a host opens a local application using multicast, IGMP is enabled automatically on the corresponding interface and the IGMP interface is operated in host mode.

You can configure this automated function in the FCI menu ***Routing*** ➜ ***Multicast*** ➜ ***Options*** by choosing the setting ***IGMP Status*** = *Auto*.

If the IGMP status is enabled (***IGMP Status*** = *Enabled)*, you must configure the respective interfaces manually for IGMP host. If an interface is operation in "Only Host Mode" (***Routing*** ➜ ***Multicast*** ➜ ***IGMP*** ➜ ***Icon to change an entry*** with ***Mode*** = *Only Host*), applications will only receive packets on this interface. Routing must be allowed (***Routing*** ➜ ***Multicast*** ➜ ***IGMP*** ➜ ***Icon to change an entry*** with ***Mode*** = *Host and Routing*) to manage IGMP statuses for other systems on this interface and to route incoming packets there.

In the ***Routing*** ➜ ***Multicast*** ➜ ***IGMP*** menu you can view the interfaces on which IGMP has been enabled by the same automated function or manually in the ***Routing*** ➜ ***Multicast*** ➜ ***IGMP*** ➜ ***New*** menu.

2.10 HTML Page for Update

In **System Software 7.8.2** an HTML page is now displayed as part of the system software when logging in under the address *http://<IP address of your gateway>/maint* that performs an update for the gateway.

2.11 SSL Tunnel

In System Software 7.8.2 you can transport unsecure TCP data securely via an SSL tunnel, without needing a VPN. Each SSL tunnel can contain up to five TCP connections, e.g. for HTTP where several TCP connections are normally set up.

You can configure SSL tunnels in the Setup Tool menu ***SECURITY*** ➜ ***SSL TUNNEL***.

The ***SECURITY*** ➜ ***SSL TUNNEL*** menu contains the following fields:

Parameter	Value
SSL Tunnel	Here you can enable and disable the function. Possible values: ■ *down* (default value): The function is disabled. ■ *up*: The function is enabled.
TCP Keepalive Retries	If no data is currently being exchanged on the TCP connection, you can specify how often a TCP packet is sent for test purposes to establish whether or not the partner is maintaining the current TCP session. The fields ***TCP KEEPALIVE RETRIES*** and ***TCP KEEPALIVE TIMEOUT (SEC)*** determine how often and at what interval a TCP packet is sent for test purposes. Possible values are *0* to *255*. The default value is *3*.

Parameter	Value
TCP Keepalive Timeout (sec)	If no data is currently being exchanged on the TCP connection, you can specify the number of seconds after which a TCP packet is sent to establish whether or not the partner is maintaining the current TCP session. The fields ***TCP KEEPALIVE RETRIES*** and ***TCP KEEPALIVE TIMEOUT (SEC)*** determine how often and at what interval a TCP packet is sent for test purposes. Possible values are *0* to *65535*. The default value is *5*.

Table 2-8: Fields in the ***SECURITY*** ➜ ***SSL TUNNEL*** menu

In the ***SECURITY*** ➜ ***SSL TUNNEL*** ➜ ***TUNNELS*** menu you can view the tunnels that have already been created. In the ***SECURITY*** ➜ ***SSL TUNNEL*** ➜ ***TUNNELS*** ➜ **ADD** menu you can create new tunnels.

The ***SECURITY*** ➜ ***SSL TUNNEL*** ➜ ***TUNNELS*** ➜ **ADD** menu contains the following fields:

Parameter	Value
Admin status	Here you can enable and disable the tunnel. Possible values: ■ *down* (default value): The tunnel is disabled. ■ *up*: The tunnel is enabled.
Description	Enter a description that uniquely defines the tunnel.

Parameter	Value
External IP	IP address of remote terminal ■ *client*: IP address to which the client connects. ■ *server*: If an IP address is specified, a connection can only be established to a client with this IP address. If no IP address is specified, a connection can be established to any client.
External port	External port used according to the setting in the ***EXTERNAL MODE*** field.
External mode	Indicates whether the tunnel is set up at the specified ***EXTERNAL PORT*** or listens at the ***EXTERNAL PORT*** because the tunnel is being set up from the remote terminal. Possible values: ■ *client*: The tunnel is set up at the ***EXTERNAL PORT***. ■ *server*: The tunnel listens at the ***EXTERNAL PORT***.
Internal IP	Local IP address of the gateway The default value is *127.0.0.1*.
Internal port	Internal port used according to the setting in the ***INTERNAL MODE*** field.

Parameter	Value
Internal mode	Indicates whether the tunnel is set up from the specified ***INTERNAL PORT*** or listens at the ***INTERNAL PORT*** because the tunnel is being set up from the remote terminal. Possible values: ■ *client*: The tunnel is set up from the ***INTERNAL PORT***. ■ *server*: The tunnel listens at the ***INTERNAL PORT***.
Certificate	Enter the certificate to be used for authentication.
CA Certificate	Enter the CA (Certificate Authority) certificate to be used for authentication.

Table 2-9: Fields in the ***SECURITY*** ➜ ***SSL TUNNEL*** ➜ ***TUNNELS*** ➜ **ADD** menu

The ***SECURITY*** ➜ ***SSL TUNNEL*** ➜ ***TUNNELS*** ➜ **ADD** ➜ ***(ADVANCED) TIMER SETTINGS*** menu contains the following fields:

Parameter	Value
Retry timeout (s)	Defines the time in seconds after which another attempt should be made to set up the tunnel if the connection setup fails. Possible values are *0* to *3600*. The default value is *60*.

Parameter	Value
Maximum retries	Defines the maximum number of attempts that should be made to set up the tunnel if the connection setup fails. Possible values are *-1* to *50*. A value of *-1* means that several attempts are made to create a tunnel without restricting the number of attempts. The default value is *3*.
Reopen delay (s)	Defines the delay after which a dropped tunnel is reopened if the connection setup is successful. Possible values are *-1* to *315360000*. A value of *-1* means that the tunnel is reopened immediately. The default value is *0*.
Short hold	Defines the idle time in seconds. Possible values are *-1* to *3600*. A value of *-1-* means that the connection is always maintained, i.e. is never cleared.

Table 2-10: Fields in the ***SECURITY*** ➜ ***SSL TUNNEL*** ➜ ***TUNNELS*** ➜ **ADD** ➜ ***(ADVANCED) TIMER SETTINGS*** menu

2.12 Query the BOSS minimum version

In **System Software 7.8.2** you can query the minimum BOSS version required for the correct operation of specific hardware. If a minimum version is specified, you will need this version or a later version.

To do this, enter *show rev* in the SNMP shell.

The following output is displayed (example):

Logic : V.1.0
Bootmon : V.7.8.2
BOSS : V.7.8.2 IPSec from 2008/12/12 00:00:00
(minimal version: 7.8.2)

The last row indicates the minimum version required.

Alternatively, you can query the minimum version with the update command.

To do this, enter *update -i* in the SNMP shell:

The following output is displayed:

Flash-ROM management shell
```
Flash-Sh >
```

Enter *info -m*.

If a minimum version is defined in the flash, the following output is displayed (example):

BOSS minimal version 7.8.2.

If a minimum version is defined, the following output is displayed:

BOSS minimal version: none specified.

2.13 VLAN prioritization

If in **System Software 7.8.2** data is received with VLAN prioritization according to IEEE 802, this data is accepted and processed further.

2.14 Checking the MAC address

To reduce the risk of spoofing attacks, an additional check has been added for the MAC address if the variable ***AllowedPeers*** = *dhcpclients* is set in the MIB table ***ipExtIfTable***.

2.15 DNS - Bailiwick Checking

In **System Software 7.8.2** Bailiwick Checking has been added, i.e. no unqueried supplied entries (Additional Resource Records) can be infiltrated in DNS replies.

2.16 FCI - Support for Opera 9.5

In **System Software 7.8.2** you can use the **Funkwerk Configuration Interface** with the browser Opera 9.5.

2.17 FCI - List entries - New filter

In the FCI the *Status* option has been added under ***Filters in*** for filtering list entries.

2.18 FCI - Defining the message level of syslog entries

In the ***Maximum Message Level of Syslog Entries*** field in the FCI menu ***System Management*** ➜ ***Global Settings*** ➜ ***System*** you can define the level up to which syslog entries should be displayed under ***Monitoring*** ➜ ***Internal Log***.

2.19 FCI - Input field for DHCP MAC Address

In **System Software 7.8.2** you can change the preset MAC address in the ***MAC Address*** field in the FCI menu ***LAN*** ➜ ***IP Configuration*** ➜ ***Interfaces*** ➜ ***New***.

2.20 FCI - New TCP MSS Clamping field

In **System Software 7.8.2** the FCI menu ***LAN*** ➜ ***IP CONFIGURATION*** ➜ ***INTERFACES*** ➜ ***NEW / ICON TO CHANGE AN ENTRY*** ➜ ***ADVANCED SETTINGS*** has been supplemented with the field ***TCP MSS CLAMPING***, which is required for RDP, VNC, Lotus Notes and SQL Syn processes over IPSec tunnels. If the ***TCP MSS CLAMPING*** setting is *enabled* the default value *1350* is displayed; you can modify this value.

2.21 FCI - WLAN - New fields Usage Area and IEEE 802.11d Compliance

A new field ***USAGE AREA*** has been added for the ***OPERATION MODE*** = *Access Client* and ***CLIENT MODE*** = *Infrastructure* settings in the FCI menu ***WIRELESS LAN*** ➜ ***WLANX*** ➜ ***RADIO SETTINGS***.

A new field ***IEEE 802.11D COMPLIANCE*** has been added for the ***OPERATION MODE*** = ***ACCESS CLIENT*** setting in the FCI menu ***WIRELESS LAN*** ➜ ***WLANX*** ➜ ***RADIO SETTINGS***.

2.22 FCI - WLAN - New option for client mode

A new option *Ad-Hoc* has been added to the ***CLIENT MODE*** field for the ***OPERATION MODE*** = *Access Client* setting in the FCI menu ***WIRELESS LAN*** ➜ ***WLANX*** ➜ ***RADIO SETTINGS***.

2.23 FCI - WLAN - New ARP processing field

The new ***ARP Processing*** field has been added in the FCI menu ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Virtual Service Sets*** ➜ **New**.

2.24 FCI - WLAN - New fields WPA Cipher and WPA2 Cipher

The fields ***WPA Cipher*** and ***WPA2 Cipher*** have been added for the ***Security Mode*** = *WPA-PSK* or ***Security Mode*** = *WPA-Enterprise* settings in the FCI menu ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Virtual Service Sets***.

The ***WPA Cipher*** field has been added for the ***Security Mode*** = *WPA-PSK* and ***WPA Mode*** = *WPA* setting and the ***WPA2 Cipher*** field has been added for the ***Security Mode*** = *WPA-PSK* and ***WPA Mode*** = *WPA2* in the FCI menu ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Client Link***.

2.25 FCI - Multicast - Extensions

If the FCI Menu ***Routing*** ➜ ***Multicast*** ➜ ***IGMP*** ➜ ***Icon to change an entry*** is exited with **OK** without created an ***Extended Route*** under ***Routing*** ➜ ***Routes*** ➜ ***IP Routes***, the message "If you exit this page by clicking "OK", multicast will be disabled for all interfaces without extended routes" appears.

A new option *Only host* has been added to the ***Mode*** field in the FCI menu ***Routing*** ➜ ***Multicast*** ➜ ***IGMP*** ➜ ***Icon to change an entry*** / ***New*** .

A new option *Auto* has been added to the ***IGMP Status*** field in the FCI menu ***Routing*** ➜ ***Multicast*** ➜ ***Options*** .

2.26 FCI - Displaying administrative access rules

You can display the administrative access rules by selecting ***DISPLAY ADMINISTRATIVE ACCESS RULES*** = *Enabled* in the FCI menu ***FIREWALL*** ➜ ***POLICIES*** ➜ ***FILTER RULES***.

2.27 FCI - DHCP options extended

In **System Software 7.8.2** the FCI menu ***LOCAL SERVICES*** ➜ ***DHCP SERVER*** ➜ ***DHCP POOL*** ➜ ***ICON TO CHANGE AN ENTRY*** ➜ ***ADVANCED SETTINGS*** has been supplemented with additional ***DHCP OPTIONS***. Click **Add** to display the ***OPTION*** dropdown menu containing the new options *Time Server*, *DNS Server*, *DNS Domain Name*, *WINS/NBNS Server*, *WINS/NBT Node Type* and *TFTP Server*. The ***VALUE*** field is also displayed so that you can enter the value of the chosen option.

2.28 FCI - Scheduling - New option

The option *Update Dynamic DNS* has been added to the ***SELECT ACTION*** field in the FCI menu ***LOCAL SERVICES*** ➜ ***SCHEDULING*** ➜ ***TIME SCHEDULE*** ➜ **New**. This option is displayed if entries are configured in the ***LOCAL SERVICES*** ➜ ***DYNDNS CLIENT*** ➜ ***DYNDNS UPDATE*** menu.

2.29 FCI - Maintenance - New system logic field

The new ***SYSTEM LOGIC*** field has been added to display the logic version in the FCI menu ***MAINTENANCE*** ➜ ***SOFTWARE & CONFIGURATION***, as logic and system software versions can vary.

2.30 FCI - Details of interface statistics

You can display the details of each interface using the magnifying glass icon in the FCI menu ***MONITORING*** ➜ ***INTERFACES*** ➜ ***STATISTICS***.

2.31 Setup Tool - WLAN - ARP Processing for Access Points

The new field ***ARP PROCESSING*** has been added under ***WLAN*** in the Setup Tool menu ***WLAN*** ➜ ***VSS CONFIGURATION*** ➜ **Edit** for the setting ***OPERATION MODE*** = *Access Point*. ARP processing reduces the ARP data traffic in the WLAN network by converting the broadcast ARP requests into unicast ARP requests and thereby increases the data transmission rate, since unicast packets can be sent at a higher speed than broadcast or multicast packets.

2.32 Setup Tool - HTTPS added

The option *https (tcp)* has been added to the ***SERVICE*** field in the Setup Tool menu ***SECURITY*** ➜ ***LOCAL SERVICES*** ➜ ***ACCESS CONTROL*** ➜ **Add**.

2.33 Setup Tool - New option for monitoring interfaces

The new option *set interface dialup* has been added to the ***OPERATION*** field in the Setup Tool menu ***MONITORING AND DEBUGGING*** ➜ ***INTERFACES*** ➜ **EXTENDED**.

2.34 DHCP - New MIB variable SendRepliesToRelay

The variable ***SENDREPLAYTORELAY*** has been added to the MIB table ***IPDHCPPOOLTABLE*** for sending DHCP replies from the internal DHCP server to the DHCP relay when required.

2.35 Bandwidth on Demand (BoD) extended

In **System Software 7.8.2** you can automatically reduce the number of unused links / B channels for incoming connections in the MIB table ***PPPEXTIFTABLE*** using the MIB variable ***BODMODE*** = *bod-reduce-incoming*.

This is useful, for example, if Windows clients have been configured for Multilink PPP dialin, but the gateway is configured without Multilink PPP and without channel bundling.

2.36 New MIB table wlanIfFeatureTable

System Software 7.8.2 comes with the new MIB table ***WLANIFFEATURETABLE***. This contains the parameters used to configure a wireless card.

2.37 New variables in MIB table authEapol

System Software 7.8.2 comes with the new MIB variables ***QUIETPERIOD***, ***TXPERIOD***, ***SUPPTIMEOUT***, ***MAXREQ***, ***REAUTHPERIOD***, ***REAUTHENABLED*** and ***KEYTXENABLED*** in the MIB table ***AUTHEAPOL***.

3 Changes

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

3.1 Password length restricted

In **System Software 7.8.2** the length of the password for the configuration file is restricted to 10 characters.

3.2 Ping function expanded

In **System Software 7.8.2** the Don't Fragment Flag can be set in outgoing IP packets. To do this, enter the *ping -M <IP Address>*.

3.3 DNS with two IP addresses

Some SIP providers use an infrastructure with optimised load balancing to guarantee high availability for their users.

When a gateway sends a DNS request to one of these providers, two IP addresses will be returned. In **System Software 7.8.2** both IP addresses are now sent by the gateway rather than only one as in previous versions. Both addresses can be determined using the `nslookup` command, for example, in Windows XP.

3.4 DNS Query IDs generated randomly

In **System Software 7.8.2** the DNS Query IDs are generated randomly for security reasons.

3.5 IP address ranges (pools) revised

The administration of IP addresses has been revised, as IP address ranges are now used by different subsystems.

The MIB table ***ipDynAddrTable*** has been replaced with two tables, the table ***ipDynaAddrTable*** for dynamically generated entries, which are not saved in the configuration, and ***ipStatAddrTable*** for manually generated entries, which are saved in the configuration. In the table ***ipDynaAddrTable*** the MIB variable ***State*** has been expanded with the values *iprequest* and *ipreply*. In addition, the MIB table ***ipDynAddrPoolTable***, which contains all of the IP addresses that

can be assigned dynamically, and the MIB table ***IPADDRTABLE*** are used in this context.

3.6 Default value for number of NAT ports increased

The default value for the number of NAT ports in global pools has been increased from 4000 to 32767.

3.7 NAT pass-through added

In **System Software 7.8.2** you can now use the new MIB table ***IPNATEXCLUDETABLE*** to work off part of the data traffic from NAT, i.e. configure NAT pass-through.

3.8 UDP port numbers generated randomly

In **System Software 7.8.2** numbers are assigned randomly in the range 1024 to 60000 to UDP ports for ***LOCAL SERVICES***. Previously, these were used in ascending order starting at 1024.

3.9 FCI - IP Configuration update

In **System Software 7.8.2** the IP Configuration has been updated following changes to the FCI Menu ***SYSTEM MANAGEMENT*** ➜ **Interface Mode / Bridge Groups** in the ***MODE / BRIDGE GROUP*** field.

3.10 FCI - Defining fast roaming channels

In the FCI menu ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Radio Settings*** ➜ ***Icon to change an entry*** you can use the setting ***Operation Mode*** = Access *Client* and ***Scan channels*** = ***Disabled*** (under *Advanced Settings*) in the ***Selected channels*** field to define the channels on which the WLAN client scans for available wireless networks.

3.11 FCI - NAT entry for outgoing connection

Previously outgoing NAT mapping was performed automatically at the same time as portforwarding for incoming connections in the FCI menu ***Routing*** ➜ ***NAT*** ➜ ***Portforwarding***, i.e. an entry in the MIB table ***ipNatOutTable***. Now you can choose whether or not this entry should be created in the ***Corresponding NAT entry for outgoing connection*** field.

3.12 FCI - DHCP configuration changed

In the FCI menu ***Local Services*** ➜ ***DHCP Server*** ➜ ***IP/MAC Binding*** the **Delete** button has been removed due to the modified DHCP configuration.

3.13 FCI - layout, spelling, terminology

Small flaws to the layout have been remedied. The usability of some menus has been improved. Spelling and terminology has been revised.

3.14 FCI / Setup Tool - DHCP Pool Configuration expanded

If you want to create a DHCP pool independently of an IP or route entry, you can select the *No Gateway* option in the ***Gateway*** field in the FCI Menu ***Local Services*** ➜ ***DHCP Server*** ➜ ***DHCP Pool*** ➜ ***New*** ➜ ***Advanced Settings***. Alternatively, you can choose the *no* option in the ***Gateway*** field in the Setup Tool menu ***IP*** ➜ ***IP Address Pools*** ➜ ***DHCP*** ➜ **ADD**. Both settings use the MIB variable ***GatewayEnabled*** in the MIB table ***ipDhcpPoolTable***.

3.15 Setup Tool - interface description changed

The description of the *Call-by-Call (dialin only)* option has been changed to the *Multiuser (dialin only)* option in the ***Special Interface Types*** field of the Setup Tool menu ***WAN Partner*** ➜ **ADD/EDIT** ➜ ***Advanced Settings*** .

3.16 Setup Tool - Configuration Management expanded

The ***Operation*** field in the Setup Tool menu ***Configuration Management*** has been expanded with the options *get-all (TFTP -> FLASH)* and *put-all (FLASH -> TFTP)*.

3.17 Setup Tool - improved configuration change

The implementation of the IP and DHCP configuration for changing an interface from routing to bridging and vice versa has been improved to obtain consistent configurations.

4 Problems Solved

Not all devices listed in chapter “Important Information” on page 9 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 7.8.2

4.1 Stacktrace for routing over L2TP or bridging over L2TP

(ID 10619)

For routing over L2TP or bridging over L2TP, high data rates could cause a panic followed by a stacktrace.

The problem has been solved.

4.2 PPPoE and Ethernet interfaces - Problems with external DSL modems

(ID 9225)

If the ***MaxTxRate*** variable in the ***qosIfTable*** table was changed, in the MIB table ***ifTable***, the MIB variable ***Speed*** was not adjusted for PPPoE and Ethernet interfaces. This led to latency problems in scenarios with external DSL modems.

The problem has been solved.

4.3 PPPoE multilink - no error checking

(ID n/a)

Previously, several interfaces with the same MAC address could be used for a PPPoE multilink because no error checking was carried out.

The problem has been solved.

4.4 Number of Telnet sessions unlimited

(ID 1882)

If several incoming Telnet sessions were opened simultaneously, the gateway stopped responding.

The problem has been solved; the number of Telnet sessions is now limited, the default value is *10*.

4.5 RIP source IP address incorrect

(ID 10378)

RIP packets with the source IP address 0.0.0.0. were sent via WAN interfaces.

The problem has been solved.

4.6 Syslog messages - Values not output

(ID 10305)

In syslog messages values were not output in 64 bit format; "u" was displayed instead.

The problem has been solved; the values are output correctly.

4.7 SNMP Shell - Faulty input/output link (pipe)

(ID n/a)

Processes sometimes froze when using a pipe.

The problem has been solved.

4.8 SNMP shell - Problems with Signal Interrupt

(ID n/a)

When sending a SIGINT (Signal Interrupt; e.g. with the key combination **Ctrl** + **c** or by entering *kill*) to the SNMP shell whilst displaying the prompt, the prompt sometimes changed and it was impossible to display the previously shown table.

The problem has been solved.

4.9 QoS - Counter overrun

(ID n/a)

Due to the high data rates of modern interfaces, the octet counter often overran when using QoS.

The problem has been solved; 64 bit counters are now used.

4.10 Multicast protocols - Loss of 64 byte blocks

(ID n/a)

When multicast protocols such as IGMP were activated, 64 byte blocks were lost if a "non-data" multicast packet was sent.

The problem has been solved.

4.11 Name server responses not accepted

(ID n/a)

"Manke" DNS requests were not accepted by mistake and were rejected with the error message "Bailiwick check failed for <xxx>.com". The domain association was miscalculated internally when validating a top level record.

The problem has been solved.

4.12 FCI - No extended routes after reboot

(ID 9386)

When extended routes were created and saved in the boot configuration, they were no longer available after a reboot.

The problem has been solved.

4.13 FCI - Errors in Online Help

(ID n/a)

Errors occurred in the navigation for FCI Online Help due to duplicate IDs.

The problem has been solved.

4.14 FCI - Active sessions displayed by mistake

(ID n/a)

Active sessions were displayed for devices in the **Wx002** series in the FCI menu ***System Management*** ➜ ***Status***.

The problem has been solved.

4.15 FCI - Active sessions not displayed

(ID 9345)

0 was always displayed in the ***Active Sessions (SIF, RTP, etc...)*** field in the FCI menu ***System Management*** ➜ ***Status***.

The problem has been solved.

4.16 FCI - Different formats for time data

(ID n/a)

Time data was displayed in different formats in the ***System Date*** field in the FCI menu ***System Management*** ➜ ***Status*** and in the ***New Date*** field in the FCI menu ***System Management*** ➜ ***Global Settings*** ➜ ***Date and Time***.

The problem has been solved; the same format is used in both fields.

4.17 FCI layout incorrect

(ID 10122)

The tab header in the browser was not the same for all device types in the FCI menu ***System Management*** ➜ ***Global Settings*** ➜ ***Date and Time*** and the layout on the page itself was incorrect.

The problems have been solved.

4.18 FCI - Bridge groups list incorrect

(ID n/a)

The list in the FCI menu ***System Management*** ➜ ***Interface Mode / Bridge Groups*** showed the virtual Ethernet interfaces, although these interfaces cannot be operated in bridging mode.

The problem has been solved.

4.19 FCI - Standard interfaces can be deleted

(ID n/a)

Standard interfaces could be deleted using the recycle bin icon in the FCI menu ***System Management*** ➜ ***Administrative Access***.

The problem has been solved; the recycle bin icon has been removed for standard interfaces.

4.20 FCI - Problems with SIF

(ID 8575)

Problems occurred with the interface-based SIF policies in FCI menu ***System Management*** ➜ ***Administrative Access***.

The problems have been solved by a standard configuration of SIF rules for physical interfaces and a standard rule for access to local services.

4.21 FCI - Switching from DHCP mode to static IP address

(ID n/a)

If the ***Address Mode*** in the FCI menu ***LAN*** ➜ ***IP Configuration*** ➜ ***Interfaces*** ➜ ***Icon to change an entry*** had been changed from *DHCP* to *Static*, it was possible to save the configuration with a blank ***IP Address*** field. If the only IP Ethernet interface was saved with this configuration, access could only be obtained via the serial console on the device.

The problem has been solved and now the message "Please enter a valid IP address!" appears when the ***IP Address*** field is left blank, irrespective of the interface selected.

4.22 FCI - Removing a VLAN failed

(ID 10230)

If all ***VLAN Members*** for a VLAN were deleted in the FCI menu ***LAN*** ➜ ***VLAN*** ➜ ***VLANs*** ➜ ***Icon to change an entry***, the VLAN itself could not be deleted. If a VLAN contained ***VLAN Members***, the recycle bin icon was still displayed for deletion.

The problems have been solved.

4.23 FCI - Wireless LAN menu revised

(ID 9287)

The FCI menu ***Wireless LAN*** did not follow the Style Guide.

The problem has been solved; the ***Wireless LAN*** menu has been revised and adapted to the FCI Style Guide.

4.24 FCI - Monitoring bridges displayed by mistake

(ID 10638)

Although no bridge could be configured in the FCI menu ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Radio Settings*** with the setting ***Operation Mode*** = *Access Client*, the ***Monitoring*** ➜ ***Bridges*** menu was displayed.

The problem has been solved.

4.25 FCI - WDS Link menu not displayed

(ID 10642)

If the field ***Operation Mode*** = *Access Point* is set in the FCI menu ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Radio Settings*** ➜ ***Icon to change an entry*** and one ***Channel*** was set to *Auto*, the ***Wireless LAN*** ➜ ***WLANx*** ➜ ***WDS Links*** menu was not displayed and no WDS link could be configured. The WDS link could be configured in the Setup Tool.

The problem has been solved.

4.26 FCI - Missing transfer rates

(ID 10608)

The values *6 mbps* and *9 mbps* in the dropdown menu were missing in the ***Max. Transmission Rate*** field in the FCI menu ***Wireless LAN*** ➜ ***WLANx*** ➜ ***Radio Settings*** ➜ ***Icon to change an entry***.

The problem has been solved.

4.27 FCI - WLAN - Missing default entries

(ID n/a)

The default entries in the FCI menu ***Wireless LAN ➜ WLANx ➜ Radio Settings ➜ Icon to change an entry ➜ Advanced Settings*** were not used correctly and a system message was displayed as long as wireless module was not activated for the first time.

The problem has been solved; the corresponding fields are only shown when the wireless module is activated.

4.28 FCI - No input for hexadecimal figures

(ID 9679)

No hexadecimal figures could be entered in the ***WEP Key 1-4*** fields in the FCI menu ***Wireless LAN ➜ WLANx ➜ Virtual Service Sets ➜ Icon to change an entry / New ➜ Security Settings*** if ***Security Mode*** = *WEP 40* or ***Security Mode*** = WEP 104. Input could be made with the Setup Tool.

The problem has been solved.

4.29 FCI - Online Help - Graphics not shown

(ID 9514)

One graphic was not displayed in the ***Wireless LAN ➜ WLANx ➜ Cient Link*** menu and the ***LAN ➜ WLANx ➜ Client Link ➜ Client Link Scan*** menu in the FCI.

The problem has been solved.

4.30 FCI - WLAN - Incorrect error message

(ID 10320)

In the WLAN configuration the ***REGION*** field in the FCI menu ***WIRELESS LAN*** ➜ ***ADMINISTRATION*** was changed to "United States", while the ***CHANNEL*** field in the ***WIRELESS LAN*** ➜ ***WLANX*** ➜ ***RADIO SETTINGS*** ➜ ***ICON TO CHANGE AN ENTRY*** menu was set to *12* or *13*, the error message "Changes not supported by the Setup Tool!" was displayed because use of this channel is not permitted in the USA.

The problem has been solved.

4.31 FCI - Port Forwarding - Protocol list incorrect

(ID 9609)

The term *Überspringen* was displayed instead of *Skip* in the dropdown menu of the ***PROTOCOL*** field in the FCI menu ***ROUTING*** ➜ ***NAT*** ➜ ***PORTFORWARDING*** ➜ **New** when ***SERVICE*** = *User Defined*.

The problem has been solved.

4.32 FCI - Load balancing 100% exceeded

(ID 9790)

In the FCI menu ***ROUTING*** ➜ ***LOAD BALANCING*** ➜ ***LOAD BALANCING GROUPS*** ➜ **New Add** could be used to configure the ***DISTRIBUTION RATIO*** across all interfaces greater than 100%.

The problem has been solved; the sum total is now limited to 100%. When the 100% limit is exceeded, an error message appears.

4.33 FCI - PPPoE - Device crashes

(ID 10612)

The device crashed when disabling the ***Prioritize TCP ACK Packets*** option with an existing Internet connection in the FCI menu ***WAN*** ➜ ***Internet + Dialup*** ➜ ***PPPoE*** ➜ **New** ➜ ***Advanced Settings***.

The problem has been solved.

4.34 FCI - PPTP callback

(ID 9786)

If the ***Callback*** field was not enabled in the FCI menu ***VPN*** ➜ ***PPTP*** ➜ ***PPTP Tunnel*** ➜ **New** ➜ **Advanced Settings**, the fields ***Incoming ISDN Number*** and ***Outgoing ISDN Number*** were still displayed.

The problem has been solved; the fields are only shown if ***Callback*** is enabled.

4.35 FCI - DynDNS Update - No input check

(ID n/a)

The fields ***Hostname*** and ***User Name*** could be left blank in the FCI menu ***Local Services*** ➜ ***DynDNS Client*** ➜ ***DynDNS Update*** ➜ **New**, an invalid selection could be made in the ***Interface*** field.

The problem has been solved.

4.36 FCI - DHCP Pool settings not saved

(ID 10823)

The setting in the ***Pool for Forwarded DHCP Requests*** field in the FCI menu ***Local Services*** ➜ ***DHCP Server*** ➜ ***DHCP Pool*** was not saved with **OK**.

The problem has been solved.

4.37 FCI - WLAN - "Unknown Interface"

(ID n/a)

If the field ***Select Action*** = *Activate WLAN* in the FCI menu ***Local Services*** ➜ ***Scheduling*** ➜ ***Time Schedule*** ➜ **New**, the dropdown list in the ***Select Interface*** field contains the value *Unknown Interface*.

The problem has been solved.

4.38 FCI - Problem with missing configuration file

(ID 10755)

If you wanted to rename, copy or delete a configuration in the FCI menu ***Maintenance*** ➜ ***Software & Configuration*** and no configuration was available, a blank dropdown menu appeared along with an unhelpful error message.

The problem has been solved; the error message "No configuration file found" now appears.

4.39 FCI - Unintentional spaces

(ID n/a)

Unintentional spaces appears in the table in the FCI menu ***Maintenance*** ➜ ***Software & Configuration***.

The problem has been solved.

4.40 FCI - IP Accounting - Page filter did not function correctly

(ID n/a)

The page filter did not function correctly when switching from *Select All* to *Deselect All* and vice versa in the ***IP ACCOUNTING*** field in the FCI menu ***EXTERNAL REPORTING*** ➜ ***IP ACCOUNTING*** ➜ ***INTERFACES***.

The problem has been solved.

4.41 FCI - Error displaying system messages

(ID 10253)

Scrolling did not function correctly or the page were not displayed correctly when scrolling if the ***VIEW*** setting was greater than 20 (e.g. 500) in the FCI menu ***MONITORING*** ➜ ***INTERNAL LOG***.

The problem has been solved.

4.42 FCI - Filter incorrect

(ID 10174 / n/a)

The filter function "Description" for WLAN interfaces did not function correctly in the FCI menu ***MONITORING*** ➜ ***INTERFACES*** ➜ ***STATISTICS***. "Not supported" was displayed in the Type column and the message "Changes not supported by the Setup Tool!" was also displayed.

The problem has been solved.

4.43 FCI - Incorrect icon displayed for detail view

(ID n/a)

The "Wrench" icon was displayed instead of the "Magnifying glass" icon for displaying the detailed view in the FCI menu ***MONITORING*** ➜ ***INTERFACES*** ➜ ***STATISTICS***.

The problem has been solved.

4.44 Setup Tool - Stacktrace for ISDN-LAN-LAN connection

(ID 9751)

An ISDN-LAN-LAN connection with static channel bundling triggered a stacktrace followed by a reboot.

The problem has been solved.

4.45 Setup Tool - WAN bridge cannot be configured

(ID n/a)

WAN bridging could not be carried out in the Setup Tool following the introduction of the new bridge concept.

PPP interfaces could no longer be used simultaneously for routing and bridging.

The problem has been solved.

4.46 Setup Tool - Problems displaying an IP address

(ID 10833)

If the IP address has been changed and not saved in the ***LOCAL IP NUMBER*** field in the ***ETHERNET*** ➜ **Edit** menu in the Setup Tool in bridging mode, the current IP address can be seen in the first ***LOCAL IP NUMBER*** field and the new IP address entered in the second ***LOCAL IP NUMBER*** field by scrolling.

The problem has been solved.

4.47 Setup Tool - Interface in bridging mode - Errors in configuration

(ID 9595)

The settings in the Setup Tool menu ***ETHERNET*** ➜ **Edit** ➜ ***ADVANCED SETTINGS*** were applied exclusively to interfaces in routing mode and not to interfaces in bridging mode. The settings could be corrected using the relevant MIB variables.

The problem has been solved.

4.48 Setup Tool - WLAN - Incorrect fields displayed

(ID n/a)

In the Setup Tool the fields ***WPA CIPHER*** or ***WPA2 CIPHER*** were displayed with the setting ***OPERATION MODE*** = *Client* under ***WLAN*** in the ***WLAN*** ➜ ***CLIENT CONFIGURATION*** menu if ***SECURITY MODE*** = *NONE*, ***SECURITY MODE*** = *WEP 40/64* or ***SECURITY MODE*** = *WEP 104/128*.

The problem has been solved; the fields are no longer displayed.

4.49 Setup Tool - PPPoE - MAC addresses not unique

(ID n/a)

If an Ethernet switch was operated in split port mode, problems occurred with PPPoE or Multilink PPPoE connections because the assigned MAC addresses appeared more than once.

The problem has been solved. A new MAC address will be assigned if required in the ***CREATE NEW (UNIQUE) MAC ADDRESS <NEW MAC ADDRESS> FOR PORT <CORRESPONDING PORT>*** field in the Setup Tool menu ***WAN PARTNER*** ➜ ***ADD*** ➜ ***ADVANCED SETTINGS*** ➜ ***EXTENDED INTERFACE SETTINGS***.

4.50 Setup Tool - SIF - Incorrect port range

(ID n/a)

Values from *0* to *65535* could be entered by mistake in the ***RANGE*** field in the the Setup Tool menu ***SECURITY*** ➜ ***STATEFUL INSPECTION*** ➜ ***EDIT SERVICES*** ➜ **ADD/EDIT**.

The problem has been solved; the possible values have been changed to *1* - *65536*.

4.51 Setup Tool - Missing field mode

(ID 9296)

The ***MODE*** field was not displayed for the settings ***ROUTE TYPE*** = *Default route* and ***NETWORK*** = *LAN* in the Setup Tool menu ***IP*** ➜ ***ROUTING*** ➜ ***ADDEXT***.

The problem has been solved.

4.52 Setup Tool - Deleting two TDRC entries triggers a stacktrace

(ID 6464)

If two entries were created for a T-DSL interface in the Setup Tool menu ***IP*** ➜ ***Bandwidth Management (TDRC / Load Balancing / BOD)*** ➜ ***TCP Download Rate Control (TDRC)*** ➜ **ADD**, one with ***Optimize Download Rate via TCP ACK priorisation*** = *yes* and the other with ***Optimize Download Rate via TCP ACK priorisation*** = *no* and ***TDRC Mode*** = *static (fixed maximum rate for TCP download)*, both entries were selected and deleted, the message "Exception: 0x1c00 Data breakpoint Debug" appeared followed by a stacktrace without reboot.

The problem has been solved.

4.53 Setup Tool - PPPoE Passthrough - Interfaces not displayed correctly

(ID 10106)

The bridge group interfaces were not displayed in the ***Physical or virtual Ethernet Port attached to PPPoE Client(s)*** area in the Setup Tool menu ***PPP*** ➜ ***PPPoE Passthrough***.

The problem has been solved.