NetComm™

Mobile VPN Firewall

Travellers Guide

VPN100

NetComm™ Broadband Solutions

NetComm™

Contents

Introduction

The VPN100 will perform three main functions when used to connect your PC, these functions are described below:

- **Internet - Provide a Network/Internet connection**

  The VPN100 will provide a safe Network/Internet connection to:

  - An Office Ethernet LAN and the Internet
  - The Internet via an ADSL modem
  - The Internet via an Cable Internet modem

- **Firewall - Prevent Hacker attacks and Network Viruses.**

  Another use for the VPN100 is simply to protect you from viruses and trojans when sharing files with a local network which you can't trust (such as downloading a file from a customer's local server when out on-site). Of course at the same time you can use that network's Internet connection to Surf or connect to your Remote Office VPN. The Hardware Firewall will protect your PC from Hacker attacks coming from the local network or from the Internet. This protection is part of the VPN100 hardware and therefore does not slow down your PC's performance.

- **VPN - access your office network from anywhere**

  The Built-in VPN end points can be pre-configured (usually by your company's Network Administrator) to connect to your Company's IPsec VPN service via the Internet. This will allow you to access your Company's Office resources from anywhere whilst maintaining data integrity and security.

Note: *The VPN100 always connects to your computer via the USB socket and USB Cable. The Ethernet socket is intended to be connected to the Internet or an Un-trusted Network. If you connect your computer to the VPN100 via the Ethernet socket, the VPN100 will not work.*

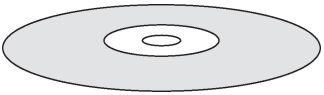
Package Contents

The following items should be contained in your NetComm Personal Firewall VPN Adaptor Package:

- NetComm Personal Firewall VPN Adaptor (VPN100)

- Package Contents Note and this Traveller's Guide

- NetComm Driver CD-ROM (including drivers and additional user guide)



- Etherent Network Cable (RJ-45)

- USB Connection Cable

Check the contents of your package and, if any parts are missing or damaged, please contact your Dealer.

VPN100 LEDs

The following figure shows the top view of the NetComm VPN100.

The LEDs on the top indicate the status of the unit.

LED	Colour	Description
Session	Orange	The Session LED indicates a successful VPN Tunnel has been established between two endpoints.
Diag	Red	The Diag LED lights up when the Adapter goes through its self-diagnosis mode during every boot-up. It will turn off upon successful completion of the diagnosis.
Link/Act	Green	The Link/Act LED serves two purposes. If the LED is continuously lit, the Adapter is successfully connected. If the LED is flickering, the Adapter is actively sending or receiving data.
Full/Col	Green	The Full/Col LED also serves two purposes. If this LED is lit up continuously, the connection is running in Full Duplex mode. If the LED flickers, the connection is experiencing collisions. If this LED flickers too often, there may be a problem with your connection. See “Appendix A: Troubleshooting” if you encounter this problem.
100	Orange	The 100 LED lights up when a successful 100Mbps connection is made. If this LED does not light up, then your connection speed is 10 Mbps.
USB	Green	The USB LED lights up when the Adapter is connected to a PC and powered on.

Connecting your VPN100

1. Before you begin, make sure that all of your hardware is powered off, including the Adapter, PCs, cable or DSL modem, and/or Router.
2. Connect one end of the USB cable to the USB port on the Adapter and the other end of the USB cable to a USB port on your PC.
3. Connect one end of an Ethernet cable to the Ethernet port on the Adapter, and the other end to an Ethernet port (LAN port) on a Network. If you are not using a Router, you can connect it directly to a Cable or DSL modem.

If the PC is powered up:

- The USB LED will light up green as soon as the Adapter is connected correctly to the PC.
- The Diag LED will light up red for a few seconds when the Adapter goes through its self-diagnostic test. This LED will turn off when the self-test is complete.

4. Turn on the PC, cable or DSL modem and/or Router.
5. If this is the first time you have connected the VPN100 Adapter to this computer, you will be prompted to install drivers by Windows. Refer to the following section and follow the instructions for the version of Windows you are using.

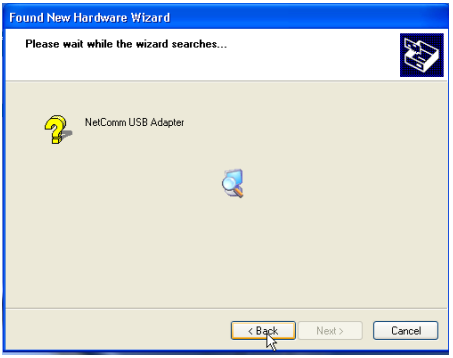
Installing USB drivers

The following section details the driver installation instructions for Windows XP. For other operating systems, please refer to the User Guide on the CD-ROM

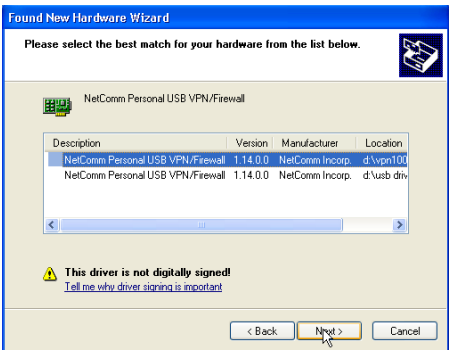
Windows XP

1. Insert the NetComm Driver CD-ROM in your CD-ROM drive and turn on your computer.
2. When prompted by the Found New Hardware Wizard confirm that "**Install the software automatically (Recommended)**" is selected and click on **Next>**.

3. The Found New Hardware Wizard will search for the correct driver.

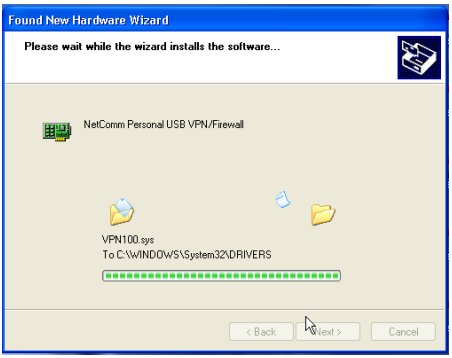


4. Select the **NetComm Personal USB VPN/Firewall** and click on **Next>**.

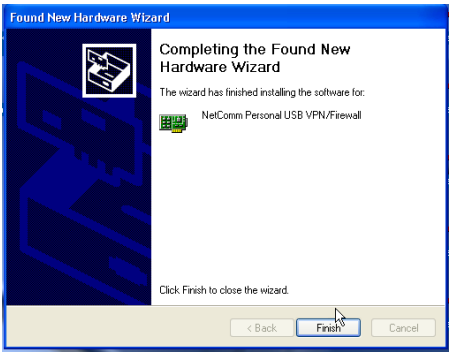


5. If prompted, click on **Continue Anyway** to proceed with the installation.

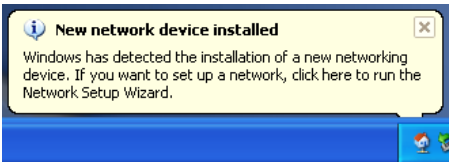
6. Windows will install the driver on your system.



7. Click on **Finish** to complete the installation.



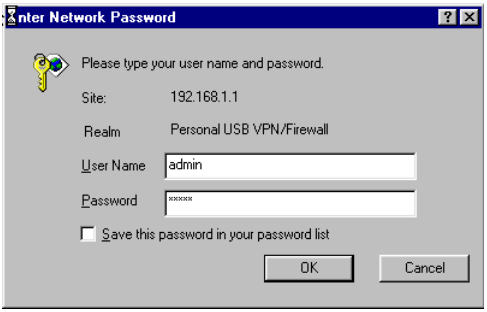
8. Windows XP will advise that a **new network device** has been installed.



Configuring the VPN100

Using the Web-based User Interface

The NetComm VPN100 uses a Web-based User Interface for configuration. Start your web browser and type http://192.168.1.1 in the browser's address box and press "Enter". This address is the factory default IP Address of your NetComm VPN100. You should check if it has been changed by your Network Administrator.



The "Username and Password Required" prompt box will appear. Leave the "User Name" empty and type "admin" (default password) for the "Password". Click "OK". The setup screen will load.

Note: *This password should be changed via the Administration page immediately. The password can be reset by restoring the factory defaults with the Reset button.*

When making changes to the settings, click on the "Apply" button before moving to another page. The router will reboot and refresh the screen in five seconds. Continue the session by selecting more menu items.

Note: *This log-in process will only be required when you are changing the connection type, configuring other options or when you are Connecting / Disconnecting VPN tunnels in the VPN100.*

The VPN100 factory defaults have the WAN connection type set as "Obtain IP Automatically" (known as DHCP). You may not need to configure anything if this is the mode that suits your connection situation.

There are three sets of Username & Passwords described in this guide:

- *The 'Admin' password which allows you to access your VPN100 to make configuration changes to it. This password belongs to the VPN100 and will always be the same unless you change it.*
- *The 'PPP' or 'Heartbeat' Username & Password which authenticates you with your ISP. (Only required when using PPP or Heartbeat connection types.) This password belongs to the ISP and it will depend upon your account with the ISP.*
- *Hotel or Airport Username & Passwords are some times issued when you are accessing the Internet via a paid service. This username and password is likely to be different for every different paid service you use.*

Choices when Travelling

Note: *If this is the first time you are using the VPN100, you will need to install the correct USB drivers for your operating system before choosing your connection type. Refer to the "Installing USB Drivers" section.*

When you are travelling you may need to change the configuration of the VPN100 to suit the type of connection you wish to use.

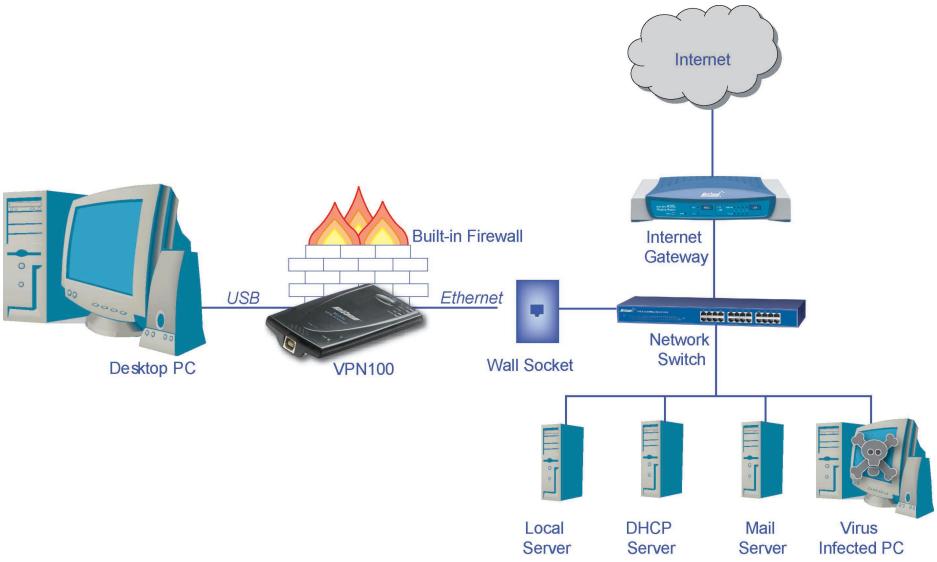
The main connection types are:

- DHCP Ethernet Connection or "Obtain IP automatically"
- A Static IP Ethernet Connection or "Static IP"
- A directly connected ADSL modem or "PPPoE service"
- A PPTP Ethernet service or "PPTP service"
- A directly connected Telstra Cable modem or "Heartbeat"

To help you choose the type of connection you may need to use for your location please see the following scenarios and follow the instructions given.

Connecting to an office LAN (Ethernet connection)

Often when you are visiting a Client's office you will need to connect back to your company's office network to retrieve a file or check your email. Most commonly, the connection provided is an Ethernet (LAN) port on the wall or a Network Switch. When connecting in this way you can access the local office, the Internet (presuming the local office has an Internet connection) and your Companies office (presuming you have a VPN server / Gateway at your remote office).



Ask the Local Network Administrator

It is advisable to speak to the Local Network Administrator of the client's office to see if there are any restrictions (such as MAC / IP filtering or lack of VPN pass-through) on the network that may block access to local resources and more importantly access to the Internet. You will also need to enquire if the LAN supports DHCP, and what IP address you should use if it does not.

DHCP or Static?

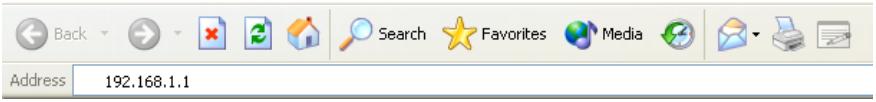
Most modern office networks run a DHCP server that will automatically allocate your VPN100 with the correct IP address settings – this is the easiest way to connect and you should try this setting first. Alternatively you should ask the Local Network Administrator for "Static IP address" settings to allow you to connect to the local network. Once you have decided your connection method please refer to one of the two options as follows:

Note: *In its factory default mode the VPN100 is already set to use DHCP.*

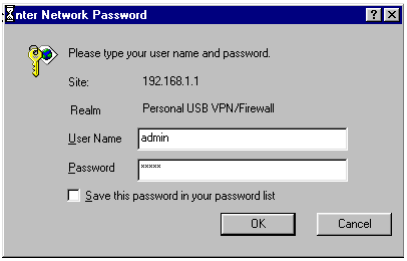
Option 1 - Using DHCP (follow these steps if the Local Network supports DHCP)

If the office uses DHCP follow the steps below to configure your connection:

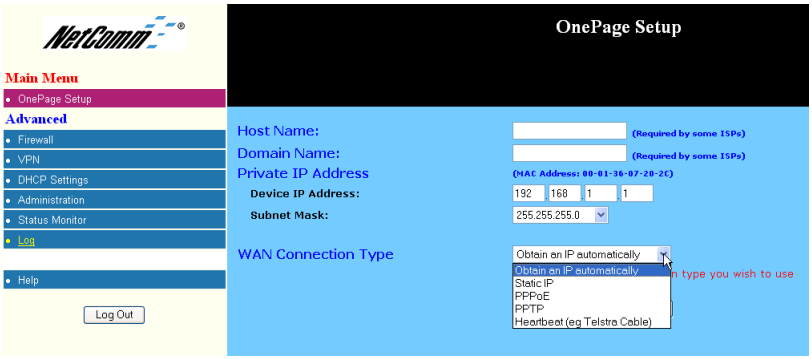
1. Join your VPN100 to your computer's USB socket with the USB cable.
2. Use the Ethernet cable provided to connect the VPN100 to an Ethernet port provided by the office you are visiting. Check that the "Link/Act" light on the VPN100 is now lit.
3. Log in to your VPN100 by typing the Device IP address into the location bar of your web browser. The Default IP address is "192.168.1.1"



4. When prompted for the Username and Password, enter them as previously set by the owner of the VPN100. The defaults are "admin" for username and "admin" for password.



5. In the Onepage setup screen, click the down arrow of the "WAN connection type" box and choose "Obtain an IP Automatically". Then click "Apply" at the bottom of the page.



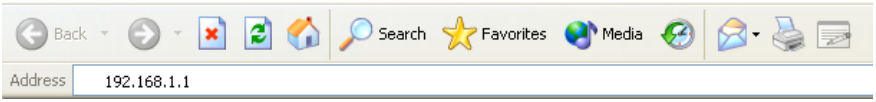
6. Your VPN100 will reboot (and your connection will be lost temporarily). Once the reboot is completed you can choose “Status Monitor” from the menu to view the IP address you have obtained via DHCP.

Note: If your “Public IP address” is shown as “0.0.0.0” then you have not been automatically assigned an IP address. Speak to the local network administrator for further advice.

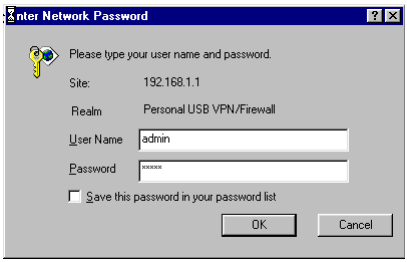
7. Your computer should now be able to view the Local Network as well as access the Internet via the local network’s Internet connection. If you have a VPN tunnel pre-configured you should also be able to enable that tunnel to connect through the Internet to your company’s office network.

Option 2 - Using Static IP (follow these steps if the Local Network does not support DHCP)

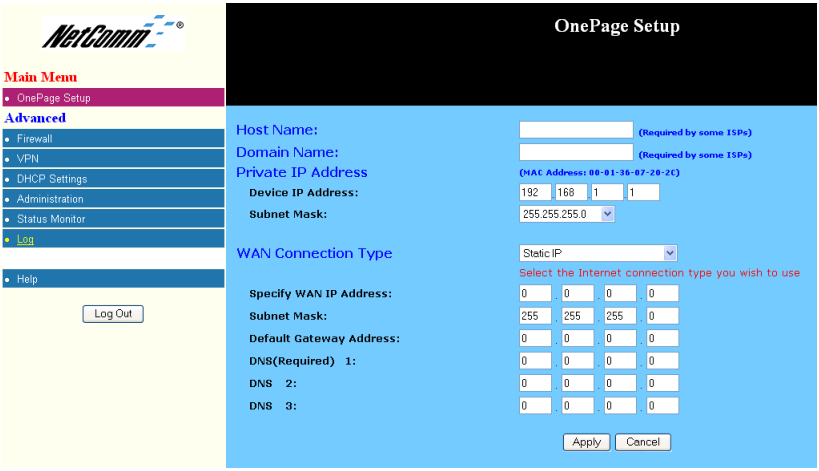
1. Consult your local Network Administrator and ask them for the following settings:
   - Static IP Address
   - Subnet Mask
   - Gateway
   - DNS
   - DNS 2 (optional)
2. Join your VPN100 to your computer’s USB socket with the USB cable.
3. Use the Ethernet cable provided to connect the VPN100 to an Ethernet port provided by the office you are visiting. Check that the “Link/Act” light on the VPN100 is now lit.
4. Log in to your VPN100 by typing the Device IP address into the location bar of your web browser. The Default IP address is “192.168.1.1”



5. When prompted for the Username and Password, enter them as previously set by the owner of the VPN100. The defaults are “admin” for Username and “admin” for password.

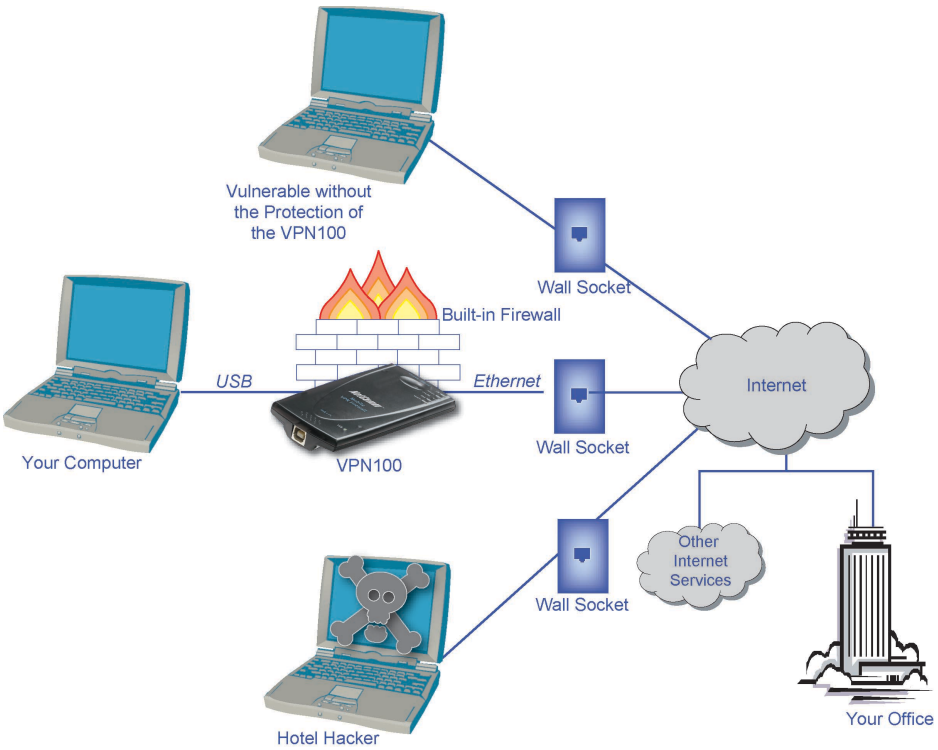


6. In the Onepage setup screen, click the down arrow of the “WAN connection type” box and choose “Static IP”. Enter the details as supplied by the Local Network Administrator, i.e. Static IP Address (WAN), Subnet Mask, Gateway (Default Gateawy), DNS1. Then click “Apply” at the bottom of the page.



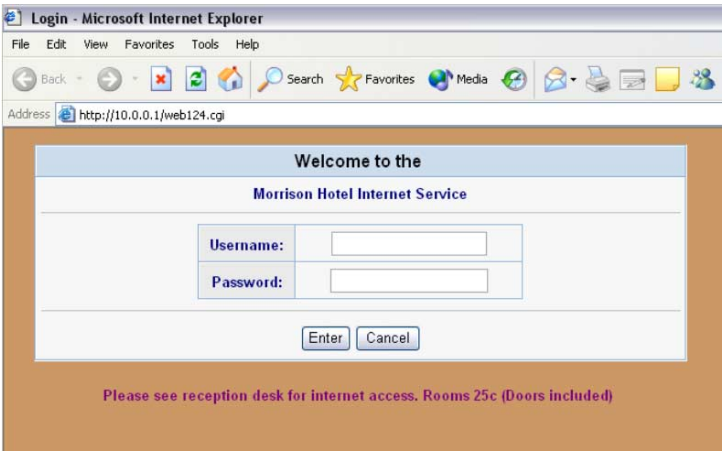
Connecting to a Hotel / Airport Ethernet (LAN) port

Often when you are visiting Hotels or Airports you will need to connect back to your office network to retrieve a file or check your email. Most commonly, the connection provided is an Ethernet port on the wall or a Network Switch. When connecting in this method using the VPN100 you can access the Internet (and run a VPN tunnel to your office) whilst remaining shielded (firewalled) from other people on the Hotel / Airport Network.



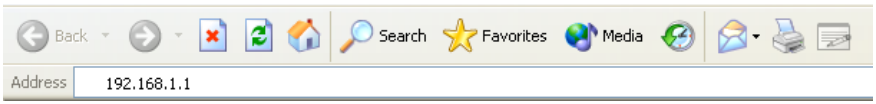
Hotel / Airport Username & Password

Because most Airport / Hotel Internet services are “Pay for time” type services you may need to also complete an extra log-in screen with a username and password that is given to you when you purchase your internet access. This log-in screen can only be accessed after you have chosen your VPN100 connection method. The Hotel / Airport log-in screen may look something like the screen below:

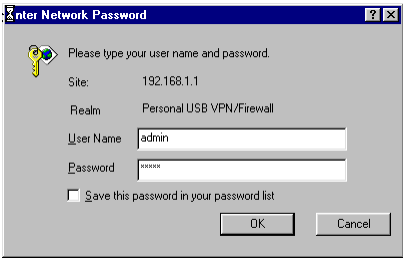


Follow the steps below to configure your connection;

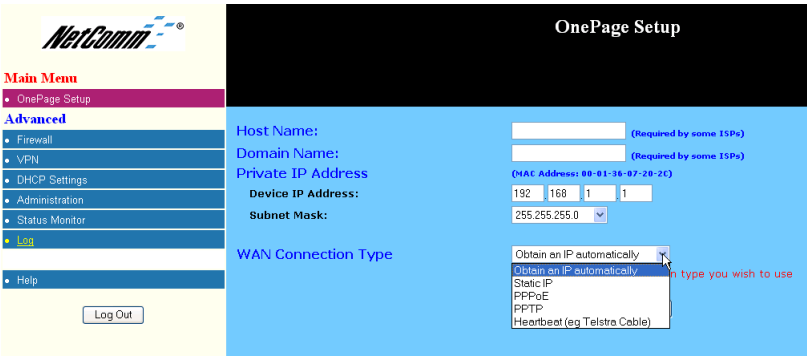
1. Join your VPN100 to your computer’s USB socket with the USB cable.
2. Use the Ethernet cable provided to connect the VPN100 to an Ethernet port provided by the Hotel / Airport you are visiting. Check that the “Link/Act” light on the VPN100 is now lit.
3. Log into your VPN100 by typing the Device IP address into the location bar of your web browser. The Default IP address is “192.168.1.1”



4. When prompted for Username and Password enter them as previously set by the owner of the VPN100. The defaults are “admin” for username and “admin” for password.



5. In the Onepage setup screen, click the down arrow of the “WAN connection type” box and choose “Obtain an IP Automatically”. Then click “Apply” at the bottom of the page.



6. Your VPN 100 will reboot (your connection will be lost temporarily). Once the reboot is completed you can choose “Status Monitor” from the menu to view the IP address you have obtained via DHCP.

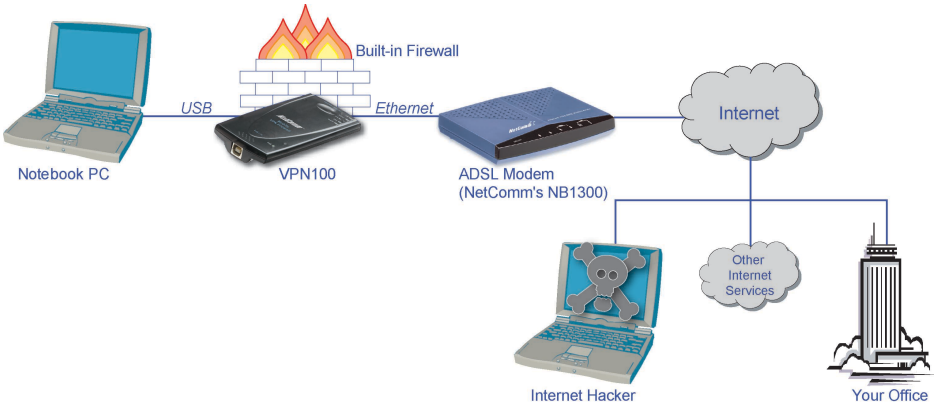
Note: *If your “Public IP address” is shown as “0.0.0.0” then you have not been automatically assigned an IP address, speak to the Hotel / Airport operator for further advice.*

7. Your computer should now be able to browse the Internet via the Hotel / Airport Internet connection. If you find that when browsing your are presented with another (different) log-in screen (such as shown above) then you may need to enter a Username and Password issued by the Hotel / Airport before being allowed access to the Internet. Once you have done this you should not only be able to access the Internet but you should also be able to enable your pre-configured VPN tunnel.

Connecting directly to an ADSL Internet modem

When using your VPN100 at home with an ADSL Internet service the best way to connect is by plugging the VPN100 Ethernet port directly into the Ethernet port of an ADSL modem. In this scenario the ADSL modem should be in 'Bridged mode' not 'Routed mode'.

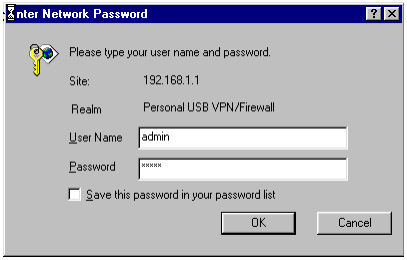
Note: *If you wish to use your VPN100 with an ADSL Router (or ADSL Gateway) which shares the ADSL connection with more than one computer then you should treat the connection as an 'Office LAN' and follow the instructions for "Connecting to an Office LAN"*



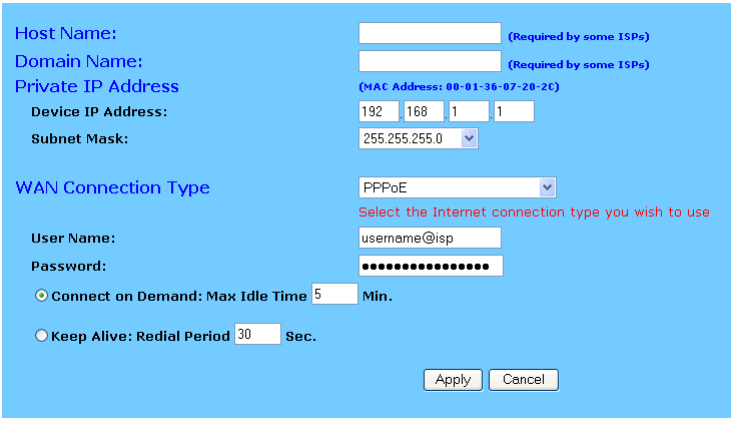
Follow the steps below to configure your connection;

1. Turn on your ADSL modem, with an enabled ADSL line connected to your ADSL modem.
2. Join your VPN100 to your computer's USB socket with the USB cable.
3. Use the Ethernet cable provided to connect the VPN100 to the Ethernet port of your ADSL modem. Check that the "Link/Act" light on the VPN100 is now lit.
4. Log into your VPN100 by typing the Device IP address into the location bar of your web browser. The Default IP address is "192.168.1.1"

5. When prompted for the Username and Password, enter them as previously set by the owner of the VPN100. The defaults are "admin" for Username and "admin" for password.



6. In the Onepage setup screen, click the down arrow of the “WAN connection type” box and choose “PPPoE”.



7. The screen will change briefly, type in your PPP username and password as given to you by your ISP (please note this is NOT the same as your Admin password used to log in to the VPN100). Then click “Apply” at the bottom of the page.

Note: If you select PPPoE, you will no longer need to use any ISP supplied PPPoE software on your computer to connect to the Internet (the VPN100 does this for you)

8. Your VPN100 will reboot (and your connection will be lost temporarily). Once the reboot is completed you can choose “Status Monitor” from the menu to view the IP address you have obtained via DHCP.

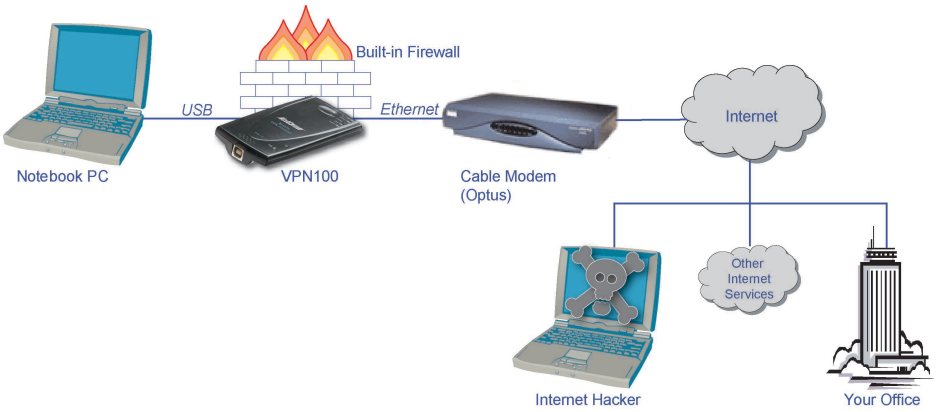
Note: If your “Public IP address” is shown as “0.0.0.0” then you have not been automatically assigned an IP address, speak to the local network administrator for further advice.

9. Your computer should now be connected to the Internet via your ADSL modem. If you have a VPN tunnel pre-configured you should also be able to enable that tunnel to connect through the Internet to your company’s office network.

Connecting directly to an Optus Cable Internet modem

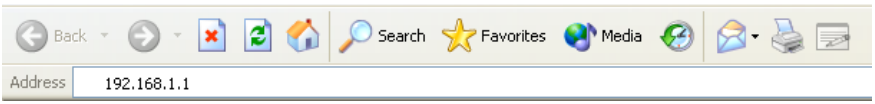
When using your VPN100 at home with an Optus Cable Internet service the best way to connect is by plugging the VPN100 Ethernet port directly into the Ethernet port of your Optus Cable modem. The Optus cable system does not require a username and password and it uses DHCP to assign you a Public IP address.

Note: *If you wish to use your VPN100 with an existing Broadband Router, which shares the Optus Cable connection with more than one computer, then you should treat the connection as an 'Office Network' and follow the instructions for "Connecting to an Office LAN".*



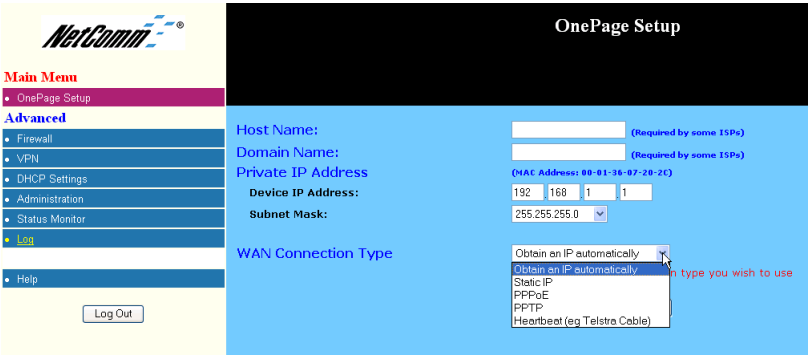
Follow the steps below to configure your connection:

1. Turn on your Optus Cable modem, ensure the Cable modem is connected to the Cable network and has "Cable Sync".
2. Join your VPN100 to your computer's USB socket with the USB cable.
3. Use the Ethernet cable provided to connect the VPN100 to the Ethernet port of your Cable modem. Check that the "Link/Act" light on the VPN100 is now lit.
4. Log into your VPN100 by typing the Device IP address into the location bar of your web browser. The Default IP address is "192.168.1.1"



5. When prompted for the Username and Password, enter them as previously set by the owner of the VPN100. The defaults are “admin” for Username and “admin” for password.

6. In the Onepage setup screen, click the down arrow of the “WAN connection type” box and choose “Obtain an IP Automatically”. Then click “Apply” at the bottom of the page.



7. Your VPN 100 will reboot (and your connection will be lost temporarily). Once the reboot has completed you can choose “Status Monitor” from the menu to view the IP address you have obtained via DHCP.

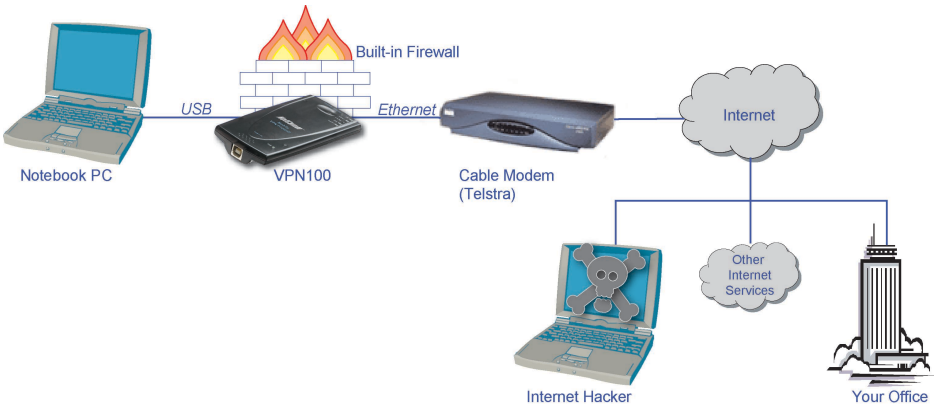
Note: *If your “Public IP address” is shown as “0.0.0.0” then you have not been automatically assigned an IP address, speak to the local network administrator for further advice.*

8. Your computer should now be able to view the Local network as well as access the Internet via the local network’s internet connection. If you have a VPN tunnel pre-configured you should also be able to enable that tunnel to connect through the Internet to your company’s office network.

Connecting directly to a Telstra Cable Heartbeat Modem

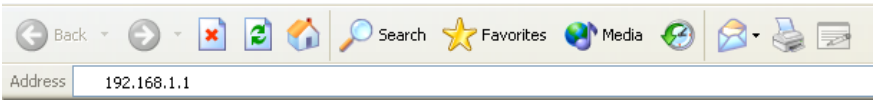
When using your VPN100 at home with a Telstra Cable Internet service the best way to connect is by plugging the VPN100 Ethernet port directly into the Ethernet port of a Telstra Cable modem.

Note: *If you wish to use your VPN100 with an existing Broadband Router, which shares the Telstra cable connection with more than one computer, then you should treat the connection as an 'Office Network' and follow the instructions for "Connecting to an Office LAN".*



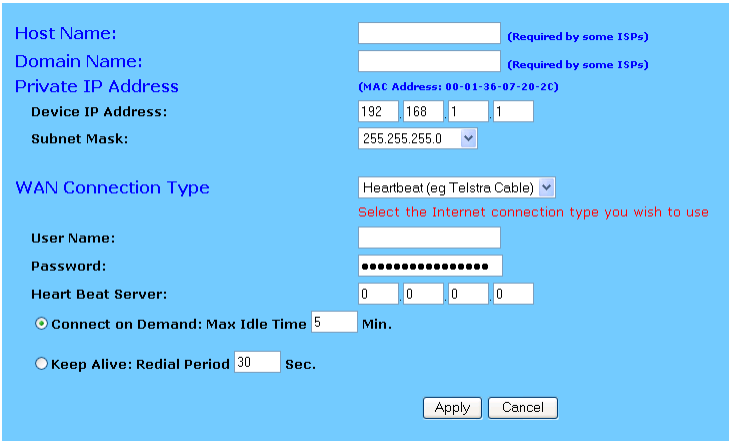
Follow the steps below to configure your connection:

1. Turn on your Telstra Cable modem.
2. Join your VPN100 to your computer's USB socket with the USB cable.
3. Use the Ethernet cable provided to connect the VPN100 to the Ethernet port of your Telstra Cable modem. Check that the "Link/Act" light on the VPN100 is now lit.
4. Log in to your VPN100 by typing the Device IP address into the location bar of your web browser. The Default IP address is "192.168.1.1"



5. When prompted for the Username and Password enter them as previously set by the owner of the VPN100. The defaults are "admin" for Username and "admin" for password.

6. In the Onepage setup screen, click the down arrow of the "WAN connection type" box and choose "Heartbeat".



7. The screen will change briefly. Type in your Heartbeat username and password as given to you by your ISP (please note this is NOT the same as your Admin password used to log into the VPN100).

8. Type in the Heartbeat Server number as provided by your ISP. Then click "Apply" at the bottom of the page.

Note: *At the time of printing the Telstra cable service was changing. If Option 1 does not work as a valid HBS number please try option 2 for your state. In the future you may not be required to specify the actual Heartbeat Server IP address at all in this case the HBS field will not be visable in the VPN100 configuration screen.*

STATE	OPTION 1	OPTION 2
NSW	61.9.192.13	61.9.192.13
VIC	61.9.128.13	61.9.128.13
QLD	61.9.208.13	61.9.128.13
WA	61.9.240.13	61.9.192.13
SA	61.9.224.13	61.9.192.13

9. Your VPN100 will reboot (and your connection will be lost temporarily). Once the reboot is completed you can choose “Status Monitor” from the menu to view the IP address you have obtained via the Cable connection.

Note: If your “Public IP address” is shown as “0.0.0.0” then you have not been automatically assigned an IP address, speak to your ISP for further advice.

10. Your computer should now be connected to the Internet via the Telstra Cable Internet connection. If you have a VPN tunnel pre-configured you should also be able to enable that tunnel to connect through the Internet to your company’s office network.

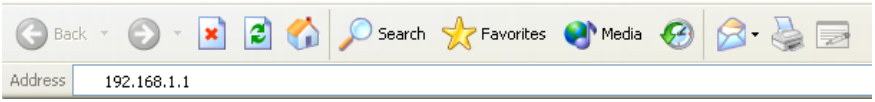
Starting / Terminating your VPN session

The VPN100 can be configured with up to five VPN tunnels that will allow you to securely connect to remote offices. The VPN tunnels can be configured to connect automatically when there is an Internet connection, but most often you will want to start them manually.

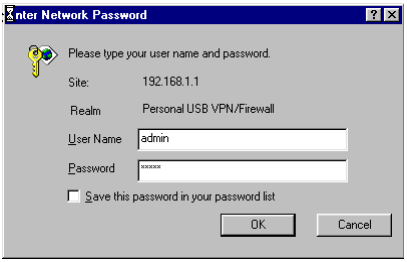
Note: *This guide does not detail how to configure the VPN tunnels. It presumes your VPN tunnels have already been correctly configured to connect to your desired network. For more information please refer to the User guide.*

To Start your VPN Session

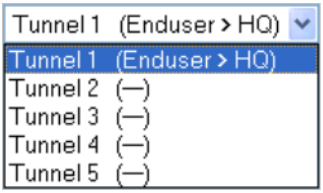
1. Connect your VPN100 via one of the methods suggested and confirm you have access to the Internet (e.g. check you can load a web page).
2. Log into your VPN100 by typing the Device IP address into the location bar of your web browser. The Default IP address is "192.168.1.1"



3. When prompted for Username and Password enter them as previously set by the owner of the VPN100. The defaults are "admin" for Username and "admin" for password.

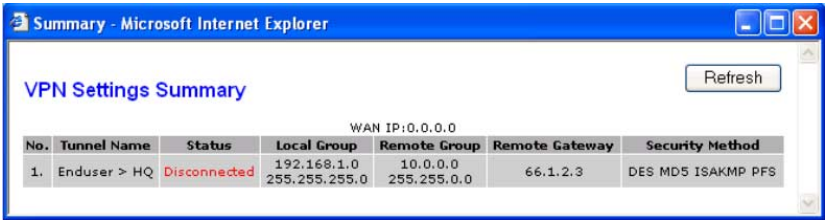


4. From the left hand menu choose VPN, when the VPN page loads choose the tunnel you wish to start.



5. Ensure the tunnel is enabled.

6. Scroll down to the bottom of the page and click ‘Connect’ (if you had to enable the tunnel first click ‘Apply’ then click ‘Connect’)
7. After a few seconds the tunnel should have been connected. Check this by refreshing your browser screen (select VPN from the left hand menu again) and check the bottom of the page for the Status. Alternatively you can click the Summary button or check that the session LED is now lit on the VPN100.



8. If the VPN tunnel status is ‘connected’ you can now start accessing resources on the remote network.

To Terminate a VPN Session

1. Follow steps 1 to 4 from the previous section (but chose the tunnel you wish to ‘Terminate’ instead of ‘Start’)
2. Once you have chosen the tunnel, scroll to the bottom of the page and click “Disconnect”. When the page refreshes the tunnel status should now be “Disconnected”. You can double check by clicking the “Summary” button to see which tunnels are connected and which have been disconnected.

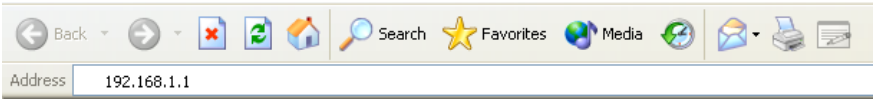
Note: *If the Advanced settings of your VPN Tunnel are set to “Keep Alive” then the VPN tunnel will be created whenever you have an internet connection. Choosing ‘Disconnect’ for this tunnel will only disconnect the tunnel temporarily. You must disable the ”keep alive” option if you do not wish this tunnel to continue automatically.*

Enabling / Disabling your firewall

The VPN100 is equipped with an Active Firewall which helps protect against Hacker attacks. However, sometimes you may need to turn off the active firewall to allow more sensitive Internet / Network applications to work through the VPN100. If you do disable the Active component of the firewall, the 'NAT process' will still be in place to offer moderate security.

To disable the Active Firewall

1. Connect your VPN100 via one of the methods suggested and confirm you have access to the Internet (e.g. check you can load a web page).
2. Log into your VPN100 by typing the Device IP address into the location bar of your web browser. The Default IP address is "192.168.1.1"



3. When prompted for the Username and Password, enter them as previously set by the owner of the VPN100. The defaults are "admin" for Username and "admin" for password.

4. From the left hand menu choose Firewall
5. When the Firewall page loads choose "Disable" and click "Apply" at the bottom of the page.

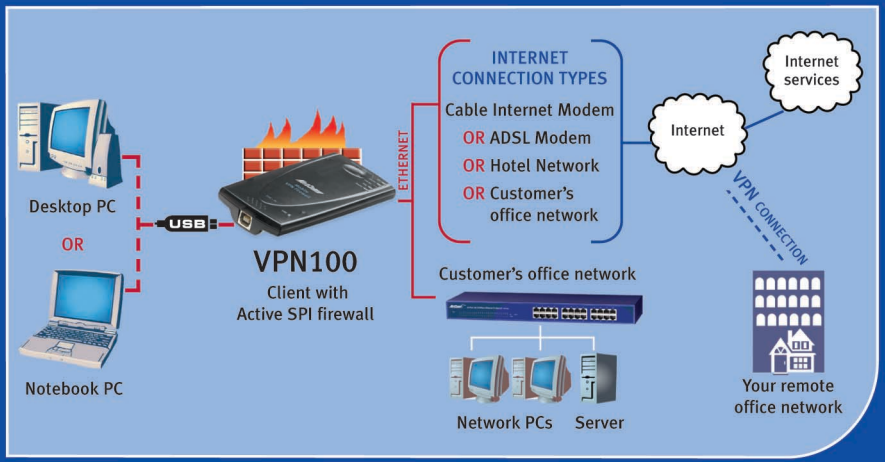
You Firewall is now disabled. You should re-enable your firewall when you have finished using the application that does not work through a firewall.

The only travelling companion for secure communications

Access your corporate or home network from wherever you are in the world with the NetComm Mobile VPN100. Advanced security features such as an active SPI firewall also ensure that you are protected from hackers.

Simple to install and configure, this small and lightweight device is perfect for any travelling executive. Just connect the NetComm Mobile VPN100 Firewall to your Notebook's USB port and access your network resources remotely from a hotel or another office via the Internet.

It's an essential travelling companion for every business executive.



KEY FEATURES

- Connects via PPPoE ADSL, LAN (DHCP) or Cable Internet
- Built-in IPsec VPN end-points with strong DES/3DES encryption
- Active hardware SPI firewall checks all incoming data
- Works with almost any Windows PC
- USB powered (no power pack required)
- Supports URL filtering – blocks; Java, ActiveX, Proxy & Cookies
- Network Address Translation hides PC from outsiders
- Easy to configure via your PC's web browser
- Back up and restore the device configuration

NetComm™

NetComm Limited, ABN 85 002 490 486 • PO Box 1200, Lane Cove NSW 2066 Australia. **PHONE** (02) 9424 2070 • **FAX** (02) 9424 2010 • **EMAIL** sales@netcomm.com.au
 Product Code: VPN100