

Manual Release Notes

9.1.7

Copyright© Version 1.1, 2013 bintec elmeg GmbH

Legal Notice

Aim and purpose

This document is part of the user manual for the installation and configuration of bintec elmeg devices. For the latest information and notes on the current software release, please also read our release notes, particularly if you are updating your software to a higher release version. You will find the latest release notes under www.bintec-elmeg.com.

Liability

This manual has been put together with the greatest possible care. However, the information contained in this manual is not a guarantee of the properties of your product. bintec elmeg GmbH is only liable within the terms of its conditions of sale and supply and accepts no liability for technical inaccuracies and/or omissions.

The information in this manual can be changed without notice. You will find additional information and also release notes for bintec elmeg devices under www.bintec-elmeg.com.

bintec elmeg devices make WAN connections as a possible function of the system configuration. You must monitor the product in order to avoid unwanted charges. bintec elmeg GmbH accepts no responsibility for data loss, unwanted connection costs and damage caused by unintended operation of the product.

Trademarks

bintec elmeg trademarks and the bintec elmeg logo, bintec trademarks and the bintec logo, elmeg trademarks and the elmeg logo are registered trademarks of bintec elmeg GmbH.

Company and product names mentioned are usually trademarks of the companies or manufacturers concerned.

Copyright

All rights reserved. No part of this manual may be reproduced or further processed in any way without the written consent of bintec elmeg GmbH. The documentation may not be processed and, in particular, translated without the consent of bintec elmeg GmbH.

You will find information on guidelines and standards in the declarations of conformity under www.bintec-elmeg.com.

How to reach bintec elmeg GmbH

bintec elmeg GmbH, Südwestpark 94, D-90449 Nuremberg, Germany, Phone: +49 911 9673 0, Fax: +49 911 688 07 25

Teldat France S.A.S., 6/8 Avenue de la Grande Lande, F-33174 Gradignan, France, Phone: +33 5 57 35 63 00, Fax: +33 5 56 89 14 05

Internet: www.teldat.fr

Table of Contents

Chapter 1	Important Information	1
1.1	Preparation and update with the GUI	1
1.2	Downgrade with the GUI	2
1.3	Supported web browsers	2
Chapter 2	New Functions	4
2.1	GUI: Upgraded input option for netmasks	4
2.2	Configuration access	4
2.2.1	Access profiles	4
2.2.2	Users	7
2.3	Wireless Bridge Link	8
2.4	Client Link	9
2.5	Wake on LAN	12
2.5.1	Wake-On-LAN Filter	12
2.5.2	WOL Rules	15
2.5.3	Interface Assignment	16
2.6	Mobile terminals and smartphones supported	17
2.7	DECT systems supported	17
2.7.1	elmeg DECT	17
2.8	PBX assistant upgraded	21
2.9	Voice mailbox: Dutch added	21
2.10	New UMTS parameters supported	23
2.11	New IPSec parameters supported	26
2.12	Commands upgraded	26

2.13	MIB: ipNatOutTable table upgraded	27
2.14	Hardware: New LED mode available	27
2.15	Hotspot - Post Login URL added	28
Chapter 3	Changes	29
3.1	Company name changed	29
3.2	Factory settings changed	29
3.3	GUI: Name changed	29
3.4	GUI: Interface and documentation changed	29
Chapter 4	Bugfixes	30
4.1	hybird: Problem with parallel calls	30
4.2	hybird: Layout incorrect	30
4.3	GUI: Filtering of display incorrect	30
4.4	SIP: Communication aborted	31
4.5	FXS ports: Communication problems	31
4.6	UMTS: Connection problems	31
4.7	Wireless LAN controller: Incorrect WPA mode	31
4.8	System: Problem when loading a configuration	32
4.9	Monitoring: Tx statistic incorrect	32
4.10	System: Problems with fragmented frames	32
4.11	Hardware: Problem with roll-out processes	32
4.12	Wireless LAN controller: Entries collected incorrectly	33
4.13	System: Problems when copying or renaming configuration files	33
4.14	WLAN: Roaming not working correctly	33

4.15	QoS: Problems with QoS queue	33
4.16	Wireless LAN controller: Status incorrect.	34
4.17	WLAN: Incorrect wireless networks displayed	34
4.18	Trace: Incorrect message displayed	34
4.19	SSH access incorrectly interrupted	35
4.20	UMTS: Password for closed user groups missing	35
4.21	GUI: Display for Ethernet interfaces non-standardised	35
4.22	GUI: Filtering of display not working	35
4.23	GUI: Unable to save setting	36
4.24	WLAN: Data packet losses	36
4.25	GUI: Source port and mode incorrectly displayed	36
4.26	Scheduling: Version check not working	36
4.27	Hotspot: Timeout for status window	37
4.28	Stacktrace	37
4.29	GUI: Firewall	37
4.30	LED: Incorrect display	37
4.31	Wireless LAN controller: Connection problem.	38
Chapter 5	Known issues	39
5.1	hybird: Problem with LDAP.	39
5.2	DECT multi-cell system: Problem with three-way conferences	39

Chapter 1 Important Information

1.1 Preparation and update with the GUI

Updating the system software with the Graphical User Interface is done using a BLUP (bintec Large Update) file so as to update all the necessary modules intelligently. All those elements that are newer in the BLUP than on your gateway are updated.



Note

The result of an interrupted updating operation could be that your gateway no longer boots. Hence, do not turn your gateway off during the update.

To prepare and carry out any update to **Systemsoftware 9.1.7** using the Graphical User Interface, proceed as follows:

- (1) For the update, you'll need the `XXXXX_b19107.xxx` file, where `XXXXX` stands for you device. Ensure that the file that you require for the update is available on your PC. If the file is not available on your PC, enter www.bintec-elmeg.com in your browser. The bintec elmeg 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 before updating. Export the current boot configuration using the **Maintenance->Software & Configuration** menu in the Graphical User 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 **Open <name of gateway>.cf** window opens. Leave the selection *Save file* and click **OK** to save the configuration to your PC. The file `<name of gateway>.cf` is saved and the **Downloads** window shows the saved file.
- (3) Update the **Systemsoftware 9.1.7** using the **Maintenance->Software & Configuration** menu. To do this, select: **Action** = *Update system software*, **Source Location** = *Local File*, **Filename** = `XXXXX_b19107.xxx`. Confirm with **Go**. The message "System request. Please stand by. Operation in progress." 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." Click **Reboot**. You will see the message "System - Reboot. Rebooting. Please wait. This takes approximately 40 seconds." The device will start with the new system software, and the browser window will open.

1.2 Downgrade with the GUI

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

- (1) Replace the current boot configuration with the previous backup version. You import the saved boot configuration using 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. Operation in progress." or "System Maintenance. Please stand by. Operation in progress." indicates that the selected configuration is being uploaded to the device. When the upload procedure is finished, you will see the message "System - Maintenance. Success. Operation completed successfully." 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) Downgrade to the software version you want using the **Maintenance->Software & Configuration** menu.
To do this, select: **Action** = *Update system software*, **Source Location** = *Local File*, **Filename** = *RXL_Series_b19105.biq* (example). Confirm with **Go**. The message "System request. Please stand by. Operation in progress." 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." Click **Reboot**. You will see the message "System - Reboot. Rebooting. Please wait. This takes approximately 40 seconds." The device will start with the new system software, and the browser window will open.

You can log into your device and configure it.

1.3 Supported web browsers

The HTML GUI supports the use of the following browsers, each in their latest version:

- Microsoft Internet Explorer
- Mozilla Firefox
-

**Important**

Ensure that you keep your browser updated to the latest version, since you need to do so to take advantage of new functions and security features. The HTML GUI does not support versions that are no longer supported by the manufacturer and supplied with software updates. If necessary, go to the software manufacturer's website to find out which versions they currently support.

Chapter 2 New Functions

Systemsoftware 9.1.7 includes a number of new functions that significantly improve performance compared with the previous version of the system software.



Note

Please note that not all the functions listed here are available for every device. Please refer, if necessary, to the current data sheet for your device or to the relevant manual.

2.1 GUI: Upgraded input option for netmasks

As of now, netmasks can also be entered using CIDR notation $/24$.


2.2 Configuration access



The new function **Configuration Access** is available in the **System Management->Configuration Access** menu.

In the **Configuration Access** menu you can configure user profiles.


To do so, you create access profiles and users and assign each user at least one access profile. An access profile makes available that part of the GUI that a user requires for their tasks. Parts of the GUI that are not required are blocked.

2.2.1 Access profiles

The menu **System Management->Configuration Access->Access Profiles** displays a list of all the access profiles that have been configured. You can delete existing entries with the icon .

By default, more than one access profile has already been created for the devices **elmeg hybrid 120/130** and **elmeg hybrid 300/600**. You can change these using the icon  or reset them to the default settings using the icon .

2.2.1.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to create additional access profiles.


To create an access profile you can use all the entries in the navigation bar of the GUI plus **Save configuration** and **Switch to SNMP Browser**. You can create a maximum of 29 access profiles.


The menu **System Management->Configuration Access->Access Profiles->New** consists of the following fields:

Fields in the menu Basic Settings






Field	Description
Description	Enter a unique name for the access profile.
Level No.	The system automatically assigns a sequential number to the access profile. This cannot be edited.



Fields in the menu Buttons

Field	Description
Save configuration	If you activate the button Save configuration the user is permitted to save configurations.
	<div data-bbox="539 1016 621 1067" style="display: inline-block; vertical-align: middle;"></div> <p>Note</p> <p>Note that the passwords in the saved file can be viewed in clear text.</p>
	<p>Enable or disable Save configuration.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>
Switch to SNMP Browser	If you activate the button Switch to SNMP Browser , the user can switch to the SNMP browser view, access the parameters and modify all the settings displayed there.


Field	Description
	<p>Caution</p> <p>Note that the permission for Switch to SNMP Browser means that the user can access the entire MIB, because no individual access profile can be created in this view. The user can save the changed MIB with the permission for Save configuration.</p> <p>With the permission for Switch to SNMP Browser you remove the configured GUI restrictions at the MIB level once more.</p> <p>Enable or disable Switch to SNMP Browser.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>


Fields in the menu Navigation Entries




Field	Description
Menus	<p>You see all the menus from the GUI's navigation bar. Menus that contain at least one sub-menu are flagged by  and .</p> <p>The icon  indicates pages.</p> <p>When you create a new access profile, no elements are assigned yet, i.e. all the available menus, sub-menus and pages are flagged with the icon .</p> <p>Each element in the navigation bar can have three values. Click the icon  in the row you want to display these three values.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Deny</i>: The menu and all its lower-level menus are blocked. • <i>Allow</i>: The menu is released. Lower-level menus may need to be specifically released. • <i>Allow all</i>: The menu and all its lower-level menus are released. <p>You can select <i>Allow</i> and <i>Allow all</i> in the corresponding row to assign elements to the current access profile.</p>

Field	Description
	<p>Elements that are assigned to the current access profile are flagged with the icon .</p> <p> indicates a menu that is blocked, but which has at least one released sub-menu.</p>


2.2.2 Users

The menu **System Management->Configuration Access->Users** displays a list of all the users that have been configured. You can delete existing entries with the icon .

You can click the button  to display the details of the configured user. You can see which fields and menus are assigned to the user.

The icon  means that **Read-only** is permitted. If a row is flagged with the icon  the information is released for reading and writing. The icon  indicates blocked entries.

2.2.2.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to enter additional users.

The menu **System Management->Configuration Access->Users->New** consists of the following fields:



Fields in the menu Basic Settings

Field	Description
User	Enter a unique name for the user.
Password	Enter a password for the user.
User must change password	<p>The administrator can use the option User must change password to specify that the user must select their own password the first time they log in. To do this, the option Save configuration needs to be enabled in the menu Access Profiles. If this option is not enabled, a warning message displays.</p> <p>Enable or disable User must change password.</p> <p>The function is enabled with <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

Field	Description
Access Level	<p>Use Add to assign at least one access profile to the user. Selecting Read-only specifies that the user can view the parameters of the access profile, but not change them. Selecting Read-only is only possible if the option Switch to SNMP Browser in the menu Access Profiles is not enabled.</p> <p>If the option Switch to SNMP Browser is enabled, a warning message displays because the user can switch to the SNMP browser view, access the parameters and make any changes they like. The option Read-only is not available in the SNMP browser view.</p> <p>If intersecting access profiles are assigned to a user, read and write have a higher priority than Read-only. Buttons cannot be set to the setting Read-only.</p>

2.3 Wireless Bridge Link

With **Systemsoftware 9.1.7** , **Bridge Links** are available.

You can configure this function in the **Wireless LAN->WLAN->Radio Settings->** menu and the **Wireless LAN->WLAN->Bridge Links->**/New menu.

The **Wireless LAN->WLAN->Radio Settings->** contains the following field:

Relevant field in the menu Wireless Settings

Field	Description
Operation Mode	<p>Define the mode in which the wireless module of your device is to operate.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Off</i> (default value): The wireless module is not active. • <i>Access-Point / Bridge Link Master</i>: Your device is used as an access point in your network. • <i>Access Client</i>: Your device serves as an Access Client in your network. • <i>Bridge Link Client</i>: Your device is used as an wireless bridge link in your network (available only for the devices bintec W1003n, W2003n, W2003n-ext and W2004n) .

The **Wireless LAN->WLAN->Bridge Links->****->New** contains the following fields:

Relevant fields in the Basic Parameters menu

Field	Description
Bridge Link Name (ID)	<p>Depending on whether you operate the radio module as access point or as wireless bridge link, you create a bridge link in master or in slave mode.</p> <p>If the radio module operates in Access-Point / Bridge Link Master mode, the bridge link is in master mode. Enter a name for the bridge link. This name also serves as the ID other devices use to connect to this bridge link.</p> <p>If the radio module is in Bridge Link Client mode, the bridge link is in slave mode. Enter the ID of the bridge link the device is supposed to connect to.</p>
Preshared Key	<p>Enter a password for this bridge link. In master mode, this is the password other devices use to connect to this bridge link. In slave mode, it is the password of that bridge link the device is to connect to.</p>

2.4 Client Link

With **Systemsoftware 9.1.7**, the **Client Link** function is available for **bintec W1003n, W2003n, W2003n-ext and W2004n**.

You can configure this function in the **Wireless LAN->WLAN->Radio Settings->** menu and the **Wireless LAN->WLAN->Client Link->** menu.

The **Wireless LAN->WLAN->Radio Settings->** menu contains the following field:

Relevant field in the menu Wireless Settings

Field	Description
Operation Mode	<p>Define the mode in which the wireless module of your device is to operate.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Off</i> (default value): The wireless module is not active. • <i>Access-Point / Bridge Link Master</i>: Your device is

Field	Description
	<p>used as an access point in your network.</p> <ul style="list-style-type: none"> • <i>Access Client</i>: Your device serves as an Access Client in your network. • <i>Bridge Link Client</i>: Your device is used as an wireless bridge link in your network (available only for the devices bintec W1003n, W2003n, W2003n-ext and W2004n).

To configure **Client Link**, select **Operation Mode** = *Access Client* and click **OK**.

The **Wireless LAN->WLAN->Client Link->**/New menu contains the following fields:


Relevant field in the Basic Parameters menu

Field	Description
Network Name (SSID)	<p>Enter the name of the wireless network (SSID).</p> <p>Enter an ASCII string with a maximum of 32 characters.</p>


Relevant fields in the Security Settings menu

Field	Description
Security Mode	<p>Select the security mode (encryption and authentication) for the wireless network.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Inactive</i> (default value): Neither encryption nor authentication • <i>WEP 40</i>: WEP 40 bits • <i>WEP 104</i>: WEP 104 bits • <i>WPA-PSK</i>: WPA Preshared Key
Transmit Key	<p>Only for Security Mode = <i>WEP 104</i></p> <p>Select one of the keys configured in WEP Key <1 - 4> as a default key.</p> <p>The default value is <i>Key 1</i>.</p>
WEP Key 1 - 4	<p>Only for Security Mode = <i>WEP 40, WEP 104</i></p> <p>Enter the WEP key.</p>

Field	Description
	<p>Enter a character string with the right number of characters for the selected WEP mode. For <i>WEP 40</i> you need a character string with 5 characters, for <i>WEP 104</i> with 13 characters, e.g. <i>hello</i> for <i>WEP 40</i>, <i>wep1</i> for <i>WEP 104</i>.</p>
WPA Mode	<p>Only for Security Mode = <i>WPA-PSK</i></p> <p>Select whether you want to use WPA or WPA 2.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>WPA</i> (default value): Only WPA is used. • <i>WPA 2</i>: Only WPA2 is used.
Preshared Key	<p>Only for Security Mode = <i>WPA-PSK</i></p> <p>Enter the WPA password.</p> <p>Enter an ASCII string with 8 - 63 characters.</p>
WPA Cipher	<p>Only for Security Mode = <i>WPA-PSK</i> and WPA Mode = <i>WPA</i></p> <p>Select which encryption method should be used.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>TKIP</i> (default value): Temporal Key Integrity Protocol • <i>AES</i>: Advanced Encryption Standard. <p>Both encryption methods are rated as secure, with AES offering better performance.</p>
WPA2 Cipher	<p>Only for Security Mode = <i>WPA-PSK</i> and WPA Mode = <i>WPA 2</i></p> <p>Select which encryption method is to be used.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>AES</i> (default value): Advanced Encryption Standard. • <i>TKIP</i> : Temporal Key Integrity Protocol <p>Both encryption methods are rated as secure, with AES offering better performance.</p>

After the desired Client Links have been configured, the  icon is shown in the list.

You use this icon to open the **Scan** menu.

After successful scanning, a selection of potential scan partners is displayed in the scan list. In the **Action** column, click **Select** to connect the local clients with this client. If the partners are connected with one another, the  icon appears in the **Connected** column. The icon appears if the connection is active.

2.5 Wake on LAN


The new function **Wake-On-LAN** is available in the **Local Services->Wake-On-LAN** menu.

With the function **Wake-On-LAN (WOL)** you can start network devices that are switched off via an integrated network card. The network card also needs a power supply, even when the computer is switched off. You can use filters and rule chains to define the conditions that need to be met to send the so-called magic packet, and select the interfaces that are to be monitored for the defined rule chains. Configuring the filters and rule chains is largely like configuring filters and rule chains in the menu **Access Rules**.

2.5.1 Wake-On-LAN Filter

The menu **Wake-On-LAN->Wake-On-LAN Filter** displays a list of all the WOL filters that have been configured.

2.5.1.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to enter additional filters.

The **Wake-On-LAN->Wake-On-LAN Filter->New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Description	Enter the name of the filter.
Service	Select one of the preconfigured services. The extensive range of services configured ex works includes the following: <ul style="list-style-type: none"> • <i>activity</i> • <i>apple-qt</i> • <i>auth</i>

Field	Description
	<ul style="list-style-type: none"> • <i>charge</i> • <i>clients_1</i> • <i>daytime</i> • <i>dhcp</i> • <i>discard</i> <p>The default value is <i>Any</i>.</p>
Protocol	<p>Select a protocol.</p> <p>The option <i>Any</i> (default value) matches any protocol.</p>
Type	<p>Only for Protocol = <i>ICMP</i></p> <p>Select the type.</p> <p>Possible values: <i>Any, Echo reply, Destination unreachable, Source quench, Redirect, Echo, Time exceeded, Timestamp, Timestamp reply</i>.</p> <p>See RFC 792.</p> <p>The default value is <i>Any</i>.</p>
Connection State	<p>With Protocol = <i>TCP</i>, you can define a filter that takes the status of the TCP connections into account.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Established</i>: All TCP packets that would not open any new TCP connection on routing over the gateway match the filter. • <i>Any</i> (default value): All TCP packets match the filter.
Destination IP Address/Netmask	<p>Enter the destination IP address of the data packets and the corresponding netmask.</p>
Destination Port/Range	<p>Only for Protocol = <i>TCP</i> or <i>UDP</i></p> <p>Enter a destination port number or a range of destination port numbers.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>-All-</i> (default value): The destination port is not specified.


Field	Description
	<ul style="list-style-type: none"> • <i>Specify port</i>: Enter a destination port. • <i>Specify port range</i>: Enter a destination port range.
Source IP Address/ Netmask	Enter the source IP address of the data packets and the corresponding netmask.
Source Port/Range	<p>Only for Protocol = <i>TCP</i> or <i>UDP</i></p> <p>Enter a source port number or a range of source port numbers.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>-All-</i> (default value): The destination port is not specified. • <i>Specify port</i>: Enter a destination port. • <i>Specify port range</i>: Enter a destination port range.
DSCP/TOS Filter (Layer 3)	<p>Select the Type of Service (TOS).</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Ignore</i> (default value): The type of service is ignored. • <i>DSCP Binary Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in binary format, 6 bit). • <i>DSCP Decimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in decimal format). • <i>DSCP Hexadecimal Value</i>: Differentiated Services Code Point according to RFC 3260 is used to signal the priority of IP packets (indicated in hexadecimal format). • <i>TOS Binary Value</i>: The TOS value is specified in binary format, e.g. 00111111. • <i>TOS Decimal Value</i>: The TOS value is specified in decimal format, e.g. 63. • <i>TOS Hexadecimal Value</i>: The TOS value is specified in hexadecimal format, e.g. 3F.
COS Filter (802.1p/Layer 2)	<p>Enter the service class of the IP packets (Class of Service, CoS).</p> <p>Possible values are whole numbers between 0 and 7. Value range 0 to 7.</p>

Field	Description
	The default value is <i>Ignore</i> .

2.5.2 WOL Rules

The menu **Wake-On-LAN+WOL Rules** displays a list of all the WOL rules that have been configured.

2.5.2.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to enter additional rules.

The **Wake-On-LAN+WOL Rules->New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Wake-On-LAN Rule Chain	<p>Select whether to create a new rule chain or to edit an existing one.</p> <p>Possible values:</p> <ul style="list-style-type: none"> <i>New</i> (default value): You can create a new rule chain with this setting. <i><Name of the rule chain></i>: Shows a rule chain that has already been created, which you can select and edit.
Description	<p>Only where Wake-On-LAN Rule Chain = <i>New</i></p> <p>Enter the name of the rule chain.</p>
Wake-On-LAN Filter	<p>Select a WOL filter.</p> <p>If the rule chain is new, select the filter to be set at the first point of the rule chain.</p> <p>If the rule chain already exists, select the filter to be attached to the rule chain.</p> <p>To select a filter, at least one filter must be configured in the Wake-On-LAN+WOL Rules menu.</p>
Action	Define the action to be taken for a filtered data packet.


Field	Description
	<p>Possible values:</p> <ul style="list-style-type: none"> • <i>Invoke WOL if filter matches</i>: Run WOL if the filter matches. • <i>Invoke if filter does not match</i>: Run WOL if the filter does not match. • <i>Deny WOL if filter matches</i>: Do not run WOL if the filter matches. • <i>Deny WOL if filter does not match</i>: Do not run WOL if the filter does not match. • <i>Ignore rule and skip to next rule</i>: This rule is ignored and the next one in the chain is examined.
Type	Select whether the Wake on LAN magic packet is to be sent as a UDP packet or as an Ethernet frame via the interface specified in Send WOL packet via interface .
Send WOL packet via interface	Select the interface which is to be used to send the Wake on LAN magic packet.
Target MAC-Address	<p>Only where Action = <i>Invoke WOL if filter matches</i> and <i>Invoke if filter does not match</i></p> <p>Enter the MAC address of the network device that is to be enabled using WOL.</p>
Password	<p>Only where Action = <i>Invoke WOL if filter matches</i> and <i>Invoke if filter does not match</i></p> <p>If the network device that is to be enabled supports the "SecureOn" function, enter the corresponding password for this device here. The device is only enabled if the MAC address and password are correct.</p>

2.5.3 Interface Assignment

In this menu, the configured rule chains are assigned to individual interfaces which are then monitored for these rule chains.

A list of all configured interface assignments is displayed in the **Wake-On-LAN+Interface Assignment** menu.

2.5.3.1 Edit or New

Choose the  icon to edit existing entries. Choose the **New** button to create other entries.

The **Wake-On-LAN+Interface Assignment->New** menu consists of the following fields:

Fields in the menu Basic Parameters

Field	Description
Interface	Select the interface for which a configured rule chain is to be assigned.
Rule Chain	Select a rule chain.

2.6 Mobile terminals and smartphones supported

The GUI supports mobile terminals and smartphones.




2.7 DECT systems supported


With **Systemsoftware 9.1.7** the systems **elmeg DECT150** and **elmeg DECT200** are supported.

2.7.1 elmeg DECT


The menu **Terminals->elmeg System Phones->elmeg DECT** displays the base stations of the connected DECT single-cell and multi-cell systems.

Any base stations that are connected are automatically detected and listed in the lower part of the overview. (DHCP is required for this.)

Choose the  icon to edit existing entries. As soon as a **Description** is entered for a base station and copied with **OK**, the entry for that device is moved to the upper part of the overview. After a short time, the icons  and  are displayed for this device.

To be able to use automatic provisioning, click the  icon again and add the relevant phone numbers.


Select the **New** button to manually set up a new base station.

Select the button  to go to the base station's Web configurator. This is described in the

user guide for the relevant DECT system!


Use the automatic provisioning to use the **elmeg hybrid** to transfer elementary telephony parameters to the DECT system. If you want to use the assistant **First Steps** to do this, you activate the value *elmeg IPlx/DECT* under **Assistants->First steps->Advanced Settings->Add** in the field **Transmit Provisioning Server for** . Instead of this, you can also set the fields **Option** = *URL (provisioning server)* and **Value** = *http://<IP address of the provisioning server>/eg_prov* under **Local Services->DHCP Server->DHCP Configuration->New->Advanced Settings** .

To register the mobile parts you first set the base station to login mode. Then you do the registering of the mobile parts on the mobile parts themselves. To configure the base station in any more detail, you need to use the DECT system's web configurator.

Select the button  to trigger an update of the device's provisioning. If the update is successful, the updated value displays in the **Last seen** column within 10 seconds.



Note

If you wish to test whether your base station is correctly configured and accessible, select the button  and check whether an updated value is displayed within 10 seconds in the **Last seen** column.



Note

If you wish to change the language currently used with a DECT single-cell system, the system has to be connected to the provisioning server of the **elmeg hybrid**. You required an installed SD card. All the languages used need to be stored on the SD card. Single-cell systems load the language required from the SD card when necessary.

2.7.1.1 General

In the menu **Terminals->elmeg System Phones->elmeg DECT->General** you make the basic settings for base stations.

The **Terminals->elmeg System Phones->elmeg DECT->General** menu consists of the following fields:

Fields in the menu Basic Settings

Field	Description
Description	To clearly identify the base station in the system, enter a de-

Field	Description
	scription for the base station.
Phone Type	<p>Displays the type of base station.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>elmeg DECT150</i> • <i>elmeg DECT200</i>
Location	<p>Select the location of the base station. You define locations in the VoIP->Settings->Locations menu. Depending on the setting in this menu, default behaviour for registration of VoIP subscribers for which no location should be defined is displayed for selection.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Not defined (Unrestricted Registration)</i>: No location is defined. According to set default behaviour, the subscriber is nevertheless registered. • <i>Not defined (No Registration)</i>: No location is defined. According to set default behaviour, the subscriber is not registered. • <i>Not defined (Registration for Private Networks Only)</i>: No location is defined. According to set default behaviour, the subscriber is only registered if located in a private network. • <i>Location</i>: A defined location is selected. The subscriber is only registered if at this location.
MAC Address	Shows the MAC address of the base station.
IP/MAC Binding	<p>Displays the IP address automatically assigned by DHCP.</p> <p>Here you have the option of permanently assigning the displayed IP address to the base station with the displayed MAC address.</p> <p>This option should be activated to enable quick re-login after a functional fault.</p>

The menu **Advanced Settings** consists of the following fields:

Fields in the menu Further Settings

Field	Description
No Hold and Retrieve	<p>The performance features hold a call and retrieve a held call are not available on certain telephones.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p>

Fields in the menu Codec Settings

Field	Description
Codec Profile	Select the Codec profile to be used. Codec profiles are configured in the VoIP->Settings->Codec Profiles menu.

2.7.1.2 Numbers

In the menu **Terminals->elmeg System Phones->elmeg DECT->Numbers** you assign **Internal Numbers** to the mobile parts. You can select from the numbers that you have created for this purpose under **Numbering->User Settings->Users**.

The system automatically assigns a serial number, the **Mobile Number**, to each mobile part so that you can identify the device. You can then use **Add** to assign a **Internal Number** to a mobile part from the list.

You can delete assigned numbers with .

Values in the list Numbers

Field	Description
Mobile Number	Displays the serial number of the mobile part. This number is permanently assigned to the mobile part so that it can be uniquely identified.
Internal Number	Displays the assigned internal number.
Displayed Description	Displays the description entered for the internal number. In standby mode this description is shown on the mobile part's display.
User	Displays the user's name.

2.7.1.3 Settings

In the **Terminals->elmeg System Phones->elmeg DECT->Settings** menu you can reset the administrator password for the base station.

The **Terminals->elmeg System Phones->elmeg DECT->Settings** menu consists of the following fields:

Fields in the menu Basic Settings


Field	Description
Admin Password	<p>Select whether the administrator password should be reset.</p> <p>The function is activated by selecting <i>Enabled</i>.</p> <p>The function is disabled by default.</p> <p>As soon as you select the OK button, the password is reset to the default setting.</p>


2.8 PBX assistant upgraded

The **Assistants->PBX->Users** menu has been added to the PBX assistant.

On the **Users** tab, the system guides you through all of the settings required to set up and configure a user.

All of the configured users are displayed in the overview. The following details are listed: the **Name** of the user, the **Internal Number** and the **External Number**.


A list field is deleted by pressing the  button.

You can also edit existing entries with by clicking .

To add a user, click **New**. Then follow the instructions. The list is called up again once the new user has been configured, allowing you to set up more users.


2.9 Voice mailbox: Dutch added

The voice mailbox can be operated in the *Dutch* language.

In the **Applications->Voice Mail System->Voice Mail Boxes-> / New** menu, you can select the desired language for the voicemail box announcements.

Relevant field in the menu **Basic Settings**

Field	Description
Voice Mail Language	<p>Select the desired language for the voicemail box announcements.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Deutsch</i>: The voicemail box uses German texts. • <i>Dutch</i>: The voicemail box uses Dutch texts. • <i>English</i>: The voicemail box uses English texts. • <i>Italian</i>: The voicemail box uses Italian texts. • <i>French</i>: The voicemail box uses French texts. • <i>Default</i> (default value): The voicemail box uses the language centrally defined for the entire voicemail system in the Applications->Voice Mail->General menu.



Note



You'll only require a setting that departs from *Default* if you wish to operate voicemail boxes with various languages within your voicemail system.

In the **Applications->Voice Mail->General** menu, you can select the language for the entire voicemail system.

Relevant field in the menu **Basic Settings**

Field	Description
Language	<p>Select the language for the entire voicemail system.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Deutsch</i> (default value) • <i>Dutch</i> • <i>English</i> • <i>Italian</i> • <i>French</i> <p>Diverging from the language set here, a language can be individually set for each voice mail box in the Applications->Voice Mail->Voice Mail Boxes ->New menu.</p>

2.10 New UMTS parameters supported

The parameters for roaming and for closed user group are available in the **Physical Interfaces->UMTS/LTE->->Advanced Settings** menu. You can display detailed statistics for the selected UMTS/LTE connection in the **Physical Interfaces->UMTS/LTE->** menu.

The menu **Advanced Settings** consists of the following fields:

Fields in the menu Roaming/PLMN Selection


Field	Description
Roaming Mode	<p>Select if you intend to use Roaming.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>Disabled</i> (Default setting): Roaming is disabled. The Home PLMN (Public Land Mobile Network) is used, i.e. the provider the SIM card is registered at. • <i>Auto</i>: Use this mode if neither Roaming Mode = <i>Disabled</i> nor Roaming Mode = <i>Fixed</i> suits your requirements. Note that first a scan across all APNs is carried out in this mode. • <i>Unrestricted</i>: This mode is intended for specific requirements. Note that first a scan across all APNs is carried out in this mode. • <i>International</i>: This mode is intended for specific requirements. Note that first a scan across all APNs is carried out in this mode. • <i>National</i>: This mode is unavailable in many countries, e.g. in Germany. Note that first a scan across all APNs is carried out in this mode. • <i>Fixed</i>: <p>If the field Local Environment is not <i>Enabled</i> you can use Roaming Mode = <i>Fixed</i> to choose a Region and a Country inside of this Region. Within the Country, you can specify a Mobile Network Provider.</p> <p>If the field Local Environment is <i>Enabled</i>, you can use Roaming Mode = <i>Fixed</i> to choose a Mobile Network Provider in your vicinity.</p>
Local Environment	Only for Roaming Mode = <i>Fixed</i>

Field	Description
	<p>Specify if you want to select a Mobile Network Provider in your vicinity.</p> <p><i>Enabled</i> activates the function.</p> <p>The function is deactivated per default.</p>
Mobile Network Provider	<p>Only for Roaming Mode = <i>Fixed</i></p> <p>Select a Mobile Network Provider from the list.</p> <p>With Local Environment <i>Enabled</i> you can select a Mobile Network Provider in your vicinity.</p> <p>Outside of your Local Environment, choose a Region, then a Country and finally a Mobile Network Provider that is available inside of the specified location.</p>
Region	<p>Only for Roaming Mode = <i>Fixed</i> and Local Environment not <i>Enabled</i></p> <p>Select the desired Region from the list.</p>
Country	<p>Only for Roaming Mode = <i>Fixed</i> and Local Environment not <i>Enabled</i></p> <p>Depending on the selected Region, select the desired Country from the list.</p>

Fields in the menu Closed User Group

Field	Description
Authentication Method	<p>Select an authentication protocol for the Closed User Group. Select only an authentication method that has been specified by your provider.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • <i>None</i>: Some providers do not use authentication. Select this option if your provider is among them. • <i>pap</i>: Execute only PAP (PPP Password Authentication Protocol), the password is sent unencrypted. • <i>chap</i>: Execute only CHAP (PPP Challenge Handshake Authentication Protocol according to RFC 1994) the password is

Field	Description
	<p>sent encrypted.</p> <ul style="list-style-type: none"> • <i>pap-chap</i> (Default value): Prefer CHAP, use PAP if not available.
Username	Enter the user name that has been supplied by your provider.
Password	Enter the password that has been supplied by your provider.
Fixed IP Address	Enter the Ip address that has been supplied by your provider.

Clicking the  button opens a page with detailed statistics on the current UMTS/LTE connection.

The menu **Physical Interfaces->UMTS/LTE->** consists of the following fields:

Values in the list Mobile Device Status

Field	Description
Device	Displays the description of the internal modem port.
Modem Model	Displays the modem model description.
IMEI	The IMEI (International Mobile Station Equipment Identity) displays the 15 digit serial number of the modem.
Oper Status	Displays the operation mode of the modem.
ICC ID	Displays the card ID stored on the SIM card.
Subscriber Number	Displays the calling number stored on the SIM card.
Service Center Address	Displays the address of the provider's service center stored on the SIM card.
Home PLMN	Displays the Home PLMN (Public Land Mobile Network), i.e. the provider the SIM card is registered at.
Selected PLMN	Displays the selected PLMN. If no PLMN is selected, the Home PLMN is displayed.
Actual Network	Displays which kind of network is currently used (e.g., UMTS or GPRS).
Network Quality	Displays the current connection quality.
Location Area Code	Displays the radio cell code of the cell the modem is currently connected to.
Cell ID	Displays the Cell ID of the cell the modem is currently registered in.

Field	Description
Last Command	Displays the last command sent to the modem by the system.
Last Reply	Displays the last reply sent by the modem.

Values in the list Mobile Operators

Field	Description
PLNM	Displays the PLMN of the carrier.
Name	Displays the name of the carrier.
Access Type	Displays the currently available network type (e.g., UMTS oder GSM).
State	Displays the registration status.

2.11 New IPSec parameters supported

The parameters **Public Interface** and **Public Interface Mode** are available in the **VPN->IPSec->IPSec Peers->New->Advanced Settings** menu.

Relevant fields in the menu Advanced IP Options

Field	Description
Public Interface	Specify the public (or WAN) interface that this peer is to use to connect to its VPN partner. If you select <i>Chosen by Routing</i> , the decision as to via which interface the data traffic is routed is made based on the current routing table. If you select an interface, the interface is used taking into consideration the setting under Public Interface Mode .
Public Interface Mode	Specify how strictly the setting under Public Interface is handled. Possible values: <ul style="list-style-type: none"> • <i>Enforce</i>: Only the selected interface is used, whatever the priorities in the current routing table. • <i>Preferred</i>: Depending on the priorities in the current routing table, the selected interface is used if no more favourable route is available via a different interface.



Note

Note that the default behavior of the gateways has been changed with this feature: If more than one IP address is configured for an interface, the first configured IP address is selected. Up to now the last one was selected. If required, specify an IP address using the option **Public Source IP Address**.

2.12 Commands upgraded

A source IP address can be specified when using the SNMP shell commands `cert get`, `cert put`, `configd` and `update`.

2.13 MIB: ipNatOutTable table upgraded

The parameters *IntPortRange* and *ExtPortRange* have been added to the MIB table **ipNatOutTable**.

2.14 Hardware: New LED mode available

With **Systemsoftware 9.1.7** a new LED mode is available for the devices **bintec RS232bu+**, **RS232j-4G** and **RS120wu**.

If you want to put a device into this mode, you can see from the LEDs which wireless standard is currently in use and which signal quality is available for the wireless network.

To change mode, press the Reset button down three times in a row for longer than 0.5 seconds and release it again.

Briefly press the Reset button to restore the regular mode.

Wireless standard

The following link exists between the lights of an LED and the wireless standard in use:

LED	Wireless standard
USB	GSM
UMTS	UMTS/HSxPA
BRI	LTE (where supported)

If the device has not yet locked in or has not yet found a signal, no LED lights up.

Signal quality

The following link exists between the signal quality and the lights of one or more Ethernet LEDs:

Signal strength in dBm	Number of the Ethernet LED
< -100	1
< -80	1, 2,
< -70	1, 2, 3
< -60	1, 2, 3, 4
>= -60	1, 2, 3, 4, 5

2.15 Hotspot - Post Login URL added

It is now possible to specify the URL a user is redirected to after logging in to the Hotspot Solution. The respective configuration is carried out in **Local Services+HotSpot Gateway->HotSpot Gateway->Post Login URL**.


Chapter 3 Changes

The following changes have been made in **Systemsoftware 9.1.7** .

3.1 Company name changed

The company name "Teldat GmbH" has been replaced by the new company name "bintec elmeg GmbH".

3.2 Factory settings changed

In the factory settings, in the menu **Physical Interfaces->ISDN Ports->ISDN External->** under **Advanced Settings**, the field **Keep Layer 2 permanently enabled** has been disabled because, with the original setting, every five seconds messages were being written to the SD card if **ISDN External** was not connected or not being used.

3.3 GUI: Name changed

The menu **Maintenance+elmeg IP1x Update** has been renamed as **Maintenance->elmeg OEM**. In this menu you can run an update for elmeg IP1x telephones and elmeg DECT systems.

3.4 GUI: Interface and documentation changed

In the menu **Terminals->Other Telephones->VoIP->New**, under **Advanced Settings**, the field **IP Address Mode** has been renamed to **SIP Client Mode**.

With the setting **IP Address Mode = *Static***, **IP address of the telephone** was being erroneously displayed. Now, instead, with **SIP Client Mode = *Static***, the field **IP Address of the SIP client** is displayed.

Chapter 4 Bugfixes



Note

Please note that the changes described below are not the only bugs that have been fixed. In particular, the changes do not necessarily apply to all products. Even if the following corrections are not relevant to your device, it will still benefit from the general improvements to the patch.

The following bugs have been fixed in **Systemsoftware 9.1.7** :

4.1 hybrid: Problem with parallel calls

(ID 17433)

With an incoming call by parallel call, if the signal is also to be external, the extension that is parallel called was unable to make an enquiry call.

The problem has been solved.

4.2 hybrid: Layout incorrect.

(ID 17963)

Under **Maintenance->Update System Telephones**, the layout of the page displayed was incorrect.

The problem has been solved.

4.3 GUI: Filtering of display incorrect

(ID 17991)

In the menu **Numbering->User Setting->Permissino Classes** the filtering of the display was not working correctly when the filter was for a particular music on hold

The problem has been solved.

4.4 SIP: Communication aborted

(ID 18004)

With outgoing calls to a mobile terminal via a SIP connection, the communication was being aborted after 30 seconds.

The problem has been solved.

4.5 FXS ports: Communication problems

(ID 18049)

Sometimes with FXS ports, communication was only possible in one direction.

The problem has been solved.

4.6 UMTS: Connection problems

(ID 18047)

No UMTS connection could be established with the HUAWEI Stick E352s-5.

The problem has been solved.

4.7 Wireless LAN controller: Incorrect WPA mode

(ID 18108)

If, in the menu **Wireless LAN Controller->Slave AP Configuration->Wireless Networks (VSS)->New**, the fields **Security Mode** = *WPA-PSK* and **WPA Mode** = *WPA 2* were set, an incorrect value displayed for the field **WPA Mode** after saving and assigning the new wireless network to the radio modules

The problem has been solved.

4.8 System: Problem when loading a configuration

(ID n/a)

When more than one VSS interface was being used, problems arose with the devices **W1003n**, **W2003n**, **W2003n ext** and **W2004n** when loading a configuration.

The problem has been solved.

4.9 Monitoring: Tx statistic incorrect

(ID n/a)

When the Tx statistic was being recorded, the EAPOL packets were missing. The message "(Tx) Unknown legacy rate: 0" was being displayed.

The problem has been solved.

4.10 System: Problems with fragmented frames

(ID 18070, 17296)

Problems were occurring with fragmented frames. For instance, a stack trace was sometimes being triggered.

The problem has been solved.

4.11 Hardware: Problem with roll-out processes

(ID 18039)

When an MC7710 module was being used, problems were occurring with roll-out processes with SIM cards with no PIN, e. g. with the XAdmin.

The problem has been solved.

4.12 Wireless LAN controller: Entries collected incorrectly

(ID 18005)

When the **Repeat Background Scan** function was being used, the results of previous scans were being incorrectly collected in the MIB table **wlcScanResultsTable**, so that after a while the table contained a huge number of entries.

The problem has been solved.

4.13 System: Problems when copying or renaming configuration files

(ID n/a)

Copying and renaming configuration files was causing all sorts of problems if the old or new file name was longer than 19 characters, even though a length of 40 characters is permitted.

The problem has been solved.

4.14 WLAN: Roaming not working correctly

(ID n/a)

Clients were sometimes "getting lost" when roaming, because the access point was failing to tell the infrastructure when a client had logged into it.

The problem has been solved.

4.15 QoS: Problems with QoS queue

(ID 17990)





With Internet Explorer 9 or 10, a QoS queue could not be added or changed in the menu

Network->QoS->QoS Interfaces/Guidelines. An error message was being displayed.

The problem has been solved.

4.16 Wireless LAN controller: Status incorrect


(ID n/a)

If, in the menu **Wireless LAN Controller->Slave AP Configuration ->Slave Access Points**, under **Action**, an access point was frequently being switched backwards and forwards between  and , **Status**  was never being displayed under **Wireless Networks (VSS)**, even though the status of the wireless network was  and merely no VSS statistics update had been carried out.

The problem has been solved.

4.17 WLAN: Incorrect wireless networks displayed

(ID 17569)

If, in the menu **Wireless LAN->WLAN->Settings Radio Module->**, an access point was configured with **Frequency Band = 5 GHz Outdoor** and **Channel = Auto**, and more than one wireless network had been created but was not yet enabled in the menu **Wireless LAN->WLAN->Wireless Networks**, the first wireless network to be enabled worked correctly. For the remaining wireless networks, incorrect wireless networks with an empty SSID were being used.

The problem has been solved.

4.18 Trace: Incorrect message displayed

(ID 14259)

When the trace command was being used when SIF was active, the output was receiving the message "12 frames per second rejected", even though only a single packet was involved.

The problem has been solved.

4.19 SSH access incorrectly interrupted

(ID 13260)

If, with SIF active in the MIB table **ipSifAliasTable**, the MIB variable **Priority** = *low-latency* had been set, SSH access to the local computer was interrupted and suppressed.

The problem has been solved.

4.20 UMTS: Password for closed user groups missing

(ID n/a)

The password for closed user groups was not being provided with QMI modems.

The problem has been solved.

4.21 GUI: Display for Ethernet interfaces non-standardised

(ID 17174)

In the menu **Network->Drop-In->Drop-in Groups->New**, there were different ways of writing the same Ethernet interface.

The problem has been resolved; the way they are written has been standardised.

4.22 GUI: Filtering of display not working

(ID 18100)

In the menu **Numbering->Call Distribution->Call Assignment**, the filtering of the display was not working if you filtered by **External Connection**. In the menu **Terminals->Overview->Overview**, the filtering of the display was not working if you filtered by **Telephone Type**.

The problem has been solved.

4.23 GUI: Unable to save setting

(ID 18090)

In the menu **Network->Routes->Configuration of IPv4 Routes->New**, no templates could be generated with the setting **Route Type** = *Template for Standard Route by DHCP*, i.e. you were unable to save this setting.

The problem has been solved.

4.24 WLAN: Data packet losses

(ID 17684)

With the devices **W1002n**, **W11040n**, **W11065n** and devices in the RS series, in client mode data packets were being lost after roaming.

The problem has been solved.

4.25 GUI: Source port and mode incorrectly displayed

(ID 18053)

In the menu **Network->Routes->Configuration of IPv4 Routes->New**, with the setting **Route Type** = *Standard Route via Gateway*, **Route Class** = *Advanced*, **Layer 4 Protocol** = *TCP* and **Source Port** = *Single*, after saving with **OK** and opening the entry just created, the field **Source Port** = *Any* was being displayed. This field was no longer editable. Also, the field **Mode** = *Dial and Wait* was set by error.

The problem has been solved.

4.26 Scheduling: Version check not working

(ID 17995)

In the menu **Local Services->Scheduling->Actions->New**, before importing a configura-

tion file, a **version check** could be run to prevent old configuration files being imported. This check was not working.

The problem has been solved.

4.27 Hotspot: Timeout for status window

(ID 17900)

With the web filter active, at times the update to the hotspot status window was not being displayed, but rather the status window was being affected by a timeout because a status session request from the hotspot client had not been answered by the gateway.

The problem has been solved.

4.28 Stacktrace

(ID 17949)

At times a stack trace was being run after the device had been running for 30 seconds.

The problem has been solved.

4.29 GUI: Firewall

(ID 17589)

If the destination port was changed by an entry in the menu **Firewall->Services->Services List**, this change was erroneously not being copied to the relevant group.

The problem has been solved.

4.30 LED: Incorrect display

(ID n/a)

With **bintec Rxxx2/RTxxx2-Serie** devices, the LED for the ISDN BRI connection was displaying the status of Layer 1 and not the number of B channels.

The problem has been solved.

4.31 Wireless LAN controller: Connection problem

(ID 18181)

When a wireless LAN controller was being used and a wireless network configured with **Safety Mode** = *WPA Enterprise* and **ACL Mode** *Enabled*, the clients with MAC addresses specified under **Permitted Addresses** were unable to connect to the wireless network.

The problem has been solved.

Chapter 5 Known issues

5.1 hybrid: Problem with LDAP

You cannot access your personal telephone book via LDAP.

5.2 DECT multi-cell system: Problem with three-way conferences

You cannot conduct a three-way conference with a DECT multi-cell system.

We recommend an external solution, e. g. a conference server.