SYSTEM

Copyright © November 18, 2004 Funkwerk Enterprise Communications GmbH
Bintec User's Guide - VPN Access Series
Version 1.1

Purpose

This document is part of the user's guide to the installation and configuration of Bintec gateways running software release 7.1.4 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.bintec.net.

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.bintec.net.

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.bintec.net.

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

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

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SYSTEM]: Change System Parameters                              MyGateway

 System Name                  vpn25
 Local PPP ID (default)       vpn25
 Location                     European Union
 Contact                      BINTEC


 Syslog Output on Serial Sonsole       no
 Message Level for the Syslog Table    info
 Maximum Number of Syslog Entries      50

 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. Default value: *European Union* 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 **VPN Access** 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*: info messages (default value) ■ *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 **VPN Access** gateway (possible values: *0* ... *1000*). Default value: *50*. You can show the saved messages in the Setup Tool under ***MONITORING AND DEBUGGING*** ➜ ***MESSAGES***.

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.

```
VPN Access 25 Setup Tool                    Bintec Access Networks 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 **VPN Access** 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**).

Warning!

Avoid configuring a WAN partner that can be reached over an ISDN dialup connection as ***CLIENT IP ADDRESS***. This can cause high costs through frequently setting up ISDN connections.

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.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SYSTEM][LOGGING][ADD]                                        MyGateway


    Log Host
    Level                       info
    Facility                    local0
    Type                        all
    Timestamp                   none


          SAVE                                    CANCEL
```

Events in the various subsystems of the gateway (e.g. ➤➤ **ISDN**, ➤➤ **PPP**, etc.) 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.

Warning!

Avoid forwarding syslog messages to log hosts reached over a dialup connection. This can cause considerable costs.

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 ***External System Logging*** ➜ ***ADD/EDIT*** 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

Field	Description
Timestamp	Format of the system time of the **VPN Access** gateway in the syslog. Possible values: ■ *all*: System time with date ■ *time*: System time without date ■ *none*: No system time shown (default value)

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.

Example scenario

If you have connected two (or more) LANs over a dialup connection, e.g. between the LAN of the head office and the LAN of a branch office, a central server is frequently located in the LAN at the head office. If this central server is configured such that it regularly sets up WAN connections to the gateway in the LAN of the branch office, e.g. for updating data, these connections are superfluous (but not free) if none of the hosts in the branch office can be reached, e.g. because all PCs are switched off. As it is not possible to determine whether the hosts can be reached until the connection is set up, costs are incurred by the calling party, i.e. the head office.

The Keepalive Monitoring function enables you to configure the gateway in the branch office to avoid unnecessary WAN connections from the head office to the branch office. The gateway of the branch office checks at regular, adjustable intervals to see whether the hosts to be monitored in its LAN can be reached. If none of the hosts to be checked answers a corresponding request after three consecutive attempts, the gateway deactivates the interface to the WAN partner at the "head office". Calls from the head office to unreachable hosts are not accepted in the first place and no costs are incurred.

Note

In some countries (e.g. Switzerland), costs may still occur for these useless dial-in attempts in spite of using Keepalive Monitoring.

If all PCs in the LAN at the branch office were inactive, a connection to the head office is not set up automatically as soon as one of the PCs to be monitored is switched on. The interface to the "head office" WAN partner is not activated and a connection cannot be set up to the head office until the gateway in the branch office has registered that a PC can be reached. The amount of time that expires before the gateway indicates that a PC can be reached again depends on the monitoring interval set (***INTERVAL***).

Note

The corresponding remote terminal, e.g. the head office, must be identifiable in the gateway of the branch office using CLID (Calling Line Identification). If this is not the case, the described benefit of Keepalive Monitoring is not available.

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**

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SYSTEM][KEEPALIVE MONITORING][ADD]: Host Monitoring          MyGateway


  Group                     0
  IPAddress
  Interval                  300
  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 **VPN Access** 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 **VPN Access** 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.
Source IP	The IP address that the gateway uses as source address of the packet sent to the host to be monitored.

Field	Description
DownAction	Defines how the status of the **VPN Access** 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 **VPN Access** 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 **VPN Access** gateway, for which the action defined under ***DownAction*** is to be executed. Default value: *4999* If you set ***FirstIfIndex*** = *10001* and ***Range*** = *0*, 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**

```
VVPN Access 25 Setup Tool                    Bintec Access Networks 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 **VPN Access** 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

Field	Description
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)
FirstIfIndex	Defines the first interface of an interface range in the **VPN Access** 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 **VPN Access** 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)

From System Software 7.1.4 onwards, your gateway is equipped with an event scheduler, which makes it possible to make any entries in the MIB as soon as a certain event (also freely configurable) occurs.

Apart from default and easily configured standard applications like time- or volume-controlled activation or deactivation of interfaces, the event scheduler permits access to any MIB parameter. This means that any event in the MIB can be defined as the trigger of any desired action.

Attention!

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:

```
VPN Access 25 Setup Tool                    Bintec Access Networks 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 *300s* 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.

4.2.1 Configuration of triggers (Events)

The events that initiate a relevant action are created and edited in the *System* ➜ *Schedule & Monitor* ➜ *Event Scheduler (Time & SNMP)* ➜ *Schedule Events* ➜ *ADD/EDIT* menu.

The default menu opens with the mask for configuring an event of the *time* type:

```
VPN Access 25 Setup Tool                    Bintec Access Networks 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
```

If you select ***TYPE*** = *value*, the menu changes as follows:

```
VPN Access 25 Setup Tool                    Bintec Access Networks 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. Possible settings are all values from *1* to *65535*.
Description	Here you enter the desired description for the event. The maximum length of the entry is 30 characters.

Field	Description
NextIndex	Here you select from the existing entries the entry that is to follow the current entry in an event chain. 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 which type of event is to initiate an action: Possible settings: ■ *time* - The action is initiated at certain times (default value). Please make sure the gateway system time is set correctly! ■ *value* - The action is initiated as soon as a MIB variable becomes a certain value.

Field	Description
Monitored event	Only for ***TYPE*** = *value*. Here you can choose between different events. Possible settings: ■ *user defined* - You can choose which of the values and MIB variables the scheduler is to respond to with an action (default value). ■ *WAN interface total charge* - A trigger becomes active if a certain total charge limit is reached for all connections at a WAN interface (the interface is selected on configuring the action). The gateway must receive charging information from the provider for this purpose. ■ *WAN interface total duration* - A trigger becomes active if the total duration of all connections of a WAN interface (in seconds) has reached a certain value. ■ *WAN interface total RX traffic* - A trigger becomes active if a WAN interface has received a certain total amount of data (in bytes) for all connections. ■ *WAN interface total TX traffic* - A trigger becomes active if a WAN interface has sent a certain total amount of data (in bytes) for all connections.
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***.

Field	Description
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***.
Index variable	Only for ***MONITORED EVENT*** = *user defined*. Here you enter the name of the index variable of the previously defined MIB table. This is the variable marked with an asterisk (*) in the table view of the desired MIB table, e.g. ***CONNIFINDEX***.
Index value	Only for ***MONITORED EVENT*** = *user defined*. Here you enter the value of the ***INDEX VARIABLE*** for the table entry that is to be used for the trigger, e.g. *10001*.

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. ■ *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 the month. For ***TYPE*** = *value*: ■ *range* - The trigger becomes active if the value of the variable is in a certain range (default value). ■ *greater* - The trigger becomes active if the value of the variable exceeds a certain value. ■ *equal* - The trigger becomes active if the value of the variable is a certain value. ■ *less* - The trigger becomes active if the value of the variable is below a certain value. ■ *notequal* - The trigger becomes active if the value of the variable is not a certain value.
Compare value	Value with which the value of ***VARIABLE*** is compared under the condition defined in ***CONDITION***. If ***CONDITION*** = *range*, this is the start value of the range of values.

Field	Description
End value	If ***CONDITION*** = *range*, this is the end value of the range of values.
Start time (hh:mm)	Only for ***TYPE*** = *time*. Here you enter the time at which the trigger is to be activated.
End time (hh:mm)	Only for ***TYPE*** = *time*. Here you enter the time at which the trigger is to be deactivated.
Status	This field cannot be edited and shows the status of the trigger. Possible values: ■ *active* - The trigger is currently active. ■ *inactive* - The trigger is inactive. ■ *notavail* - The status cannot be determined, e.g. if the scheduler is not activated. ■ *error* - An error has occurred; the configuration of the trigger is not consistent.

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

4.2.2 Configuration of the Action (Command)

The action executed as soon as one of the events configured as trigger occurs is created or edited in the *SYSTEM ➜ SCHEDULE & MONITOR ➜ EVENT SCHEDULER (TIME & SNMP) ➜ SCHEDULE COMMANDS ➜ ADD/EDIT* menu.

The default menu opens for configuring the actions as follows:

```
VPN Access 25 Setup Tool                    Bintec Access Networks 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
```

If you select the value *user defined* for the ***EXECUTE COMMAND*** field, the menu changes as follows:

```
VPN Access 25 Setup Tool                    Bintec Access Networks 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
```

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. Possible settings are all values from *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	Here you select if the configured action is to be active or inactive. Possible settings: ■ *enable* (default value) ■ *disable*
1st Event Index	Here you define the first event of an event chain. The event chain is activated only by this entry, preceding entries are ignored. The default value is *none*.
Eventlist Condition	Here you define whether all the entries of an event chain must occur before an action is executed. Possible settings: ■ *all* - All events of an event chain must occur if the action is to be executed (default value). ■ *one* - At least one of the events of an event chain must occur if the action is to be executed. ■ *none* - None of the events of an event chain may occur if the action is to be executed. ■ *one_not* - At least one of the events of an event chain must not occur if the action is to be executed.

Field	Description
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*, default value). ■ *enable interface* - The interface set in the ***INTERFACE*** field is activated (its ***ADMINSTATUS*** is set to *up*). ■ *user defined* - The action is configured as desired in the following fields.
Interface	Here you select which interface is to be activated or deactivated if *disable interface* or *enable interface* is selected for ***EXECUTE COMMAND***.
Table	Only for ***EXECUTE COMMAND*** = *user defined*. Here you enter the MIB table containing the variable to be set, e.g. *ifTable*.
Variable	Only for ***EXECUTE COMMAND*** = *user defined*. Here you enter the MIB variable to be set, e.g. *AdminStatus*.
Index variable	Only for ***EXECUTE COMMAND*** = *user defined*. Here you enter the index variable of the previously selected MIB table. This is the variable marked with an asterisk (*) in the table view of the desired MIB table, e.g. *Index*.
Index value	Only for ***EXECUTE COMMAND*** = *user defined*. Here you enter the value of the index variable for the table entry that is to be changed by the action, e.g. *10001*.

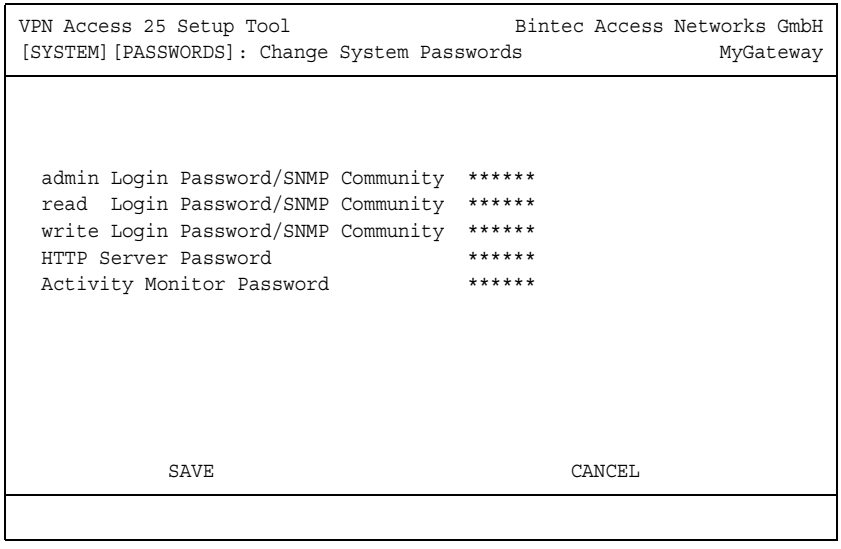
Field	Description
Set value active	Only for ***EXECUTE COMMAND*** = *user defined*. Here you enter the value the ***VARIABLE*** is to be assigned by the action. The value is set as soon as an appropriate trigger becomes active and is retained until the trigger becomes inactive again.
value inactive	Only for ***EXECUTE COMMAND*** = *user defined*. Here you enter the value the ***VARIABLE*** is to become as soon as the trigger becomes inactive. This value is also assigned to the variable after a gateway restart or if the system time is not set correctly.
Notify	Here you select the mechanisms to be used to notify actions. Possible settings: ■ *all* - Both SNMP traps and syslog messages are generated. (Default value) ■ *snmptrap* - Only SNMP traps are generated. ■ *syslog* - Only syslog messages are generated. ■ *none* - No messages are generated.
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. ■ *error* - An error has occurred; the configuration of the action is not consistent.

Field	Description
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.



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 HTTP status page of your gateway.

Field	Description
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.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[SYSTEM][TIME]: Set System Time and Date                      MyGateway

     Time is currently controlled by:            ISDN

     Current Time:
     Tue Jan 13   6:24:52  1970



     New Time: 06:23

     New Date: 01/13/1970




              SET                                BACK
```

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 ISDN or a time server. The relevant configuration is made in the ***IP*** ➜ ***STATIC SETTINGS*** menu.
- 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 ***SYSTEM*** ➜ ***TIME AND DATE*** menu contains the settings for manually entering the time and date in your gateway.

The ***TIME AND DATE*** menu consists of the following fields:

Field	Description
Time is currently controlled by:	Shows the settings defined under ***IP*** ➜ ***STATIC SETTINGS*** for deriving the time automatically.
Current Time:	Shows the system time (date and time) currently set in the **VPN Access** gateway.
New Time:	Here you enter the new time to be used by the **VPN Access** gateway (hh:mm).
New Date:	Here you enter the new date to be used by the **VPN Access** gateway (mm/dd/yyyy).

Table 6-1: ***TIME AND DATE*** menu fields

Index: System