SYSTEM

System

1 System Menu

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

```
R232bw Setup Tool              Funkwerk Enterprise Communications GmbH
[SYSTEM]: Change System Parameters                        MyGateway


 System Name                r232bw
 Local PPP ID (default)     r232bw
 Location
 Contact                    BINTEC


 Syslog Output on Serial Sonsole      no
 Message Level for the Syslog Table   info
 Maximum Number of Syslog Entries     20
 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	Indicates where your gateway is located.
	Is shown, for example, on the HTML system information page or in the login message.
Contact	Indicates the responsible contact person. Here you can enter the e-mail address of the system administrator, for example.
	Default value: *BINTEC*.
	Is shown, for example, on the HTML system information page.
Syslog Output on Serial Console	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.
	You should normally use *EXTERNAL SYSTEM LOGGING*. Possible values:
	■ *yes*
	■ *no* (default value)

Field	Description
Message Level for the Syslog Table	Specifies the priority of the syslog messages to be recorded internally. Possible values: ■ *emerg*: emergency messages (highest priority) ■ *alert*: alert messages ■ *crit*: critical messages ■ *err*: error messages ■ *warning*: warning messages ■ *notice*: notice messages ■ *info* (default value): info messages ■ *debug*: debug messages (lowest priority) 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 *debug*.
Maximum Number of Syslog Entries	Maximum number of syslog messages saved internally in the gateway (possible values: *0 ... 1000*). Default value: *20*. You can show the saved messages in the Setup Tool under **MONITORING AND DEBUGGING** ➜ **MESSAGES**.
Maximum Number of Acctlog Entries	Maximum number of accounting messages saved internally in the gateway (possible values: *0 ... 1000*). Default value: *20*.

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

1 System Menu

2 Submenu External Activity Monitor

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

```
R232bw 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 *255.255.255.255* means that the broadcast address of the first LAN interface is used.
Client UDP Port	Port number for the bintec Activity Monitor (default value: *2107*, registered by IANA - Internet Assigned Numbers Authority).
Type	Type of information sent in the UDP packets to the Windows application. Possible values: ■ *off*: Deactivates the **Activity Monitor** (default value) ■ *physical*: Only information about physical interfaces ■ *physical_virt*: Information about physical and virtual interfaces
Update Interval (sec)	Update interval in seconds. Possible values: *0* to *60* (default value: *5*). The value *0* 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.

```
R232bw Setup Tool              Funkwerk Enterprise Communications GmbH
[SYSTEM][LOGGING][ADD]                                       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), . 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.

⚠️
Warning!

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	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. 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*.
Facility	Syslog facility at *LOG HOST*. Only required if the *LOG HOST* is a Unix computer. Possible values: *local0 - 7* (default value *local0*).
Type	Message type. Possible values: ■ *all*: All messages (default value) ■ *system*: Syslog messages except ➤➤ **accounting** messages. ■ *accounting*: Accounting messages
Timestamp	Format of the system time of the **R Series** gateway in the syslog. Possible values: ■ *all*: System time with date ■ *time*: System time without date ■ *none*: No system time shown (default value)

Field	Description
Method	Protocol for sending syslog messages. Possible values: ■ *udp* (default value) ■ *tcp*

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

```
R232bw Setup Tool              Funkwerk Enterprise Communications GmbH
[SYSTEM][KEEPALIVE MONITORING][ADD]: Host Monitoring          MyGateway


   Group                    0
   IPAddress
   Interval                 300
   Trials
   Source IP
   DownAction               down
   FirstIfIndex             10001
   Range                    4999



          SAVE                              CANCEL

```

If *hosts* has been selected, the **KEEPALIVE MONITORING** ➜ **ADD/EDIT** menu con-
sists 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	Defines how the status of the gateway interfaces selected in **FIRSTIFINDEX** and **RANGE** is set if all hosts in a group are not reachable. Possible values:
	■ *down*: Interfaces are deactivated, i.e. admin status is set to *down*. (Default value)
	■ *none*: No action, i.e. admin status is set to *up*.
	■ *up*: Interfaces are activated.
	The status of the interfaces is set to the original value again when at least one host in a group can be reached again.
	Note: **DOWNACTION** must be configured identically within a group!
FirstIfIndex	Defines the first interface of an interface range in the gateway, for which the action (*down* or *up*) defined under **DOWNACTION** is to be executed.
	Possible values: *100* .. *65536*
	Default value: *10001*
	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 `ifstat`.

Field	Description
Range	Defines the range of interfaces in the gateway, for which the action defined under *DOWNACTION* is to be executed. Default value: *4999* If you set *FIRSTIFINDEX* = *10001* and *RANGE* = *1*, only the interface with the index *10001* is affected. If you set *FIRSTIFINDEX* = *10001* and *RANGE* = *19*, the interfaces with the indices *10001* to *10020* are affected.

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

WHAT TO MONITOR: Interfaces

```
VR232bw 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	Defines the interface to be monitored in the gateway.
	Enter the interface **INDEX** here. The **INDEX** can be determined, for example, with the command `ifstat`.
	Default value: *0.*
Trigger	Defines the status of **INTERFACE**, which initiates a certain **ACTION**.
	Possible values:
	■ *down*: Interface is deactivated (default value)
	■ *up*: Interface is activated
Action	Defines the action that is to follow the status defined in **TRIGGER**. The action is executed on the interface range from **FIRSTIFINDEX** and **FIRSTIFINDEX** + **RANGE**.
	Possible values:
	■ *none:* No action (default value)
	■ *down*: Deactivation of interface(s)
	■ *up*: Activation of interface(s)

Field	Description
FirstIfIndex	Defines the first interface of an interface range in the gateway, for which the action (*down* or *up*) defined under *DOWNACTION* is to be executed.
	Possible values: *100 .. 65536*
	Default value: *10001*
	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 `ifstat`.
Range	Defines the range of interfaces in the gateway, for which the action defined under *ACTION* is to be executed.
	If you set *FIRSTIFINDEX* = *10001* and *RANGE* = *0*, only the interface with the index *10001* is affected.
	If you set *FIRSTIFINDEX* = *10001* and *RANGE* = *4999* (default value), the interfaces with the indices *10001* to *14999* are affected.

Table 4-2: Fields in *KEEPALIVE 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.

Attention!

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

```
R232bw 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*:

```
R232bw 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*:

```
R232bw 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	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*. It should be unique. Possible settings: *1* to *65535*.
Description	Here you enter the desired description for the event. The maximum length of the entry is 30 characters.
NextIndex	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.
Type	Here you select the type of event: Possible settings: ■ *time* - The action is initiated time dependent (default value). Please make sure the gateway system time is set correctly! ■ *value* - The action is initiated depending on a MIB variable.

Field	Description
Monitored event	Only for *TYPE* = *value*. Here you can choose between different events. Possible settings: ■ *user defined* - The event is defined depending on the value of a specific MIB variable (default value). ■ *WAN interface total charge* - The event is defined depending on the fees summed up for an ISDN interface. ■ *WAN interface total duration* - The event is defined depending on the total connection duration of a ppp interface. ■ *WAN interface total RX traffic* - The event is defined depending on the total received data volumn of a ppp interface. ■ *WAN interface total TX traffic* - The event is defined depending on the total sent data volumn of a ppp interface.
Table	Only for *MONITORED EVENT* = *user defined*. Here you enter the name of the MIB table containing the MIB variable that is to be used for the trigger, e.g. *BIBOPPPSTATTABLE*.
Variable	Only for *MONITORED EVENT* = *user defined*. Here you enter the name of the MIB variable that is to be used for the trigger, e.g. *TOTALDURATION*.

Field	Description
Index variable	Only for *MONITORED EVENT* = *user defined*. 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. *ConnIfIndex*. The combination of *INDEX VARIABLE* and *INDEX VALUE* defines the specific table entry.
Index value	Only for *MONITORED EVENT* = *user defined*. 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 *CONNIFINDEX*.

Field	Description
Condition	For *TYPE* = *time*:
	■ *daily* - The trigger becomes active daily (default value).
	■ *<day of week>* - The trigger becomes repeatedly active on a certain day of the week.
	■ *mon_fri* - The trigger becomes active daily from Monday to Friday.
	■ *mon_sat* - The trigger becomes active daily from Monday to Saturday.
	■ *sat_sun* - The trigger becomes repeatedly active on Saturdays and Sundays only.
	■ *day <1 .. 31>* - The trigger becomes repeatedly active on a certain day of each month.
	For *TYPE* = *value*:
	■ *range* - The trigger becomes active if the value of the variable is in the range of *COMPARE VALUE* and *END VALUE* (default value).
	■ *greater* - The trigger becomes active if the value of the variable exceeds *COMPARE VALUE*.
	■ *equal* - The trigger becomes active if the value of the variable is *COMPARE VALUE*.
	■ *less* - The trigger becomes active if the value of the variable is below *COMPARE VALUE*.
	■ *notequal* - The trigger becomes active if the value of the variable is not *COMPARE VALUE*.

Field	Description
Compare value	■ For **MONITORED EVENT** = *user defined* and **TYPE** = *value*. The compare value relevant for **VARIABLE**. For **CONDITION** = *range* this is the start value of the range. ■ For **MONITORED EVENT** not *user defined* and **TYPE** = *value*. The compare value relevant for **MONITORED EVENT**.
End value	For **CONDITION** = *range* The end value of the range of values.
Start time (hh:mm)	Only for **TYPE** = *time*. 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** = *time*. 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	This field cannot be edited and shows the status of the trigger. Possible values: ■ *error* - An error has occurred; the configuration of the trigger is not consistent. ■ *notavail* - The status cannot be determined, e.g. if the scheduler has not yet been activated. Possible values for *TYPE* = *time*: ■ *active* - The trigger is currently active. ■ *inactive* - 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

```
R232bw 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

```
R232bw 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             en1-0




     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.
Mode	Here you select if the configured action is to be enabled or not. Possible settings: ■ *enable* (default value); action is enabled. ■ *disable*: action is disabled.
1. Event Index	Here you choose the beginning of the event chain that is to control the action. The default value is *none*.

Field	Description
Eventlist Condition	Here you define how many entries of the selected event chain must occur before an action is executed. Possible settings: ■ *all* - The action is to be active if all events of the event chain are active (default value). ■ *one* - The action is to be active if at least one of the events of the event chain is active. ■ *none* - The action is to be active if none of the events of the event chain is active. ■ *one_not* - The action is to be active if at least one of the events of the event chain is not active..
Execute command	Here you define the action that is executed by a trigger. Possible settings: ■ *disable interface* - The interface set in the *INTERFACE* field is deactivated (its *ADMINSTATUS* is set to *down*). ■ *enable interface* - The interface set in the *INTERFACE* field is activated (its *ADMINSTATUS* is set to *up*). ■ *user defined* (default value)- The action is defined by a MIB variable.
Interface	Only for *EXECUTE COMMAND* = *disable interface* resp. *enable interface.* Here you select which interface is to be activated or deactivated.

Field	Description
Table	Only for **EXECUTE COMMAND** = *user defined*. Here you enter the name of the MIB table containing the variable to be set, e.g. *ifTable*.
Variable	Only for **EXECUTE COMMAND** = *user defined*. Here you enter the name of the MIB variable to be set, e.g. *AdminStatus*.
Index variable	Only for **EXECUTE COMMAND** = *user defined*. 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. *Index*. The combination of **INDEX VARIABLE** and **INDEX VALUE** defines the specific table entry.
Index value	Only for **EXECUTE COMMAND** = *user defined*. 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** = *user defined*. Here you enter the value the **VARIABLE** is to be assigned when the action is active.
value inactive	Only for **EXECUTE COMMAND** = *user defined*. Here you enter the value the **VARIABLE** is to be assigned when the action is inactive.

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

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.

```
R232bw Setup Tool              Funkwerk Enterprise Communications GmbH
[SYSTEM][PASSWORDS]: Change System Passwords                 MyGateway


  admin Login Password/SNMP Community  ******
  read  Login Password/SNMP Community  ******
  write Login Password/SNMP Community  ******
  HTTP Server Password                 ******
  Activity Monitor Password



        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 admin.
read Login Password/SNMP Community	Password for user name read.
write Login Password/SNMP Community	Password for user name write.
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.

```
R232bw 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. *SET BY* 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 *86400*.
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 *enabled* and *disabled*, the default value is *disabled*.
System Time Offset from GMT	Here you enter the offset (in seconds) between system time and time received from the time server. Values between *1* and *23* 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 *0*.
Name/Address	Here you can enter up to three time servers, either by their domain name or by their IP address.

Field	Description
Protocol	Here you choose the protocol used for querying the time server. Possible values: ■ *SNTP* - This server uses the Simple Network Time Protocol with UDP port 123. ■ *disabled* - This time server is currently not used for time retrieval. ■ *TIME*/*UDP* - This server uses the Time-service with UDP port 37. ■ *TIME*/*TCP* - This server uses the Time-service with TCP port 37.

Table 6-1: *SYSTEM* ➜ *TIME AND DATE*

6 Submenu Time and Date

Index: System