

User's Guide
bintec R4100 / R4300
System

Copyright © July 18, 2006 Funkwerk Enterprise Communications GmbH
Version 1.0

Purpose This document is part of the user's guide to the installation and configuration of bintec gateways running software release 7.4.3 or later. For up-to-the-minute information and instructions concerning the latest software release, you should always read our **Release Notes**, especially when carrying out a software update to a later release level. The latest **Release Notes** can be found at www.funkwerk-ec.com.

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, changes and **Release Notes** for bintec gateways 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 All rights are reserved. No part of this publication may be reproduced or transmitted in any form or by any means – graphic, electronic, or mechanical – including photocopying, recording in any medium, taping, or storage in information retrieval systems, without the prior written permission of Funkwerk Enterprise Communications GmbH. Adaptation and especially translation of the document is inadmissible without the prior consent of Funkwerk Enterprise Communications GmbH.

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	Bintec France 6/8 Avenue de la Grande Lande F-33174 Gradignan France Telephone: +33 5 57 35 63 00 Fax: +33 5 56 89 14 05 Internet: www.bintec.fr
--	---

1	System Menu	3
2	Submenu External Activity Monitor	7
3	Submenu External System Logging	9
4	Submenu Schedule & Monitor	13
4.1	Submenu Keepalive Monitoring (Hosts & Ifc)	13
4.2	Submenu Event Scheduler (Time & SNMP)	18
4.2.1	Configuration of triggers (Events)	19
4.2.2	Configuration of the Action (Command)	26
5	Submenu Password Settings	33
6	Submenu Time and Date	35
	Index: System	39

1 System Menu

The fields of the **SYSTEM** menu are described below.

R4100 Setup Tool	Funkwerk Enterprise Communications GmbH
[SYSTEM]: Change System Parameters	MyGateway
System Name	r4100
Local PPP ID (default)	r4100
Location	
Contact	funkwerk
Syslog Output on Serial Sonsole	no
Message Level for the Syslog Table	info
Maximum Number of Syslog Entries	50
Maximum Number of Acctlog Entries	20
External Activity Monitor	>
External System Logging	>
Schedule & Monitor	>
Password Settings	>
Time and Date	>
SAVE	CANCEL

The **SYSTEM** menu is used for e.g. entering the basic system data of your gateway.

The **SYSTEM** menu consists of the following fields:

Field	Description
System Name	Defines the system name of your gateway; is also used as PPP host name. Appears as input prompt when logging in to the device. The device type is entered as default value.
Local PPP ID (default)	This entry is necessary to identify your gateway if the remote gateway requests the PPP ID before the gateway has identified itself to the remote terminal. The device type is entered as default value.

Field	Description
Location	<p>Indicates where your gateway is located.</p> <p>Is shown, for example, on the HTML system information page or in the login message.</p>
Contact	<p>Indicates the responsible contact person. Here you can enter the e-mail address of the system administrator, for example.</p> <p>Default value: <i>funkwerk</i>.</p> <p>Is shown, for example, on the HTML system information page.</p>
Syslog Output on Serial Console	<p>Enables the display of syslog messages on the PC connected to the serial interface of the gateway. Use this setting only if you make a fault analysis, as a very large output over the serial console adversely affects the throughput of the other interfaces.</p> <p>You should normally use EXTERNAL SYSTEM LOGGING. Possible values:</p> <ul style="list-style-type: none">■ <i>no</i> (default value)■ <i>yes</i>

Field	Description
Message Level for the Syslog Table	<p>Specifies the priority of the syslog messages to be recorded internally. Possible values:</p> <ul style="list-style-type: none"> ■ <i>emerg</i>: emergency messages (highest priority) ■ <i>alert</i>: alert messages ■ <i>crit</i>: critical messages ■ <i>err</i>: error messages ■ <i>warning</i>: warning messages ■ <i>notice</i>: notice messages ■ <i>info</i> (default value): info messages ■ <i>debug</i>: debug messages (lowest priority) <p>Syslog messages are only recorded internally if they have a higher or identical priority to that indicated, i.e. all messages generated are recorded at syslog level <i>debug</i>.</p>
Maximum Number of Syslog Entries	<p>Maximum number of syslog messages saved internally in the gateway (possible values: 0 ... 1000).</p> <p>Default value: 50.</p> <p>You can show the saved messages in the Setup Tool under MONITORING AND DEBUGGING → MESSAGES.</p>
Maximum Number of Acctlog Entries	<p>Maximum number of accounting messages saved internally in the gateway (possible values: 0 ... 1000).</p> <p>Default value: 20.</p>

Table 1-1: **SYSTEM** menu fields

2 Submenu External Activity Monitor

The fields of the **EXTERNAL ACTIVITY MONITOR** submenu are described below.

R4100 Setup Tool	Funkwerk Enterprise Communications GmbH
[SYSTEM]: [ACTIVMON]: External Activity Monitor	MyGateway
Client IP Address	255.255.255.255
Client UDP Port	2107
Type	off
Update Interval (sec)	5
SAVE	CANCEL

The **SYSTEM → EXTERNAL ACTIVITY MONITOR** menu contains the settings necessary for monitoring your gateway with the Windows Activity Monitor tool (part of **BRICKware for Windows**).

Purpose The **Activity Monitor** enables Windows users to monitor the activities of the gateway. Important information about the status of physical interfaces (e.g. ISDN line) and virtual interfaces (e.g. WAN partner) is easily obtained with one tool. A permanent overview of the utilization of the gateway is possible.

Method of operation A Status Daemon collects information about the gateway and transfers it in the form of UDP packets to the broadcast address of the first LAN interface (default setting) or to an explicitly entered IP address. One packet is sent per time interval, which can be adjusted individually to values from 1 - 60 seconds. Up to 100 physical and virtual interfaces can be monitored, provided the packet size of 4,096 bytes is not exceeded. The Activity Monitor on your PC receives the packets and can display the information contained in them in various ways according to configuration.

Activate the **Activity Monitor** as follows:

- Configure the relevant gateway(s) to be monitored.

- Start and configure the Windows application on your PC (see **BRICKware for Windows**).

The **EXTERNAL ACTIVITY MONITOR** menu consists of the following fields:

Field	Description
Client IP Address	IP address to which the gateway sends the UDP packets. The default value <i>255.255.255.255</i> means that the broadcast address of the first LAN interface is used.
Client UDP Port	Port number for the bintec Activity Monitor (default value: <i>2107</i> , registered by IANA - Internet Assigned Numbers Authority).
Type	Type of information sent in the UDP packets to the Windows application. Possible values: <ul style="list-style-type: none"> ■ <i>off</i>: Deactivates the Activity Monitor (default value) ■ <i>physical</i>: Only information about physical interfaces ■ <i>physical_virt</i>: Information about physical and virtual interfaces
Update Interval (sec)	Update interval in seconds. Possible values: <i>0</i> to <i>60</i> (default value: <i>5</i>). The value <i>0</i> deactivates the function.

Table 2-1: **EXTERNAL ACTIVITY MONITOR** menu fields

3 Submenu External System Logging

The fields of the **EXTERNAL SYSTEM LOGGING** submenu are described below.

The **SYSTEM** → **EXTERNAL SYSTEM LOGGING** menu shows the log host settings.

R4100 Setup Tool [SYSTEM] [LOGGING] [ADD]	Funkwerk Enterprise Communications GmbH MyGateway
Log Host	
Level	info
Facility	local0
Type	all
Timestamp	none
Method	udp
SAVE	CANCEL

Events in the various subsystems of the gateway (e.g. ►► **PPP**) are logged in the form of syslog messages (system logging messages), see “System Menu” on page 3. The number of messages visible depends on the level set (eight steps from *emerg* and *info* to *debug*).

In addition to the data logged internally on the gateway, all information can and should also be passed to one or more external PCs for storage and processing, e.g. to the system administrator’s PC. The syslog messages saved internally on the gateway are lost on a restart.



Make sure you only pass syslog messages to a safe computer. Check the data regularly and ensure that there is always enough spare capacity available on the hard disk of your PC.

Syslog Daemon All Unix operating systems support the recording of syslog messages. For Windows PCs, the Syslog Daemon included in the **DIME Tools** can record the data and distribute to various files depending on the contents (see **BRICKware for Windows**).

The settings for saving syslog messages externally are made in **SYSTEM** → **EXTERNAL SYSTEM LOGGING** → **ADD/EDIT**.

The menu consists of the following fields:

Field	Description
Log Host	➤➤ IP address of the host to which syslog messages are passed.
Level	<p>Priority of the syslog messages to be sent to LOG HOST. The possible values correspond to those in “Message Level for the Syslog Table” on page 5.</p> <p>Only syslog messages with the same or higher priority than indicated are passed to the LOG HOST, i.e. all the messages created are passed to the LOG HOST in syslog LEVEL Debug.</p>
Facility	<p>Syslog facility at LOG HOST. Only required if the LOG HOST is a Unix computer.</p> <p>Possible values: <i>local0</i> - 7 (default value <i>local0</i>).</p>
Type	<p>Message type. Possible values:</p> <ul style="list-style-type: none"> ■ <i>all</i>: All messages (default value) ■ <i>system</i>: Syslog messages except ➤➤ accounting messages. ■ <i>accounting</i>: Accounting messages
Timestamp	<p>Format of the system time of the gateway in the syslog. Possible values:</p> <ul style="list-style-type: none"> ■ <i>all</i>: System time with date ■ <i>time</i>: System time without date ■ <i>none</i>: No system time shown (default value)

Field	Description
Method	Protocol for sending syslog messages. Possible values: <ul style="list-style-type: none">■ <i>udp</i> (default value)■ <i>tcp</i>

Table 3-1: **EXTERNAL SYSTEM LOGGING** menu fields

4 Submenu Schedule & Monitor

The fields of the *SCHEDULE & MONITOR* submenu are described below.

The *SCHEDULE & MONITOR* menu offers access to other submenus:

- *KEEPALIVE MONITORING (HOSTS & IFC)*
- *EVENT SCHEDULER (TIME & SNMP)*

4.1 Submenu Keepalive Monitoring (Hosts & Ifc)

The *SYSTEM → SCHEDULE & MONITOR → KEEPALIVE MONITORING* menu contains settings for the "Keepalive Monitoring" feature.

Keepalive Monitoring cannot be configured in the gateway for WAN partners that are authenticated via a RADIUS server!

SYSTEM → SCHEDULE & MONITOR → KEEPALIVE MONITORING lists the *hosts* and *interfaces* monitored by Keepalive Monitoring. The reachability of the hosts is listed under **STATE**: *alive* if the host was reachable on the last check, *down* if the host was not reachable.

The *WHAT TO MONITOR*: menu is used to set whether the configuration is made for *hosts* or *interfaces*.

WHAT TO MONITOR: hosts

R4100 Setup Tool		Funkwerk Enterprise Communications GmbH	
[SYSTEM] [KEEPALIVE MONITORING] [ADD]: Host Monitoring		MyGateway	
Group	0		
IPAddress			
Interval	300		
Trials	3		
Source IP			
DownAction	down		
FirstIfIndex	10001		
Range	4999		
SAVE		CANCEL	

If *hosts* has been selected, the **KEEPALIVE MONITORING** → **ADD/EDIT** menu consists of the following fields:

Field	Description
Group	Defines a group of hosts, whose reachability is to be monitored by the gateway. Each host to be monitored is assigned to a group. A total of 256 groups can be created. Possible values: 0 (default value) ... 255.
IP Address	Defines a host that is to be monitored by the gateway.
Interval	Defines the time interval in seconds to be used for checking the reachability of hosts. Possible values: 1 ... 65536 (default value: 300 s). The smallest INTERVAL of the group members is used within a group.
Trials	Defines the number of pings, that are sent to check the availability of hosts. Possible values: 1 ... 65536 (default value: 3).

Field	Description
Source IP	The IP address that the gateway uses as source address of the packet sent to the host to be monitored.
DownAction	<p>Defines how the status of the gateway interfaces selected in FIRSTINDEX and RANGE is set if all hosts in a group are not reachable. Possible values:</p> <ul style="list-style-type: none"> ■ <i>down</i>: Interfaces are deactivated, i.e. admin status is set to <i>down</i>. (Default value) ■ <i>none</i>: No action, i.e. admin status is set to <i>up</i>. ■ <i>up</i>: Interfaces are activated. <p>The status of the interfaces is set to the original value again when at least one host in a group can be reached again.</p> <p>Note: DOWNACTION must be configured identically within a group!</p>
FirstIfIndex	<p>Only for DOWNACTION = <i>up</i> or DOWNACTION = <i>down</i>.</p> <p>Defines the first interface of an interface range in the gateway, for which the action (<i>down</i> or <i>up</i>) defined under DOWNACTION is to be executed.</p> <p>Possible values: 100 .. 65536</p> <p>Default value: 10001</p> <p>Interfaces with indices from 10001 to 14999 are provided for dialup connections to WAN partners. You can find the indices of the interfaces with, for example, the command <code>ifstat</code>.</p>

Field	Description
Range	<p>Only for DOWNACTION = <i>up</i> or DOWNACTION = <i>down</i>.</p> <p>Defines the range of interfaces in the gateway, for which the action defined under DOWNACTION is to be executed.</p> <p>Default value: 4999</p> <p>If you set FIRSTINDEX = 10001 and RANGE = 1, only the interface with the index 10001 is affected.</p> <p>If you set FIRSTINDEX = 10001 and RANGE = 19, the interfaces with the indices 10001 to 10020 are affected.</p>

Table 4-1: Fields in **KEEPALIVE MONITORING** hosts menu

WHAT TO MONITOR: Interfaces

VR4100 Setup Tool		Funkwerk Enterprise Communications GmbH	
[SYSTEM] [KEEPALIVE MONITORING] [ADD]: Interface Monitoring		MyGateway	
Interface	0	Trigger	down
Action			none
SAVE		CANCEL	

If **WHAT TO MONITOR: interfaces** has been selected, the **KEEPALIVE MONITORING** → **ADD/EDIT** menu consists of the following fields:

Field	Description
Interface	<p>Defines the interface to be monitored in the gateway.</p> <p>Enter the interface INDEX here. The INDEX can be determined, for example, with the command <code>ifstat</code>.</p> <p>Default value: <code>0</code>.</p>
Trigger	<p>Defines the status of INTERFACE, which initiates a certain ACTION.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ <i>down</i>: Interface is deactivated (default value) ■ <i>up</i>: Interface is activated
Action	<p>Defines the action that is to follow the status defined in TRIGGER. The action is executed on the interface range from FIRSTINDEX and FIRSTINDEX + RANGE.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ <i>none</i>: No action (default value) ■ <i>down</i>: Deactivation of interface(s) ■ <i>up</i>: Activation of interface(s)

Field	Description
FirstIfIndex	<p>Defines the first interface of an interface range in the gateway, for which the action (<i>down</i> or <i>up</i>) defined under DOWNACTION is to be executed.</p> <p>Possible values: 100 .. 65536</p> <p>Default value: 10001</p> <p>Interfaces with indices from 10001 to 14999 are provided for dialup connections to WAN partners. You can find the indices of the interfaces with, for example, the command <code>ifstat</code>.</p>
Range	<p>Defines the range of interfaces in the gateway, for which the action defined under ACTION is to be executed.</p> <p>If you set FIRSTIFINDEX = 10001 and RANGE = 0, only the interface with the index 10001 is affected.</p> <p>If you set FIRSTIFINDEX = 10001 and RANGE = 4999 (default value), the interfaces with the indices 10001 to 14999 are affected.</p>

Table 4-2: Fields in **KEPALIVE MONITORING interfaces** menu

4.2 Submenu Event Scheduler (Time & SNMP)

Your gateway is equipped with an event scheduler, which makes it possible to modify existing MIB variables as soon as a certain event (e.g. time-dependent) occurs.

In general, any event in the MIB can be defined as the trigger.



Standard actions are the time or data volume dependent activation resp. deactivation of interfaces.

The configuration of actions that are not available as defaults requires extensive knowledge of the method of operation of bintec gateways. An incorrect configuration can cause considerable disturbances in operation. If applicable, save the original configuration e.g. on your PC.

The event scheduler is configured in the **SYSTEM → SCHEDULE & MONITOR → EVENT SCHEDULER (TIME & SNMP)** menu:

R4100 Setup Tool	Funkwerk Enterprise Communications GmbH
[SYSTEM] [SCHEDULED]: Event Schedule	MyGateway
Event Scheduler	disabled
Schedule Events >	
Schedule Commands >	
SAVE	CANCEL

Activate (*enabled*) or deactivate (*disabled*) the scheduler in the **EVENT SCHEDULER** field; the default setting is deactivated. When the **EVENT SCHEDULER** is activated, the schedule interval is set to 300 seconds as default.

Configure the events that are to initiate a certain action at the gateway in the **SCHEDULE EVENTS** menu and the actions to be executed in the **SCHEDULE COMMANDS** menu. The triggers (events) can be linked to event chains, so that complex conditions for initiating an action can also be created.

To be able to use the Event Scheduler function, the date on the gateway must be at least January 1, 2000.

4.2.1 Configuration of triggers (Events)

The **SYSTEM → SCHEDULE & MONITOR → EVENT SCHEDULER (TIME & SNMP) → SCHEDULE EVENTS** menu displays a list of all already configured events.

New events are added with **ADD**, existing entries are modified with **EDIT**.

Menu with *TYPE = time*:

R4100 Setup Tool		Funkwerk Enterprise Communications GmbH	
[SYSTEM] [SCHEDULED] [SCHED_EVT] [ADD]: Scheduler Events		MyGateway	
Index	1	Description	
NextIndex	none		
Type	time		
Condition		daily	
Start time (hh:mm)			
End time (hh:mm)			
Status		notavail	
	SAVE		CANCEL

Menu with *TYPE = value*:

R4100 Setup Tool		Funkwerk Enterprise Communications GmbH	
[SYSTEM] [SCHEDULED] [SCHED_EVT] [ADD]: Scheduler Events		MyGateway	
Index	1	Description	
NextIndex	none		
Type	value		
Monitored event		user defined	
Table			
Variable			
Index variable			
Index value			
Condition		range	
Compare value			
End value			
Status		notavail	
	SAVE		CANCEL

The menu contains the following fields depending on the setting:

Field	Description
Index	<p>The gateway assigns an index number for the entry automatically. This value can also be edited. The index defines the order of display in SYSTEM → SCHEDULE & MONITOR → EVENT SCHEDULER (TIME & SNMP) → SCHEDULE EVENTS.</p> <p>It should be unique.</p> <p>Possible settings: 1 to 65535.</p>
Description	<p>Here you enter the desired description for the event. The maximum length of the entry is 30 characters.</p>
NextIndex	<p>Here you select from the existing entries the entry that is to follow the current entry in an event chain if applicable. The entries in an event chain form a complex condition for an action to be executed. How the event chain leads to an action is configured in the SYSTEM → SCHEDULE & MONITOR → EVENT SCHEDULER (TIME & SNMP) → SCHEDULE COMMANDS menu.</p>
Type	<p>Here you select the type of event:</p> <p>Possible settings:</p> <ul style="list-style-type: none"> ■ <i>time</i> - The action is initiated time dependent (default value). Please make sure the gateway system time is set correctly! ■ <i>value</i> - The action is initiated depending on a MIB variable.

Field	Description
Monitored event	<p>Only for TYPE = value.</p> <p>Here you can choose between different events. Possible settings:</p> <ul style="list-style-type: none"> ■ <i>user defined</i> - The event is defined depending on the value of a specific MIB variable (default value). ■ <i>WAN interface total charge</i> - The event is defined depending on the fees summed up for an ISDN interface. ■ <i>WAN interface total duration</i> - The event is defined depending on the total connection duration of a ppp interface. ■ <i>WAN interface total RX traffic</i> - The event is defined depending on the total received data volume of a ppp interface. ■ <i>WAN interface total TX traffic</i> - The event is defined depending on the total sent data volume of a ppp interface.
Table	<p>Only for MONITORED EVENT = user defined.</p> <p>Here you enter the name of the MIB table containing the MIB variable that is to be used for the trigger, e.g. BIBOPPPSTATABLE.</p>
Variable	<p>Only for MONITORED EVENT = user defined.</p> <p>Here you enter the name of the MIB variable that is to be used for the trigger, e.g. TOTALDURATION.</p>

Field	Description
Index variable	<p>Only for MONITORED EVENT = <i>user defined</i>.</p> <p>Here you enter the name of the MIB variable in TABLE that is to be used as "index" to clearly define one specific data record in the table, e.g. <i>ConnIfIndex</i>.</p> <p>The combination of INDEX VARIABLE and INDEX VALUE defines the specific table entry.</p>
Index value	<p>Only for MONITORED EVENT = <i>user defined</i>.</p> <p>Here you enter the value of the INDEX VARIABLE that clearly defines the data record that contains the required trigger variable, e.g. <i>10001</i> for CONNIFINDEX.</p>

Field	Description
Condition	<p>For TYPE = time:</p> <ul style="list-style-type: none"> ■ <i>daily</i> - The trigger becomes active daily (default value). ■ <i><day of week></i> - The trigger becomes repeatedly active on a certain day of the week. ■ <i>mon_fri</i> - The trigger becomes active daily from Monday to Friday. ■ <i>mon_sat</i> - The trigger becomes active daily from Monday to Saturday. ■ <i>sat_sun</i> - The trigger becomes repeatedly active on Saturdays and Sundays only. ■ <i>day <1 .. 31></i> - The trigger becomes repeatedly active on a certain day of each month. <p>For TYPE = value:</p> <ul style="list-style-type: none"> ■ <i>range</i> - The trigger becomes active if the value of the variable is in the range of COMPARE VALUE and END VALUE (default value). ■ <i>greater</i> - The trigger becomes active if the value of the variable exceeds COMPARE VALUE. ■ <i>equal</i> - The trigger becomes active if the value of the variable is COMPARE VALUE. ■ <i>less</i> - The trigger becomes active if the value of the variable is below COMPARE VALUE. ■ <i>notequal</i> - The trigger becomes active if the value of the variable is not COMPARE VALUE.

Field	Description
Compare value	<ul style="list-style-type: none"> ■ For MONITORED EVENT = <i>user defined</i> and TYPE = <i>value</i>. The compare value relevant for VARIABLE. For CONDITION = <i>range</i> this is the start value of the range. ■ For MONITORED EVENT not <i>user defined</i> and TYPE = <i>value</i>. The compare value relevant for MONITORED EVENT.
End value	For CONDITION = <i>range</i> The end value of the range of values.
Start time (hh:mm)	Only for TYPE = <i>time</i> . Here you enter the time starting at which the trigger is to be activated. Activation is executed with the next schedule intervall.
End time (hh:mm)	Only for TYPE = <i>time</i> . Here you enter the time starting at which the trigger is to be deactivated. Deactivation is executed with the next schedule intervall. If no END TIME is entered or END TIME is set equal to START TIME , the trigger is activated and deactivated after 10 seconds.

Field	Description
Status	<p>This field cannot be edited and shows the status of the trigger.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ <i>error</i> - An error has occurred; the configuration of the trigger is not consistent. ■ <i>notavail</i> - The status cannot be determined, e.g. if the scheduler has not yet been activated. <p>Possible values for <i>TYPE = time</i>:</p> <ul style="list-style-type: none"> ■ <i>active</i> - The trigger is currently active. ■ <i>inactive</i> - The trigger is inactive.

Table 4-3: **SYSTEM → SCHEDULE & MONITOR → EVENT SCHEDULER (TIME & SNMP) → SCHEDULE EVENTS → ADD/EDIT**

4.2.2 Configuration of the Action (Command)

The **SCHEDULE COMMANDS** menu is described below.

The **SYSTEM → SCHEDULE & MONITOR → EVENT SCHEDULER (TIME & SNMP) → SCHEDULE COMMANDS** menu displays a list of all already configured actions.

Entries are added or modified in the **SYSTEM → SCHEDULE & MONITOR → EVENT SCHEDULER (TIME & SNMP) → SCHEDULE COMMANDS → ADD/EDIT** menu.

Menu with EXECUTE
COMMAND = user defined

R4100 Setup Tool		Funkwerk Enterprise Communications GmbH	
[SYSTEM] [SCHEDULED] [SCHED_CMD] [ADD]: Scheduler Commands		MyGateway	
Index	1	Description	
Mode		enable	
1. Event Index		none	
Eventlist Condition		all	
Execute command		user defined	
Table			
Variable			
Index variable			
Index value			
Set value active			
value inactive			
Notify		all	
Status	notavail	Last Change	01/01/1970 0:00:00
	SAVE		CANCEL

Menu with EXECUTE
COMMAND = disable
interface oder enable
interface

R4100 Setup Tool		Funkwerk Enterprise Communications GmbH	
[SYSTEM] [SCHEDULED] [SCHED_CMD] [ADD]: Scheduler Commands		MyGateway	
Index	1	Description	
Mode		enable	
1. Event Index		none	
Eventlist Condition		all	
Execute command		disable interface	
Interface		enl-0	
Notify		all	
Status	notavail	Last Change	01/01/1970 0:00:00
	SAVE		CANCEL

Menu with EXECUTE

COMMAND = exec
applicatopm

R4100 Setup Tool		Funkwerk Enterprise Communications GmbH	
[SYSTEM] [SCHEDULED] [SCHED_CMD] [ADD]: Scheduler Commands		MyGateway	
Index	1	Description	
Mode		enable	
1. Event Index		none	
Eventlist Condition		all	
Execute command		exec application	
Appl.name			
Argum.list active			
Argum.list inactive			
Notify		all	
Status	notavail	Last Change	01/01/1970 0:00:00
SAVE		CANCEL	

The menu contains the following fields depending on the setting selected:

Field	Description
Index	The gateway assigns an index number for the entry automatically. This value can also be edited. The index defines the order of display in SYSTEM → SCHEDULE & MONITOR → EVENT SCHEDULER (TIME & SNMP) → SCHEDULE COMMANDS . It should be unique. Possible settings: 1 to 65535.
Description	Here you enter the desired description for the action. The maximum length of the entry is 30 characters.

Field	Description
Mode	<p>Here you select if the configured action is to be enabled or not.</p> <p>Possible settings:</p> <ul style="list-style-type: none"> ■ <i>enable</i> (default value); action is enabled. ■ <i>disable</i>; action is disabled.
1. Event Index	<p>Here you choose the beginning of the event chain that is to control the action.</p> <p>The default value is <i>none</i>.</p>
Eventlist Condition	<p>Here you define how many entries of the selected event chain must occur before an action is executed.</p> <p>Possible settings:</p> <ul style="list-style-type: none"> ■ <i>all</i> - The action is to be active if all events of the event chain are active (default value). ■ <i>one</i> - The action is to be active if at least one of the events of the event chain is active. ■ <i>none</i> - The action is to be active if none of the events of the event chain is active. ■ <i>one_not</i> - The action is to be active if at least one of the events of the event chain is not active..

Field	Description
Execute command	<p>Here you define the action that is executed by a trigger.</p> <p>Possible settings:</p> <ul style="list-style-type: none"> ■ <i>disable interface</i> - The interface set in the INTERFACE field is deactivated (its ADMINSTATUS is set to <i>down</i>). ■ <i>enable interface</i> - The interface set in the INTERFACE field is activated (its ADMINSTATUS is set to <i>up</i>). ■ <i>user defined</i> (default value)- The action is defined by a MIB variable. ■ <i>exec application</i>: The Shell application specified in APPL. NAME is to be executed.
Interface	<p>Only for EXECUTE COMMAND = <i>disable interface</i> resp. <i>enable interface</i>.</p> <p>Here you select which interface is to be activated or deactivated.</p>
Table	<p>Only for EXECUTE COMMAND = <i>user defined</i>.</p> <p>Here you enter the name of the MIB table containing the variable to be set, e.g. <i>ifTable</i>.</p>
Variable	<p>Only for EXECUTE COMMAND = <i>user defined</i>.</p> <p>Here you enter the name of the MIB variable to be set, e.g. <i>AdminStatus</i>.</p>
Index variable	<p>Only for EXECUTE COMMAND = <i>user defined</i>.</p> <p>Here you enter the name of the MIB variable in TABLE that is to be used as "index" to clearly define one specific data record in the table, e.g. <i>Index</i>.</p> <p>The combination of INDEX VARIABLE and INDEX VALUE defines the specific table entry.</p>

Field	Description
Index value	Only for EXECUTE COMMAND = <i>user defined</i> . Here you enter the value of the INDEX VARIABLE that clearly defines the data record that contains the required trigger variable, e.g. 10001 for INDEX .
Set value active	Only for EXECUTE COMMAND = <i>user defined</i> . Here you enter the value the VARIABLE is to be assigned when the action is active.
value inactive	Only for EXECUTE COMMAND = <i>user defined</i> . Here you enter the value the VARIABLE is to be assigned when the action is inactive.
Appl. name	Only for EXECUTE COMMAND = <i>exec application</i> . Here you specify the command, the scheduler is to execute, e.g. update.
Argum.list active	Only for EXECUTE COMMAND = <i>exec application</i> . Here you can specify arguments (options) the scheduler is to use with the command as soon as the Schedule Event becomes active and the command is to be executed.
Argum.list inactive	Only for EXECUTE COMMAND = <i>exec application</i> . Here you can specify arguments (options) the scheduler is to use with the command as soon as the Schedule Event becomes inactive and the command is to be executed.

Field	Description
Notify	<p>Here you select if syslog messages or traps are generated for this action.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ <i>all</i> - Both SNMP traps and syslog messages can be generated. (Default value) ■ <i>snmptrap</i> - Only traps can be generated. ■ <i>syslog</i> - Only syslog messages are generated. ■ <i>none</i> - No syslog messages or traps are generated. <p>To generate SNMP traps you must, if applicable, generate a respective entry in the <i>BIBOADMUSRTRAPTABLE</i>.</p>
Status	<p>This field cannot be edited and shows the status of the action.</p> <p>Possible values:</p> <ul style="list-style-type: none"> ■ <i>active</i> - The action is currently active. ■ <i>inactive</i> - The action is inactive. ■ <i>notavail</i> - The status cannot be determined, e.g. if the scheduler is not activated or no event has been assigned. ■ <i>error</i> - The configuration of the action is not consistent.
Last Change	<p>Shows the time of the last status change. This field cannot be edited.</p>

Table 4-4: **SYSTEM → SCHEDULE & MONITOR → EVENT SCHEDULER (TIME & SNMP) → SCHEDULE COMMANDS → ADD/EDIT**

5 Submenu Password Settings

The fields of the *PASSWORD SETTINGS* submenu are described below.

R4100 Setup Tool	Funkwerk Enterprise Communications GmbH
[SYSTEM] [PASSWORDS]: Change System Passwords	MyGateway
<pre> admin Login Password/SNMP Community ***** read Login Password/SNMP Community ***** write Login Password/SNMP Community ***** HTTP Server Password ***** Activity Monitor Password </pre>	
SAVE	CANCEL

Setting the passwords is one of the basic system settings. (Detailed information about the user rights of the various users can be found in **Access and Configuration**.)

The *PASSWORD SETTINGS* menu consists of the following fields:

Field	Description
admin Login Password/SNMP Community	Password for user name <code>admin</code> .
read Login Password/SNMP Community	Password for user name <code>read</code> .
write Login Password/SNMP Community	Password for user name <code>write</code> .
HTTP Server Password	Password for the system variables pages accessible via the HTTP status page of your gateway.
Activity Monitor Password	Password for the ACTIVITY MONITOR .

Table 5-1: *PASSWORD SETTINGS* menu fields

**Attention!**

All bintec gateways are shipped with the same user name and password. As long as the password remains unchanged, they are not protected against unauthorized use.

Change the password to prevent unauthorized access to the gateway.

As long as the password remains unchanged, the following warning appears on logging in: "Password not changed".

6 Submenu Time and Date

The fields of the *TIME AND DATE* submenu are described below.

R4100 Setup Tool	Funkwerk Enterprise Communications GmbH	
[SYSTEM] [TIME]: Control System Time and Date	MyGateway	
Current System Time: Wed 2005/Feb/28 19:19:37 setby: None		
Change System Time:	2005/Feb/28 19:19:17	CHANGE
Time Update Interval	: 86400	Seconds
Update System Time from ISDN	: disabled	
System Time Offset from GMT	: 0	Seconds
Time Servers:		
	Name/Address	Protocol
1:		SNTP
2:		SNTP
3:		SNTP
	SAVE	CANCEL

System time You need the system time for tasks such as correct timestamps for system messages, accounting or IPSec certificates.

You can derive the system time:

- automatically, e.g. via different time servers.
- manually in the gateway.



Note

If a method for deriving the time automatically is set in the gateway, the values obtained in this way have higher priority. Any system time entered manually is overwritten.

The menu for the configuration of the time retrieval is accessible via the **SYSTEM** menu (**SYSTEM → TIME AND DATE**).

To assure that your gateway uses the correct current time, it is recommended to configure time servers.

The menu consists of the following fields:

Field	Description
Current System Time	Here the current date and system time are displayed. The entry cannot be changed. <i>SET BY</i> displays how the time has been set.
Change System Time	Here you can manually set the current date and system time. The modification is set with CHANGE .
Time Update Interval	Here you enter the interval (in seconds) at which automatic time updates are carried out. Default value is <i>86400</i> .
Update System Time from ISDN	Here you can choose whether the time information received at the beginning of an incoming ISDN connection is used to update the system time. This option is used as long as a time update has been received from a time server since boot time. Available values are <i>enabled</i> and <i>disabled</i> , the default value is <i>disabled</i> .
System Time Offset from GMT	Here you enter the offset (in seconds) between system time and time received from the time server. Values between <i>1</i> and <i>23</i> are interpreted as hours and are converted to seconds upon saving the configuration. Positive values can be entered as well as negative ones, the default value is <i>0</i> .
Name/Address	Here you can enter up to three time servers, either by their domain name or by their IP address.

Field	Description
Protocol	<p>Here you choose the protocol used for querying the time server.</p> <p>Possible values:</p> <ul style="list-style-type: none">■ <i>SNTP</i> - This server uses the Simple Network Time Protocol with UDP port 123.■ <i>disabled</i> - This time server is currently not used for time retrieval.■ <i>TIME/UDP</i> - This server uses the Time-service with UDP port 37.■ <i>TIME/TCP</i> - This server uses the Time-service with TCP port 37.

Table 6-1: **SYSTEM** → **TIME AND DATE**

Index: System

Numerics	1st Event index	29
A	Action	17
	Activity Monitor	7
	Appl. name	31
	Argum.list active	31
	Argum.list inactive	31
B	Basic system data	3
C	Central server	13
	Change System Time	36
	CLID	13
	Client IP address	8
	Client UDP port	8
	Compare value	25
	Condition	24
	Contact	4
	Current System Time	36
D	Description	21, 28
	DownAction	15
E	End time	25
	End value	25
	Event protocol	9
	Eventlist condition	29
	Execute command	30
	External Activity Monitor	7
	External system logging	9
F	Facility	10
	FirstIfIndex	15, 18

G	Group	14
H	Hosts	13
I	Index	21, 28
	Index value	23, 31
	Index variable	23, 30
	Interface	17, 30
	Interfaces	13
	Interval	14
	IP address	14
K	Keepalive Monitoring	13
L	LAN	13
	Last change	32
	Level	10
	Local PPP ID (default)	3
	Location	4
	Log host	9, 10
M	Maximum Number of Acctlog Entries	5
	Maximum number of syslog entries	5
	Message level for the syslog table	5
	Method	11
	Mode	29
	Monitored event	22
N	Name/Address	36
	Next index	21
	Notify	32

P	Password settings	33
	Activity Monitor	33
	admin	33
	Ex works state	33
	HTTP server	33
	read	33
	write	33
	Protocol	37
R	Range	16, 18
S	Set value active	31
	Source IP	15
	Start time	25
	Status	26, 32
	Subsystems	9
	Syslog messages	9
	Syslog output on serial console	4
	System name	3
	System time	35
	Accounting	35
	Automatic	35
	Manual	35
	System Time Offset from GMT	36
T	Table	22, 30
	Time and date	35
	Time Update Interval	36
	Timestamp	10
	Trials	14
	Trigger	17
	Type	8, 10, 21
U	Update interval	8
	Update System Time from ISDN	36

V Value inactive
Variable

31
22, 30