bintec elmeg
Teldat Group Company

Release Notes

9.1.9

Copyright© Version 1.0, 2014 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 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 **System Software 9.1.9** using the Graphical User Interface, proceed as follows:

(1) For the update, you'll need the XXXXX_bl9109.xxxfile, 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 **System Software 9.1.9** using the **Maintenance**->**Software &Configuration** menu. To do this, select: **Action** = *Update system software*, **Source Location** = *Local File*, **Filename** = *XXXXX_bl9109.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_bl9105.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 9.1.9 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 WLAN Controller Monitoring

Systemsoftware 9.1.9 introduces significantly expanded functions for monitoring the Wireless LAN Controller.

Note

In order to ensure adequate timing between the WLAN Controller and the connected Slave APs, the internal time server of the WLAN Controller should be enabled.

2.1.1   WLAN Controller

Fig. 2: **Wireless LAN Controller**->**Monitoring**->**WLAN Controller**

In the **Wireless LAN Controller**->**Monitoring**->**WLAN Controller** menu, an overview of the most relevant Wireless LAN Controller parameters is displayed. The display is refreshed every 30 seconds.

Values in the Overview list

Status	Meaning
AP discovered	Displays the number of discovered access points.
AP offline	Displays the number of access points not connected to the Wireless LAN Controller.

Status	Meaning
AP managed	Displays the number of managed access points.
WLAN Controller: VSS throughput	Displays the data traffic in receive and transmit direction in bytes per second.
CPU usage [%]	Displays the percentaged CPU load over time.
Memory usage [%]	Displays the percentaged memory consumption over time.
Connected clients/VSS	Displays the number of connected clients per wireless network (VSS) over time.

2.1.2 Slave Access Points

Fig. 3: **Wireless LAN Controller**->**Monitoring**->**Slave Access Points**

LAN MAC Address

Via the 🔍 icon, you can open an summary with additional details about the **Slave Access Points**.

2.1.2.1 Overview

In the **Overview** menu, additional information about the selected access point is displayed. The display is refreshed every 30 seconds.
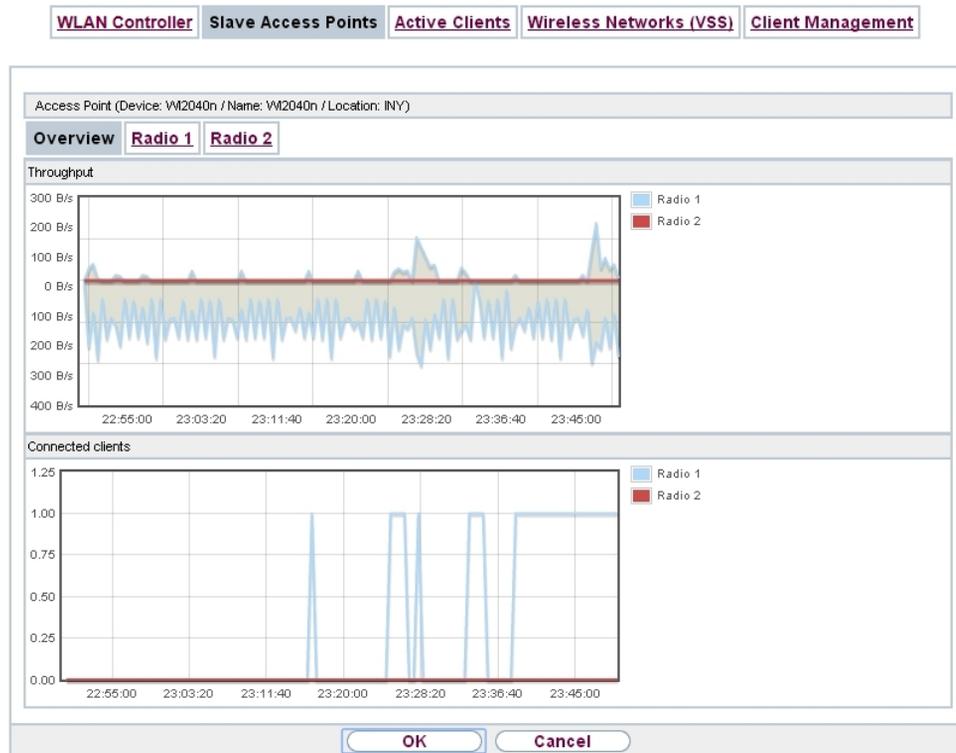
Fig. 4: **Wireless LAN Controller**->**Monitoring**->**Slave Access Points**->**Overview**

Values in the Overview list

Status	Meaning
Throughput	Displays the received and transmitted data traffic per radio module over time.
Connected clients	Displays the number of connected clients per radio module over time.

2.1.2.2 Radio 1

In the **Radio Module** menu, the received and transmitted data traffic per client is displayed over time. Each graph in the display is distinctly assigned to a client by its color and MAC address.
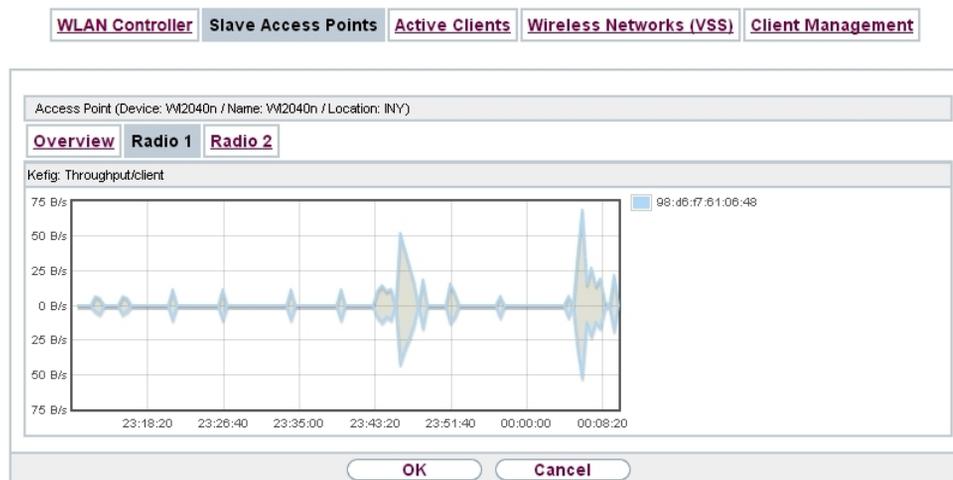
Fig. 5: **Wireless LAN Controller**->**Monitoring**->**Slave Access Points**->**Radio**

Values in the Radio list

Status	Meaning
Throughput/client	Displays the received and transmitted data traffic per client over time.

2.1.3 Active Clients
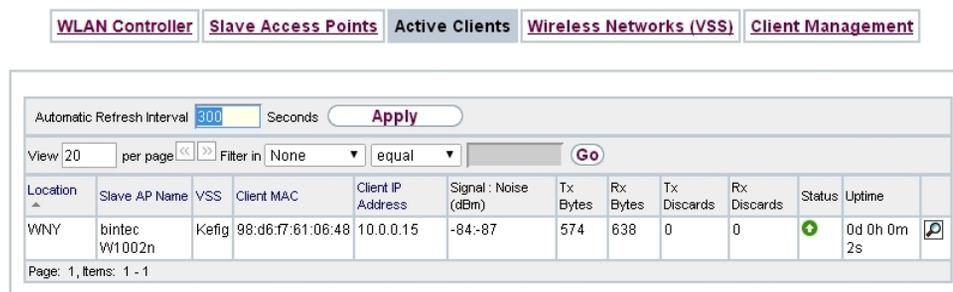
Fig. 6: **Wireless LAN Controller**->**Monitoring**->**Active Clients**

In the **Wireless LAN Controller**->**Monitoring**->**Active Clients** menu, current values of all active clients are displayed.

For each client you will see an entry with the following parameter set: **Location**, **Slave AP Name**, **VSS**, **Client MAC**, **Client IP Address**, **Signal : Noise (dBm)** , **Tx Bytes**, **Rx Bytes**, **Tx Discards**, **Rx Discards**, **Status**, **Uptime**.

Possible values for Status

Status	Meaning
None	The client is no longer in a valid status.
Logon	The client is currently logging on with the WLAN.
Associated	The client is logged on with the WLAN.
Authenticate	The client is in the process of being authenticated.
Authenticated	The client is authenticated.

Via the 🔍 icon, you can open a summary with additional details about the **Active Clients**.
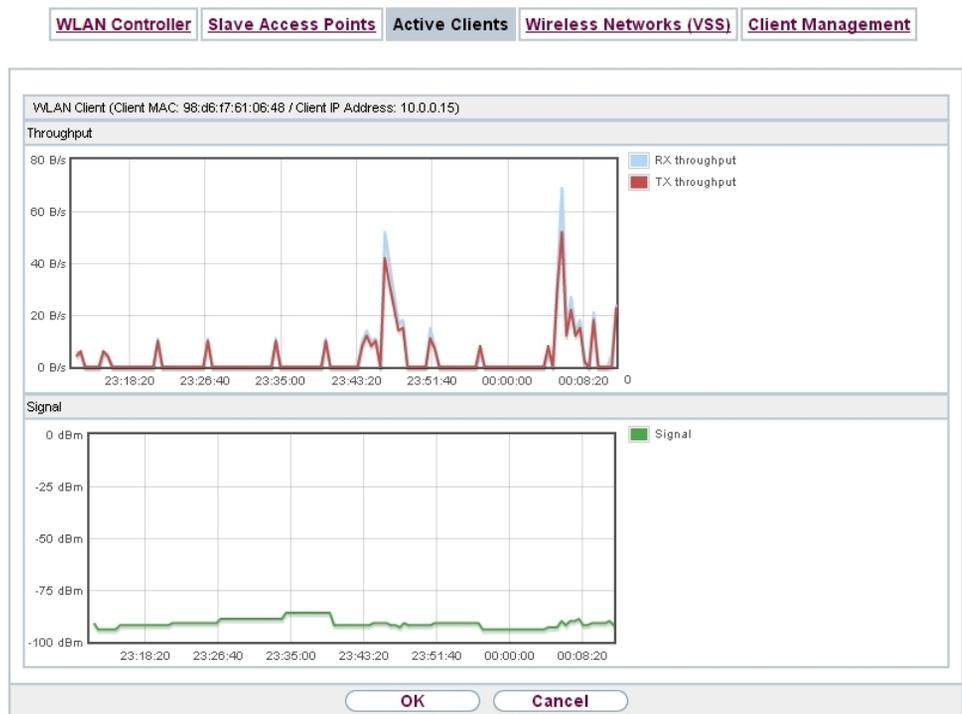
Fig. 7: **Wireless LAN Controller**->**Monitoring**->**Active Clients**-> 🔍

Value in the list WLAN Client list

Status	Meaning
Throughput	Displays the data traffic - separated into received and transmitted traffic - for the selected WLAN client over time.
Signal	Displays the signal strength of the selected WLAN client over time.

2.1.4 Wireless Networks (VSS)

Fig. 8: **Wireless LAN Controller**->**Monitoring**->**Wireless Networks (VSS)**

In the **Wireless LAN Controller**->**Monitoring**->**Wireless Networks (VSS)** menu, an over-
view of the currently used AP is displayed. You see which wireless module is assigned to
which wireless network. For each wireless a parameter set is displayed (**Location**, **Slave
AP Name**, **VSS**, **MAC Address (VSS)**, **Channel**, **Status**).

2.1.5 Client Management

Fig. 9: **Wireless LAN Controller**->**Monitoring**->**Client Management**

The **Wireless LAN Controller**->**Monitoring**->**Client Management** menu displays informa-
tion on the client management by the access points. You can, e.g., see the number of con-
nected clients, the number of clients that are affected by the **2,4/5 GHz changeover** and
the number of rejected clients.

You can delete the values of an entry using the 🗑 symbol.

2.2 WLAN Bandwidth Control

The bandwidth available for indiviadual clients can be restricted in recieve as well as in transmit direction with the options **Rx Shaping** and **Tx Shaping** in the menu **Wireless LAN**->**WLAN**->**Wireless Networks (VSS)**->**Edit/New** or **Wireless LAN Controller**->**Slave AP configuration**->**Wireless Networks (VSS)**->**Edit/New**. The following values are available:

Fields in the menu Bandwidth limitation for each WLAN client

Field	Description
Rx Shaping	Select a bandwidth limitation in the receive direction. Possible values are • *No limit* (default value) • *0,25 Mbit/s*, *0,5 Mbit/s*, *1 Mbit/s* up to *10 Mbit/s* in single Mbit/s steps, *15 Mbit/s*, *20 Mbit/s*, *30 Mbit/s*, *40 Mbit/s* and *50 Mbit/s*.
Tx Shaping	Select a bandwidth limitation in the transmit direction. Possible values are • *No limit* (default value) • *0,25 Mbit/s*, *0,5 Mbit/s*, *1 Mbit/s* up to *10 Mbit/s* in single Mbit/s steps, *15 Mbit/s*, *20 Mbit/s*, *30 Mbit/s*, *40 Mbit/s* and *50 Mbit/s*.

2.3 DHCP Options for bintec 4Ge-LE

For the operation of **bintec 4Ge-LE System Software 9.1.9** offers additional DHCP options via the GUI.

In the menu **Local Services**->**DHCP Server**->**DHCP Configuration**->**Advanced Settings**, proceed as follows in order to specify the respective parameter:

(1) Click the **Add** button in the **DHCP Options** field and choose **Option** = *Vendor String*.

(2) Click the ⟁ button to edit the entry.
      The window **Basic Parameters** opens.

(3) Under **Select vendor**, select *bintec*.

(4) Add the desired values for your **4Ge-LE** in the fields **APN** and **PIN** and click **Apply**.

Chapter 3 Changes

The following changes have been made in **System Software 9.1.9** .

3.1 WLAN - Number of wireless networks increased

The number of wireless networks (VSS) you can configure per radio module has been increased from 8 to 16.

Chapter 4 Bug fixes

The following errors have been corrected in **System Software 9.1.9** :

4.1 Assistants - VoIP PBX in LAN error

ID 18542

If the fields **WAN interface for VoIP prioritisation** = *en1-4*, **Maximum Upload Speed** = *640* and **IP Address of VoIP PBX within your LAN** = *192.168.0.100* (example values) were configured in the menu **Assistants**->**VoIP PBX in LAN**->**VoIP PBX in LAN**->**New** and were confirmed with **OK**, an error message was displayed and *0 kbit/s* was displayed in the column **VoIP bandwidth** .

4.2 RADIUS - Panic and reboot

ID 18406

60 minutes after closing the first of several PPTP connections authenticated through RADIUS, there was a panic.

4.3 DHCP - Multiple IP address assignment

ID 18440

Using a **bintec elmeg** device together with another **bintec elmeg** and an Android device as WLAN clients it could happen that - after repeated connects and disconnects - the same IP address was assigned to both clients.

4.4 Wireless LAN - Wrong calculation of octets

ID n/a

If A-MPDU frames were sent, the sum of the calculated octets was wrong.

4.5 Wireless LAN Controller - Access point reboot

ID 18408

If a data packet was lost during the configuration of an access point by a Wireless LAN Controller, it could happen that the access point rebooted before the configuration was complete. In a network with significant packet loss, the access point could potentially enter a reboot loop.

4.6 Wireless LAN Controller - Management faulty

ID 18453

If a new generation WLAN device was configured to use the Wireless LAN Controller to manage its own radio module with the use of the **Wireless LAN** assistant, and if the field **LED mode** was set to *Off* in the menu **System Management**->**Global Settings**->**System**, the Wireless LAN Controller removed its radio module from the management and all other modules were disabled.

4.7 Routing - Irrelevant error messages

ID 18489

If the field **Route Type** in the menu **Network**->**Routes**->**IPv4 Route Configuration**->**New** was set to *Network Router via Interface* and a valid IP address and netmask were specified, clicking **OK** triggered the error message "For Network Type 'Direct' an Interface must be specified" even though no network type "direct" was shown.

If the **Route Type** was set to *Host Route via Interface* or to *Default Route via Interface*, confirming with **OK** equally triggered irrelevant error messages.

4.8 Drop-In - Route configuration not possible

ID 18434

It was not possible to create a route via a gateway if the respective interface was part of a drop-in group.

4.9 IPSec - Wrong use of the loopback address

ID 18399

The loopback address *127.0.0.1* was occasionally used as source IP address for IKE.

4.10 IPSec - Wrong use of default route

ID 18509

If no netmask or *0.0.0.0* was specified for **Route Entries** in the menu
VPN->**IPSec**->**IPSec Peers**->**New**, a default route was activated without notice.

4.11 IPSec - CIDR notation not supported

ID 18531, ID 18490

Specifying a netmask in the CIDR notation (e.g. */24*) was not possible for
VPN->**IPSec**->**IPSec Peers**->**New**->**Additional Traffic Filter** and for **Network**->**Load Balancing**->**Special Session Handling**->**New**->**Source IP Address/Netmask**.

4.12 DNS - Irrelevant error message

ID 18467

If ,e.g., **DNS Hostname** = *test.test.de* and **IP Address** = *1.0.127.127* was specified
in **Local Services**->**DNS**->**Static Hosts**->**New**, the error message " Input Error: Please
specify a valid IP address when setting a non-negative response!" was displayed.

4.13 Setup Tool - Extended route configuration not possible

ID 18448

After the first establishment of an LTE WAN connection, it was impossible to create an extended route of the type "WAN without transit network".

Index