

TELSTRA ELITE® GATEWAY

USER GUIDE

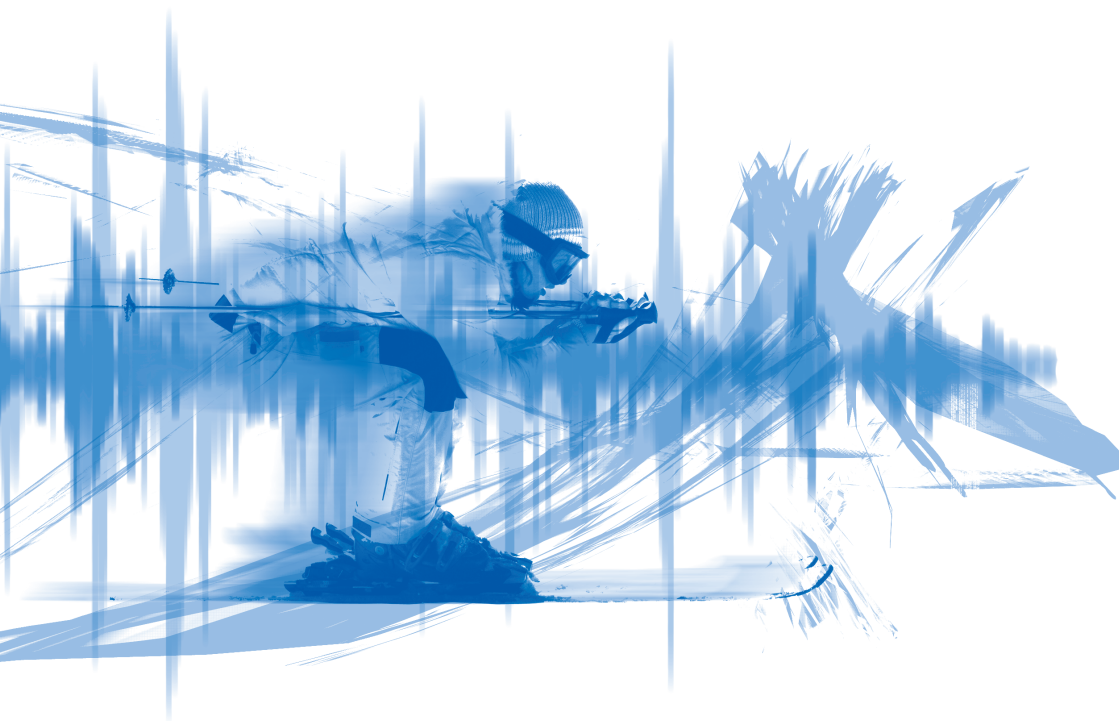


TABLE OF CONTENTS

1 – GETTING STARTED	7
1.1 Features.....	7
1.2 Package Contents	8
1.3 LED Indicators.....	9
1.4 Panels	10
2 – QUICK SETUP	12
2.1 Setup Procedure (with USB Key)	12
3 – ADVANCED SETUP	14
3.1 Setup Procedure (without USB Key).....	14
3.2 TCP/IP Settings.....	14
3.3 Default Settings.....	21
3.4 Login Procedure	22
4 – BASIC	24
4.1 Web User Interface Homepage.....	24
5 – NEXT G™ SETTINGS	27
5.1 Next G™ Service Setup	27
5.1.1 Profile Setup	27
5.2 Signal Selection.....	29
5.3 PIN Configuration	30
5.3.1 PIN Code Protection	30
5.3.2 PIN Code Change.....	33
6 – WI-FI	35
6.1 Settings	36
6.2 Security	38
6.3 Configuration	40
6.4 MAC Filter	43
6.5 Wireless Bridge	44
6.6 Station Info.....	45

7 – MANAGEMENT	47
7.1 Device Settings	47
7.1.1 Backup Settings	47
7.1.2 Update Settings	48
7.1.3 Restore Default	48
7.1.4 Update Firmware	49
7.2 Access Control.....	50
7.2.1 Services.....	50
7.2.2 Passwords	51
7.3 Configure SNMP agent	52
7.4 Simple Network Time Protocol (SNTP)	53
7.5 Save and Reboot.....	54
8 – ADVANCED SETTINGS	56
8.1 Local Area Network (LAN)	56
8.2 Network Address Translation (NAT)	58
8.2.1 Port Forwarding	58
8.2.2 Port Triggering	60
8.2.3 Demilitarized (DMZ) Host.....	62
8.3 Security	63
8.3.1 IP Filtering.....	63
8.3.2 Parental Control.....	65
8.4 Routing.....	67
8.4.1 Static Route	67
8.4.2 Dynamic Route	68
8.5 Domain Name Server (DNS)	69
8.5.1 DNS Server Configuration	69
8.5.2 Dynamic DNS.....	69
8.6 USB Print Server.....	71
8.7 USB Storage.....	82
9 – DIAGNOSTICS.....	88
9.1 Diagnostics	89
9.2 System Log	91
9.3 Next G™ Network.....	93
9.4 Statistics.....	95
9.4.1 LAN Statistics.....	95
9.4.2 Next G™ Statistics	95
9.5 Route	96
9.6 ARP	97
9.7 Dynamic Host Configuration Protocol (DHCP)	98
9.8 PING.....	99

INTRODUCTION

INTRODUCTION

Welcome to Telstra Wireless Broadband – Thanks for choosing us!

This guide is designed to help you get the most out of your Telstra Wireless Broadband experience. We're sure you're itching to get started, so don't feel that you have to study the entire user guide right away. However! It's important to read through the Quick Setup section to ensure you set up your TELSTRA ELITE® GATEWAY correctly. The rest will be there when you need it.

As a Telstra Wireless Broadband Member, you can now enjoy a huge range of Internet services, including state of the art security options, great account tools, flexible plans, extra email features, worlds of 'unmetered' content, special shopping deals and lots more.

So let's get started.

GETTING STARTED

GETTING STARTED

1.1 FEATURES

- Combines Next G™ Broadband service, Wi-Fi and an Ethernet gateway in one device
- Dual-band HSPA+/UMTS (850 / 2100 MHz)
- Embedded multimode HSUPA/HSDPA/HSPA+/UMTS module
- 2 x USB 2.0 host ports
- WEP/WPA/WPA2 and 802.1x
- SIM card PIN configuration
- MAC address and IP filtering
- Static route functions
- DNS Proxy
- Integrated 802.11n AP (backward compatible with 802.11b/g)
- CLI command interface
- Web-based management
- Support Telstra IP WAN service
- Support Telstra IP Telephony on LAN port
- Supports Half-bridging
- NAT/PAT
- DHCP Server/Relay/Client
- Configuration backup and restoration



1.2 PACKAGE CONTENTS

Your package contains the following:

- TELSTRA ELITE® GATEWAY
- Printed Quick Start Guide
- USB key (Containing Telstra Connection Manager and User Guide)
- Ethernet Cable
- Security Card
- Power Supply

1.3 LED INDICATORS

The LED indicators are explained in the table below.

LED	Icon	Color	Mode	Description
High		Blue	On	High signal strength
			Off	No activity, gateway powered off or on other signal strength
Med		Blue	On	Medium signal strength
			Off	No activity, gateway powered off or on other signal strength
Low		Blue	On	Low signal strength
			Off	No activity, gateway powered off or on other signal strength
3G		Blue	On	Connection established with the 3G network
			Off	Either there is no activity, the gateway is powered off, or there is no cable or no powered device connected to the associated port
			Blinking	Connecting with 3G network
2G		Blue	On	Connection established with the 2G network
			Off	Either there is no activity, the gateway is powered off, or there is no cable or no powered device connected to the associated port
			Blinking	Connecting with 2G network
LAN 1~4		Blue	On	Powered device connected to the associated LAN port (includes devices with Wake-on-LAN capability where a slight voltage is supplied to an Ethernet connection)
			Off	No device connected or connected device is off
			Blinking	LAN activity present (traffic in either direction)
Internet		Blue	On	Internet connection established
			Off	No connection to the Internet or gateway powered off
			Blinking	Data is currently being transmitted through the Internet connection
Wi-Fi		Blue	On	Local Wi-Fi access to the gateway is enabled and working
			Off	Local Wi-Fi access to the gateway is disabled
			Blinking	Data being transmitted or received over Wi-Fi.
POWER		Blue	On	Power on
			Off	Power off

1.4 PANELS

The rear and side panels shown below contain the ports for data and power connections.



- (1) USIM card slot
- (2) Four RJ-45 Ethernet LAN ports
- (3) Reset button
- (4) Power jack for DC power input (12VDC / 1.5A).
- (5) External 3G SMA Connector (Optional)

Note: The External 3G Connector allows you to plug in an external 3G antenna (not provided) and select it as the main 3G signal input. By default, the gateway obtains a stable 3G signal from the internal antennas (built-in the gateway). For more details please refer to Chapter 5.2 Signal Selection.

- (6) Two USB Printer/Hard Drive ports
- (7) Power Button

QUICK SETUP

QUICK SETUP

2.1 SETUP PROCEDURE (WITH USB KEY)

These steps explain how to quickly setup your Next G™ Gateway:

- 1: Insert your SIM card (until you hear a click) into the USIM slot on the rear of the gateway.
- 2: Connect the yellow Ethernet cable to one of the yellow LAN ports found on the back of the gateway.
- 3: Connect the other end of the yellow networking cable to the Ethernet port on your computer.
- 4: Connect the power adapter to the power socket on the back of the gateway.
- 5: Plug the power adapter into a wall socket and press the power button into the ON position.
- 6: Configure the gateway through the Web User Interface (WUI).

NOTE: [Chapters 4 through 8](#) explain how to set up and use the WUI

- 7: Save the gateway configuration and reboot (see section 7.5).

ADVANCED SETUP

3.1 SETUP PROCEDURE (WITHOUT USB KEY)

These steps explain how to quickly setup your Next G™ Gateway:

- 1: Insert your SIM card (until you hear a click) into the USIM slot on the rear of the gateway.
- 2: Connect the yellow Ethernet cable to one of the yellow LAN ports found on the back of the gateway.
- 3: Connect the other end of the yellow networking cable to the Ethernet port on your computer.
- 4: Connect the power adapter to the power socket on the back of the gateway.
- 5: Plug the power adapter into a wall socket and press the power button into the ON position (depressed).
- 6: Configure the gateway through the Web User Interface (WUI).

NOTE: Chapters 4 through 8 explain how to set up and use the WUI

- 7: Save the gateway configuration and reboot (see section 7.5).

3.2 TCP/IP SETTINGS

It is likely that your computer will automatically obtain an IP Address and join the network. This is because the Dynamic Host Configuration Protocol (DHCP) server (on the device) will start automatically when your gateway powers up.

This automatic assignment requires that DHCP is configured on your computers. It is likely that this is already the case but should you be required to configure this, please see the instructions on the following page.

WINDOWS XP

To access the dialog box that allows you to configure your network connection, click on Start > Control Panel > Network Connections. Then right mouse click on the Local Area Connection and select Properties. Select Internet Protocol (TCP/IP) then select Properties

DHCP MODE

You can set your PC to DHCP mode by selecting Obtain an IP address automatically in the dialog box shown below.

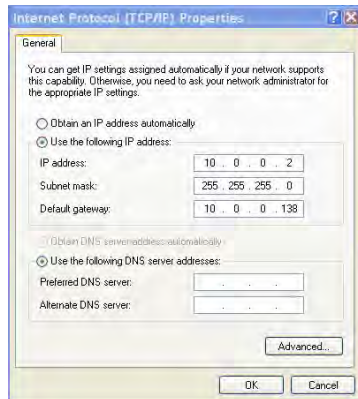


STATIC IP MODE

The following steps show how to assign a Static IP address to your PC using subnet 10.0.0.x.

- 1: Set the IP address to 10.0.0.x. (where x is a number between 1 and 254) with subnet mask of 255.255.255.0.
- 2: Set the default gateway and DNS server to the gateway's IP address.

NOTE: The IP address of the gateway is 10.0.0.138. (Default), so the PC must be set with a different IP. In the case below, the PC's IP address is set as 10.0.0.2



- 3: Click OK to submit the settings.

MAC OSX 10.4

To access the dialog box that allows you to configure your network connection, browse to the Apple menu and select System Preferences. From the System Preferences menu, click the Network icon and then select the Ethernet connection.

DHCP MODE

You can set your Mac to DHCP by selecting DHCP from the Configure drop down list. After clicking Apply, your Mac's IP Address will now be automatically assigned from the gateway.



STATIC MODE

1. From the Configure drop down list, you can set your computer to Static IP mode by selecting the option Manually.



The following steps show how to assign a Static IP address to your Mac

2. Set the IP address to 10.0.0.x. (where x is a number between 1 and 254) with subnet mask of 255.255.255.0.
3. Set the default gateway and DNS server to the gateway's IP address.

NOTE: The IP address of the gateway is 10.0.0.138. (default), so the computer must be set with a different IP to the gateway. In the case below, the PC's IP address is set as 10.0.0.2



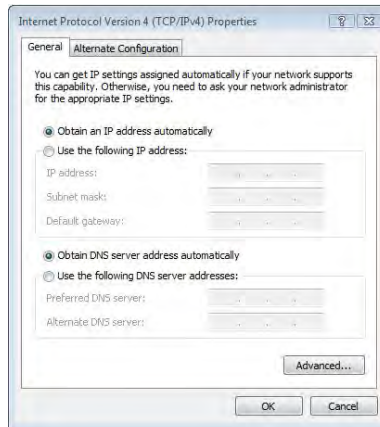
4. Click Apply to submit the settings.

WINDOWS VISTA

To access the dialog box that allows you to configure your network connection, click on Start > Control Panel > Network Connections. Then right mouse click on the Local Area Connection and select Properties. Select Internet Protocol (TCP/IP) then select Properties

DHCP MODE

You can set your PC to DHCP mode by selecting Obtain an IP address automatically in the dialog box shown below.

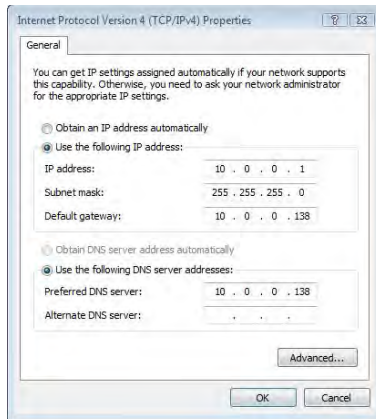


STATIC IP MODE

To configure your gateway manually, your PC must have a static IP address within the gateway's subnet. The following steps show how to assign a Static IP address to your PC using subnet 10.0.0.x.

- 1: Set the IP address to 10.0.0.x. (where x is a number between 1 and 254) with subnet mask of 255.255.255.0.
- 2: Set the default gateway and DNS server to the gateway's IP address.

NOTE: The IP address of the gateway is 10.0.0.138. (default), so the PC must be set with a different Ip. In the case below, the PC's IP address is set as 10.0.0.1



3. Click OK to apply the settings.

3.3 DEFAULT SETTINGS

The following are the default settings for the gateway:

- Local (LAN) access (username: admin, password: admin)
- Remote (WAN) access (username: support, password: support)
- User access (username: user, password: user)
- LAN IP address: 10.0.0.138
- Remote WAN access: disabled
- NAT and firewall: enabled
- Dynamic Host Configuration Protocol (DHCP) server on LAN interface: enabled

Technical Note:

During power on, the device initializes all settings to default values. It will then read the configuration profile from the permanent storage section of flash memory. The default attributes are overwritten when identical attributes with different values are configured. The configuration profile in permanent storage can be created via the web user interface, telnet user interface, or other management protocols. The factory default configuration can be restored either by pushing the reset button for more than five seconds until the power LED blinks or by clicking the Restore Default Configuration option in the Restore Default Settings screen (see section 7.1.3).

3.4 LOGIN PROCEDURE

To login to the web interface, follow the steps below:

NOTE: The default settings can be found in 3.3 Default Settings.

- 1: Open a web browser and enter the default IP address for the gateway in the Web address field at the top of the web browser window. In this case, the address is <http://10.0.0.138>

NOTE: For remote access, the WAN IP address assigned to the gateway needs to be a public IP address. It is shown on the WUI Homepage screen. The remote WAN access via HTTP also needs to be enabled, for details please refer to chapter 7.2.

- 2: A dialog box will appear as illustrated below. Enter the default username and password as defined in section 3.3 Default Settings.



Click OK to continue.

NOTE: The login password can be changed later (see 7.2.2 Passwords)

BASIC

BASIC

4.1 WEB USER INTERFACE HOMEPAGE

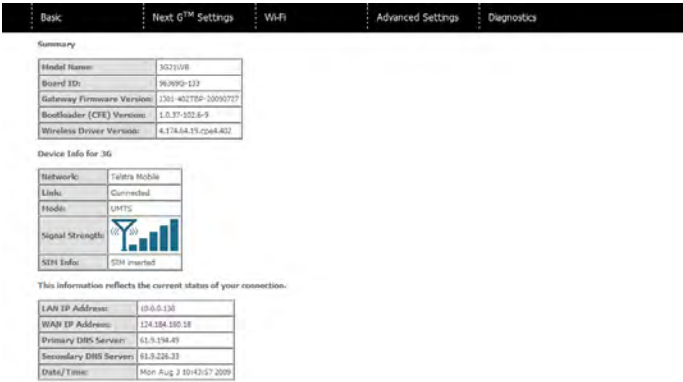
The web user interface (WUI) is divided into two window panels, the main menu (on the top) and the display screen (on the bottom). The main menu has the following options: Basic, Next G™ Settings, Wireless, Management, Advanced and Status.

Selecting one of these options will open a submenu with more options. Basic is discussed below while subsequent chapters introduce the other main menu selections.

NOTE: The menu options available within the web user interface are based upon the device configuration and user privileges (i.e. local or remote).

BASIC / HOME

The Basic / Home screen is the WUI homepage and the first selection on the main menu. It provides information regarding the firmware, 3G, and the IP configuration.



The following table provides further details.

Option	Description
Model Name	The model name of the device.
Board ID	The hardware version of the device
Bootloader version	The bootloader version of the device.
Gateway Firmware version	The firmware version of the device.
Wireless driver version	The wireless driver version of the wireless module.
MAC Address	The MAC address of the device's LAN interface.
Serial Number	The Serial Number of the device.
Network	The name of or other reference to the mobile network operator.
Link	Shows the connection status of the current Next G™ connection.
Mode	The radio access technique currently used to enable Internet access. It can be HSPA, HSDPA, UMTS, or Disconnected.
Selected Signal input	The 3G signal input currently selected by the gateway. It can be either Internal or External antenna(s)
Signal strength	The mobile network (UMTS) signal quality available at the device location. This signal quality affects the performance of the unit. If two or more bars are blue, the connection is usually acceptable.
SIM info	Shows the SIM card status on the device.
LAN IP Address	Shows the IP address for LAN interface.
WAN IP Address	Shows the IP address for WAN interface.
Primary DNS Server	Shows the IP address of the primary DNS server.
Secondary DNS server	Shows the IP address of the secondary DNS server.
Date/Time	The time according to the device's internal clock

NEXT G™ SETTINGS

NEXT G™ SETTINGS

This menu includes Next G™ service Setup.

NOTE: Sections 8.3 and 8.4.2 also provide information about the Next G™ service.

5.1 NEXT G™ SERVICE SETUP

Select your next Next G™ service settings according to predefined or custom profiles. Setup instructions are provided in the following sections for your assistance.

5.1.1 PROFILE SETUP

Telstra will provide the information required to complete the first time setup instructions below.

For most users this includes a profile; for others this may also includes the authentication method, username and password. Only complete those steps for which you have information and skip the others.

1. If your SIM card is not inserted into the gateway, please turn the gateway off, then insert the SIM and turn the gateway on.
2. Select one of the two pre-configured APNs from the drop-down list or type the APN in the APN field. Authentication method (visible when Custom APN is selected) should be provided by Telstra; or just leave it AUTO if not acquired required. If you have not received the username and password, leave these fields empty and select AUTO authentication.



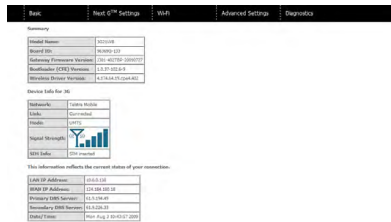
3. Some users may require deleting the two pre-configured Telstra APNs from the web interface if they do not need to use those services. They can do this by selecting the option below, and then click the Save button.



4. Click the Save button to save the new settings.
5. Press the Connect button to connect to Internet. The Device Info for 3G network box in the WUI Basic screen should indicate an active connection, as shown below. The 3G and Internet LEDs on the front panel of the gateway should also be blinking.

Note: You can also delete the pre-configured APNs permanently from the installation Software (the USB key). For PC users, please plug the USB key into your PC and click on DeletePreSetAPN.exe. Click Run to confirm deleting the pre-configured APN permanently. For Mac OS users, please double click into the folder named Mac. Click on DeletePreSetAPN.app and then click Yes to delete the pre-set APN information.

6. Select IP compression and Data compression to be on or off. By default they are set to off.
7. Select Band option for 2G/3G connection. By default it is set to 3G 850 MHz only.
8. Click the Save button to save the new settings.
9. Press the connect button to connect to Internet. The Device Info for 3G network box in the WUI Basic screen should indicate an active connection, as shown below. The 3G and Internet LEDs on the front panel of the gateway should also be blinking.



If the LEDs are off, then either your profile settings are incorrect, the SIM card is not working or the 3G service is unavailable. Contact Technical Support for further instructions.

NOTE: If the LEDs light blink in an on/off pattern this indicates that your SIM is PIN Locked, please see PIN Lock off in the 5.3 PIN Configuration section for instructions on how to fix this.

5.2 SIGNAL SELECTION

Signal Selection allows you to manually select the 3G signal input to be either the internal antennas or an external antenna (not included). By default, a stable signal is obtained from the antennas built into the gateway. To use an external 3G antenna, please connect it to the Antenna Connector next to the Power Input on the back of the gateway.

If the external antenna does not support 850 MHz frequency, please go to Next G Settings > Settings and select All Bands/Automatic before selecting signal input.

The gateway can detect and automatically select the higher signal strength between either the internal antennas or from the external input. To initiate the auto select process, please select Auto Select and click on Save/Apply. The Auto Select process takes about 170 seconds. Close the web browser on your computer and do not use the Internet during the whole process.

The results of the selection will be shown on screen. If the internal and external signals are on the same level, the gateway will select the Internal Antennas as input.



The gateway is able to remember the last selected signal input before power-off. If the signal input is changed to the External Antenna it will obtain a signal from the external antenna after restart.

5.3 PIN CONFIGURATION

This screen allows for changes to the 3G SIM card PIN code protection settings.

NOTE: If you have entered the incorrect PIN 3 times, your SIM card will be locked for your security. Please call Telstra for assistance.

5.3.1 PIN CODE PROTECTION

PIN code protection prevents the use of a SIM card by unauthorized persons. To use the 3G Internet service with this gateway however, the PIN code protection should be disabled. If the SIM card inserted into the gateway is locked with a PIN code, the web user interface will display the following screen after first login.

The inserted SIM card needs PIN code to unlock.

If Remember PIN is Yes, the correct PIN code will be remember by the Gateway unless reset to default.

If Remember PIN is No, users need to input PIN code each time after the Gateway reboots.

Please enter the PIN code.

Enter PIN Code

PIN Code:

Confirm PIN Code:

Remember PIN code: **No** ☒

Times remaining:

Please input the PIN code, select Remember PIN code as Yes and click Apply.

PIN Lock Off

If you wish to always connect to the Internet using a PIN locked SIM card, you should first turn PIN code protection off, then click on PIN Configuration from the menu.

Next G™ Settings > PIN Configuration

PIN Configuration allows you to enable/disable the PIN code or change the PIN Code on the SIM card.
To enable/disable the PIN code, please select Change PIN Protection. To change the PIN code please select PIN Code Change.
The original PIN code is required to be input.

☒ Change PIN Code Protection

☐ Enable PIN Lock

PIN Code:

Confirm PIN Code:

Remember PIN code:

Times remaining:

☐ PIN Code Change

Old PIN Code:

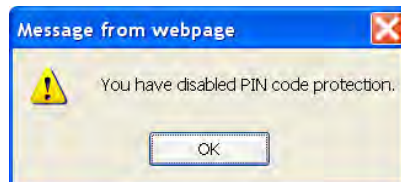
New PIN Code:

Confirm PIN Code:

Times remaining:

Select Change PIN Code Protection. Un-tick Enable PIN Lock, enter the PIN code twice. Please keep in mind you only have 3 attempts before your SIM card is locked. The Times remaining shows how many attempts are left. Once you have entered the Pin Code, click apply and the following dialog box should now appear.

Contact Telstra if you require assistance.



PIN Lock On

After you are finished using your SIM card for Internet access, you may wish to lock the SIM card again. In this case go to the PIN configuration screen as shown below.

Next G™ Settings > PIN Configuration

PIN Configuration allows you to enable/disable the PIN code or change the PIN Code on the SIM card.
To enable/disable the PIN code, please select Change PIN Code Protection. To change the PIN code please select PIN Code Change.
The original PIN code is required to be input.

☒ Change PIN Code Protection

☒ Enable PIN Lock

PIN Code:

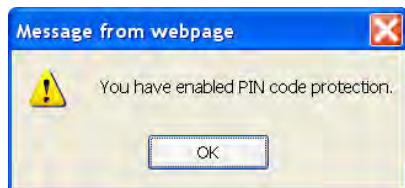
Confirm PIN Code:

Remember PIN code:

Times remaining:

Select Change PIN Code Protection. Tick Enable PIN Lock and enter the PIN code twice. You can change the Remember PIN code to yes so you don't need to input the PIN code every time the gateway turns on with this SIM inserted. Then click Apply.


After you do so, the following dialog box should appear.



You can now return your SIM card to your cellular phone or other mobile device.

5.3.2 PIN CODE CHANGE

If you wish to change your PIN code for greater security, go to the previous section and follow the procedure listed under PIN Lock On. After locking the SIM card, select PIN Code Change and enter your old and new PIN codes in the fields provided, then click apply to activate the change. Keep in mind you only have 3 attempts before your SIM card is locked. The Times remaining shows how many attempts left. Contact Telstra if you require any assistance.

 PIN Code Change

Old PIN Code:

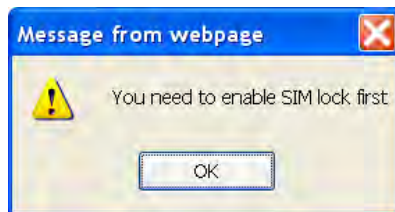
New PIN Code:

Confirm PIN Code:

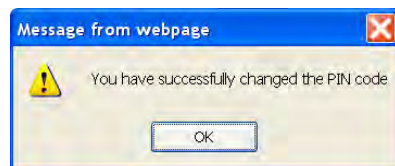
Times remaining:

Apply

If you forget to turn on PIN lock protection before changing your PIN, you will see this dialog box as a helpful reminder.



If your PIN code change request was successful the following dialog box will display.



WI-FI

WI-FI

The Wi-Fi submenu provides access to Wireless Local Area Network (WLAN) configuration settings including:

- Wireless network name
- Channel restrictions (based on country)
- Security
- Access point or bridging behaviour
- Station information



6.1 SETTINGS

This screen allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. The Wireless Guest Network function adds extra networking security when connecting to remote hosts.

Basic

Next G™ Settings

WiFi

Advanced Settings

Diagnostics

WiFi > Settings

This page allows you to configure your WiFi settings. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements. Click "Apply" to configure the basic wireless options.

☒ Enable WiFi

☒ Enable SSID Broadcast

☐ Client Isolation

Enables the wireless (WiFi) network name to be broadcasted publicly to any wireless users within wireless range of your network. Disabling the SSID broadcast makes the network name private and provides enhanced security by requiring wireless users to enter the network name manually when creating a wireless network profile on their computer.

SSID:

BSSID:

Country:

Max Clients:

Wireless - Guest/Wireless Access Points

Enabled	SSID	Hidden	Isolate Clients	Max Clients	BSSID
<input checked="" type="checkbox"/>	wifi_guest1	<input type="checkbox"/>	<input type="checkbox"/>	32	N/A
<input checked="" type="checkbox"/>	wifi_guest2	<input type="checkbox"/>	<input type="checkbox"/>	32	N/A
<input checked="" type="checkbox"/>	wifi_guest3	<input type="checkbox"/>	<input type="checkbox"/>	32	N/A

Save/Apply

Option	Description
Enable Wi-Fi	A checkbox that enables or disables the wireless LAN interface. When selected the Web UI displays Hide Access point, SSID, and Country settings. The default is Enable Wi-Fi.
Enable SSID Broadcast	<p>Deselect Enable SSID Broadcast to protect the access point from detection by wireless active scans.</p> <p>To check AP status in Windows XP, open Network Connections from the Start Menu and select View Available Network Connections. If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.</p>
Clients Isolation	<ol style="list-style-type: none"> 1. Prevents client PCs from seeing one another in My Network Places or Network Neighborhood. 2. Prevents one wireless client communicating with another wireless client.
SSID	<p>Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.</p> <p>The naming conventions are: Minimum number of characters: 1, maximum number of characters: 32.</p>
BSSID	The BSSID is a 48bit identity used to identify a particular BSS (Basic Service Set) within an area. In Infrastructure BSS networks, the BSSID is the MAC (Medium Access Control) address of the AP (Access Point) and in Independent BSS or ad hoc networks, the BSSID is generated randomly.
Country	A drop-down menu that permits worldwide and specific national settings. Each country listed in the menu enforces specific regulations limiting channel range: US= worldwide, Japan=1-14, Jordan= 10-13, Israel= 1-13
Max Clients Wireless - Guest / Virtual Access Points	<p>The maximum number of clients that can access the router.</p> <p>This router supports multiple SSIDs called Guest SSIDs or Virtual Access Points. To enable one or more Guest SSIDs select the radio buttons under the Enable heading. To hide a Guest SSID, select its radio button under the Hidden heading. Do the same for Isolate Client. For a description of this function, see the entry for "Client Isolation" in this table. Similarly, for Max Clients and BSSID headings, consult the matching entries in this table.</p> <p>NOTE: Remote wireless hosts are unable to scan Guest SSIDs.</p>

6.2 SECURITY

This gateway includes a number of options to help provide a secure connection to the Wi-Fi Network.

Security features include:

- WEP / WPA / WPA2 data encryption
- MAC address IP filtering

You can authenticate or encrypt your service on the Wi-Fi Protected Access algorithm, which provides protection against unauthorized access such as eavesdropping.

The following screen appears when Security is selected. The Security page allows you to configure security features of your gateway's wireless WLAN interface. You can set the network authentication method, select data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.

Wi-Fi > Security

This page allows you to configure security features of the wireless LAN interface.
You may setup configuration manually.

Manual Setup AP

You can set the network authentication method, select data encryption,
specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Save/Apply" when done.

Select SSID:

Network Authentication:

WPA Pre-Shared Key: [Click here to display](#)

WPA Group Rekey Interval:

WPA Encryption:

WEP Encryption:

Click Save/Apply to configure the wireless security options.

Option	Description
Select SSID	Your Service Set Identifier (SSID), sets your Wireless Network Name. You can connect multiple devices including Laptops, Desktop PCs and PDAs to your Wireless Gateway. To connect additional devices, scan for a network and locate the SSID shown on your Wireless Security Card. If the SSID does not match, access is denied.
Network Authentication	This option is used for authentication to the wireless network. Each authentication type has its own settings. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and key fields.
WEP Encryption	This option indicates whether data sent over the network is encrypted. The same network key is used for data encryption and network authentication. Whilst four network keys can be defined, only one can be used at any one time.
Encryption Strength	This drop-down list box will display when WEP Encryption is enabled. The key strength is proportional to the number of binary bits comprising the key. This means that keys with a greater number of bits have a greater degree of security and are considerably more difficult to crack. Encryption strength can be set to either 64-bit or 128-bit. A 64-bit key is equivalent to 5 ASCII characters or 10 hexadecimal numbers. A 128-bit key contains 13 ASCII characters or 26 hexadecimal numbers.

6.3 CONFIGURATION

The following screen appears when you select Configuration. This screen allows you to control the advanced features of the Wireless Local Area Network (WLAN) interface:

- Select the channel which you wish to operate from
- Force the transmission rate to a particular speed
- Set the fragmentation threshold
- Set the RTS threshold
- Set the wake-up interval for clients in power-save mode
- Set the beacon interval for the access point
- Set Xpress mode
- Program short or long preambles

Click Save/Apply to set the advanced wireless configuration.

The screenshot shows the 'WLAN Configuration' screen with the following settings:

- Basic** (Selected tab)
- Channel:** 2.4GHz (Current: 10)
- Auto Channel Overlap:** Auto
- Bandwidth:** 20MHz in Both Bands (Current: 20MHz)
- Fragmentation Threshold:** 2347
- RTS Threshold:** 2347
- Wake-up Interval:** 100
- Beacon Interval:** 100
- Xpress Mode:** Disabled
- Transmit Power:** 100%

At the bottom right, there is a 'Save/Apply' button.

Option	Description
Band	The new amendment allows IEEE 802.11g units to fall back to speeds of 11 Mbps, so IEEE 802.11b and IEEE 802.11g devices can coexist in the same network. The two standards apply to the 2.4 GHz frequency band. IEEE 802.11g creates data-rate parity at 2.4 GHz with the IEEE 802.11a standard, which has a 54 Mbps rate at 5 GHz. (IEEE 802.11n has other differences compared to IEEE 802.11b or g, such as offering more channels.)
Channel	Drop-down menu that allows selection of a specific channel.
Auto Channel Timer (min)	Auto channel scan timer in minutes (0 to disable)
802.11n/EWC	With drop-down menu, "Auto" is for 11n and "Disable" is for 11g
Bandwidth	Drop-down menu specifies the following bandwidth: 20MHz and 40MHz.
Control Sideband	This is available for 40MHz. Drop-down menu allows selecting upper sideband or lower sideband
802.11n Rate	Drop-down menu specifies the following fixed rates. The maximum rate for bandwidth, 20MHz, is 130MHz and the maximum bandwidth, 40MHz, is 270MHz
802.11n Protection	It is similar as 802.11g protection. In Auto mode the router will use RTS/CTS to improve 802.11n performance in mixed 802.11n/ 802.11g/ 802.11b networks. Turn protection off to maximize 802.11n throughput under most conditions.
Support 802.11n client only	Drop-down menu allows selecting "On/Off". Choosing "On" allows the client with 11n only to connect, not for 11g or 11b; choosing "Off" allows the client with 11n/11g/11b to connect
54g Rate	Drop-down menu that specifies the following fixed rates: Auto: Default. Uses the 11 Mbps data rate when possible but drops to lower rates when necessary. 1 Mbps, 2Mbps, 5.5Mbps, or 11Mbps fixed rates. The appropriate setting is dependent on signal strength.
Multicast Rate	Setting multicast packet transmit rate.
Basic Rate	Setting basic transmit rate.
Fragmentation Threshold	A threshold, specified in bytes, that determines whether packets will be fragmented and at what size. On an 802.11 WLAN, packets that exceed the fragmentation threshold are fragmented, i.e., split into smaller units suitable for the circuit size. Packets smaller than the specified fragmentation threshold value are not fragmented. Enter a value between 256 and 2346. If you experience a high packet error rate try to slightly increase your Fragmentation Threshold. The value should remain at its default setting of 2346. Setting the Fragmentation Threshold too low may result in poor performance.
RTS Threshold	Request to Send, (when set in bytes) specifies the packet size beyond which the WLAN Card invokes its RTS/CTS mechanism. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The NIC transmits smaller packet without using RTS/CTS. The default setting of 2347 (maximum length) disables RTS Threshold.

Option	Description
DTIM Interval	<p>Delivery Traffic Indication Message (DTIM), also known as Beacon Rate. The entry range is a value between 1 and 65535. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value.</p> <p>AP Clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.</p>
Beacon Interval	<p>The amount of time between beacon transmissions. Each beacon transmission identifies the presence of an access point. By default, radio NICs passively scan all RF channels and listen for beacons coming from access points to find a suitable access point.</p> <p>Before a station enters power save mode, the station needs the beacon interval to know when to wake up to receive the beacon (and learn whether there are buffered frames at the access point). The entered value is represented in ms. Default is 100. Acceptable entry range is 1 to 0xffff (65535)</p>
Global Max Clients	<p>The device can support 4 SSIDs, and each SSID can set its own max clients, but it can't be bigger than the Global max clients setting. "Global Max Clients" limits the total associated clients of the 4 SSIDs combined.</p>
Xpress™ Technology	<p>Xpress™ Technology is compliant with draft specifications of two planned wireless industry standards.</p>
Transmit Power	<p>The router will set different power outputs (by percentage) according to this selection.</p>

6.4 MAC FILTER

This screen appears when Media Access Control (MAC) Filter is selected. This option allows access to be restricted based upon the unique 48-bit MAC address assigned to a network enabled device. To add a MAC Address filter, click the Add button shown below.

To delete a filter, select it from the table below and click the Remove button.

Option	Description
MAC Restrict Mode	<p>Disabled – Disables MAC filtering</p> <p>Allow – Permits access for the specified MAC addresses.</p> <p>NOTE: Add a wireless device's MAC address before clicking the Allow radio button or else you will need to connect to the gateway's web user interface using the supplied yellow Ethernet cable and add the wireless device's MAC address.</p> <p>Deny – Rejects access for the specified MAC addresses</p>
MAC Address	<p>Lists the MAC addresses subject to the MAC Restrict Mode. The Add button prompts an entry field that requires you type in a MAC address in a two-character, 6-byte convention: xx:xx:xx:xx:xx:xx where xx are hexadecimal numbers. A maximum of 60 MAC addresses can be added.</p>

Enter the MAC address on the screen below and click Save/Apply.

6.5 WIRELESS BRIDGE

The following screen appears when selecting Wireless Bridge, and goes into a detailed explanation of how to configure the wireless bridge features of the wireless LAN interface. Click Save/Apply to implement new configuration settings.



Option	Description
AP Mode	Selecting Wireless Bridge (Wireless Distribution System) disables Access Point (AP) functionality while selecting Access Point enables AP functionality. In Access Point mode, wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
Bridge Restrict	Selecting Disabled disables the Wireless Bridge restriction, which means that any wireless bridge will be granted access. Selecting enabled or enabled (Scan) enables the wireless bridge restrictions. Only those bridges selected in Remote Bridges will be granted access. Click Refresh to update the station list when Bridge Restrict is enabled.

6.6 STATION INFO

The following screen appears when you select Station Info and shows authenticated wireless stations and their status. Click the Refresh button to update the list of stations in the WLAN



Option	Description
MAC	The MAC (Media Access Control) address of the AP (Access Point).
Associated	Lists all the stations that are associated with the Access Point, along with the amount of time since packets were transferred to and from each station. If a station is idle for too long, it is removed from this list.
Authorized	Lists those devices with authorized access.

MANAGEMENT

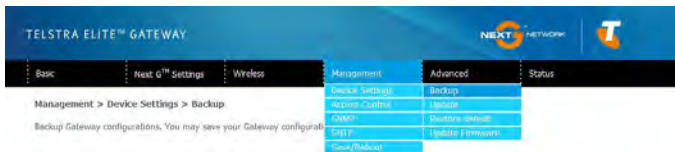
MANAGEMENT

The Management menu has the following maintenance functions and processes:

- 7.1 Device Settings
- 7.2 Access Control
- 7.3 Simple Network Management Protocol (SNMP)
- 7.4 Simple Network Time Protocol (SNTP)
- 7.5 Save and Reboot

7.1 DEVICE SETTINGS

The Device Settings screens allow you to backup, retrieve and restore the default settings of your gateway. It also provides a function for you to update your gateway's settings.



7.1.1 BACKUP SETTINGS

The following screen appears when Backup is selected. Click the Backup Settings button to save the current configuration settings.

You will be prompted to choose the location to save a backup of your settings to on your PC.



7.1.2 UPDATE SETTINGS

The following screen appears when selecting Update from the submenu. By clicking on the Browse button, you can locate a previously saved filename as the configuration backup file. Click on the Update settings to load it.



7.1.3 RESTORE DEFAULT

The following screen appears when selecting Restore Default. By clicking on the Restore Default Settings button, you can restore your gateway's default firmware settings. To restore system settings, reboot your gateway.



NOTE: The default settings can be found in section 3.3 Default Settings.

Once you have selected the Restore Default Settings button, the following screen will appear. Close the window and wait 2 minutes before reopening your browser. If required, reconfigure your computer's IP address to match your new configuration (see section 3.2 TCP/IP Settings for details).

Gateway Restore

The Gateway configuration has been restored to default settings and the Gateway is rebooting.

Close the Gateway Configuration window and wait for 2 minutes before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

NOTE: The Restore Default function has the same effect as the reset button. If the reset button is continuously pushed for more than 5 seconds (and not more than 12 seconds), the boot loader will erase the configuration settings saved on flash memory.

7.1.4 UPDATE FIRMWARE

The following screen appears when selecting Update Firmware. By following the steps on this screen, you can update your gateway's firmware.

Management > Device Settings > Update Firmware

Step 1: Obtain an updated firmware image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Update Firmware" button once to upload the new image file.

NOTE: The update process for the Gateway takes about 2 minutes to complete, and for the 3G modem takes about 10 minutes, and your Gateway will reboot. Please DO NOT close the Browser and reload/or change the webpage during the update process.

Firmware File Name:

1. Obtain an updated software image file
2. Enter the path and filename of the firmware image file in the Software File Name field or click the Browse button to locate the image file.
3. Click the Update Software button once to upload and install the file.

NOTE: The update process will take about 2 minutes to complete. The gateway will reboot and the browser window will refresh to the default screen upon successful installation.

It is recommended that you compare the Gateway Firmware Version at the top of the Basic screen (WUI homepage) with the firmware version installed, to confirm the installation was successful.

7.2 ACCESS CONTROL

The Access Control option found in the Management drop down menu configures access related parameters in the following two areas:

1. Services
2. Passwords

Access Control is used to control local and remote management settings for your Gateway.



7.2.1 SERVICES

The Service Control List (SCL) allows you to enable or disable your Wide Area Network (WAN) services by ticking the checkbox as illustrated below. The following access services are available: FTP, HTTP, ICMP, SSH, TELNET, and TFTP. Click Save/Apply to continue.



7.2.2 PASSWORDS

The Passwords option configures your account access password for your gateway. Access to the device is limited to the following three user accounts:

1. admin is to be used for unrestricted access control via WAN or LAN; the password is admin (lower case) by default.
2. support is to be used for remote maintenance of the device via WAN only; the password is support (lower case) by default.
3. user is to be used for restricted view to the Basic and Status information; the password is user (lower case) by default.

Use the fields illustrated in the screen below to change or create your password. Passwords must be no more than 16 characters with no spaces. Click Save/Apply to continue.

The screenshot shows the 'Management' tab selected in the top navigation bar. The breadcrumb trail is 'Management > Access Control > Passwords'. The page contains the following text:

Access to your Gateway is controlled through three user accounts: 'admin', 'support', and 'user'.

The user name "admin" has unrestricted access to change and view configuration of your Gateway.

The user name "support" is used to allow an ISP technician to access your Gateway for maintenance and to run diagnostics.

The user name "user" can access the Gateway, view configuration settings and statistics, as well as, update the Gateway's software.

Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords. Note: Password cannot contain a space.

Below the text are four input fields labeled 'Username:', 'Old Password:', 'New Password:', and 'Confirm Password:'. The 'Username:' field is a dropdown menu with a blue arrow icon. To the right of the input fields is a button labeled 'Apply/Save'.

7.3 CONFIGURE SNMP AGENT

The Simple Network Management Protocol (SNMP) allows a network administrator to monitor a network by retrieving settings on remote network devices. To do this the administrator typically runs an SNMP management station program such as MIB browser on a local LAN host to obtain information from the SNMP agent, in this case the 3G21WT (if SNMP is enabled). An SNMP ‘community’ performs the function of authenticating SNMP traffic. A ‘community name’ acts as a password that is typically shared among SNMP agents and managers.

By default, SNMP agent is enabled on the gateway.

Setting up SNMP agent

- 1. Go to Management > SNMP. Enable SNMP agent and set up all options according to the screenshot below.
- 2. Click Save/Apply to activate these settings.



Option	Description
Read Community	Read Device Settings
Set Community	Read and change Device Settings
System Name	Set to 3G21WT by default
System Location	User-defined value
System Contact	User-defined value
Trap Manager IP	IP address of admin machine

7.4 SIMPLE NETWORK TIME PROTOCOL (SNTP)

This screen allows you to configure the time settings of your gateway. To automatically synchronize with Internet time servers, tick the box as illustrated below.

BasicNext G™ SettingsWirelessManagementAdvancedStatus

Management > SNTP

This page allows you to the modem's time configuration.

☒ Automatically synchronize with Internet time servers

First NTP time server:Other0.netcomm.pool.ntp.org

Second NTP time server:Other1.netcomm.pool.ntp.org

Third NTP time server:None

Fourth NTP time server:None

Fifth NTP time server:None

Time zone offset:(GMT+10:00) Canberra, Melbourne, Sydney

Save/Apply

The following options are available for configuration.

First NTP time server:	Select the required server.
Second NTP time server:	Select second time server, if required.
Time zone offset:	Select the local time zone.

Configure these options and then click Save/Apply to activate.

NOTE: SNTP must be activated to use Parental Control (section 8.3.2).

7.5 SAVE AND REBOOT

This function saves the current configuration settings and reboots your gateway.



NOTE1: It may be necessary to reconfigure your TCP/IP settings to adjust for the new configuration. For example, if you disable the Dynamic Host Configuration Protocol (DHCP) server you will need to apply Static IP settings.

NOTE2: If you lose all access to your web user interface, simply press the reset button on the rear panel for 6 to 8 seconds to restore default settings.

ADVANCED

ADVANCED SETTINGS

8.1 LOCAL AREA NETWORK (LAN)

This screen allows you to configure the Local Area Network (LAN) interface on your gateway

Basic

Next G™ Settings

Wi-Fi

Advanced Settings

Diagnostics

Note: These settings are for advanced users. We recommend that you do not change it if you are unsure of what you are doing. If you do run into problems, you can reset the Gateway back to default settings. To do this, insert a pointed object (like a straightened paperclip) into the hole at the back of the Gateway labelled 'Reset'. Press and hold the reset button till the power light starts flashing - then release the button, you will need to run the Install CD that came in your kit again once you reset the Gateway.

Advanced Settings > Local Area Network (LAN) Setup

IP Address:

10.0.0.138

Subnet Mask:

255.255.255.0

☐ Enable IGMP Snooping

☒ Enable NAT

☒ Enable UPnP

☐ Disable DHCP Server

☒ Enable DHCP Server

Start IP Address:

10.0.0.1

End IP Address:

10.0.0.137

Leased Time (hour):

24

Static IP Lease List: (A maximum 32 entries can be configured)

MAC Address

IP Address

Remove

Add Entries...

Remove Entries...

☐ Enable DHCP Server Relay

DHCP Server IP Address:

☐ Configure the second IP Address and Subnet Mask for LAN interface

Save/Reload

See the field descriptions below for more details.

NOTE: If you change the gateway's address (first option on the chart), you also need to change the gateway ip address on the usb key so the installation software can communicate with the gateway.

For pc users, please plug the usb key into your pc and click on [changegatewayip](#) or [changegatewayip.Exe](#). Type in the new gateway ip address and click run.

For mac os users, please double click into the folder named mac. Click on [changegatewayip.App](#) and enter the new gateway ip. Then click on save and close.

Option	Description
IP Address	Enter the IP address for the LAN interface
Subnet Mask	Enter the subnet mask for the LAN interface
Enable Internet Group Management Protocol (IGMP) Snooping	<p>Enable by ticking the box Standard Mode: In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group.</p> <p>Blocking Mode: In blocking mode, the multicast data traffic will be blocked. When there are no client subscriptions to a multicast group, it will not flood to the bridge ports.</p>
Enable NAT	To enable/disable Network Address Translation (NAT, please refer to 7.2 for NAT setting). By default NAT is enabled.
Enable UPnP	Tick the box to enable Universal Plug and Play
Dynamic Host Configuration Protocol (DHCP) Server	Select enable DHCP server and enter your starting and ending IP addresses and the lease time. This setting configures the gateway to automatically assign IP, default gateway and DNS server addresses to every DHCP client on your LAN
Static IP Lease List	To specify the IP address assigned through DHCP according to the MAC address of the hosts connected to the gateway.
Enable DHCP Server Relay	To relay DHCP requests from the subnet with no DHCP server on it to a DHCP server on other subnets. DHCP Server Relay is disabled by default. To access enable DHCP relay, please un-tick NAT enable first, that means to disable NAT first, and then press save button. The enable DHCP server Relay option will then show up on the same page as below:

Configure a second IP address by ticking the checkbox shown below and enter the following information:

IP Address:	Enter the secondary IP address for the LAN interface.
Subnet Mask:	Enter the secondary subnet mask for the LAN interface.

NOTE: The Save button saves new settings to allow continued configuration, while the Save/Reboot button not only saves new settings but also reboots the device to apply the new configuration (i.e. all new settings).

8.2 NETWORK ADDRESS TRANSLATION (NAT)

BasicNext G™ SettingsWi-FiAdvanced SettingsDiagnostics

Note: These settings are for advanced users. We recommend that you do not change it if you are unsure of what you are doing. If you do run into problems, you can reset the Gateway back to default settings. To do this, insert a pointed object (like a straightened paperclip) into the hole at the back of the Gateway labelled 'Reset'. Press and hold the reset button till the power light starts flashing - then release the button. You will need to run the Install CD that came in your kit again once you reset the Gateway.

Advanced Settings > NAT > Port Forwarding

Port Forwarding allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
-------------	---------------------	-------------------	----------	---------------------	-------------------	-------------------	---------------	--------

LANNATSecurityRoutingParental ControlDNSDevice SettingsAccess ControlSNMPSMTPTR-069 ClientUSB SettingsSave/Reboot

8.2.1 PORT FORWARDING

Port Forwarding allows you to direct incoming traffic from the Internet side (identified by Protocol and External port) to an internal server with a private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.

BasicNext G™ SettingsWi-FiAdvanced SettingsDiagnostics

Note: These settings are for advanced users. We recommend that you do not change it if you are unsure of what you are doing. If you do run into problems, you can reset the Gateway back to default settings. To do this, insert a pointed object (like a straightened paperclip) into the hole at the back of the Gateway labelled 'Reset'. Press and hold the reset button till the power light starts flashing - then release the button. You will need to run the Install CD that came in your kit again once you reset the Gateway.

Advanced Settings > NAT > Port Forwarding

Port Forwarding allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.

AddRemove

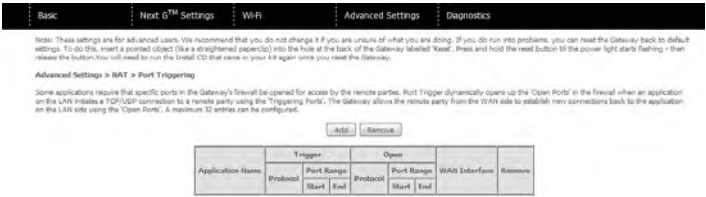
Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
-------------	---------------------	-------------------	----------	---------------------	-------------------	-------------------	---------------	--------

To add a Port Forwarding rule, click the Add button. The following screen will display.

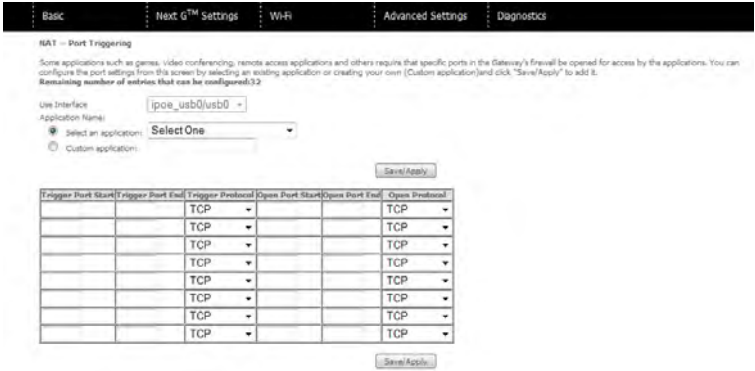
Options	Description
Select a Service Or Custom Server	User should select the service from the list. Or create a custom server and enter a name for the server
Server IP Address	Enter the IP address for the server.
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected the port ranges are automatically configured.
Protocol	User can select from: TCP, TCP/UDP or UDP.
Internal Port Start	Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected the port ranges are automatically configured.

8.2.2 PORT TRIGGERING

Some applications require specific ports in the gateway’s firewall to be open for access by remote parties. Port Triggering opens up the ‘Open Ports’ in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using one of the ‘Triggering Ports’. The gateway allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the ‘Open Ports’. A maximum 32 entries can be configured



To add a Trigger Port, simply click the Add button. The following will be displayed.



Options	Description
Select an Application or Custom Application	User should select the application from the list. or User can enter the name of their choice.
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Port End	Enter the ending trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Protocol	TCP, TCP/UDP or UDP.
Open Port Start	Enter the starting open port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Open Port End	Enter the ending open port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Open Protocol	TCP, TCP/UDP or UDP.

8.2.3 DEMILITARIZED (DMZ) HOST

Your gateway will forward IP packets from the Wide Area Network (WAN) that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.

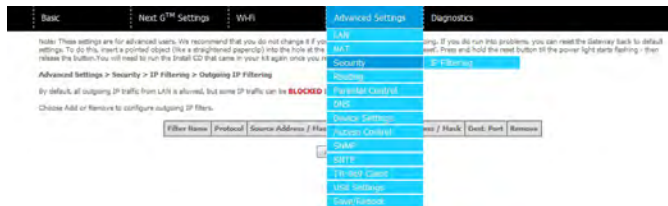
Enter the computer's IP address and click Apply to activate the DMZ host.

Clear the IP address field and click Apply to deactivate the DMZ host.

Basic	Next G™ Settings	Wi-Fi	Advanced Settings	Diagnostics
<p><small>Note: These settings are for advanced users. We recommend that you do not change it if you are unsure of what you are doing. If you do run into problems, you can reset the Gateway back to default settings. To do this, insert a pointed object (like a straightened paperclip) into the hole at the back of the Gateway labeled "Reset". Press and hold the reset button till the power light starts flashing, then release the button. You will need to run the Install CD that came in your kit again once you reset the Gateway.</small></p> <p>Advanced Settings > NAT > DMZ Host</p> <p>The Gateway will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.</p> <p>Enter the computer's IP address and click "Apply" to activate the DMZ host.</p> <p>Clear the IP address field and click "Apply" to deactivate the DMZ host.</p> <p>DMZ Host IP Address: <input type="text"/></p> <p><input type="button" value="Save/Apply"/></p>				

8.3 SECURITY

Your gateway can be secured with the IP Filtering function.



8.3.1 IP FILTERING

The IP Filtering screen sets filter rules that limit incoming and outgoing IP traffic. Multiple filter rules can be set with at least one limiting condition. All conditions must be fulfilled to allow individual IP packets to pass through the filter.

Outgoing IP Filter

The default setting for Outgoing traffic is ACCEPTED. Under this condition, all outgoing IP packets that match the filter rules will be BLOCKED.



To add a filtering rule, click the Add button. The following screen will display.

Basic

Next G™ Settings

Wi-Fi

Advanced Settings

Diagnostics

Add IP Filter – Outgoing

The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.

Filter Name:

Protocol:

Source IP address:

Source Subnet Mask:

Source Port (port or port:port):

Destination IP address:

Destination Subnet Mask:

Destination Port (port or port:port):

Apply/Save

Options	Description
Filter Name	The filter rule label
Protocol	TCP, TCP/UDP, UDP or ICMP
Source IP address	Enter source IP address
Source Subnet Mask	Enter source subnet mask
Source Port (port or port:port)	Enter source port number or port range
Destination IP address	Enter destination IP address
Destination Subnet Mask	Enter destination subnet mask
Destination port (port or port:port)	Enter destination port number or range

Click Save/Apply to save and activate the filter.

Incoming IP Filter

The default setting for all Incoming traffic is BLOCKED. Under this condition only those incoming IP packets that match the filter rules will be ACCEPTED.

Basic

Next G™ Settings

Wi-Fi

Advanced Settings

Diagnostics

Notes: These settings are for advanced users. We recommend that you do not change it if you are unsure of what you are doing. If you do run into problems, you can reset the Gateway back to default settings. To do this, insert a pointed object (like a sharpened pencil) into the hole at the back of the Gateway (labeled 'Reset'). Press and hold the reset button till the power light starts flashing. Then release the button. You will need to run the Setup CD that came in your package once you reset the Gateway.

Advanced Settings in Security > IP Filtering > Incoming IP Filtering

Under the firewall is enabled on a Wi-Fi or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Filter Name

Protocol

Source Address / Mask

Source Port

Dest. Address / Mask

Dest. Port

Remove

Add

Remove

To add a filtering rule, click the Add button. The following screen will display.

Please refer to the Outgoing IP Filter table for field descriptions.

Click Save/Apply to save and activate the filter.

8.3.2 PARENTAL CONTROL

Parental Control allows you to restrict access from a device on your Local Area Network (LAN) to the Internet through the gateway on selected days at certain times. Make sure to activate the Internet Time server synchronization as described in section 8.4 SNTP, so that the scheduled times match your local time.

Click Add to display the following screen. Enter the MAC address of the device that you wish to restrict access for and select days of the week and times to apply the restriction.

Basic

Next G™ Settings

Wireless

Management

Advanced

Status

Time of Day Restriction

This page adds time of day restriction to a special LAN device connected to the Gateway. The "Browser's MAC Address" automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

Policy Name

☒ Browser's MAC Address

00:24:e8:93:13:76

☐ Other MAC Address

(xx:xx:xx:xx:xx:xx)

Days of the week

MonTueWedThuFriSatSun

Click to select

☐☐☐☐☐☐☐

Start Blocking Time (hh:mm)

End Blocking Time (hh:mm)

Save/Apply

Complete the fields listed below and click Save/Apply to apply the settings.

Options	Description
User Name	A user-defined label for this restriction
Browser's MAC Address	Allows easy identification of MAC address of the computer you are currently using.
Other MAC Address	MAC address of another LAN device
Days of the Week	Select one more more days for the restrictions for the entered MAC address to apply to.
Start Blocking Time	Enter the time of day you want the restriction for the entered MAC address to start
End Blocking Time	Enter the time of day you want the restriction for the entered MAC address to end

8.4 ROUTING

Static Route and Dynamic Route settings can be found in the Routing link as illustrated below.



8.4.1 STATIC ROUTE

The Static Route screen displays the configured static routes. Click the Add or Remove buttons to change settings.



Click the Add button to display the following screen.

The screenshot shows the 'Static Route Add' screen with the following fields and options:

- Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Save/Apply" to add the entry to the routing table.
- Destination Network Address:
- Subnet Mask:
- ☐ Use Gateway IP Address
- ☒ Use Interface: ipoe_usb0/usb0
-

Enter Destination Network Address, Subnet Mask, gateway IP Address and/or WAN Interface. Then click Save/Apply to add the entry to the routing table.

8.4.2 DYNAMIC ROUTE

To activate this option, select the enabled radio button for Global RIP Mode.

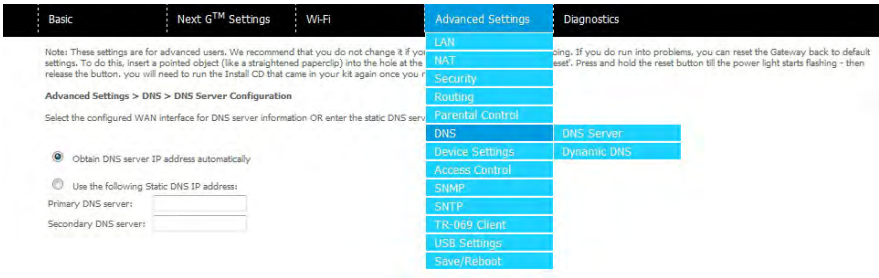
To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the enabled checkbox for that interface. Click Save/Apply to save the configuration and to start or stop dynamic routing.



8.5 DOMAIN NAME SERVER (DNS)

8.5.1 DNS SERVER CONFIGURATION

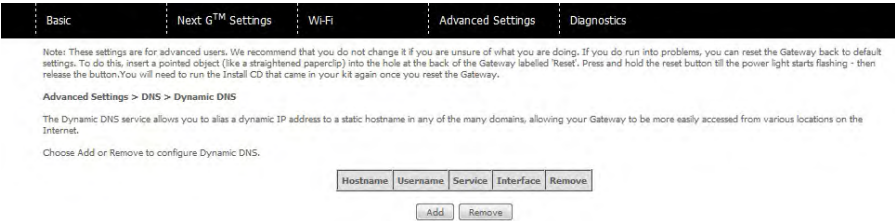
If Enable Automatic Assigned DNS is selected, this device will accept the first received DNS assignment from the Wide Area Network (WAN) interface during the connection process. Otherwise, you can enter the primary and optional secondary DNS server IP addresses. Click on Save to apply.



NOTE: Click the Save button to save the new configuration. To make the new configuration effective, reboot your gateway.

8.5.2 DYNAMIC DNS

The Dynamic DNS service allows a dynamic IP address to be aliased to a static hostname in any of a selection of domains, allowing the gateway to be more easily accessed from various locations on the Internet.



NOTE: The Add/Remove buttons will be displayed only if the gateway has been assigned an IP address from the remote server.

To add a dynamic DNS service, click the Add button and this screen will display

Basic

Next G™ Settings

Wi-Fi

Advanced Settings

Diagnostics

Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider

DynDNS.org

Hostname

Interface

ipoe_usb0/usb0

DynDNS Settings

Username

Password

Apply/Save

Options	Description
D-DNS provider	Select a dynamic DNS provider from the list.
Hostname	Enter the name for the dynamic DNS server.
Interface	Select the interface from the list.
Username	Enter the username for the dynamic DNS service
Password	Enter the password for the dynamic DNS service.

8.6 USB PRINT SERVER

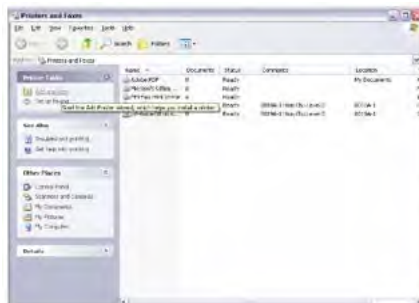
These steps explain the procedure for enabling the Print Server.

1. To enable the print server, select Enable on-board print server checkbox and enter Printer name and Make and model

NOTE: The printer name can be any text string up to 40 characters. The Make and model can be any text string up to 128 characters.

FOR WINDOWS XP:

- 2: Go to the Printers and Faxes application in the Control Panel and select the Add a printer function (as located on the side menu below).



3. Click Next to continue, when you see the dialog box below.

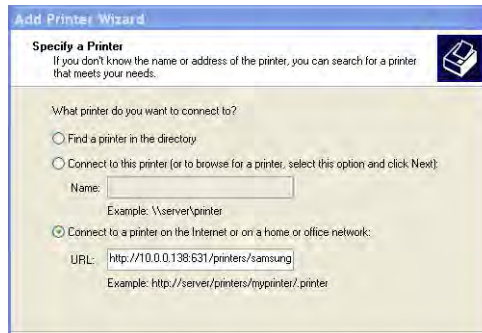


4. Select Network Printer and click Next.



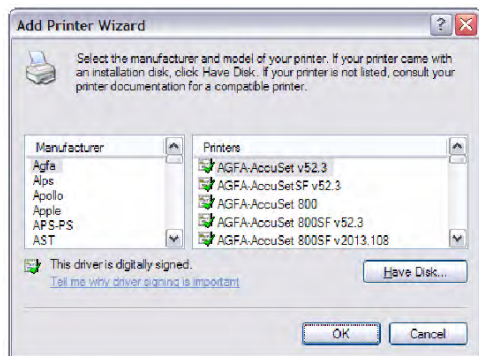
5. Select **Connect to a printer on the Internet** and enter your printer link, (e.g. <http://10.0.0.138:631/printers/printername>) and click **Next**.

NOTE: the printer name must be the same name entered in the web user interface "printer server setting" as in step 1.



The screenshot shows a window titled "Add Printer Wizard" with a blue header bar. Below the header, the section "Specify a Printer" is displayed. It includes a sub-header "Specify a Printer" and a descriptive text: "If you don't know the name or address of the printer, you can search for a printer that meets your needs." To the right of this text is a printer icon. Below the text, the question "What printer do you want to connect to?" is followed by three radio button options. The first option is "Find a printer in the directory". The second option is "Connect to this printer (or to browse for a printer, select this option and click Next);", which has a text input field labeled "Name:" and an example "Example: \\server\printer". The third option is "Connect to a printer on the Internet or on a home or office network:", which is selected with a green checkmark. This option has a text input field labeled "URL:" containing the text "http://10.0.0.138:631/printers/samsung" and an example "Example: http://server/printers/myprinter/printer".

6. Next, select the driver that came with your printer. Browse through the list to select your printer driver, or click 'Have Disk' if you have your printer driver installation media.



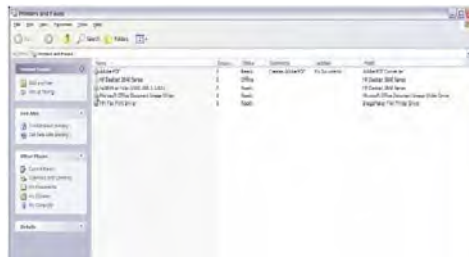
7. Choose Yes or No for default printer setting and click Next.



8. Click “Finish”.



9. Check the status of printer from Windows Control Panel, printer window. Status should show as Ready.

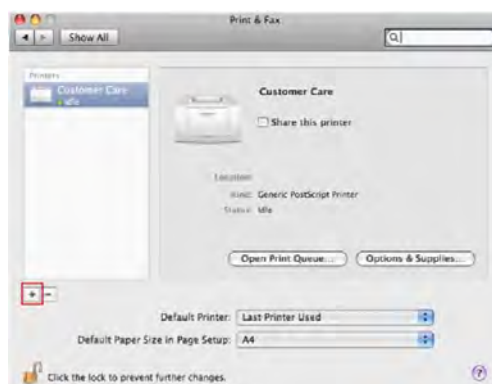


FOR MAC OS X:

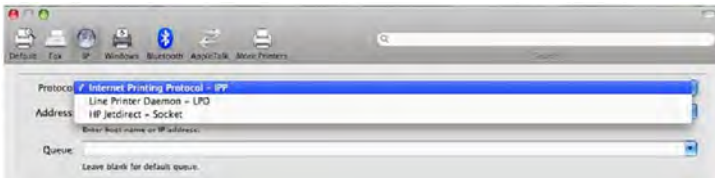
2. Browse to the Apple menu and select System Preferences. In the System Preferences menu click on Print & Fax.
3. With your Printer driver installed, please add your printer from the Printer & Fax menu.



4. Click + to add your printer from the Print & Fax menu.



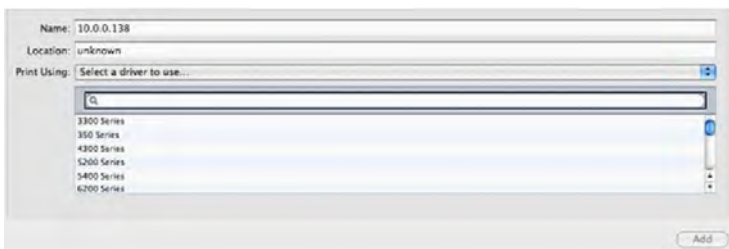
5. Select Internet Printing Protocol – IPP from the Protocol drop down list.



6. Type into the Address field “gatewayIPAddress:631” where gatewayIPAddress is the IP address of your gateway (default: 10.0.0.138). See screenshot below for an example. Also enter into the Queue field “/printers/PrinterName”, where PrinterName is the name you gave your printer in step 1



7. Select your printer from the Print Using drop down list.



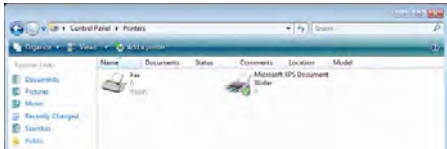
8. Click Add and check the printer status.



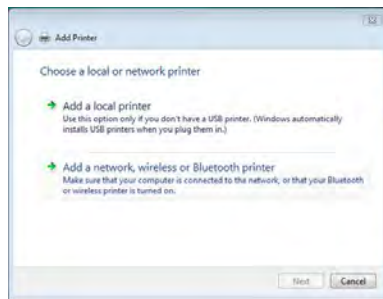
Print Server set up is now complete. You will now be able to print from common applications by selecting this printer from the Print dialogue box.

FOR WINDOWS VISTA

2. Go to the control panel, and select Printers. Once in the Printers page, click the Add a printer button as shown below.

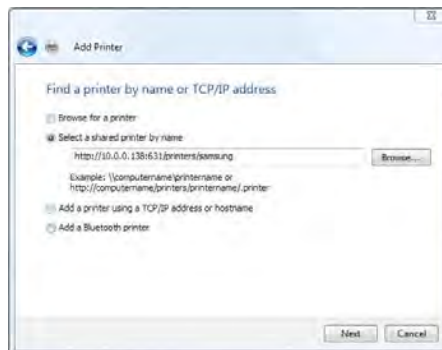


3. Select add a network, wireless or Bluetooth printer.

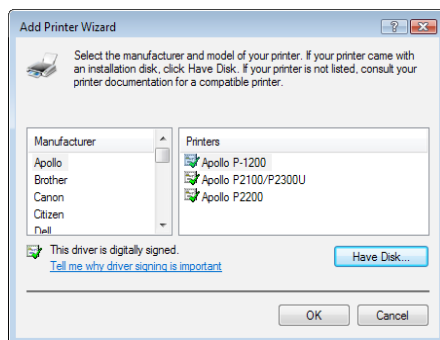


4. Click on the radio-button labeled Select a shared printer by name, and type “`http://10.0.0.138:631/printers/PrinterName`” in the box below. Click Next.

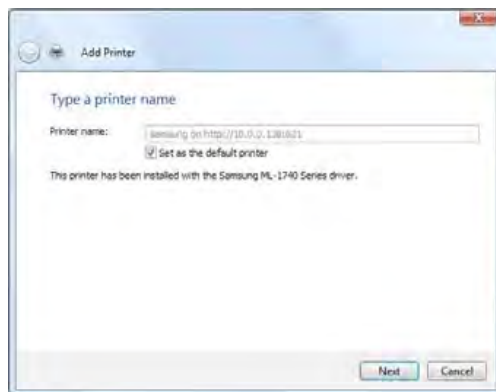
NOTE: The printername must be the same as the printer name entered in the Web User Interface during step 1



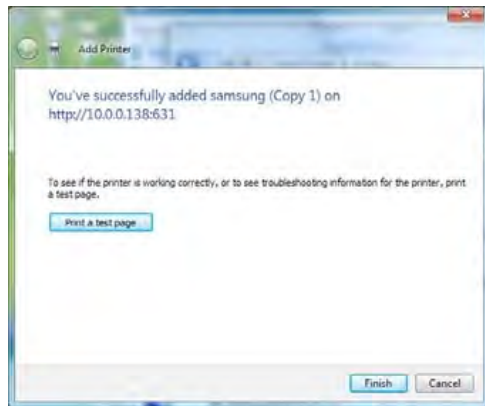
- Next, select the driver that came with your printer. Browse through the list to select your printer driver, or click 'Have Disk' if you have your printer driver installation media.



- Choose whether you want this printer to be the default printer, and then click Next.



7. Click Finish. Your device is now configured and ready for use.



8.7 USB STORAGE

The TELSTRA ELITE™ GATEWAY allows you to connect a USB storage device and share it with all of the users on the network.

By default, this feature is already enabled, so it is simply a matter of connecting your USB storage device and entering the appropriate network location.

If you wish to modify any of these features, the steps below explain the procedure for enabling the USB Storage.

1: Ensure that the Enable USB Storage checkbox is checked in the Web User Interface.

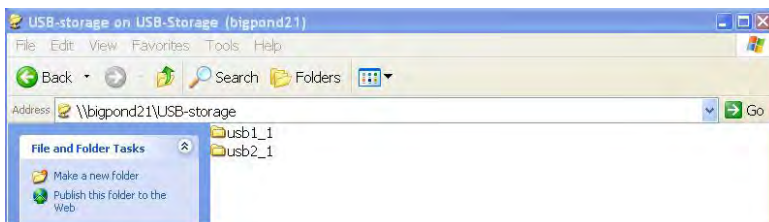
To do this, log on the WUI then select Advanced > USB Storage from the menu along the top of the page. Select the Enable USB Storage checkbox and enter the Gateway Name and USB Drive Name

Field	Description
Gateway Name	The hostname of the gateway device. This should only be modified if there are multiple TELSTRA ELITETM GATEWAY's on your network. The default name is "Telstra21".
USB Drive Name	The name of USB drive. This should only be modified if there are multiple USB devices connected to your TELSTRA ELITETM GATEWAY. The default name is "USB-Storage"

FOR WINDOWS XP:

2. Open a web-browser (such as Internet explorer, Firefox or Safari) and type in the address `\\gatewayName\"USBDriveName\"` (e.g. `\\Telstra21\USB-Storage`)

NOTE: There is no username and password required to access the USB drive, the user will be able to read/write to the folder/files on the USB drive.

**To map the USB Storage Drive**

To enable easy access to the USB Storage Drive, you can map the network location. To do this, use the following steps:

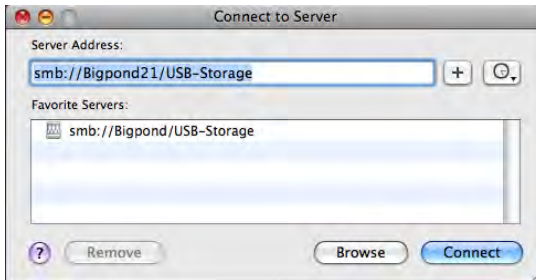
1. Click on the Start button and click My Computer
2. Click on tools > Map network drive
3. In the Folder field, enter the address of the USB Storage Drive `\\gatewayName\USBDriveName` (e.g. `\\Telstra21\USB-Storage`)
4. To access the USB Storage Drive in the future, you can simply double-click on the item in the My Computer menu

FOR MAC OSX:

2. From the Finder, select the Go and then click Connect to Server
3. In the address field of the Connect to Server dialog, type in the address:
smb://"gatewayName"/"USBDriveName" (e.g. smb://Telstra21/USB-Storage)



4. Click the + button to add this server to the list of Favourites and then click Connect

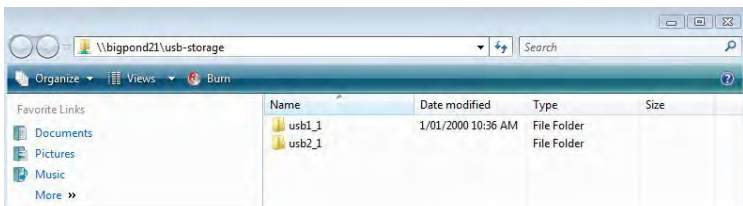


5. Select the Guest radio button and then click Connect



FOR WINDOWS VISTA

2. Open a web-browser (such as Internet explorer, Firefox or Safari)
3. Type in the address "\\gatewayName\USBDriveName\" (e.g. \\Telstra21\USB-Storage)



NOTE: There is no username and password required to access the USB drive. Any network user will be able to read/write the folder/files in the USB drive.

TO MAP THE USB STORAGE DRIVE

To enable easy access to the USB Storage Drive, you can map the network location. To do this, use the following steps:

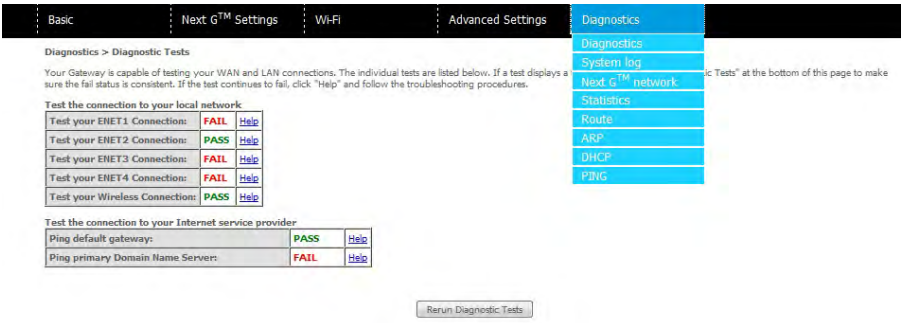
1. Click on the Start button and click Computer
2. Click the Map network drive button
3. In the Folder field, enter the address of the USB Storage Drive \\gatewayName\USBDriveName (e.g. \\Telstra21\USB-Storage)
4. To access the USB Storage Drive in the future, you can simply double-click on the item in the Computer menu

DIAGNOSTICS

DIAGNOSTICS

The Diagnostics menu has the following submenus:

- Diagnostics
- System Log
- Next G™ Network
- Statistics
- Route
- ARP
- DHCP
- PING



9.1 DIAGNOSTICS

The Diagnostics menu provides feedback on the connection status of the device. The individual tests are listed below. If a test displays a fail status click on the Help link and follow the steps shown:

- 1. Now click Re-run Diagnostic Tests at the bottom of the screen to re-test and confirm the error
- 2. If the test continues to fail contact technical support for further assistance

BasicNext G™ SettingsWi-FiAdvanced SettingsDiagnostics

Diagnostics > Diagnostic Tests

Your Gateway is capable of testing your WAN and LAN connections. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

Test the connection to your local network:

Test your ENET1 Connection:	FAIL	Help
Test your ENET2 Connection:	PASS	Help
Test your ENET3 Connection:	FAIL	Help
Test your ENET4 Connection:	FAIL	Help
Test your Wireless Connection:	PASS	Help

Test the connection to your Internet service provider:

Ping default gateway:	PASS	Help
Ping primary Domain Name Servers:	FAIL	Help

Rerun Diagnostic Tests

Field	Description
ENET Connection	Pass: Indicates that the Ethernet interface from your computer is connected to the LAN port of this gateway.
	Fail: Indicates that the gateway does not detect the Ethernet interface on your computer.
Wireless connection	Pass: Indicates that the wireless card is ON.
	Down: Indicates that the wireless card is OFF.
Ping Default Gateway	Pass: Indicates that the gateway can communicate with the first entry point to the WAN network. It is usually the IP address of the ISP's local Gateway.
	Fail: Indicates that the gateway was unable to communicate with the first entry point on the WAN network.
Ping Primary Domain Name Server	Pass: Indicates that the gateway can communicate with the primary Domain Name Server (DNS).
	Fail: Indicates that the gateway was unable to communicate with the primary Domain Name Server (DNS).

9.2 SYSTEM LOG

This function allows you to view system events and configure related options. Follow the steps below to enable and view the System Log.

1. Click Configure System Log to continue.

Basic | Next G™ Settings | Wi-Fi | Advanced Settings | Diagnostics

Diagnostics > System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

Click "View System Log" to view the System Log.

Click "Configure System Log" to configure the System Log options.

View System Log | Configure System Log

2. Select the system log options (see table below) and click Save/Apply.

Basic | Next G™ Settings | Wi-Fi | Advanced Settings | Diagnostics

Diagnostics > System Log > Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both', events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both', events will be recorded in the local memory.

Select the desired values and click 'Apply/Save' to configure the system log options.

Log: ☒ Disable ☐ Enable

Log Level:

Display Level:

Mode:

Back | Apply/Save

Name	Description
Log	Indicates whether the system is currently recording events. You can enable or disable event logging. By default, it is disabled.
Log level	<p>Allows you to configure the event level and filter out unwanted events below this level. The events range from the highest critical level</p> <p>“Emergency” down to this configured level will be recorded to the log buffer on the gateway’s SDRAM. When the log buffer is full, the newest event will wrap up to the top of the log buffer and overwrite the oldest event. By default, the log level is “Debugging”, which is the lowest critical level. The log levels are defined as follows:</p> <p>Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level emergency level will be recorded. If the log level is set to error, only error and the level above will be logged.</p>
Display Level	Allows you to select the logged events and displays on the View System Log window for events of this level and above to the highest emergency level.
Mode	<p>Allows you to specify whether events should be stored in the local memory be sent to a remote syslog server, or to both simultaneously. If remote mode is selected, the view system log will not be able to display events saved in the remote syslog server.</p> <p>When either Remote mode or Both mode is configured, the Web UI will prompt the you to enter the Server IP address and Server UDP port where syslog is running.</p>

3: Click View System Log. The results are displayed as follows.



9.3 NEXT G™ NETWORK

Select this option for detailed status information on your gateway's 3G connection.

Basic	Next G™ Settings	Wi-Fi	Advanced Settings	Diagnostics																		
Diagnostics > Next G™ network																						
<table border="1"> <tr> <td>Manufacturer</td> <td>Sierra Wireless, Inc.</td> </tr> <tr> <td>Model</td> <td>MC8700</td> </tr> <tr> <td>FW Rev</td> <td>M3.0.4.2AD</td> </tr> <tr> <td>IMEI</td> <td>356079030021509</td> </tr> <tr> <td>ESN</td> <td>D921469114510</td> </tr> </table>					Manufacturer	Sierra Wireless, Inc.	Model	MC8700	FW Rev	M3.0.4.2AD	IMEI	356079030021509	ESN	D921469114510								
Manufacturer	Sierra Wireless, Inc.																					
Model	MC8700																					
FW Rev	M3.0.4.2AD																					
IMEI	356079030021509																					
ESN	D921469114510																					
<table border="1"> <tr> <td>IMEI</td> <td>50501344273582</td> </tr> <tr> <td>HW Rev</td> <td>1.0</td> </tr> </table>					IMEI	50501344273582	HW Rev	1.0														
IMEI	50501344273582																					
HW Rev	1.0																					
<table border="1"> <tr> <td>Temperature</td> <td>60</td> </tr> <tr> <td>System mode</td> <td>WCDMA</td> </tr> <tr> <td>WCDMA band</td> <td>WCDMA800</td> </tr> <tr> <td>GSN band</td> <td>Unknown</td> </tr> <tr> <td>WCDMA channel</td> <td>4136</td> </tr> <tr> <td>GSN channel</td> <td>65535</td> </tr> <tr> <td>GSN (PS) state</td> <td>REGISTERED</td> </tr> <tr> <td>MM (CS) state</td> <td>IDLE</td> </tr> <tr> <td>Signal Strength</td> <td>-67 (dBm)</td> </tr> </table>					Temperature	60	System mode	WCDMA	WCDMA band	WCDMA800	GSN band	Unknown	WCDMA channel	4136	GSN channel	65535	GSN (PS) state	REGISTERED	MM (CS) state	IDLE	Signal Strength	-67 (dBm)
Temperature	60																					
System mode	WCDMA																					
WCDMA band	WCDMA800																					
GSN band	Unknown																					
WCDMA channel	4136																					
GSN channel	65535																					
GSN (PS) state	REGISTERED																					
MM (CS) state	IDLE																					
Signal Strength	-67 (dBm)																					
<table border="1"> <tr> <td>Signal level(RSSI)</td> <td>20</td> </tr> <tr> <td>Quality(Ec/Io)</td> <td>-8.5 dB -12.5 dB</td> </tr> <tr> <td>Network Registration Status</td> <td>registered</td> </tr> <tr> <td>Network Name</td> <td>Telstra Mobile</td> </tr> <tr> <td>Country Code</td> <td>505</td> </tr> <tr> <td>Network Code</td> <td>01</td> </tr> <tr> <td>Cell ID</td> <td>00CC14BF</td> </tr> <tr> <td>Primary Scrambling Code (PSC)</td> <td>0070 (REF)</td> </tr> <tr> <td>Data Session Status</td> <td>Connected</td> </tr> </table>					Signal level(RSSI)	20	Quality(Ec/Io)	-8.5 dB -12.5 dB	Network Registration Status	registered	Network Name	Telstra Mobile	Country Code	505	Network Code	01	Cell ID	00CC14BF	Primary Scrambling Code (PSC)	0070 (REF)	Data Session Status	Connected
Signal level(RSSI)	20																					
Quality(Ec/Io)	-8.5 dB -12.5 dB																					
Network Registration Status	registered																					
Network Name	Telstra Mobile																					
Country Code	505																					
Network Code	01																					
Cell ID	00CC14BF																					
Primary Scrambling Code (PSC)	0070 (REF)																					
Data Session Status	Connected																					
<table border="1"> <tr> <td>HSPA Category</td> <td>6</td> </tr> <tr> <td>HSPA Category</td> <td>14</td> </tr> <tr> <td>Received Signal Code Power(RSCP)</td> <td>-74 dBm -78 dBm</td> </tr> <tr> <td>Battery Connection Status(BCS)</td> <td>MT is powered by the battery.</td> </tr> <tr> <td>Battery Charge Level(BCL)</td> <td>100</td> </tr> </table>					HSPA Category	6	HSPA Category	14	Received Signal Code Power(RSCP)	-74 dBm -78 dBm	Battery Connection Status(BCS)	MT is powered by the battery.	Battery Charge Level(BCL)	100								
HSPA Category	6																					
HSPA Category	14																					
Received Signal Code Power(RSCP)	-74 dBm -78 dBm																					
Battery Connection Status(BCS)	MT is powered by the battery.																					
Battery Charge Level(BCL)	100																					

Consult the table on the next page for detailed field descriptions

Field	Description																		
Manufacturer	The manufacturer of the embedded 3G module.																		
Model	The model name of the embedded 3G module.																		
FW Rev.	The firmware version of the 3G module.																		
IMEI	The IMEI (International Mobile equipment Identity) is a 15 digit number that is used to identify a mobile device on a network.																		
FSN	Factory Serial Number of the 3G module.																		
IMSI	The IMSI (International Mobile Subscriber Identity) is a unique 15-digit number used to identify an individual user on a UMTS network.																		
HW Rev.	The hardware version of the 3G module.																		
Temperature	The temperature of the 3G module in degrees Celsius.																		
System Mode	WCDMA/Europe CMDA 2000 / America																		
WCDMA band	The 3G radio frequency band which supports dual-band UTMS/HSDPA/HSUPA frequencies (850/2100 MHz), IMT2000 is 2100 MHz, WCDMA800 is 850MHz																		
WCDMA channel	The 3G channel.																		
MM (CS) state	Circuit Switching state																		
Signal Strength	<div>The 3G signal strength in dBm.<table><tr><td>Signal level in dBm</td><td>-109 ~ -103</td><td>-101 ~ -93</td><td>-91 ~ -87</td><td>-85 ~ -79</td><td>-77 ~ -52</td></tr><tr><td>5 Signal bars</td><td colspan="5"><div><div></div><div></div><div></div><div></div><div></div></div></td></tr><tr><td>LED</td><td colspan="2">Low</td><td colspan="2">Medium</td><td>High</td></tr></table></div>	Signal level in dBm	-109 ~ -103	-101 ~ -93	-91 ~ -87	-85 ~ -79	-77 ~ -52	5 Signal bars	<div><div></div><div></div><div></div><div></div><div></div></div>					LED	Low		Medium		High
Signal level in dBm	-109 ~ -103	-101 ~ -93	-91 ~ -87	-85 ~ -79	-77 ~ -52														
5 Signal bars	<div><div></div><div></div><div></div><div></div><div></div></div>																		
LED	Low		Medium		High														

9.4 STATISTICS

These screens provide detailed information for:

- Local Area Network (LAN) and Wireless Local Area Network (WLAN)
- 3G Interfaces

NOTE: These statistics pages refresh every 15 seconds

Diagnostics > Statistics > LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	0	0	0	0	40049	178	0	0
eth1	174450	2142	0	0	262991	1925	0	0
eth2	0	0	0	0	78657	175	0	0
eth3	0	0	0	0	18783	174	0	0
wlan	0	0	0	0	0	0	76	0

Reset Statistics

9.4.1 LAN STATISTICS

This screen displays statistics for the Ethernet and Wireless LAN interfaces.

Diagnostics > Statistics > LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	0	0	0	0	42239	188	0	0
eth1	894397	2219	0	0	328119	995	0	0
eth2	0	0	0	0	42047	185	0	0
eth3	0	0	0	0	41983	184	0	0
wlan	0	0	0	0	0	0	76	0

Reset Statistics

9.4.2 NEXT G™ STATISTICS

Click Next G™ network in the Statistics submenu to display the screen below.

Diagnostics > Statistics > Next G™ network

Statistics of WAN	Inbound	Outbound
Objects	22784	771452
Packets	319	1121
Drops	0	0
Error	0	0

9.5 ROUTE

Select Route to display the paths the gateway has found.

Basic

Next G™ Settings

Wi-Fi

Advanced Settings

Diagnostics

Diagnostics > Route

Flags: U - up, I - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
10.0.0.0	0.0.0.0	255.255.255.0	U	0		br0
0.0.0.0	10.237.21.139	0.0.0.0	UG	0	ipoe_usb0	usb0

Field	Description
Destination	Destination network or destination host
Gateway	next hop IP address
Subnet Mask	Subnet mask of Destination
Flag	U: route is up
	!: reject route
	G: use gateway
	H: target is a host
	R: reinstate route for dynamic routing
	D: dynamically installed by daemon or redirect
	M: modified from routing daemon or redirect
Metric	The 'distance' to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.
Service	Shows the name for WAN connection
Interface	Shows connection interfaces

9.6 ARP

Click ARP to display the ARP information.



Field	Description
IP address	Shows IP address of a connected device
Flags	Complete Incomplete Permanent Publish
HW Address	Shows the MAC address of a connected device
Device	Shows the connection interface

9.7 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

Click DHCP to display the DHCP information.

Basic	Next G™ Settings	Wi-Fi	Advanced Settings	Diagnostics
Diagnostics > DHCP Leases				
Hostname	MAC Address	IP Address	Expires In	
NetComm	00:21:9b:d2:ba:82	10.0.0.1	0 seconds	

Field	Description
Hostname	Shows the device/host/PC network name
MAC Address	Shows the Ethernet MAC address of the device/host/Pc
IP address	Shows IP address of device/host/PC
Expires In	Shows how much time is left for each of the listed DHCP Leases

9.8 PING

The PING menu provides a connection test to an IP address or a host name.

Basic	Next G™ Settings	Wi-Fi	Advanced Settings	Diagnostics
Diagnostics > PING				
Please type in a host name or an IP Address. Click Submit to check the connection automatically.				
Host Name or IP Address: <input type="text"/>				
<input type="button" value="Submit"/>				

Input an IP address or a host name, e.g www.google.com and press Submit. The connection test result will be shown as below.

Basic	Next G™ Settings	Wi-Fi	Advanced Settings	Diagnostics
PING www.l.google.com (74.125.127.103): 56 data bytes 56 bytes from 74.125.127.103: icmp_seq=0 ttl=41 time=270.1 ms 56 bytes from 74.125.127.103: icmp_seq=1 ttl=41 time=272.0 ms 56 bytes from 74.125.127.103: icmp_seq=2 ttl=41 time=256.8 ms 56 bytes from 74.125.127.103: icmp_seq=3 ttl=41 time=272.1 ms --- www.l.google.com ping statistics --- 4 packets transmitted, 4 packets received, 0% packet loss round-trip min/avg/max = 256.8/267.7/272.1 ms <input type="button" value="Back"/>				

The above screen shows a successful ping result.

FOR MORE INFORMATION

CALL 1300 136 841

VISIT [TELSTRA.COM](https://www.telstra.com)

VISIT A TELSTRA STORE