User Manual

NetComm®

HSPA WiFi Router with Voice

TELUS Smart Hub
HSPA WiFi Router with Voice

1 Introduction

The TELUS Smart Hub creates a secure WiFi network, providing Internet access for up to 15 users and simultaneous phone service using the TELUS 3G+ network. With quick and easy setup the TELUS Smart Hub provides a landline experience without the need for fixed line connections. Simply plug the Smart Hub into a power outlet then insert an active TELUS SIM card into the slot on the rear panel to access a 3G+ Internet connection within minutes.

The TELUS Smart Hub incorporates a WLAN 802.11b/g/n access point, two Ethernet 10/100Mbps ports and two phone ports for making and receiving telephone calls. It features the latest security options such as WPA and WPA2 data encryption, SPI (Stateful Packet Inspection) Firewall and VPN pass through.

1.1 Package contents

- Smart Hub – HSPA WiFi Router with Voice
- 12VDC~1.5A Power Adapter
- RJ45 LAN Cable
- RJ11 Phone Cable
- Quick Start Guide
- Wireless Security Card
- CD (Quick Start Guide and User Manual in PDF format)

1.2 Key features

1. Up to 7.2Mbps down / 5.76Mbps up[1]
2. 2 x Voice ports (circuit-switched)
3. 1 x 10/100 LAN Ethernet port
4. 802.11n/300Mbps Wireless[2] (Backward compatible with 802.11b/g)
5. WAN Ethernet port for optional alternate Internet connectivity (ADSL/Cable/Satellite)
6. Supports auto Internet fallback to 3G+
7. 2 x Internal WiFi antennas
8. WiFi Protected Setup (WPS) for wireless connectivity
9. Browser based interface for configuration and management
10. Wireless security options- WEP, WPA, WPA2

---

1   Speeds are dependent on network coverage. See TELUS coverage maps for more details. The total number of WiFi users can also affect data speeds.

2   Maximum wireless signal rate and coverage values are derived from IEEE Standard 802.11g and 802.11n specifications. Actual wireless speed and coverage are dependent on network and environmental conditions included but not limited to volume of network traffic, building materials and construction/layout.

2 Basic Setup

2.1   A note about your SIM

Your Smart Hub will lock itself to a SIM card once it has been inserted. Once your Smart Hub has been locked to a particular SIM card, two things will happen.

1. You won't be able to use the SIM card in any other device (including other Smart Hubs).
2. You won't be able to use other SIM cards in your Smart Hub (including other TELUS SIM cards).

Please note that a firmware upgrade or factory reset will not affect the SIM lock to the Smart Hub.

For additional support please contact TELUS Client care at 1-866-558-2273

2.2   Network and system requirements

Before continuing with the installation of your Smart Hub, please confirm that you comply with the minimum system requirements below.

▪ An activated TELUS SIM card.
▪ Computer with Windows, Macintosh, or Linux-based operating systems with a working Ethernet adapter with TCP/IP Protocol installed.
▪ A Web browser such as Internet Explorer, Netscape Navigator, Mozilla Firefox, Opera, Safari etc.

Wireless device system requirements
▪ Computer or device with a working 802.11b, 802.11g or 802.11n wireless adapter.

2.3   Placement of your Smart Hub

Just like your mobile phone, the Smart Hub's location will affect its signal strength from the TELUS Mobile Base Station (Cell Tower). The data speed achievable from the Smart Hub is relative to this signal strength, which is affected by many environmental factors. When choosing a location to place your Smart Hub, please keep in mind that the Smart Hub will need adequate 3G+ signal strength in order to provide Internet connectivity.

Similarly, the wireless connection between your Smart Hub and your WiFi devices will be stronger the closer your connected devices are to your Smart Hub. Your wireless connection and performance will degrade as the distance between your Smart Hub and connected devices increases. This may or may not be directly noticeable, and is greatly affected by the individual installation environment.

If you have concerns about your network's performance that might be related to range or obstruction factors, try moving the computer or WiFi device to a position between three to five meters from the Smart Hub in order to see if distance is the problem.

Note: While some of the items listed below can affect network performance, they will not prohibit your wireless network from functioning; if you are concerned that your network is not operating at its maximum effectiveness, this checklist may help.

Please ensure that your Smart Hub's 3G external antenna is positioned vertically (toward the ceiling).

If you experience difficulties connecting wirelessly between your WiFi devices and your Smart Hub, please try the following steps:

▪ In multi-storey offices or homes, place the Smart Hub on a floor that is as close to the centre of the location as possible. This may mean placing the Smart Hub on an upper floor.
▪ Try not to place the Smart Hub near a cordless telephone that operates at the same radio frequency as the Smart Hub (2.4GHz).

2.4 Avoid obstacles and interference

Avoid placing your Smart Hub near devices that may emit radio "noise", such as microwave ovens. Dense objects that can inhibit wireless communication include:

- Refrigerators
- Washers and/or dryers
- Metal cabinets
- Large aquariums
- Metallic-based, UV-tinted windows

If your wireless signal seems weak in some spots, make sure that objects such as these are not blocking the signal's path (between your devices and the Smart Hub).

2.5 Cordless phones

If the performance of your wireless network is impaired after considering the above issues, and you have a cordless phone:

- Try moving cordless phones away from your Smart Hub and your wireless-enabled computers.
- Unplug and remove the battery from any cordless phone that operates on the 2.4GHz band (check manufacturer's information). If this fixes the problem, your phone may be interfering with the Smart Hub.
- If your phone supports channel selection, change the channel on the phone to the farthest channel from your wireless network. For example, change the phone to channel 1 and move your Smart Hub to channel 11 please see section 5.3.1 to change the Smart Hub wireless channel and see your phones user manual for changing the cordless phone's wireless channel.
- If necessary, consider switching to a 900MHz or 5GHz cordless phone.

2.6 Choose the "quietest" channel for your Wireless Network

In locations where homes or offices are close together, such as apartment buildings or office complexes, there may be wireless networks nearby that can conflict with your wireless network.

Use the Site Survey capabilities found in your Wireless client (laptop, computer, etc) to locate any other wireless networks that are available (see your wireless adapter's user manual for instructions). Switch your Smart Hub to a wireless channel not used or least used by surrounding wireless networks. Please see section 5.3.1 for assistance changing the wireless channel on your Smart Hub.

Experiment with more than one of the available channels, in order to find the clearest connection and avoid interference from neighboring cordless phones or other wireless devices. Please see the section above for changing your channel.

2.7 Connecting and configuring your Smart Hub

The Smart Hub has been designed to be placed on a desktop. All of the cables exit from the rear for better organization. The LED indicator display is visible on the front of the Smart Hub to provide you with information about network activity and device status. See below for an explanation of each of the indication lights.

Front Panel	Icon	Description
Wireless		Solid blue light when WLAN is enabled. Blinks on traffic (data transfer)
WAN		Solid blue light when the Smart Hub is connected via the WAN Ethernet Port
LAN		Solid blue light when LAN connection is established. Blinks on LAN port traffic
3G		Solid blue light when the Smart Hub is connected via 3G, blinks on traffic
Line 1		Solid blue light when the handset connected to Line 1 is off hook, blinks on incoming call.
Line 2		Solid blue light when the handset connected to Line 2 is off hook, blinks on incoming call.
Power		Solid amber light when device is powered on. Blinking during device start up.

Please note that all lights will flash simultaneously if a firmware upgrade takes place.

Rear Ports

SIM Slot	Insert your SIM card here (until you hear a click). Please be careful to insert the SIM in the correct orientation by viewing the printed icon beside the slot.
3G Antenna	Attach in the 3G Antenna here in a clockwise direction.
WAN	Optional WAN Ethernet port for Fixed Line (ADSL/Cable/Satellite) connection
LAN	LAN Port for wired Ethernet clients (Computers, Laptops, etc)
Line 1	Phone Port for Handset(s)
Line 2	Phone Port for Handset(s)
Reset/WPS	Hold this button down for over 10 seconds to reset to factory defaults.
	Hold and release this button for less than 10 seconds to enable the WPS push-button-connect function.
Power	Power connector, connects to a DC 12V 1.5A Power Adapter

2.8   Hardware installation

1. Attach the supplied antenna to the port marked 3G Antenna. [This should be attached in a clockwise direction.]
2. Insert your SIM card (until you hear a click) into the SIM slot.
   Please note – SIM cards are assigned specific rate plans for the TELUS Smart Hub. Once activated in your Smart Hub, these plans and SIM card will not work in other TELUS devices
3. For voice functionality, connect a standard Analog telephone to the port labeled Line 1 using the RJ-11 Cable provided.
4. If required, to activate jacks in your home or office connect an RJ-11 cable from the port labeled Line 2 to any wall jack.
5. Connect the power adapter to the Power socket on the back of the Smart Hub.
6. Plug the power adapter into the wall socket and switch on the power.
7. Wait approximately 60 seconds for the Smart Hub to power up.

2.9   Connecting via a cable

1. Connect the yellow Ethernet cable provided to the port marked **LAN** at the back of the Smart Hub.
2. Connect the other end of the yellow Ethernet cable to your computer.
3. Wait approximately 30 seconds for the connection to establish.
4. Open your Web browser, type 192.168.20.1 into the address bar and press enter.
5. Follow the steps to set up your TELUS Smart Hub.
6. After the setup process is completed you will be connected to the Internet

2.10 Connecting wirelessly

1. Ensure WiFi is enabled on your device (computer/laptop/Smartphone).
2. Scan for wireless networks in your area and connect to the network name that matches the Wireless Network Name found on the Wireless Security Card (included in the box).
3. When prompted for your wireless security settings, enter the Wireless Security Key listed on your Wireless Security Card.
4. Wait approximately 30 seconds for the connection to establish.
5. Open your Web browser, type 192.168.20.1 into the address bar and press enter.
6. Follow the steps to set up your TELUS Smart Hub.
7. After the setup process is completed you will be connected to the Internet.
8. To connect additional devices via WiFi, repeat steps 1 through 4.

Wireless Network Name (SSID):
Nom du réseau sans fil (SSID):
XXXXXXXXXXXXXXXXXXXXXXX

Wireless Security Key (WPA):
Clé de sécurité sans fil (WPA):
XXXXXXXXXXXXXXXXXXXXXXX

2.11 Smart Hub Default Settings

LAN (Management)

- Static IP Address: 192.168.20.1
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.20.1

WAN (Internet)

- WAN mode: DHCP

Wireless

- SSID: TELUS_Smart_Hub_xx*
- Security: WPA-PSK
- Security Key: Refer to your Wireless Security Card or label on the bottom of your Smart Hub

* For security purpose, each Smart Hub comes with a unique SSID that varies by a 2 digit number at the end eg. SSID: "TELUS_Smart_Hub_25."

Smart Hub Web Interface Access

- Username: admin
- Password: admin

APN for 3G Connection

- APN: isp.TELUS.com

2.12 First time simple configuration wizard

When you log in to your Smart Hub for the first time, you will be presented with the TELUS Smart Hub "Set-up Wizard" as shown in the screenshot below. This wizard can be skipped by clicking on the link shown on the screenshot below. You can re-run the Setup Wizard again anytime after first use by selecting the "Startup Wizard" option under the "Administration" tab in the Advanced View of the management console.
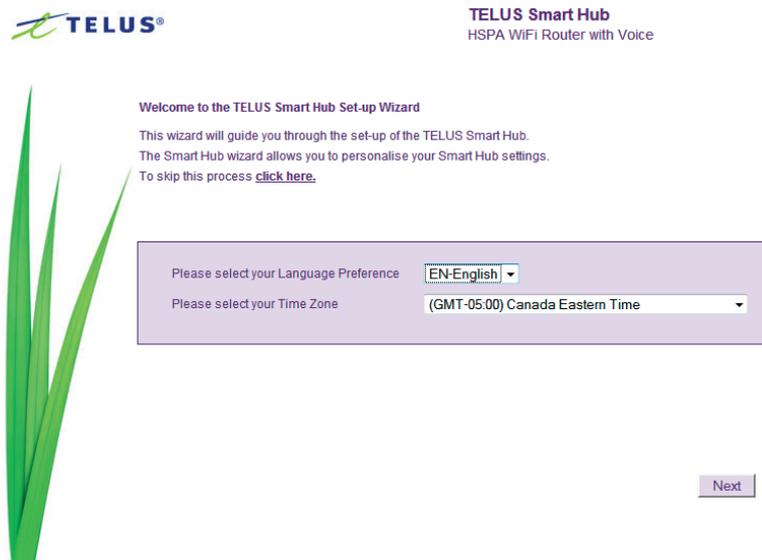
Select your Language Preference and Time Zone then click "Next";

This page allows you to customize the username and password required to administer your Smart Hub. It is recommended that you choose a unique password for added security. Please enter a user name and password that you wish to use, or leave these fields unchanged to use the default (admin/admin). Click "Next" to continue.

The next page "Smart Hub Security" allows you to configure basic WiFi settings.

Wireless (WiFi):	"On" by default. Changing this option to "Off" will turn off the wireless feature. Your Smart Hub will no longer broadcast a WiFi network and you will not be able to connect to your Smart Hub via WiFi devices.
SSID Broadcast Name (Max 32 Characters):	The SSID (Service Set Identifier) is the name of the wireless network broadcast by your Smart Hub. Use a unique name to identify your wireless network so that you can easily connect from your wireless clients. This field is case sensitive and can be up to 32 characters. You should change the default SSID for added security.
SSID Broadcast:	Select 'Disable' to hide the SSID of your Smart Hub. If disabled, other people will not be able scan and detect your Smart Hub's SSID. Your Smart Hub will continue to broadcast the wireless network and you or other users who you have provided the SSID to will be able to connect to the Smart Hub

Configure your Wireless settings in this page then click "Next";

This page allows you to configure WiFi security settings for your Smart Hub. Setting up a high wireless security level can prevent unauthorized access to your wireless network. WPA2-PSK with the AES algorithm is recommended for maximum security, followed by WPA-PSK with TKIP for strong security with maximized compatibility for older devices. Click "Next" to continue after choosing your security settings.

Review your settings then click "Finish" to save configuration. Click "Back" if you want to make changes.

After clicking Finish, the Smart Hub will save your configuration and reboot itself. Please wait as this process takes approximately 2 minutes. You will be guided back to the Management Console once the process is complete.

2.13 Management Console login procedure

After the first time setup wizard has been run, the management console will be password protected to prevent unauthorized access to the configuration settings of your Smart Hub.

To log in to the Management Console and view the status and make changes to your Smart Hub, please follow the steps below:

1. Open your web browser (e.g. Internet Explorer/Firefox/Safari) and navigate to http://192.168.20.1
2. Enter the username and password configured during the first time setup wizard and click submit. The default username and password is admin if the details haven't been customized. Click Login to continue.

Please Note – If you forget the username and password you selected during the Smart Hub set-up process, holding the reset button for over 10 seconds will restart the unit with the original settings (username: admin / password: admin).

3 Using the Smart Hub to make and receive telephone calls

The Smart Hub provides circuit switched voice services via two telephony line interfaces offering the ability to make and receive telephone calls via a regular analog telephone using the TELUS 3G+ mobile network.

It's important to note that the Smart Hub has two separate line interfaces (ports) that share a single outbound/inbound telephone line. This means that a handset(s) connected via one port will not be able to use the line at the same time as a handset(s) connected via the other port.

If a call is already in progress via the first port, the user on the handset(s) connected to the second port will receive a busy signal.

Incoming calls will ring and can be answered on either port, however once a call is answered from one port, the handset(s) on the second port will receive a busy signal.

3.1 Handset requirements

The Smart Hub allows you to make telephone calls over the TELUS 3G+ network using a standard analog telephone via the built in RJ-11 Phone ports. Please refer to the documentation provided by the manufacturer of your analog telephone for assistance with the operation of your telephone handset.

3.2 Maximum REN Loading

Please note that each of the line interfaces on the Smart Hub is capable of supporting multiple analog telephones connected via splitters. The ringer equivalence number (REN) for each line is 5. Therefore, a maximum of 5 handsets each with a REN number of 1 can be connected to each line port.

Before you start making any phone calls, make sure you checked the following:

1. You have an activated TELUS SIM card inserted prior to powering on the Smart Hub.
2. Your Smart Hub is powered on and in running condition.
3. A working analog telephone connected into either the Line 1 or Line 2 port.
4. You hear the dial tone and the Line LED on the front of your Smart Hub should light up after lifting the handset.

3.3 How to place a call

To make a call, simply lift the handset and dial the number following the instructions provided by your telephone handset manufacturer.

3.4 How to receive a call

When an incoming call is received, both Line 1 and Line 2 lights will start flashing and any phones connected to the Smart Hub will ring. Answer the telephone following the instructions provided by your telephone handset manufacturer to conduct the call.

Please note that if the call is answered from a telephone connected to Line 1, telephones connected to Line 2 will receive a busy tone for the duration of the call.

If no phone is connected the Smart Hub, all incoming calls will be transferred to voicemail.

3.5   Accessing voicemail

1. To access your voicemail, please dial your own mobile number from the Smart Hub and follow the prompts.
2. To access another TELUS voicemail number from the Smart Hub, please dial ## followed by the 10 digit number.

3.6   Calling features

3.6.1   Quick Reference Table

The Smart Hub supports a number of calling features for supplementary services. Please check your Smart Hub monthly plan for included calling features or speak with a TELUS representative to have additional features added.

Feature	Activation	Deactivation	Status
Caller ID	#31# (to block an individual call)	*31#(to unblock an individual call)	N/A
Call Waiting	*43#	#43#	*#43#
Unconditional Call Forwarding	*21*<Directory Number> #	#21#	*#21#
No-reply Call Forwarding	*61* <Directory Number > #	#61#	*#61#
Busy Call Forwarding	*67* <Directory Number > #	#67#	*#67#
Unreachable Call Forwarding	*62*<Directory Number >#	#62#	*#62#

3.6.2   Caller ID

Caller ID transmits a caller's number to the called party's telephone equipment when the call is being set up but before the call is answered. Where available, caller ID can also provide a name associated with the calling telephone number.

- To force Caller ID to be blocked for an outbound call, dial #31# followed by the number you wish to dial.
- To force Caller ID to be unblocked for an outbound call, dial *31# then follow the dialing number.

3.6.3   Call Waiting

Call waiting allows for indication and answering of an incoming telephone whilst an existing call is underway.

- To disable call waiting, dial #43#, and hang up after you hear 2 high pitch beeps.
- To enable call waiting, dial *43#, and hang up after you hear 2 low pitch beeps.
- To check the status of Call Waiting, dial *#43# or view the advanced status page of the management console.
    a. Call waiting is disabled if you hear 2 high pitch beeps.
    b. Call waiting is enabled if you hear 2 low pitch beeps.

- To answer a 2nd incoming call, press Recall/Flash [Wait for a dialtone] and then dial 2
- To reject a 2nd incoming call, press Recall/Flash [Wait for a dialtone] and then dial 0
- To end the 2nd current call and return to the other call, press Recall/Flash [Wait for a dialtone] and then dial 1

Call forwarding (or call diverting), is a feature that allows an incoming call to be redirected to another number depending on the circumstances at the time of receiving the call.

Note: The Call Waiting feature will automatically turn off if you enable Call forwarding. Call Waiting will need to be enabled again after Call Forwarding is disabled.

3.6.4   Call Forwarding Unconditional

Call forwarding Unconditional will divert all incoming calls to a phone number that you desire.

- To enable Call Forwarding Unconditional, dial *21*<Directory Number> # (Where directory number is the number you wish to forward calls to)
- Hang up after you hear 2 low pitch beeps.
- To disable Call Forwarding Unconditional, dial #21#
- Hang up after you hear 2 high pitch beeps.
- To check the status of Call Forwarding Unconditional, dial *#21# or view the advanced status page of the management console.
    a. Call Forwarding Unconditional is disabled if you hear 2 high pitch beeps.
    b. Call Forwarding Unconditional is enabled if you hear 2 low pitch beeps.

3.6.5   Call Forwarding No Answer
Call forwarding No Answer will divert all incoming calls to a phone number that you desire only if the incoming call is not answered.

- To enable Call Forwarding No Answer, dial *61* <Directory Number > #
- (Where directory number is the number you wish to forward calls to)
- Hang up after you hear 2 low pitch beeps.
- To disable Call Forwarding No Answer, dial #61#
- Hang up after you hear 2 high pitch beeps.
- To check the status of Call Forwarding No Answer, dial *#61# or view the advanced status page of the management console.
    a. Call Forwarding No Answer is disabled if you hear 2 high pitch beeps.
    b. Call Forwarding No Answer is enabled if you hear 2 low pitch beeps.

3.6.6   Call Forwarding Busy
Call forwarding busy will divert all incoming calls to a phone number that you desire only if your telephone is busy on another call.

- To enable Call Forwarding Busy, dial *67* <Directory Number > #
- (Where directory number is the number you wish to forward calls to)
- Hang up after you hear 2 low pitch beeps.
- To disable Call Forwarding Busy, dial #67#
- Hang up after you hear 2 high pitch beeps.
- To check the status of Call Forwarding Busy, dial *#67# or view the advanced status page of the management console.
    a. Call Forwarding Busy is disabled if you hear 2 high pitch beeps.
    b. Call Forwarding Busy is enabled if you hear 2 low pitch beeps.

3.6.7   Call Forwarding Not Reachable
Call forwarding busy will divert all incoming calls to a phone number that you desire only if your telephone is unreachable by the network.

- To enable Call Forwarding Not Reachable dial *62*<Directory Number >#
- (Where directory number is the number you wish to forward calls to)
- Hang up after you hear 2 low pitch beeps.
- To disable Call Forwarding Not Reachable, dial #62#
- Hang up after you hear 2 high pitch beeps.
- To check the status of Call Forwarding Not Reachable, dial *#62# or view the advanced status page of the management console.
    a. Call Forwarding No Answer is disabled if you hear 2 high pitch beeps.
    b. Call Forwarding No Answer is enabled if you hear 2 low pitch beeps.

Please confirm the feature codes supported on your service by checking your plan or by consulting a TELUS representative.

3.6.8   Conference Call
To turn a two-party call into a three-party conference call, follow the instructions below.

- To start a 3way conference call between a held call and an active call, press Recall/Flash [Wait for a dialtone] and then dial 3
- To originate a 2nd call whilst already on a call, press Recall/Flash [Wait for a dialtone] and then dial the other party. Wait for the party to answer then press hook-flash and dial 3

3.6.9   Troubleshooting
What do I do if I have no dial tone?
Please follow the procedure listed below:

1. Check to make sure the phone is plugged into your Smart Hub on either Line 1 port or Line 2 port.
2. Check to make sure you are using the correct cable (Cat-3 UTP Telephone Cable with RJ-11 plugs).
3. Check to make sure the line light on the front panel of the Smart Hub turns solid blue if you lift the handset.
4. Check to make sure the blue 3G indication light on the front of the Smart Hub is blinking.
5. Check to make sure your TELUS SIM card is activated and insert into your Smart Hub properly.
6. If after these steps there is still no dial tone, reboot your Smart Hub by holding the reset button for 10-15 seconds (please note this will reset any stored user configurations).
7. Check and see if you get the dial tone after rebooting your Smart Hub.

I have noise interference during telephone calls. How can I fix this?
To resolve this issue, try the following:
- Verify that the RJ-11 cable is securely connected and not damaged.
- Try to remove any telephone splitters from the connection between your phone and the Smart Hub.
- Try rebooting your Smart Hub.

4 Management Console

4.1 Basic Status overview

The basic status page provides basic system related information. It is shown after logging in to the Smart Hub, and can also be accessed by selecting Basic Status from the menu.
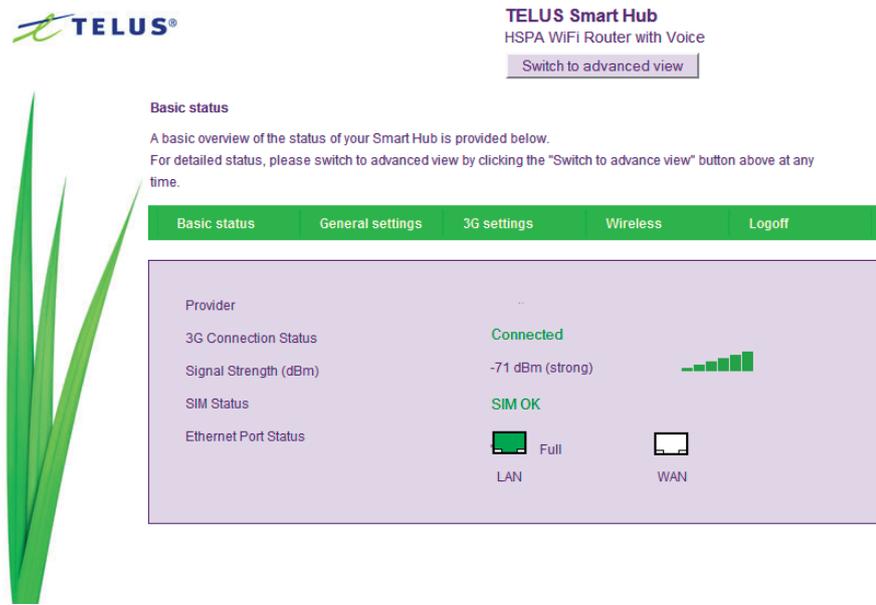
The status page shows the 3G connection status, Signal Strength (dBm), SIM Status and Ethernet Port Status.

4.2 General settings
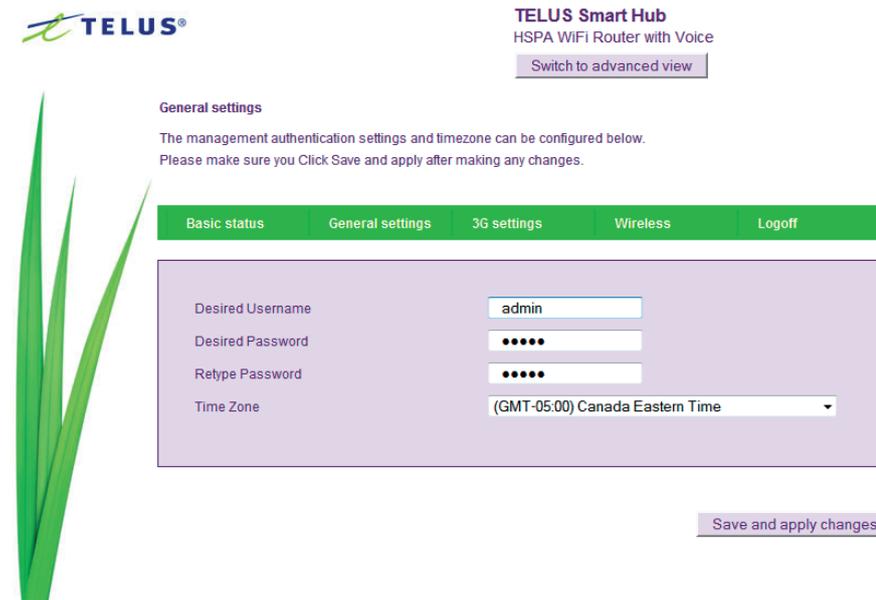
The General Settings tab allows you to change your Web Interface login name/Password and the Time Zone used on the Smart Hub.

4.3 3G settings

The 3G Operation mode can be configured on this page. This allows for automatic failover to be configured if desired. Please see the table below for options allowed for the 3G operation mode:

'Always ON'	Enables the 3G internet connection and, does not disconnect, even if idle.
'OFF'	The Smart Hub will not connect to the Internet
'Automatic 3G Backup'	The Automatic 3G Backup feature of the Smart Hub is designed to provide a backup 3G Internet connection when you use the WAN connection as your primary, when the primary fails. The Internet connection will automatically switch back to your WAN connection once your WAN Internet connection is back online. To use this feature, you will need both an Ethernet WAN connection (from an xDSL modem/ISDN/Satellite etc) and a 3G connection. To configure your WAN settings according to your network environment, please switch to advanced view □ "Internet Settings" □"WAN". Click "Save and apply settings" to finish.

4.4   Wireless
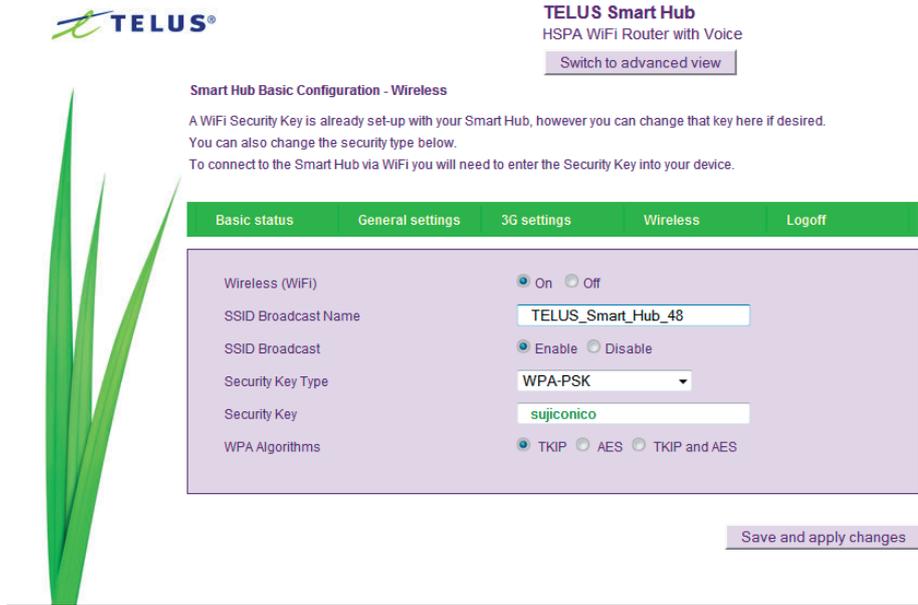
This page allows you to configure basic WiFi settings for this device such as enabling/disabling the WiFi functionality, changing the Wireless Network Name (SSID) and Wireless Security settings.

Wireless (WiFi) ON/OFF:	Changing this option to Off will turn off the WiFi network broadcast feature on the Smart Hub and you will not be able to connect to your Smart Hub wirelessly.
SSID Broadcast Name (SSID):	The SSID (Service Set Identifier) is the name of your wireless network. Use a unique name to identify your wireless device so that you can easily connect to it from your wireless clients. This field is case sensitive and can be up to 32 characters.
SSID Broadcast:	Select 'Disabled' to hide the SSID of your Smart Hub. If disabled, other people will not be able to easily see your Smart Hub's SSID. To add wireless devices with broadcast disabled, the SSID will need to be manually configured on each wireless device.
Security Key Type:	Select the security type for the wireless network. You may choose from the following wireless security options: WPA-PSK, WPA2-PSK, WPA-PSK-WPA2-PSK.
Security Key:	The default WPA-PSK key is printed on the wireless security card and on the Product ID on the bottom of the Smart Hub. Please note the key can be customized on this page, however the key will revert to the default (printed on the Product ID) if the Smart Hub is reset to factory default.

5 Advanced Features

The basic configuration interface is intended to provide access to all the settings that most people will want to use on their Smart Hub. There are advanced settings available, if desired, which are accessible by viewing the advanced settings pages. Click "Switch to advanced view" for configuring the advanced features of your Smart Hub.

5.1   Status

The status page provides system related information and is displayed when you login to the Smart Hub management console and switch to Advanced View. By default, the status page will show System Info, Local Network, WWAN, Connection Status and Ethernet Status.

To view either WAN, PPPoE or PPTP status individually, click on their relevant buttons below the green menu bar. To view them all, click on the All Status button.

5.2 Internet Settings

5.2.1 3G Internet Settings

This page allows you to setup your WWAN (Wireless Wide Area Network) connection.

The 3G settings on your Smart Hub are preconfigured for the TELUS Network. It is recommended that you do not change the settings unless advised by a TELUS representative.

The Smart Hub's 3G Internet Settings can be viewed and configured by selecting the "3G Internet Settings" menu item under the "Internet Settings" tab in the Advanced View of the Management Console.

Item	Description
Profile Name	Description for the profile
APN	Please enter the APN name you wish to connect to in this field. Please don't edit this unless you are aware of what effect it will have.
3G NAT	Enabled by Default, this option allows you to switch NAT (Network Address Translation) on or off.
Interface Metric	This field allows you to customize the metric of the 3G interface. This setting will have no effect for most users, but may be required for advanced routing configurations (Static Routes, RIP, VPN, etc)
Operation Mode	There are 3 Options as follows:
'Always ON'	Keeps the Internet connection alive, does not disconnect
'OFF'	Does not connect to the Internet
'Automatic 3G Backup'	The Automatic 3G Backup feature of the Smart Hub is designed to provide a backup 3G Internet connection when you use the WAN connection as your primary, when the primary fails.

The Internet connection will automatically switch back to your WAN connection once your WAN Internet connection is back online.

To use this feature, you will need both an Ethernet WAN connection (from an xDSL modem/ISDN/Satellite etc) and a 3G connection. |

5.2.2   Band Settings

The Smart Hub's Band and Operator Settings can be viewed and configured by selecting the "Band Settings" menu item under the "Internet Settings" tab in the Advanced View of the Management Console.

Band Settings: By default the Smart Hub will automatically choose the operator and band based on the SIM card inserted. If required, you can choose a specific band or operator on this page.

5.2.3   WAN

The WAN page allows you to configure the optional WAN Ethernet port. Select the WAN connection type suitable for your environment and configure parameters according to the selected connection type.

The Smart Hub's WAN Ethernet Settings can be viewed and configured by selecting the "WAN" menu item under the "Internet Settings" tab in the Advanced View of the Management Console.

5.2.3.1   STATIC (fixed IP)

If your WAN connection uses a static IP address, please select "STATIC(fixed IP)" and fill in the required information in the fields provided.

Name	Description
IP Address	Type in the IP address assigned by your Internet Service Provider
Subnet Mask	Type in the Subnet mask assigned by your Internet Service Provider
Default Gateway	Type in the WAN Gateway assigned by your Internet Service Provider
Primary/Secondary DNS	Type in the DNS address assigned by your Internet Service Provider
MAC Clone	Please input the MAC address if your computer here if your service provider only permits computers with a certain MAC address to access the internet. If you are using the computer which used the connect to the internet via a cable modem you can simply press the 'Default' button to fill the MAC address field with the MAC address of your computer.

Click 'Apply' to save the settings.

5.2.3.2   DHCP

This connection will get the IP address from the Internet service provider. Leave everything as default unless instructed by your Internet Service Provider.

Name	Description
Host Name	Please input the host name of your computer. This is optional, and only required if your service provider asks you to do so.
Mac Clone	Please input the MAC address of your computer here if your service provider only permits computers with a certain MAC address to access the Internet. If you are using a computer which used to connect to Internet via a cable modem, you can simply press the 'Default' button to fill the MAC address field with the MAC address of your computer.

Click 'Apply' to save the settings.

5.2.3.3   PPPoE (ADSL)

Most ADSL/ADSL2+ services use the PPP over Ethernet protocol. Use this if you connect your Smart Hub to a bridged ADSL modem.

Name	Description
Username/ Password	Please input the host name of your computer. This is optional, and only required if your service provider asks you to do so.
Operation Mode - There are 3 Modes	
Keep Alive	Keeps the internet connection alive, does not disconnect.
On Demand	Only ocnnects to the internet when there's a connect attempt
MAC Clone	Please input the MAC address of your computer here if your service provider only permits computers with a certain MAC address to access the Internet. If you are using a computer which used to connect to Internet via a cable modem, you can simply press the 'Default' button to fill the MAC address field with the MAC address of your computer.

Click 'Apply' to save the settings.

5.2.3.4   PPTP

Name	Description
Server IP	Type in the server IP address assigned by your Internet Service Provider.
User Name/ Password	Type in the username and password assigned by your provider.
Address Mode	Select Dynamic if your service uses a DHCP server, or select Static and type in the IP address, Subnet Mask and Default Gateway assigned by your Internet Service Provider.
Operation Mode	
'Keep Alive'	Keeps the Internet connection alive, does not disconnect.
'On Demand'	Only connects to Internet when there's a connection attempt
'Manual'	Only connects to the Internet when the 'Connect' button on this page is pressed, and disconnects when the 'Disconnect' button is pressed.
Mac Clone	Please input the MAC address of your computer here if your service provider only permits computers with a certain MAC address to access the Internet. If you are using a computer which used to connect to the Internet via a cable modem, you can simply press the 'Default' button to fill the MAC address field with the MAC address of your computer.

Click 'Apply' to save the settings.

5.2.4   WAN Failover Backup

The WAN Failover Backup feature of the Smart Hub is designed to provide a backup 3G Internet connection in case your primary connection should fail. To use this feature, you will need both an Ethernet WAN connection (from an xDSL modem/ISDN/Satellite etc) and a 3G WAN connection.

To set up WAN failover on your Smart Hub, first tick "Enable automatic 3G backup", then fill in the fields that appear. The Smart Hub's Internet failover settings can be viewed and configured by selecting the "WAN" menu item under the "Internet Settings" tab in the Advanced View of the Management Console.

WAN Failover Backup	
Automatic 3G backup	Enable
Profile Name	Telus ISP
APN	isp.telus.com
3G NAT	Enable
Interface Metric	20
Internet Host	www.google.com
	Apply Cancel

Name	Description
Automatic 3G Backup	Default setting is "Enable". Please leave it as "Enable" if you intend to turn on the Automatic 3G Backup function.
Internet Host	Enter an Internet address here to check the Internet Connection. The default value is www.google.com.
APN	Enter the APN for your 3G connection (e.g isp.telus.com)
Interface Metric	The default value is 20; please enter the valid value from 1 to 9999 suitable for your network environment.

Click' Apply' to save the settings.

5.2.5 LAN

The Smart Hub's LAN Settings can be viewed and configured by selecting the "LAN" menu item under the "Internet Settings" tab in the Advanced View of the Management Console.

LAN functionality of the Smart Hub can be configured from this page. Using this page, a user can change the LAN Subnet, gateway IP address, DHCP settings, Static DHCP Lease settings, and many others.

Name	Description
IP Address	The local IP address of Smart Hub
Subnet Mask	The subnet mask for the local network.
LAN 2	Used to configure a secondary LAN IP Address (optional)
LAN 2 IP Address	The local IP address of the secondary LAN IP Address
LAN2 Subnet Mask	The subnet mask of the secondary IP Address
DHCP Type	Please leave this set to "Server" unless you have another DHCP server on the same network.
Start IP Address	The Start IP address of your DHCP IP Pool.
End IP Address	The End IP address of your DHCP IP Pool.
Subnet Mask	The subnet mask of the IP Address
Primary DNS Server/ Secondary DNS Server	This Feature allows you to manually assign DNS Servers
Default Gateway	The default is the IP of your Smart Hub
Lease Time	DHCP Lease time of the DHCP Client of your Smart Hub
Statically Assigned	This feature allows you to statically assign IP addresses to the MAC Addresses. The Format of MAC address is XX:XX:XX:XX:XX:XX
802.11d Spanning Tree	The default is "Disable", select "Enable" to enable this feature.
LLTD	Link Layer Topology Discovery (LLTD). The default is "Disable", select "Enable" to enable this feature.
IGMP Proxy	Internet Group Management Protocol (IGMP), The default is "Disable", select "Enable" to enable this feature.
UPnP	Universal Plug and Play (UPnP), The default is "Enabled", select "Disable" to disable this feature.
Router Advertisement	The default is "Disable", select "Enable" to enable it.
PPPoE relay	The default is "Disable", select "Enable" to enable it.
DNS Proxy	The default is "Enable", select "Disable" to disable it.

Click 'Apply' to save the settings.

5.2.6 Advanced Routing

This page allows you to configure static and dynamic routing rules for your Smart Hub.

The Smart Hub's Advanced Routing Settings can be viewed and configured by selecting the "Advanced Routing" menu item under the "Internet Settings" tab in the Advanced View of the Management Console.
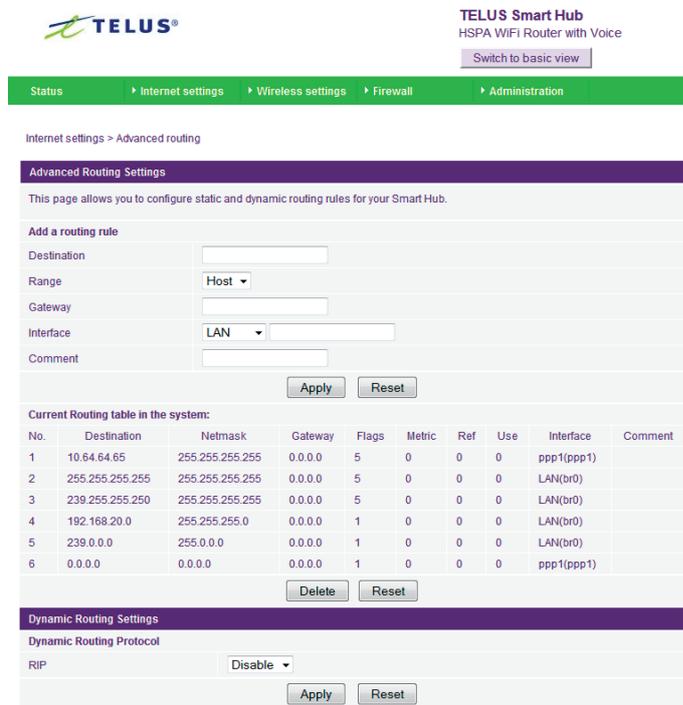
5.2.6.1 Advanced Routing – Static

Static Routing allows computers that are connected to your Smart Hub to communicate with computers on another LAN segment which are connected to it via another router. To set a rule, you need to specify the following:

- Destination
- Subnet mask
- Gateway
- Interface

5.2.6.2 Advanced Routing – Dynamic

Dynamic Routing uses the RIP protocol to allow the Smart Hub to adapt to changes in the network. RIP enables the device to determine the best route for each packet based on the "hop count" or number of hops between Source and Destination. To enable Dynamic Routing, select Enable from the drop box and click Apply.

5.2.7 DHCP Client List

This page allows you to view the current DHCP clients that have obtained IP leases from your Smart Hub. The MAC address, assigned IP address and the expiry period is shown for all computers who have automatically obtained addresses from the Smart Hub. Please note that this list is stored in the device's volatile memory, and is therefore cleared if the device is reset or if any changes are applied to configuration.

The Smart Hub's DHCP Client list can be viewed by selecting the "DHCP clients" menu item under the "Internet Settings" tab in the Advanced View of the Management Console.

5.3 Wireless Settings

5.3.1 Basic

This page allows you to define the basic wireless settings for the Smart Hub.

The Smart Hub's basic Wireless settings can be viewed and configured by selecting the "Basic" menu item under the "Wireless Settings" tab in the Advanced View of the Management Console.

Radio On/Off: On by default. Changing this option to off will turn off the wireless network broadcast functionality on the Smart Hub and you will not be able to connect to your Smart Hub wirelessly.

Network Mode: You can select which wireless standards are able to connect to your wireless network:

11b/g mixed mode: Both 802.11b and 802.11g wireless devices are allowed to connect to your Smart Hub.

11b only: Select this if all of your wireless clients are 802.11b.

11g only: Select this if all of your wireless clients are 802.11g.

11/b/g/n Mixed mode: Select this if 802.11b and 802.11g and 802.11n wireless devices are in your network.

- Network Name (SSID): The SSID (Service Set Identifier) is the name of your wireless network. Use a unique name to identify your wireless device so that you can easily connect to it from your wireless clients. This field is case sensitive and can be up to 32 characters. You should change the default SSID for added security.
- Frequency (Channel): This setting configures the frequency that the Wireless Radio uses for wireless connectivity. Select one channel that you wish to use from the drop down list.
- WDS Mode: WDS (Wireless Distribution System) is a system that enables the wireless interconnection of access points, and allows a wireless network to be expanded using multiple access points without a wired backbone to link them. Each WDS Access Point needs to be set with the same channel and encryption type.

Click 'Apply' to save the settings.

5.3.1 Basic

5.3.2   Advanced

This page allows you to modify the advanced wireless settings for your Smart Hub. These settings should not be changed unless you are aware of what effect they will have.

The Smart Hub's advanced Wireless settings can be viewed and configured by selecting the "Advanced" menu item under the "Wireless Settings" tab in the Advanced View of the Management Console.

BG protection mode:	It is recommended to use this option in a mixed mode (11b/g) environment. It is used by the 11g clients to reserve bandwidth with the Access Point by informing the 11b clients to hold their transmission, using a CTS-to-self packet.
Beacon Interval:	Interval of time in which the wireless router broadcasts a beacon which is used to synchronize the wireless network.
Data Beacon Rate (DTIM):	Enter a value between 1 and 255 for the Delivery Traffic Indication Message (DTIM). A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages
Fragment Threshold:	This specifies the maximum size of a packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.
RTS Threshold:	When the packet size is smaller than the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.
AP Isolation:	This feature allows you to isolate clients on your wireless network. To enable communication between the wireless clients connected to your Smart Hub, select Disabled. To terminate the communication between the wireless clients, please choose Enabled.
TX Power:	This determines the output power of the antenna
WMM Capable:	WMM (WiFi MultiMedia) if enabled, supports QoS for experiencing better audio, video and voice in applications
WMM Parameters:	Click on the WMM Configuration button to configure the WMM parameters
Broadcast Network Name (SSID):	Select 'Disabled' to hide the SSID of your Smart Hub. If disabled, other people will not be able scan and detect this product's SSID.

Click Apply to save the settings.

5.3.3 Security

This page allows you to configure the wireless security for your Smart Hub. Setting up sufficient wireless security can prevent unauthorized access to your wireless network. The Smart Hub's Wireless Security settings can be viewed and configured by selecting the "Security" menu item under the "Wireless Settings" tab in the Advanced View of the Management Console.

SSID Choice: Select the SSID that you wish to configure the security settings of.

Security Mode: Select the security mode for the wireless network. See below for more information

Access Policy: This feature allows MAC Address Control, which prevents unauthorized clients from accessing your wireless network. Select whether to allow/block users on the policy list, and add their MAC addresses to the list on the format XX:XX:XX:XX:XX:XX

Click 'Apply' to save the settings.

5.3.3.1   Security Mode

You may choose from the following wireless security options: Disabled, Open, Shared, WEP AUTO, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA-PSK-WPA2-PSK, WPA1-WPA2 or 802.1x.

WEP

WEP (Wired Equivalent Privacy) helps prevent against unwanted wireless users accessing your Smart Hub. It offers a lower level of security in comparison to WPA-PSK and WPA2-PSK.

WPA1/WPA2

WPA (WiFi Protected Access) authentication is suitable for enterprise applications. It must be used in conjunction with an authentication server such as RADIUS to provide centralized access control and management. It provides a stronger encryption and authentication solution.

WPA-PSK/WPA2-PSK

A newer type of security is WPA-PSK (TKIP) and WPA2-PSK (AES). This type of security gives a more secure network compare to WEP. Use TKIP Encryption Type for WPA-PSK and AES for WPA2-PSK. After that, please enter the key in the PassPhrase field. The key needs to be more than 8 characters and less than 63 characters and it can be any combination of letters and numbers. Please note that the configuration for WPA-PSK and WPA2-PSK is identical.

Your Smart Hub uses WPA-PSK by default. Check your Wireless Security Card or device label on the bottom of the Smart Hub for your default SSID and Security key to begin connecting your wireless devices.

802.1x

In order to use 802.1X security, you need to have a RADIUS server on your network that will act as the authentication server. Please type in the details for your RADIUS server in the fields required.

Note: After configuring wireless security, you also need to configure your wireless adapter to use the same security settings before you can connect wirelessly. Not all wireless adapters support WPA-PSK/WPA2-PSK/WPA/WPA2 security; please refer to your wireless adapter user guide for more details. It is strongly recommended to set up a simple wireless security such as WPA-PSK (when the wireless client supports WPA-PSK) in order to secure your network. Most wireless adapters in computers and laptops support at least WEP and WPA.

5.3.4   WiFi Protected Setup (WPS)

WPS is the simplest way to establish a connection between wireless clients and your Smart Hub. This method removes the need to manually select the encryption mode and fill in the PassPhrase. You only need to press a button on both wireless client and the Smart Hub, and the WPS will do the rest for you. The Smart Hub supports two types of WPS:

WPS via Push Button – you have to push a specific button on the wireless client or in your wireless client utility to start the WPS mode. Then switch the Smart Hub to WPS mode. You can simply push the WPS button of the wireless router, or click the 'Start to Process' button in the web configuration interface.

WPS via PIN code – you have to know the PIN code of the wireless client and switch it to WPS mode, then input the wireless client PIN to the Smart Hub web interface.

The Smart Hub's WPS settings can be viewed and configured by selecting the "WPS" menu item under the "Wireless Settings" tab in the Advanced View of the Management Console.
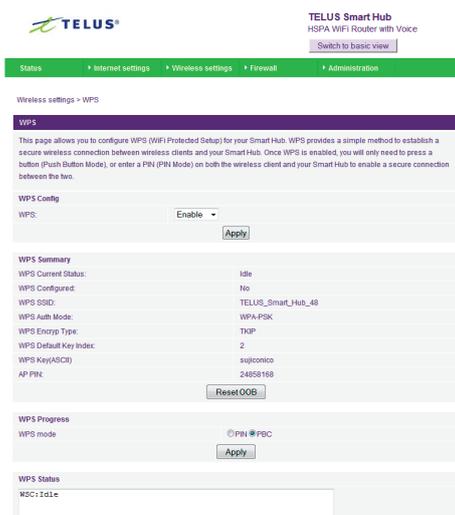
WPS	Use the drop box to either enable or disable the WPS function.
WPS Current Status	If the wireless security (encryption) function of this wireless router is properly set, you will see a 'Success' message here. Otherwise, you will see 'Idle'.
WPS SSID	This is the network broadcast name (SSID) of the router.
WPS Auth Mode	It shows the active authentication mode for the wireless connection.
WPS PIN	This is the WPS PIN code of the wireless router. You may need this information when connecting to other WPS-enabled wireless devices.
WPS Mode	Select either PIN mode or PBC (which is the WPA via Push Button).

5.3.5   Station List

The Station List shows the wireless devices currently associated with your Smart Hub. The wireless clients connected to your Smart Hub are shown by selecting the "Station List" menu item under the "Wireless Settings" tab in the Advanced View of the Management Console.

5.4 Firewall

5.4.1 MAC/IP/Port Filtering

This page allows you to setup MAC, IP and port filtering rules to protect your network from malicious activity. The filtering rules can be used to either allow or block certain users and/or ports from accessing the Internet. The Smart Hub's MAC/IP/Port Filtering settings can be viewed and configured by selecting the "MAC/IP/Port Filtering" menu item under the "Firewall" tab in the Advanced View of the Management Console.

5.4.1.1 Basic Settings

MAC/IP/Port Filtering: Select Enable to enable MAC/IP/Port Filtering

Default Policy: Select whether packets that do not match any rules are accepted or dropped

5.4.1.2 MAC/IP/Port Filtering Settings

MAC Address: MAC address of a local computer

Dest IP Address: Destination IP Address for the filter rule

Source IP Address: Source IP Address for the filter rule

Protocol: Select the port number protocol type (TCP, UDP or both). If you are unsure, then leave it to the default "TCP&UDP" setting

Dest Port Range: Destination Port Range of the filter rule

Source Port Range: Source Port Range of the filter rule

Action: Either accept or drop the packet that matches the rule

Comment: Add a comment to identify the rule (optional)

Click 'Apply' to save the settings.

5.4.2 Port Forwarding

This page allows you to configure port forwarding rules to allow remote users to access services such as Web (HTTP) or FTP on your local computers. This allows you to redirect a particular port number (from the Internet/WAN port) to a particular LAN IP address. Port forwarding can be viewed and configured on the Smart Hub by selecting the "Port Forwarding" menu item under the "Firewall" tab in the Advanced View of the Management Console.

Virtual Server Settings: Enable/Disable port forwarding.

IP Address: The LAN IP address that the public port number packet will be sent to.

Port Range: The public port numbers to be sent to the specific LAN IP address.

Protocol: Select the port number protocol type (TCP, UDP or both). If you are unsure, then leave it as the default "TCP&UDP" setting

Comment: Add a comment to identify the rule (optional)

Click' Apply' to save the settings.

5.4.3   DMZ

If you have a client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, then you can open up the firewall restrictions to allow unrestricted two-way Internet access by defining a DMZ Host.

The DMZ function allows you to re-direct all packets going to your WAN port IP address, to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server re-directs a particular service/Internet application (e.g. FTP, websites) to a particular LAN client/server, whereas DMZ re-directs all packets (regardless of services) going to your WAN IP address to a particular LAN client/server. The Smart Hub's DMZ settings can be viewed and configured by selecting the "DMZ" menu item under the "Firewall" tab in the Advanced View of the Management Console.
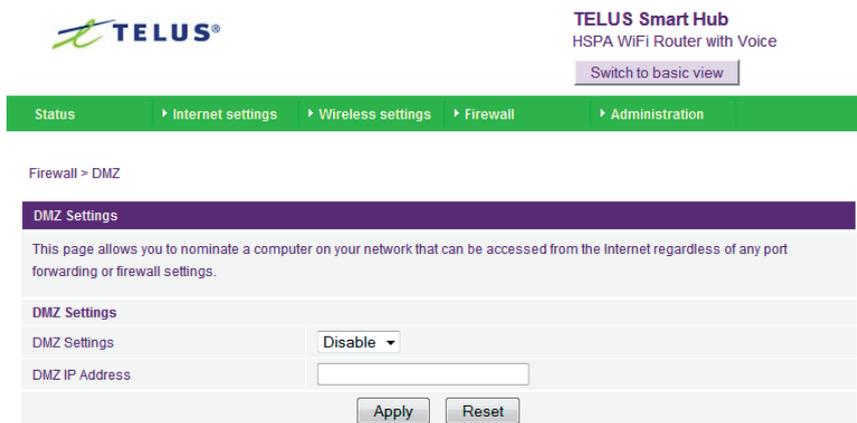
DMZ Settings: Enable/disable DMZ.

DMZ IP Address: Fill in the IP address of a particular host in your LAN Network that will receive all the packets originally going to the WAN port/Public IP address of your Smart Hub.

Click 'Apply' to save the above configurations.

5.4.4   System Security

This page allows you to improve the security of your Smart Hub through the SPI (Stateful Packet Inspection) firewall and remote access settings. The Smart Hub's system security settings can be viewed and configured by selecting the "System Security" menu item under the "Firewall" tab in the Advanced View of the Management Console.
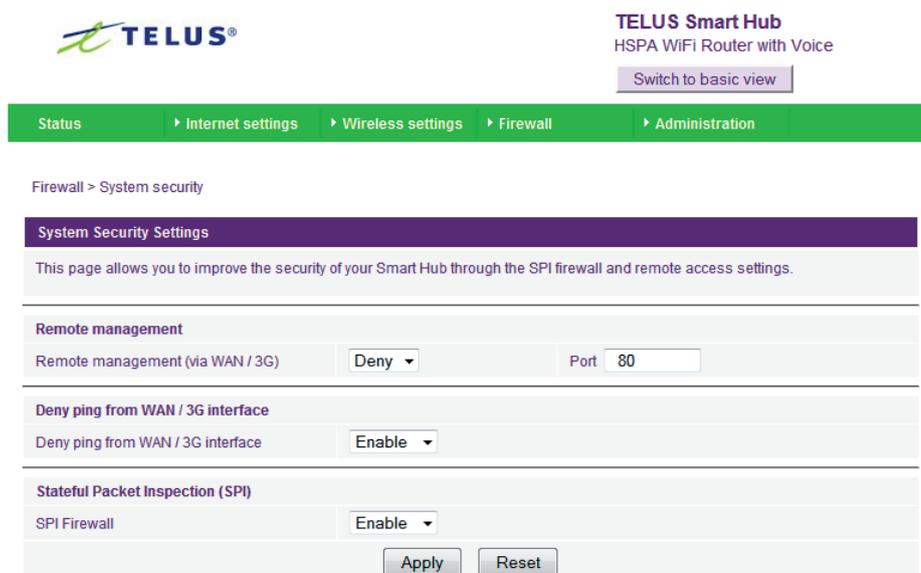
Remote Management (via WAN): Enable/Disable remote management on the WAN interface.

Deny ping from WAN interface: Select Enable to deny ICMP packets received on the WAN interface. Otherwise, select "Disable" to allow ICMP packets received on the WAN interface.

SPI Firewall: Enable/Disable the SPI (Stateful Packet Inspection) firewall to improve the security of your Smart Hub.

Click 'Apply' to save the settings.

5.4.5 Content Filtering

This page allows you to configure content, URL and host filters to restrict improper content access from LAN computers. The Smart Hub's content filtering settings can be viewed and configured by selecting the "Content Filtering" menu item under the "Firewall" tab in the Advanced View of the Management Console.

Web Content Filter: Tick the boxes to enable Proxy, Java or ActiveX content filtering. Click "Apply" to save the settings.

URL Filter: Block access to a website by entering its full URL address and clicking Add. Rules can be deleted at any time via this page.

Host Filter: Block access to certain websites by entering a keyword. Rules can be deleted at any time via this page.

5.5   Administration

5.5.1   Start Wizard

If you wish to re-run the initial setup wizard, you can do so by selecting the "Start Wizard" menu item under the "Administration" tab in the Advanced View of the Management Console.

5.5.2   Management

This page allows you to configure administrator system settings including the administrator username and password, NTP settings, and DDNS settings. The Smart Hub's administration settings can be viewed and configured by selecting the "Management" menu item under the "Administration" tab in the Advanced View of the Management Console.

Administrator Settings (account/password): Configure a new administrator username and password.

NTP Settings: The NTP (Network Time Protocol) settings allow your router to synchronize its internal clock with the global Internet Time. These settings will affect functions such as System Log entries and Firewall settings.

DDNS: DDNS (Dynamic Domain Name Service) allows you to map a static domain name to a dynamic IP address. To use this features, you must sign up for an account from a DDNS service provider. This router supports DynDNS, TZO and other common DDNS service providers.

Green AP: To provide optional reduction in power usage, you can assign a particular time to reduce the WiFi power output. Please note that a reduction in the WiFi power output can potentially reduce coverage, data throughput speeds, and stability. If you are having problems with your WiFi coverage, stability, or throughput speed, please disable the GreenAP functionality.

Click 'Apply' to save the settings.

5.5.3 System Monitor

The System Monitor functionality of the Smart Hub can be viewed and configured by selecting the "System Monitor" menu item under the "Administration" tab in the Advanced View of the Management Console.

The Periodic Ping Reset Monitor configures the Smart Hub to transmit controlled ping packets to user specified IP addresses. If the router does not receive a response to the pings the router will reset the cellular data connection. The purpose of this feature is to ensure recovery of the device if the internet connection disconnects and does not reconnect for some reason.

This feature works as follows:-

- Every "Periodic Ping Timer" value in seconds, the Smart Hub sends 3 consecutive pings to the "Destination Address".
- If all 3 pings fail the Smart Hub sends 3 consecutive pings to the "Second Address".
- The Smart Hub then sends 3 consecutive pings to the "Destination Address" and 3 consecutive pings to the "Second Address" every "Periodic Ping Accelerated Timer" seconds.
- If all accelerated pings in the step above fail, the Smart Hub resets the cellular data connection after waiting the amount of time entered in the "Fail Count" times.

"Periodic Ping Timer" should never be set to a value less than 60 seconds; this is to allow the Smart Hub time to reconnect to the cellular network following a reboot.

To disable the Periodic Ping Reset Monitor simply set to "Fail Count" 0

The Smart Hub can be configured to automatically reboot on a periodic interval specified in minutes. While this is not necessary, it does ensure that in the case of remote installations it will reboot the Smart Hub if some anomaly occurs.

The default value is 0 which disables the Periodic Reset Timer.

The maximum value is 65535 minutes.

5.5.4   Upload Firmware

This page allows you to upgrade the Smart Hub's internal software. To upgrade the firmware of your Smart Hub, you need to download the upgrade image file to your local hard disk, and then click the Browse button to locate the firmware file on your computer. The firmware loaded on the Smart Hub can be upgraded by selecting the "Upload Firmware" menu item under the "Administration" tab in the Advanced View of the Management Console.

Once you have selected the new firmware file, click 'Apply' to start the upgrade process.
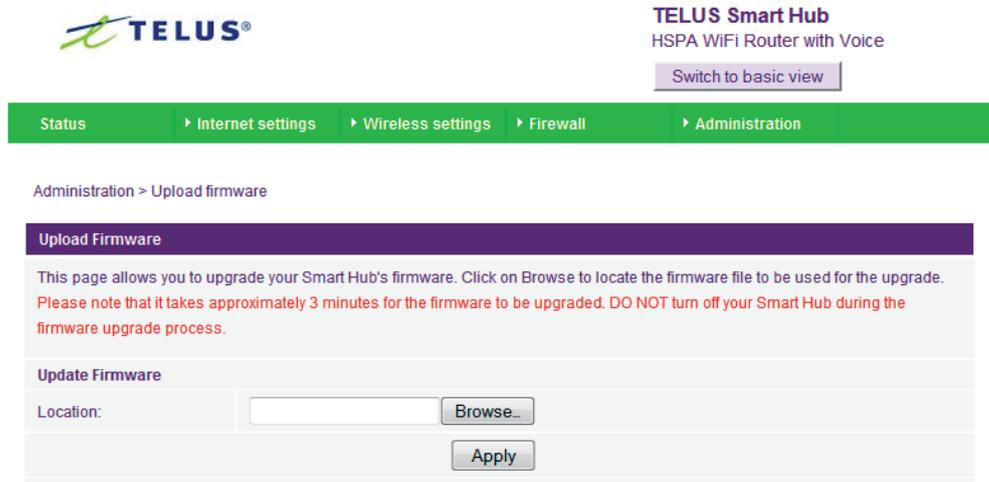
The upgrade process takes several minutes, so please be patient whilst this process is carried out. All lights on the front of the Smart Hub will flash during the firmware upgrade. Please make sure the power supply is uninterrupted during the upgrade process.

5.5.5   Settings Manager

This page allows you to import/export the system settings, reset your Smart Hub to factory defaults, or reboot your Smart Hub. The Smart Hub's configuration settings can be managed by selecting the "Settings Manager" menu item under the "Administration" tab in the Advanced View of the Management Console.
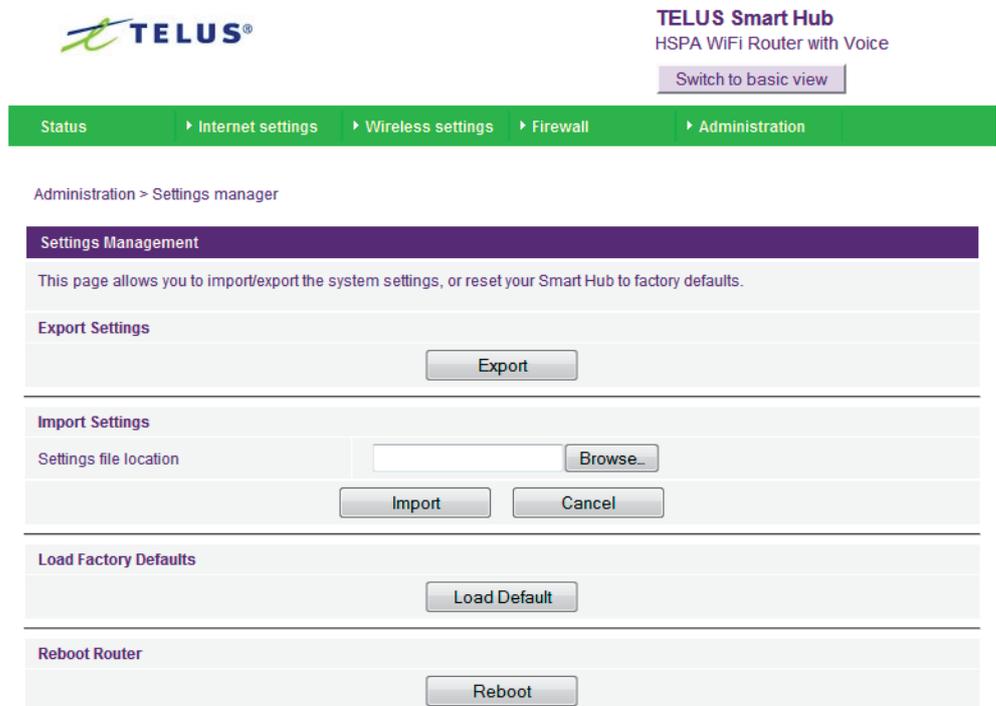
5.5.6 Statistics

This page allows you to view the LAN, WAN and wireless statistics of your Smart Hub.

The Smart Hub's advanced statistics can be viewed by selecting the "Statistics" menu item under the "Administration" tab in the Advanced View of the Management Console.

5.5.7 System Log

All important system events are logged. You can use this page to check the log of your Smart Hub for troubleshooting and diagnostic purposes. The Smart Hub's System Log can be viewed by selecting the "System Log" menu item under the "Administration" tab in the Advanced View of the Management Console.

6 FAQ

Q. Does the Smart Hub require any configuration out of the box?

A. No. The Smart Hub is plug and play device. Plug the device into an electrical outlet and once the status indicator lights are on, plug in your landline (Analog) phone and LAN cable for voice and data connectivity. For WiFi connectivity the SSID (Service Set Identifier) and network key (password) are located on the bottom of the device. If you would like to customize your settings you can enter 192.168.20.1 into your Web browser to access the Management Console and device settings.

Q. What are the minimum requirements for my system and network to work with the Smart Hub?
- A compatible TELUS SIM card with an active Smart Hub service plan
- A computer with Windows, Macintosh, or Linux-based operating systems with a working Ethernet adapter with TCP/IP Protocol installed or
- A computer with a working wireless adapter
- A Web browser such as Internet Explorer, Netscape Navigator, Mozilla Firefox, Opera, Safari etc.

Q. How can I see the data usage on my Smart Hub?

A. Any TELUS subscriber can log into www.TELUSmobility.com/youraccount to view the data usage on their TELUS device. TELUS Business Clients - log in to your TELUS account, select 'e.care', then click the 'view airtime usage' or 'view data usage' link to get details.

Q. Can I make voice calls from the Smart Hub?

A. Yes. By simply connecting a regular landline (Analog) telephone to the port labeled Line 1 using the RJ-11 Cable provided. To activate the phone jacks in your home or office connect an RJ-11 Cable from the port labeled "Line 2" to any wall jack. When you lift the receiver you will hear a dial tone and can place your call.

Q. How do I see I have a voicemail message?

A. Voicemail is a feature of the TELUS network and your TELUS service, not a feature embedded in the device. If you have a voicemail messages waiting you will hear an intermittent dial tone on your phone, and if your phone has a message waiting indicator light, it will be lit.

Q. Why am I not able to see I have a voicemail waiting?

A. The Smart Hub service plans include TELUS Voicemail to Text service. Once enabled, your voicemails will be converted to text and emailed to the address you specify. Once this process is setup you will not see a message waiting indicator on the Smart Hub, however you can still dial in to your voicemail should you want to check your messages in that way. If you do not enable your TELUS Voicemail to Text service you should receive your voicemail messages in your voicemail inbox, and see the message waiting indicator light on the Smart Hub blink.

Q. Is the Smart Hub secure; can other people access my wireless network?

A. The Smart Hub comes configured with WPA-PSK WiFi security enabled. When you first access the Internet, type 192.168.20.1 into the address bar, the wizard will pop up to configure your computer to connect with the security setting (please see the Quick Start Guide for more information on connecting your data devices to the Smart Hub). Only people you allow access to, will be able to connect to the Smart Hub ensuring your connection is secure and safe.

Q. Can I change the name and password of my wireless network?

A. Yes. You can change your Smart Hub settings from the browser user interface by typing 192.168.20.1 into the address bar of your Web browser. You can change the SSID (Service Set Identifier), security standard (WPA, WPA2, WEP) and your WiFi password.

Q. How do I share my Internet connection, using the Smart Hub, with other users?

A. Provide any users you want to share your WiFi Internet connection with, the SSID (Service Set Identifier) and WiFi network password for your Smart Hub. Each user will need to select the Smart Hub SSID, on their WiFi enabled computer or device and enter the network password you provide.

Q. What is the difference between upload and download speeds and why do they differ?

A. Upload is when you send information (e.g. emails) from your computer and download is when you receive information via the Internet. The speeds at which upload and download operate depend on the way you use the Internet and the size of files you send and receive.

Q. Do I need to attach an antenna on this device?

A. Yes. Your Smart Hub comes equipped with an antenna, you need to attach the 3G+ antenna to get the 3G+ signal.

Q. I seem to have low 3G+ signal strength, what should I do?

A. Just like your mobile phone, the Smart Hub's location will affect its signal strength to the 3G Mobile Base Stations (Cell Tower). The data speed achievable from the Smart Hub is relative to this signal strength, which is affected by many environmental factors. Please keep in mind that the Smart Hub will need adequate signal strength in order to provide Internet connectivity when choosing a location to place your Smart Hub.

Similarly to the 3G connectivity aspect, the WiFi connection between the Smart Hub and your WiFi devices will be stronger the closer your connected devices are to your Smart Hub. Your WiFi connection and performance will degrade as the distance between your Smart Hub and connected devices increases. This may or may not be directly noticeable, and is greatly affected by the individual installation environment.

If you have concerns about your WiFi network's performance that might be related to range or obstruction factors, try moving the computer (or WiFi device) to a position between 3 to 5 metres from the Smart Hub in order to see if distance is the problem. If difficulties persist even at close range, please contact TELUS Client Care.

Generally speaking, the following steps are advisable to follow to improve your WiFi performance:

- Ensure that your Smart Hub is positioned vertically.
- In multi-storey office locations or homes, place the Smart Hub on a floor that is as close to the centre of the location as possible. This may mean placing the Smart Hub on an upper floor.
- Try not to place the Smart Hub near a cordless telephone that operates at the same radio frequency as the Smart Hub's WiFi radio (2.4GHz)

Q. I have lost the security card that came with the setup instructions. What can I do?

A. If you have lost your security card, and forgotten the wireless security details (SSID and WiFi network password), there is a label stuck to the base of your Smart Hub with all your original security details. If the label is unreadable or has been removed, the WiFi network password can be viewed/reset by logging in to the Management Console using an Ethernet Cable connected to the LAN port of the Smart Hub.

Q. I forgot my Management Console password. What can I do?

A. If you have forgotten your Management Console password and cannot access the Web user interface, you will need to reset your Smart Hub back to default settings. To reset your device press and hold the reset button on the back of your Smart Hub for 10-15 seconds, all the indicator lights on the unit will flash when your device is reset. After a reset, the default WiFi settings (SSID and WPA key) can be found on the base of your Smart Hub. (Note - this will also reset any custom settings and passwords you may have already set up).

Q. Can I use the Smart Hub overseas?

A. No. The Smart Hub is not equipped for international roaming or data services. If you require the capability to call international locations, please speak with your TELUS representative or call Client Care to enable international calling on your Smart Hub.

Q. What do the LED lights represent?

A. Your Smart Hub shows you the status of the following:

- 3G+ signal
- WiFi signal
- LAN ports status
- Line/Phone status
- Power status

Q. Can I use a SIM card from other carriers in the Smart Hub?

A. No, the Smart Hub is built to connect only to the TELUS network and SIM cards from other carriers will not provide any service when inserted into the Smart Hub.

Q. Can I use the Smart Hub SIM card in other TELUS devices?

A. No, the Smart Hub SIM card is locked to the Smart Hub and will not work or provide voice or data service in other TELUS devices.

Q. Can I use other TELUS SIM cards in the Smart Hub?

A. No, other TELUS SIM cards (and rate plans) will not work in the Smart Hub. Any other TELUS SIM cards inserted into the Smart Hub will become locked to the device and will not provide service.

7 Legal & Regulatory Information

This manual is copyright. Apart from any fair dealing for the purposes of private study, research, criticism or review, as permitted under the Copyright Act, no part may be reproduced, stored in a retrieval system or transmitted in any form, by any means, be it electronic, mechanical, recording or otherwise, without the prior written permission of NetComm Limited. NetComm Limited accepts no liability or responsibility, for consequences arising from the use of this product.

NetComm Limited reserves the right to change the specifications and operating details of this product without notice.

NetComm is a registered trademark of NetComm Limited.

All other trademarks are acknowledged the property of their respective owners.

7.1 FCC Warning

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

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

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

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

7.2   IC Important Note

IC Radiation Exposure Statement:

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

The County Code Selection feature is disabled for products marketed in the US/Canada.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that required for successful communication

This device has been designed to operate with an antenna having a maximum gain of 4.35 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

NetComm

NETCOMM LIMITED Head Office
PO Box 1200, Lane Cove NSW 2066 Australia
P: 02 9424 2070 **F:** 02 9424 2010
E: int.sales@netcomm.com.au
W: www.netcommlimited.com

NETCOMM LIMITED Head Office
PO Box 1200, Lane Cove NSW 2066 Australia