

# **ACCESS AND CONFIGURATION**

Copyright © 18. November 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](http://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](http://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](http://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: <a href="http://www.funkwerk-ec.com">www.funkwerk-ec.com</a>	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: <a href="http://www.bintec.fr">www.bintec.fr</a>
--	---



<b>1</b>	<b>About this Manual</b> .....	<b>3</b>
1.1	Contents .....	3
1.2	Use of Typographical Elements .....	5
<b>2</b>	<b>Access Options</b> .....	<b>7</b>
2.1	Access via Serial Interface .....	7
2.1.1	Access via Serial Connection .....	7
2.2	Access via LAN .....	9
2.2.1	Telnet .....	9
2.2.2	SSH .....	10
2.3	Access via ISDN .....	12
<b>3</b>	<b>Login</b> .....	<b>15</b>
3.1	User Names and Passwords in Ex Works State .....	15
3.2	Login for Configuration .....	16
<b>4</b>	<b>Configuration Options</b> .....	<b>19</b>
4.1	<b>HTML Wizard</b> .....	<b>20</b>
4.1.1	ASCII Version .....	20
4.2	Setup Tool .....	21
4.2.1	Menu Navigation .....	22
4.2.2	Menu Commands .....	24
4.2.3	Search Lists .....	25
4.2.4	Change Password .....	26
4.2.5	Menu Architecture .....	27
4.2.6	The Setup Tool IPsec Wizard .....	31
4.3	SNMP Shell .....	32
4.4	SNMP Manager .....	32



# 1 About this Manual

This chapter explains the structure of this manual and the content of the individual chapters and the use of symbols and typographical elements.

## 1.1 Contents

This manual is divided into a "Basics" and a "Reference" section (a "Workshop" section containing application specific configuration instructions will be added as soon as possible). These are complemented by a glossary as well as an overall index of all chapters.

The "Basics" section contains the following chapters:

Chapter	Contents
<b>Quick Install Guide</b>	Instructions on installing and taking your gateway into operation, and how to create in a few minutes a basic configuration using the <b>HTML Wizard</b> .
<b>Technical Data</b>	The technical data for the devices of the <b>VPN Access</b> series.
<b>Access and Configuration</b>	Description of all access and configuration options. Basics for working with the Setup Tool.

Table 1-1: List of Chapters in the "Basics" section

The "Reference" section is an evolving collection of documents on advanced gateway configuration. It grows as the number of available functions grows. As of now, it contains the following chapters:

Chapter	Contents
<b>Licenses</b>	Information on license dependent functions and license mechanisms.

Chapter	Contents
<b>System</b>	Information on basic gateway parameters like syslog and password settings.
<b>Ethernet</b>	Information on all parameters available for the configuration of Ethernet interfaces.
<b>ISDN</b>	Information on all parameters available for the configuration of ISDN interfaces.
<b>AUX</b>	Information on all parameters available for the configuration of the auxiliary serial interface which can be used for backing up your gateway with an analog modem.
<b>WAN Partner</b>	Information on the configuration of WAN Partners.
<b>Security</b>	Information on the configuration of security features like the Stateful Inspection Firewall and IP Access Lists.
<b>IPSec</b>	Information on the configuration of encrypted data exchange using IPSec.

Table 1-2: List of Chapters in the "Reference" section

The **Glossary** contains a reference of the most commonly used technical terms of networking, the **Index** is an assembled version of the individual indices found throughout the reference section. It will help you finding relevant information on all topics by using the Acrobat Reader search function.

## 1.2 Use of Typographical Elements

To help you locate and interpret information easily, this manual uses the following visual aids:






Symbol	Meaning
	Indicates text where troubleshooting notes are given.
 <b>Note</b>	Indicates general important notes.
 <b>Attention!</b>  <b>Warning!</b>	Indicates warnings. Levels: Attention (indicates possible danger that, if unheeded, could cause material damage) Warning (indicates possible danger that, if unheeded, could cause bodily harm or death)

Table 1-3: List of symbols

The following typographical elements are used to help you find and interpret the information in this manual:

Typographical element	Meaning
 — —	Lists up to level 2.
<b>MENU → SUBMENU</b>	Indicates menus or submenus in the Setup Tool.
<b>File → Open</b>	Indicates menus or submenus in the Windows interface.

Typographical element	Meaning
non-proportional (Courier), e.g. ping 192.168.1.254	Indicates commands (e.g. in the SNMP shell), that you must enter as displayed. Display in the Setup Tool.
<b>bold, e.g.</b> <b>&gt;&gt; MIB</b>	Indicates terms you can find in the glossary (Online the link to the glossary is opened by a click).
bold, e.g. <b>Windows start menu</b>	Indicates keys, key combinations and Windows terms.
bold and cursive, e.g. <b><i>BIBOADMLOGINTABLE</i></b>	Indicates fields in the Setup Tool and MIB tables/variables.
cursive, e.g. <i>none</i>	Indicates values you can enter in the Setup Tool or for MIB variables resp. which can be adjusted.
Online: <a href="#">blue</a>	Indicates hyperlinks.

Table 1-4: Typographical elements



## 2 Access Options

**In the following chapter you will find a description of the different access options. Please select the option that fits best to your convenience.**

For the configuration of your gateway you have the following access options:

- via the serial interface ([page 7](#))
- via your >> LAN ([page 9](#))
- via your >> ISDN-connection ([page 12](#))

### 2.1 Access via Serial Interface

**Each Bintec gateway is equipped with a serial interface at which you can setup a direct connection to a PC. The following chapter describes what to observe when setting up a serial connection and how to configure the gateway.**

#### 2.1.1 Access via Serial Connection

**Access via serial interface is recommended if you like to create the initial gateway configuration and if a LAN connection is not possible via the pre-configured IP address (192.168.0.254/255.255.255.0).**

**Windows** Please follow the instructions in the **Quick Install Guide** to connect your gateway to your PC via serial interface. The printed version of the Quick Install Guide is included in the gateway delivery size. Additionally, you can find the electronic version on the Companion CD.

If you use a Windows-PC for setting up the serial connection a terminal program is required, e.g. HyperTerminal. Please check whether HyperTerminal was installed during the Windows installation. You can also use any other terminal program that can be adjusted to the respective parameters (see below).

**ToDo** If you have installed **BRICKware** as described in the **Quick Install Guide**, two links are provided. If you use these for the serial connection of your gateway, you do not need to specify any settings.

Please take the following steps to access your gateway via serial interface:

1. Click **Programs** → **BRICKware** → **Device at COM1** (resp. **Device at COM2** if you use the COM2 interface at your PC) in the Windows start menu to start HyperTerminal.
2. Press **Return** (possibly several times) when the HyperTerminal screen has opened.

The login prompt window is displayed. You are on the SNMP shell of your gateway. Now you can log in to your gateway and start the configuration.

**Check** If the login prompt is not displayed even after repeatedly pressing **Return**, the connection of your gateway failed.

Therefore check the settings of COM1 resp. COM2 at your PC:

1. Click **File** → **Properties**.
2. In **Connect To** click **Configure...**  
The following settings are required:
  - Bits per second: *9600*
  - Data bits: *8*
  - Parity: *None*
  - Stopbits: *1*
  - Flow Control: *None*
3. Insert values and click **OK**.
4. In **Settings** select:
  - Emulation: *VT100*
5. Click **OK**.

To enable the modifications of the terminal program settings please disconnect and reconnect your gateway.

If you use Windows HyperTerminal, umlauts and special characters may be displayed incorrectly. If necessary set HyperTerminal to *Auto detect* instead of *VT 100*.

**Unix** A terminal program such as `cu` (for System V), `tip` (for BSD) or `minicom` (for Linux) is required. The settings for these tools are as described above.

Example for a command line to use `cu`: `cu -s 9600 -c/dev/ttyS1`

Example for a command line to use `tip`: `tip -9600 /dev/ttyS1`

## 2.2 Access via LAN

**Accessing your gateway via one of the Ethernet interfaces provides the possibility to configure the gateway via HTML user interface. The HTML-Wizard is the easiest configuration option.**

### 2.2.1 Telnet

You can access the SNMP shell not only via a web browser but also via a Telnet connection so that you can adjust additional configuration settings as described in the chapter [“Configuration Options” on page 19](#).

**ToDo** You do not need any further software on your PC to set up a Telnet connection to your gateway: Telnet is a standard tool of all operating systems.

Take the following steps:

- Windows**
1. Click **Run...** in the Windows start menu.
  2. Enter `telnet <IP address of your gateway>`.
  3. Click **OK**.

The login prompt window is displayed. You have now accessed the SNMP shell of your gateway.

4. Continue with [“Login for Configuration” on page 16](#).

**Unix** Under UNIX and Linux you can set up a Telnet connection as well:

1. Enter `telnet <IP address of your gateway>` in a terminal.

The login prompt window is displayed. You have now accessed the SNMP shell of your gateway.

2. Continue with [“Login for Configuration” on page 16](#).

## 2.2.2 SSH

In addition to an unencrypted and potentially compromisable Telnet connection you can also connect to your gateway via an SSH connection. This is encrypted and allows you to securely make use of all remote maintenance options offered by Bintec products.

In order to connect to your gateway via SSH, the following requirements must be met:

- You need to have encryption keys created by your gateway and stored in the Flash ROM.
- You need a SSH client installed on your PC.

### Encryption Keys

**ToDo** First of all you must make sure that the encryption keys required for a SSH connection have been created on your gateway:

1. Login to your gateway using one of the already available connection methods (e.g. Telnet - for logging in, see [“Login” on page 15](#)).
2. At the the command prompt, type `update -i`. You now have access to the Flash management shell.
3. Call a listing of all files stored on the gateway: `ls -al`.

If you see something like this, the keys have been created and you can login to your gateway via SSH:

```
Flash-Sh > ls -al
  Flags  Version  Length          Date Name ...
Vr-xpbc-B 7.1.04 2994754 2004/09/02 14:11:48 box150_srel.ppc860
Vrw-pl--f 0.0      350 2004/09/07 10:44:14 sshd_host_rsa_key.pub
Vrw-pl--f 0.0      1011 2004/09/07 10:44:12 sshd_host_rsa_key
Vrw-pl--f 0.0.01   730 2004/09/07 10:42:17 sshd_host_dsa_key.pub
Vrw-pl--f 0.0.01   796 2004/09/07 10:42:16 sshd_host_dsa_key
Flash-Sh >
```



### Note

For each of the so called algorithms the gateway creates a key pair, i.e. two files must have been stored in the Flash for each algorithm (see screenshot above).

If there are no keys stored in the Flash, you need to create them. Proceed as follows:

1. Leave the Flash Management Shell: `exit`.
2. Open a Setup Tool session and navigate to the menu **SECURITY → SSH DAEMON → CERTIFICATION MANAGEMENT**.
3. To have the gateway create a key, simply place the cursor on the desired key and confirm with **Enter**. The gateway will create the respective key and store it in the Flash ROM.
4. Make sure, both keys, DSA and RSA, have been successfully created. To do so repeat the procedure described above.

### Login via SSH

Once you have made sure the necessary keys are available, you should make sure that an SSH client is installed on your PC. Most UNIX and Linux distributions per default install a command line client. PCs running a version of Windows, however, usually need additional software, like e.g. PuTTY.

**ToDo** To connect to your gateway, now take the following steps:

- UNIX**
1. Enter `ssh <IP address of your gateway>` in a terminal.

The login prompt window is displayed. You have now accessed the SNMP shell of your gateway.

2. Continue with [“Login for Configuration” on page 16](#).

- Windows**
1. The ways of setting up a SSH connection greatly depend on the software used. Refer to the documentation of the software you are using.

Once you have connected to your gateway, the login prompt window is displayed. You have now accessed the SNMP shell of your gateway.

2. Continue with “[Login for Configuration](#)” on page 16.



**Note**

PuTTY may need to use specific settings for successfully establishing a SSH connection with a Bintec gateway. You can find a FAQ detailing the necessary settings in the support section of [www.bintec.net](http://www.bintec.net).

## 2.3 Access via ISDN

**All gateways with ISDN interface can be addressed and configured by another gateway using an ISDN call.**

Access via **ISDN** with **ISDN login** is especially recommended if your gateway is to be operated via remote configuration and maintenance. This is possible even if your gateway configuration is still in ex works state. The gateway then is accessed by means of a Bintec gateway already configured or a PC with ISDN card in the remote LAN. The Bintec gateway in the own LAN that is to be configured is addressed by a calling number of the ISDN connection (e.g. 1234). This e.g. enables the administrator in the remote LAN to configure your gateway without being on site.



**Attention!**

**If you connect an unconfigured gateway and a telephone system (PABX) in parallel at the ISDN connector, the telephone system cannot answer incoming calls as long as no ISDN number is configured on the gateway.**

**Consider the costs of an ISDN connection! If your gateway and your PC are connected to the same LAN, the access to your gateway via LAN or via the serial interface is more economical.**

- ToDo** Your gateway in your LAN only needs to be connected to ISDN and to be switched on.

Take the following steps to address your gateway via ISDN login:

1. Connect your gateway to the ISDN connector.

2. Log in to your Bintec gateway in the remote LAN as administrator.
3. Enter `isdnlogin <ISDN call number of your gateway>` into the SNMP shell, e.g. `isdnlogin 1234`.

The login prompt window is displayed. You have now accessed the SNMP shell of your gateway.

4. Continue with [“Login for Configuration” on page 16](#) .





## 3 Login

**By means of predefined access data you can log in to your gateway and carry out different operations. The range of the operations allowed is limited according to the authorizations of the respective user.**

In each access option, first the login prompt is displayed. Without authorisation you cannot read any information on your gateway nor modify the configuration. You do not need to log in to read the basic information which is displayed on the HTTP status page. You can open it via LAN by entering the IP address of the gateway (in ex works state: *192.168.0.254*) into a web browser.

### 3.1 User Names and Passwords in Ex Works State

Following user names and passwords are preconfigured on your gateway:

User name	Password	Authorisations
admin	bintec	Read and change system variables, save configurations, use the Setup Tool.
write	public	Read and write system variables (except passwords) (changes are lost when you switch off your gateway).
read	public	Read system variables (except passwords).
http	bintec	Open HTTP status page of your gateway, read system variables (except passwords), no login.

Table 3-1: User names and passwords in ex works state

It is possible to modify and save the configuration only if you login with the user name `admin`. As well the access data (user names and passwords) can only

be modified if the user logs in as `admin`. The passwords are not displayed in plain text in the Setup Tool for safety reasons, but are visible as asterisks. The user names, however, are written in plain text.

For safety reasons with the user name `read` you can read all configuration settings except the access data. Thus it is impossible to login with `read`, then read the password of the user `admin` and afterwards login as `admin` to modify the configuration.

## 3.2 Login for Configuration

**ToDo** Setup a connection to the gateway by one of the access options described in chapter [“Access Options” on page 7](#).

How you log in to the SNMP shell:

1. Enter your user name , e.g. `admin`, and confirm with **Enter**.
2. Enter your password, e.g. `bintec`, and confirm with **Enter**.

Your gateway answers with the login prompt, e.g. `VPN 100:>` . Login has been successfully completed. You now accessed the SNMP shell.

How to login via the HTML user interface:

1. Enter your user name into the field **User name** of the login window.
2. Enter your password into the field **Password** of the login window.

The HTTP status page of the gateway opens in the browser and displays the available options.



**Attention!**

**All Bintec gateways are shipped with the same user names and passwords. As long as the password remains unchanged, they are not protected against unauthorized use. How to change the passwords is described in [“Change Password” on page 26](#).**

**Change the passwords to prevent unauthorized access to your gateway.**

**If you have forgotten your password, you must reset your gateway to the ex works state, which means your configuration will be lost.**

**Leave SNMP shell** To leave the SNMP shell after completing the configuration enter `exit` and press **Enter**.



## 4 Configuration Options

This chapter contains not only an overview of the different tools you can use for the configuration of your gateway, but also an introduction to the application of the Setup Tool.

The following configuration options are available:

- **HTML Wizard** ([page 20](#))
- Setup Tool ([page 21](#))
- SNMP shell commands ([page 32](#))
- **Configuration Manager** and other SNMP manager ([page 32](#))

The availability of the configuration options depends on the type of connection to your gateway:

Type of connection	Possible configuration options
LAN	HTML Wizard, HTML Setup Tool, ASCII Wizard, ASCII Setup Tool, Configuration Manager, Shell commands
Serial connection	ASCII Wizard, ASCII Setup, Shell commands
ISDN Login	ASCII Wizard, ASCII Setup, Shell commands

Table 4-1: Connection and configuration options

For each type of connection several configuration options are hence available.



### Note

You must login as `admin` to be able to modify the configuration! Configuration modification is impossible without knowing the respective password. This applies for all configuration options.

## 4.1 HTML Wizard

The **Quick Install Guide** contains a short description of the configuration by means of the **HTML Wizard**. It is required for the basic configuration of your gateway and suitable if you can address your gateway from your LAN at its preconfigured IP configuration. The **HTML Wizard** normally covers all standard configurations.

If you would like to adjust further settings, you can select one of the other configuration options mentioned above. You can first configure your gateway with the **HTML Wizard** and then extend or modify the initial configuration using one of the other options. The mere configuration with the **HTML Wizard**, however, normally is sufficient.

The Wizard guides you through the steps of the gateway configuration. After completion of the Wizard sequence your gateway is ready for operation. The data you need to enter during the Wizard run as well as the prerequisites for configuration are described in the **Quick Install Guide** (printed version also included in delivery size).

Open issues can be clarified by means of the comprehensive help system of the Wizard. Therefore, the Wizard is not described in this chapter in detail.

### 4.1.1 ASCII Version

**If you cannot access your gateway via your LAN or cannot start the HTML Wizard for any other reason, you can start the ASCII version of the Wizard on the SNMP shell. Thus you can use all features of the Wizard via a serial connection.**

**ToDo** You can start the ASCII version of the Wizard with all available types of connection: connection to the gateway via LAN, via serial connection or via ISDN login. Log in as `admin` and access on SNMP shell is required.

Take the following steps:

1. Log in to the gateway as `admin` (see [“Login for Configuration” on page 16](#)).
2. After the command prompt enter `wizard` and press **Enter**.

The ASCII version of the Wizard starts. In this version all configuration options of the HTML version are available. The help texts can be opened by selecting the **HELP** menu.

## 4.2 Setup Tool

**The Setup Tool is a menu-driven tool for configuration and administration of your gateway. The configuration with the Setup Tool is much easier and more transparent than the configuration with SNMP commands, whilst offering the same access option to all parameters like the SNMP commands.**

Like in the Wizard you can start two versions of the Setup Tool:

- As HTML page in each web browser currently available with activated Javascript. In the **Quick Install Guide**, you find a short description of how to start the HTML Setup Tool (printed version included in delivery size or available on the Companion CD).
- As ASCII Version. The access to this version is described as follows.

The two versions of the Setup Tool differ in presentation but include the same functionalities.

**ToDo** You can start the ASCII version of the Setup Tool with any connection to the gateway: connection via LAN, via serial interface or via ISDN login.

Take the following steps to start the Setup Tool session:

1. Log in to your gateway as `admin` (see [“Login for Configuration” on page 16](#)).
2. After the command prompt enter `setup` and press **Enter**.

The root menu of the ASCII Setup Tools is displayed.

### Setup Tool menu

Depending on the type of your **VPN Access Gateway** the root menu can differ. The Setup Tool menu is divided into three sections:

- The menu line contains a navigation help that displays the menu of the Setup Tool you are currently editing. Additionally, the system name of your

gateway is displayed which helps especially when you configure several Bintec gateways with different system names.

- The configuration window contains the lines where you actually enter or adjust the required settings. All settings are displayed as well. The field where the cursor is currently positioned is displayed inverse.
- The help line indicates the possible entries or navigation options in the respective menu.

In general, the menu looks as follows:

<b>Menu Line</b>	<pre>VPN Access Setup Tool                               BinTec Access Networks GmbH   MyGateway</pre>
<b>Configuration Window</b>	<pre>System Physical Interfaces:     Ethernet Unit 1     Ethernet Unit 2     Ethernet Unit 3     ISDN S0     AUX WAN Partner Security PPTP IPSEC IP PPP BRRP CREDITS QoS VoIP GRE Configuration Management Monitoring and Debugging Exit</pre>
<b>Help Line</b>	<pre>Press &lt;Ctrl-n&gt;, &lt;Ctrl-p&gt; to scroll through menu items, &lt;Return&gt; to enter</pre>

Figure 4-1: The Setup Tool menu

You will quickly get familiar with the easy handling of the Setup Tool. Nevertheless, you should go in for the basic options.

### 4.2.1 Menu Navigation

You can use the following keys or key combinations to navigate the various menus in the Setup Tool:

Key combination	Meaning
<b>Tabulator</b>	To move to the next item in a menu.



Key combination	Meaning
<b>Return</b>	To open a submenu or activate a menu command (e.g. <b>SAVE</b> ).
<b>up or down</b> (arrow keys)	To move forwards or backwards between menu fields (functions with VT 100 emulation when using a terminal program).
<b>left or right</b> (arrow keys)	To scroll backwards or forwards in the same field to reveal possible entries (functions with VT 100 emulation when using a terminal program).
<b>Esc Esc</b>	<b>Esc</b> twice in succession: To return to the previous menu. Cancels any changes made.
<b>Space</b>	To toggle the delete flag for list entries that are to be deleted. The tagged entry is marked with <i>D</i> . Pressing <b>Space</b> again removes the tag marking.  To select possible values of a variable (like arrow keys).
<b>Ctrl - l</b>	To reload the screen.
<b>Ctrl - n</b>	To move to the next item in a menu.
<b>Ctrl - p</b>	To move to the previous item in a menu.
<b>Ctrl - f</b>	To scroll forward a list that cannot be displayed in whole on the screen. An "=" character at the bottom right indicates the end of the list or a "v" indicates further entries.
<b>Ctrl - b</b>	To scroll back a list that cannot be displayed in whole on the screen. An "=" character at the top right indicates the beginning of the list or a "^" indicates further entries.
<b>Ctrl - c</b>	Quit the Setup Tool.

Table 4-2: Navigation in the Setup Tool

## 4.2.2 Menu Commands

When you navigate in the Setup Tool, you will notice that some menus include specific command options, e.g. **DELETE**, **SAVE**, **CANCEL**. The respective commands have the following meaning:

Menu command	Meaning
<b>ADD</b>	To add an item to a list. A submenu opens for entering the required settings.
<b>CANCEL</b>	To discard all changes made in the current menu.
<b>DELETE</b>	To delete all entries tagged with the <b>Space</b> bar for deletion from a list. These changes become effective immediately.
<b>OK</b>	To confirm the changes in the current menu. These changes become effective when <b>SAVE</b> is pressed in the next menu.
<b>SAVE</b>	All entries set in the current menu and all its submenus are saved to memory. These changes become effective immediately.
<b>EXIT</b>	To leave the current menu and return to the previous menu. Any entries made are lost.

Table 4-3: Menu commands in the Setup Tool



To save the configuration to the flash memory, you must quit the Setup Tool with **Save as boot configuration and exit**.

### 4.2.3 Search Lists

Some menus in the Setup Tool contain lists with several items, e.g. the menu **WAN PARTNER**, where all **WAN partners** are listed:

```

VPN Access 25 Setup Tool                               Bintec Access Networks GmbH
[WAN]: WAN Partners                                   MyGateway

Current WAN Partner Configuration

Partnername      Protocol      State
BigBoss          ppp          dormant
ISP              ppp          dormant
Partner1         ppp          dormant
Partner2         ppp          dormant
Provider         ppp          dormant

ADD              DELETE        EXIT

Press <Ctrl-n>, <Ctrl-p> to scroll, <Space> tag/untag DELETE, <Return>
to edit
Search: p

```

The entries are listed in alphabetical order of the content of the first field. The search for list entries is incremental. This is most helpful with very long lists.

**ToDo** Take the following steps:

1. Enter the initial character of the entry you are looking for with the cursor located on one of the list items. Entries can be made in upper or lower case.
2. To refine the search enter further characters.
3. Edit the search parameters with **Backspace** or **Delete**.

The Cursor automatically moves to the first match. The characters entered for the search are displayed in the help line at the bottom of the menu.

Do not enter invisible characters, such as Tabulator or Space, as they stop the search and could lead to a function initiation.



**Note**

Make sure the cursor is positioned on a list item.

The search cannot be initiated if the cursor is positioned on a commando field, e.g. **ADD** or **DELETE**.

In the menu **WAN PARTNER** described above the entries provide the following search results:

Entry	Cursor moves to entry
p or P	Partner1
pr, Pr, pR, PR	Provider
partner2	<b>Partner1</b> , after entering 2 to <b>Partner2</b>

Table 4-4: Search results

## 4.2.4 Change Password

The procedure described below for changing the password applies to all passwords for your gateway: the access passwords for the user names `admin`, `read` and `write`, the HTTP server password, the PPP password, the provider password, and the Activity Monitor password.

Any character may be used for entering a password. Passwords are only displayed as asterisks, even during password changes. The number of asterisks is the same as the number of characters in the password.



### Note

To start the Setup Tool of your gateway in a mode in which the passwords are displayed in plain text and can be changed once by editing, you must enter the command `setup -p`. This option is only available if you have logged in to your gateway with the user name `admin`.

In the password field the Backspace key always deletes the complete entry, not just one character.

### Change password

Take the following steps:

1. Select the password field in the desired menu and enter the new password.
2. The field changes to change mode and the message `Change Password` is displayed in the help line.

3. Now press **Return**, **Tabulator** or a **Cursor key**.  
The field changes to confirm mode and `Confirm Password` is displayed in the help line.
4. Now enter the new password again and confirm by pressing **Return**, **Tabulator** or a **Cursor key**.  
If you have entered the repeat password correctly, the password is changed. The new password is saved on leaving the menu with the **SAVE** button. If you leave the menu by pressing **CANCEL** or **Esc Esc**, the password change is not saved.  
If the two entries did not match, the field is reset to the old password and the help line shows the following message: "Password doesn't match. Try again." in the display.

## 4.2.5 Menu Architecture

The root menu of the Setup Tool looks as follows:

```

VPN Access 25 Setup Tool                               Bintec Access Networks GmbH
                                                       MyGateway
-----
Licenses                System
Physical Interfaces:
    Ethernet Unit 1
    Ethernet Unit 2
    Ethernet Unit 3
    ISDN S0
    AUX
WAN Partner Security PPTP IPSEC
IP PPP BRRP CREDITS QoS VoIP GRE
Configuration Management
Monitoring and Debugging
Exit
-----
Press <Ctrl-n>, <Ctrl-p> to scroll through menu items, <Return> to
enter

```

The menu architecture (root menu and first submenu) of the Setup Tool has the following structure:

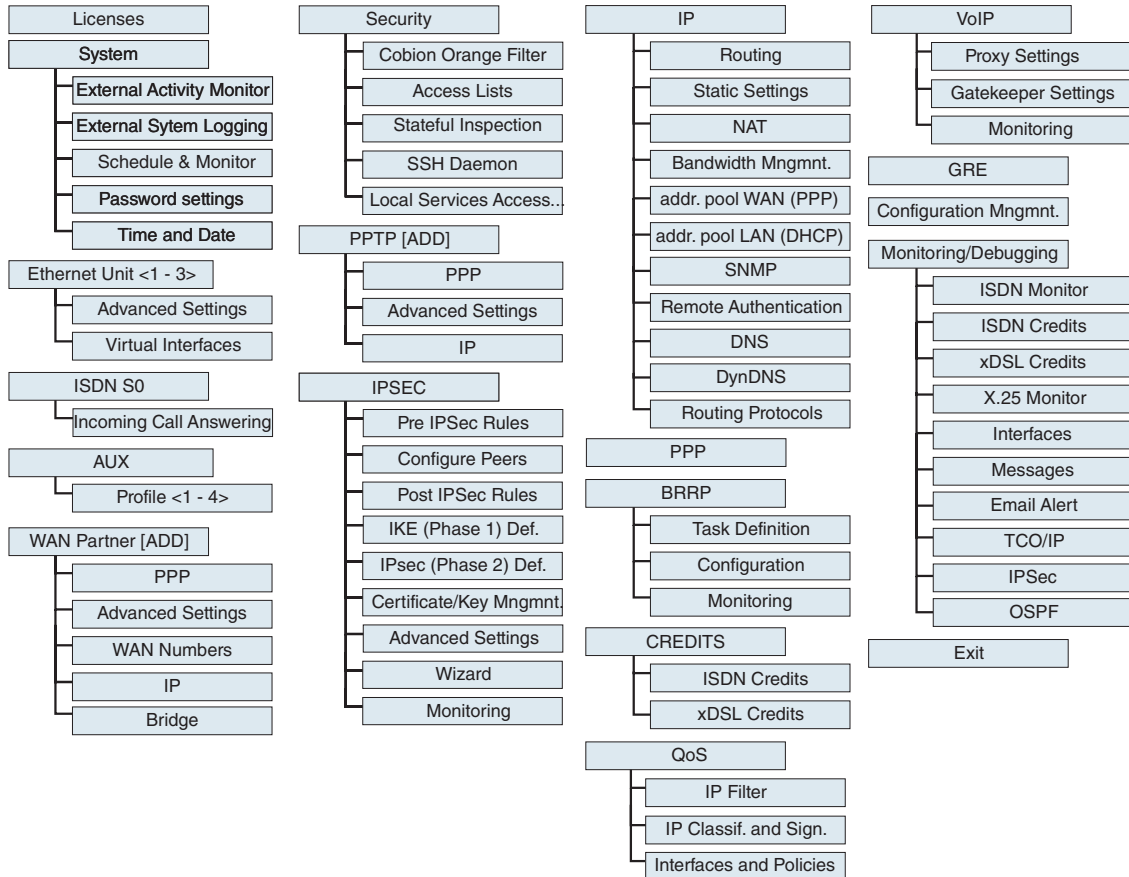


Figure 4-2: Setup-Tool menu architecture

### Convention

The following convention is used in this manual:

■ Example: "Go to **IP** → **ROUTING**"

Explanation: Tag the **IP** menu in the main menu of the Setup Tool and press **Return**. Tag the **ROUTING** submenu there and press **Return**.

- Example: "Go to **WAN PARTNER** → **ADD** → **WAN NUMBERS** → **ADD** → **ADVANCED SETTINGS**"

Explanation: Tag the **WAN PARTNER** menu in the main menu of the Setup Tool and press **Return**. Tag the **ADD** button there and press **Return**. Tag the **WAN NUMBERS** submenu and press **Return**. Tag the **ADD** button there and press **Return**. Now tag the **ADVANCED SETTINGS** submenu and press **Return**.

- Example: "Go to **WAN PARTNER** → **EDIT** → **WAN NUMBERS**"

Explanation: Tag the **WAN PARTNER** menu in the main menu of the Setup Tool and press **Return**. Select an existing entry there and press **Return**. Now tag the **WAN NUMBERS** submenu and press **Return**.

### Summary

For easier orientation during configuration the menus are briefly described as follows:

Menu	Function
<b>LICENSES</b>	In this menu you manage any licenses that may be necessary for using certain functions.
<b>SYSTEM</b>	In this menu you enter the basic system settings of your gateway, as e.g. system name and passwords.
<b>ETHERNET UNIT &lt;1 TO 3&gt;</b>	In this menu you configure the >> <b>Ethernet</b> interfaces of your gateway. Here you enter data such as IP address and net mask of the device. According to your requirements you can assign the interfaces as LAN or WAN interfaces, or even as >> <b>DMZ</b> .

Menu	Function
<b>ISDN S0</b>	In this menu you configure the ISDN interface of your gateway. Here you enter e.g. which type of ISDN connection your gateway is connected to. Submenu <b>ISDN S0 → INCOMING CALL ANSWERING</b> assigns the available ISDN call numbers to the required services (e.g. PPP-Routing, >> <b>ISDN-Login</b> ).
<b>AUX</b>	In this menu you configure the connection to an analog or GSM modem.
<b>WAN PARTNER</b>	In this menu you define all WAN partners, e.g. your Internet-Service-Provider (>> <b>ISP</b> ). All entered WAN partners are listed with partner name, protocol used and current status.
<b>SECURITY</b>	In this menu you configure the security functions of your gateway, e.g. >> <b>Stateful Inspection Firewall</b> and Content Filtering.
<b>PPTP</b>	In this menu you configure >> <b>VPN</b> connections via PPTP for the secured data transfer via Internet.
<b>IPSEC</b>	In this menu you configure >> <b>VPN</b> connections via IPsec.
<b>IP</b>	In this menu you enter all settings concerning the >> <b>IP</b> protocol.
<b>PPP</b>	Contains general >> <b>PPP</b> settings, e.g. "Authentication Protocol", which do not only apply for individual WAN partners. The gateway uses these settings to perform the authentication negotiation for incoming calls, if the calling party number cannot be identified (e.g. because the call is made from an analog line that does not transfer the calling party number).



Menu	Function
<b>BRRP</b>	In this menu you can configure a redundant network environment.
<b>CREDITS</b>	In this menu you administrate your gateway's Credits Based Accounting System.
<b>QoS</b>	In this menu you configure all settings for Quality of Service.
<b>VoIP</b>	In this menu you configure Bintec Voice-over-IP features.
<b>GRE</b>	In this menu you configure connections via GRE (Generic Routing Encapsulation).
<b>CONFIGURATION MANAGEMENT</b>	In this menu you can administrate your gateway's configuration files. You can save them e.g. either locally on your gateway or on your PC.
<b>MONITORING AND DEBUGGING</b>	Includes submenus that enable you to locate problems in your network and monitor activities, e.g. at your gateway's WAN interface.
<b>EXIT</b>	Quit the Setup Tool with <b>EXIT</b> . You save the configuration file in the flash memory with <b>EXIT → Save as boot configuration and exit</b> . This file is loaded on restarting your gateway. Leave the Setup Tool without saving the configuration in the flash memory with <b>EXIT → Exit without saving</b> .

Table 4-5: Setup Tool Menus

## 4.2.6 The Setup Tool IPSec Wizard

The configuration of an IPSec-VPN requires comprehensive knowledge of cryptography as well as of basic network technology. Thus the Setup Tool contains an additional Wizard that guides you through the IPSec basic configuration without starting the HTML or the ASCII Wizard.

The IPsec Wizard is initiated once you select the **IPSEC** menu without all the parameters set for an IPsec connection. If you do not configure an IPsec-VPN by means of the HTML-Wizard, you should apply the IPsec Wizard: some required settings are fixed in its non-interactive part and are not executable in a manual configuration.

In general you could abort the IPsec Wizard after the automatic sequence and complete the configuration manually. This procedure, however, is not recommended: The IPsec Wizard ensures that the IPsec configuration on your gateway is correct and executable.



Attention!

**An incomplete configuration can result in the abort of all LAN connections. In this case you can only access the gateway via serial interface or ISDN login.**

## 4.3 SNMP Shell

➤➤ **SNMP** (Simple Network Management) is a ➤➤ **protocol**, that defines how to access the configuration settings.

All configuration settings are stored in the so-called ➤➤ **MIB** (Management Information Base) as MIB tables and MIB variables. You can access these settings by means of SNMP commands directly from the SNMP shell. For this configuration method advanced knowledge of Bintec gateways is required.

## 4.4 SNMP Manager

The **Configuration Manager** is an SNMP manager based upon Windows platforms. The user interface resembles the Windows-Explorer and enables the access to all MIB tables and variables of your gateway.

You can access and modify the MIB tables and variables with other SNMP managers as well, e.g. SNM, HP OpenView or Transview. The configuration using SNMP shell commands or SNMP managers, however, requires extensive

knowledge of the structure and relations of the tables and subsystems of your gateway. Thus this method is only recommended for expert users. This User Manual does not describe how to handle MIB tables and MIB variables. For detailed information about MIB tables see the MIB reference on the download site at [www.bintec.net](http://www.bintec.net).

