VPN Access 250, VPN Access 1000, X8500

Release Notes
System Software 7.9.1

Version 1.0

Goal and Purpose

This document describes the new features, changes and bugfixes in **System Software 7.9.1**.

Liability

This document has been put together with the greatest possible care. 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 contained in this document is subject to change without notice. You can find additional information and changes 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.

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

Copyright

Guidelines and Standards

Bintec gateways comply with the following guidelines and standards:

R&TTE Directive 1999/5/EC

CE symbol for all EU states

You can find further information in the declarations of conformity under www.funkwerk-ec.com.

How to reach Funkwerk Enterprise Communications GmbH

Funkwerk Enterprise Communications GmbH
Südwestpark 94
D-90449 Nürnberg
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 7.9.1 carefully to avoid problems when updating or using the software.

1.1 Applicability

System Software 7.9.1 is available only for the following devices and cannot be used on other devices:

- **VPN Access 250**
- **VPN Access 1000**
- **X8500**.

1.2 Incompatibility

Configurations created or saved with **System Software 7.9.1** may be incompatible with some versions of our system software.

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

1.2.1 Preparation and update

To prepare and carry out an update to **System Software 7.9.1**, proceed as follows:

1. Backup the current boot configuration. Use one of the following possibilities:
   a) In the SNMP shell, enter `cmd=save path=boot.alt`. This backs up the current boot configuration in the Flash ROM of your gateway 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 7.9.1** as usual and reboot the gateway.
   The gateway will start with the new software, the existing boot-configuration will be used.

1.2.2 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 Set-up 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 gateway. The device will start with the previously backed up boot configuration and the old version of the system software.

2 New Functions

System Software 7.9.1 includes a number of new functions that significantly extend the performance compared with System Software 7.8.7:

2.1 Time zone selection for automatic daylight saving

In System Software 7.9.1 your device automatically switches from summer time to standard time in autumn and from standard time to summer time in spring on the respective changeover date.

In the Setup Tool menu ***System*** ➜ ***Time and Date*** you can select the required time zone for your system (e.g. *Europe/Berlin*) in the new ***System Time Zone*** field. If summer time and standard time are defined for the chosen time zone, the changeover is carried out automatically on the changeover date.

Note

Note that automatic daylight saving can have an undesirable effect on events that are configured in the ***System*** ➜ ***Schedule & Monitor*** ➜ ***Event Scheduler (Time & SNMP)*** menu.

Note

Note that automatic daylight saving can result timestamps being duplicated for recorded events when switching from summer time to standard time.

2.2 ISAKMP Configuration Method (IKE Config Mode) in client mode

The ISAKMP Configuration Method (IKE Config Mode for short) allows you to connect a mobile PC workstation (Secure IPSec Client) to the head office over IPSec.

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 IPSec gateway on request. This method allows a dynamic IP address to be assigned, e.g. from the internal address range for the head office (see Release Notes 7.8.7).

In **System Software 7.9.1** you can now not only configure your device as a server as before, but also as a client for IKE Config Mode; previously you could use an NCP Secure Client, for example as a client.

The new setting ***IP Transit Network*** = *IKE Config Client Mode* in the ***IPSec*** ➜ ***Configure Peers*** ➜ **EDIT** ➜ ***Interface IP Settings*** ➜ ***Basic IP-Settings*** menu allows you to configure your gateway as a client for IKE Config Mode.

2.3 cert get command with HTTPS

In System Software 7.9.1 the *cert get* command is available to import certificates over HTTPS.

2.4 Scheduler - Placeholder available for serial number

In System Software 7.9.1 you can use the character string SN as a placeholder for the serial number in commands in the Scheduler.

For example, you can set the field ***SET VALUE ACTIVE*** to *get_all;http://10.9.1.2/tftp:file SN.cf* in the setup tool menu ***SYSTEM*** ➜ ***SCHEDULE & MONITOR*** ➜ ***EVENT SCHEDULER (TIME & SNMP)*** ➜ ***SCHEDULE COMMANDS*** ➜ **ADD** to obtain the configuration files for several gateways.

2.5 DynDNS Provider www.dnsexit.com

In System Software 7.9.1 the DynDNS Provider www.dnsexit.com is now available.

2.6 IPSec - Multiple users over the same peer

In System Software 7.9.1 you can configure an IPSec peer so that multiple users can dialin over this IPSec peer.

To do this, select ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ **EDIT** ➜ ***PEER SPECIFIC SETTINGS*** from the Setup Tool menu and set ***SPECIAL PEER TYPE*** to *Dynamic Client*. We also recommend setting the ***IP TRANSIT NETWORK*** field to *IKE Config Server Mode* in the ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ **EDIT** ➜ ***INTERFACE IP SETTINGS*** ➜ ***BASIC IP-SETTINGS*** menu.

2.7 Setup Tool - ISDN statistics

In System Software 7.9.1 the statistics for terminated calls, and not just current calls as in previous versions, are available using the command *s* in the setup tool menu *MONITORING AND DEBUGGING* ➜ *ISDN MONITOR*.

2.8 New MIB variable HttpRedirect

In System Software 7.9.1 the new MIB variable *HTTPREDIRECT* is now available in the MIB table *IPEXTIFTABLE*.

With the variable ***HTTPREDIRECT*** you can either redirect HTTP requests to the local HTTP demon (*local*) or to the local content filter (*proxy*).

3 Changes

The following changes have been made in System Software 7.9.1 to improve performance and usability:

3.1 Java SNMP browser removed

In **System Software 7.9.1** the Java SNMP browser has been removed.

3.2 Credits functionality removed

In **System Software 7.9.1** the Credits functionality has been removed.

3.3 Preshared Keys - Warning added

The following warning has been added in **System Software 7.9.1** to prompt the user to change the default setting of the Preshared Key: “Change the default Preshared Key! If the key has not been changed, your device will not be protected against unauthorised access!”

3.4 SIF alias names changed for interfaces

In **System Software 7.9.1** the SIF alias names for interfaces have been improved to avoid misunderstandings. A distinction can now be made between the following categories: LAN, WLAN, IPSec, Leased, Bundle and Bridge. For example, the current interface is *LAN_PEER_2_R4100_1* but will now be renamed *IPSEC_PEER_2_R4100_1*.

3.5 Setup Tool - QoS - Value range expanded

In the Setup Tool menu ***QoS*** ➜ ***Interfaces and Policies*** ➜ **Edit** ➜ ***QoS Scheduling and Shaping*** the setting ***Queueing and Scheduling Algorithm*** = *priority queueing (PQ)* and ***Specify Traffic Shaping*** = ***yes*** displays the field ***Maximum Transmit Rate (Bits per Second)***. The value range for this field has been expanded from *100000000* to *1000000000*.

3.6 Giving parameters when making outgoing calls from your own subscriber number

To "give" specific parameters in accordance with Q.931 when making outgoing calls from your own subscriber number, the MIB variable ***Screening*** in MIB table ***biboDialTable*** can also be used for outgoing calls. The new MIB variable ***TypeOfLocalNumber*** is also available for this purpose.

4 Problems Solved

The following problems have been solved in System Software 7.9.1:

4.1 Stacktrace due to memory problems

(ID n/a)

Clients with the incorrect WPA mode, repeatedly attempted to connect and caused a stacktrace due to a memory overrun.

The problem has been solved.

4.2 Stacktrace due to wrong Lifetime Policy

(ID 12531)

During configuring IPSec with the Setup tool, exceeding the value range *0* .. *4294967295* in the ***LIFETIME POLICY*** field caused a stacktrace. There was no difference between setting the value in seconds or in kbps.

The problem has been solved.

4.3 PIM - Stacktrace

(ID n/a)

When shutting down PIM, a stacktrace occurred when the corresponding interface was unavailable.

The problem has been solved.

4.4 PPP connections failed

(ID 11303)

In rare cases, the set-up of a PPP connection failed and the interface froze until it was manually reset or rebooted.

The problem has been solved.

4.5 IPSec - Problems setting up phase 2

(ID 12163)

When setting up phase 2 of an IPSec connection problems occurred when selecting the source address.

The problem has been solved.

4.6 IPSec - trace did not display UDP packets

(ID 12455)

When performing a trace of an IPSec tunnel, data packets sent with high priority by the router were not displayed.

The problem has been solved.

4.7 IPSec - IKE Config Mode - Wrong entry in MIB table ipDynaAddrTable

(ID 12471)

In IKE config mode the MIB table ***ipDynaAddrTable*** contains the entry ***ifIndex*** = *10001* (instead of ***ifIndex*** = *100002* for the IPSec Peer).

The problem has been solved.

4.8 IPSec - No tunnel with certificate

(ID 11313)

With IPSec no connection could be established over RADIUS if the certificate used had a parameter user name with a length of more than 64 characters.

The problem has been solved.

4.9 Saving the configuration failed

(ID 12251)

When there was not much free memory in the flash, a boot configuration was not saved correctly but no error message appeared.

The problem has been solved.

4.10 Multicast not functioning

(ID n/a)

In some cases multicast did not function because it had been enabled several times.

The problem has been solved.

4.11 Multicast - Forwarding packets failed

(ID n/a)

In scenarios with Source Specific Multicast (SSM), the forwarding of packets failed.

The problem has been solved.

4.12 Multicast failed on IPSec interfaces

(ID n/a)

No multicast packets could be transferred on IPSec interfaces.

The problem has been solved.

4.13 Multicast - Timer problem

(ID n/a)

In some cases, many queries and reports have been sent and received on an interface.

The problem has been solved; the timers have been adjusted.

4.14 RADIUS reload did not work

(ID n/a)

The non-functioning RADIUS dialout reload caused a continuous loop of get requests.

The problem has been solved.

4.15 Setup Tool - Scheduler - Incorrect interval after change

(ID 12096)

If the field ***SET VALUE ACTIVE*** was set to *1800* rather than *10* in the setup tool menu ***SYSTEM*** ➜ ***SCHEDULE & MONITOR*** ➜ ***EVENT SCHEDULER (TIME & SNMP)*** ➜ ***SCHEDULE COMMANDS*** ➜ **ADD**, *10* was used once after saving the change and then *1800*.

The problem has been solved.

4.16 Setup Tool - Port 1 incorrectly set to disabled

(ID 12567)

If the Setup tool menu ***ETHERNET SWITCH*** ➜ ***SWITCH CONFIGURATION*** was selected and closed with **Save** on a device in ex works state, port 1 was set to disabled and you could not change this setting.

The problem has been solved.

4.17 Setup Tool - Leased Line - Error when selecting the timeslot

(ID 11323)

If the ***ISDN SWITCH TYPE*** field is set to *leased line, chan. B1..B31* in the setup tool menu ***PRI2-4*** and the field ***BUNDLE TYPE*** is set to *PPP Multilink* under ***PRI2-4*** ➜ ***BUNDLE CONFIGURATION*** ➜ ***ADD***, all timeslots are selected by default even if they are saved with **Save**. When a timeslot, e.g. timeslot 11, was removed from the selection and the cursor was moved to the next timeslot, all timeslots were removed from the selection.

The problem has been solved.

4.18 Setup Tool - IPSec - Tunnel blocked

(ID 12115)

If the fields ***ISDN CALLBACK*** = *both*, ***TRANSFER OWN IP ADDRESS OVER ISDN*** = *yes* and ***MODE*** = *use B channel* were set in the setup tool menu ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ **APPEND** ➜ ***IPSEC CALLBACK***, problems occurred with callback and in some cases no connection could be established.

The problem has been solved.

4.19 Incorrect entries in MIB table ipHostAccessClientTable

(ID n/a)

After a reboot, some entries accidentally stay in the MIB table ***IPHOSTACCESSCLIENTTABLE***.

The problem has been solved; the entries are deleted on reboot.