QUICK INSTALL GUIDE

1 Introduction

Your VPN Access Gateway is extensively equipped for encrypted data transfer and Internet access for both single users and companies.

Essential system requirements:

■ Windows 95, Windows 98, Windows ME, Windows NT 4.0, Windows 2000 or Windows XP
(The instructions on testing/installing the TCP/IP protocol and configuring the PC apply to Windows 2000 or Windows XP. For Windows 95, Windows 98, Windows ME or Windows NT 4.0, please see the instructions in the User's Guide **Basic Configuration Compact Routers**, which you will find on your Bintec **Companion CD** or can download from www.bintec.de.)

■ Network card installed (Ethernet)

■ CD-ROM drive

■ Microsoft TCP/IP protocol installed (see "Checking the TCP/IP protocol" on page 13)

■ High color display (more than 256 colors) for correct display of graphics

Companion CD The **Companion CD** enclosed in the delivery size contains all tools necessary for the configuration and management of your gateway.

This Quick Install Guide shows you how to set up a basic configuration for your **VPN Access** Gateway step by step using the **HTML Wizard**. (**VPN Access 250** and **VPN Access 1000** cannot be configured by means of the **HTML Wizard**. Use the HTML Setup Tool or the ASCII Setup Tool. See "Further gateway access options" on page 18.) Detailed knowledge of networking is not necessary. A detailed online help system gives you extra support.

The **BRICKware** includes helpful applications for the management of your gateway.

Congratulations on your new purchase and have fun!

1 Introduction

2 Taking into Operation

The basic requirements for taking your VPN Access Gateway into operation are described below.

You can integrate your gateway into a local area network (LAN):
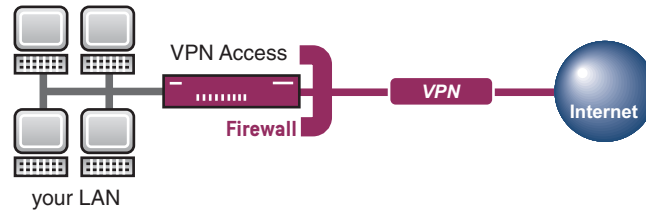
Figure 2-1: Basic scenario

Note Please read the safety precautions carefully before installing and taking your **VPN Access** Gateway into operation. These are supplied together with the gateway. The current version is also available at www.bintec.de.

2.1 Connections

All connections on VPN Access 5, VPN Access 25 and VPN Access 100 are located at the rear of the unit. With the exception of the power supply, the connections on VPN Access 250 and VPN Access 1000 are at the front.

VPN Access 5
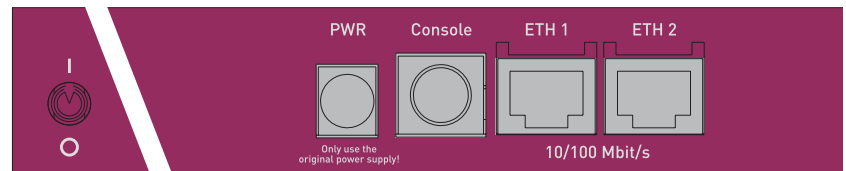
Figure 2-2: Rear of **VPN Access 5**

VPN Access 25
VPN Access 100
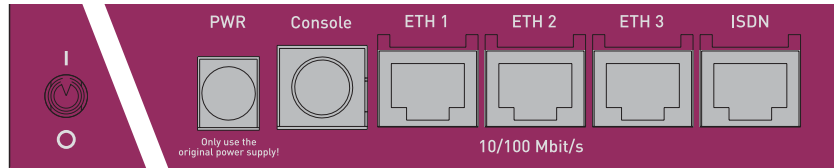
Figure 2-3: Rear of **VPN Access 25** and **VPN Access 100**

VPN Access 250
VPN Access 1000
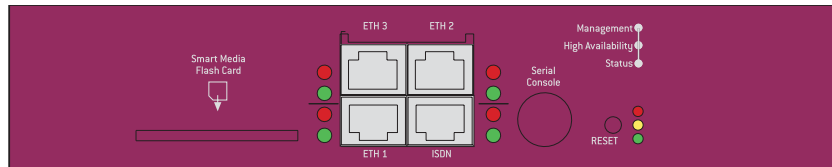
Figure 2-4: Front of **VPN Access 250** and **VPN Access 1000**

2.2   Setting Up and Connecting

After you have carried out the following steps, the gateway is ready for configuration with the HTML Wizard.

All you need for this is the cables supplied with the equipment (only **VPN Access 100**, **VPN Access 250** and **VPN Access 1000** are not supplied with an Ethernet cable). If you wish to set up a WAN connection immediately, you need a second Ethernet cable, if the connection is not to be set up over ISDN. This second cable is not supplied with the equipment.

⚠
Attention!

The use of the wrong mains adaptor may damage your gateway! Use only the mains adaptor supplied with the equipment!

Incorrect cabling of the ISDN and LAN interfaces may also damage your gateway! Make sure you connect the LAN interface of the gateway to the LAN interface of the PC/hub and the ISDN interface of the gateway to the ISDN connection.

Set up and connect the gateway in the following order:

1.   Place your **VPN Access** Gateway on a firm, level base or mount it in a 19-inch cabinet.

2. Serial connection: Connect the serial port of your PC (COM1 or COM2) to the serial port of your gateway. Use only the serial cable (gray) supplied with the equipment. This can be left out if you do not need a serial connection to the gateway.

3. LAN: Connect the preconfigured Ethernet interface (ETH1) of your gateway to your LAN using the Ethernet cable supplied. The device detects automatically whether it is connected to a switch or directly to a PC.
   (**VPN Access 250** and **1000** do not automatically detect the connection type. Connecting to a PC requires a crossover cable.)

4. WAN: If applicable, connect another Ethernet interface (ETH2 or ETH3) of your gateway to your WAN connection via another Ethernet cable.

5. ISDN: Connect the ISDN interface of the gateway to your ISDN socket using the black ISDN cable supplied.
   (**VPN Access 5** is not equipped with an ISDN interface.)

6. Optional LAN/WAN: Connect the remaining Ethernet interface (ETH2 or ETH3) of your gateway to any other desired LAN or WAN interface using another Ethernet cable.

7. Mains supply: Connect your gateway to a mains socket using the mains adaptor or IEC AC power cord supplied (**VPN Access 250** and **VPN Access 1000**).

8. Switch the gateway on with the on/off switch.

The gateway is now prepared for configuration using the **HTML Wizard**.

2 | Taking into Operation

3   Configuration

The initial configuration of your gateway and the preparations are de-scribed below. On completion of configuration work your gateway is ready for operation in accordance with the configuration elements you have selected.

As preliminary preparation for the configuration, you should collect certain data and check whether the PC from which you wish to make the configuration meets the necessary requirements. You can also install **BRICKware**, which provides additional tools for working with your gateway. This installation is optional and not essential for the configuration or operation of the gateway.

Once you have made all the preparations you can configure your gateway. You may then need to adjust a few settings on your PC, after which you can finally check the configuration and operability of your gateway.

Preconfigured values of your gateway   Your **VPN Access** gateway is shipped with a predefined IP configuration:

■   *IP ADDRESS*: *192.168.0.254*

■   *NETMASK*: *255.255.255.0*.

In ex works state use the following user name and password to access your gateway for configuration:

■   *USER NAME*: *admin*

■   *PASSWORD*: *bintec*.

⚠ **Attention!**

All Bintec gateways are shipped with the same user names and pass-words. As long as the password remains unchanged, they are not protect-ed against unauthorized use.

Change the passwords to prevent unauthorized access to your gateway! (See Bintec User's Guide chapter Access and Configuration.)

Software update   Your gateway is equipped with the latest system software version available for manufacturing. Newer versions of the software may be available in the mean-time. How to check the current software version of your gateway and, if appli-

cable, carry out a software update is described in the **Bintec User's Guide** chapter **Gateway Management** (in the Basics section).

3.1 In Advance of Configuration

Only a few steps are necessary to prepare the configuration of your gateway: gather some information for the basic configuration (optional for Internet access and corporate network connection), configure the PC which is used to carry out the gateway configuration, and install the BRICKware.

3.1.1 Gathering Information

The essential information for basic configuration with the HTML Wizard is soon gathered, as no information is required that needs in-depth network knowledge. If applicable, you can use the example values.

Before you start the configuration, you should gather the data for the following purposes:

■ Basic configuration
  (obligatory if your gateway is in the ex works state)

■ Internet access
  (optional)

■ Connecting to a corporate network
  (optional).

The following table shows examples of possible values for the necessary access data. You can fill in the table with your personal data under the heading "Your value", so that you can refer to these values later when needed.

If you configure a new network, you can use the given example values for IP addresses and netmask. If in doubt, ask your system administrator.

Basic configuration　For the basic configuration of your gateway, you need information about your ISDN connection and network environment:

Access data	Example	Your value
ISDN extensions You received the ISDN extensions with your ISDN connection.	*967310* *967311* *967312*	
IP address of your gateway	*192.168.0.254*	
Netmask of your gateway	*255.255.255.0*	

Table 3-1:　Basic information

> **Note**　If you do not want to configure your gateway for ISDN access to the Internet or another ISDN service, you do not need the ISDN-specific information.
>
> The **HTML Wizard** assumes the settings for the connection of your gateway to the NTBA adaptor. If you are connecting to a PABX, note the special characteristics of your connection and refer to your PABX documentation if necessary.

Internet access　If you want to configure an Internet access, you will need an Internet Service Provider (ISP). You receive your personal access data from your ISP. The terms used for the required access data may vary from provider to provider, but the type of information you need for dialing in is basically the same.

The following table lists the access data that your gateway needs for a connection to the Internet.

Access data	Example	Your value
Provider name	*GoInternet*	
Access number, if applicable The ISDN extension you use to dial in to your ISP. Not necessary for a DSL connection.	*1234567*	
Your user name	*MyName*	
Password	*TopSecret*	

Table 3-2:　Data for Internet access

Some Internet Service Providers such as T-Online require additional information:

Access data	Example	Your value
T-Online number	*081512345678*	
Joint user account (other user code)	*0001*	

Table 3-3: Additional information for T-Online

Corporate network connection

To connect to a WAN partner (e.g. head office), you will need some information about the remote terminal that is to take your call. The remote terminal must also know your details. These data must be agreed between both ends of the connection.

Your gateway and the gateway at your head office check the incoming data before every connection to see if they should take the call from the partner. To protect the network against unauthorized access, the call is accepted only after correct authentication. This authentication is based on a common password and two codes that you and your partner use for the connection.

Access data	Example	Your value
Partner's name Code of head office	*BigBoss*	
Access number Number of head office gateway	*0911987654321*	
Local name Your own code. Your partner (at head office) must enter this name as partner name on his gateway.	*LittleIndian*	
Password Common password for this connection (enter on both gateways)	*Secret*	
Network address(es) of your head office	*10.1.1.0*	

Access data	Example	Your value
Netmask(s) of your head office	*255.255.255.0*	

Table 3-4:   Data for connection to a corporate network

3.1.2   Configure the PC

A number of conditions must be fulfilled at the PC with which you carry out the configuration, before you can reach your gateway over the network and configure it using the HTML Wizard.

Make sure the TCP/IP protocol is installed before you start the configuration.

Then you must assign a fix IP address to the PC to be able to set up a connection to the gateway.

Checking the TCP/IP protocol

Proceed as follows to check whether you have installed the protocol:

1. Click **Settings ➜ Network and Dial-up Connections** resp. **Control Panel ➜ Network Connections** in the Start menu.
2. Double click **LAN Connection**.
3. Click **Properties** in the status window.
4. Look for **Internet Protocol (TCP/IP)** in the list of network components.

Installing the TCP/IP protocol

If you cannot find the entry **TCP/IP**, install the TCP/IP protocol as follows:

1. First click **Properties**, then **Install** in the status window of the **LAN Connection**.
2. Select the **Protocol** entry.
3. Click **Add**.
4. Select **Internet Protocol (TCP/IP)** and click **OK**.
5. Follow the instructions on the screen and finally restart your PC.

Assign PC an IP address

Assign your PC an IP address as follows:

1. Select **Internet Protocol (TCP/IP)** and click **Properties**.
2. Select **Use the following IP address** and enter an IP address.

Your PC should now fulfill all the conditions for the configuration of your gateway using the **HTML Wizard**.

Enter gateway IP address at PC

Continue by entering the IP address of your gateway into the PC configuration as follows:

3. Enter the IP address of your gateway into **Default gateway** in **Internet Protocol (TCP/IP)** ➔ **Properties**.

   If you do not use the preconfigured IP address of the gateway nor have yet defined one according to your network requirements, carry out the first steps of the gateway configuration. You can perform an automatic determination of a free IP address within your network. Enter the resulting IP address here ().

4. Enter the IP address of your gateway into **Use the following DNS server addresses**.

5. Click **OK**.

6. Close the dialog box with **OK**.

The PC now has an IP configuration and can access the Internet via the gateway.

3.1.3 Installing BRICKware

BRICKware contains a number of programs to help you when working with your gateway. The installation is optional.

You only need the **Companion CD** supplied with your gateway for the installation. Your PC should also fulfill the conditions stated in see .

Tool	Description
Activity Monitor	**Activity Monitor** provides a permanent overview of the interface status and the data traffic. The administrator has the password-protected option to selectively control individual interfaces and connections by a set of commands that allow him to, e.g., set up and clear connections or change a pre-configured Internet provider.
SNMP Manager	The **SNMP Manager**, provides simple access to all SNMP tables and SNMP system variables via a graphical user interface. The desired configuration part can be selected from a tree structure and then configured in the usual Windows-style dialog boxes.
CAPI	The Bintec remote access drivers - RMCC and Remote CAPI - equip the PC with standard software interfaces such as CAPI 2.0 for communication applications. They are configured via the setup utility **CAPI configuration**. On Windows NT 4.0 and newer systems, the Remote Multi-CAPI Client provides a CAPI 2.0 interface for several gateways simultaneously.
Dime Tools	The **Dime Tools** are a set of tools for configuration, maintenance and diagnosis. They comprise a BootP server, a TFTP server, a Syslog Daemon, a Time Server and the DIME Tracer for ISDN and CAPI.

Table 3-5:   **BRICKware** tools

Proceed as follows to install the software:

1.   Close all Windows programs on your PC.

2. Place your Bintec **Companion CD** in the CD-ROM drive of your PC. The Start window appears automatically after a short time. If the Start window does not open automatically, click your CD-ROM drive in Windows Explorer and double-click **setup.exe**. (For Unix systems: Open the file **index.htm** in your standard browser.)

3. Click **BRICKware** in the Add ons section. A new window opens. Here you can start the configuration or display descriptions of the individual **BRICKware** tools. Click the respective button to start the setup.

4. Specify the directory in which **BRICKware** should be installed.

5. Select your gateway, i.e. **VPN Access 5**, **VPN Access 25**, etc.

6. Select the software components you wish to install.

The installed programs are available for use immediately after the installation of **BRICKware**. It is not usually necessary to restart the PC.

3.2 Configuring the Gateway

Your gateway can be configured quickly and easily with the HTML Wizard.

Note If you have already created a configuration with the Wizard, the Wizard can use the preset values. You are informed about this possibility during configuration.

The configuration of your gateway is started as follows:

1. Select **Installation** on the Bintec **Companion CD** and click the button **Configure Gateway**.

2. Note the information on how to determine a free IP address for your gateway in the network. Click **Assign automatically...** or enter your defined IP address and netmask.

3. Start the configuration with **Finish**.

You can carry out the configuration in either Quick Mode or Advanced Mode. If you are unfamiliar with networking technologies, choose Quick Mode. Your gateway is ready for operation when you have completed the configuration.

You can select from the following configuration items:

■ basic configuration

■ Internet access

■ corporate network connection (LAN-LAN connection).

The basic configuration is essential if your gateway is still in the ex works state, as it integrates the gateway into your local network.

Proceed as follows:

1. Select the desired items and follow the instructions on the screen.

2. To be able to use your gateway in your local network, it may be necessary to make a few more settings on the PCs connected in the network.
You can set up Internet access over your gateway for all PCs in the same network as your gateway. To do this, you should configure all PCs as DHCP clients. Otherwise you must assign a fix IP address to each PC and define your **VPN Access** Gateway as default gateway and as DNS server ().

The configuration of the gateway and its integration into your network are now completed.

Further gateway access options The predefined IP configuration (192.168.0.254/255.255.255.0) of your **VPN Access** Gateway enables simple access to further configuration options.

Enter *192.168.0.254*/*wizard* to start the HTML configuration assistant (**HTML Wizard**) with any current Web browser (java script must be activated).

The **HTML Setup Tool** can also be opened with any current Web browser (java script must be activated). Enter *192.168.0.254*/*setup* to start a Setup Tool session.

You can also start both configuration tools from the HTML status page of the gateway. To access the status page, just enter *192.168.0.254* in your Web browser.

Other means of access and configuration information are described in the chapter **Access and Configuration** of the **Bintec User's Guide** (as a part of the Basics section).

3.3 Testing the Configuration

You have completed the configuration of your gateway and can now test the connection in your LAN and to the Internet.

Carry out the following steps to test your gateway:

1. Remove the serial cable from your gateway if you no longer need the serial connection.

2. Test the connection to your gateway. Click **Run** in the Start menu and enter `ping`, followed by a space and the IP address of your gateway (192.168.0.254). A window appears with the response **"Reply from..."**.

3. Test the Internet access by entering **www.bintec.de** in the Internet browser. The Bintec Internet site offers you the latest news, updates and documentation.

Attention!

Incorrect configuration of the devices in your LAN may result in unwanted connections and increased charges! Monitor your gateway and make sure it does not set up unwanted connections (and charges). Watch the LEDs on your gateway (LED ISDN-D, ISDN-B and the Ethernet interface to which you have connected your WAN; see manual for meaning of LEDs) or use the Activity Monitor (see BRICKware for Windows).

3 Configuration

4   Support Information

Contact numbers and addresses of the Bintec Support Center of Funk-werk Enterprise Communications GmbH:

Germany
Switzerland
Austria

Available from monday till friday 9 a.m. - 5 p.m. (CET)

■   First Level Support:
   –   **Telephone: 00 800 7333 7333**
      Free of charge within 6 weeks after purchase
      (the telephone number is free of charge, only reachable from a conventional telephone network from Germany, Switzerland, Austria and France)
      Please keep the hardware serial number of your device ready for verification of support authorization!
   –   **Telephone: 0190 – 85 10 68** (EUR 1,86/min. from a conventional telephone network only in Germany)

■   Second Level Support:
      Telephone: +49 - 180 300 9191 550
      Fax: +49 - 180 300 9191 599

E-Mail: hotline@funkwerk-ec.de

For further information on the Bintec support services please see www.bintec.net.

France

Available during local normal trading hours.

■   First Level Support and Second Level Support:
      Telephone: 08.90.71.05.71 (TTC EUR 0,15/min.)

E-Mail: support.france@funkwerk-ec.com

Spain Portugal   Available during local normal trading hours.

- First Level Support:
  Telephone: + 34 - 91 658 7504
  E-Mail: support.spain@funkwerk-ec.com

- Second Level Support:
  Telephone: +49 - 911 9673 1550 or +49 - 180 300 91 91 550
  Fax: +49 - 911 9673 1599 or +49 - 180 300 9191 599
  E-Mail: support@funkwerk-ec.com

Italy   Available during local normal trading hours.

- First Level Support:
  E-Mail: support.italy@funkwerk-ec.com

- Second Level Support:
  Telephone: +49 - 911 9673 1550 oder +49 - 180 300 91 91 550
  Fax: +49 - 911 9673 1599 or +49 - 180 300 9191 599
  E-Mail: support@funkwerk-ec.com

Great Britain   Available from monday till friday 9 a.m. - 5 p.m. (CET)

- Second Level Support:
  Telephone: +49 - 911 9673 1550 or +49 - 180 300 91 91 550
  Fax: +49 - 911 9673 1599 or +49 - 180 300 9191 599
  E-Mail: support@funkwerk-ec.com