REMOTE CONFIGURATION

bintec Workshop

Version 0.9

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

Copyright

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 Introduction

The following chapters present various possible ways of remotely configuring the router. These include ISDN Login, Telnet, HTML Setup and SSH Client.

The Setup Tool is used for the configuration, parallel to the shell.

1.1 Requirements

The following requirements must be fulfilled for the configuration:

- Basic configuration of router. The basic configuration using the Wizard is recommended.
- A boot image of version 7.1.1 or later.
- Brickware with the **DIME Tools** must be installed.
- You need a software client for SSH access, e.g. SecureCRT or PuTTY.

2 Configuration

2.1 ISDN Login

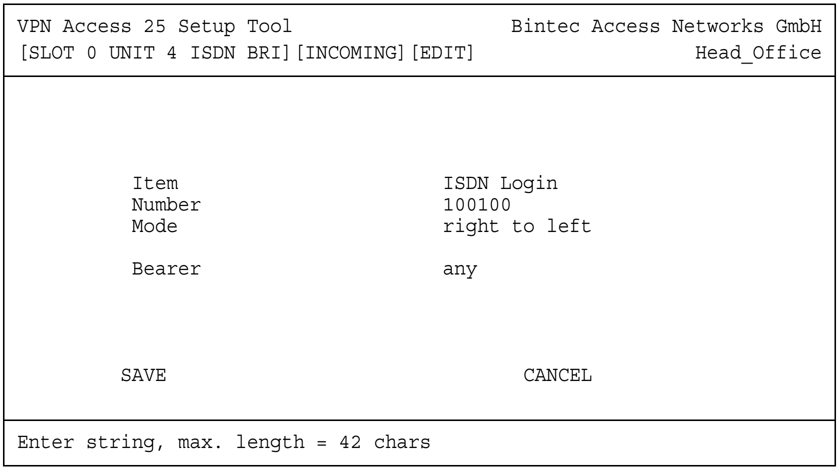
For accessing a remote router, you have the option of using the **ISDN Login** tool from a bintec router.

Just connect the bintec router to your ISDN connection. The router carries out automatic D-channel detection and then accepts every incoming call for the ISDN Login service.

If you have entered at least one service in the ***ISDN S0 ➜ INCOMING CALL ANSWERING*** menu, you must also make an entry for remote administration.

Go to the following menu to configure the entry for ISDN Login:

ISDN S0 ➜ INCOMING CALL ANSWERING ➜ ADD.



```
VPN Access 25 Setup Tool                      Bintec Access Networks GmbH
[SLOT 0 UNIT 4 ISDN BRI][INCOMING][EDIT]                      Head_Office



          Item                            ISDN Login
          Number                          100100
          Mode                            right to left

          Bearer                          any




         SAVE                                  CANCEL

Enter string, max. length = 42 chars
```

The following fields are relevant:

Field	Meaning
Item	For selecting the service that is to react to your own number.

Field	Meaning
Number	Enter your own number (MSN) in this field.

Table 2-1: Relevant fields in ***ISDN S0*** → ***INCOMING CALL ANSWERING*** → ***ADD***

Proceed as follows to configure the entry:

- Set ***ITEM*** to *ISDN Login* for remote administration.
- Enter your number under ***NUMBER***, e.g. *100100*.

Note

If you only have one number available on the connection, which you also need for telephoning, you can set the bearer to *data*.

To carry out an ISDN Login on the router from a remote router, you must enter the following:

e.g. `isdnlogin 100100`

If you do not have a bintec router available from which you can carry out an ISDN Login, you can also set up a connection using a normal ISDN card.

To do this, open your terminal program, create a new connection, enter the number of the remote terminal and just select the X.75 transparent protocol to carry out remote administration.

2.2 Telnet

You can execute the Telnet program to the router in the ex works state, as every bintec router with software 6.3.4 or later has a fixed IP address (192.168.0.254) entered in the LAN interface.

To set up a connection to the router, just open the command prompt of your PC and enter the following:

e.g. `telnet 192.168.0.254`

The login window opens for entering your authentication data.

```
Welcome to VPN Access 25 version V.7.1 Rev. 6 (Patch 7) IPSec from
2005/01/18 00:00:00
System name is Head_Office, location is European Union


Login: admin
Password: bintec


Password not changed. Call "setup" for quick configuration.

Head_Office:>
```

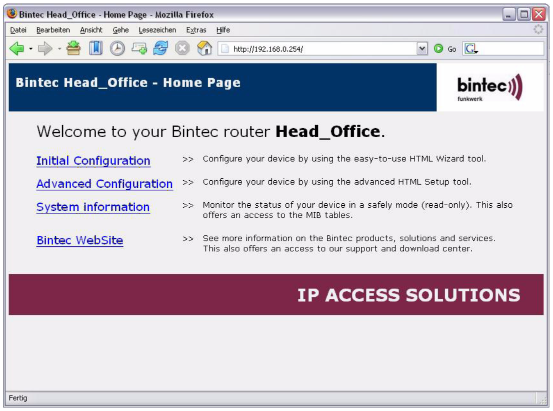
Proceed as follows to log in with the standard access code:

- Enter *admin* for ***Login***.
- Enter *bintec* under ***Password***.
- Enter *setup* to open the Setup Tool.

2.3 HTML Setup

The bintec router also offers several options for configuration via HTML. Open your Internet Explorer and enter the IP address of the router in the URL bar.

e.g. `http://192.168.0.254`


Bintec Head_Office - Home Page - Mozilla Firefox
Datei Bearbeiten Ansicht Gehe Lesezeichen Extras Hilfe
http://192.168.0.254/
Go
bintec funkwerk
Fertig

Bintec Head_Office - Home Page

Welcome to your Bintec router **Head_Office**.

Initial Configuration >> Configure your device by using the easy-to-use HTML Wizard tool.

Advanced Configuration >> Configure your device by using the advanced HTML Setup tool.

System information >> Monitor the status of your device in a safely mode (read-only). This also offers an access to the MIB tables.

Bintec WebSite >> See more information on the Bintec products, solutions and services. This also offers an access to our support and download center.

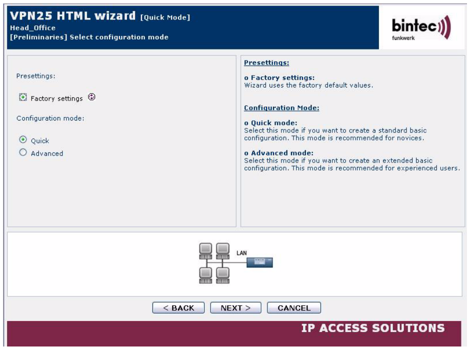
IP ACCESS SOLUTIONS

Here you have a choice of two items you can use for configuration of your router:

Field	Meaning
Initial Configuration	A Wizard helps you to create the basic configuration.
Advanced Configuration	Here you find the Setup Tool, which is also available over Telnet.

Proceed as follows to start the Wizard:

- Click ***INITIAL CONFIGURATION*** link.
- Enter the login data of your router, e.g. *admin* / *bintec*.
- Select the Wizard language, e.g. *English (Englisch)*.


VPN25 HTML wizard [Quick Mode]
Head_Office
[Preliminaries] Select configuration mode

Presettings:

☑ Factory settings

Configuration mode:

● Quick
○ Advanced

Presettings:

o Factory settings:
Wizard uses the factory default values.

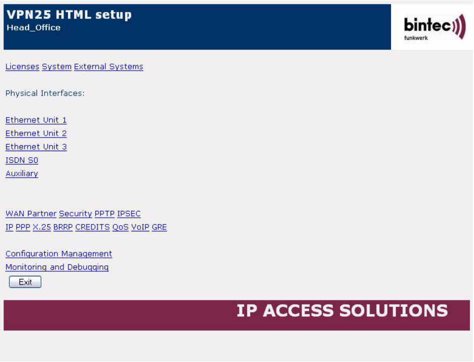
Configuration Mode:

o Quick mode:
Select this mode if you want to create a standard basic configuration. This mode is recommended for novices.

o Advanced mode:
Select this mode if you want to create an extended basic configuration. This mode is recommended for experienced users.

Proceed as follows to start the Setup Tool:

- Click the ***Advanced Configuration*** link.
- Enter the login data of your router, e.g. *admin* / *bintec*.


VPN25 HTML setup
Head_Office

Licenses System External Systems

Physical Interfaces:

Ethernet Unit 1
Ethernet Unit 2
Ethernet Unit 3
ISDN S0
Auxiliary

WAN Partner Security PPTP IPSEC
IP PPP X.25 BRRP CREDITS QoS VoIP GRE

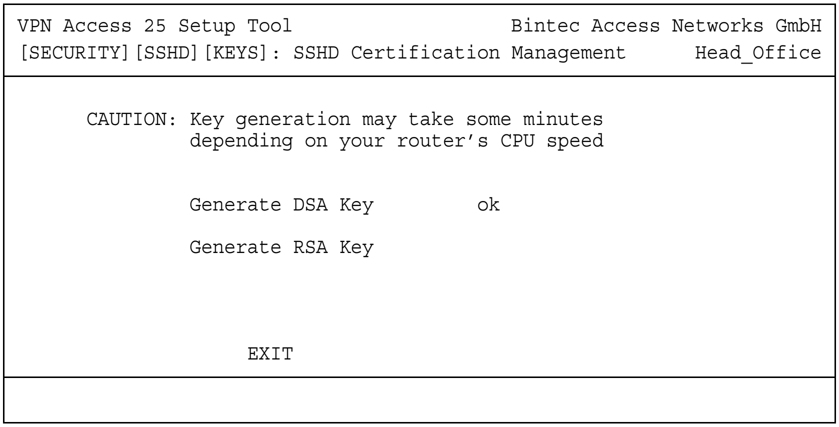
Configuration Management
Monitoring and Debugging

2.4 SSH Client

bintec routers with software 7.1.1 or later offer the possibility of setting up a secure connection for the configuration. All data, such as passwords or configuration parameters, were previously transferred in Telnet in clear text, but these are encrypted in SSH.

The SSH Deamon is not, however, available in the ex works state, as you must first create a host key. Go to the following menu for this:

SECURITY ➜ SSH DAEMON ➜ CERTIFICATION MANAGEMENT



```
VPN Access 25 Setup Tool                       Bintec Access Networks GmbH
[SECURITY][SSHD][KEYS]: SSHD Certification Management      Head_Office

      CAUTION: Key generation may take some minutes
               depending on your router's CPU speed


               Generate DSA Key         ok

               Generate RSA Key



                    EXIT
```

The following fields are relevant:

Field	Meaning
Generate DSA Key	For generating a DSA key.
Generate RSA Key	For generating an RSA key.

Table 2-2: Relevant fields in ***SECURITY ➜ SSH DAEMON ➜ CERTIFICATION MANAGEMENT***

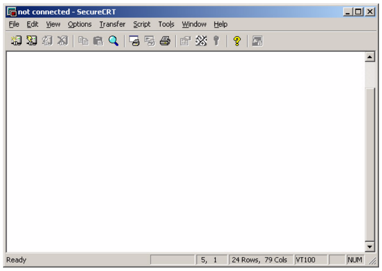
Proceed as follows to generate keys:

- Generate a DSA key by confirming the ***GENERATE DSA KEY*** field.

Note

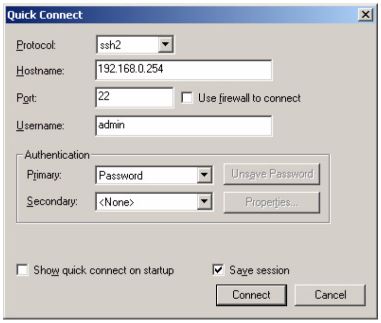
The time taken to generate a key may vary according to device and CPU power.

After installation of an SSH client, e.g. here we have used SecureCRT, you must configure the software for the connection to the router. Start the SSH client:



not connected - SecureCRT
File Edit View Options Transfer Script Tools Window Help
Ready
5, 1
24 Rows, 79 Cols
VT100
NUM

You can create a connection under ***FILE* ➜ *QUICK CONNECT***.



Protocol: ssh2

Hostname: 192.168.0.254

Port: 22 ☐ Use firewall to connect

Username: admin

Authentication

Primary: Password

Secondary: <None>

☐ Show quick connect on startup ☑ Save session

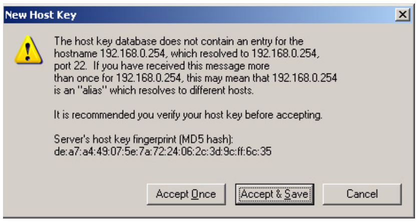
The following fields are relevant:

Field	Meaning
Protocol	Select the protocol for the connection.
Hostname	Enter the IP address of the router.
Port	The SSH service normally runs on port 22.
Username	Enter a login name.

Proceed as follows to generate keys:

- Leave ***PROTOCOL*** set to *ssh2*.
- Enter the IP address under ***HOSTNAME***, e.g. *192.168.0.254*
- The ***PORT*** remains set to *22*.
- Enter *admin* for ***USERNAME***.

You now receive the following message:



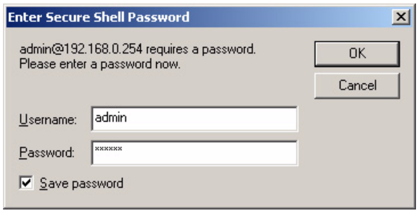
The host key database does not contain an entry for the hostname 192.168.0.254, which resolved to 192.168.0.254, port 22. If you have received this message more than once for 192.168.0.254, this may mean that 192.168.0.254 is an "alias" which resolves to different hosts.

It is recommended you verify your host key before accepting.

Server's host key fingerprint (MD5 hash):
de:a7:a4:49:07:5e:7a:72:24:06:2c:3d:9c:ff:6c:35

- Confirm the message with **Accept & Save**.

A window now appears for entering your admin password for login:



admin@192.168.0.254 requires a password.
Please enter a password now.

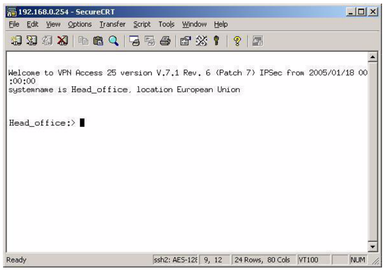
Username: admin

Password: ******

☑ Save password

- Enter a ***Password***, e.g. *bintec*.
- Click **OK**.

You have now configured and set up an encrypted connection to the router.


192.168.0.254 - SecureCRT
File Edit View Options Transfer Script Tools Window Help
Ready
ssh2: AES-128
9, 12
24 Rows, 80 Cols
VT100
NUM

```
Welcome to VPN Access 25 version V.7.1 Rev. 6 (Patch 7) IPSec from 2005/01/18 00
:00:00
systemname is Head_office, location European Union


Head_office:>
```