Vololink
the future is wireless

VoloAccess™

3G+ Convergent Wireless Terminal

Voice • SMS • Data

USER MANUAL

TABLE OF CONTENTS

COPYRIGHT NOTICE

Safe and Efficient Use

Note: please read this information before using your VoloAccess.

Save this user manual as it contains important safety information and operating instructions.

- The VoloAccess is intended for indoor use only.
- The VoloAccess must not be connected to telephone cabling that leaves the building.
- Use only the supplied AC adaptor.
- Should it be necessary please return the VoloAccess to your supplier for repair. There are no user serviceable parts inside.
- If the base is used, ensure the main unit is securely located on the base.

Radio Frequency Energy

Your VoloAccess is both a radio transmitter and receiver. When the VoloAccess is turned on, it receives and transmits RF (Radio Frequency) energy. The system that handles your call when you are using your VoloAccess controls the power level at which your VoloAccess transmits.

All VoloAccess terminals are designed to operate within the limits for exposure to RF energy set by national authorities and international health agencies. These limits are verified by SAR (Specific Absorption Rate) measurements; which are usually performed on products that are intended for use at the ear. As the VoloAccess is not intended to be used close to the human body SAR measurements are not applicable to the VoloAccess.

Electronic Devices

Most modern electronic equipment, for example equipment in hospitals and cars, is shielded from the effects of RF energy. However, certain electronic equipment is not, so the RF energy from the VoloAccess may affect some electronic equipment, therefore:

- Do not use your VoloAccess near medical equipment without requesting permission.
- Do not use your VoloAccess in airplanes.
- Pacemaker patients should be aware that the use of a VoloAccess close to a pacemaker may cause the pacemaker to malfunction.
- Some hearing aids might be disturbed if placed very close to the VoloAccess.

Electrical devices connected to the same AC power outlet that is used by the VoloAccess may generate excessive interference to the VoloAccess.

About the VoloAccess

The VoloAccess Convergent Wireless Terminal is the equivalent of an Internet connection and (on voice enabled models) a phone line combined. Telephone handsets and computer equipment can be connected to the VoloAccess in the normal way using standard connectors.

The VoloAccess Convergent Wireless Terminal is a wireless voice and high speed data access point for use over HSPA or HSPA+ capable UMTS networks. The VoloAccess provides both voice and advanced wireless services, such as wireless broadband Internet services in areas where conventional telephone lines either do not exist or are too far from the nearest xDSL enabled exchange. Using the VoloAccess also offers a convenient and cost effective alternative to wireline connections for voice and high speed data services, when mobility is important. Standard telephone, SMS and Internet connections are all simultaneously available.

The VoloAccess enables simultaneous HSPA or HSPA+ data access for multiple users via the Ethernet ports, or wirelessly using WiFi.

Once the VoloAccess has been connected and powered up, the following services are available:

Voice Services

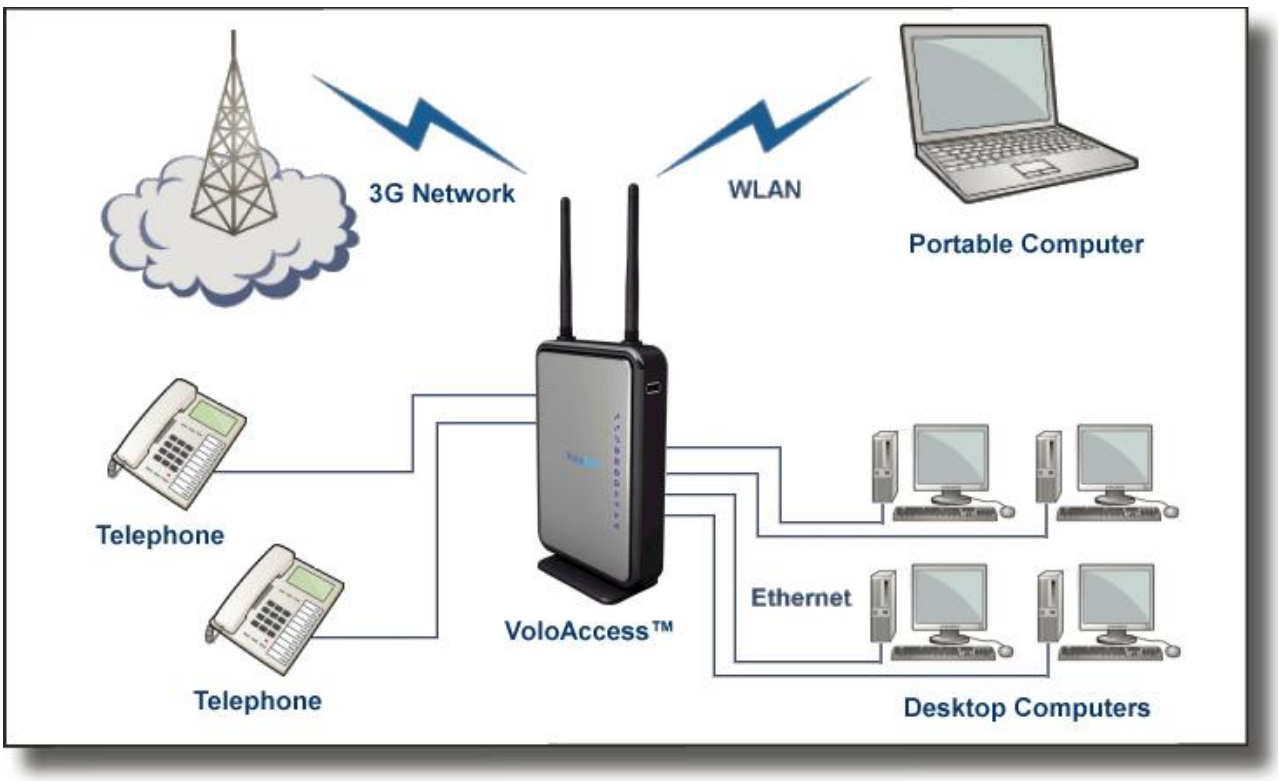
Voice enabled models of the VoloAccess provide the equivalent of a PSTN or fixed line connection via the 3G mobile network. Just plug in a standard analogue handset, or an answering system with extension handsets. The VoloAccess is compatible with most phones available on the market today that support tone dialling. The VoloAccess does not support old devices that are capable of pulse dialling only.

Internet Services

The VoloAccess provides a true broadband solution with HSPA services enabled on the 3G network. Connect your computer and you will be able to surf the Internet at speeds up to 7.2Mbps for HSPA version and 21Mbps for HSPA+ version.

SMS Services

The VoloAccess is a 3G mobile device so you can receive and send SMS messages. On your computer you can create, view and reply to SMS messages in the same way you would with any mobile phone.



Getting Started

The first step is to check that the VoloAccess package that you have purchased is complete.

The following is the packing list:

1 Getting Started Guide
1 VoloAccess
1 Base
1 Power Supply
1 Ethernet Cable
2 Antennas
1 CD (Contains the User Manual)

If any component is missing, please contact the retailer where you purchased the VoloAccess.

How to use this Manual

The manual is arranged in easy to follow sections. Use the Contents page to locate a particular topic.

Each section refers to its functionality as follows:

Voice How to use the VoloAccess as a Phone connection. (Voice enabled models only)

Internet How to use the VoloAccess as your Internet connection.

SMS How to use the VoloAccess to send and receive SMS messages.

As with computers, there is a lot of jargon and acronyms associated with wireless communications. To make understanding this manual easier, a Glossary of Terms is included.

For the technically minded a full Specification Sheet is included at the end of this manual.

There is a Troubleshooting section to assist with any difficulties that you may have with the VoloAccess.

Conventions used in this Manual

- A list has bullets in the left margin - the same bullets as used in this list.
- An important note or warning has the  icon in the left margin.
- A suggestion or hint has the  icon in the left margin.
- Informational text has the  icon in the left margin.
- Emphasized text is displayed **bold**.
- Critical text is displayed in **bold bright red**.
- Hyperlinks are displayed in underlined blue.

VoloAccess variants covered by this Manual

VoloAccess Series	VA121V	VA122V	VA125
Max Downlink data rate	7.2Mbps	7.2Mbps	21.0Mbps
Max Uplink data rate	5.76Mbps	5.76Mbps	5.76Mbps
850/1900/2100MHz	✓		
900/2100MHz		✓	
850/900/1900/2100MHz			✓
Two voice ports	✓	✓	

Installing the SIM (Subscriber Identity Module)

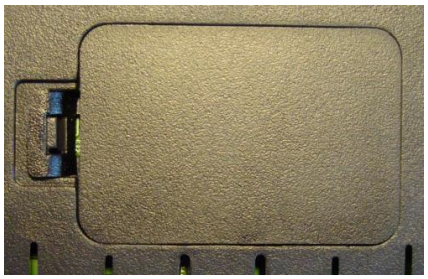
USIM (**U**niversal **S**ubscriber **I**dentity **M**odule) correctly describes the identity module used in 3G mobile devices like the VoloAccess. However, SIM which is the identity module used in 2G mobile devices is the term in common usage. For simplicity, the term SIM is used throughout this manual.

Before attempting to install the SIM, disconnect the power supply.

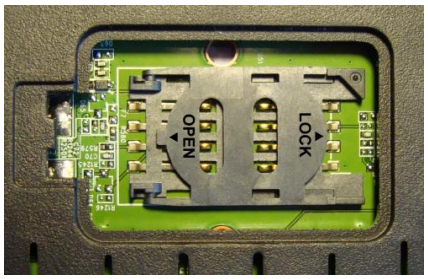
The SIM is installed in the side of the VoloAccess as follows:

Remove the side panel (the one without the Indicators on) by slipping a narrow object like a credit card or a small screwdriver under the edge and gently prise it off to reveal the SIM compartment.

Latch ►

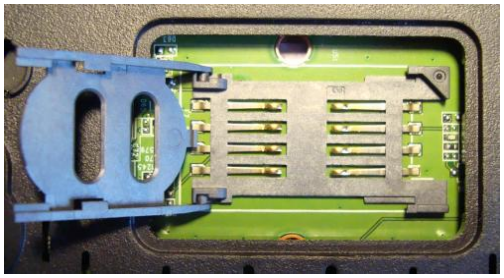


Press the cover latch and remove the cover to reveal the SIM holder as shown in the next image.

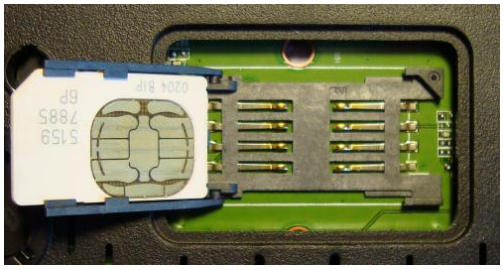


Gently slide the retainer in the OPEN direction.

(OPEN/LOCK is marked on the retainer)

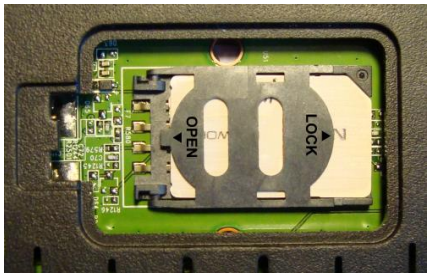


Turn the retainer over to expose the SIM slot. (the retainer is hinged)



Slide the SIM into the retainer with the cut corner positioned as shown.

The contact pads on the SIM should be facing up ready to engage the connectors in the base of the holder.



Turn the retainer over and slide in the LOCK direction to secure the SIM in position.

Complete installing the SIM by:

- replacing the SIM compartment cover, and
- refitting the side panel.

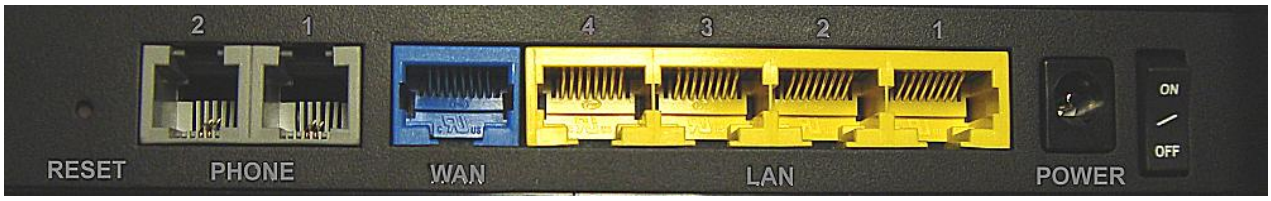
Removing the SIM

Before attempting to remove the SIM, disconnect the power supply.

To remove the SIM simply perform the above steps in the reverse order.

VoloAccess Connections

The following image shows the rear panel of the VoloAccess and describes the purpose of each connection.



RESET Reset button – Use a paper clip to reset the VoloAccess. See below for further information on resetting the VoloAccess.

PHONE* Phone ports – Connect a phone here (Voice enabled models only).

WAN By default, the WAN port can be used as a LAN port. In this configuration the VoloAccess is a five port switch. If the WAN port is configured to connect the VoloAccess to an external modem for alternative WAN access, the VoloAccess is then a four port switch.

The WAN port can be disabled. See Operating Mode under Settings on the WAN Ethernet page for further information.

LAN Ethernet ports (LAN) – Connect locally attached computers here.

POWER Power supply – Connect the power supply cable here. Use the adjacent switch to turn the VoloAccess On/Off.

* The two phone ports on the VoloAccess share a common phone line. If two phones are connected to the VoloAccess, the first handset lifted will get the line and can place a call. While a call is in progress, any attempt to make a call from the second phone results in the busy signal. For inbound calls, both phones ring – the first handset lifted will take the call; the other handset receives the busy signal.

Front Panel Connections

The following shows the front panel of the VoloAccess and describes the purpose of each connection.

WiFi Protected Setup (WPS) button and indicator. Used for establishing WiFi connection using WPS. See WPS for further information.

USB port – Reserved for future use.

WiFi Protected Setup (WPS)

The WPS function is designed to assist with setting up a secure WiFi connection.

A WPS-capable network interface device is required to use this feature.

WPS button

The following table describes the behaviour of the WPS button indicator.

Status	WPS Indicator
WPS enabled and idle	**ON** – solid
WPS session in progress	**ON** – flashing
WPS disabled	**OFF**

For further information on using the WPS feature refer to the WPS section.

Resetting the VoloAccess

The unit can be reset at any time after the power-up indicators sequence is finished and the unit enters normal operation. This is done by pressing and holding down the reset button at the back of the unit.

The VoloAccess reset button has three functions described in the following table: (see notes below)

Reboot the VoloAccess (Same as switching off and on)	**Reset the VoloAccess** (Reset to factory configuration)	**Clear VoloAccess flash memory** (Reset and clear saved data)
Press the reset button for less than 5 seconds	Press the reset button for more than 5 seconds and less than 10 seconds	Press the reset button for more than 10 seconds
WPS, Signal Strength and Mobile Network Indicators turn off	WPS, Signal Strength and Mobile Network Indicators turn on	WPS, Signal Strength and Mobile Network Indicators turn off

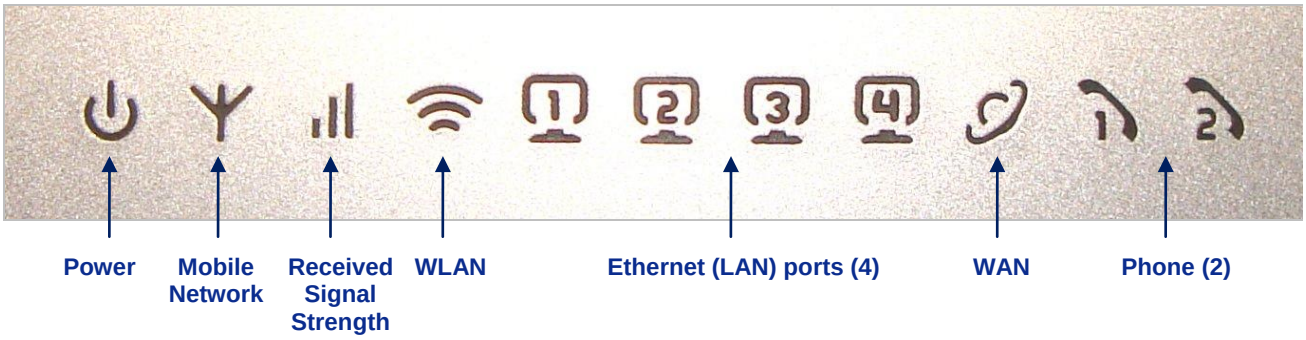
Notes:

- The first row defines the function.
- The second row describes the timing of the reset button press.
- The third row describes the behaviour of the VoloAccess indicators.

Clearing the VoloAccess flash memory should be used as a last resort when troubleshooting a problem. Data stored in flash memory includes items like SMS Messages and the Log files.

VoloAccess Indicators

The following image shows the VoloAccess Indicators and describes what each one represents.



The following tables describe the behaviour of the indicators.

Power Supply

Status	Power Indicator
The VoloAccess is connected to mains power and switched ON.	**ON** – solid
The VoloAccess is not connected to mains power or it is switched OFF.	**OFF**

Mobile Network Connection

Status	Mobile Network Indicator
SIM is not available (missing or locked)	**OFF**
Searching for a mobile network	**ON** – flashing at 1 second intervals
Connected to a mobile network – voice and SMS available, but no data service	**ON** – flashing at 2 second intervals
Broadband data service established - all services available	**ON** – solid

Received Signal Strength

Status	Received Signal Strength Indicator
Good signal present	**ON** – solid
Weak signal present	**ON** – flashing at 1 second intervals
No signal present	**OFF**

Wireless Local Area Network (WLAN)

Status	WLAN Indicator
WiFi is not enabled	**OFF**
WiFi is enabled	**ON** – solid
WiFi network traffic is detected	**ON** – flashing

Local Area Network (LAN)

Status	LAN Indicator
Network cable is not connected	**OFF**
Network cable is connected to the VoloAccess and a LAN is present	**ON** – solid
Network traffic is detected	**ON** – flashing

Wide Area Network (WAN)

Status	WAN Indicator
Network cable is not connected to the WAN port	**OFF**
Network cable is connected to the WAN port and a WAN is present	**ON** – solid
WAN network traffic is detected	**ON** – flashing

Phone 1 / Phone 2

Status	Phone 1 / Phone 2 Indicators
Phone is On Hook and idle	**OFF**
Phone is Off Hook	**ON** – flashing at 1 second intervals
Phone is receiving a call or dialling out	**ON** – flashing at 1 second intervals

Power up sequence

During start up, the VoloAccess flashes the WiFi Protected Setup, Signal Strength and Mobile Network indicators at 1 second intervals for about 10 seconds.

Setting up the VoloAccess

VoloAccess Location

The signal strength available at the VoloAccess location affects the performance of the unit. The stronger the signal, the better the VoloAccess performance.

Test several locations by moving the VoloAccess while looking at the Signal Strength indicator. (Wait 10 to 20 seconds after each change of location for the Signal Strength to be measured and displayed – a flashing indicator represents a weak signal). Select a location where the Signal Strength indicator is on and solid.

Moving the VoloAccess as little as 5 cm can affect the Signal Strength.

Recommendations:

- Select an indoor location, preferably close to a window and the roof. Generally, you will experience better Signal Strength in these locations.
- Position the VoloAccess antennas as high as possible for better reception.
- Do not install the VoloAccess in a bathroom, a wet or damp environment or an outdoor location.
- Do not install the VoloAccess in locations or rooms that contain large amounts of metal, steel or wiring. Locations that contain large amounts of metal inhibit the transmission of Radio Frequency (RF).
- Do not expose the VoloAccess to extreme temperatures (near radiators, cooling vents, etc).
- If you experience poor Signal Strength, an (optional) higher gain antenna may result in improvement.

Mounting Position

The VoloAccess can be mounted in a vertical position by attaching the supplied base as shown here.

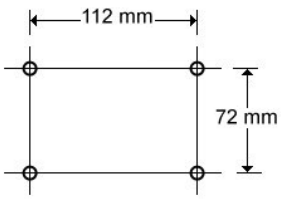
or,

It can be mounted horizontally by removing the side cover (the one without the indicators) and standing it on the rubber feet. Turn the hinged antennas to the vertical position.

or,

The VoloAccess can be wall mounted by removing the side cover and attaching it to (at least two) screws with a maximum head diameter of 7mm.

Wall Mounting drilling dimensions ⇨



Connecting the VoloAccess to a Computer

The VoloAccess is connected to a computer using one of the four Ethernet (LAN) ports on the back of the unit and the Ethernet port on the computer. Use an Ethernet cable for this purpose.

If you are connecting a computer to the VoloAccess wirelessly, refer to the WiFi section for details

If the computer that you are connecting to the VoloAccess is already configured to obtain an IP Address and DNS server address automatically, skip this section and move to Checking the Connection. If this is not the case, continue with the following instructions.

Preparation

To prepare the computer for connection to the VoloAccess do the following:

Using Windows XP:

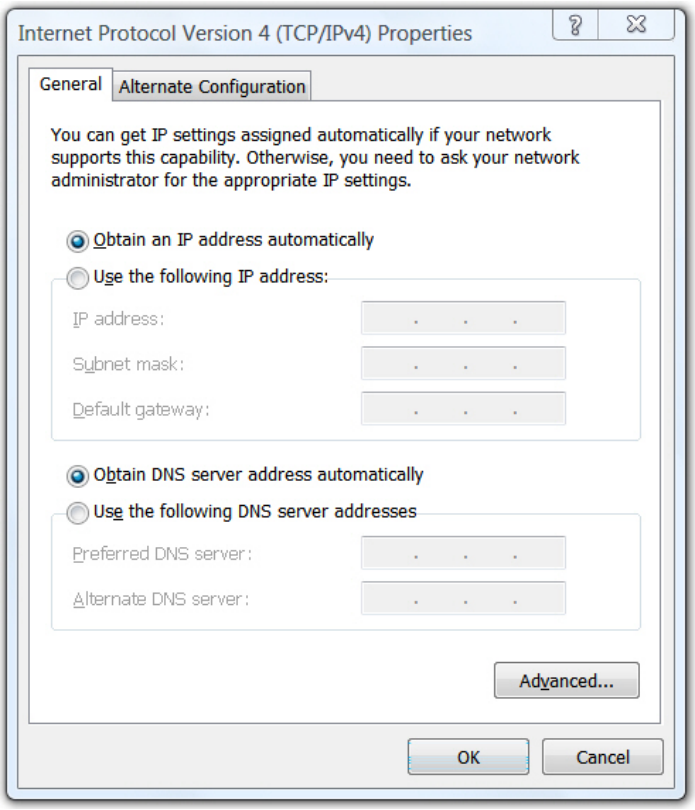
- Load the Windows Control Panel and double-click **Network Connections.**
- Under the heading **LAN or High-Speed Internet** right-click **Local Area Connection** and select **Properties**.
- Select **Internet Protocol (TCP/IP)** and click the **Properties** button.

A dialog box similar to the one below appears.

Using Windows Vista:

- Load the Windows Control Panel and double-click **Network and Sharing Center**.
- Click **View status**; located next to **Local Area Connection**.
- The **Local Area Connection Status** window is displayed. Click the **Properties** button.
- The **Local Area Connection Properties** window is displayed. Select **Internet Protocol Version 4 (TCP/IPv4)** and click the **Properties** button.

  A dialog box similar to the one below appears.



- Ensure that **Obtain an IP address** and **Obtain DNS Server** address are both set to **automatic**.

The VoloAccess is a DHCP server and will provide both of these addresses.

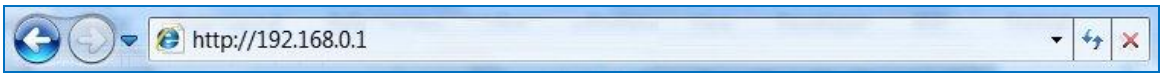
Checking the Connection

When the VoloAccess has been connected and the above steps completed, check that a connection exists between the VoloAccess and the computer. This is done by viewing the (blue) LAN indicator on the VoloAccess. It should be lit and steady.

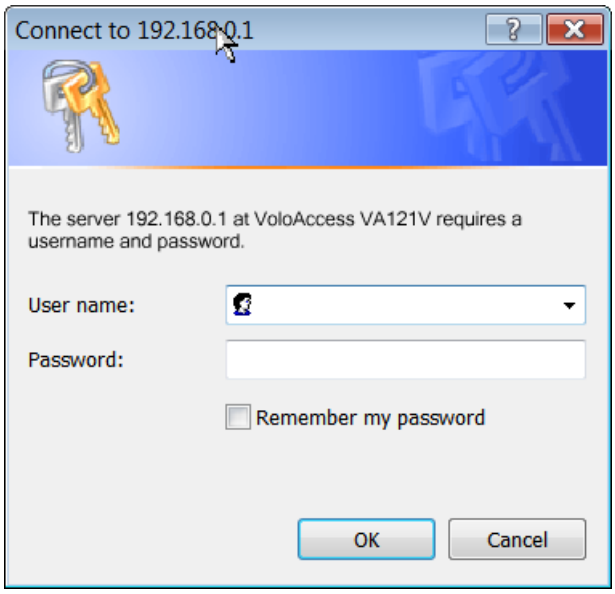
The next step is to connect to the Admin interface as follows:

Loading the Admin page

- Open your browser and enter the address http://192.168.0.1 in the Address line shown below, then press **Enter**.



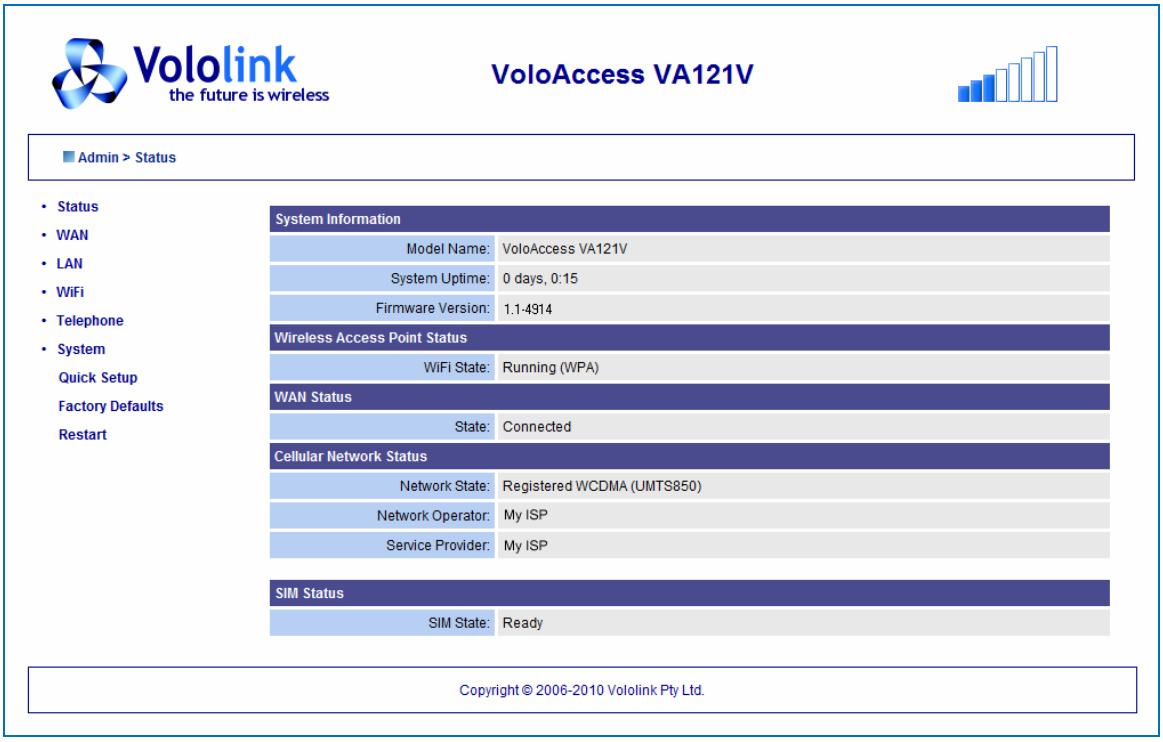
The **VoloAccess Log In** dialog appears.



- Type the User name – the User name is: **admin**
- Type the Password – the default password is: **password** (you can change this later)
- Click the **OK** button – the **VoloAccess Index** page appears:

- Click **Admin** - the **Admin Status** page is displayed.

To switch between SMS and Admin click the Vololink logo in the top left corner of any page - you will be returned to the Index page shown above.



If the WAN State is **Connected**, you are ready to use your VoloAccess to surf the Internet.

If this is not the case, continue by checking the configuration of the APN (Access Point Name).

Signal Strength Indicator

The Admin Status page also displays a graphic readout of the Signal Strength in the top right corner. Solid blue bars represent signal, outlined bars represent no signal. In the image above, the signal strength is 3.

Voice Services (Voice enabled models only)

To use the VoloAccess as a wireless telephone connection:

- Plug the phone lead into one of the Phone ports on the back of the VoloAccess.
- Lift the handset (you should hear a dial tone) and dial the number you wish to call. The Phone Indicator for the selected line  on the front of the VoloAccess will flash when the handset is off-hook.

If **Power-on PIN Lock** has been enabled, the dial tone will be different (an intermittent tone instead of the normal dial tone). On a voice enabled VoloAccess unlock the SIM using the telephone keypad by lifting the handset and entering **#NNNN#** (where NNNN is the SIM PIN) then replace the handset.

You can dial international numbers in two ways:

- dialing <International Prefix><Country Code><Phone Number> or,
- dialing +<Country Code><Phone Number> using '**' for '+'.

Admin

This section covers the administration of the VoloAccess. There are many configurable features; however, if your VoloAccess was purchased as a packaged unit including a configured SIM, it is not necessary to configure any settings to make your VoloAccess work.

APN (Access Point Name)

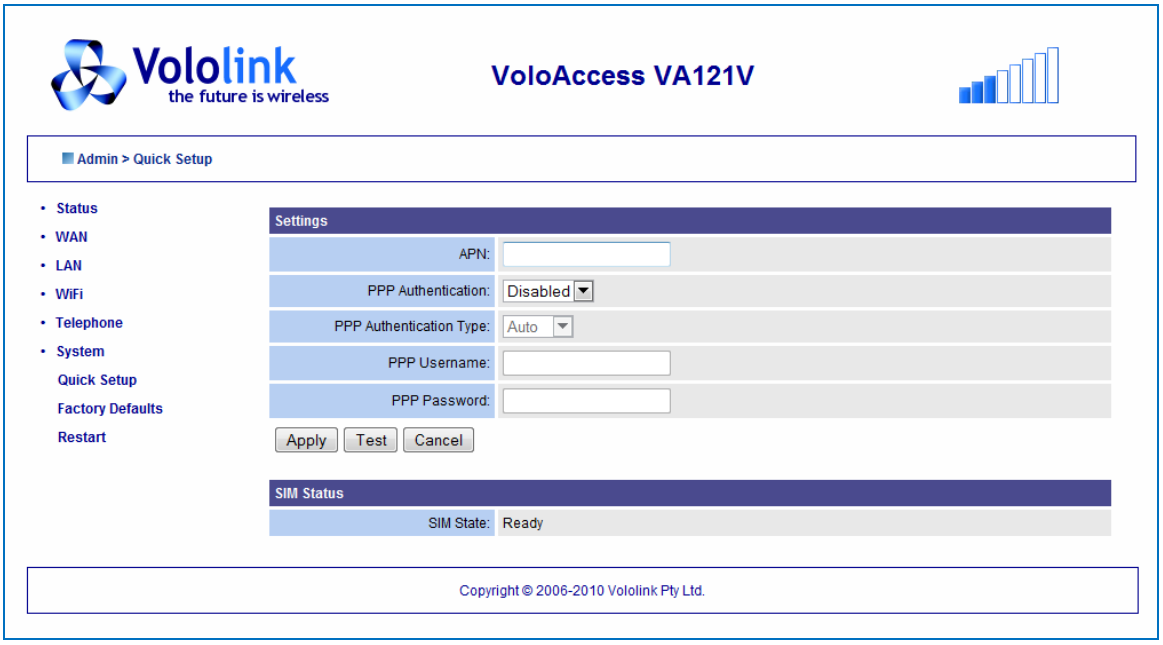
If your VoloAccess was purchased as a packaged unit including a configured SIM, you do not need to configure the APN (Access Point Name).

It is recommended that even if you have a pre-configured unit, you complete the next step and record the APN. This is to save time obtaining it from your service provider in the event it is lost due to a configuration error or a reset sometime in the future.

What is the APN? – The APN is the name of your 3G services provider's wireless access point.

To configure the APN for your 3G services provider, start by loading Admin as described above.

- From the Navigation panel on the left select **Quick Setup** - the **Quick Setup** page appears:



- Enter your 3G services provider's **APN** in the editbox provided.
- Click the **Apply** button.

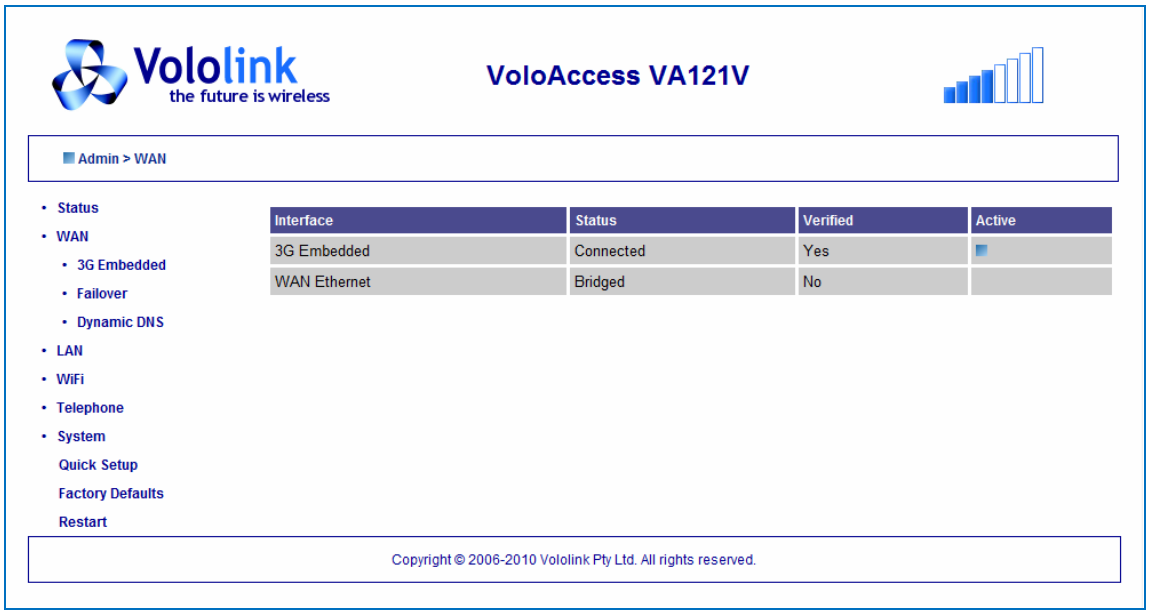
The Test Button

On many of the configuration pages a **Test** button is present. Use the Test button to test the functionality that you have just configured. When you are satisfied with the new configuration, click the **Apply** button. Clicking the **Apply** button saves any changed settings permanently in non-volatile memory.

The rest of this section covers items that you may wish to view or change.

WAN

The WAN (Wide Area Network) page displays the status of the 3G Embedded interface. The WAN Ethernet interface may be used if Failover is enabled. To view the WAN status click **WAN** in the Navigation panel - the WAN page appears:

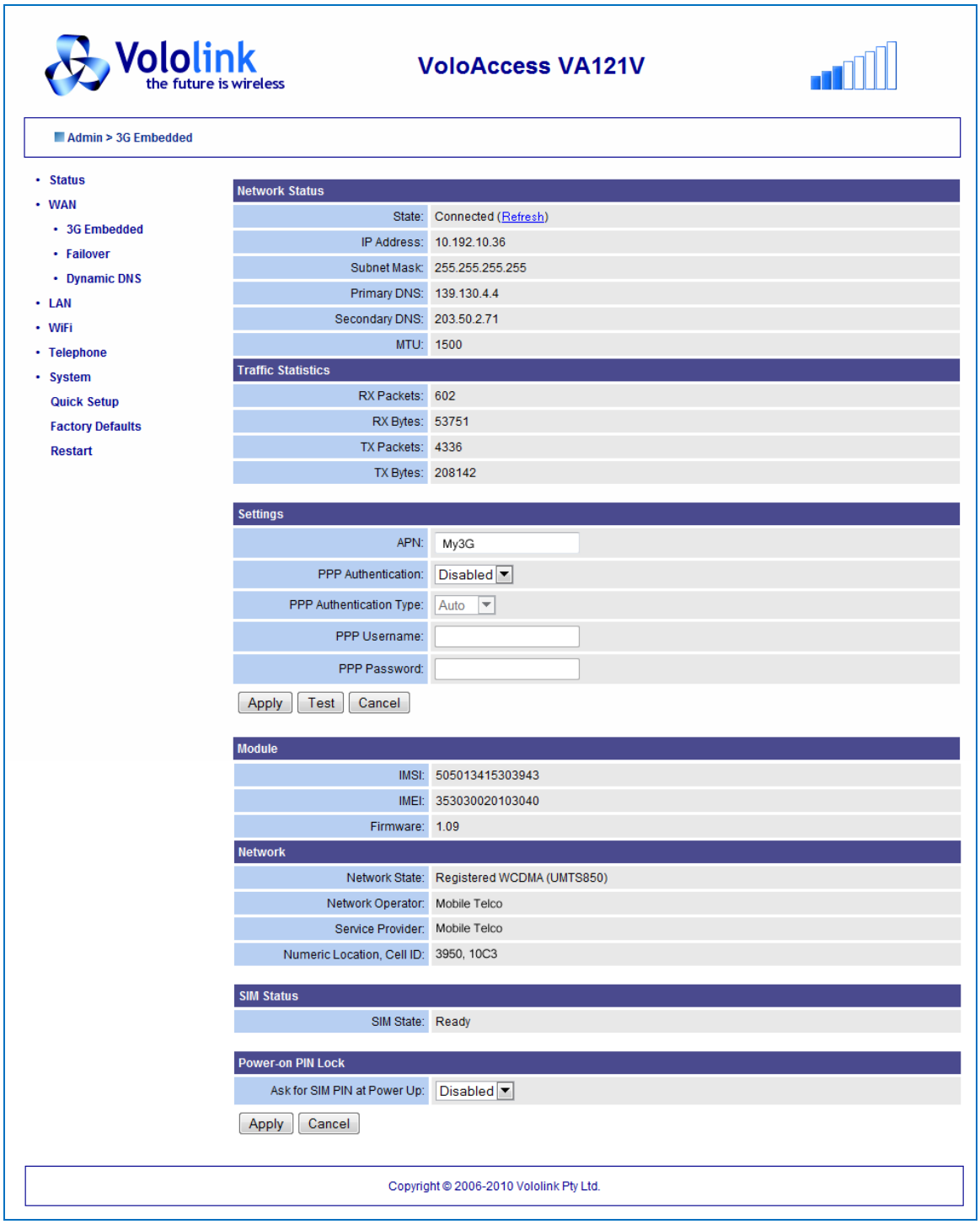


Following is a description of the items displayed.

- **Interface** The name of the Interface.
- **Status** Displays the current status of the interface.
- **Verified** Displays the Verified status.
- **Active** The active interface has a blue icon in this field.

3G Embedded

The 3G Embedded page displays information about the 3G Embedded WAN interface together with various settings. To view the page status click **WAN** then **3G Embedded** in the Navigation panel.



Following is a description of the information displayed together with the settings:

- **Network Status** Displays the 3G interface connection status as follows:

State	Connection Status – click 'Refresh' to update the display
IP Address	The IP address allocated to the VoloAccess
Subnet Mask	the network Subnet Mask
Primary DNS	IP address of the Primary Domain Name Server
Secondary DNS	IP address of the Secondary Domain Name Server
MTU	Maximum Transmission Unit - the size of the largest packet that a network protocol can transmit

- **Traffic Statistics** — The number of packets and bytes received (RX) and transmitted (TX).
- **Settings**
  - APN — Enter your 3G service provider's **APN** in the editbox provided then click the **Apply** button.
  - PPP Authentication — In most cases **P**oint-to-**P**oint **P**rotocol (PPP) authentication is not required by a 3G service provider.

    PPP is used to establish an authenticated connection between two host systems. The authentication is in the form of a Username and Password pair known to both hosts. The Authentication Type (protocol) also needs to be selected.

    PPP Authentication is configured as follows:

    - Click the drop-down list next to **PPP Authentication** and select **Enabled**.
    - Select the **Authentication Type** from the drop-down list. The options are:
      - **Auto** Automatically select the Authentication Type
      - **CHAP** **C**hallenge **H**andshake **A**uthentication **P**rotocol
      - **PAP** **P**assword **A**uthentication **P**rotocol
    - Enter the **PPP Username** in the editbox provided.
    - Enter the **PPP Password** in the editbox provided.
    - Click the **Apply** button.

    PPP authentication can also be configured on the Quick Setup page.
- **Module**
  - IMSI — **I**nternational **M**obile **S**ubscriber **I**dentity. The IMSI number is a unique 15-digit code that is attached to every SIM and makes it possible for mobile networks to identify the home country and network of a subscriber.
  - IMEI — The **I**nternational **M**obile **E**quipment **I**dentity number. A number unique to every GSM and UMTS mobile device, in this case, your VoloAccess. The IMEI number is used identify the device only, it is not related to the SIM or the subscriber.
  - Firmware — The firmware version of the wireless module.
- **Network**
  - Network State — The type of cellular network that the VoloAccess is logged on to.
  - Network Operator — The name of the network operator that the VoloAccess is connected to.
  - Service Provider — The name of the service provider that the VoloAccess is connected to.
  - Numeric Location, Cell ID — The Location Area Code and the Cell ID that the VoloAccess is connected to. These values are displayed in hexadecimal notation.
- **SIM Status**
  - SIM State — The state of the SIM installed in the VoloAccess.

Use this page is to manage the function of the PIN. From this page you can:

- Enable/Disable Power-on PIN Lock
- Change the PIN

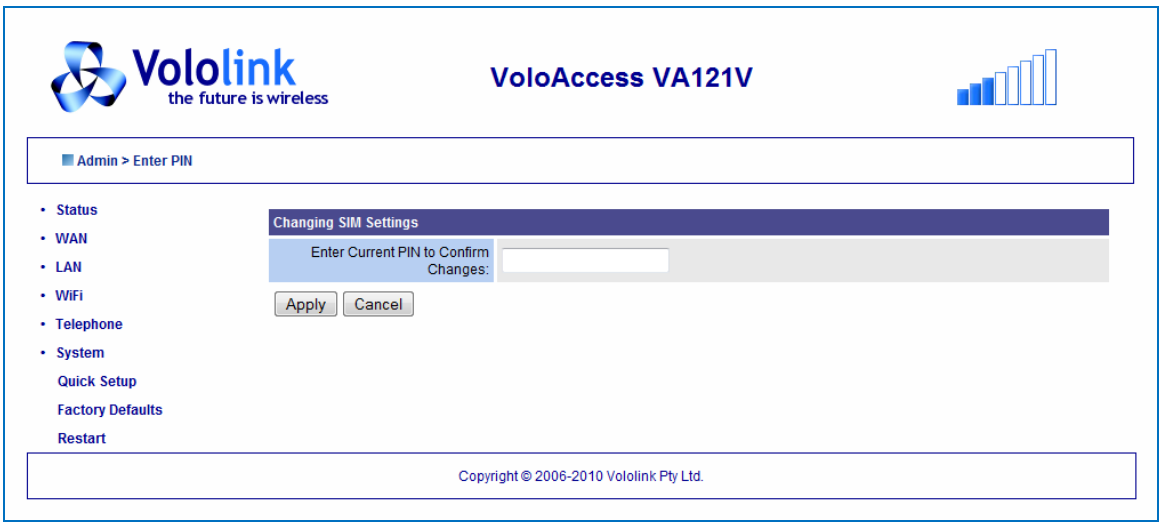
If **Power-on PIN Lock** is disabled, **Change PIN** is not available.

Power-on PIN Lock

Power-on PIN Lock requires the SIM PIN to be entered at power up. It is configured as follows:

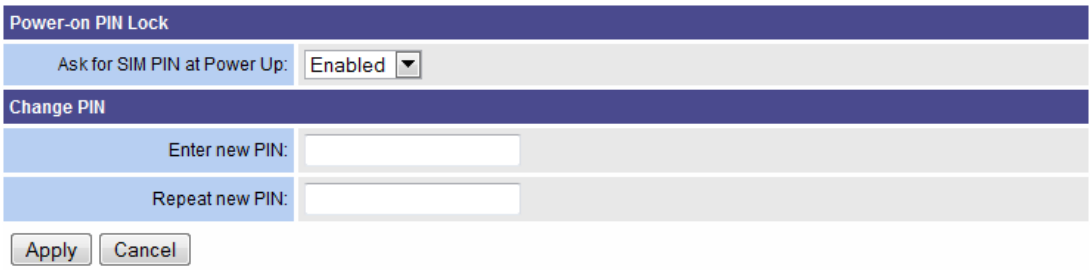
- Click the drop-down list next to **Ask for SIM PIN at Power Up** and select **Enabled** then click the **Apply** button.

  You are prompted to enter the **Current PIN** as confirmation:



- Enter the current PIN in the editbox provided and click the **Apply** button

  The page changes to reflect the **Enabled** state and provide the **Change PIN** facility as follows:



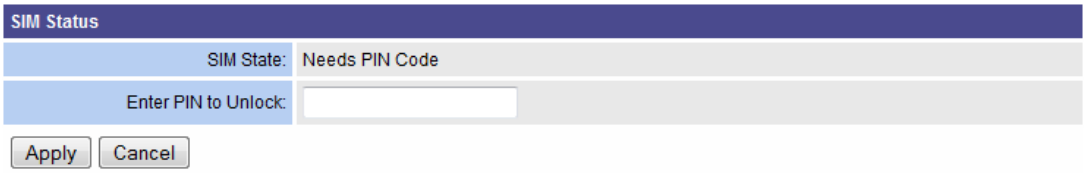
When Power-on PIN Lock is enabled, all services except emergency calls (voice enabled models only) are not available until the SIM is unlocked.

To unlock the SIM using the telephone keypad on a voice enabled VoloAccess:

- Lift the handset and enter **#NNNN#** (where NNNN is the SIM PIN), then
- Replace the handset.

To unlock the SIM using **Admin**:

- Select **Status** from the navigation panel.
- Enter the **SIM PIN** in the editbox provided.



- Click the **Apply** button.

The **Enter PIN to Unlock** field only appears if **Power-on PIN Lock** is enabled.

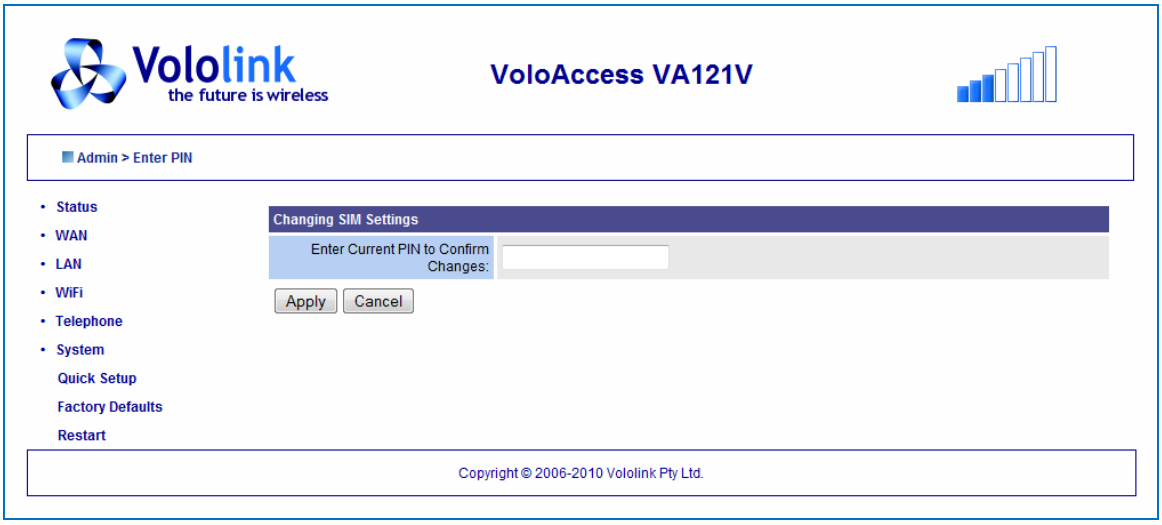
The SIM PIN can also be entered in the **3G Embedded** or **Quick Setup** pages.

Change PIN

To change the PIN:

- Enter the new **PIN** in the editbox provided.
- Re-enter the new PIN in the **Repeat new PIN** editbox.
- Click the **Apply** button to make the change.

You are prompted to enter the current (old) PIN as confirmation.

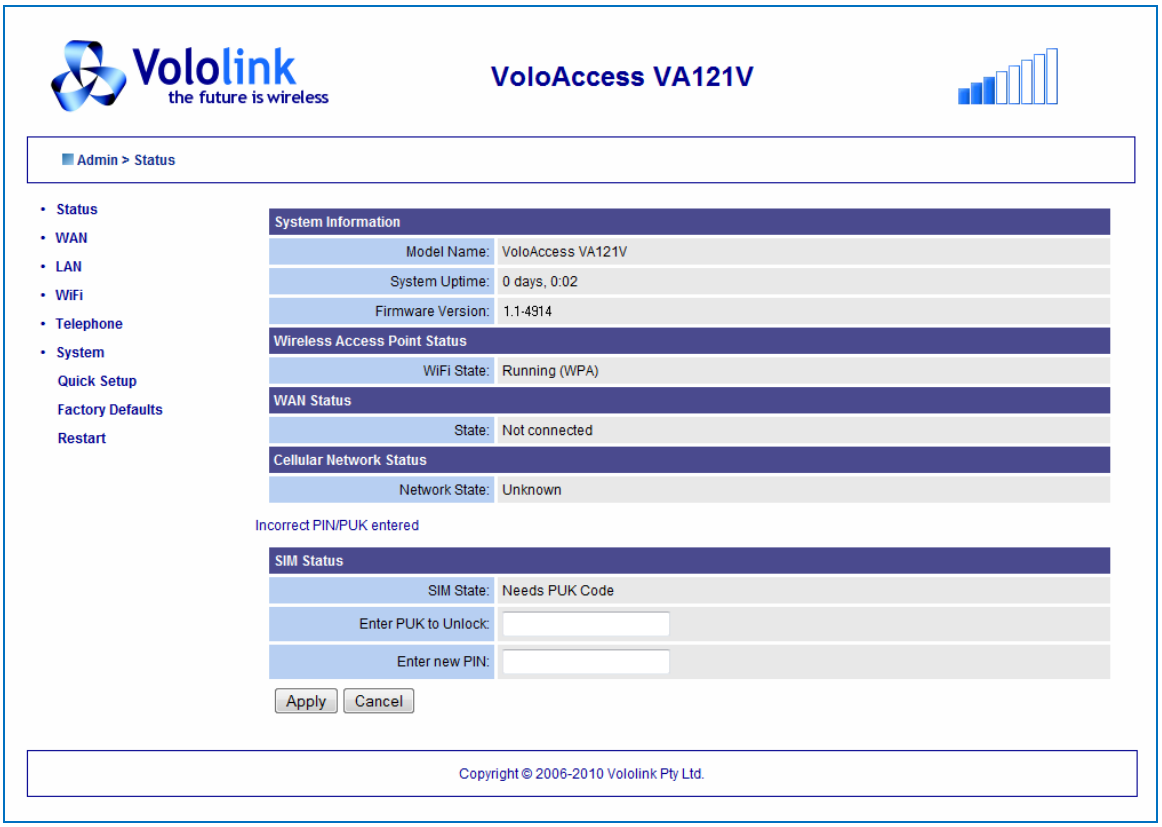


- Enter the current (old) PIN in the editbox provided and click the **Apply** button.

  The PIN is now changed.

PUK

If the PIN is entered incorrectly three times, the SIM is locked and the following page is displayed. It is necessary to contact your service provider to obtain the PUK (Personal Unlocking Key) for your SIM.



To unlock the SIM:

- Enter the **PUK** in the editbox provided.
- Enter a new **PIN** in the editbox provided.
- Click the **Apply** button.

After about 5 - 10 seconds

- The Mobile Network Connection indicator on the VoloAccess turns **ON**.
- On the Admin Status page, the **WAN Status**, **State** changes from **Not Connected** to **Connected**.

Failover

Failover is the capability to switch automatically to a secondary network when the primary network fails.

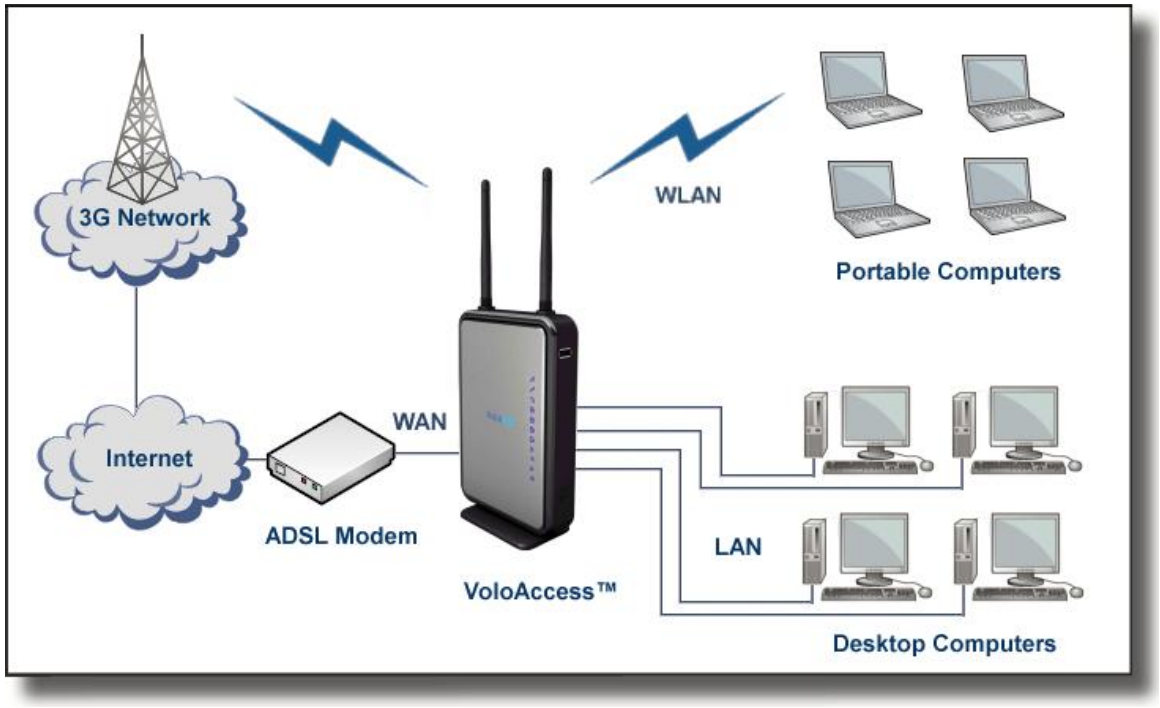
By default Failover is disabled. Once enabled, the VoloAccess supports failover between multiple WAN interfaces. Automatic failover provides enhanced availability and reliability.

WAN failover takes place when a WAN device fails due to disconnection, for example, the 3G network goes offline. If the primary WAN interface fails, the VoloAccess redirects network traffic through the secondary WAN interface until the primary WAN interface becomes available and its connectivity is verified.

By default, the WAN Ethernet is established as the primary interface together with the embedded 3G wireless module as the secondary interface.

The preference (primary or secondary) of the WAN interfaces is configurable. Factors that may contribute to the selection of the primary interface are items like cost, reliability and speed.

The following diagram shows the VoloAccess utilizing both a 3G wireless broadband connection and a wired connection (ADSL modem) to implement automatic failover.



The connectivity of the WAN interfaces is verified by regular monitoring of reliable hosts. When a DNS lookup of a reliable host via an interface fails, the VoloAccess marks that interface as failed and automatically activates an alternate interface.

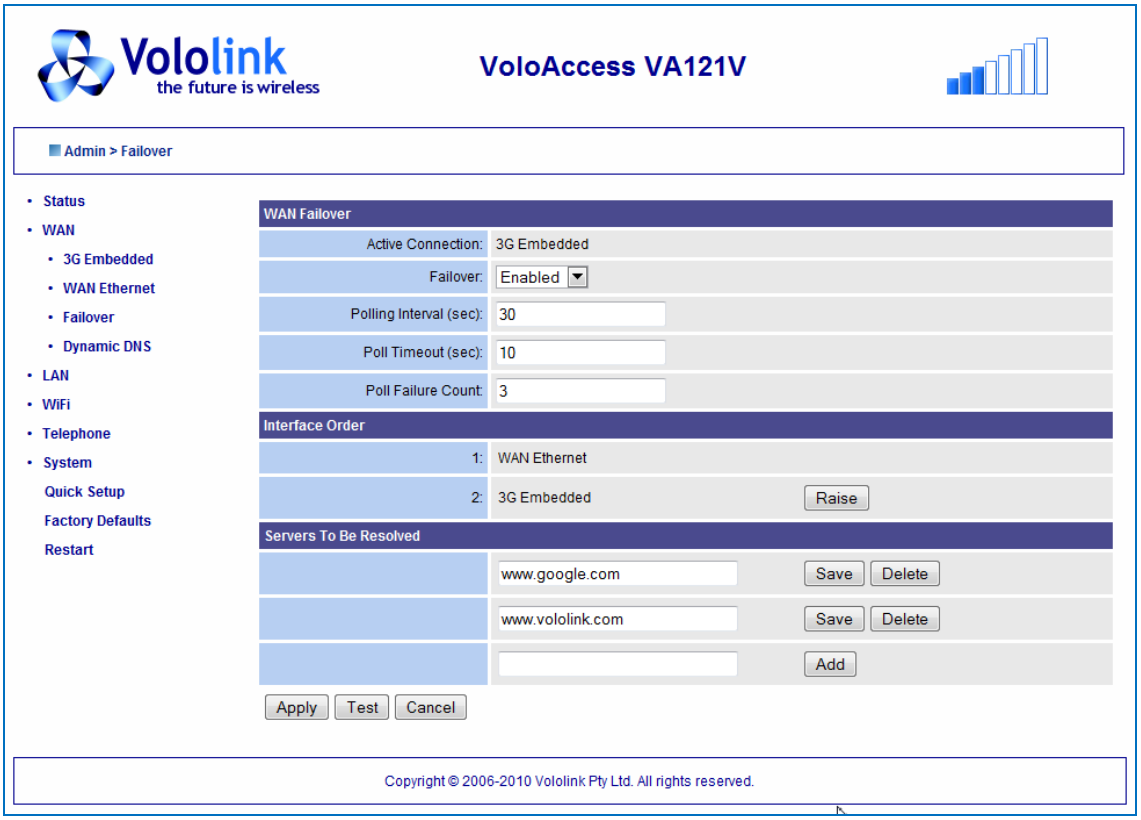
Setting up Failover

Following is an example of setting up a wired modem as the secondary WAN interface.

Do not connect a WAN Ethernet cable until Failover has been enabled and configured.

To access the WAN Failover page select **WAN** then **Failover** in the navigation panel – the Failover page appears.

- Select **Enabled** from the drop-down list box and click the **Apply** button.



After enabling Failover and selecting the interface order, it is necessary to enable the WAN port before connecting the VoloAccess to a secondary WAN interface.

The following items can be configured if necessary.

- **Polling Interval** — The length of time (in seconds) between DNS resolution attempts. The polling requests are the regular monitoring of the WAN interfaces.

  A short interval between DNS polling provides fast detection of connection failure, but results in increased data usage. The range of values is: Min: 5 seconds to Max: 1 day.

- **Poll Timeout** — The number of seconds to wait for a DNS reply. It may be necessary to increase this value for slow links in order to provide sufficient time to receive a reply. The range of values is: Min: 1 second to Max: 3 minutes.

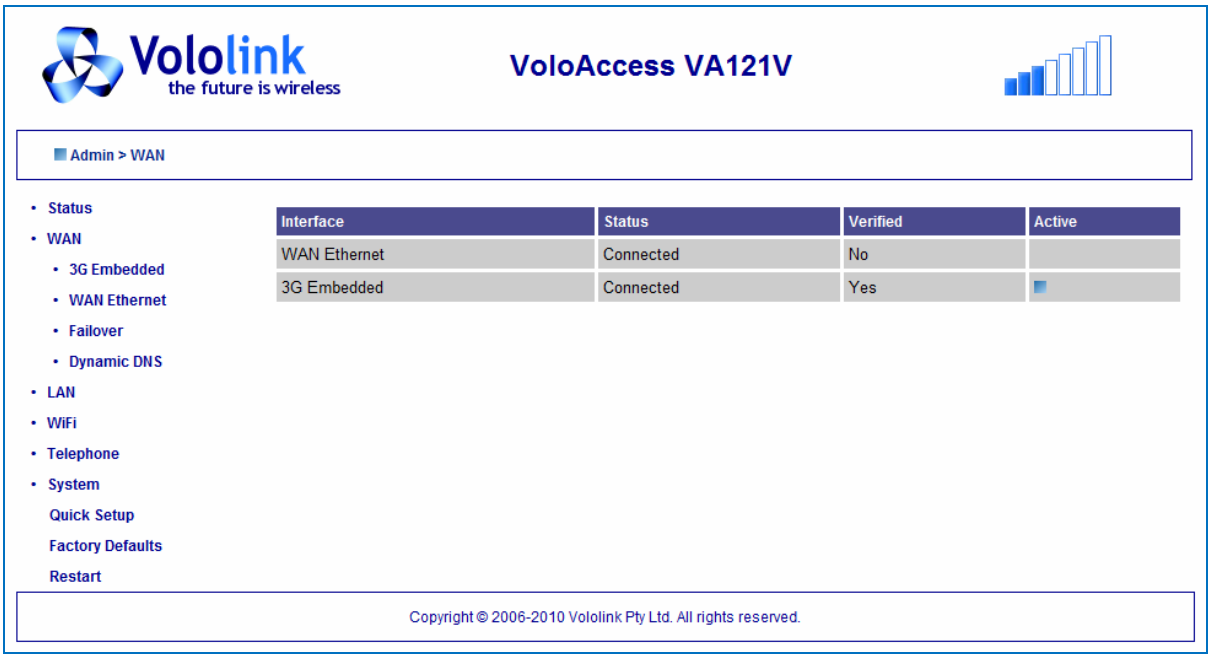
- **Poll Failure Count** — The number of successive DNS resolution failures before the interface is considered to have failed. Once the specified number of failures has been reached, the next available interface will become the active interface. The range of values is: Min: 1 to Max: 100

- **Interface Order** — Defines the preferred order of interface usage. The primary interface is used in preference to the secondary interface until it fails at which time the VoloAccess will switch to the next interface. To change the interface order, click the **Raise** button.

- **Servers To Be Resolved** — The list of host names to resolve. The default hosts can be replaced or deleted. Additional host names can also be defined. Use the **Save**, **Delete** and **Add** buttons to manage these items. At least one host must be defined.

After making changes to this page click the **Apply** button.

After enabling Failover, the WAN page changes to reflect the status of the primary and secondary WAN interfaces and the WAN section of the navigation panel expands to include **WAN Ethernet** as shown in the following image.



The WAN page displays the following:

- **Interface** The name of the Interface
- **Status** Displays the current status of the interface. Additional information may be displayed, depending on the interface type. A connected interface has the status "Connected". Other status messages will depend on the type of interface. For example a 3G interface may have a status of:

  "Connected"

  "Not connected, network not online"

  "Not connected"

  A WAN interface may have a status of:

  "Connected"

  "Bridged"

  "Disabled"

  "Connecting"

  By default, the WAN port is Bridged – see Enable WAN Ethernet Port for further information.

  Other status messages may also be displayed.
- **Verified** Indicates whether the interface has passed the DNS resolution test.
- **Active** The active interface is marked with a blue icon.

WAN Failover is not yet fully configured – continue as follows:

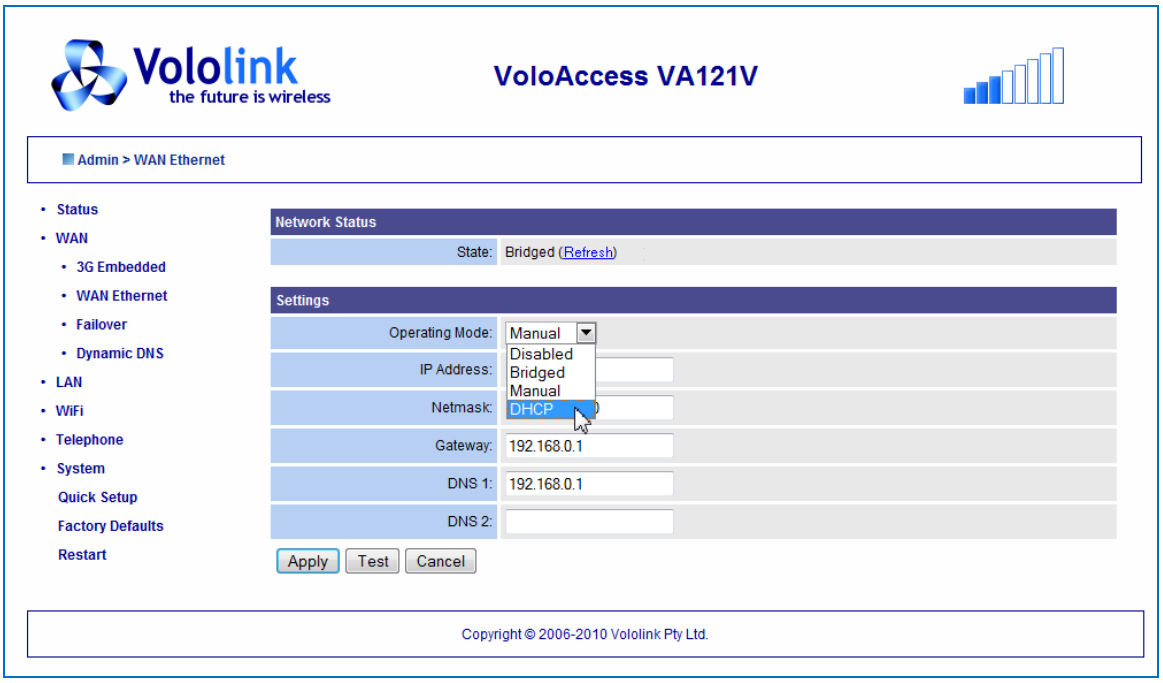
Enable WAN Ethernet Port

The WAN Ethernet port can be configured manually or, by selecting DHCP to automatically obtain an IP address from an external WAN modem/router. Selecting DHCP should be suitable for most users. If Manual is selected, it is necessary to enter the following information:

- **IP Address** **IP Address** for the VoloAccess to use on the external Ethernet WAN
- **Netmask** **Netmask** of the external Ethernet WAN
- **Gateway** IP address of the external Ethernet WAN **Gateway**
- **DNS 1** IP address of the external Ethernet WAN Primary **DNS** server
- **DNS 2** IP address of the external Ethernet WAN Secondary **DNS** server

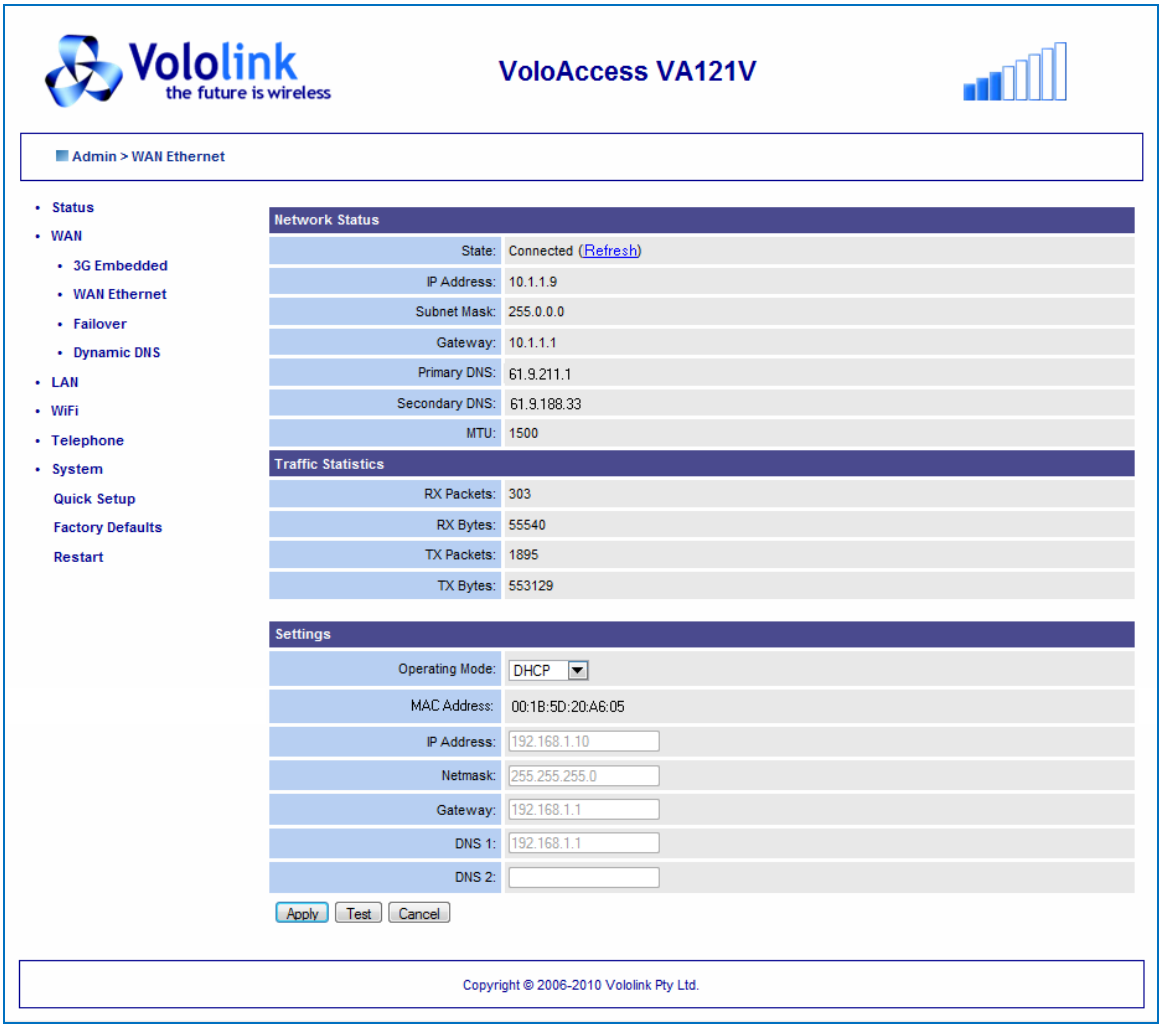
The above information can be obtained by accessing the configuration page(s) of the external WAN modem/router. Refer to the modem/router documentation for further information.

- Configure the WAN Ethernet port to obtain an IP address automatically as follows:
- In the navigation panel select **WAN Ethernet** – the WAN Ethernet page appears.



- Use the drop-down list box to select **DHCP**.
- Click the **Apply** button. The WAN Ethernet port is now enabled and configured.
- Connect the WAN port of the VoloAccess to a modem using an Ethernet cable.
- Wait for 10 seconds then click Refresh - the page reloads with DHCP enabled and expands to include further Network information together with Traffic Statistics as follows:

It may be necessary to repeat the Refresh several times before the updated information appears.

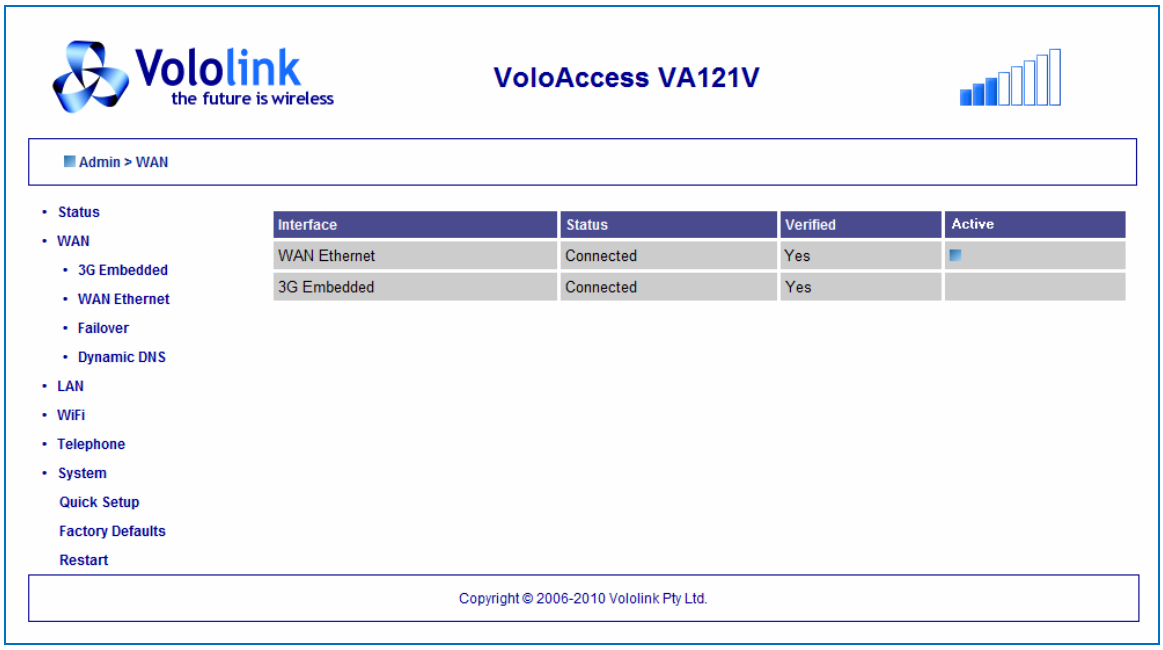


The WAN Ethernet page displays the following information:

- **Network Status** Displays the following:
  - WAN Ethernet interface connection status
  - the **IP Address** allocated to the VoloAccess on the Ethernet WAN
  - the **Subnet Mask**
  - IP address of the WAN Ethernet **Gateway**
  - IP addresses of the **Domain Name Servers** (Primary and Secondary)
  - **MTU** (Maximum Transmission Unit).
- **Traffic Statistics** The number of packets and bytes received (RX) and transmitted (TX).
- **Settings** The Operating Mode of DHCP should be suitable for most users, however these items can be configured if necessary. To configure these settings, select **Manual** as the Operating Mode.
  - **Operating Mode** From the drop-down list box select the **Operating Mode**.
    The options are:
    - **Disabled** – The Ethernet interface is disabled
    - **Bridged** – The WAN Ethernet port is bridged and operates as a LAN port. In this configuration, the VoloAccess is a 5 port switch
    - **Manual** – The Ethernet interface can be configured manually
    - **DHCP** – The Ethernet interface will be configured via DHCP
  - **MAC Address** The **MAC** address of the VoloAccess WAN Ethernet interface
  - **IP Address** The **IP Address** for the VoloAccess to use on the Ethernet WAN
  - **Netmask** The **Netmask** of the Ethernet WAN

- **Gateway** The IP address of the WAN Ethernet **Gateway**
- **DNS 1** The IP address of the WAN Ethernet Primary **DNS** server
- **DNS 2** The IP address of the WAN Ethernet Secondary **DNS** server

Review the implementation of Failover by returning to the WAN page – in the navigation panel select **WAN**.



Observe the Connection and Verification status of the WAN interfaces. When all interfaces are fully operational, they are shown as being Connected and Verified with the primary interface Active.

Dynamic DNS

To a user, domain names like vololink.com make perfect sense, but not to a computer. Computers work with numbers in the form of IP addresses like 124.177.145.95 to communicate with each other on the Internet.

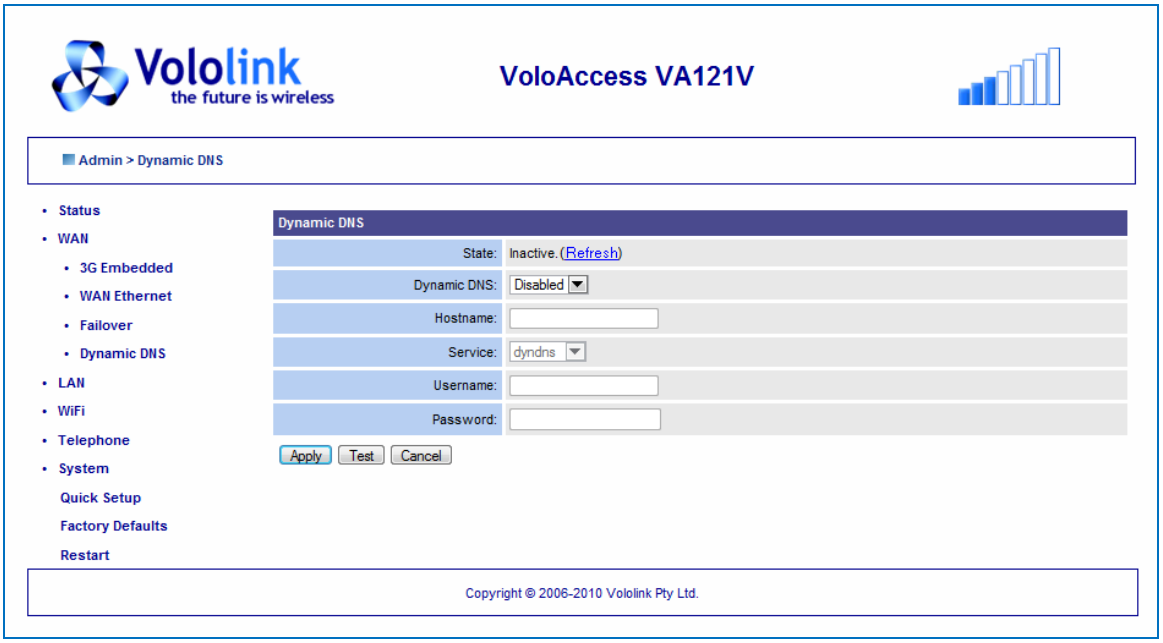
DNS translates domain names into IP addresses (and the other way around) making it possible for computers to communicate; however dynamically assigned IP addresses change.

Dynamic DNS (Domain Name System) works by reassigning IP addresses to domain names. Dynamic DNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes.

Admin allows you to configure Dynamic DNS using a third-party provider.

It is necessary to register with a Dynamic DNS provider before configuring the VoloAccess to use Dynamic DNS.

To access the Dynamic DNS page select **Dynamic DNS** in the navigation panel – the Dynamic DNS page appears.

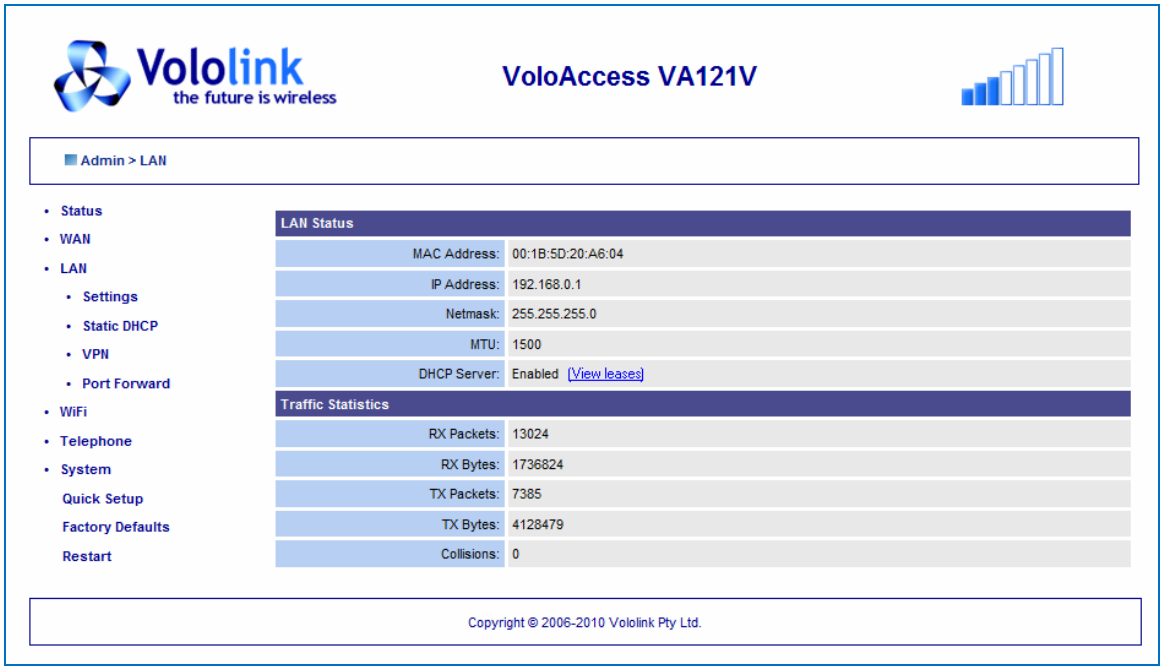


Dynamic DNS is configured as follows:

- Select **Enabled** from the drop-down list next to Dynamic DNS.
- Enter the **Hostname** supplied by the Dynamic DNS provider in the editbox provided.
- Select the **Dynamic DNS** service provider from the drop-down list next to Service.
- Enter the **Username** supplied by the Dynamic DNS provider in the editbox provided.
- Enter the **Password** supplied by the Dynamic DNS provider in the editbox provided.
- Click the **Apply** button.

LAN

The LAN (Local Area Network) page displays the LAN status and traffic statistics. To view the LAN page click **LAN** in the Navigation panel - the LAN page appears:



LAN Status displays the following:

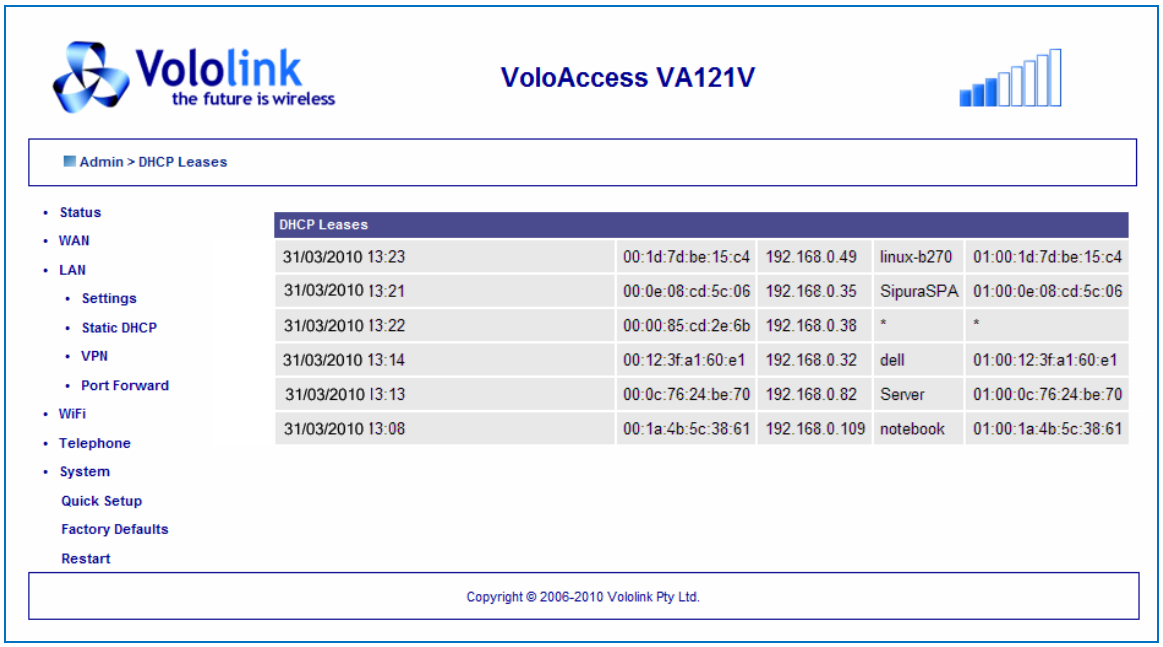
- MAC Address — The **MAC** (**M**edia **A**ccess **C**ontrol) address of the VoloAccess.
- IP Address and Netmask — The **IP** (**I**nternet **P**rotocol) Address and **Netmask** of the VoloAccess.
- MTU — **MTU** (**M**aximum **T**ransmission **U**nit - the size of the largest packet that a network protocol can transmit).
- DHCP Server — The status of the **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol) Server in the VoloAccess with an option to **View leases**. (see below).

Traffic Statistics displays the following:

- RX Packets and Bytes — The number of data packets and bytes received.
- TX Packets and Bytes — The number of data packets and bytes transmitted.
- Collisions — The number of collisions on the network.

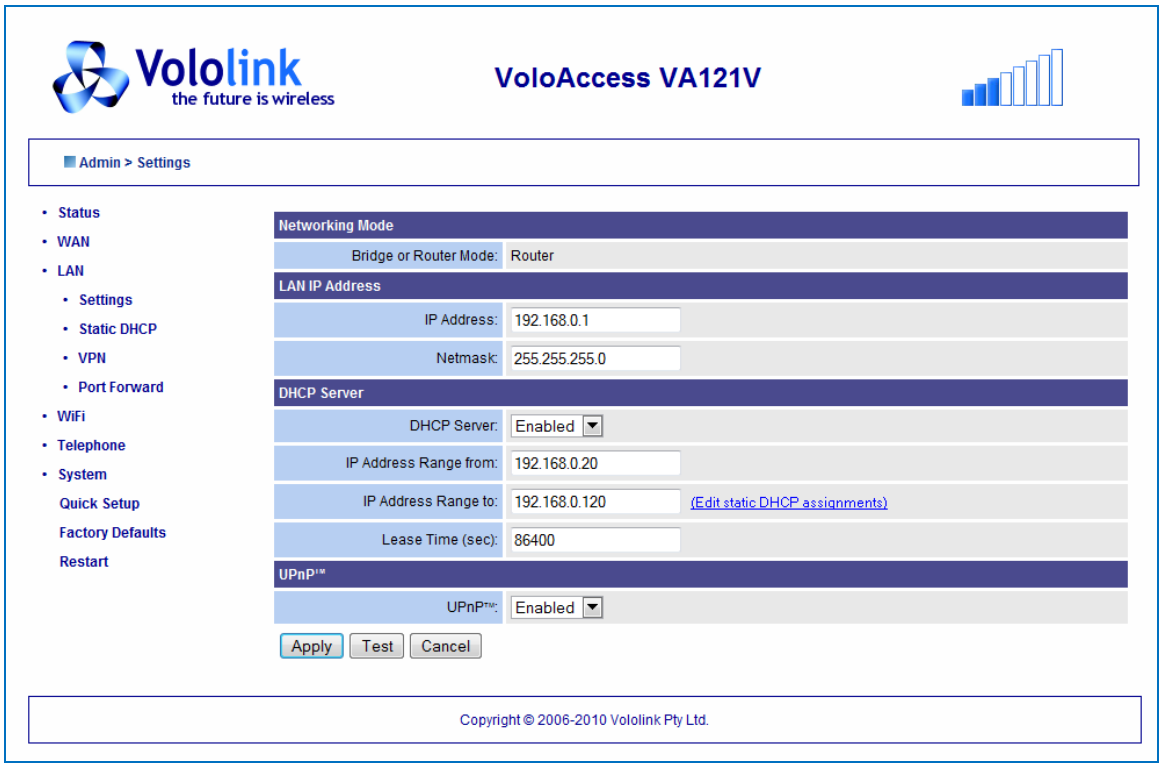
View Leases

To view the leases assigned by the DHCP server, click **View leases** – The current DHCP leases are displayed.



Settings

To view or edit the LAN Settings select **LAN** followed by **Settings** in the Navigation panel - the LAN Settings page appears:



Most users will not need to change anything on this page. However, if necessary, you can define the **IP Address** and **Netmask** of the VoloAccess as well as Enable or Disable the **DHCP Server** together with the **IP Range** (assigned by the DHCP Server) and the **Lease Time** of the IP Address.

The VoloAccess incorporates a DHCP server that assigns dynamic IP addresses to local clients (computers connected to the VoloAccess). The IP addresses are allocated from the predefined range of addresses defined on this page. The default address range is suitable for most local networks. The option to **Edit static DHCP assignments** is the same as selecting Static DHCP from the navigation panel.

The DHCP server allocates the IP address for the term of the Lease Time defined on this page. The lease is the amount of time that an IP address is valid for a specific device. If the lease expires and the device is still connected, the lease is automatically renewed.

UPnP™

UPnP (Universal Plug and Play) provides automatic port forwarding between certain Internet applications and your LAN. UPnP needs to be enabled to allow programs like MSN Messenger and most games to work through the VoloAccess firewall. The default setting for UPnP is Enabled.

To enable/disable this feature:

- Select **Enabled** or **Disabled** in the drop-down list next to **UPnP** on the **Settings** page.
- Click the **Apply** button – the **Settings** page reappears with **UPnP** reconfigured.

Static DHCP

Static DHCP configures the DHCP server on your VoloAccess to always assign the same (static) IP address to a specific network adapter installed in a computer on the LAN. Every network card has its own unique address - the MAC (Media Access Control) address that is used to identify it on the LAN. At boot time the computer requests its IP address from the VoloAccess DHCP server. The DHCP server recognises the MAC address of the computer's network card and assigns the static IP address to it.

Static DHCP is required if you want your computer to always have the same IP address. This is sometimes required by certain programs. Static DHCP should be used in conjunction with Port Forward. If you forward an external WAN TCP/UDP port to a port on a server running inside your LAN, you have to provide that server with a static IP address - this can be achieved using Static DHCP.

To assign static IP addresses to computers on your LAN select **Static DHCP** in the navigation panel – the Static DHCP window appears.

Enter the following data for each computer to be assigned a static DHCP address:

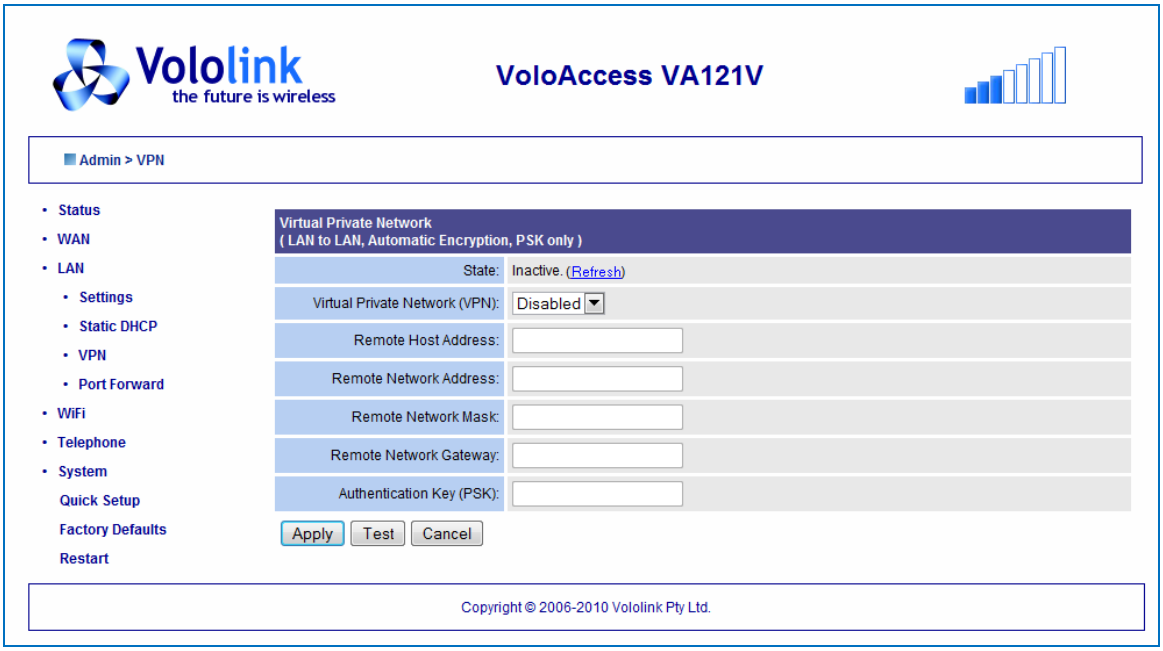
MAC Address	Enter the MAC address e.g. 00:1a:4b:5c:38:61
IP Address	Enter the IP address e.g. 192.168.0.150
Host Name	Enter a Host Name (optional) – recommended as it helps identify the computer. (It is in readable format rather than a number – see View leases.)

Click the **Add** button to complete assigning a static DHCP address.

VPN

The VoloAccess can be configured as a VPN (Virtual Private Network) Host. To do this, proceed as follows:

- Select **LAN** followed by **VPN** in the Navigation panel - the VPN Page appears:
- Select **Enabled** from the drop-down list and proceed to configure VPN.
- Click the **Apply** button



You will need to obtain the following information from the administrator of the remote server:

- Remote Host Address
- Remote Network Address
- Remote Network Mask
- Remote Network Gateway
- Authentication Key – A Pre-Shared Key (PSK)

The VPN is implemented using IPsec in Network-to-Network mode. This means that the VoloAccess is a VPN router providing connectivity between two LANs.

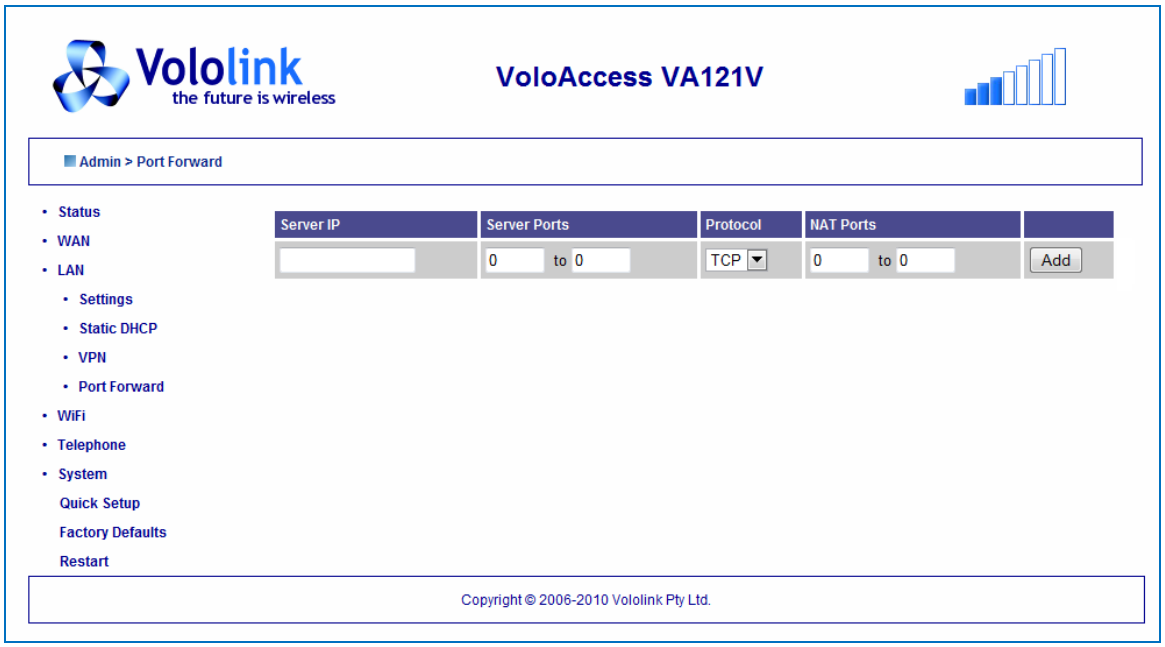
Currently, the supported settings are authentication via pre-shared key using SHA1, with 3DES encryption. The Diffie-Hellman group is modp1024.

Port Forward

Port forward is used to allow an external user to reach a port on a private IP address (inside a LAN) from the outside via a NAT-enabled router (VoloAccess).

When a computer on the Internet sends data to the public IP address of the VoloAccess, it needs to know how to manage the data. Port Forward tells the VoloAccess which computer on the local area network to send the data to.

To configure Port Forward select **LAN** followed by **Port Forward** in the Navigation panel - the Port Forward page is displayed:



Enter the **Server IP** address and **Server Port(s)**, select the **Protocol** from the drop-down list, and enter the **NAT Port(s)** then click the **Add** button.

Example

In this example, port forward is used to allow incoming access to an internal web server.

Configuration Item	Explanation
Server IP: 192.168.0.100	The IP address of the server on the internal network where the port will be forwarded.
Server Port: 8080 to 8081	The port numbers on the internal server.*
Protocol: TCP	The protocol to be forwarded.
NAT Port: 80 to 81	The port numbers on the VoloAccess to be forwarded.*

* To define a single port, enter the same value for both. For example, to define a single Server Port enter **8080** to **8080**.

WiFi

Your WiFi VoloAccess enables you to connect your computer wirelessly to the Internet as shown in the following diagram.

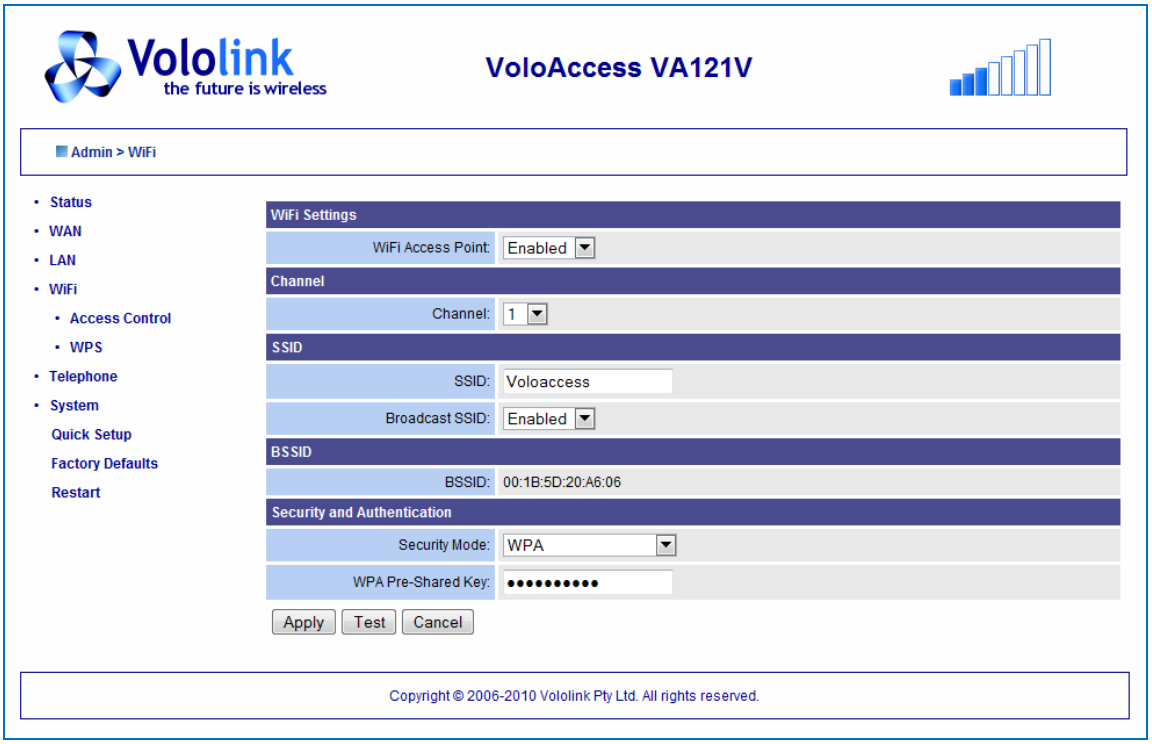
WiFi is also referred to as WLAN.

By default WiFi is Disabled. To set up a wireless network it is necessary to configure both the VoloAccess and the computer (or computers) that will be connecting wirelessly.

Configuring WiFi

WiFi on the VoloAccess is configured as follows:

- Select **WiFi** from the navigation panel – the WiFi page appears.
- Use the drop-down list next to **WiFi Access Point** and select **Enabled**.



Configure each of the following taking into account network security and performance.

Channel The VoloAccess WiFi network operates in the 2.4GHz frequency range. The operation of your WiFi network may be affected by other devices, such as cordless phones. If you experience any interference or slow connection, try selecting another channel.

SSID This is the **S**ervice **S**et **I**dentifier, or Network Name of your WiFi network. The VoloAccess broadcasts this information regularly. This feature allows clients to dynamically discover and roam between WiFi networks.

Enter a name for your WiFi network in the editbox.

BSSID The **B**asic **S**ervice **S**et **I**dentifier - the BSSID is the MAC address of a wireless access point, in this case the VoloAccess.

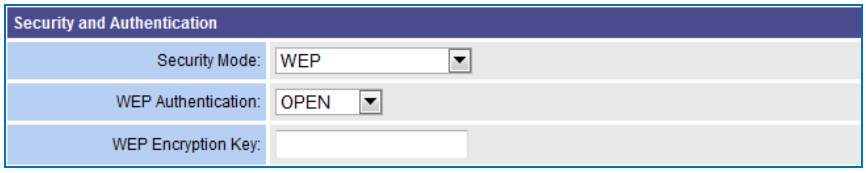
Broadcast SSID The default setting is Enabled. This allows clients to discover and connect to the VoloAccess.

Security and Authentication By default the **Security Mode** is set to **None** making it an open system. This is the least secure of all settings and is not recommended.

There are three settings available for Security Mode – they are:

WEP Wired Equivalent Privacy is a protocol used to secure WiFi networks.

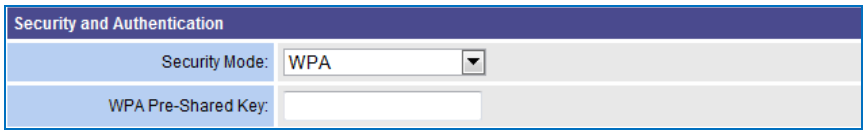
To configure WEP as the Security Mode, select **WEP** from the drop-down list – the page reloads automatically and displays the WEP Authentication and WEP Encryption Key edit boxes.



Select the **WEP Authentication** method from the drop-down list, then enter a **WEP Encryption Key** (must be **exactly 5** or **exactly 13** ASCII characters) in the editbox provided, and click the **Apply** button.

WPA WiFi Protected Access is a protocol used to secure WiFi networks.

To configure WPA as the Security Mode, select **WPA** from the drop-down list – the page reloads automatically and displays the WPA Pre-Shared Key editbox.



Enter a **WPA Pre-Shared Key** (8-63 ASCII characters) in the editbox provided and click the **Apply** button.

WPA2 WiFi Protected Access version 2 is a more secure version of the WPA protocol. This protocol may not work with some older network cards.

To configure WPA2 as the Security Mode, select **WPA2** from the drop-down list – the page reloads automatically and displays the WPA Pre-Shared Key editbox.

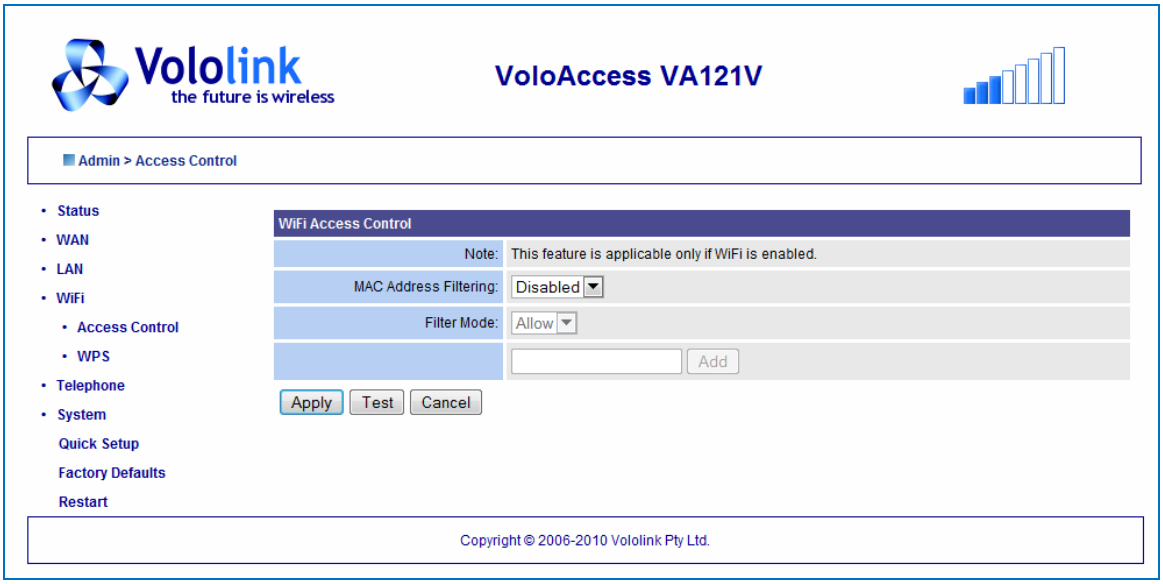
Enter a **WPA Pre-Shared Key** (8-63 ASCII characters long) in the editbox provided and click the **Apply** button.

WiFi Access Control

MAC address filtering is provided to allow you to restrict access to your WiFi network to specific computers. The MAC address is a unique address applied to a network adapter.

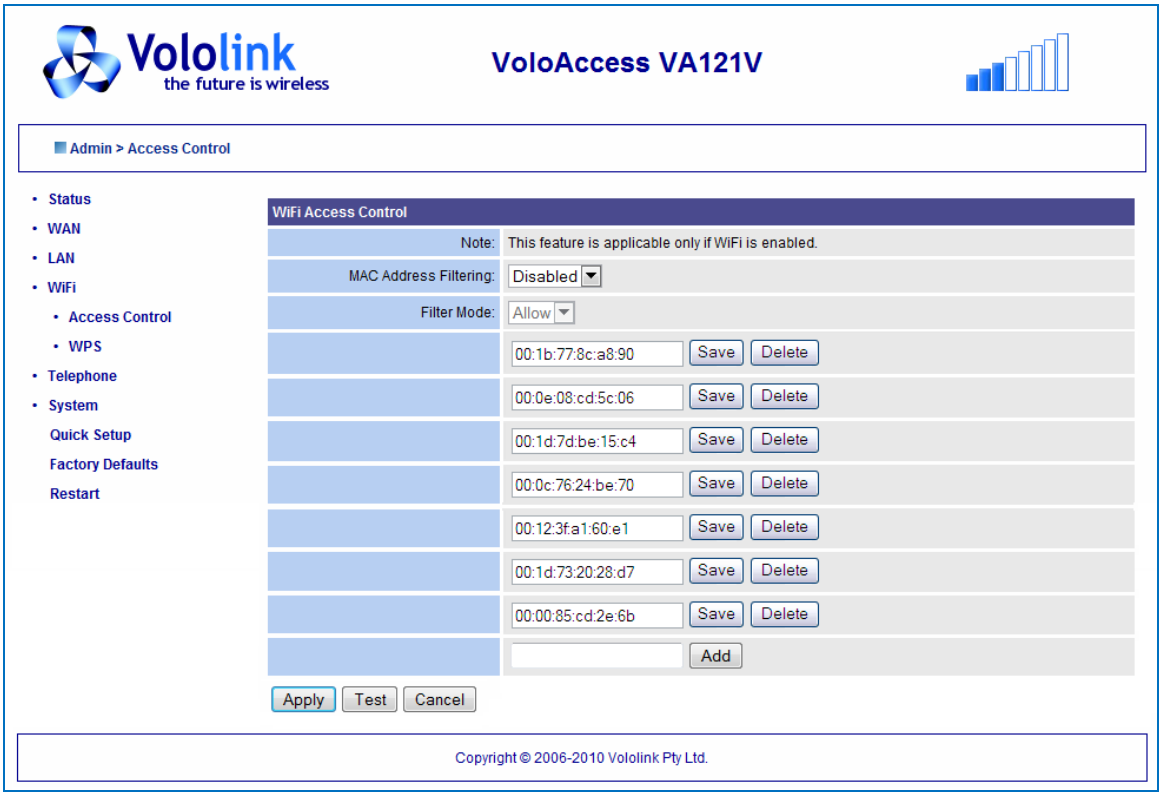
Access Control is configured as follows:

Select **WiFi** then **Access Control** in the navigation panel – the Access Control page appears.



- From the drop-down list next to **MAC Address Filtering** select **Enabled**.
- From the drop-down list next to **Filter Mode** select **Allow** or **Deny**. You can choose to allow or deny all specified clients, that is, all allowed or all denied access.
- Enter the MAC address of the client in the format **nn:nn:nn:nn:nn:nn** and click the **Add** button.
- Continue adding MAC addresses and when complete, click the **Apply** button.

Following is an example of a WiFi Access Control configuration:

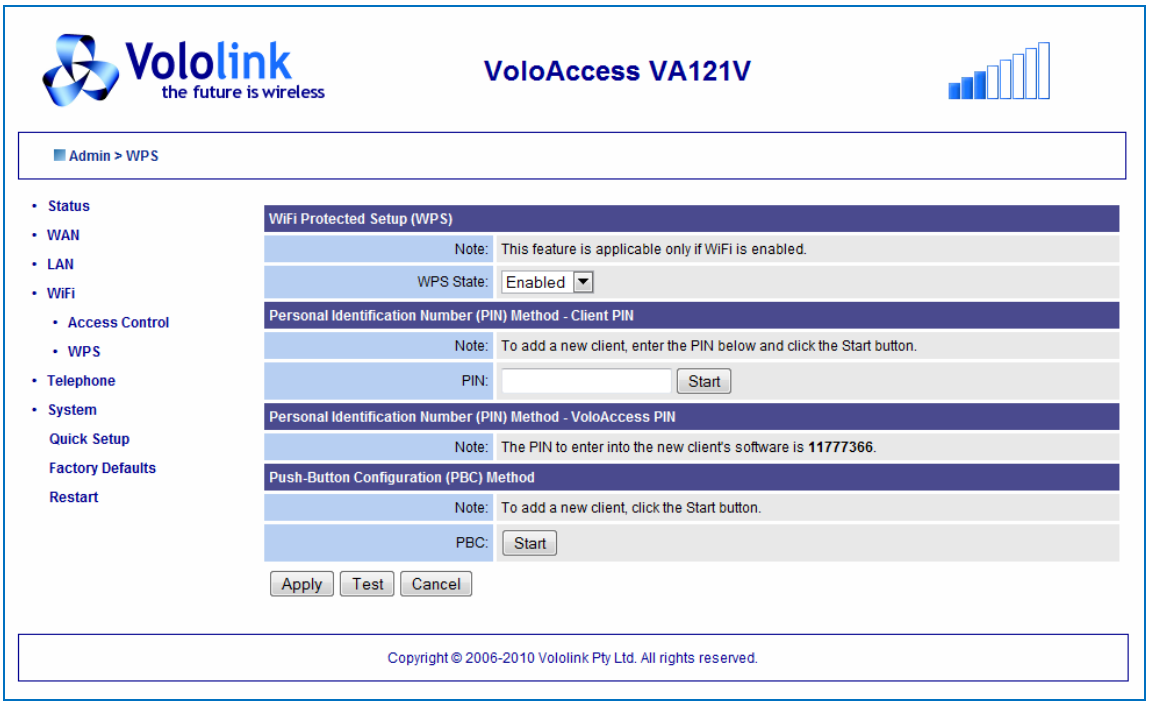


- To modify an entry, edit the MAC address then click the **Save** button next to it.
- To delete an entry, click the **Delete** button next to it.

WPS (WiFi Protected Setup)

If your wireless clients (computers with WiFi devices installed) support WiFi Protected Setup (WPS), you can use this feature to connect the wireless client securely and easily to the VoloAccess.

To access the WPS page select **WiFi** then **WPS** from the navigation panel – the WPS page is displayed.



To use WPS to connect wireless clients to the VoloAccess it is necessary to configure WiFi as described in the Configuring WiFi section of this manual, then continue as follows:

It is recommended that you read the user manual that came with the WPS-capable WiFi device prior to proceeding.

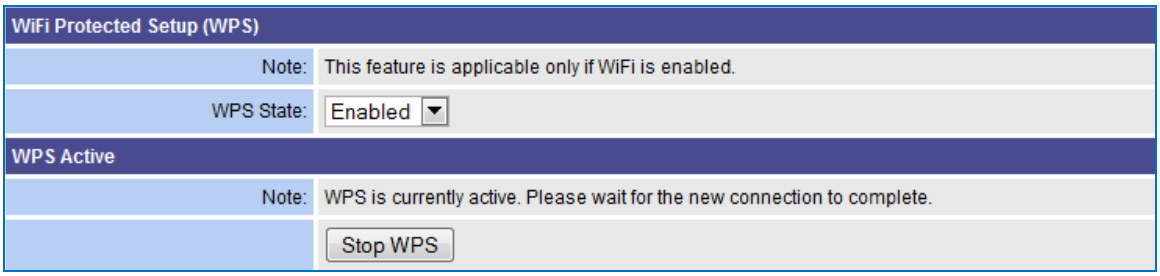
WPS supports two methods of connection; the PIN method and the Push Button Configuration (PBC) method.

It is recommended that the WPS feature only be used with WPA or WPA2 security implemented.

PIN Method

- On the client computer, run the Setup program supplied with the WPS-capable device. This usually involves inserting the supplied CD into the computer's DVD/CD drive and allowing it to run automatically. If this is not the case, refer to the user manual supplied with the WPS-capable device on how to install the software.
- The Setup program should take you through the steps required to connect to a WPS-capable Access Point, in this case, the VoloAccess.
- If an option for PIN or PBC method of connection is offered, select PIN.
- Continue by following the steps offered by the Setup program.
- The PIN method has two forms; the first is where the PIN is provided by the WPS-capable WiFi device (Client PIN), the second is where the PIN is provided by the Access Point (VoloAccess PIN).
  - For the Client PIN method; when prompted, enter the PIN provided by the Setup program in the **Client PIN** editbox of the WPS page of Admin. Wait until prompted by the Setup program, then click the **Start** button in the WPS page of Admin.
  - For the Access Point method; when prompted, enter the PIN, displayed on the WPS page under VoloAccess PIN, into the new client's Setup program.

- During negotiation the WPS page changes to reflect the **WPS Active** state and the WPS indicator on the VoloAccess flashes.

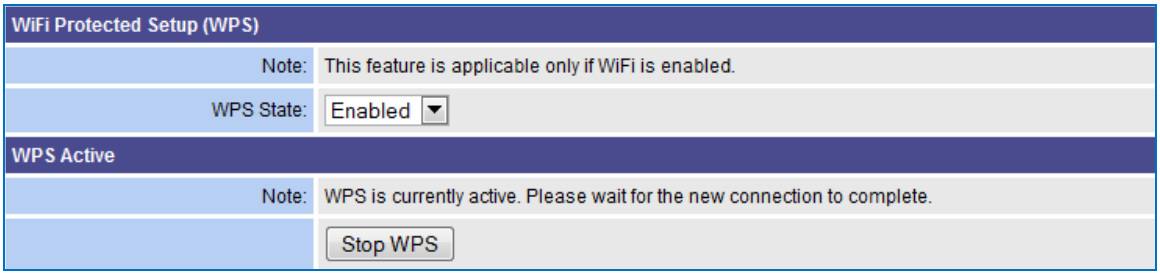


- After WPS negotiation has completed, verify the connection by selecting **LAN** > **View Leases** in Admin.

PBC Method

- On the client computer, run the Setup program supplied with the WPS-capable device. This usually involves inserting the supplied CD into the computer's DVD/CD drive and allowing it to run automatically. If this is not the case, refer to the user manual supplied with the WPS-capable device on how to install the software.
- The Setup program should take you through the steps required to connect to a WPS-capable Access Point, in this case, the VoloAccess.
- If an option for PIN or PBC method of connection is offered, select PBC.
- Continue by following the steps offered by the Setup program.
- If prompted by the Setup program to initiate WPS on the Access Point, press the **WPS** button (shown here) on the VoloAccess or, click the **Start** button in the **WPS** page of Admin.

During negotiation the WPS page changes to reflect the **WPS Active** state and the WPS indicator on the VoloAccess flashes.



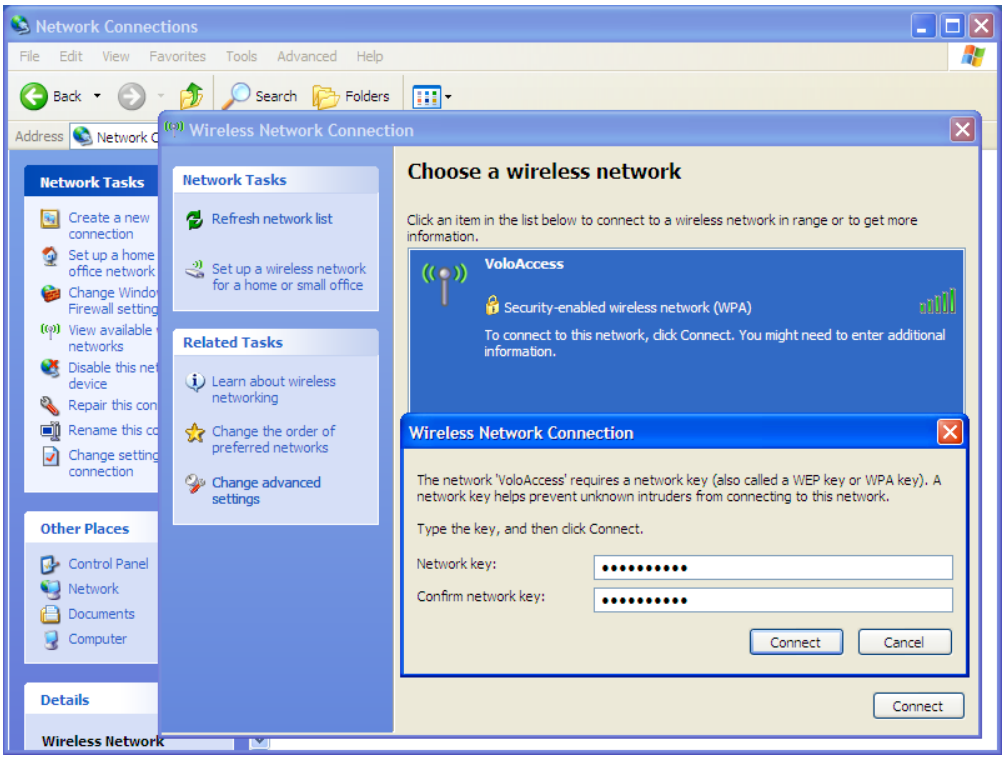
- After WPS negotiation has completed, verify the connection by selecting **LAN** > **View Leases** in Admin.

You can still connect non-WPS-capable wireless clients using the process described in the next section.

Configuring Wireless Networking on your computer

Windows XP

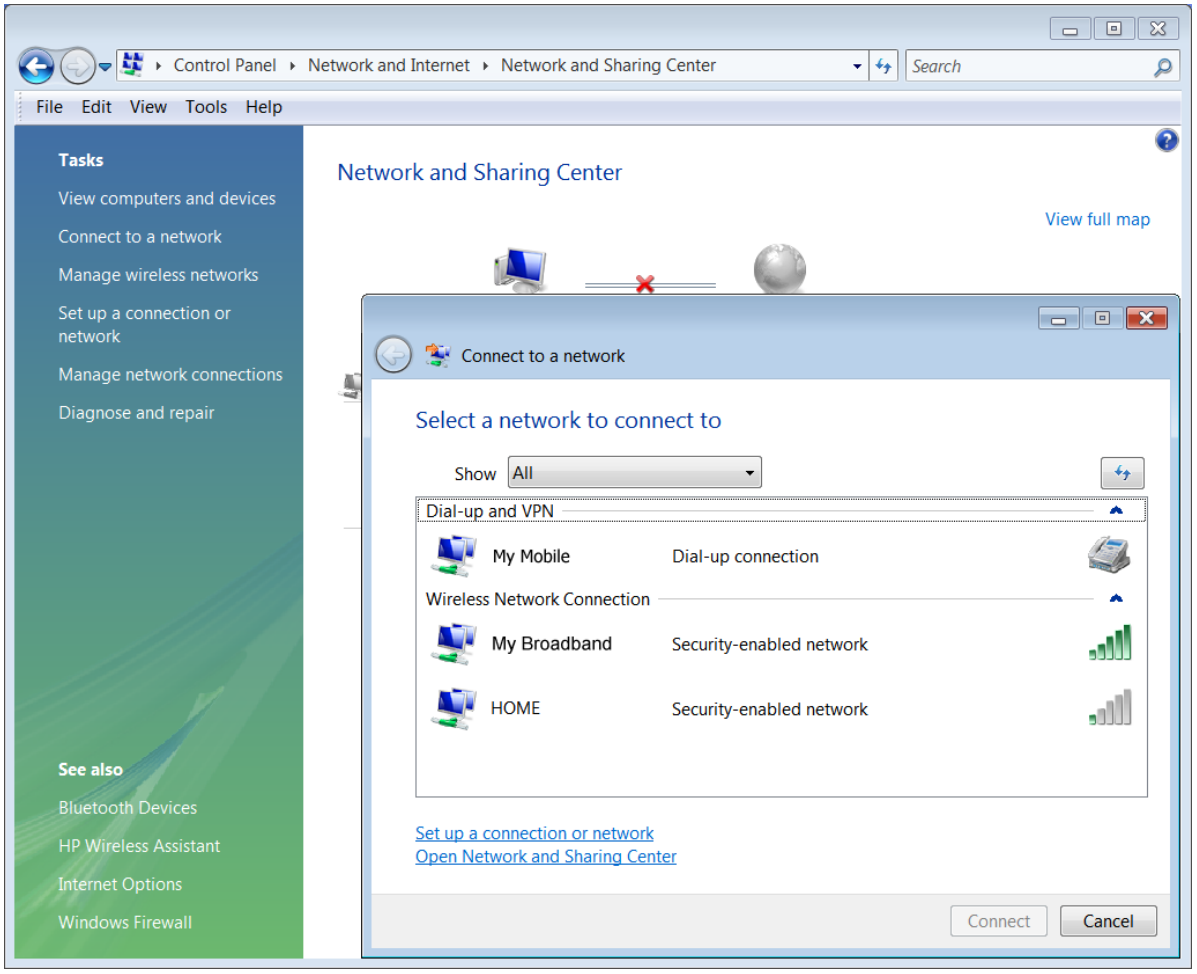
- Click **Start**, then **Control Panel**.
- Double-click **Network Connections**.
- Locate your WiFi adapter in the list. Right-click this and select **View Wireless Networks**.
- Select the network name (SSID) that you defined when setting up WiFi on the VoloAccess and click **Connect**.
- If security is configured on the VoloAccess, a dialog box is displayed requesting a **Network key**.



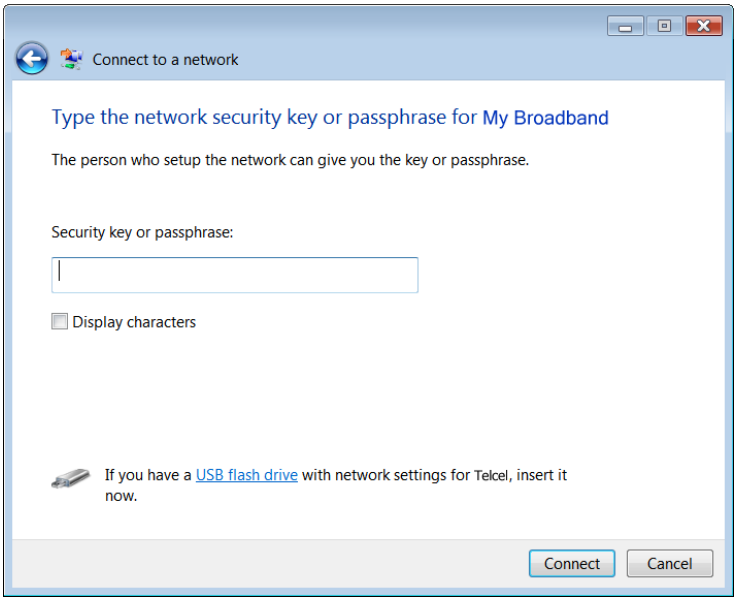
- Type in the same pre-shared key that was entered when setting up WiFi on the VoloAccess. Re-enter the key as confirmation then click **Connect**.
- After a delay of approximately 5 to 10 seconds the message **Connected** should display in the dialog box and an icon ( ) is displayed in the Windows XP notification area.
- Open your web browser; you should be online and able to access the Internet.

Windows Vista

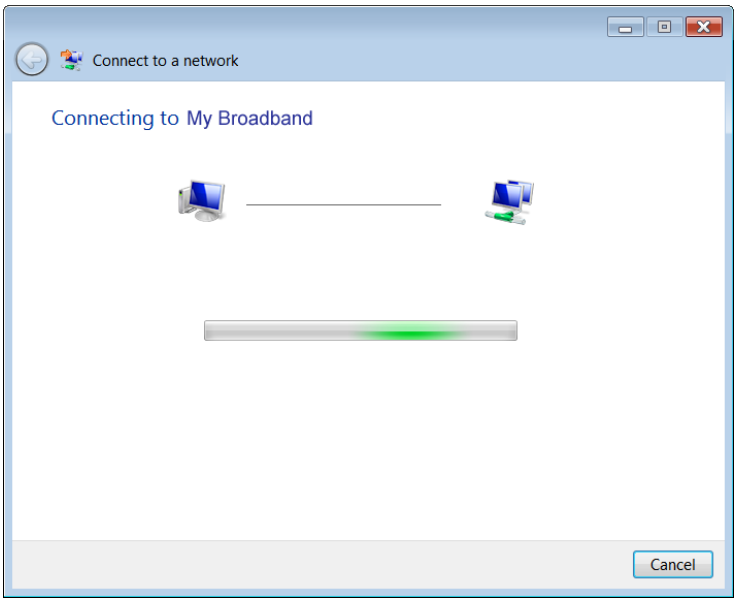
- Click **Start**, then **Control Panel**.
- Click **Network and Internet**.
- Click **Network and Sharing Center**.
- Click **Connect to a network** – the following dialog box appears for you to select a network.



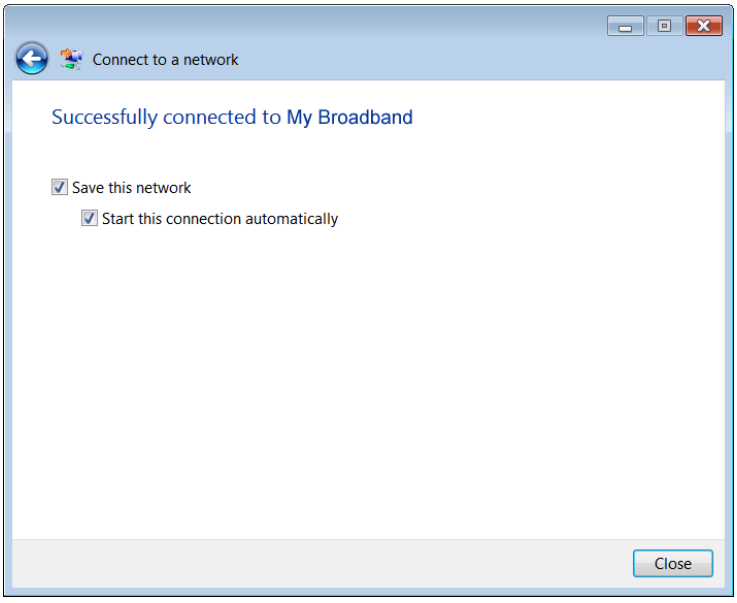
- Select the network name (SSID) that you defined when setting up WiFi on the VoloAccess and click **Connect** – the **Connect to a network** dialog box appears.



- Type in the same pre-shared key that was entered when setting up WiFi on the VoloAccess then click **Connect** – please wait while Windows networking connects to the VoloAccess.



- After a delay of approximately 5 to 10 seconds the following dialog box appears:



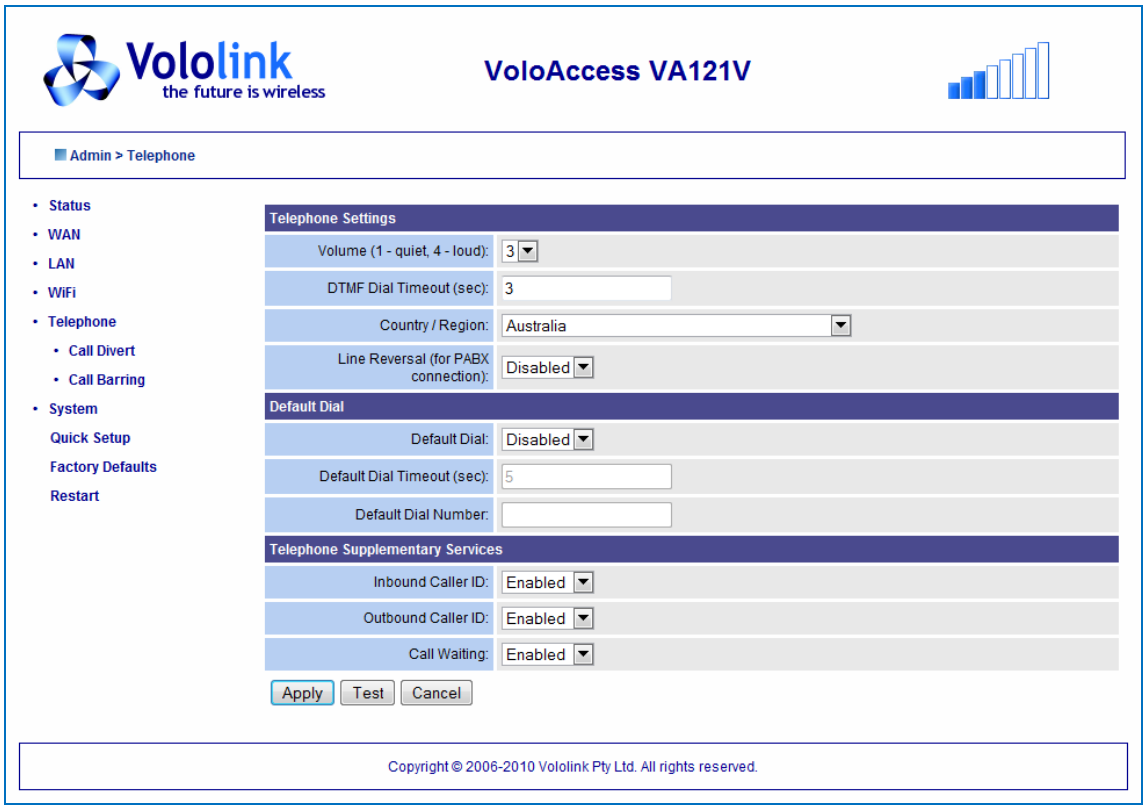
- Click the **Close** button.
- Open your web browser; you should be online and able to access the Internet.

If you are unable to access the Internet, please refer to the Troubleshooting guide.

Telephone

This section, including Supplementary Services, applies only to Voice Enabled models of the VoloAccess.

To configure operation of the telephone select **Telephone** from the Navigation panel - the Telephone page is displayed:



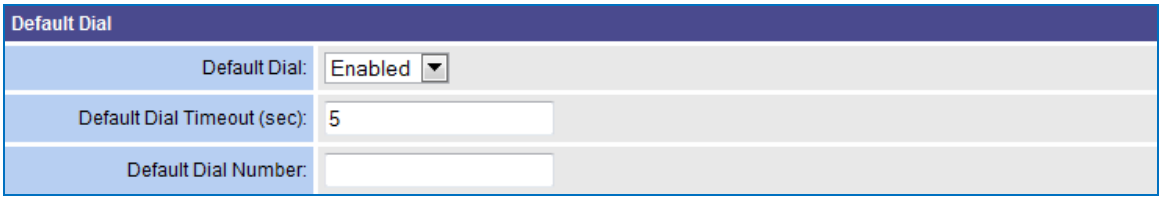
Telephone Settings

The following settings can be configured:

Volume	This is the handset earpiece volume (1- quiet, 4 – loud).
DTMF Dial Timeout	Define the time from dialling to call setup. This is the time lag between when you finish keying the number to call, and when the phone starts to dial. The timeout range is between 2 and 10 seconds. The default setting is 3 seconds.
Country/Region	Select from the drop-down list.
Line Reversal	If a **P**rivate **A**utomatic **B**ranch e**X**change (PABX) is connected to one of the VoloAccess phone ports, it may be necessary to enable this feature as some features of a PABX require Line Reversal to clear down the line or help hang up the call. This feature is required when a PABX is using PSTN as opposed to ISDN. To enable **Line Reversal**, select **Enabled** from the drop-down list.

Default Dial

Default Dial is a number that can be configured for the VoloAccess to dial automatically after a defined timeout simply by lifting the handset. This feature can be used as an emergency call facility. To implement this feature, Enable **Default Dial** using the drop-down list then click **Apply**.



Enter the **Default Dial Timeout** (in seconds) and the **Default Dial** number then click the **Apply** button. The valid range for the timeout is between 0 and 10 seconds. The default setting is 5 seconds.

Telephone Supplementary Services

Support of Supplementary Services is dependent on the network. For this reason, all of the VoloAccess services may not be available.

You can also configure:

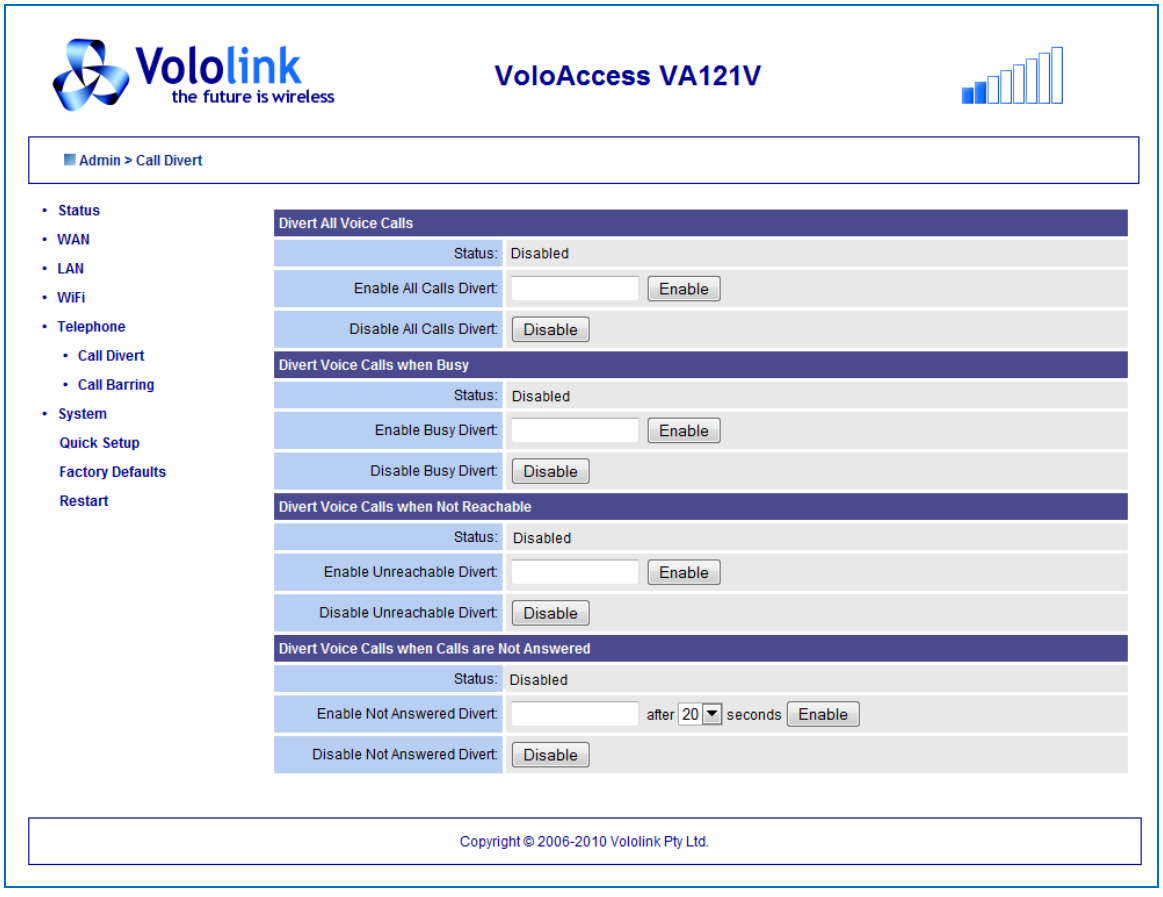
Inbound Caller ID	To display the Caller ID of an incoming call on a Caller ID capable handset.
Outbound Caller ID	Own Number sending.
Call Waiting	Call Waiting notification.

Call Divert settings override Call Waiting settings.

To enable/disable these settings, use the drop-down list then click the **Apply** button.

Call Divert

To configure Call Divert, select **Telephone** followed by **Call Divert** in the Navigation panel - the Call Divert page is displayed:



The following can be configured:

Divert All Voice Calls	Unconditional Call Diversion.
Divert Voice Calls when Busy	Busy Call Diversion.
Divert Voice Calls when Not Reachable	Phone Not Reachable Call Diversion.
Divert Voice Calls when Calls are Not Answered	No Answer Call Diversion (after a defined number of seconds).

To enable any of these settings first enter a phone number to divert to, then click the **Enable** button.

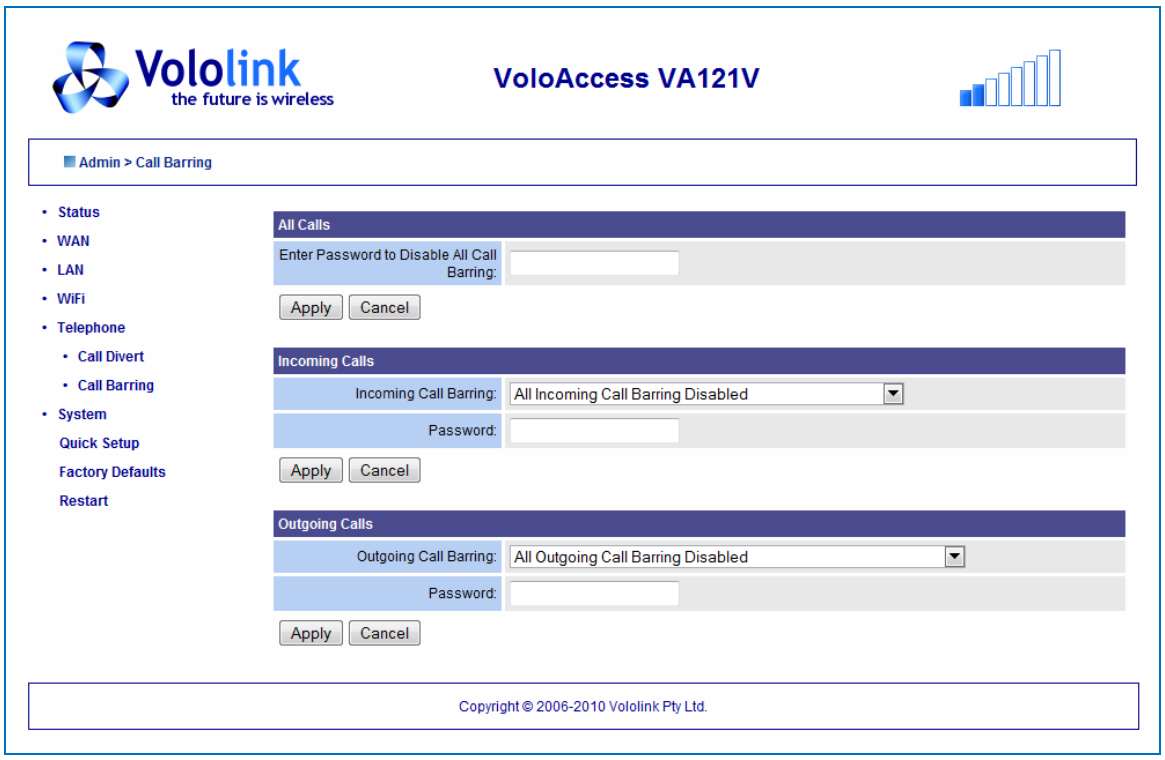
To disable a setting, click the **Disable** button.

Call Divert settings override Call Waiting settings.

When a setting has been enabled, the **Status** changes to reflect the current setting. For example, if you configured Divert Voice Calls when Calls are Not Answered to divert after 20 seconds the status would change to: Enabled, diverting to +[number] (where +[number] is the number to divert to) after 20 seconds.

Call Barring

To configure Call Barring, select **Telephone** followed by **Call Barring** in the Navigation panel - the Call Barring page is displayed:



Call Barring can be configured for:

Call Type	Setting	Explanation
All Calls	Disable Call Barring for All Calls	All Call Barring is disabled
Incoming Calls	All Incoming Call Barring Disabled	All Incoming Call Barring is disabled
	All Incoming Calls Barred	All Incoming Calls to the VoloAccess are Barred
	All Incoming International Calls when Roaming Barred	All Incoming International Calls are barred when the VoloAccess is Roaming
Outgoing Calls	All Outgoing Call Barring Disabled	All Outgoing Call Barring is disabled
	All Outgoing Calls Barred	All Outgoing Calls from the VoloAccess are Barred
	All Outgoing International Calls Barred	All Outgoing International Calls from the VoloAccess are Barred
	All Outgoing International Calls except to Home Country Barred	All Outgoing International Calls from the VoloAccess are Barred except those to your Home Country

To configure these settings, use the drop-down list to select the action, enter the Password and click the **Apply** button. You will need to obtain the password for Call Barring from your service provider.

Configuring Supplementary Services using the Phone Keypad

Introduction

Support of Supplementary Services is dependent on the SIM installed in the VoloAccess and also on the network. For this reason, all of the documented services may not be available.

The VoloAccess supports the following list of Supplementary Services.

- Inbound Caller ID
- Outbound Caller ID
- Call Waiting
- Call Divert
- Call Barring
- Multi-party Calls
- Call Transfer
- Call Holding
- Call Waiting

Throughout this section the instructions will refer to the **Flash** key, which can be labelled as **Flash** or **Recall** on a telephone.

Not all telephones have a **Flash** key. In which case, use the Telephone page in Admin to configure Telephone Supplementary Services.

When you see this icon  in the instructions, lift the telephone handset Off Hook.

When you see this icon  in the instructions, replace the telephone handset On Hook.

Keypad commands will work with a DTMF capable (tone dialling) phone only.

Table of Supplementary Phone Services

Feature	Keypad sequence
General Settings	
Inbound Caller ID **enable** Inbound Caller ID **disable**	***30Flash** **#30Flash**
Outbound Caller ID **enable** Outbound Caller ID **disable**	***31Flash** **#31Flash**
Call Waiting **enable** Call Waiting **disable**	***43Flash** **#43Flash**
Volume Setting (Where Volume Level = 1 – 4)	**#69* [Level] Flash**
Inbound Caller ID Notes This feature is only applicable for handsets that support Caller ID Display.	
Call Divert	In the following section [number] is the number to divert to. **Note:** The Country Code prefix of **+** is entered as ******
Divert all Voice Calls **enable** Divert all Voice Calls **disable**	***21*[number]*Flash** **#21**Flash**
Divert Call when Phone is Busy **enable** Divert Call when Phone is Busy **disable**	***67*[number]*Flash** **#67**Flash**
Divert Call when No Reply **enable** Divert Call when No Reply **disable**	***61*[number]*[delay]Flash** (where delay is 5 to 30 seconds) **#61**Flash**
Divert Call when Not Reachable **enable** Divert Call when Not Reachable **disable**	***62*[number]*Flash** **#62**Flash**
Call Diversion Notes: 1. If diversion of all voice calls is enabled and call diversion when either Phone is Busy or No Reply or Not Reachable is enabled, it will first disable All Voice Calls Diversion and then enable that particular diversion. 2. When diversion of all voice calls is enabled, this will override all other diversion settings.	
Call Barring	You will need to obtain the password for Call Barring from your service provider.
All Call Barring **disable**	**#330*<password>Flash**
Bar all Incoming Calls **enable** Bar all Incoming Calls **disable**	***35*<password>Flash** **#35*<password>Flash**
Bar All Incoming International Calls when Roaming **enable** Bar All Incoming International Calls when Roaming **disable**	***351*<password>Flash** **#351*<password>Flash**
All Incoming Call Barring **disable**	**#353*<password>Flash**

This section continued on next page…

Call Barring continued…

Bar All Outgoing Calls **enable** Bar All Outgoing Calls **disable**	***33*<password>Flash** **#33*<password>Flash**
Bar All Outgoing International Calls **enable** Bar All Outgoing International Calls **disable**	***331*<password>Flash** **#331*<password>Flash**
Bar All Outgoing International Calls except to Home Country **enable** Bar All Outgoing International Calls except to Home Country **disable**	***332*<password>Flash** **#332*<password>Flash**
All Outgoing Call Barring **disable**	**#333*<password>Flash**

The next section refers to **In Call** features. These commands are executed while a call is in progress.

Feature	Keypad sequence
Answer a Call in Waiting	**Flash2#** Alternates between the calls
Multiparty Call – A call is in progress and there is another incoming call	**Flash2#** to put current call on hold and pick up the incoming call; then, **Flash3#** to connect all calls
Multiparty Call – A call is in progress and you make another call	**Flash2#** to put current call on hold, make another call by **Flash**[**number**]***,** when call is answered, **Flash3#** to connect all calls

Cancelling a Command

For all commands except the In-Call Feature commands, hanging up the telephone handset or pressing the Cancel button in Admin will cancel it.

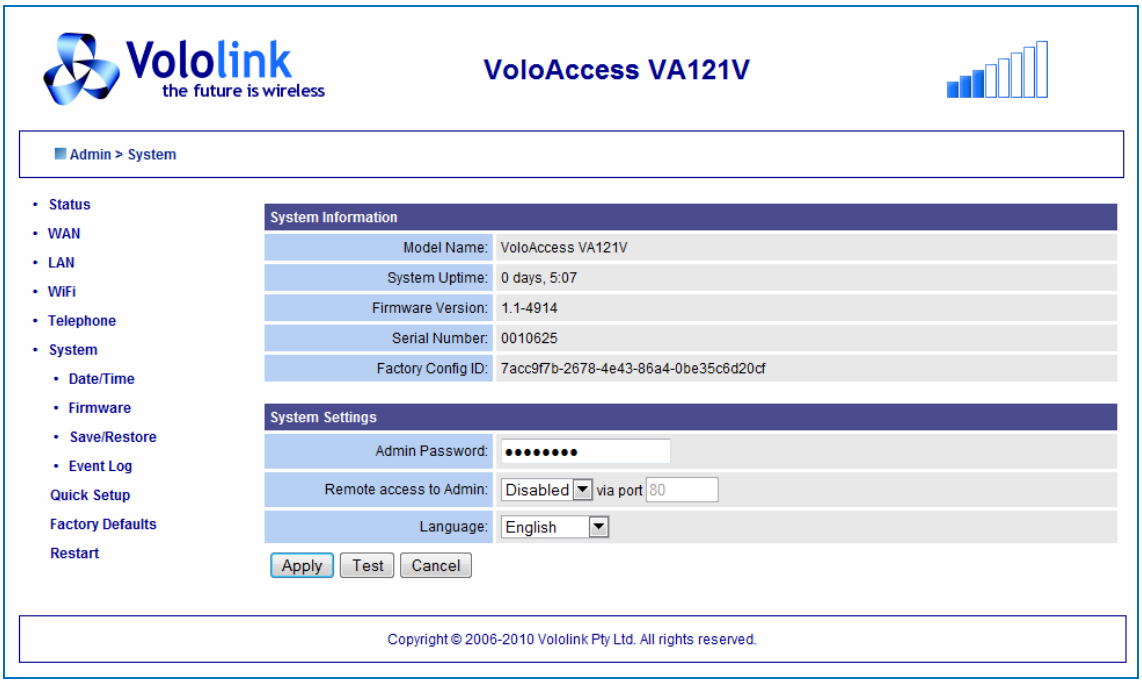
Command Success/Failure Indication

For a command entered using the keypad, you will hear a high pitched beeping (higher than the dial tone pitch) to indicate success. A low pitched beeping (similar to the dial tone pitch) indicates failure.

System

The System page displays System Information and allows the configuration System Settings.

From the Navigation panel, select **System** - the **System** page appears.



Under the **System Information** heading the following items appear:

- **Model Name** — This is the Model Name of the VoloAccess.
- **System Uptime** — The lapsed time since the VoloAccess was powered on.
- **Firmware Version** — The Version Number of the Firmware installed on the VoloAccess.
- **Serial Number** — The Serial Number of the VoloAccess.
- **Factory Config ID** — The ID of the factory configuration that the VoloAccess will revert to when Reset to Factory Defaults.

Under the **System Settings** heading the following items appear:

- **Admin Password** — The default password for the VoloAccess is "**password**". This should be changed to protect access to your VoloAccess. (see below).
- **Remote access to Admin** — Enable/disable remote access to Admin using the WAN IP Address (see below).
- **Language** — Select the Language from the drop-down list.

To change the **Admin** Password:

- Enter the new password in the editbox, and then click the **Apply** button.
- You are prompted to Log in using the new password.
- Enter the new password and click the **OK** button.

If **Remote Access to Admin** is enabled, it is recommended that you change the default password to prevent unauthorized access.

To enable/disable **Remote Access to Admin**:

- Select Enabled or Disabled from the dropdown list. You can also define the port that Remote Access will use. The default value is port 80.
- Click the **Apply** button.

Accessing Admin Remotely

To access Admin remotely use a Web Browser as follows:

- Enter the WAN IP Address of the VoloAccess into the address area of a Web Browser and press **Enter**. The WAN IP address is obtained from the WAN > 3G Embedded page in Admin under the heading *Network Status*.
- When prompted enter the Admin **User ID** and **Password**, then click **OK**. This is the same User ID and Password used to access Admin locally.

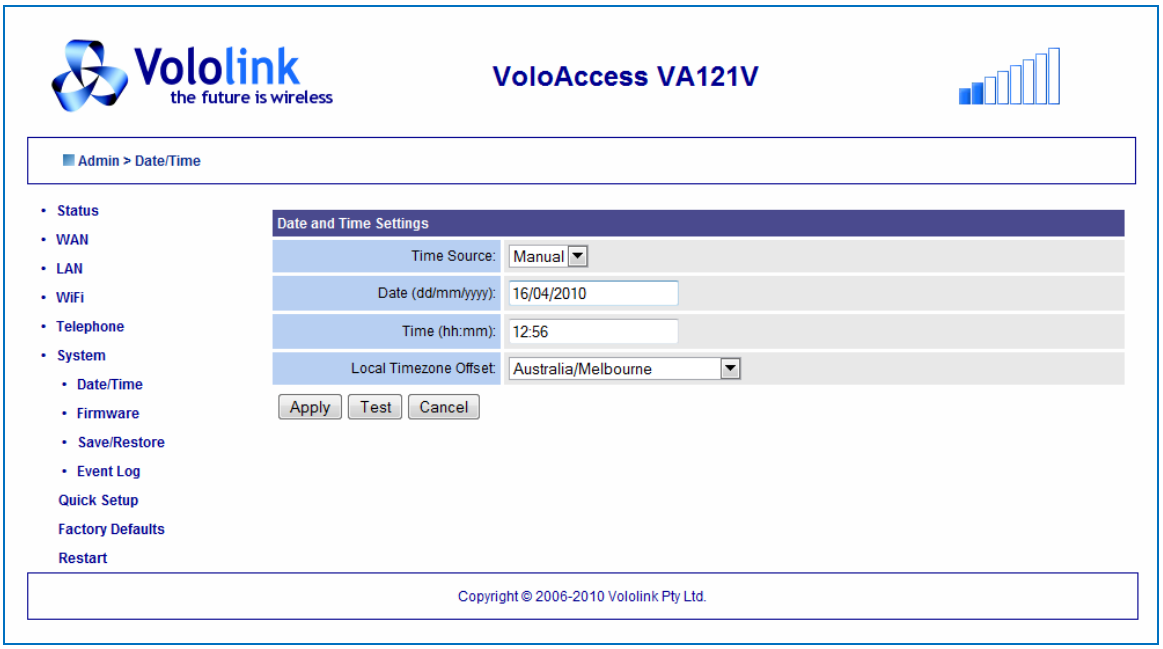
If your 3G service provider allocates a private IP address to the VoloAccess (this is known to happen in some cases) then Remote Access to Admin will not work. A private IP address is in one of the following ranges:

10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

Setting the Date and Time

To set the Date and Time on the VoloAccess follow these steps:

- From the Navigation panel select **System** followed by **Date/Time** - the Date/Time page appears:

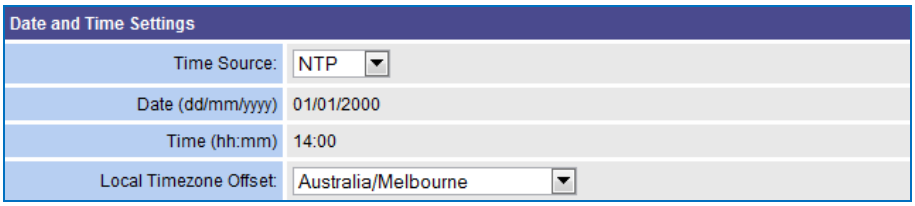


- By default, the **Time Source** is **Manual**.
- Enter the current **Date and Time**.
- Select your **Local Timezone Offset** from the drop-down list.
- Click the **Apply** button to save the settings.

The **Time Source** can also be configured to **NTP** (**N**etwork **T**ime **P**rotocol) or **NITZ** (**N**etwork **I**dentity and **T**ime **Z**one) meaning the VoloAccess will synchronise the date and time with a time server.

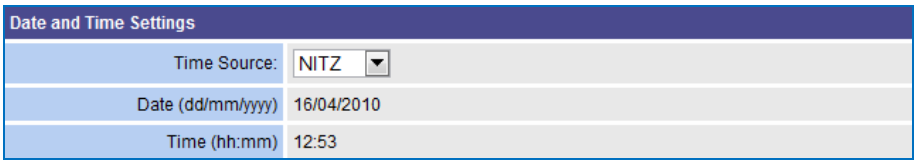
To select the NTP Time Server:

- Select **NTP** from the drop-down list.



- Select your **Local Timezone Offset** from the drop-down list.
- Click the **Apply** button.

To select the NITZ Time Server:



- From the drop-down list select **NITZ** then click the **Apply** button.

It is not necessary to specify a Local Timezone Offset as the NITZ protocol automatically determines this in conjunction with the mobile network.

NITZ support is network operator dependent.

Updating the VoloAccess Firmware

From time to time it may be necessary to update the VoloAccess firmware. To obtain updated firmware please contact your VoloAccess supplier then proceed as follows:

If you are updating the firmware on a WiFi enabled VoloAccess, connect the VoloAccess to the computer using the supplied Ethernet cable.

- From the navigation panel select **System** followed by **Firmware** – the Firmware page appears:

- Click the **Browse** button to locate the Firmware Update file - a browse box opens.
- Select the Firmware Update file.
- Click the **Open** button to select the update.
- Click the **Update Firmware** button to start the process.

The Firmware update will take between 3 and 8 minutes to complete.

Make sure that you click 'Update Firmware' only once.

Do not attempt to cancel or interrupt the firmware update.

Do not navigate away from the Firmware Update page until complete.

When the update is complete the VoloAccess will reboot automatically and the **Firmware Update Complete** page will appear.

The VoloAccess will restart automatically and display the VoloAccess Index page.

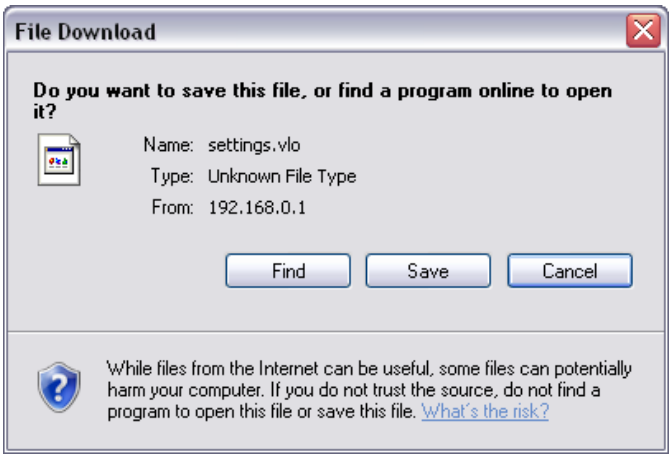
Save/Restore Configuration

It is good practice to save the VoloAccess configuration to a file so that it can be restored at a later date if it becomes necessary to recover from a configuration error. To save the configuration, proceed as follows:

- Select **System** followed by **Save/Restore** in the Navigation panel - the **Save/Restore** page appears:

- Click the **Save Configuration** button.

  A confirmation dialog appears. Click the **Save** button.



The **Save As** dialog appears.

- Select a location to save the backup configuration file.
- Click the **Save** button to complete the task.
- A **Download Complete** dialog appears – click **Close**.

To **Restore** a saved configuration:

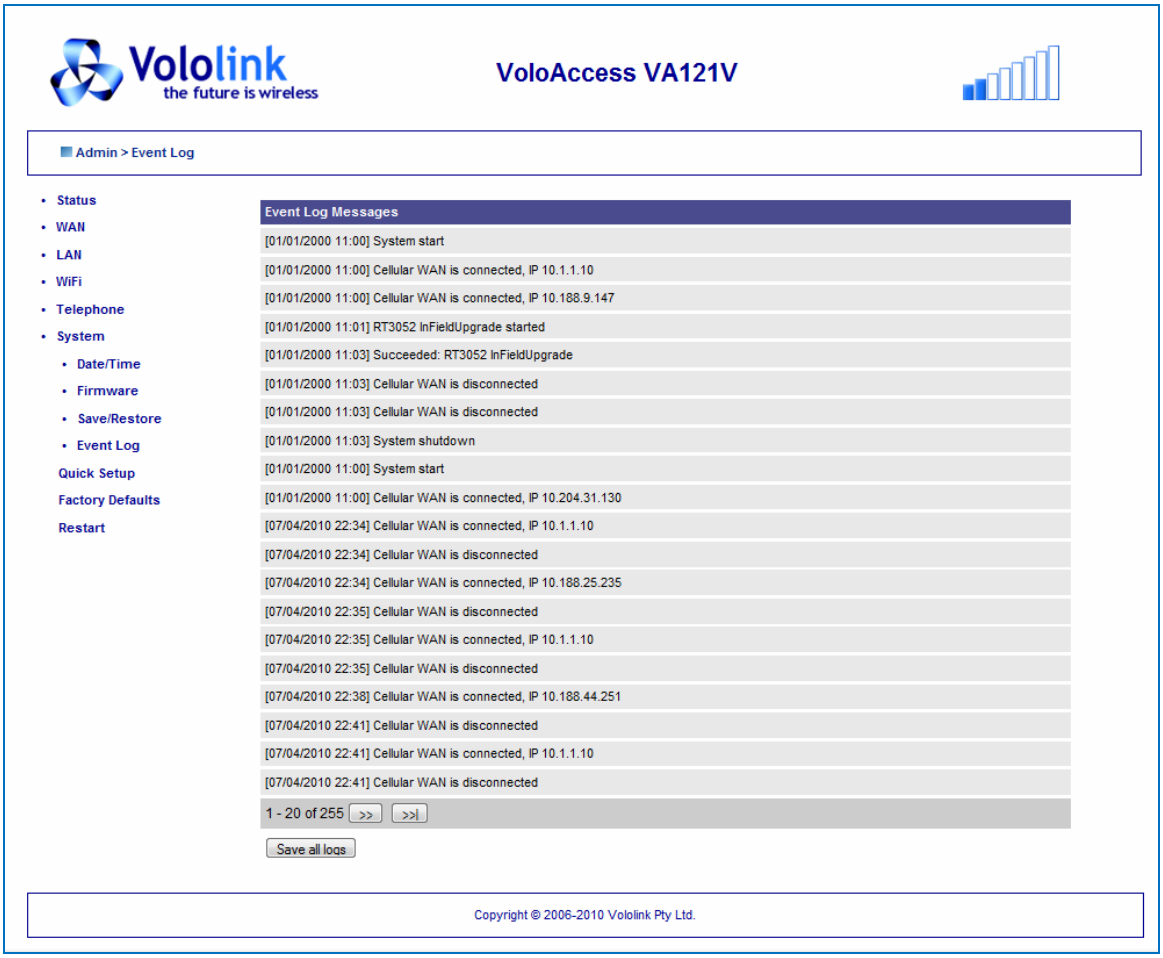
- Under the heading **Restore Configuration** click the **Browse** button - a dialog opens for you to locate and select the previously saved backup configuration file.
- Click the **Restore Configuration** button.

Do not attempt to cancel or interrupt this operation.

After the upload has completed it is necessary to restart the VoloAccess for the restored configuration to take effect.

Event Log

To view the **Event Log** select **System** followed by **Event Log** in the Navigation panel - the Event Log page appears:



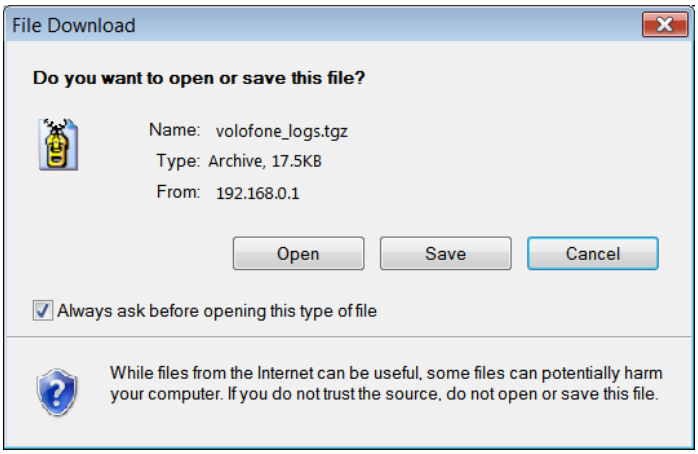
Events are displayed in groups of 20 items. Use the Back/Forward keys (see below) at the bottom of the page to move through the Event Log.

|<<	Move to the first page of the Event Log.
<<	Move to the previous page of the Event Log.
>>	Move to the next page of the Event Log.
>>|	Move to the last page of the Event Log.

If you lodge a support request you may be asked to view the Event Log to assist in diagnosis.

To save a copy of all VoloAccess logs:

- Click the **Save all logs** button – the following dialog box appears:

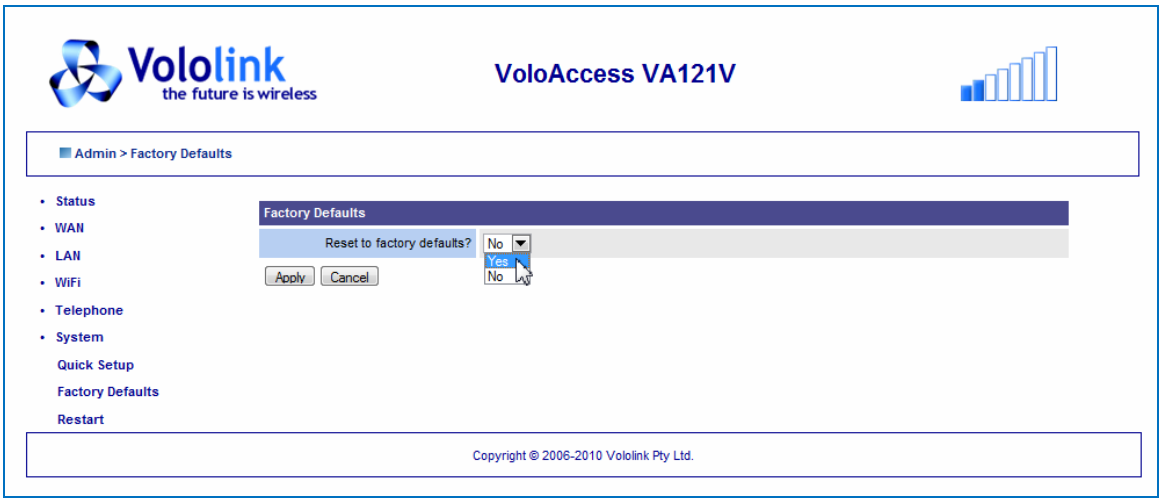


- Click the **Save** button.
- A **Save** dialog appears for you to select a location to save the file.
- Click the **Save** button – a **Download complete** dialog appears.
- Click the **Close** button.

Factory Defaults

Setting the VoloAccess to factory defaults will overwrite all configuration items including the Admin password. The configuration settings can be saved using the Save Configuration feature. This saved file can be restored once the VoloAccess has restarted.

To restore the VoloAccess to the factory settings select **Factory Defaults** from the Navigation panel - the **Factory Defaults** page appears:



- Select **Yes** from the drop-down list.
- Click the **Apply** button.

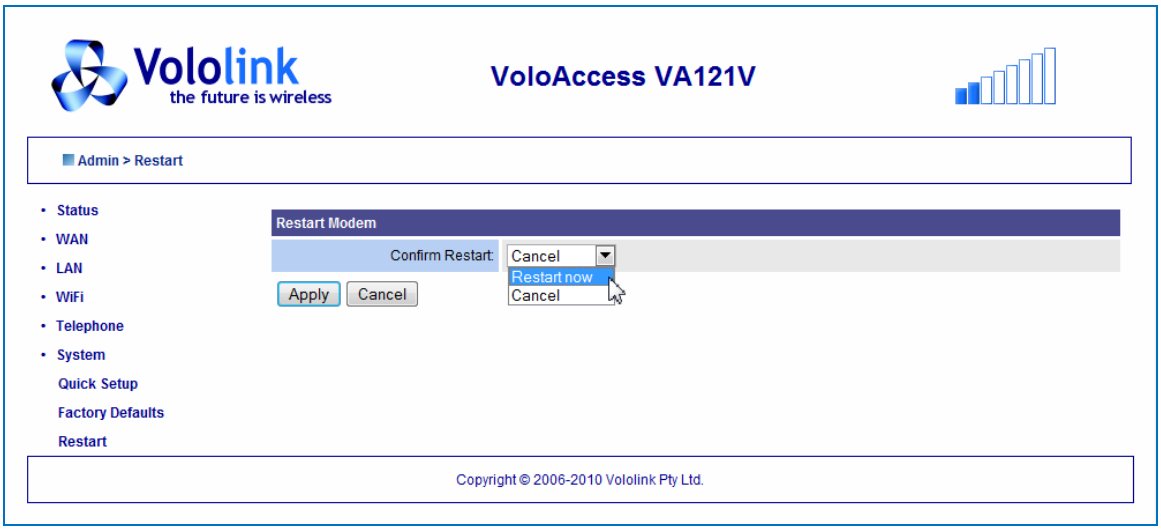
The VoloAccess will restart and display the Restarting page containing a prompt to 'click here to refresh'. If JavaScript is enabled in your Web browser, this is not necessary to reload the page – the refresh will happen automatically.

It is necessary to re-enter the APN before the VoloAccess will connect to the Internet.

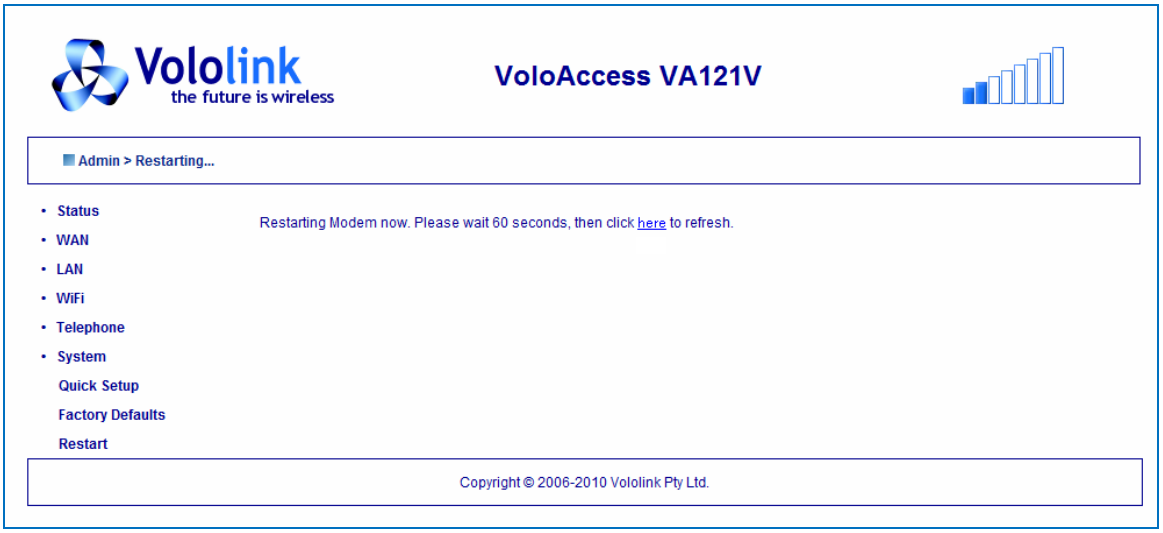
Setting the VoloAccess to factory defaults can also be done using the Reset button.

Restarting the VoloAccess

To restart the VoloAccess select **Restart** from the Navigation panel - the **Restart** page is displayed:



- From the Drop-down list select **Restart now**.
- Click the **Apply** button - the **Restarting** page appears.



- The VoloAccess will restart automatically and display the Index page.

If JavaScript is enabled in your Web browser, it is not necessary to 'click here refresh' to reload the page – the refresh will happen automatically.

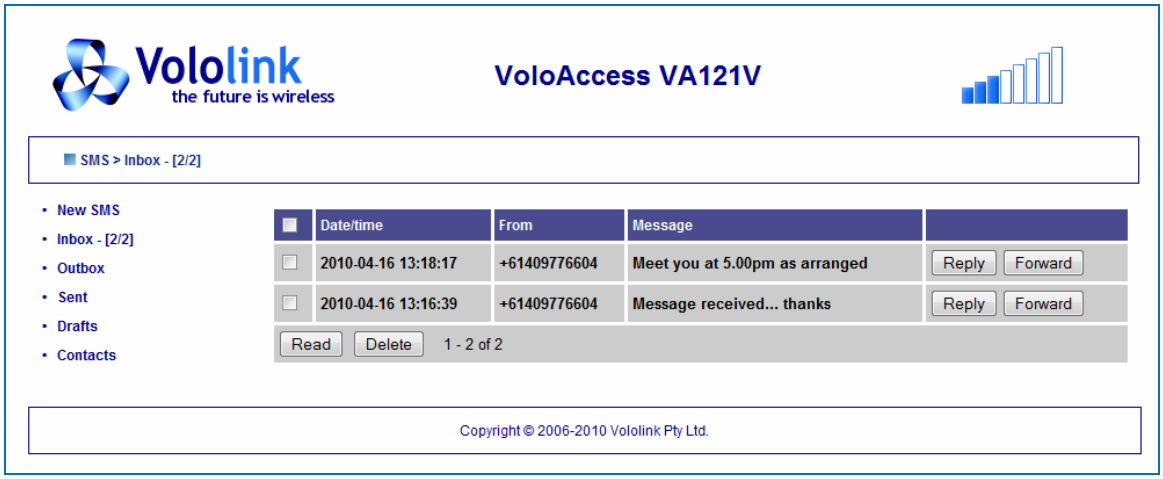
The VoloAccess can also be restarted using the Reset button.

SMS Services

To use the VoloAccess to send or view received SMS messages proceed as follows:

- Return to the VoloAccess Index page and select **SMS** – the SMS Inbox page appears.

To return to the VoloAccess Index page, click the Vololink logo in the top left of any page.



Use this page to read SMS messages received by the VoloAccess.

Unread messages are displayed in bold text. To mark a message as “Read”, click the checkbox next to the message(s) and click the **Read** button.

There is no audible or visual notification that an SMS message has been received. It is necessary to load SMS and check the Inbox.

- The **Date/time** column shows the Date and Time the SMS message was received.
- The **From** column displays the sending mobile number.
- The **Message** column displays the text of the message.

From this page you can **Reply**, **Forward** or **Delete** a message. (see below)

Reply to an SMS message

- Click the **Reply** button next to the message to reply to.
- The **New SMS** page appears with the recipient’s number in the **Phone Number** editbox.
- Enter the message text, then click the **Send** button.

Forward an SMS message

- Click the **Forward** button next to the message to forward.
- The **New SMS** page appears with the message in the **Message** editbox.
- Enter the phone number (or click the **Contacts** button to select a recipient), then click the **Send** button.

Delete an SMS message

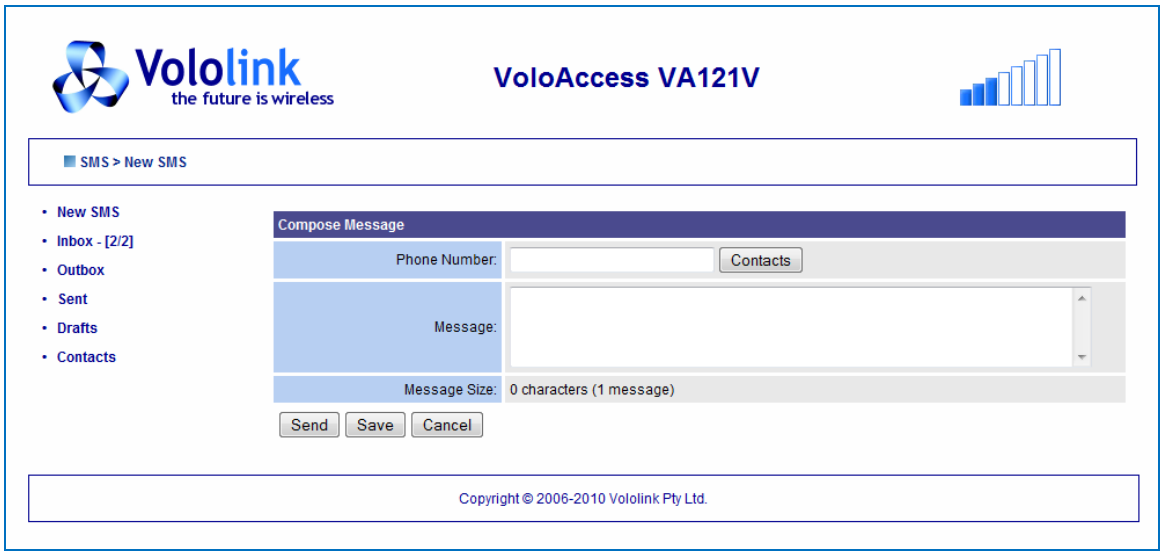
- Click the checkbox next to the message(s) to delete.
- Click the **Delete** button.

The message is deleted immediately without further confirmation.

Creating a new SMS message

To create a new SMS message, follow the steps below:

- In the Navigation Panel click **New SMS** - the New SMS page appears.



- Enter the **Mobile Phone Number(s)** or, **Select from Contacts** (the Contacts page appears).

When entering multiple mobile phone numbers, use a comma (,) or semicolon (;) as a separator. For example, NNNNNNNNN,NNNNNNNNN.

- Select a recipient by clicking the checkbox next to the contact's name (multiple recipients may be selected), then click the **OK** button to add the number(s) to the Recipients list.
- Type the message in the Message edit box. As the message is entered, the Message Size (in characters) is displayed.
- The maximum number of characters per message is 160. Longer messages are split into smaller messages and combined at the receiving end.
- Click the **Send** button to complete sending an SMS message.

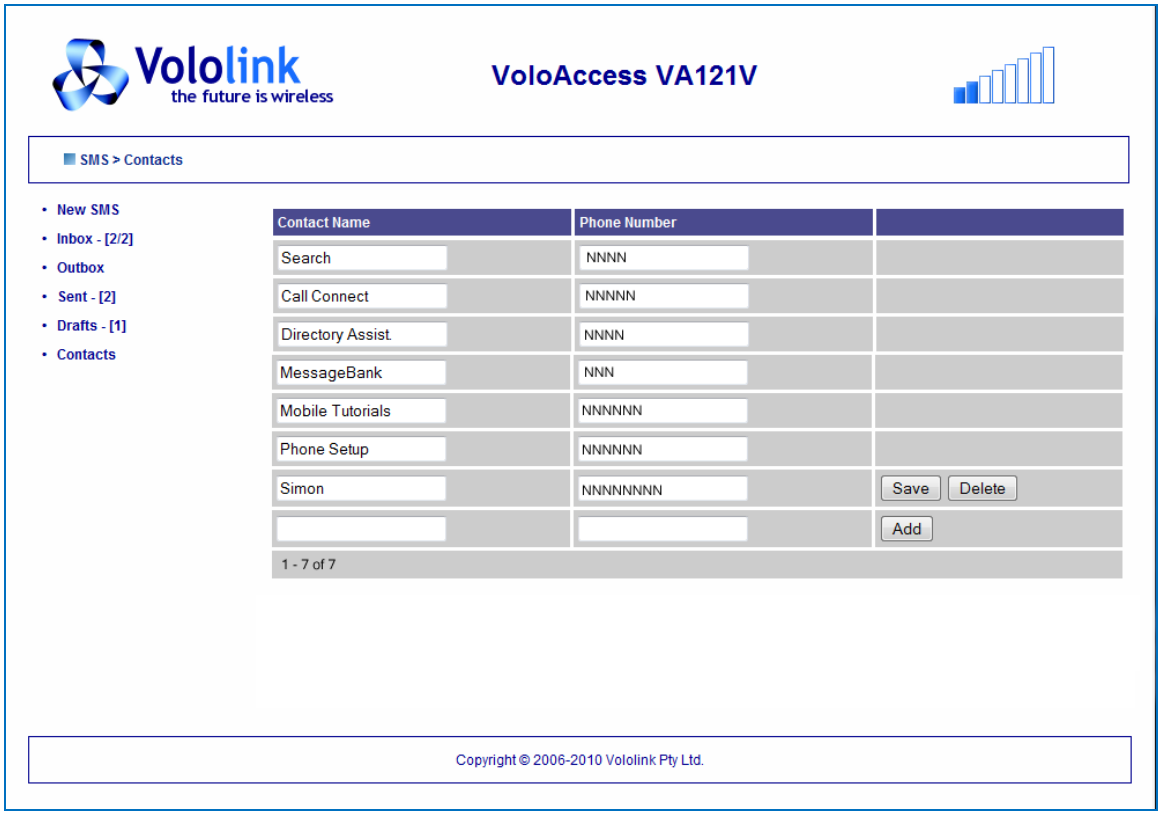
Adding new entries to the Contacts page

Use the SMS Contacts page to store mobile phone numbers of the people that you correspond with via SMS.

To add a new entry, proceed as follows:

- In the Navigation Panel click **Contacts** - the **Contacts** page appears.

The contacts already stored on the SIM are read and displayed.



- In the blank **Contact Name** editbox at the bottom of the list enter the new contact's name**.**
- In the blank **Phone Number** editbox at the bottom of the list enter the new contact's phone number.
- Click the **Add** button to add the new contact to the Contacts list.

Contacts are arranged in alphabetical order.

Contacts that you add can be edited or deleted; those added by the SIM provider are read only and cannot be edited or deleted.

Editing an entry in the Contacts list

To edit an existing contact:

- Make the required changes to the **Contact Name** or **Phone Number**, then click the **Save** button.

Deleting an entry in the Contacts list

- Click the **Delete** button next to the contact to delete.

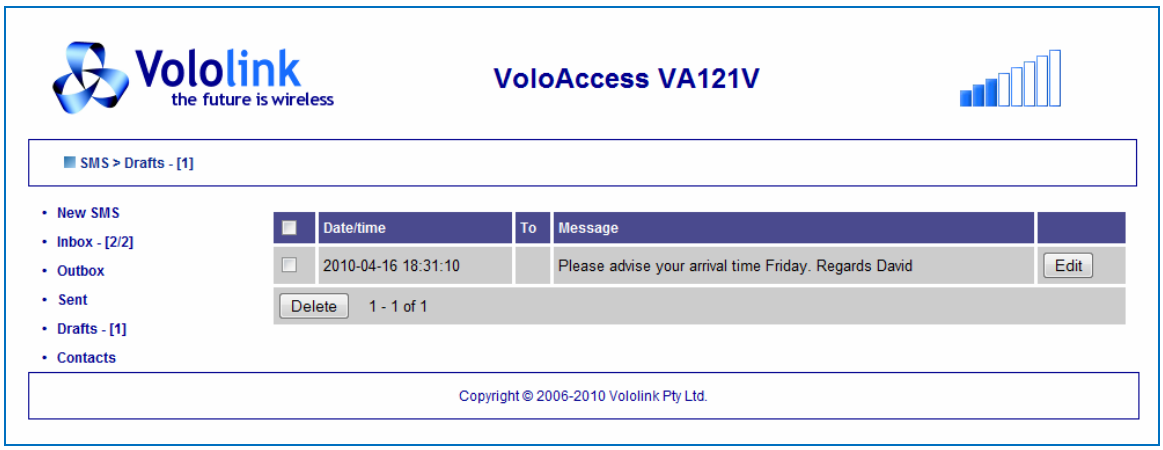
The contact is deleted immediately without further confirmation.

Saving a Draft Copy of a Message

There are occasions when you may wish to create a message to be sent later. To do this, open the New SMS page and compose the new message. When complete, click the **Save** button – the message is saved in the **Drafts** area for later use.

To use a previously saved **Draft** message:

- In the Navigation Panel select **Drafts** - the Drafts page appears:



- Click the **Edit** button next to the message to process - the message is loaded into the New SMS message page for editing and sending.

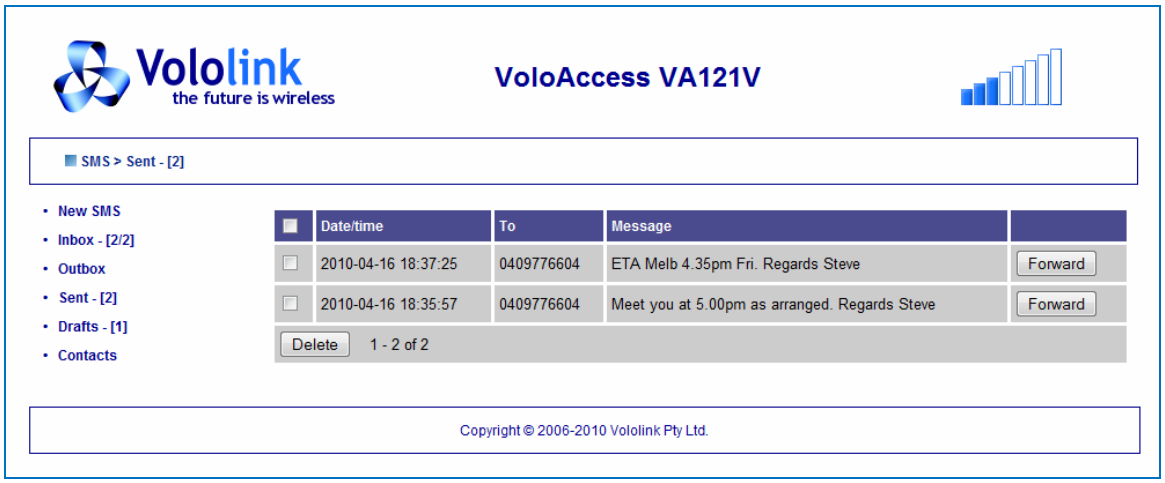
To delete a draft message, click the checkbox next to the message to delete, and then click the **Delete** button.

The message is deleted immediately without further confirmation.

Sent Messages

The Sent page is used to view previously sent SMS messages.

- Click **Sent** in the Navigation panel - the Sent page appears:



Sent messages are displayed for viewing.

The Sent page can also be used to forward a message to another recipient as follows:

- Click the checkbox next to the message to forward.
- Click the **Forward** button - the message is loaded into the New SMS message page for editing.
- Enter the **Mobile Phone Number(s)** or, **Select from Contacts** (the Contacts page appears).

Multiple phone numbers can be entered. Use a comma (,) or semicolon (;) to separate the numbers.

- Select a recipient by clicking the checkbox next to the contact's name (multiple contacts may be selected), then click the **OK** button to add the number(s) to the Recipients list.
- Click the **Send** button to complete forwarding an SMS message.

To delete a sent message, click the checkbox next to the message to delete, and then click the **Delete** button.

The message is deleted immediately without further confirmation.

Troubleshooting

This section describes how to solve a number of issues that could occur during installation, configuration, and use of the VoloAccess.

Before attempting any of the methods described in this section, make sure that the connected cables are securely inserted and that the Power indicator on the VoloAccess is On.

If none of the suggested methods resolve the issue, it is recommended that you:

- Restart the VoloAccess.
- Reset the VoloAccess to default factory configuration and reconfigure the unit.

To restart the VoloAccess, click **Restart i**n the navigation panel of the Admin page. If you still cannot access the VoloAccess, switch the VoloAccess off then wait for 30 seconds before switching it on again.

To reset the settings to default factory configuration, use a paper clip to press the Reset button. Refer to Reset the VoloAccess to default factory configuration for further information.

The default factory configuration contains the original settings of your VoloAccess.

A reset to default factory configuration cannot be undone. If you reset the VoloAccess to default factory configuration, all your previous configuration changes are replaced. If you have previously changed the password, you will have to login to the VoloAccess Index page with the default User name “admin” and Password “password”.

Indicators

What do the VoloAccess Indicators mean… what are they telling me?

Please refer to VoloAccess Indicators. There you will find a comprehensive description of the function of each indicator.

The VoloAccess Signal Strength Indicator and Network Indicators are not On

There are a several possibilities:

- First, check that the SIM is inserted. If the SIM is missing, please insert the SIM in the correct orientation. Refer to the diagram under Installing the SIM.
- If the SIM is inserted correctly, the most likely cause would be the SIM has the **Pin Lock** enabled. The SIM could be locked after entering an incorrect PIN multiple times. The SIM could also be faulty.
- The dial tone sounds different for PIN lock and PUK lock which, due to obvious limitations, is not possible to describe here. PIN or PUK lock is best verified using the Admin Web page. Both PIN and PUK unlocking can be done via the **Admin > WAN > 3G Embedded** page. On a voice enabled VoloAccess the PIN can also be entered using the phone keypad. Unlock the SIM using the telephone keypad by lifting the handset and entering **#NNNN#** (where NNNN is the SIM PIN) then replace the handset.
- If the Network indicator is still not On a few seconds after you have entered the correct PIN/PUK, the SIM may be faulty or, you have inserted it incorrectly. Remove the SIM and reinsert it, referring to the diagram Installing the SIM.
- The easiest way to check if a SIM is faulty is to insert it in a mobile phone and attempt to make a call. If it does not work, the SIM is faulty - you need to contact your service provider to obtain a replacement.
- If the VoloAccess still does not work after performing the above steps, please contact your Place of purchase.

The VoloAccess Signal Strength Indicator is On and the Network Indicator is Off

- The SIM you are using is not recognized by your service provider. Please contact your service provider to register your service or have the SIM replaced.

I have entered the APN provided by my Service Provider, but the Network Indicator is still not On. How do I solve this?

- Check the status from the **Admin > WAN > 3G Embedded** page. If it reports “Not connected”, please check the APN entered. Spelling, including spaces, has to be correct for it to be accepted by the network.
- On the **Admin > Status** page check that the **SIM State** is 'Ready' under **Cellular Network Status**, the **Network Operator** is correct and the **Network State** is 'Registered <a data capable technology, EDGE, GPRS, WSDMA etc>'.
- Confirm that your service provider does not require PPP Authentication. If PPP Authentication is required, you need to configure the VoloAccess with the correct username and password. Refer to Configuring PPP Authentication for further information.
- If this does not solve the problem, try turning the VoloAccess off and on again.
- If this still does not solve the problem, please return the unit to the Place of purchase.

When I pick up the handset, the Telephone Indicator does not flash. Why?

- If you do not get a dial tone either, the cable between the telephone and VoloAccess is probably the cause. Replace this cable or, if you have another telephone, try connecting it to the VoloAccess.
- If you do have a dial tone, check that you are able to make phone calls. If you can, the phone Indicator may be faulty. Please return the unit to the Place of purchase.

Telephone (Voice enabled models only)

When I pick up the telephone handset, I do not hear anything. Why?

- See Telephone Indicator answer.

Why do I not get the normal dial tone?

See Network Indicator answer.

- **Telephone Service not available**

If you cannot make or receive a call from a phone connected to the VoloAccess, perform the following actions to identify and solve the problem:

- Make sure that the phone is working; try connecting it to a fixed line telephone network (PSTN). The phone has to be of a standard touch tone type (with DTMF keypad support).

Some older phones have a keypad, but do not support DTMF. These phones are not supported by the VoloAccess.

- Connect the phone directly to the Phone connector on the VoloAccess. Verify that a dial tone is heard when picking up the handset. If not, replace the handset and restart the VoloAccess. Allow sufficient time for the VoloAccess to restart (the Signal Strength indicator should be On and solid – flashing indicates a weak signal) and then listen for the dial tone again.
- Lift the handset and the phone indicator should flash. If this does not happen:
  - Check the phone connection.
  - If using a cordless phone, check that power supply is on.
  - Check the Call Barring setting using Admin. If necessary, disable all Call Barring. Refer to Call Barring in the User Manual for further information.
  - Check the SIM is not locked. If the SIM PIN is required, the dial tone is different (an intermittent tone instead of the normal dial tone). On a voice enabled VoloAccess unlock the SIM using the telephone keypad by lifting the handset and entering **#NNNN#** (where NNNN is the SIM PIN) then replace the handset.

SIM

SIM Insertion

- See Network Indicator answer.
- Make sure the SIM is inserted correctly. Refer to Installing the SIM.
- If the Network Indicator is Off a PIN is required or, the SIM is locked as a result of entering an incorrect PIN multiple times, in which case, the PUK is required to unlock the SIM. This can be verified on voice enabled models by connecting a telephone handset and listening to the dial tone, or load the **Admin > Status** page and check **SIM Status** - should be **Ready** if the SIM is functioning correctly.
- If the SIM is seated correctly but the SIM Status is not Ready; it is necessary to verify that the SIM is working. The easiest way of verifying a SIM is to install it in a mobile phone and attempt to make a call.

Administration Web page

I can access the VoloAccess Administration Web page at http://192.168.0.1, but when I try to click on Admin, Internet Explorer responds with the error, "The web page you requested is not available offline"

- According to Microsoft, "Internet Explorer searches for an Internet connection before it attempts to serve local Web pages. This behavior is by design."
- To correct this, from the **File** menu in Internet Explorer, uncheck the **Work Offline** option.

Unable to Access Admin

If you cannot access Admin, perform the following actions to identify and solve the problem:

Check that the computer is configured to obtain an IP address automatically using DHCP. If not, change the computer TCP/IP settings. For further information, see Connecting the VoloAccess to a Computer or the manual of your operating system.

Check that an IP Address has been allocated to your computer by the VoloAccess. Use the procedure described under No LAN Connection.

If the VoloAccess IP address has been changed and you do not know the current IP address, use the **Reset** button to reset the VoloAccess to default factory configuration (see above). This will set the IP address to 192.168.0.1.

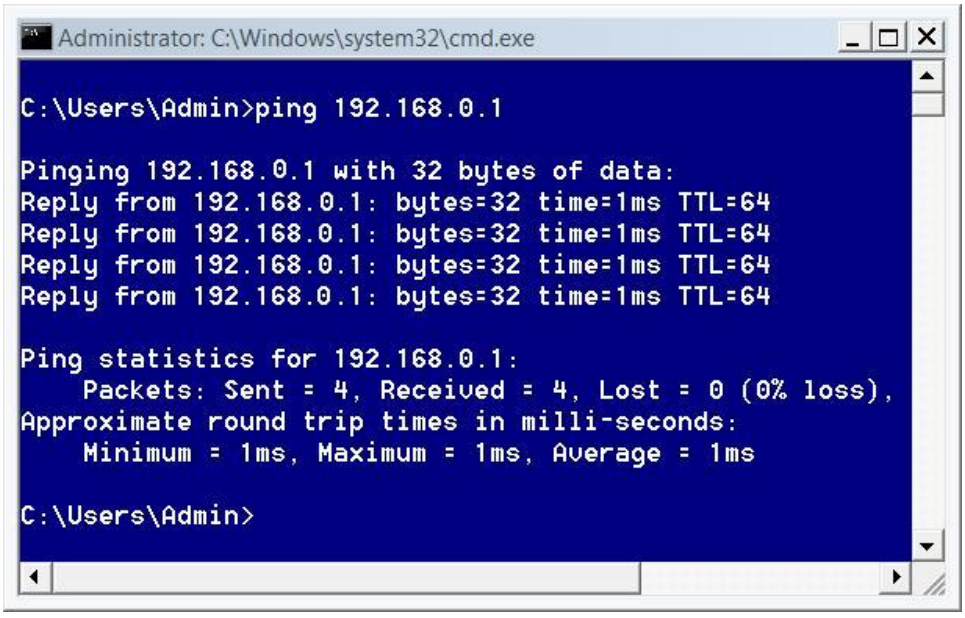
Make sure you are using the correct login details. If the default password has been changed and you do not know the current password, use the **Reset** button to reset the VoloAccess to default factory configuration (see above). This will reset the login details to default values. The default User Name is "admin" and the Password is "password".

If the computer is connected to the VoloAccess via an Ethernet cable, check that the corresponding LAN connector indicator is illuminated. If not, make sure that the cable is properly connected or try using another Ethernet cable.

Connectivity Problems

Before attempting to resolve connectivity problems, always check the following first:

- Check that one end of the Ethernet cable is plugged into the VoloAccess and the other end into a network switch or directly into a computer.
- Check the LAN indicator on the VoloAccess. It should be On and solid blue. If this is not the case, the cable may be faulty or not plugged in properly. Check the connections, if they are solidly connected and the LAN indicator is not lit, the cable is faulty. Replace the cable.
- Ping the VoloAccess from a Command prompt as follows:
- From the **Start Menu**, select **Run**, then type **cmd** and press **Enter** – a Command prompt window opens.
- Select this window and type **ping 192.168.0.1** then press **Enter**.
- The response should be similar to the following diagram:



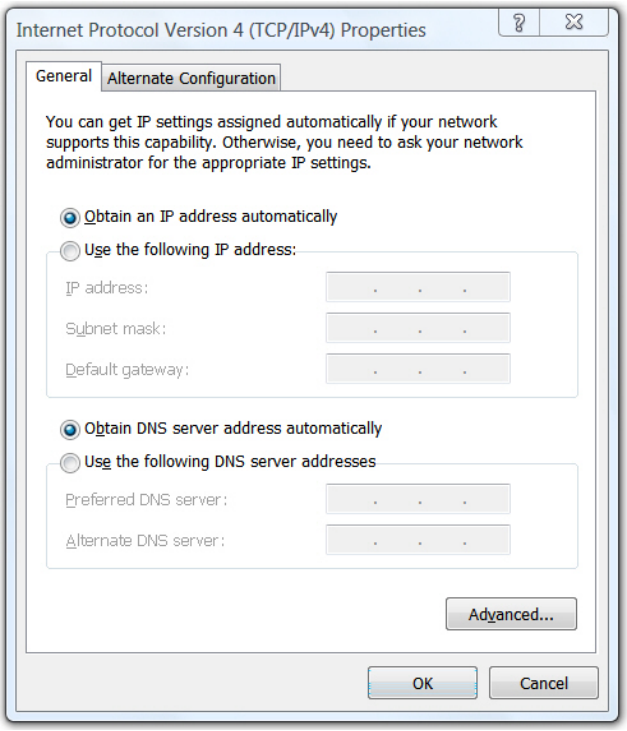
- If the ping command responds with '**Destination Host Unreachable'** or '**Timeout'**, the attempt to ping the VoloAccess has failed.

- If the attempt to ping the VoloAccess fails, check network connection setup on your Computer as follows:

In Windows XP:

- Load **Windows Control Panel** and double-click **Network Connections.**
- Under the heading **LAN or High-Speed Internet** right-click **Local Area Connection** and select **Properties**.
- Select **Internet Protocol (TCP/IP)** and click the **Properties** button.

  The adjacent dialog appears:

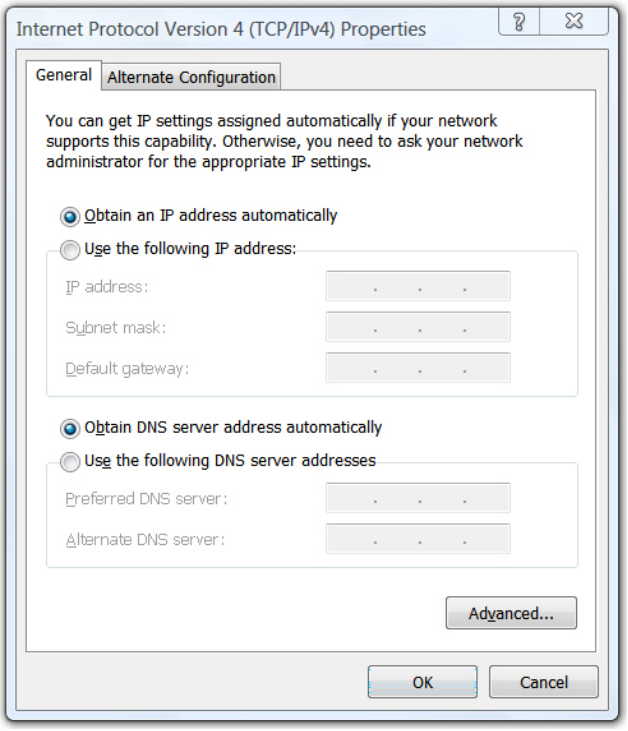


- Ensure that **Obtain an IP address** and **Obtain DNS Server** address are both set to **automatic**.

In Windows Vista:

- Load **Windows Control Panel** and double-click **Network and Sharing Center**.
- Next to **Local Area Connection**, click **View status**.
- The **Local Area Connection Status** window is displayed. Click the **Properties** button.
- The **Local Area Connection Properties** window is displayed. Select **Internet Protocol Version 4 (TCP/IPv4)** and click the **Properties** button.

  The adjacent dialog appears:



- Ensure that **Obtain an IP address** and **Obtain DNS Server** address are both set to **automatic**.

  The VoloAccess is a DHCP server and will provide both of these addresses.

When I try to connect to the VoloAccess Administration Web page at http://192.168.0.1, my Browser responds with the error "The Page Cannot be Displayed"

The most likely cause of this problem is your Browser is configured to use a proxy server.

In IE7 and IE8:

- From the **Tools** menu select **Internet Options** then click the **Connections** tab.
- Click on the LAN Settings button – the Local Area Network (LAN) Settings dialogs appears.
- Uncheck Use Proxy Server for your LAN.

In Firefox 3: (Windows version)

- From the **Tools** menu select **Options** – the Options dialog appears.
- Click the **Advanced** icon in the Toolbar.
- Click the **Network** tab – the Network dialog appears.
- Click the **Settings** button under **Connection**.
- Click the **No Proxy** radio button.
- Click the **OK** button (twice) to complete the task.

In Firefox: (Linux version)

- From the **Edit** menu select **Preferences** – the Firefox Preferences dialog appears.
- Click the **Advanced** icon in the Toolbar.
- Click the **Network** tab.
- Click the **Settings** button next to **Connection** – the Connection Settings dialog appears.
- Click the **No Proxy** radio button.
- Click **OK** then **Close** to complete the task.

If the above steps do not resolve the problem, check the Ethernet cable connection and the status of the LAN Indicators.

No Internet Access

I cannot access any Web pages.

- If you cannot access the Internet from any of your local devices, perform the following actions to identify and solve the problem:
- First check the Network Indicator, it should be solid On. If this is not the case refer to the instructions for Network Indicator.
- If the Network Indicator is On and flashing, refer to the instructions above for checking the Ethernet cable and how to ping the VoloAccess.
- On the **Admin > WAN > 3G Embedded** page, make sure that the **Network Status** is "Connected" and that an IP address is assigned.
- Still on the **Admin > WAN > 3G Embedded** page, ensure that the APN (Access Point Name) is configured according to the information from your service provider. (Found under the Settings heading.) Carefully check the spelling of the APN – one incorrect character and you will not be able to access the Internet.
- Make sure that the antennas are firmly connected to the VoloAccess.
- Check the Signal Strength indicator in Admin. If there is no display, a signal is not present. Check with your 3G service provider for a service outage.
- If the Signal Strength indicator is flashing, indicating a very weak signal, move the VoloAccess to another location. Refer to Setting up the VoloAccess™ for further information.

Voice/Data Problems

No voice

- Does your account with your Service Provider have voice support?
- Check the Telephone handset.

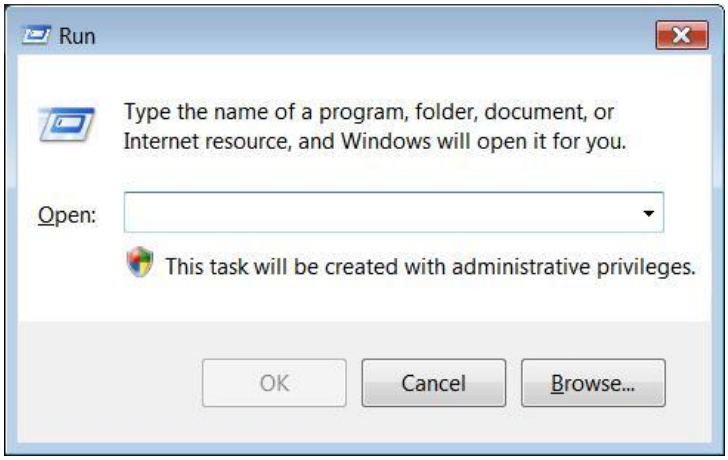
Low Data Throughput

- From the **Admin > Status** page, check the **Cellular Network Status**. The best connection speed will be available if it reports **Logged on WCDMA**. There is nothing that can be done to improve data throughput if the area you are using the VoloAccess in is not serviced by a high speed network.

LAN Problems

No LAN Connection

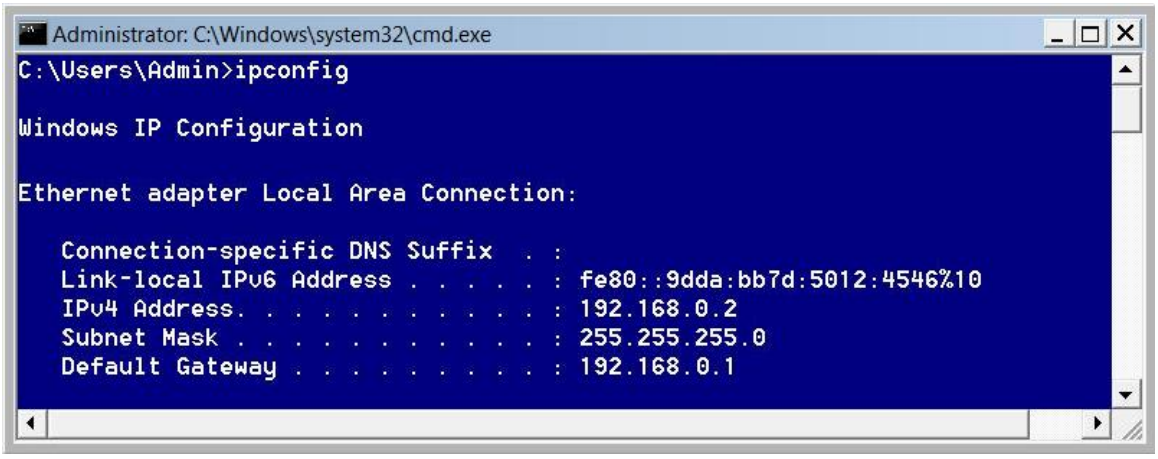
- If you cannot access the local network from a computer that is connected to the VoloAccess, perform the following actions to identify and solve the problem:
- Check that at least one of the LAN connector indicators is On. If not, check that the Ethernet cable is properly connected or try using another Ethernet cable. Also, the yellow Activity light on the computer's Network Interface Card (NIC) should flash if network traffic is present.
- Check that the computer is configured to obtain an IP address automatically using DHCP. If not, change the computer's TCP/IP settings. For further information, see Checking the Computer's network configuration or the manual of your operating system.
- Check that an IP Address has been allocated to your computer by the VoloAccess. To do this, proceed as follows:
- From the **Windows Start** menu select **Run**.
- The **Run** dialog appears.



- Enter **cmd** as the command to run and press **Enter**.

  The **Windows Cmd** window appears.
- Type **ipconfig** and press **Enter**.

  The **Windows IP Configuration** is displayed.



Under the heading **Ethernet adapter Local Area Connection** the IP address allocated to the computer by the VoloAccess is displayed. In this example, 192.168.0.2.

Supplementary Telephone Features (Voice enabled models only)

I picked up the handset and the phone starts dialing out after a brief period before I dial any numbers! Why?

This is most likely due to the **Default Dialing** feature being enabled and, with the **Timeout** set to a short period. You can disable this feature (see below) or, you can simply increase the timeout period to 10 seconds. This will provide an adequate delay before dialing a number.

To prevent this behavior, disable the **Default Dial** feature as follows:

- Load the Administration Web page at http://192.168.0.1.
- Select **Telephone** from the navigation panel.
- From the drop-down list next to **Default Dial** select **Disabled**.
- Click the **Apply** button.

I cannot enable Call Divert

- Check that the phone number is specified including the **International Dialing Prefix** and **Country Code**:
- From Admin, it is **+NN** (where NN is the International Dialing Prefix), and
- From the keypad, it is ****NN** (where NN is the International Dialing Prefix). **Note**: The **+** is entered as ****** when using the keypad.

  If you still cannot enable Call Divert, please contact your service provider, this service may not be enabled for your account.

I cannot disable Call Divert

- Contact your service provider and request that the service be disabled.

I enabled the Call Waiting feature but it does not work. Why?

- The **Call Divert** feature settings override **Call Waiting**. Check your **Call Divert** configuration.
- If you have enabled **Unconditional Call Divert** or **Call Divert on Busy**; it will prevent Call Waiting from working. You have to disable the above mentioned Call Divert features for Call Waiting to work.
- If the above step does not help, please contact your service provider.

Advanced Data Features

Port Forward

I have configured Port Forwarding for my Web Server but still cannot access the site. Why?

- First, check that the configuration settings are correct on the **Admin > LAN > Port Forward** page. The **Server IP** address is the IP address of your machine which is running the Web Server. The Protocol is **TCP**.
- The second thing to check is the firewall settings on the Web Server machine. Make sure that you are not filtering (blocking) the traffic and the port.

VPN

I have configured VPN but still cannot connect to the remote VPN server. How do I fix this?

- Verify that your 3G service provider provides an externally linkable (routable) IP address. This is the WAN IP Address which you can see on the **Admin > WAN > 3G Embedded** page. This address cannot be in the following (non-routable) ranges for VPN to operate:

  10.0.0.0 - 10.255.255.255

  172.16.0.0 - 172.31.255.255

  192.168.0.0 - 192.168.255.255

  These IP addresses have been reserved by the Internet Assigned Numbers Authority (IANA) for use by private (internal) networks.

  It is a known issue that some ISPs do provide internal (non-routable) IP addresses, in which case your VoloAccess cannot be configured as a VPN host.

- VPN has strict rules for security reasons. The credentials on both the remote server and your local client have to match for VPN to work. You need to provide your WAN IP Address to your VPN Server administrator and obtain the Server's host and network details and the authentication key to be configured in Admin.
- Each time you turn your VoloAccess off and on, your service provider allocates a new WAN IP Address unless your account has a static address. (A static IP address can be arranged with your 3G service provider) If your WAN IP Address is dynamic (changes each time), you will need to notify your VPN Server's administrator to update the connection details on the Server side.

Time Server

The VoloAccess displays incorrect date and time. Why?

- If after 15 minutes, the VoloAccess still doesn't display the correct date and time, check that a Time Server has been enabled in Admin.

If NITZ is selected as the Time Server, the Date/Time update should occur in a matter of seconds; however, an NTP Time Server can take considerably longer to respond.

- Refer to Setting the Date and Time in the User Manual for further information.

VoloAccess fails to start normally

If the VoloAccess has been started, but the WiFi Protected Setup, Signal Strength and Mobile Network indicators repeatedly flash at 1 second intervals, the software is trying to load but failing.

Perform the following actions to solve the problem:

- Turn the VoloAccess off, wait for 30 seconds, then turn it on – the WiFi Protected Setup, Signal Strength and Mobile Network indicators flash at 1 second intervals until ready to enter normal operation.
- While the unit is in the flashing sequence, push the reset button for more than 10 seconds – this performs a hard reset.
- Wait for the VoloAccess to restart and check its operation.

If the VoloAccess fails to start normally, return the unit for repair.

It is important that the reset button is pressed during the flashing sequence.

WiFi Problems

Unable to connect wirelessly to the VoloAccess.

Check the following WiFi configuration items – connect the VoloAccess to a computer using an Ethernet cable, then using a Browser load Admin and select **WiFi** from the navigation panel.

- If the computer is situated a long way from the VoloAccess or there is a wall or partition containing metal in between, try moving the computer closer to the VoloAccess. All diagnostic measures should be performed with the two wireless devices in line-of-sight and in close proximity.
- Ensure that WiFi is enabled.
- Try using a different channel – interference from another wireless device or appliance that uses the same frequency range (2.4 GHz) may be causing connection problems.
- If **Broadcast SSID** is disabled, try enabling it and attempt to reconnect. Some wireless equipment can have difficulty connecting with the SSID broadcast disabled.
- Check that the **SSID** (also known as Network Name) is spelled exactly the same in the VoloAccess' WiFi configuration and the computer's wireless network setup. The SSID is case sensitive.
- Check that the **Security Mode** (also known as Network Authentication) is the same in the computer's WiFi setup as was configured on the VoloAccess.
- Check that the **Encryption Key** or **Pre-Shared Key** is the same in the computer's WiFi setup as was configured on the VoloAccess.
- Remove the Ethernet cable.
- Restart the VoloAccess and the computer, then attempt to reconnect.

If the above does not correct the problem, try the following:

Windows XP

- From the **Windows® Start Menu** select **Control Panel** and double-click **Network Connections**.
- Right-click on **Wireless Network Connection**.
- From the menu select **Repair** – Windows® Network Connections will disable, then re-enable the wireless adapter in the computer - it will then attempt to obtain a new IP address.

Windows Vista

- From the **Windows® Start Menu** select **Control Panel** and click **Network and Internet**.
- Under **Tasks** click **Diagnose and repair**.
- Windows will attempt to diagnose and repair the problem.

Intermittent disconnection from the Wireless LAN

- This is probably caused by interference from another wireless device like a cordless phone or an appliance that uses the same 2.4 GHz frequency. To overcome this try using a different channel.
- Load Admin and select **WiFi** from the navigation panel.
- Change the **Channel** using the drop-down list, then click the **Apply** button.

Connected to the VoloAccess but cannot connect to the Internet

Once the computer has successfully connected wirelessly to the VoloAccess, the same causes as a wired setup prevail. See the No Internet Access section for further assistance.

Glossary

A

ADSL – **A**symmetric **D**igital **S**ubscriber **L**ine. Transmits high-speed data downstream to the end user and lower-speed data upstream toward the network. Many wired broadband services use ADSL.

APN – **A**ccess **P**oint **N**ame. The name of a 3G service provider's wireless access point.

B

Broadband – A term used when describing the bandwidth or capacity needed to carry multiple voice, video or data channels simultaneously. Broadband technology was introduced to help deliver increased amounts of speeds and advanced capabilities. These advancements now give consumers better access to the Internet, related services, and facilities.

BSSID – **B**asic **S**ervice **S**et **I**dentifier - the BSSID is the MAC address of a wireless access point.

C

CHAP – **C**hallenge **H**andshake **A**uthentication **P**rotocol. CHAP is used in PPP authentication to verify the identity of a peer system.

Convergent Wireless Terminal – A single wireless terminal that can be used to access different services offered by different networks.

D

DHCP – **D**ynamic **H**ost **C**onfiguration **P**rotocol. A set of rules used by communications devices such as a computer, router or network adapter to allow the device to request and obtain an IP address from a server which has a list of addresses available for assignment. See also Static DHCP

DNS – **D**omain **N**ame **S**ystem. The Domain Name System associates various information with domain names; most importantly, it serves as the "phone book" for the Internet by translating human-readable computer hostnames, e.g. www.vololink.com, into IP addresses, e.g. 208.77.188.166, which networking equipment needs to deliver information.

DDNS - **D**ynamic **D**omain **N**ame **S**ystem. A method, protocol, or network service that provides the capability for a networked device using the Internet Protocol Suite, such as an IP router or computer system, to notify a domain name server to change, in real time, the active DNS configuration of its configured hostnames, addresses or other information stored in DNS.

DTMF – **D**ual **T**one **M**ulti-**F**requency. Frequency signalling is used for telephone signalling over the line in the voice-frequency band to the call switching center.

E

EDGE – **E**nhanced **D**ata **G**SM **E**nvironment. A faster version of the GSM standard. It is faster than GSM because it can carry messages using broadband networks that employ more bandwidth than standard GSM networks.

F

Failover – WAN Failover is the capability to switch automatically to a secondary network when the primary network fails.

Frequency – Assigned channel space within the radio wave spectrum.

G

GPRS – **G**eneral **P**acket **R**adio **S**ervice. A technology that sends packets of data across a wireless network at speeds of up to 114Kbps. It is a step up from the circuit-switched method; wireless users do not have to dial in to networks to download information. With GPRS, wireless devices are always on - they can receive and send information without dial-ins. GPRS is designed to work with GSM.

GSM – **G**lobal **S**ystem for **M**obile (Communications). GSM is a digital mobile telephone system that is widely used in Europe and other parts of the world. GSM uses a variation of Time Division Multiple Access (TDMA). Since many GSM network operators have roaming agreements with foreign operators, users can often continue to use their mobile phones when they travel to other countries.

H

HSPA – **H**igh **S**peed **P**acket **A**ccess refers to UMTS based 3.5G networks that support both HSDPA and HSUPA data for improved download and upload speeds.

HSPA+ – Also referred to as High Speed Packet Access (HSPA) Evolved or enhanced HSPA. Supports peak data rates of up to 42 Mbps on the downlink and up to 11 Mbps on the uplink. HSPA+ doubles data capacity and triples voice capacity providing more efficient and lower cost broadband.

HSDPA – **H**igh **S**peed **D**ownload **P**acket **A**ccess is a 3.5G mobile telephony communications protocol in the High-Speed Packet Access (HSPA) family, which allows networks based on Universal Mobile Telecommunications System (UMTS) to have higher data transfer speeds and capacity.

HSUPA – **H**igh **S**peed **U**plink **P**acket **A**ccess. An upgrade to UMTS that allows for uplink connections as fast as 5.76Mbps, compared to HSDPA which allows uplink connections of up to 2Mbps.

HTTP – **H**yper**T**ext **T**ransfer **P**rotocol. The protocol used by the Web server and the client browser to communicate and move documents around the Internet.

I

IMEI – The **I**nternational **M**obile **E**quipment **I**dentity is a number unique to every GSM and UMTS mobile phone. It is usually found printed on the phone underneath the battery and can also be found by dialling the sequence *#06# into the phone. The IMEI number is used by the GSM network to identify valid devices and therefore can be used to stop a stolen phone from accessing the network.

IMSI – **I**nternational **M**obile **S**ubscriber **I**dentity. The IMSI number is a unique 15-digit code that is attached to every SIM and makes it possible for mobile networks to identify the home country and network of a subscriber.

ISP – **I**nternet **S**ervice **P**rovider. An Internet service provider is a business or organization that provides consumers or businesses access to the Internet and related services.

K

Kbps – **k**ilo**b**its **p**er **s**econd. A kilobit per second is a unit of data transfer rate equal to 1,000 bits per second.

L

LAN – **L**ocal **A**rea **N**etwork. A LAN is a computer network covering a small geographic area, like a home, office, or group of buildings.

M

MAC – **M**edia **A**ccess **C**ontrol address

A MAC address is a unique value associated with a network adapter. The MAC address is also known as hardware address or physical address. It uniquely identifies an adapter on a LAN. A MAC address is a 12-digit hexadecimal number (48 bits in length). By convention, a MAC address is usually written in one of the following two formats:

MM:MM:MM:SS:SS:SS

MM-MM-MM-SS-SS-SS

The first half of a MAC address contains the ID number of the adapter manufacturer. The second half of a MAC address represents the serial number assigned to the adapter by the manufacturer.

MTU – **M**aximum **T**ransmission **U**nit. The size of the largest packet that a network protocol can transmit.

N

NAT – **N**etwork **A**ddress **T**ranslation. NAT is a technique of transceiving network traffic through a router that involves re-writing the source and/or destination IP addresses and usually also the TCP/UDP port numbers of IP packets as they pass through.

P

PABX – **P**rivate **A**utomatic **B**ranch e**X**change. A PABX is a telephone exchange that serves a particular business or office, as opposed to one that a telephone company operates for the general public.

PAP – **P**assword **A**uthentication **P**rotocol. PAP is used in PPP authentication to verify the identity of a peer system.

PBC – **P**ush **B**utton **C**onfiguration.

PIN – **P**ersonal **I**dentification **N**umber. A PIN is a secret numeric password shared between a user and a system that can be used to authenticate the user to the system.

PPP – **P**oint to **P**oint **P**rotocol. PPP is used to establish an authenticated connection between two host systems. The authentication is in the form of a Username and Password pair known to both hosts.

Protocol – The rules of order by which a communications network is operated.

PUK – **P**ersonal **U**nlocking **K**ey. Used in GSM mobile phones to unlock a locked SIM.

R

RF – **R**adio **F**requency is the frequency or rate of oscillation of a radio signal.

S

SIM – **S**ubscriber **I**dentity **M**odule. A SIM is a removable card for mobile cellular telephony devices such as mobile computers and mobile phones. A SIM securely store the service-subscriber key used to identify a subscriber. The SIM allows users to change phones by simply removing the SIM from one mobile phone and inserting it into another mobile phone.

SMS – **S**hort **M**essaging **S**ervice. A service through which users can send text based messages from one device to another.

SSID – **S**ervice **S**et **I**dentifier. A SSID (also known as Network Name) is a name used to identify a 802.11 wireless LAN.

Static DHCP - Static DHCP is a feature which makes the DHCP server on your router (VoloAccess) always assign the same IP address to a specific computer on your LAN.

T

TCP/IP – **T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol. The basic communication language or protocol of the Internet.

U

UPnP™ – **U**niversal **P**lug a**n**d **P**lay. A set of computer network protocols that allow devices to connect seamlessly and to simplify the implementation of networks (data sharing, communications, and entertainment) in the home and corporate environments.

UMTS – **U**niversal **M**obile **T**elecommunications **S**ystem. UMTS is a so-called 'third-generation (3G),' broadband, packet-based transmission of text, digitised voice, video, and multimedia.

SIM – **U**niversal **S**ubscriber **I**dentity **M**odule. A SIM is an application for UMTS mobile telephony which is inserted in a 3G mobile phone.

V

VoIP – **V**oice **o**ver **I**nternet **P**rotocol. A term used in IP telephony for a set of facilities for managing the delivery of voice information using the Internet Protocol (IP).

VPN – **V**irtual **P**rivate **N**etwork. A VPN is a communications network tunnelled through another network. One common application is secure communications through the public Internet.

W

WAN – Wide **A**rea **N**etwork. A WAN is a computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries). The largest and most well-known example of a WAN is the Internet.

WEP – Wired **E**quivalent **P**rivacy. WEP is a (now superseded) algorithm to secure IEEE 802.11 wireless networks. WEP was intended to provide confidentiality comparable to that of a traditional wired network; however several serious weaknesses have been identified with the result that a WEP connection can be cracked with readily available software within minutes. WEP has been superseded by Wi-Fi Protected Access (WPA).

WCDMA – **W**ideband **C**ode **D**ivision **M**ultiple **A**ccess. WCDMA is a type of 3G cellular network. WCDMA is the higher speed transmission protocol used in the UMTS system, a third generation follow-on to the 2G GSM networks deployed worldwide.

WiFi – **Wi**reless **Fi**delity. is the marketing name for the wireless technology used in computers, mobile phones, PDAs, gaming consoles and more. It covers the various 802.11 technologies.

WPA – **W**iFi **P**rotected **A**ccess. WPA is a security protocol used to secure wireless computer networks. This protocol implements most of the IEEE 802.11i standard.

WPA2 – **W**iFi **P**rotected **A**ccess version **2**. An advanced more secure form of the WPA protocol that implements all of the mandatory elements of the IEEE 802.11i standard. This advanced protocol will not work with some older network cards.

WPS – **W**iFi **P**rotected **S**etup. - A standard for easy and secure establishment of a wireless network.

Technical Specification

VoloAccess™

VA100 Series 3G+ Convergent Wireless Terminal with WiFi

Features

- The VoloAccess is a Convergent Wireless Terminal for use over HSPA+ capable UMTS networks.
- The VoloAccess provides both voice and wireless broadband Internet services in areas where conventional telephone lines either do not exist or are too far from the nearest xDSL enabled exchange.
- The VoloAccess is easy to use, just plug and play.
- Broadband Internet access via four Ethernet ports or high speed WiFi.
- Support for analog phone(s) via RJ11 ports. (Voice enabled models only).
- The VoloAccess provides Least Cost Routing between enterprise fixed line PBXs and 3G wireless networks.
- Automatic fall back to HSUPA/ HSDPA/EDGE/GPRS/GSM, if a HSPA+ network is not available.
- Supports locking the terminal to the 3G network (network lock).
- Supports locking the SIM to the terminal (SIM PIN lock).
- Automatic updates of the latest firmware via 'Over The Air' download feature.
- Built-in internet redundancy (IP failover) via either WAN port or externally connected 3G USB modem.
- Flexible design - Voice and Data or Data only.
- Optional rechargeable Li-ion battery pack for continuous operation during power failures.

Vololink
the future is wireless

Vololink Pty Ltd
Melbourne, Australia
sales@vololink.com
www.vololink.com

3G+ Wireless Network
- Air Interface: WCDMA
- GSM/GPRS/EDGE frequencies: 850/900/1800/1900MHz

WLAN
- 802.11b/g/n WiFi access point
- 2.4000~2.4835GHz (ISM Band)
- 2 x 2 MIMO
- WiFi Protected Setup

Internet Protocols
- DHCP server
- PPP client
- NAT
- NAT port forwarding
- NAT ALGs
- DNS proxy server
- SNTP client

Security
- Firewall
- VPN tunnelling
- VPN pass-through
- WLAN - 64/128-bit WEP, WPA and WPA2

Indicators
- Power, Mobile network status, Signal strength, 4 x LAN, WAN, WLAN, Phone 1, Phone 2, WPS

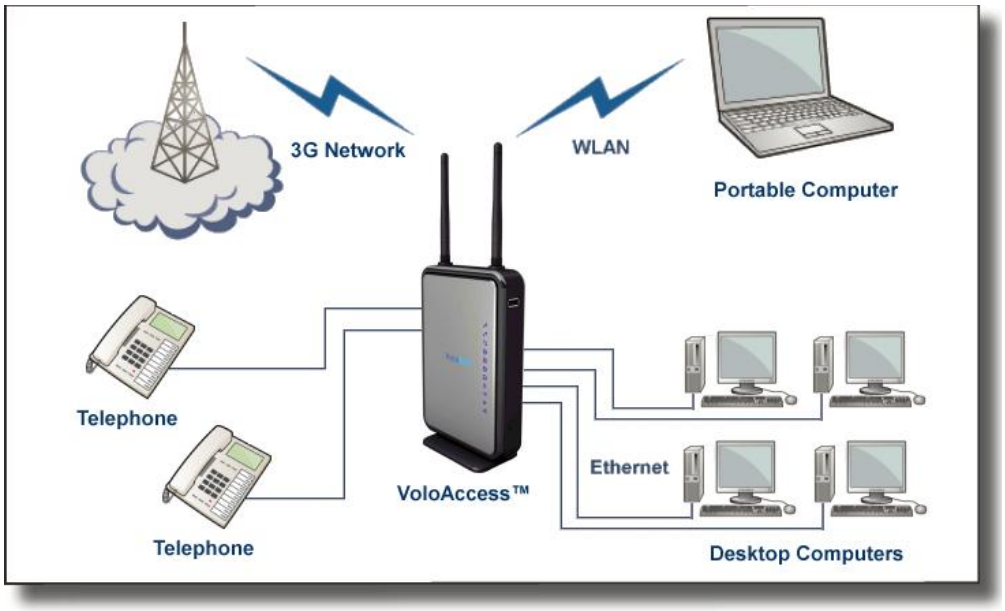
Connectors
- Four RJ45 Ethernet ports
- Two antenna connectors (SMA 50 ohm)
- Connector for external SIM
- DC power supply
- Two RJ11 connectors (Voice enabled models only)
- RJ45 WAN port
- USB host port

Antenna
- Dual external omni-directional, 50 ohm (3G)
- Dual internal omni-directional, 50 ohm (WLAN)
- Optional higher gain directional 3G antennas and extension cables available

Environment
- Operating temperature: 0° to +45°C
- Storage temperature: -20° to +70°C
- Operating humidity: 5% to 95%

AC-to-DC Power Supply
- Input: 100 – 240V/50 – 60Hz AC
- Output: +12V 2A DC
- Plug options: Australia, Europe, UK, USA
- Rechargeable Li-ion battery pack (optional)

Dimensions
- 178 x 118 x 33 mm (excluding stand and antennas)



Appendix

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.