

Telstra Outdoor Gateway with Indoor Access Point



Copyright
Copyright©2012 NetComm Wireless. All rights reserved.

Copyright

Copyright© 2012 NetComm Wireless Limited. All rights reserved.

The information contained herein is proprietary to NetComm Wireless Limited. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of NetComm Wireless Limited.



Please note: This document is subject to change without notice.

When this equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separately from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this device can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste. You may be subject to penalties or sanctions under the law. Instead, ask for disposal instructions from your municipal government.

Please be responsible and protect our environment.

This manual covers the following products:

Telstra Outdoor Gateway with Indoor WiFi Access Point

DOCUMENT VERSION	DATE
1.0- Initial document release	25/10/2012

Table 1 - Document Revision History

Table of Contents

Overview	4
Product Introduction	5
Physical Dimensions and Indicators.....	7
Default Settings	12
Implementation and Deployment Scenario	14
Installation and Configuration of the Outdoor Gateway	15
Logging in via the web-based user interface	16
Status	17
Advanced Status	19
Internet Settings.....	21
Mobile Broadband	21
LAN.....	26
Routing.....	28
VPN	33
USSD.....	41
Wireless Settings	42
Basic.....	42
Advanced.....	45
MAC Filter	46
Station Info	47
Services	48
Dynamic DNS	48
NTP.....	48
System Monitor	49
SNMP	50
SMS.....	51
System.....	61
Log	61
Load / Save.....	62
Administration.....	66
System Configuration.....	67
TR-069.....	68
Logoff.....	69
Reboot	69
Configuration of the Indoor WiFi Access Point	70
Status	70
DHCP Server.....	71
Wireless 2.4GHz and 5GHz.....	71
WDS Setting.....	72
WPS Setting	72
Wireless Client List.....	73
Change Password	73
System Time.....	73
Restore Settings	74
Firmware Upgrade	74
Backup Settings	74
Reset to Default	75
Reboot	75
Miscellaneous.....	75
Logout	75
Technical Data.....	76
Additional Product Information.....	78
Unlocking the SIM.....	78
Appendix A: Tables	79
Legal and Regulatory	80

Overview

Introduction

This document details the process of installing the outdoor gateway and indoor access point as well as mounting and deployment advice. This advice will include a few demonstration deployments and an explanation of related technologies that this outdoor gateway is suitable for.

Prerequisites

Before continuing with the installation of your Telstra Outdoor Gateway and Indoor WiFi Access Point, please confirm that you comply with the minimum system requirements below.

- An activated 3G SIM card.
- Device with a working Ethernet or wireless (802.11b/g/n) network adapter
- A Web Browser such as Internet Explorer, Netscape Navigator, Mozilla Firefox, Opera, Safari etc.

Notation

The following symbols are utilised in this installation manual:



The following note requires attention



The following note provides a warning



The following note provides relevant information

Product Introduction

Product Overview

- Powerful and flexible industrial cellular router platform supporting various networks and service types: UMTS/HSDPA/HSUPA & GSM/GPRS/EDGE
- Industrial Features – rugged enclosure, wide operating temperature range -25°C to 75°C, IP67 rating (sealed against water and dust), wall or pole mount option.
- Multiple power options – Power over Ethernet (PoE) 48V DC, optional 8-28V DC power supply or PoE with DC power as a backup.
- Web interface for easy centralized configuration and management from any PC.
- 10/100Base-TX port with Auto MDIX for Ethernet connections.
- VPN support for establishing a secure connection over a public cellular network using OpenVPN, PPTP or GRE
- Supports SNMPv1/v2 with cellular specific MIB.
- Supports PPPoE, MAC Filtering, PPP (PAP/CHAP), RIPv1/v2, VRRP, Dynamic DNS, NAT, DMZ.
- System monitoring, diagnostic log viewer via browser, system status and security logs, firmware upgrade via LAN or Over-The-Air (FOTA).
- WiFi IEEE 802.11b/g/n 2T2R, Peak Data Rate: Max 300Mbps¹ (MIMO, WPA2).

Package Contents

The Telstra Outdoor Gateway package consists of:

- Telstra Outdoor Gateway
- AC/DC Converter (ADP-48) with Power Cord
- PoE Injector (STB-48V)
- 2 x Wi-Fi Antennas (Type N)
- 2 x 3G Antennas (Type N)
- 4 x Mounting screws (Diameter = 6mm, Length = 14.85mm)
- 4 x Wall mounting screws (Diameter = 6mm, Length = 25mm)
- Hose clamps for pole mounting (1" to 3")
- Mounting bracket
- 10m outdoor rated Cat 5e Ethernet cable with IP67 Water-proof Plug Cable Gland
- Ferrite Core
- Indoor WiFi Access Point
- Indoor WiFi Access Point Power Supply
- Wi-Fi Antenna for Indoor Access Point
- 1.5m Cat 5e Ethernet cable
- Wireless Security Card

If any of these items are missing or damaged, please contact NetComm Support immediately by visiting the NetComm Support website at: <http://www.netcommwireless.com/contact-forms/support>

¹ 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.

Product Features

The Telstra Outdoor Gateway is designed to deliver high speed internet to homes and businesses with otherwise little to no Internet access available. It is a robust 3G (DC-HSPA+) outdoor gateway which can be pole or wall mounted and connects to the Telstra 3G network. The gateway features a powerful antenna system and wireless radio together in a single unit. This tight integration between the radio receiver and antenna system in an outdoor unit provides great benefits to signal strength compared with separated solutions involving signal degradation along lengthy antenna cabling. The gateway integrates a powerful Sierra Wireless module (MC8801) and delivers download speeds of up to 42Mbps which is then transmitted via Ethernet to the Indoor WiFi Access Point inside the property.

Power is delivered to the outdoor gateway via Power over Ethernet technology making installation quick and easy as there is no power source required at the outdoor mount point, and both power and data can be provided via a single cable from inside the property. With an IP67 rating, the device also withstands diverse temperature and weather environments.

The Indoor WiFi Access Point provides all your wireless devices inside your property with network access. The access point is dual band, enabling you to connect devices on both 2.4GHz and 5GHz radio bands. The WiFi Access Point also has 4 Ethernet ports allowing you to connect up to 3 devices via Ethernet (1 port is used to connect to the outdoor gateway).

Physical Dimensions and Indicators

LED Indicators

The Telstra Outdoor Gateway uses 7 LEDs to display the current system and connection status.

Note: 3G signal strength lower than -109dBm is considered too low for data connection. In this case, all five signal strength LEDs will stay off.



Figure 1 – Telstra Outdoor Gateway LED Indicators

TELSTRA OUTDOOR GATEWAY			
LED INDICATOR	ICON	COLOUR	DEFINITION
High Signal		Green	High 3G Signal strength available (-77 dBm to -47 dBm).
Medium to High Signal		Green	Medium to High 3G Signal strength available (-85 dBm to -78 dBm).
Medium Signal		Green	Medium 3G Signal strength available (-91dBm to -86 dBm).
Low to Medium Signal		Green	Low to Medium 3G Signal strength available (-101 dBm to -92 dBm).
Low Signal		Green	Low 3G Signal strength available (-109 dBm to -102 dBm).
Internet		Green	The Gateway is currently connected to the Internet.
Power		Orange	The unit is powered on.

Table 2 - LED Indicators

The 5 LEDs also indicate whether the device is MEP locked, SIM is not inserted and if the SIM is PIN or PUK locked by flashing in certain patterns. Below is a table outlining the various LED flash sequences and their meanings.

LED PATTERN	DESCRIPTION
All signal LEDs flash ON and OFF every 2 seconds	SIM not inserted
The signal LEDs flash in a pattern with one, three and 5 LEDs flashing in a sequence.	MEP Lock
The signal LEDs flash in a sequential order starting with the Low signal LED to the High signal LED.	SIM is PIN locked
The signal LEDs flash in a sequential order starting with the High signal LED to the Low signal LED.	SIM is PUK locked

Physical Dimensions

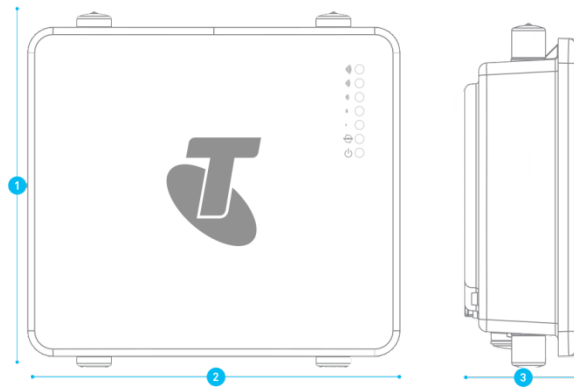


Figure 2 – Telstra Outdoor Gateway Dimensions

OUTDOOR GATEWAY (WITHOUT ANTENNAS ATTACHED)	
Length	255 mm
Depth	80 mm
Height	240 mm
Weight	1750 g <i>(w/o mounting bracket and antennas)</i>

Table 3 - Device Dimensions

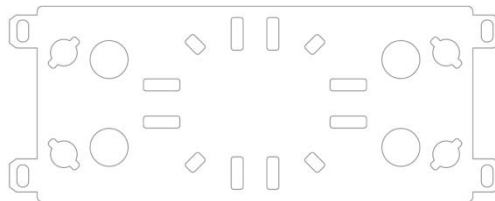


Figure 3 – Outdoor Gateway Mounting Bracket

OUTDOOR MOUNTING BRACKET	
Length	110 mm
Depth	12 mm
Height	290 mm
Weight	410 g <i>(w/o Telstra Outdoor Gateway attached)</i>

Table 4 - Mounting Bracket Dimensions



Figure 4 – Outdoor Gateway Antenna

3G AND WIFI ANTENNA	
Length	180 mm
Diameter	20 mm
Weight	60 g <i>(w/o Telstra Outdoor Gateway attached)</i>

Table 5 - Antenna Dimensions

Interfaces

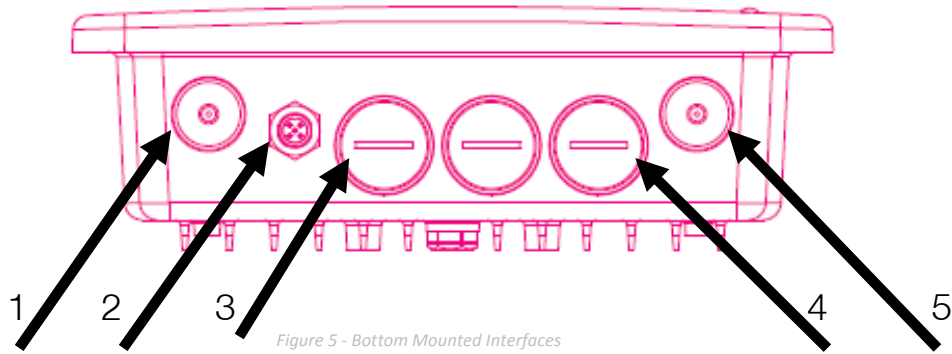


Figure 5 - Bottom Mounted Interfaces

ITEM	INTERFACE	FUNCTION
1	WiFi antenna connector (Type N)	Connect one of the WiFi antennas here.
2	DC power port	Connect the optional DC power supply to the outdoor gateway.
3	10/100Base-TX Ethernet RJ-45 (w/auto MDX) port	Connect the outdoor gateway to an Ethernet enabled device or Switch and deliver power through Power over Ethernet (PoE) technology.
4	Mini USB 2.0 Console Port	Connect a Mini USB cable to access the NTC-30WT console.
	Reset	Reset the gateway to factory defaults.
	SIM card reader	Insert an active SIM to provide 3G connectivity.
5	WiFi antenna connector (Type N)	Connect one of the WiFi antennas here.

Table 6 - Bottom Mounted Interfaces

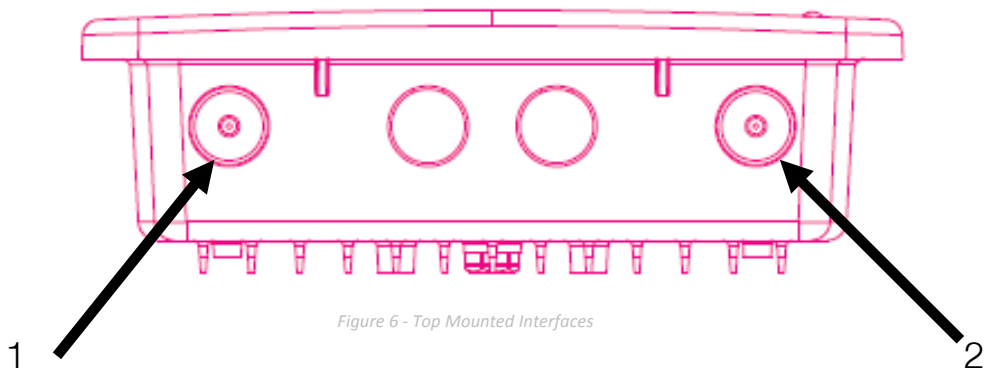


Figure 6 - Top Mounted Interfaces

ITEM	INTERFACE	FUNCTION
1	1 x 3G Aux antenna connector (Type N)	Connect one of the 3G antennas here.
2	1 x 3G Main antenna connector (Type N)	Connect one of the 3G antennas here.

Table 7 - Top Mounted Integrated Interfaces

Default Settings

The following tables list the default settings for the Telstra Outdoor Gateway.

LAN (MANAGEMENT)	
Static IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.1.1

Table 8 - LAN Management Default Settings

WIRELESS (WIFI)	
SSID:	NetComm XXXX <i>(where XXXX is 4 random numbers)</i>
Security:	WPA2-PSK
Security Key:	XXXXXXXXXX <i>(where XXXXXXXXXXX are 10 random characters)</i>

Table 9 - WiFi Default Settings



For security purposes, it is recommended to change the Default SSID and Wireless Security Key.

ADMIN MANAGER ACCOUNT		ROOT MANAGER ACCOUNT	
Username:	admin	Username:	root
Password:	admin	Password:	admin

Table 10 - System Management Accounts



Note: The admin manager account allows you to manage most of the settings of the router except functions such as Firmware Upgrade, Device Configuration Backup, Mobile Broadband Connection settings, and Reset to Factory Default Settings, which are privileged only to the root manager account. First time users should use the root manager account to configure Mobile Broadband settings.

Restoring Factory Default Settings

Restoring the gateway's factory default settings will erase any configuration changes you have made to the gateway. You may encounter situations where you need to restore the factory defaults on your gateway such as:

- You have lost your username and password and are unable to login to the web configuration page.
- You are asked to perform a factory reset by support staff.

There are two methods you can use to restore factory default settings on your Telstra Outdoor Gateway:

- Using the web-based user interface
- Using the reset button on the interface panel of the gateway

Using the web-based user interface

In order to restore your gateway to its factory default settings, please follow these steps:

1. Ensure that your outdoor gateway is powered on (for at least 10 seconds);
2. Use a paper clip or a pencil tip to depress the reset button for ten seconds and release. At this point, the reset is in progress. Do not power off the unit.
3. Logon to the default web interface page at <http://192.168.1.1> using `root` as the User Name and `admin` as the password. You will be re-directed into the gateway recovery mode. Select the **System** menu option and then click **Load/Save**. Press the Restore button to complete the factory reset.
4. When the Power light returns to a steady red, the reset is complete. The default settings are now restored. The entire process takes about 45 seconds to complete.

Using the reset button on the interface panel of the gateway

Hold the reset button down until all LEDs on the front panel of the gateway stop flashing simultaneously and then release the button. The gateway will restore the factory default settings and reboot.

Once you have reset your Telstra Outdoor Gateway to its default settings you will be able to access the device's configuration web interface using <http://192.168.1.1> with username `admin` and password `admin`.

Implementation and Deployment Scenario

The Telstra Outdoor Gateway is a robust 3G (DC-HSPA+) router that connects to the 3G network and is mounted either on the wall or a pole and positioned in an optimal position on the outside of a property. The gateway features a powerful antenna system and radio modem together in the one unit in an outdoor location. This tight integration between the radio receiver and antenna system in an outdoor unit provides great benefits to signal strength compared with separated solutions resulting in signal degradation along lengthy antenna cabling.

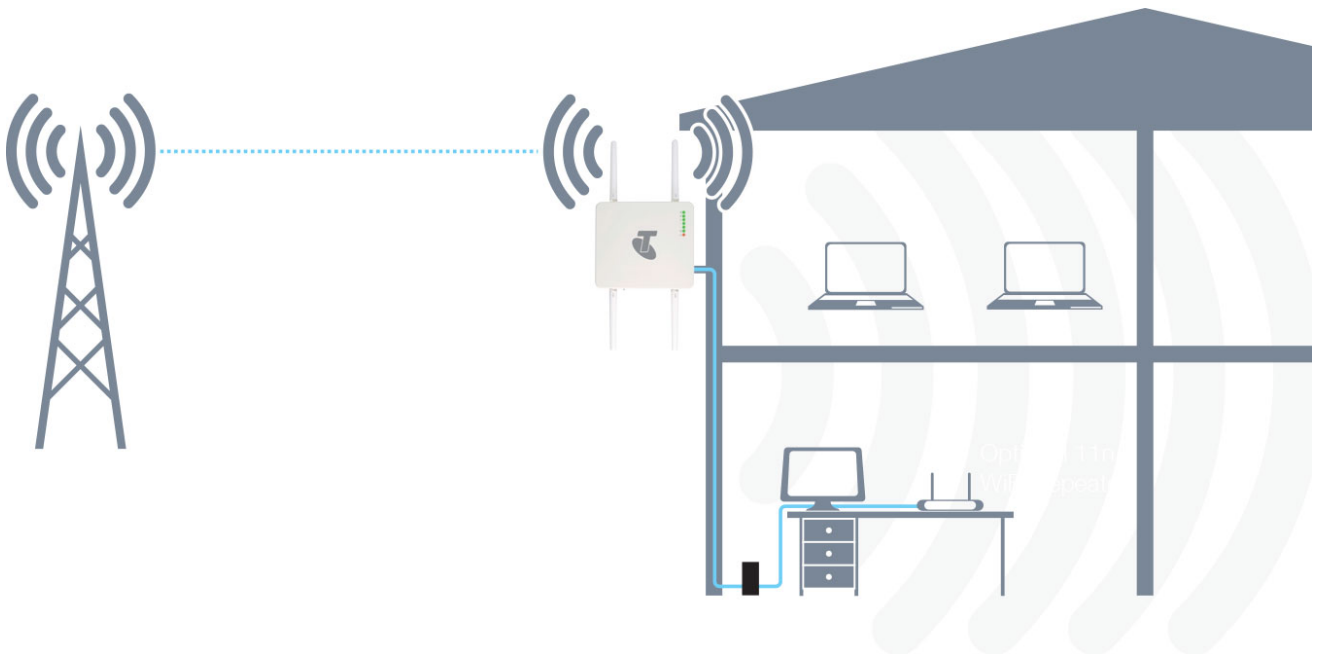


Figure 7 - Typical Telstra Outdoor Gateway Deployment - House

Power is delivered to the outdoor gateway via Power over Ethernet technology (as shown above) making installation quick and easy as there is no power source required at the outdoor mount point, and both power and data can be provided via a single cable from inside the property. With an IP67 rated enclosure, the device also withstands diverse temperature and weather environments. Utilising an 802.11n WiFi repeater further increases the WiFi range of the gateway meaning a wireless connection is possible in all corners of your house or property.

The outdoor gateway is able to be mounted either to a pole or secured directly to a wall, allowing flexibility in the choice of an installation location.

Installation and Configuration of the Outdoor Gateway

Hardware Installation

Please refer to the Telstra Outdoor Gateway Quick Start Guide for instructions on mounting and placing the gateway.

Powering the Gateway via a Power over Ethernet (PoE) Cable

Please refer to the Quick Start Guide for step-by-step instructions on connecting the devices. The diagram below summarises the assembly when connecting via Power over Ethernet cable.

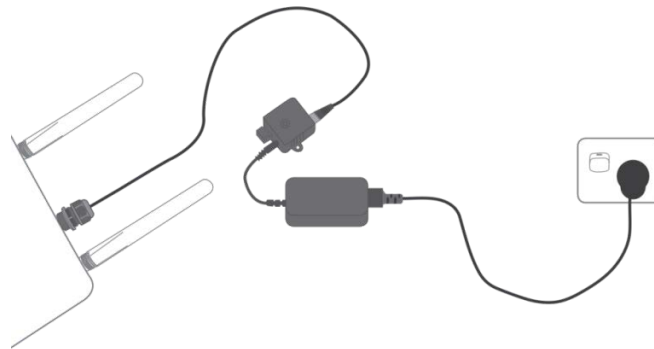


Figure 8 – Example of how to connect the outdoor gateway when connecting via Power over Ethernet (PoE) cable

 Please note: The DC Injector supplies 48V. Do not use this power supply for anything except for powering the outdoor gateway.

Powering the Gateway via DC Power Supply (Optional)

Your router is provided with a waterproof DC jack allowing it to be powered by a 9~28V DC power supply.

1. On the bottom interface panel of the router, locate the DC power port and unscrew the protective cap to expose the connection pins.
2. Connect the DC power jack as shown below to the DC power port of the router and turn the metal securing ring clockwise to secure the DC jack in position.
3. At the other end of the cable, wire the red (positive +) and black (grounding) wires to your 9~28V DC power supply source.

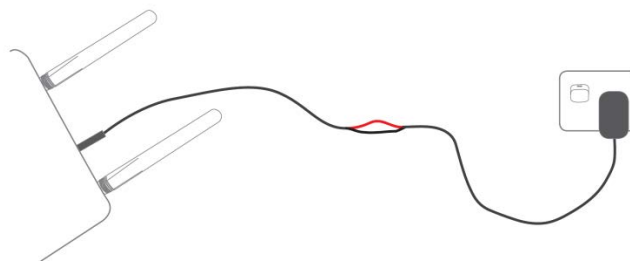


Figure 9 - Example of how to connect the outdoor gateway when connecting via optional DC power supply

Connecting wirelessly

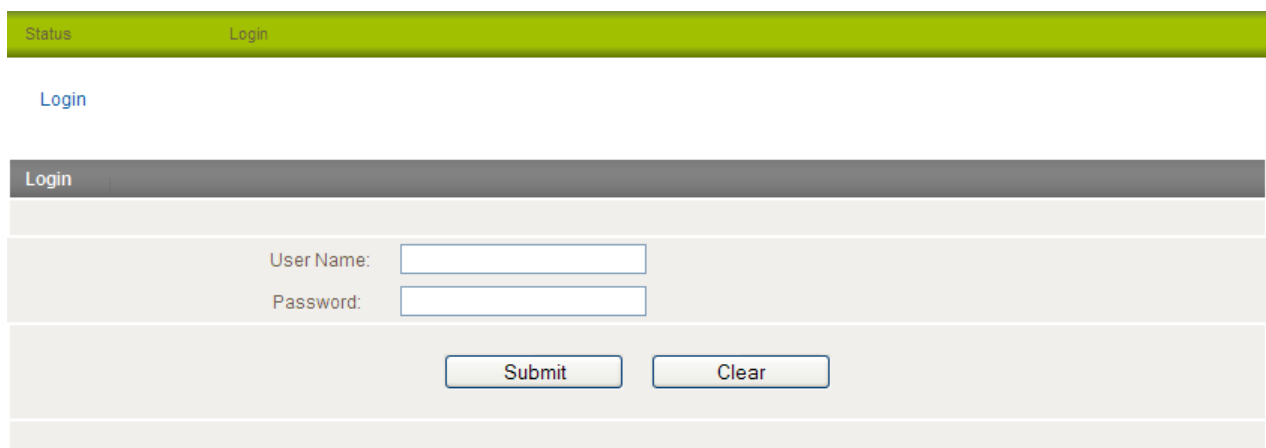
1. Ensure WiFi is enabled on your device (e.g. computer/laptop/smartphone).
2. Scan for wireless networks in your area and connect to the network name that matches the Wireless network name configured on the gateway (see the Wireless Security Card for default configuration).
3. When prompted for your wireless security settings, enter the Wireless security key configured on the gateway.
4. Wait approximately 30 seconds for the connection to establish.

Configuring the Telstra Outdoor Gateway

Logging in via the web-based user interface

To log in to the management console, view the status and make changes to your outdoor gateway, please follow the steps below:

1. Open a web browser (e.g. Internet Explorer/Firefox/Safari) and navigate to <http://192.168.1.1>
2. Enter the username and password configured during the first time setup and click the Submit button. The default username and password is admin if the login details haven't been customized. Click the Submit button to continue.



The screenshot shows a web-based user interface for logging in. At the top, there is a green navigation bar with two tabs: 'Status' and 'Login'. Below this bar, the word 'Login' is displayed in blue text. A dark grey horizontal bar contains the word 'Login' in white text. The main content area has a light grey background and contains two input fields: 'User Name:' and 'Password:'. Below the input fields are two buttons: 'Submit' and 'Clear'.

Figure 10 - Login prompt for the Web based User Interface

After logging in, the Status page is displayed.

Status

The status page provides system related information and is displayed when you login to the gateway management console. By default, the status page will show System Information, Ethernet Port Status, WWAN Status, IPsec Status and the 3G service connection details.

Figure 11 - The Status Page

ITEM	DEFINITION
System Uptime	The current uptime of the gateway.
Router Version	The firmware version running on the gateway.
Phone Module	The type of phone module, the firmware version of the module and the current module temperature.
MAC Address	The MAC Address of the gateway which serves as a unique identifier of network devices.
Ethernet Port Status	The current speed and status of the Ethernet port.
WWAN	The current connection profile, Interface, status, APN, and local address of the WWAN connection.
Connection Up Time	The duration of the current internet connection session.
Provider	The current 3G service provider detected.
Coverage	The type of 3G connection available for use.
IMEI	The International Mobile Equipment Identity of the gateway.
Frequency	The frequency band currently in use.
Signal Strength	The strength of the 3G signal detected
SIM Status	The status of the SIM currently inserted into the gateway.

Table 11 - Status page items

To view the LAN, PPPoE, PPTP or IPsec status individually, click on the links below the green menu bar. To view them all, click on the All Status link.

LAN	
IP	192.168.1.1 / 255.255.255.0
MAC Address	00:60:64:84:DF:D7

Figure 12 - Status Page - LAN Details

ITEM	DEFINITION
IP	The current LAN IP Address and Subnet Mask.
MAC Address	The current MAC Address of the LAN port.

Table 12 - Status Page - LAN Details

PPPoE	
PPPoE Status	DISABLED
PPPoE IP Address	N/A

Figure 13 - Status Page - PPPoE Details

ITEM	DEFINITION
PPPoE Status	The current status of the PPPoE connection.
PPPoE IP Address	The current PPPoE IP Address in use.

Table 13 - Status Page - PPPoE Details

PPTP	
PPTP Status	DISABLED
PPTP IP Address	
PPTP P-t-P	

Figure 14 - Status Page - PPTP Details

ITEM	DEFINITION
PPTP Status	The current status of the PPTP connection.
PPTP IP Address	The current PPTP connection IP Address.
PPTP P-t-P	The current PPTP Remote Gateway Address.

Table 14 - Status Page - PPTP Details

IPSec						
No.	Profile Name	Interface	Local LAN	Remote Gateway	Remote LAN	Status

Figure 15 - Status Page - IPSec Details

ITEM	DEFINITION
No.	The IPsec tunnel number.
Profile Name	The name assigned to the IPsec profile.
Interface	The current interface used by the IPsec tunnel.
Local LAN	The local IP address making up one end of the IPsec tunnel.
Remote Gateway	The WAN gateway of the other end of the IPsec tunnel.
Remote LAN	The WAN IP Address that the IPsec tunnel is connecting to.
Status	The current condition of the IPsec tunnel.

Table 15 - Status Page - IPSec Details

Advanced Status

To view further information regarding the phone module onboard the gateway and the current connection press the “Advanced Status” button.

Status	▶ Internet Settings	▶ Wireless Settings	▶ Services	▶ System
--------	---------------------	---------------------	------------	----------

[Status > Advanced Status](#)

Module Information	
Phone Module	Model: MC8801 Hardware: 1.0 Firmware: N2_0_8_4AP R1299 CARMD-EN-10526 2011/04/29 16:22:49
Module Boot Version	N2_0_8_4BT R1299 CARMD-EN-10526 2011/04/29 16:20:54
Module PRIID	Revision: 1.1 PRI Part Number: 9900075
System Up time	00:16:02

Connection Status	
Provider	Telstra
Country Code	505
Network Code	1
Coverage	UMTS
Connection Status	Up
IMEI	351829040043025
Frequency	WCDMA 850
Signal Strength	-70 dBm
Signal Quality (Ec/Io)	Carrier 0: -8.0 dB Carrier 1: n/a
Received Signal Code Power (RSCP)	Carrier 0: -74 dBm Carrier 1: n/a
RX level	Carrier 0: -64 dBm Carrier 1: -106 dBm
HSUPA Category	6
HSDPA Category	24
SIM ICCID	89610177166202000030
Primary Scrambling Code (PSC)	88
Location Area Code (LAC)	337
Routing Area Code (RAC)	0
IMSI	50501505013470372313
Cell ID	19795
Channel Number	4412

Figure 16: Advanced Status Page

ITEM	DEFINITION
Phone Module	The phone module name, hardware and firmware version
Module Boot version	The installed bootloader version of the phone module.
Module PRID	The Protocol ID of the phone module.
System Uptime	The time in minutes and seconds that the gateway has been up.
Provider	The current connection's 3G provider.
Country Code	Each country has a unique code that helps to identify the 3G network.
Network code	Each 3G provider has a unique network code for network identification purposes.
Service Type	The type of 3G service the current connection is using. Many networks use both a 3G and 2G connection simultaneously.
Coverage	The coverage type of 3G service the current connection is using.
Connection Status	The current status of the gateway's connection.
IMEI	The International Mobile Equipment Identity number unique to each cellular network device.
Frequency	The frequency of the current connection.
Signal Strength (dBm)	The signal strength of the 3G connection measured in decibels.
Signal Quality (Echo/Location)	A measurement of the portion of the received signal that is usable. This is basically the signal strength minus the signal noise level.
Received Signal Code Power (RSCP)	The power level of the signal on the current connection's particular channel.
SIM ICCID	The Integrated Circuit Card Identifier of the SIM card used. A unique number up to 19 digits in length.
Primary Scrambling Code (PSC)	The Primary Scrambling Code for the current signal.
Location Area Code (LAC)	The ID of the cell tower grouping the current signal is broadcasting from.
Routing Area Code (RAC)	The Routing Area Code is a subset of the Location Code and helps to identify the group of or individual cell towers the current connection is broadcasting from.
IMSI	The International Mobile Subscriber Identity is a unique identification for the current 3G connection.
Cell ID	A unique code that identifies the base station from within the Location Area of the current 3g signal.
Channel Number	The channel number of the current 3G connection.

Table 16: Advanced Status Settings

Internet Settings

This section describes how to set up the gateway to initiate a mobile broadband connection. There are 2 different ways to set up a mobile broadband connection:

- Initiating the Mobile Broadband Connection directly from the gateway (most common).
- Initiating the PPP Connection from a different PPP client (i.e. laptop or router) with the gateway running in transparent PPPoE mode.

Mobile Broadband

Connection

Click on the “Internet Settings” menu followed by “Mobile Broadband” and then the “Connection” menu item on the right.

Status▶ Internet Settings▶ Wireless Settings▶ Services▶ System

[Internet Settings > Mobile Broadband > Connection](#)

Mobile Broadband Profile Settings

Profile Name	<input type="text" value="Profile1"/> <input type="checkbox"/> Automatically configure my mobile broadband
APN Name	<input type="text"/>
Mobile Broadband Connection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	<input type="text"/>
Password	<input type="text"/>
Authentication Type	<input checked="" type="radio"/> CHAP <input type="radio"/> PAP
Reconnect Delay	<input type="text" value="30"/> (30-65535) secs
Reconnect Retries	<input type="text" value="0"/> (1-65535, 0=Unlimited)
Metric	<input type="text" value="20"/> (1-65535)
MTU	<input type="text" value="1400"/> (1400-1430)
NAT Masquerading	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Profile Name	Enabled	APN	User
Profile1	Yes		
Profile2	No		
Profile3	No		
Profile4	No		
Profile5	No		
Profile6	No		

Figure 17 - Connection Settings

To connect using a Connection profile

The router supports multiple APN profiles; these profiles allow you to configure the settings that the router will use to connect to the 3G network. By default, the “Automatically configure my mobile broadband” option is selected. This automatically detects the most appropriate APN from the inserted SIM by querying a database on the router.

You can also manually enter the connection details by performing the following steps:

1. Remove the check from the “Automatically configure my mobile broadband” box
2. Select the profile that you wish to configure from the “Profile Name” drop down list.
3. Enter the APN Name (Access Point Name) and if required, the username and password.
4. Select Enable for the “Mobile Broadband Connection” option. If there is already another profile enabled you will need to select that profile first and disable it since only one profile can be used at a time.
5. Select the Authentication Type.
6. Enter the Reconnect Delay (if needed - the default should be suitable in most cases).
7. Enter the number of Reconnection attempts the router should make.
8. Enter the network metric for the connection.
9. Select to enable or disable NAT Masquerading for the connection.
10. Click Save.

To confirm successful connection

Click on the Status menu item at the top of the page to return to the Status page.

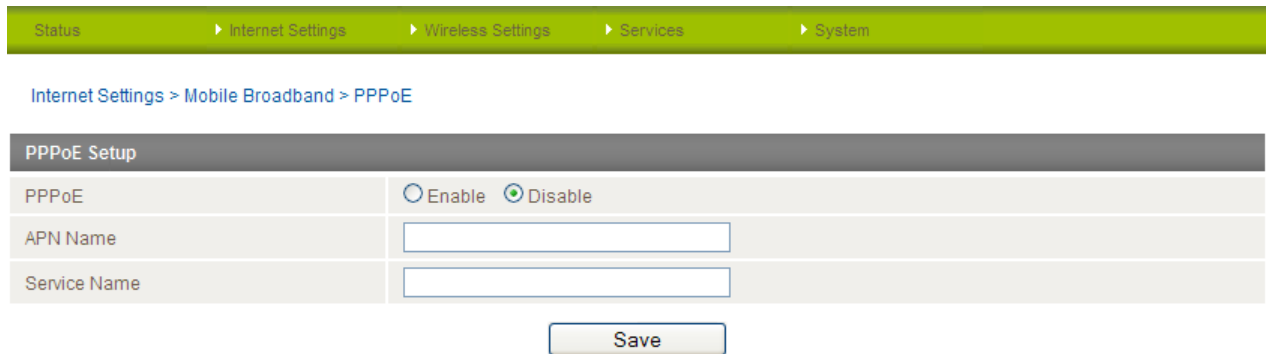
If the Mobile Broadband connection has been established successfully, the WWAN status will be “Up”. The IP Address field shows the current IP address that the network has allocated for the router. The mobile broadband internet connection is now ready to use.

Restoring the Automatic Configuration option after manually configuring an APN profile

When you have manually configured an APN and want to have the router automatically configure your broadband connection again, you must first set “Mobile Broadband Connection” to Disable for that profile and then remove the APN Name from the “APN Name” field and click “Save”. This is because the router saves the manually configured APN profile in flash memory and will always try to connect to that APN first regardless of whether “Automatically configure my mobile broadband” is enabled.

PPPoE

The PPPoE page is used to configure a transparent PPPoE connection. This can be used to provide a bridged connection. To enable PPPoE mode, firstly ensure that “Auto Connect” is disabled in all the profiles on the “Connection” configuration page by clicking on the “Internet Settings” menu followed by “Mobile Broadband” and then the “Connection” menu item on the right. Then select each connection profile, disable the Auto Connection option and save the updated settings.



The screenshot shows a web interface for configuring PPPoE. At the top, there is a navigation bar with links: Status, Internet Settings, Wireless Settings, Services, and System. Below this, the breadcrumb trail reads "Internet Settings > Mobile Broadband > PPPoE". The main content area is titled "PPPoE Setup" and contains a form with the following fields:

PPPoE	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
APN Name	<input type="text"/>
Service Name	<input type="text"/>

Below the form is a "Save" button.

Figure 18 - PPPoE Settings

1. Select “Enable” to enable PPPoE.
2. Specify the APN supplied by your 3G provider.

(Optional)

3. Specify a “Service Name”.

This is particularly useful if you have more than one PPPoE router or modem on a single Ethernet network.

Click “Save” to save your settings and enable PPPoE.

Band / Provider

The band settings page enables you to select which frequency band you will use for your connection and enables you to scan for available network operators in your area.

Status > Internet Settings > Wireless Settings > Services > System

Internet Settings > Mobile Broadband > Band settings

Band Settings

This page allows you to set up the frequency band and scan for all the available network operators. You can choose an operator manually from the Operator Name List after scanning.

Current Band: All bands Change Band: All bands

Apply

Figure 19 - Band / Provider Selection

You may want to do this if you're using the gateway in a country with multiple frequency networks that may not all support HSPA. You can select the gateway to only connect on the network frequencies that suit your requirements. Make your selection from the "Change Band:" drop down list.

The following band settings options are available:

- WCDMA ALL
- North America
- Europe
- GSM ALL
- North America 2G
- Europe 2G
- North America 3G
- Europe 3G
- All Bands

The default setting of "All bands" should be appropriate for the majority of users.

You can also scan for available 3G service providers in your area by selecting "Manual" for the "Current Operator Selection Mode" and then clicking the scan button.

Operator Settings

Current Operator Selection Mode: Automatic Select Operator Mode Automatic Manual

Operator Name List:	MCC	MNC	Operator Status	Network Type
---------------------	-----	-----	-----------------	--------------

Scan Apply

Figure 20 - Manual Operator Selection

A list of the detected 3G service carriers in your area will be displayed. Select the most appropriate 3G service from the list shown and click "Apply".

The default setting of "Automatic" should be appropriate for the majority of users and locations.

SIM Security

If the SIM card is locked you will need to unlock it with a PIN provided with your SIM card.

You can find out if the SIM is locked by viewing the SIM Status on the Status page:



Connection Status	
Provider	N/A
Service Type	Not Available
Coverage	N/A
IMEI	354155040002309
Frequency	N/A
Signal Strength (dBm)	dBm (not available)
SIM Status	SIM PIN

Figure 21 - SIM Security - Status Page Warning

If the SIM Status is “SIM PIN” as above then do the following:

- Click on the “Internet Settings” menu at the top of the page and then the “SIM Security” item from the WWAN (3G) menu item on the right.



Internet Settings > WWAN (3G) > SIM Security

PIN Settings	
SIM Status	SIM PIN
Number of Retries Remaining	
PIN	<input type="text"/>
Confirm PIN	<input type="text"/>
Remember PIN:	Disabled <input type="radio"/> Enable <input type="radio"/> Disable
PIN Protection:	Enabled <input type="radio"/> Disable PIN <input type="radio"/>

Save Help

Figure 22 - SIM Security - SIM PIN Needed

- Enter the PIN code in the “PIN” field and then enter it again in the “Confirm PIN” field to confirm the PIN code.

 Please note: You can also select to “Remember PIN” so that entering the PIN code each time the SIM is inserted is not required. Alternatively you can also disable SIM PIN protection by selecting to “Disable PIN” from the “PIN Protection” drop down menu.

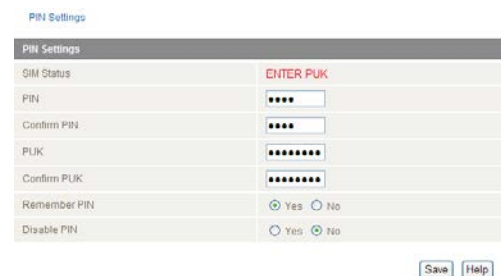
- Click Save.

Enter PUK

After three incorrect attempts at entering the PIN code, you are requested to enter a PUK code.

 Please note: You will need to contact your 3G provider to obtain this number.

Your carrier will issue you a PUK code to enable you to unlock the SIM and enter a new PIN code. Enter the new PIN and PUK codes and click Save.



PIN Settings

PIN Settings	
SIM Status	ENTER PUK
PIN	<input type="text"/>
Confirm PIN	<input type="text"/>
PUK	<input type="text"/>
Confirm PUK	<input type="text"/>
Remember PIN	<input checked="" type="radio"/> Yes <input type="radio"/> No
Disable PIN	<input type="radio"/> Yes <input checked="" type="radio"/> No

Save Help

Figure 23 - SIM Security - SIM PUK Needed

Remember PIN

This feature allows the gateway to automatically send the PIN to the SIM each time the SIM asks for it (usually at power up).

This enables the SIM to be PIN Locked (to prevent unauthorised re-use of the SIM elsewhere), while still allowing the gateway to connect to the cellular service.

When this feature is enabled the PIN entered by the user when they set the “Remember PIN” feature is encrypted and stored locally in the gateway. The next time the SIM asks the gateway for the PIN the gateway decrypts the PIN and automatically sends it to the SIM without user intervention.

When this feature is disabled and the SIM is PIN locked, the PIN must be manually entered via the gateway’s configuration interface. This is clearly not desirable where the gateway is unattended.

LAN

IP Setup

The IP Setup page is used to configure the LAN Settings of the gateway and to enable or disable DNS Masquerade.

Status ▶ Internet Settings ▶ Wireless Settings ▶ Services ▶ System

Internet Settings > LAN > IP Setup

LAN Configuration

IP Address	<input type="text" value="192"/>	<input type="text" value="168"/>	<input type="text" value="1"/>	<input type="text" value="1"/>
Subnet Mask	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="0"/>

DNS Masquerade

DNS Masquerade	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
----------------	---

Figure 24 - IP Setup Settings

The default IP of the Ethernet port is 192.168.1.1 with subnet mask 255.255.255.0. To change this, enter the new IP Address and/or Subnet mask and click “Save”.

 Please note: If the IP address has changed you will have to re-enter the new IP address configured in your browser to access the configuration pages.

DNS Masquerading

DNS masquerading allows the gateway to forward DNS requests to dynamically assigned DNS servers. Clients on the gateway’s LAN can then use the gateway as a DNS server without needing to know of the dynamically assigned DNS servers assigned by the cellular network.

There should be no need to disable this feature in most cases, however, if you need to do so simply select “Disable” and click the “Save” button.

DHCP

The DHCP page is used to adjust the DHCP settings used by the gateway. The DHCP settings are then passed onto any device connecting via DHCP. You can manually set the DHCP Start and End range, the DHCP Lease time, the default Domain name suffix, Primary and Secondary DNS Server, the Primary and Secondary WINS Server, as well as the NTP, TFTP and Option 150/Option 160 (VoIP options) settings.

The screenshot shows the DHCP Configuration page with the following sections:

- DHCP Configuration:**
 - DHCP: Enable Disable
 - DHCP Start Range: 192 . 168 . 1 . 100
 - DHCP End Range: 192 . 168 . 1 . 199
 - DHCP Lease Time: 86400 (seconds)
 - Default Domain Name Suffix: []
 - DNS Server 1 IP Address: 0 . 0 . 0 . 0
 - DNS Server 2 IP Address: 0 . 0 . 0 . 0
 - WINS Server 1 IP Address: 0 . 0 . 0 . 0
 - WINS Server 2 IP Address: 0 . 0 . 0 . 0
 - NTP Server (Option 42): 0 . 0 . 0 . 0
 - TFTP Server (Option 66): []
 - Option 150: []
 - Option 160: []
- DHCP Relay Configuration:**
 - DHCP Relay: Enable Disable
 - DHCP Server Address: 0 . 0 . 0 . 0
- Address Reservation List:**

Computer Name	MAC Address	IP Address	
[]	[]	0 . 0 . 0 . 0	<input type="button" value="Add"/>
- DHCP Client List:**

Computer Name	MAC Address	IP Address	Expire Time
[]	[]	0 . 0 . 0 . 0	[]

At the bottom of the page is a button.

Figure 25 - DHCP Settings

After entering the applicable details, click the “Save” button.

You can also assign a particular IP address to a specific device every time that device makes a DHCP request as follows:

The screenshot shows the Address Reservation List table with one entry:

Computer Name	MAC Address	IP Address	
[]	[]	0 . 0 . 0 . 0	<input checked="" type="checkbox"/> Enable <input type="button" value="Remove"/>

Figure 26 - DHCP Settings - Fixed Mapping

1. Click the “Add” button.
2. Enter a name for the computer or device into the “Computer Name” textbox.
3. Enter the computer’s or device’s MAC address into the “MAC Address” textbox.
4. Enter the IP address you wish to assign to the device in the IP Address text boxes.
5. Select the Enable checkbox to enable the rule.
6. Click the “Save” button to save the new settings.

Routing

Static

The Static Route page is used to add or delete static routes. Static routes can be used to facilitate communication between devices on different networks.

Internet Settings > Routing > Static

Enabled Profile List

Profile Name	Interface Name	IP Address	Default Route	NAT Masquerading
Enabled Profile List is empty				

Static Routes

Item No. (1-65535) Only required if you want to edit the existing mapping!

Route Name

Destination IP . . .

Subnet Mask . . .

Gateway IP . . .

Network Interface

Metric (0-65535)

Item No.	Route Name	Destination IP	Subnet Mask	Gateway IP	Network Interface	Metric	
0	Static Route 1	192.168.1.3	255.255.255.0	192.168.1.1	auto	1	Delete Entry

Active Routing Table

Item No.	Destination IP	Subnet Mask	Gateway IP	Network Interface	Metric	Flags	Ref	Use
0	192.168.1.0	255.255.255.0	0.0.0.0	br0	0	U	0	0

Figure 27 - Static Route Settings

Some routes are added by default by the gateway on initialisation such as the Ethernet subnet route for routing to a device on the Ethernet subnet. A PPP route is also added upon obtaining a WAN PPP connection.

Adding Static Routes

- Enter the required values in the fields (as shown above) for the route being added.
- Click the “Add” button.

 Please note: You must increment the “Item No” by 1 for each route rule added in the “Item No” field otherwise the previous route will be overwritten.

The Static Route will be displayed at the bottom of the Static Routes section.

Deleting Static Routes

Click the “Delete Entry” text (in blue).

RIP

RIP (Routing Information Protocol) is used for advertising routes to other routers. Thus all the routes in the router's routing table will be advertised to other nearby routers. For example, the route for the router's Ethernet subnet could be advertised to a Router on the PPP interface side so that a Router on this network will know how to route to a device on the router's Ethernet subnet. You will have to add the routes as necessary in the Static Routes section – see Adding Static Routes.



Please note: Some routers will ignore RIP.

RIP Routing	
RIP Enable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Version	2
<input type="button" value="Save"/>	

Figure 28 - RIP Settings

1. Click the Enable option on the RIP Page.
2. Select the RIP version you wish to use.
3. Click the "Save RIP" button to save the settings.

VRRP

Virtual Router Redundancy Protocol (VRRP) is a non-proprietary redundancy protocol designed to increase the availability of the default gateway servicing hosts on the same subnet. This increased reliability is achieved by advertising a “virtual router” (an abstract representation of master and backup routers acting as a group) as a default gateway to the host(s) instead of one physical router. Two or more physical routers are then configured to stand for the virtual router, with only one doing the actual routing at any given time. If the current physical router that is routing the data on behalf of the virtual router fails, an arrangement is made for another physical router to automatically replace it. The physical router that is currently forwarding data on behalf of the virtual router is called the master router.


Master routers have a priority of 255 and backup router(s) can have priority between 1 and 254.

A virtual router must use 00-00-5E-00-01-XX as its (MAC) address. The last byte of the address (XX) is the Virtual Router Identifier (VRID), which is different for each virtual router in the network. This address is used by only one physical router at a time, and is the only way that other physical routers can identify the master router within a virtual router.

VRRP Configuration	
VRRP Enable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Virtual Device ID	<input type="text" value="1"/> (1-255)
Router Priority	<input type="text" value="1"/> (1-255)
Virtual IP Address	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>

Figure 29 - VRRP Settings

1. Click Enable to activate the VRRP service.
2. Enter an ID – this is the VRRP ID which is different for each virtual router on the network
3. Enter a priority – a higher value is a higher priority
4. Enter the VRRP IP address – this is the virtual IP address that both virtual routers share
5. Click Save VRRP

 Please note: Configuring VRRP changes the MAC address of the Ethernet port and therefore if you want to resume with the web configuration you must use the new IP address (VRRP IP) or on a command prompt type: `arp -d <ip address>` (i.e. `arp -d 192.168.1.1`) to clear the arp cache.(old MAC address).

NAT

The NAT page is used to configure the Network Address Translation rules currently in use on the gateway. The gateway is in NAT mode by default.

Figure 30 - NAT Settings


This is only needed if you need to map inbound requests to a specific port on the WAN IP address to a device connected on the Ethernet interface, e.g. a web camera.

How to configure Port Forwarding

OPTION	DEFINITION
Mapping no	Number to identify the port mapping, numbered from 1 to as many as needed.
Protocol	Specify the protocol to use for the port mapping. Options include TCP, UDP or All protocols.
Source IP Address	This field specifies either a "Friendly" IP address that is allowed to access the router or a wildcard IP address of 0.0.0.0 that allows all IP addresses to access the gateway.
Incoming Port Range	This field specifies the external port(s) to listen to.
Destination IP Address	The Local Area Network Address of device to forward inbound requests to.
Destination Port Range	The Local Area Network Port(s) to forward connections to.

Table 17 - NAT Configuration Items

1. Enter the IP Mapping configuration information as appropriate.
2. Click the "Save" button to save any changes to the settings.

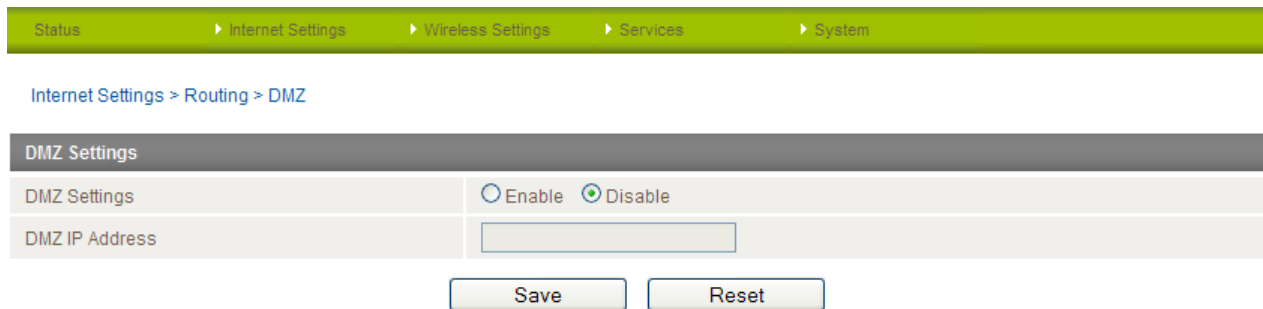
 Please note: If the "Incoming Port Range" specifies a single port (as above) then the destination port can be set to any port. If the "Incoming Port Range" specifies a range of port numbers then the "Destination Port Range" MUST be the same as the "Incoming Port Range".

To delete a port forwarding rule, click on the corresponding "Delete Entry" link from the list of IP Mappings.

DMZ

The Demilitarised Zone (DMZ) enables a device to utilise a direct connection to the WAN. This means any incoming connections are forwarded directly to this device.

The DMZ page is used to specify the IP Address of the device to this feature.



The screenshot shows a web interface for configuring DMZ settings. At the top, there is a navigation bar with the following items: Status, Internet Settings, Wireless Settings, Services, and System. Below this, the breadcrumb path is "Internet Settings > Routing > DMZ". The main content area is titled "DMZ Settings" and contains two rows of settings. The first row is "DMZ Settings" with two radio buttons: "Enable" (unselected) and "Disable" (selected). The second row is "DMZ IP Address" with an empty text input field. At the bottom of the form, there are two buttons: "Save" and "Reset".

Figure 31 - DMZ Settings

1. Click the "Enable" button.
2. Enter the IP Address of the device you wish to become the DMZ host.
3. Click the "Save" button.

VPN

A Virtual Private Network (VPN) is a tunnel providing a private link between two networks or devices over a public network. Data to be sent via a VPN tunnel needs to be encapsulated and as such is generally not visible to public networks.

The advantages of a VPN connection include:

- Data Protection
- Access Control
- Data Origin Authentication
- Data Integrity

How to configure a VPN connection

1. Move your mouse over the **Internet Settings** menu and then move your mouse over **VPN**. You can select from the following types of VPN connection:
 - IPSec
 - PPTP
 - OpenVPN
 - GRE

The following pages detail the configuration options available for the different VPN connection types.

IPsec

When you select IPsec, a list of configured IPsec VPNs is displayed. Click the “Add” button to configure an IPsec VPN connection.

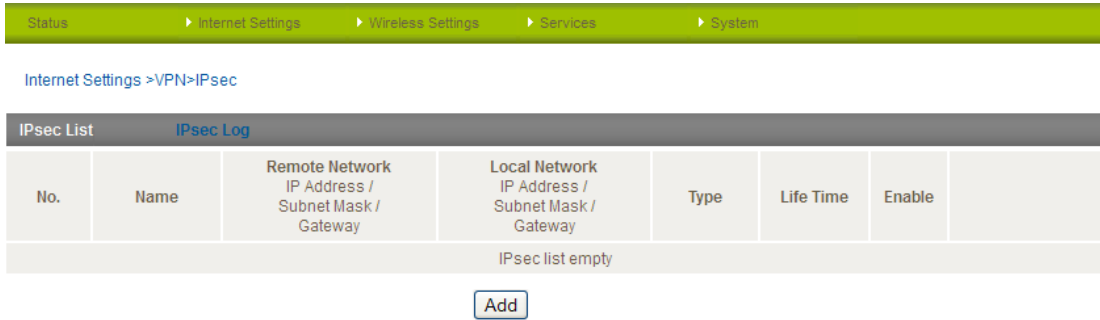


Figure 32 - IPsec VPN List

IPsec operates on Layer 3 of the OSI model and as such can protect higher layer protocols. IPsec is used for both Site to Site VPN and Remote Access VPN. The Telstra Outdoor Gateway supports IPsec end points and can be configured with Site to Site VPN tunnels with third party VPN routers.

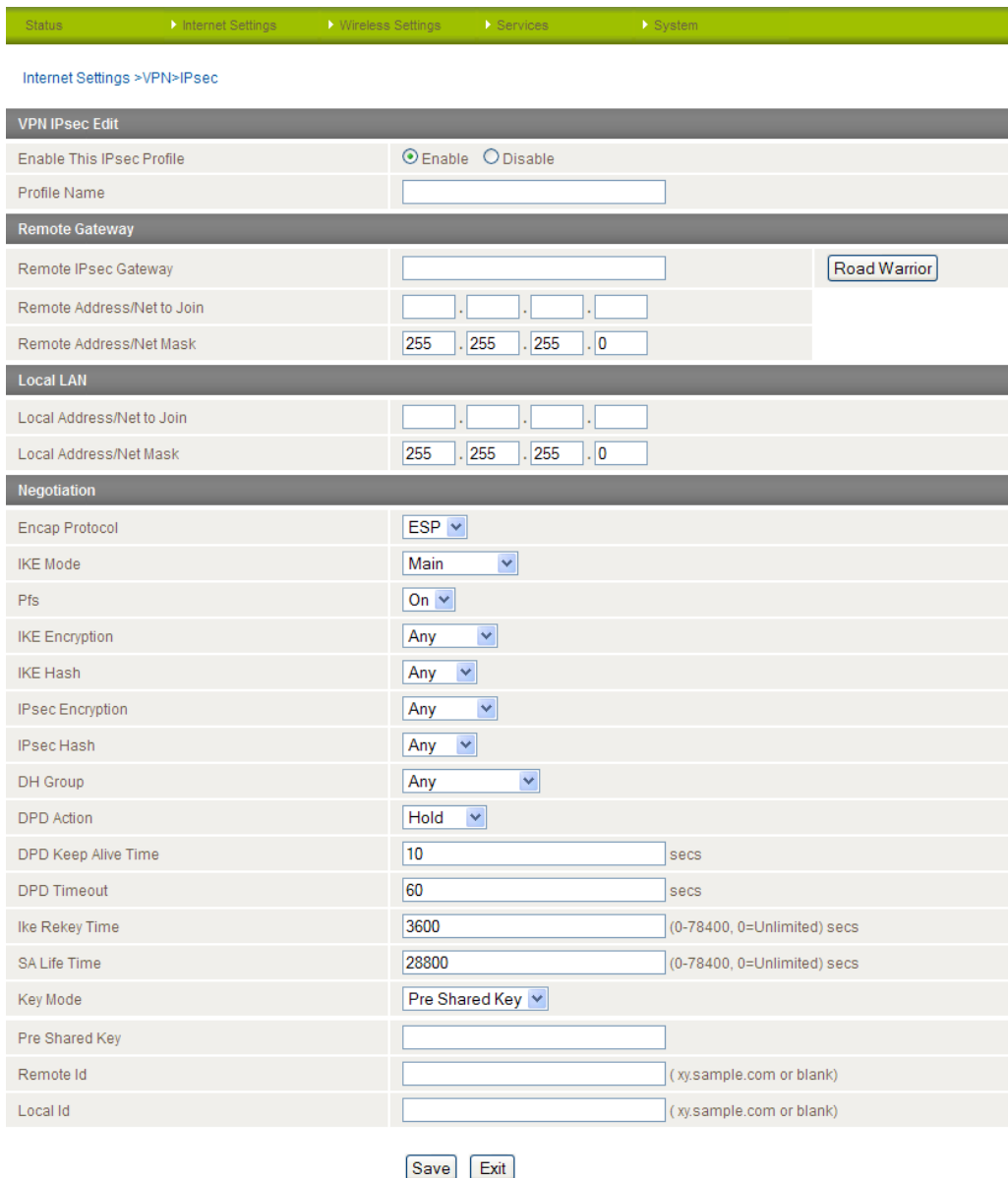


Figure 33 - VPN Connection Settings – IPsec

Please view the IPsec field descriptions on the following page.

VPN - IPsec Field Descriptions

ITEM	DEFINITION
Enable VPN	Enable or Disable the VPN connection.
Profile Name	A name used to identify the VPN connection.
Remote IPsec Gateway	The IP address that the IPsec server is running on.
Road Warrior	Click this to configure the VPN connection for Road Warrior (connection from a dynamic IP Address) use.
Remote Address/Net to Join	Enter the Remote IP address or Network for use on the VPN connection.
Remote Address/Net Mask	Enter the subnet mask in use on the remote network.
Local Address/Net to Join	Enter the Local IP address or Network for use on the VPN connection.
Local Address/Net Mask	Enter the subnet mask in use on the local network.
Encap Protocol	Select the encapsulation protocol to use with the VPN connection.
IKE Mode	Select the IKE mode to use with the VPN connection.
Pfs	Select whether or not to use PFS for the VPN connection.
IKE Encryption	Select the IKE encryption type to use with the VPN connection.
IKE Hash	Select the IKE Hash type to use for the VPN connection.
IPsec Encryption	Select the IPsec encryption type to use with the VPN connection.
IPsec Hash	Select the IPsec Hash type to use for the VPN connection.
DH Group	Select the appropriate DH Group for use with the VPN connection.
DPD Action	Select the appropriate DPD (Dead Peer Detection) Action to use on the VPN connection.
DPD Keep Alive Time	The time in seconds to keep alive a VPN tunnel where DPD has detected a dead peer.
DPD Timeout	The time in seconds before DPD will timeout.
IKE Rekey Time	Enter the appropriate IKE Rekey time for the VPN connection.
SA Life Time	Enter the appropriate SA Life time for the VPN connection.
Key Mode	<p>Select the type of key mode in use for the VPN connection. You can select from:</p> <ul style="list-style-type: none"> • Pre Shared Key • RSA Keys • Certificates <p>Each type of Key mode requires different configuration options. For more information, please refer to the VPN Document available from the NetComm Website.</p>

Table 18 - IPsec Configuration Items

OpenVPN

When you select OpenVPN, a list of configured OpenVPN VPNs is displayed. Click the “Add” button to configure an OpenVPN VPN connection.

The screenshot shows a web interface for configuring OpenVPN. At the top, there is a navigation bar with the following items: Status, Internet Settings, Wireless Settings, Services, and System. Below the navigation bar, the breadcrumb path is "Internet Settings > VPN > OpenVPN".

There are three main sections, each with a table header and a message indicating the list is empty:

- OpenVPN Server List**: A table with columns: Name, Network Address/Mask, Authentication Type, User Name, Enable. Below the table, it says "VPN list empty".
- OpenVPN Client List**: A table with columns: Name, Server Address, Authentication Type, User Name, Enable. Below the table, it says "VPN list empty".
- OpenVPN Peer-T-Peer List**: A table with columns: Name, Server Address, Local IP, Remote IP, Remote Network/Mask, Enable. Below the table, it says "VPN list empty".

Below the Peer-T-Peer List, there is a blue button labeled "Add".

Figure 34 - OpenVPN List

OpenVPN is an open source virtual private network (VPN) program for creating point-to-point or server-to-multi-client encrypted tunnels between host computers. It can traverse network address translation (NAT) and firewalls and allows authentication by certificate, pre-shared key or username and password. OpenVPN works well through proxy servers and can run over TCP and UDP transports. Support for OpenVPN is available on several operating systems, including Windows, Linux, Mac OS, Solaris, OpenBSD, FreeBSD, NetBSD and QNX.

Status > Internet Settings > Wireless Settings > Services > System

Internet Settings > VPN > OpenVPN

OpenVPN Edit

Enable OpenVPN	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Profile Name	<input type="text"/>
OpenVPN Type	Server
Server Port	1194 <input type="text"/> UDP
VPN Network Address	10.0.0.0
VPN Network Mask	255.255.255.0
Diffie-Hellman parameters	<input type="button" value="Generate DH..."/>
Server Certificates	Not Before : N/A Not After : N/A Country : <input type="text"/> State : <input type="text"/> City : <input type="text"/> Organization : <input type="text"/> Email : <input type="text"/> <input type="button" value="Generate CA certificate..."/>
Authentication Type	<input checked="" type="radio"/> Certificate <input type="radio"/> User Name / Password
Certificate Management	Certificate : New... Name : <input type="text"/> Country : <input type="text"/> State : <input type="text"/> City : <input type="text"/> Organization : <input type="text"/> Email : <input type="text"/> <input type="button" value="Generate"/> <input type="button" value="Download"/> <input type="button" value="Revoke"/> Network address: <input type="text"/> Network Mask: <input type="text"/> <input type="button" value="Set Network Information"/>

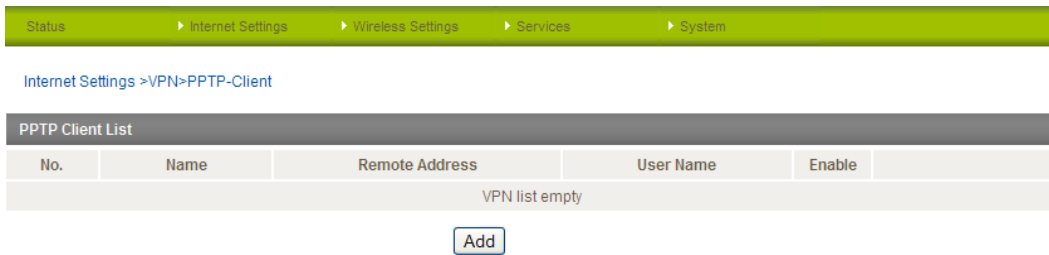
Figure 35 - VPN Connection Settings - OpenVPN

ITEM	DEFINITION
Enable VPN	Enable or Disable the VPN connection.
Profile Name	A name used to identify the VPN connection.
OpenVPN Type	Select the type of OpenVPN session to use.
Server Port	Enter the port the OpenVPN server is running on.
VPN Network Address	Enter the network address for use on the VPN connection.
VPN Network Mask	Enter the network mask for use on the VPN connection.
Diffie-Hellman parameters	Generate the server and client keys used by the VPN connection.
Server Certificates	Enter the applicable details to identify the OpenVPN server and create a CA certificate based on this information.
Authentication Type	Select the type of authentication in use for the VPN connection. You can select from: <ul style="list-style-type: none"> - Certificate - User Name / Password Each type of Key mode requires different configuration options. For more information, please refer to the VPN Document available from the NetComm Website.

Table 19 - OpenVPN Configuration Items

PPTP-Client

When you select PPTP-Client, a list of configured PPTP-Client VPNs is displayed. Click the “Add” button to configure a PPTP-Client VPN connection.



The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks using a TCP and GRE tunnel to encapsulate PPP packets. PPTP operates on Layer 2 of the OSI model and is included on Windows computers.

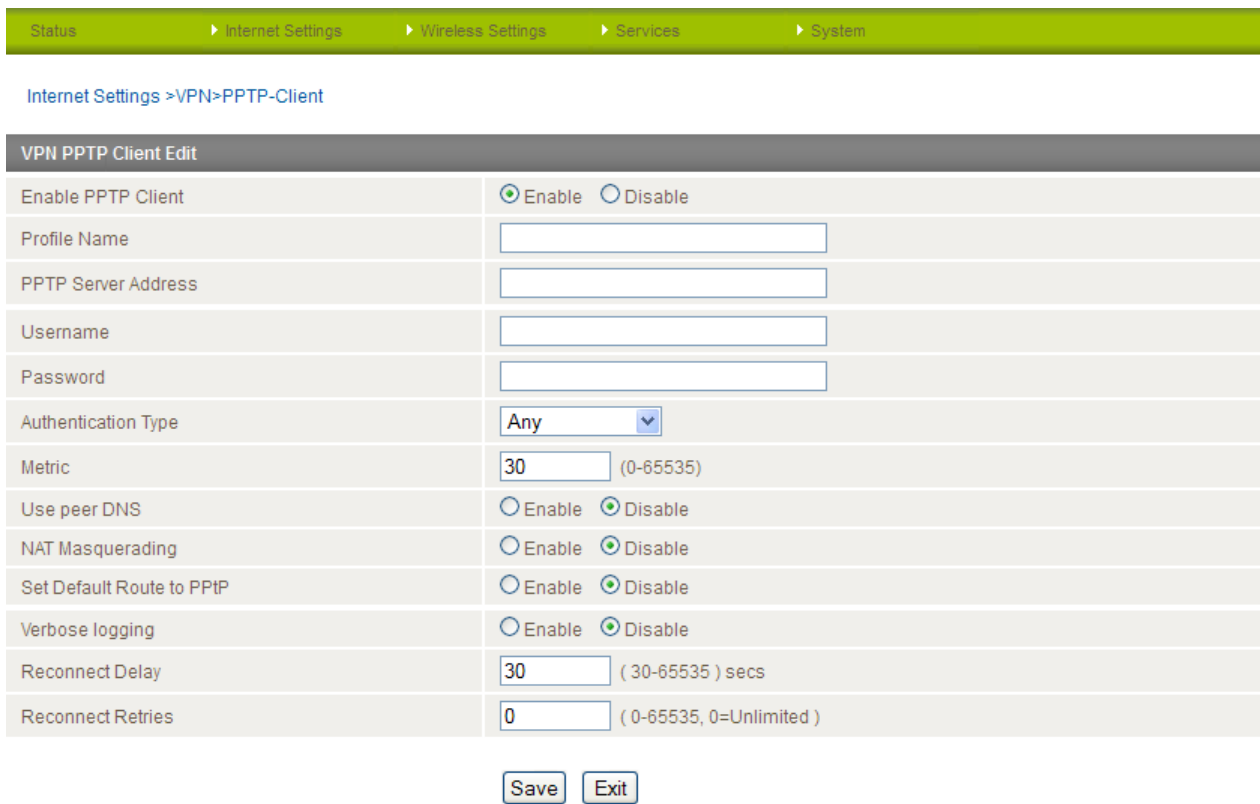


Figure 36 - VPN Connection Settings - PPTP

ITEM	DEFINITION
Enable VPN	Enable or Disable the VPN connection.
Profile Name	A name used to identify the VPN connection.
VPN Server Address	The IP Address on which the VPN server is running.
Username	The username required to login to the VPN service.
Password	The password required to login to the VPN service.
Authentication Type	The authentication type required for connecting to the VPN service.
Metric	The route metric to apply to the VPN connection.
Use peer DNS	Select whether to use the VPN server DNS settings or not.
NAT Masquerading	Select whether to use NAT Masquerading for the VPN connection.
Set Default Route to PPTP	Make the VPN connection the default route for traffic to use.
Verbose Logging	Enable extended logging information for the VPN connection.
Reconnect Delay	The delay before attempting to reconnect to the VPN service.
Reconnect Retries	The number of times to attempt to reconnect to the VPN service.

Table 20 - PPTP Configuration Items

GRE

When you select GRE, a list of configured GRE VPNs is displayed. Click the “Add” button to configure a GRE VPN connection.

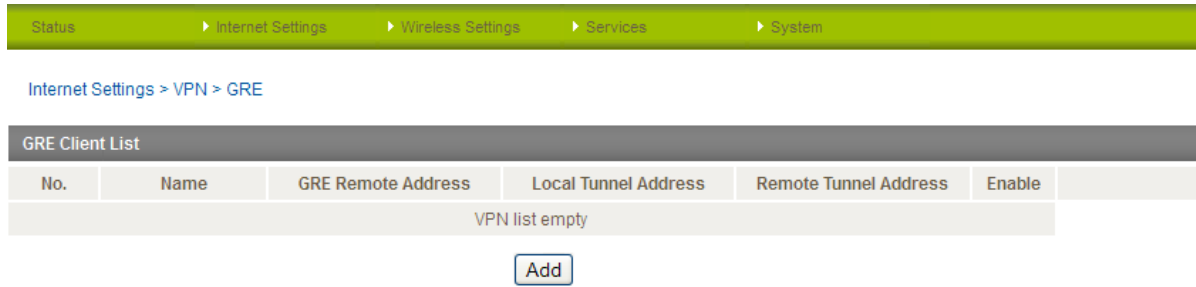


Figure 37 - GRE VPN List

Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco that works in conjunction with PPTP to create a virtual private network.

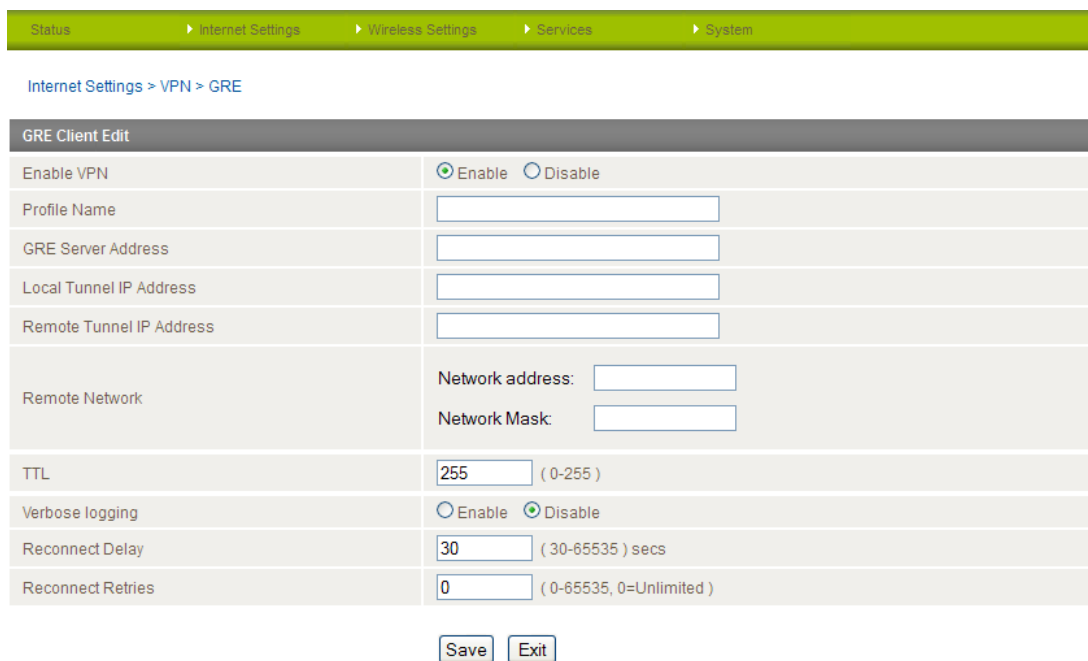


Figure 38 - GRE VPN Settings

ITEM	DEFINITION
Enable VPN	Enable or Disable the VPN connection.
Profile Name	A name used to identify the VPN connection.
GRE Server Address	The IP Address on which the GRE VPN server is running.
Local Tunnel IP Address	The Local IP address of the VPN tunnel.
Remote Tunnel IP Address	The Remote IP address of the other end of the VPN tunnel.
Remote Network	Enter the remote network address and subnet mask.
TTL	The Time To Live field, an 8-bit field used to remove an undeliverable data packet from a network to avoid unnecessary network traffic across the internet. The default value of 255 is the upper limit on the time that an IP datagram can exist. The value is reduced by at least one for each hop the data packet takes to the next router on the route to the datagram's destination. If the TTL field reaches zero before the datagram arrives at its destination the data packet is discarded and an error message is sent back to the sender.
Verbose Logging	Enable extended logging information for the VPN connection.
Reconnect Delay	The delay before attempting to reconnect to the VPN service.
Reconnect Retries	The number of times to attempt to reconnect to the VPN service.

Table 21 - GRE VPN Settings

USSD

The USSD page is used to send USSD (short SMS style) messages to the 3G service provider.

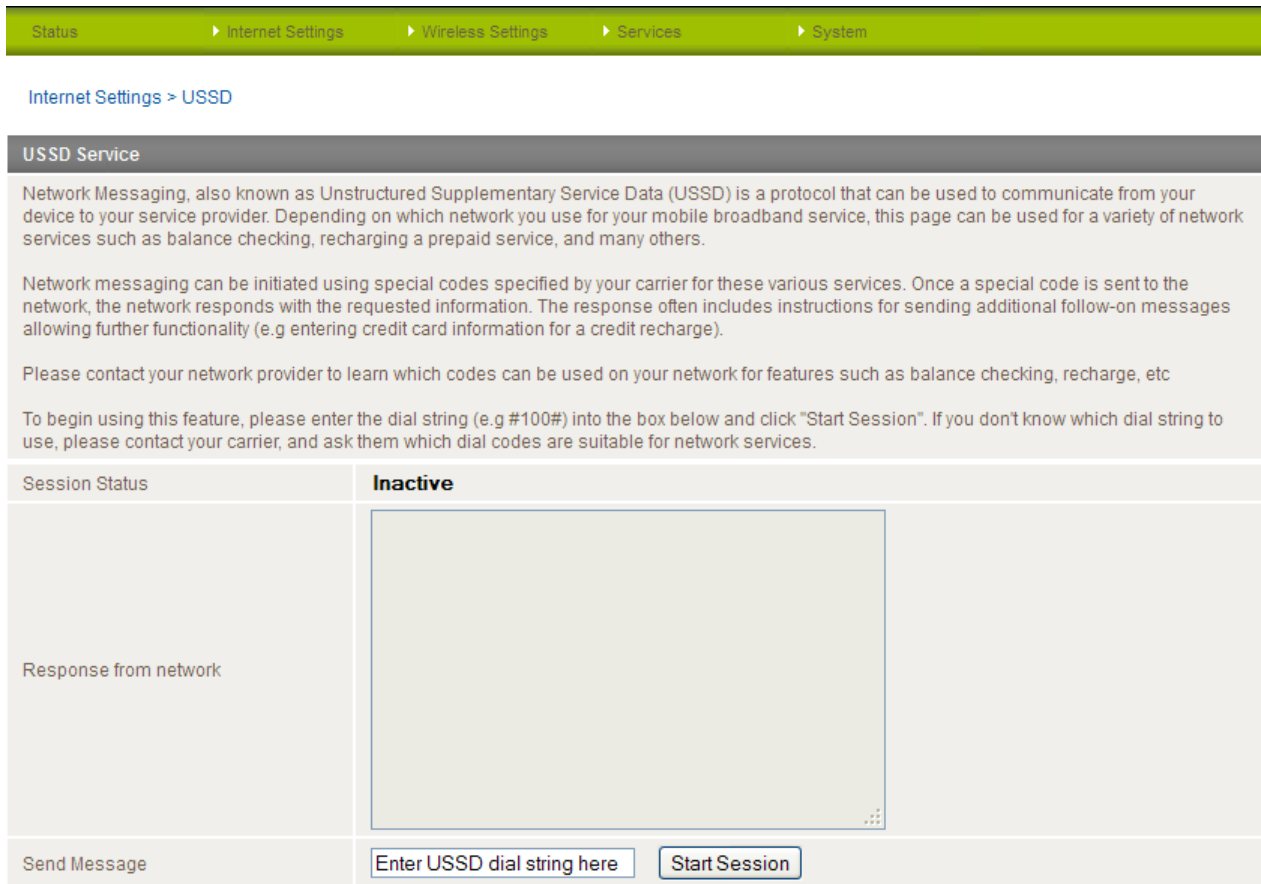


Figure 39 - USSD Messaging

USSD is a real-time messaging service usually utilised to perform mobile account related tasks such as:

- Checking available credit for a mobile service account.
- Obtaining more credit for a mobile service account.
- Verifying your mobile account information.

Enter the USSD message to be sent in the "Send Message" field at the bottom of the screen and then click "Start Session".

Any responses from your 3G Service Provider will be displayed in the "Response from Network" box in the middle of the page.

Please contact your 3G Service provider for a list of available USSD commands for your 3G service.

Wireless Settings

Basic

The basic configuration page is used to define the basic wireless settings for the gateway such as the SSID and Wireless Security in use.

Figure 40 - Wireless Configuration - Basic Settings

OPTION	DEFINITION
Radio On/Off	WiFi is turned on by default. Changing this option to OFF will turn OFF the wireless functionality on the outdoor gateway and you will not be able to connect wirelessly.
Country	Select the country where the gateway is operating.
Network Mode	Depending on the capability of your wireless device's wireless network card select the network mode to use. There are 5 available options. They are: <ul style="list-style-type: none"> • 11 b/g mixed mode • 11b only • 11g only • 11n only • 11 b/g/n mixed mode If you are not sure which protocol to use the 11 b/g/n mixed mode is recommended.
Frequency	The frequency or wireless channel that the gateway is broadcasting with. Recommended channels are 1, 6 or 11.
SSID	The SSID (Service Set Identifier) or network name in use for the wireless network.
Network Authentication	The wireless security settings for the gateway. Please see below for further details.
WPA Pre-Shared Key	The wireless password in use by the gateway.
WPA Group Rekey interval	This is the time in seconds before a new key is generated.
WPA Encryption	The type of WPA encryption used with the wireless security settings.
MAC Address	The MAC Address of the Wireless Access Point.
WDS Mode	Set Wireless Distribution System (WDS) to enable or disable.

Table 22 - Wireless Configuration - Basic Configuration Items

Click 'Apply' to save any changes to the settings.

Security Settings

You may choose from the following wireless security options:

- Open
- Shared
- WPA
- WPA-PSK
- WPA2
- WPA2- PSK
- WPA-PSK-WPA2-PSK
- WPA1-WPA2
- 802.1x

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.

Security Settings	
SSID:	<input type="text" value="NetComm XXXX"/>
Network Authentication:	<input type="text" value="WPA1-WPA2"/>
WPA Group Rekey interval:	<input type="text" value="600"/>
RADIUS Server IP Address:	<input type="text" value="0.0.0.0"/>
RADIUS Port:	<input type="text" value="1812"/>
RADIUS Key:	<input type="text"/>
WPA Encryption:	AES

Figure 41 - Advanced View – WiFi Security Settings - WPA1/WPA2

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 compared 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 can be any combination of letters and numbers.



Please note that the configuration for WPA2, WPA-PSK-WPA2-PSK, WPA-PSK and WPA2-PSK is identical.

Security Settings	
SSID:	<input type="text" value="NetComm XXXX"/>
Network Authentication:	<input type="text" value="WPA2-PSK"/>
WPA Pre-Shared Key:	<input type="text" value="••••••••"/> Click here to display
WPA Group Rekey interval:	<input type="text" value="600"/>
WPA Encryption:	AES

Figure 42 - Advanced View – WiFi Security Settings - WPA-PSK/WPA2-PSK



Please note: Your gateway uses WPA2-PSK by default. Check your Wireless Security Card or the device label on the bottom of the outdoor gateway 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.

Security Settings	
SSID:	<input type="text" value="NetComm XXXX"/>
Network Authentication:	<input type="text" value="802.1X"/>
RADIUS Server IP Address:	<input type="text" value="0.0.0.0"/>
RADIUS Port:	<input type="text" value="1812"/>
RADIUS Key:	<input type="text"/>
802.1x WEP	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

Figure 43 - Advanced View – WiFi Security Settings - 802.1x

Please 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 type 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.

Advanced

The Advanced page is used to modify the advanced wireless settings for the gateway. These settings should not be changed unless you are aware of what effect they will have.

Wireless Settings > Advanced

Advanced Wireless Configuration

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

BG Protection Mode	Auto
Client Idle Timeout	300 sec (range 60 - 600, default 300)
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	2 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 (range 1 - 100, default 100)
Short Preamble	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Apply Reset

Figure 44 - Wireless Settings - Advanced

OPTION	DEFINITION
BG Protection Mode	A protective measure designed to prevent collisions among 802.11b/g modes. Mode options include Auto, On, or Off.
Client Idle Timeout	The time in seconds that a wireless client session can be idle before the gateway cancels the session and defines the wireless client as not connected.
Beacon Interval:	Interval of time in which the wireless gateway broadcasts a beacon which is used to synchronize the wireless network.
Data Beacon Rate (DTIM)	Enter a value in milliseconds 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.
Fragmentation 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 gateway will not use the RTS/CTS mechanism to send this packet.
TX Power	This determines the output power of the antenna.
Short Preamble	Enable or disable short preambles in use on the wireless network. Using short preambles should improve throughput, however some wireless network adapters must use long preambles.

Table 23 - Wireless Settings - Advanced Configuration Items

Click the “Save” button to save any changes to the settings.

MAC Filter

The Wireless LAN MAC filter feature ensures the network accessibility for the wireless client devices can be controlled. When the MAC filter is enabled with an Allow policy only those wireless clients whose MAC address is listed in the MAC filter list will be able to gain network access. All other wireless client devices will be denied network access. When the MAC filter is enabled with a Block policy all wireless client devices listed whose MAC address is listed in the MAC filter list will be denied network access. All other wireless client devices will be allowed network access.

Wireless Settings > MAC Filtering

Access Policy

Filtering Policy:

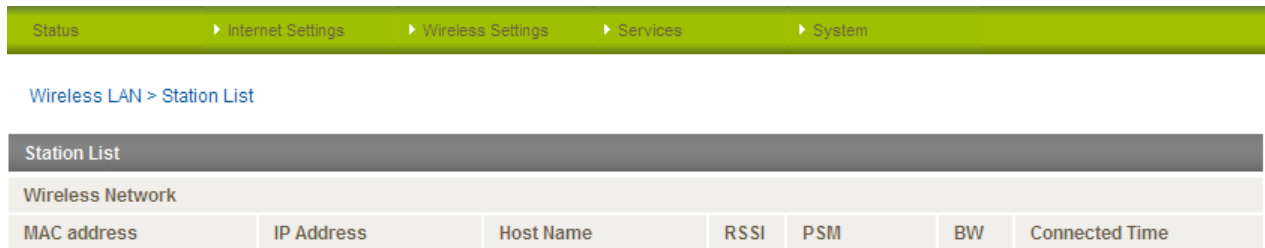
Add a MAC address to the filtering list: : : : : :

No.	SSID	MAC Address	Filtering Policy
MAC Filtering Table Empty			

Figure 45 - Wireless Settings - MAC Filter

Station Info

The Station Information page shows the number of devices currently connected to your outdoor gateway via WiFi. The MAC address, Host Name and IP address of these devices are displayed.



Wireless LAN > Station List

Wireless Network						
MAC address	IP Address	Host Name	RSSI	PSM	BW	Connected Time

Figure 46 - Wireless Station List

Services

Dynamic DNS

The DDNS page is used to configure the Dynamic DNS feature of the gateway. There are a number of dynamic DNS hosts from which you can choose.

The screenshot shows the DDNS Configuration page. At the top, there is a navigation bar with links for Status, Internet Settings, Wireless Settings, Services, and System. Below this, the breadcrumb path is 'Services > Dynamic DNS'. The main content area is titled 'DDNS Configuration' and contains a form with the following fields:

DDNS Configuration	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DDNS Settings	
Server Address	www.dhs.org
Host Name	
User Name	
Password	
Verify Password	

At the bottom of the form is a 'Save' button.

Figure 47 - DDNS Settings

Dynamic DNS provides a method for the gateway to update an external name server with the current WAN IP address.

To configure dynamic DNS:

1. Select the "Enable" option for the DDNS Configuration field.
2. Select the Dynamic DNS service that you wish to use. Enter your dynamic DNS account credentials.
3. Click the "Save" button to save any changes to the settings.

NTP

The NTP page is used to configure the local time zone and to select the NTP server used for synchronisation.

The screenshot shows the NTP Settings page. At the top, there is a navigation bar with links for Status, Internet Settings, Wireless Settings, Services, and System. Below this, the breadcrumb path is 'Services > NTP'. The main content area is titled 'Time Zone' and contains a form with the following fields:

Time Zone	
Current Time	Wed Sep 12 14:47:38 EST 2012
Time Zone	(GMT+10:00) Australia (Canberra, Melbourne, Sydney)
Click here to show the Daylight Saving Time details	
Network Time Protocol (NTP) Settings	
NTP Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
NTP Server Address	0.netcomm.pool.ntp.org

At the bottom of the form is a 'Save' button.

Figure 48 - NTP Settings

The NTP (Network Time Protocol) settings allow your gateway to synchronise its internal clock with a global Internet Time server. This setting will affect functions such as System Log entries and Firewall settings where the current system time is displayed. You can use the default NTP server or enter one manually if required.

System Monitor

The System Monitor page is used to configure the behaviour of the Periodic Ping monitor function.

Periodic PING Settings	
Destination Address	<input type="text"/>
Redundant Address	<input type="text"/>
Retry Period	<input type="text"/> (0:disable, 120-65535) secs
Failure Retry Period	<input type="text"/> (0:disable, 1-65535) secs
Failures Before Reset	<input type="text"/> (0:disable, 1-65535)

Periodic Reset	
Force reset every	<input type="text"/> (0:disable, 2-65535) mins

Figure 49 - System Monitor Settings

The Periodic Ping Reset Monitor configures the gateway to transmit controlled ping packets to two specified IP addresses. Should the gateway not receive responses to the pings, the gateway will reboot.

This works as follows:

1. After every “Retry Period” configured interval, the gateway sends 3 consecutive pings to the “Destination Address”.
2. If all 3 pings fail, the gateway sends 3 consecutive pings to the “Redundant Address”.
3. The gateway then sends 3 consecutive pings to the “Destination Address” and 3 consecutive pings to the “Redundant Address” every “Failure Retry Period” configured interval.
4. If all pings in step 3 above fail the number of times configured in “Failures Before Reset”, the gateway reboots.
5. If any ping succeeds, the gateway returns to step 1 and does not reboot.



Please note: The “Retry Period” cannot be set to a value less than 120 seconds; this is to allow the gateway time to reconnect to the cellular network following a reboot.

How to disable the Periodic Ping Monitor

To disable the Periodic Ping Reset Monitor simply set “Retry Period” to 0.



Please note: The traffic generated by the periodic ping feature is counted as chargeable usage, please keep this in mind when selecting how often to ping.

How to configure a Forced Reset

This facility is available by clicking on the “Services” menu followed by the “System Monitor” menu item on the right.

The gateway can be configured to automatically reboot after a period of time specified in minutes. While this is not necessary, it does ensure that in the case of remote installations, it will reboot the gateway if some anomaly occurs.

The default value is 0 which disables the Forced Reset Timer. The maximum value is 65535 minutes.

SNMP

The SNMP page is used to configure the SNMP features of the gateway.

Services > SNMP

SNMP Configuration

Enable SNMP Enable Disable

Read-Only Community Name

Read-Write Community Name

Download MIB File [Download](#)
(This is a brief version of the MiB file only)

SNMP Traps

Trap Destination (IP Address)

Heartbeat Interval (seconds)

Trap Persistence Time (seconds)

Trap Retransmission Time (seconds)

[Send Heartbeat Now](#)


[Save](#)

Figure 50 - SNMP Settings

SNMP (Simple Network Management Protocol) is used to remotely monitor the gateway for conditions that may warrant administrative attention. It can be used to retrieve information from the gateway such as the signal strength, the system time, the interface status, etc.

To configure SNMP:

1. Select the “Enable” option for the Enable SNMP field.
2. Enter the Community Names or leave them as default.

 Community names are used as a type of security to prevent access to reading and/or writing to the gateway's configuration. It is recommended to change the Community names to something other than the default when using this feature.

3. Click the “Save” button to save the new settings.

ITEM	DEFINITION
Trap Destination (IP Address)	The IP Address that SNMP data is to be sent to.
Heartbeat Interval (seconds)	The number of seconds between SNMP heartbeats.
Trap Persistence Time (seconds)	The length of time an SNMP trap persists.
Trap Retransmission Time (seconds)	The length of time between SNMP trap retransmissions can be configured here.

Table 24 - SNMP Configuration Options

You can also trigger an SNMP Heartbeat manually by clicking the “Send Heartbeat Now” button.

SMS

The SMS pages are used to perform functions using the built-in SMS tools application. The SMS Tools application offers basic SMS functionality such as sending a message, receiving a message and redirecting an incoming message to another destination. You can also utilise this feature to read and change run-time variables on the gateway.

Basic functionality supported:

- Ability to send a text message via a 3G network and store in permanent storage.
- Ability to receive a text message via a 3G network and store in permanent storage.
- Ability to forward incoming text messages via a 3G network to another remote destination which may be a TCP/UDP server or other mobile devices.
- Ability to read run-time variables from the device (e.g. uptime) and send result to a remote destination which may be a TCP/UDP server or other mobile devices.
- Ability to change live configuration on the device (e.g. connection APN).
- Ability to execute supported commands (e.g. reboot).

Setup

General SMS functionality is enabled by default. You can open the Setup page in order to configure additional settings. To do this, click on “Services”, then “SMS” and then “Setup”.

Figure 51 - SMS Function Setup

OPTION	DEFINITION
Messages / Page	Enter the number of SMS messages to display per page.
Encoding Scheme	The encoding method used for SMS messages.
SMSC Address	The short message service number of your mobile provider.
Redirect to Mobile	Forward incoming text messages to the remote destination defined.
Redirect to TCP	Forward incoming text messages to the remote TCP destination defined.
TCP Port to Redirect	The TCP port on which to connect to the remote destination on.
Redirect to UDP	Forward incoming text messages to the remote UDP destination defined.
UDP Port to Redirect	The UDP port on which to connect to the remote destination on.
Enable Remote Diagnostics	Enable diagnostics to be performed by a specially crafted SMS message.

Table 25 - SMS Setup Configuration Items

SMS Configuration for Redirection

Incoming text messages can be redirected to another mobile device and/or a TCP/UDP message server.

Redirect to Mobile

You can forward incoming text messages to a different destination number. This destination number can be another mobile phone or 3G gateway phone number. To disable the feature, simply delete the number in the 'Redirect To Mobile' field and click the "Save" button.

For Example:

If someone sends a text message and Redirect To Mobile is set to "0412345678", this text message is stored on the gateway and forwarded to "0412345678" at the same time.

Redirect to TCP & TCP Port, Redirect to UDP & UDP Port

You can also forward incoming text messages to a TCP/UDP based destination. The TCP or UDP server can be any kind of public or private server if the server accepts incoming text-based message.

The TCP/UDP address can be an IP address or domain name. The port number range is from 1 to 65535. Please refer to your TCP/UDP based SMS server configuration for which port to use.

For Example:

If someone sends a text message and Redirect to TCP is set to "192.168.20.3" and "2002", this text message is stored in the gateway and forwarded to "192.168.20.3" on port "2002" at the same time.

SMS Configuration for Remote Diagnostics

Enable Remote Diagnostics

Here you can enable or disable the Remote Diagnostics feature. If this setting is enabled all incoming text messages are parsed and tested for Remote Diagnostics commands.

If Remote Diagnostics commands are found, the gateway executes those commands. This feature is disabled by default.



Please note: It is possible to adjust settings and prevent your gateway from functioning correctly. If this occurs, you will need to perform a factory reset in order to restore normal operation.



It is highly recommended to enable security when utilising this feature.

New Message

The New Message page is used to send an SMS text message to multiple recipients.

The screenshot shows the 'New Message' page in a web interface. The page has a green header with navigation links: Status, Internet Settings, Wireless Settings, Services, and System. Below the header, the breadcrumb path is 'Services > SMS > New Message'. The main content area is titled 'Create New Message' and contains a table with 10 rows for destination numbers (001 to 010). Each row has a checkbox and a text input field. The first row is checked and contains '+61XXXXXXXX'. Below the table is a 'Message Body' section with a text area containing 'Test Message' and a character count '12 / 160'. A note explains character limits for GSM7 and UCS2 modes. At the bottom are 'Send' and 'Refresh' buttons.

Figure 52 - New SMS Message

A new SMS message can be sent to a maximum of 100 recipients at the same time. After sending the message, the result is displayed next to the destination number as “Success” (in blue) or “Failure” (in red).

By default 10 recipient entry fields are shown on this page however you can increase or decrease this number by pressing the + or – button at the right side of the last recipient entry field.

You can select to enable or disable individual message recipients by selecting the checkbox beside each entered number. After entering the appropriate recipient numbers, type your SMS message in the “Message Body” field and then click the “Send” button.

Inbox / Outbox

You can check all sent SMS messages in the SMS Outbox or you can read, delete, reply or forward an SMS message to another mobile device from the SMS Inbox. You are also able to add the SMS message sender to the “White List” which is used to secure the Remote Diagnostics feature. Simply select the sender or recipient number and click the “Add White List” button.

Status > Internet Settings > Wireless Settings > Services > System

Services > SMS > Inbox

Received Messages - Total 0 Messages

<input type="checkbox"/>	From	Time	Message
--------------------------	------	------	---------

[Delete](#) [Reply](#) [Forward](#) [Refresh](#) [Add White List](#) 1 / 1

Figure 53 - SMS Inbox

Status > Internet Settings > Wireless Settings > Services > System

Services > SMS > Outbox

Sent Messages - Total 0 Messages

<input type="checkbox"/>	To	Time	Message
--------------------------	----	------	---------

[Delete](#) [Forward](#) [Refresh](#) [Add White List](#) 1 / 1

Figure 54 - SMS Outbox

Diagnostics

The Diagnostics page is used to configure the SMS Diagnostics and Command execution configuration. This enables you to change the configuration or check on the status of the gateway via SMS commands.

[Status](#) > [Internet Settings](#) > [Wireless Settings](#) > [Services](#) > [System](#)

[Services](#) > [SMS](#) > [Diagnostics & Command Execution Setup](#)

SMS Diagnostics & Command Execution Configuration

Enable Authentication	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Send Ack. SMS for Set Command	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Send Ack. SMS to	<input type="radio"/> Fixed Number <input checked="" type="radio"/> SMS Sender Number
Fixed Ack. SMS Number	<input type="text"/>
Send Error SMS for Get/Set/Exec Command	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Send Error SMS to	<input type="radio"/> Fixed Number <input checked="" type="radio"/> SMS Sender Number
Fixed Error SMS Number	<input type="text"/>
Max. Diag. SMS Tx Limit	<input type="text" value="100"/> messages per <input type="text" value="DAY"/> 0 / 100 messages sent <input type="button" value="Reset"/>

Limit the maximum number of diagnostic text messages to be sent within a certain time period. The current "messages sent" count automatically resets at the beginning of the designated time unit. For example, the counter will reset to 0 at 1:00, 2:00... for "HOUR", 00:00 for "DAY", 00:00 Monday for "WEEK" and the 1st day of the month for "MONTH".

White List for Diagnostic or Execution SMS Messages

Incoming diagnostic or execution SMS messages are first checked with this White List. If the sender and password of the message do not match any of the destination numbers and passwords in the list, the message is ignored and an error message is sent either to the sender, or a predefined destination. Destination numbers can be easily added from SMS Inbox/Outbox pages using the "Add White List" button, up to a maximum of 20 entries.

Index	Destination Number	Password	Control
01	<input type="text"/>	<input type="text"/>	<input type="button" value="Delete"/> <input type="button" value="+"/> <input type="button" value="-"/>

Figure 55 - SMS Diagnostics Settings

The following pages detail the configuration items available.

Enable Authentication

Enable or disable checking the sender's phone number against the allowed sender "White List" for incoming Diagnostics/Command Execution SMS messages.

If authentication is enabled, the gateway will check if the sender's number exists in the "White List". If it exists, the gateway then checks the password in the incoming message against the password in the "White List" for the corresponding sending number. If they match, the Diagnostics/Command is executed.

If the number does not exist in "White List" or the password does not match, the gateway does not execute the incoming Diagnostics/Command Execution SMS message.

This is enabled by default.



It is highly recommended to enable security when utilising the Diagnostics/Command Execution feature.

Send Ack. SMS for Set Command

Enable or disable sending an acknowledge message after execution of a "Set" command.

If disabled the gateway does not send any acknowledgement after execution of a "Set" command. This can be useful to determine if a command was received and executed by the gateway. This is disabled by default.

Send Ack. SMS to

Select destination to send an acknowledgement message to after the execution of a "Set" command.

If "Fixed Ack. SMS Number" is selected, the acknowledgement message will be sent to the predefined number in the "Fixed Ack. SMS Number" field.

If the SMS Sender Number is selected, the acknowledgement message will be sent to sender directly. The default setting is to use "SMS Sender Number".

Fixed Ack. SMS Number

Use this field to enter the destination number to which acknowledgement messages are sent after the execution of a "Set" command.

Send Error SMS for Get/Set/Exec Command

Enable or disable the sending of an error message resulting from the execution of a Get/Set/Exec command.

If disabled, the gateway does not send any error notifications after the execution of a Get/Set/Exec command.

This function is disabled by default.

Send Error SMS to

Select the destination of the error messages from the execution of a Get/Set/Exec command.

If "Fixed Number" is selected, any error messages will be sent to the predefined number in the "Fixed Error SMS Number" field.

If "SMS Sender Number" is selected, any error messages will be sent to the sender directly.

The default setting is to use "SMS Sender Number".

Fixed Error SMS Number

The destination number to which error messages from the execution of a Get/Set/Exec command should be sent.

Max. Diag. SMS Tx Limit

You can set the maximum number of acknowledgement and error messages sent when an SMS Diagnostics and/or Command is executed. You can set the maximum limit on a per hour/day/week or month basis.

The default is to send a maximum of 100 messages per day.

You can check the current sent message count by looking next to the “Max. Diag. SMS Tx Limit” field. If the maximum number has been exceeded, you can also reset sent the message counter by pressing the “Reset” button.

The Total transmitted message count resets after a reboot or at the beginning of the time frame specified.



Please note: Times displayed are in UTC format.

For Example:

- If the time frame is set to “**HOUR**” and the current time is “04:30”, then the counter will reset to zero at “05:00”.
- If time frame is set to “**DAY**” and current date and time is “04:30” 17th of March, then the counter will reset to zero at “00:00” 18th of March.
- If time period is set to “**WEEK**” and current date and time is “04:30” Saturday, then the counter will reset to zero at “00:00” on the coming Monday.
- If time period is set to “**MONTH**” and current date and time is “04:30” 17th of March, then the counter will reset to zero at “00:00” 1st of April.

White List

A maximum number of 20 entries can be stored in the gateway.

If Authentication is enabled, any incoming Diagnostics/Command Execution SMS messages are processed only if the sender’s number exists in White List and the message password matches with the password specified in the White List.

One blank entry is shown by default and you can add or delete an entry by pressing the “+” or “-” button. The White List numbers and passwords can be cleared by pressing the “Delete” button.

To add an entry, simply enter the appropriate phone number and password and click “Save”.

Message Storage for Diagnostic Messages

Diagnostic messages (Diagnostic commands, acknowledgements and error notification messages) sent to remote destination are stored in Inbox/Outbox.

Security

In order to provide security for SMS command execution, it is recommended that all SMS commands be subject to successful authentication against the White List as well as setting a password for each phone number entered.

This prevents unauthorised or accidental execution of SMS commands.

SMS Command format

Generic Format for reading variables:

get VARIABLE
PASSWORD get VARIABLE

Generic Format for writing to variables:

set VARIABLE=VALUE
PASSWORD set VARIABLE=VALUE

Generic Format for executing a command:

executeCOMMAND
PASSWORD executeCOMMAND

Replies

Upon receipt of successfully formatted, authenticated (if required) command, the gateway will reply to the SMS in the following format:

TYPE	SMS CONTENTS	NOTES
Get Command	"VARIABLE=VALUE"	
Set Command	"Successfully set VARIABLE to VALUE"	Only sent if the acknowledgment message function is enabled
Execute Command	"Successfully executed command COMMAND"	

Table 26 - SMS Diagnostic Command Syntax

Where "VARIABLE" is the name of the value to be read

Where "VARIABLE (x)" is the name of another value to be read

Where "VALUE" is the content to be written to the "VARIABLE"

Where "COMMAND" is a supported command to be executed by the device (e.g. reboot)

Where "PASSWORD" is the password (if configured) for the corresponding sender number specified in the White List

Multiple commands can be sent in the same message, if separated by a semicolon.

For Example:

```
get VARIABLE1; get VARIABLE2; get VARIABLE3  
PASSWORD get VARIABLE1; get VARIABLE2  
set VARIABLE=VALUE1 ; set VARIABLE2=VALUE2  
PASSWORD set VARIABLE1=VALUE1; set VARIABLE2=VALUE2; set VARIABLE3=VALUE3
```

If required, values can also be bound by an apostrophe, double apostrophe or back tick.

For Example:

```
"set VARIABLE='VALUE'"  
"set VARIABLE=""VALUE""  
"set VARIABLE=`VALUE`"  
"get VARIABLE"
```

A password (if required), only needs to be specified once per SMS, but can be prefixed to each command if desired.

```
"PASSWORD get Variable1"; "get VARIABLE2"  
"PASSWORD set VARIABLE1=VALUE1"; "set VARIABLE2=VALUE2"
```

If the command sent includes the "reboot" command and has already passed the White List password check, the device keeps this password and executes the remaining command line after the reboot with this same password.

For Example:

```
"PASSWORD execute reboot; getVariable1"; "get VARIABLE2"  
"PASSWORD execute reboot; PASSWORD get Variable1"; "get VARIABLE2"
```

Commands are case insensitive, however variable names and values are case sensitive.

List of valid commands (which can be used in conjunction with the execute command):

“pdpcycle”, “pdpdown” and “pdpup” commands can have a profile number suffix ‘x’ added. Without the suffix specified, the command operates against the current active profile or last active profile.

#	COMMAND NAME	DESCRIPTION
1	reboot	Immediately perform a soft reboot
2	pdpcycle or pdpcyclex	Disconnect (if connected) and reconnect the 3G connection. If a profile number is selected in the command, try to disconnect/reconnect the specified profile in case the profile is active. If no profile number is selected, try to disconnect/reconnect the current active profile. Reports an error if no profile number is selected and there is no currently activated profile.
3	pdpdown or pdpdownx	Disconnect the PDP. If a profile number is selected in the command, try to disconnect the specified profile in case the profile is active. If no profile number is selected, try to disconnect the current active profile. Reports an error if no profile number is selected and there is no currently activated profile.
4	pdpup or pdpupx	Reconnect the PDP. If a profile number is selected in the command, try to connect with the specified profile. If no profile number is selected, try to connect to the last active profile. The gateway will check the currently activated profile and disconnect this profile before executing the command. Reports an error if no profile number is selected and there is no stored last active profile number.

Table 27 - List of Valid SMS Diagnostic Commands

The following table lists valid variables where “x” is a profile number (1-6). If no profile is specified, variables are read or written to for the current active profile. If a profile is specified, variable are read or written to for the specified profile number (‘x’).

#	RDB VARIABLE NAME	SMS VARIABLE NAME	READ/ WRITE	DESCRIPTION	EXAMPLE
0	link.profile.x.enable link.profile.x.apn link.profile.x.user link.profile.x.pass link.profile.x.auth_type link.profile.x.iplocal link.profile.x.status	profile or profilex	RW	Profile	Read: (profile no,apn,user,pass,auth,iplocal,status) 1,Telstra.internet,username,password, chap,202.44.185.111,up Write: (apn, user, pass,auth) telstra.internet,username,password
1	link.profile.x.apn	apn or apnx	RW	APN	telstra. Internet
2	link.profile.x.user	username or usernamex	RW	3G username	Guest, could also return “null”
3	link.profile.x.pass	password or password	RW	3G password	Guest, could also return “null”
4	link.profile.x.auth_type	authtype or authtypex	RW	3G Authentication type	“pap” or “chap”
5	link.profile.x.iplocal	wanip or wanipx	R	WAN IP address	202.44.185.111
6	wwan.0.radio.information.signal_strength	rsi	R	3G signal strength	65 dBm
7	wwan.0.imei	imei	R	IMEI number	359102128941027512
8	statistics.usage_current	<u>usage</u>	R	3G data usage of current session	“Rx 500 bytes, Tx 1024 bytes, Total 1524 bytes” or “Rx 0 byte, Tx 0 byte, Total 0 byte” when wwan down
9	statistics.usage_current	wanuptime	R	Up time of current 3G session	1 days 02:30:12 or 0 days 00:00:00 when wwan down
10	/proc/uptime	deviceuptime	R	Device up time	1 days 02:30:12
11	wwan.0.system_network_status.current_band	band	R	Current 3G frequency	WCDMA 850

Table 28 - List of SMS Diagnostics Variables

SMS Diagnostics Examples

The examples below demonstrate various combinations of supported commands. This is not a complete list. To obtain a complete list, please contact NetComm.

DESCRIPTION	AUTHENTICATION	INPUT EXAMPLE
Send SMS to change APN	Not required	set apn1=Telstra.internet set apn2="3netaccecss"
	Required	Password1234 set apn1=Telstra.internet Password1234 set apn2=3netaccecss
Send SMS to change the 3G username	Not required	set username='NetComm'
	Required	Password1234 set username= "NetComm"
Send SMS to change the 3G password	Not required	set password= 'NetComm'
	Required	Password1234 set password= 'NetComm'
Send SMS to change the 3G authentication	Not required	set authtype= 'pap'
	Required	Password1234 set authtype = pap
Send SMS to reboot	Not required	execute reboot
	Required	Password1234 execute reboot
Send SMS to check the WAN IP address	Not required	get wanip
	Required	Password1234 get wanip
Send SMS to check the 3G signal strength	Not required	get rssi
	Required	Password1234 get rssi
Send SMS to check the IMEI number	Not required	get imei
	Required	Password1234 get imei
Send SMS to check the current band	Not required	get band
	Required	Password1234 get band
Send SMS to Disconnect (if disconnected) and reconnect the 3G connection	Not required	execute pdpcycle
	Required	Password1234 execute "pdpcycle1"
Send SMS to disconnect the 3G connection	Not required	execute pdpdown1
	Required	Password1234 execute "pdpdown1"
Send SMS to connection the 3G connection	Not required	execute pdpup
	Required	Password1234 execute pdpup1
Send multiple get command	Not required	get wanip; get rssi
	Required	Password1234 get wanip; get rssi
Send multiple set command	Not required	set apn1="3netaccecss"; set password1='NetComm'
	Required	Password1234 set APN="3netaccecss"; set password=NetComm

Table 29 - SMS Diagnostics - Example Commands

System

Log

The Log page is used to download or display the current System Log of the gateway.



Figure 56 - System Log


The System Log enables you to troubleshoot any issues you may be experiencing with your gateway. Selecting the appropriate logging level will show you either informational messages about your gateway or every message produced when “All” is selected.

LOG LEVEL	DEFINITION
All	Display all system log messages.
Debug	Show extended system log messages with full debugging level details.
Info	Show informational messages only.
Notice	Show normal system logging information.
Warning	Show warning messages only.
Error	Show error condition messages only.

Table 30 - System Log Detail Levels

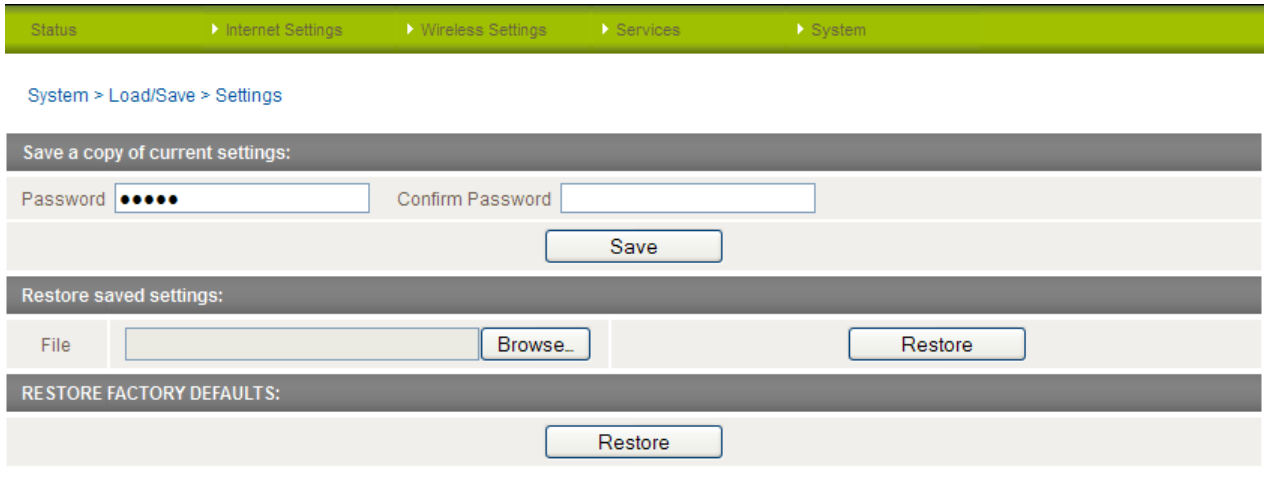
You can also download the current System Log to your computer for off-line viewing. To do this, click the “Download Log File” link at the bottom of the page.

Load / Save

 Please Note: the Load/Save menu is only available to users logged in to the gateway using the user name `root`. To perform Firmware upgrade, device configuration backup and reset the gateway to factory defaults, you need to login as the root user.

Settings

The settings page is used to backup or restore the gateway's configuration or to reset it to factory default settings.



The screenshot shows the 'Load/Save' configuration page. At the top, there is a navigation bar with 'Status', 'Internet Settings', 'Wireless Settings', 'Services', and 'System'. Below this, the breadcrumb 'System > Load/Save > Settings' is displayed. The page is divided into three main sections: 1. 'Save a copy of current settings:' which includes a 'Password' field (masked with dots), a 'Confirm Password' field, and a 'Save' button. 2. 'Restore saved settings:' which includes a 'File' input field, a 'Browse...' button, and a 'Restore' button. 3. 'RESTORE FACTORY DEFAULTS:' which includes a 'Restore' button.

Figure 57 - Load / Save Configuration Page

 Please note: In order to perform an update, you must be logged into the gateway as the root user (see the [Remote Administration](#) section for more details).

To save a copy of the gateway's configuration

Type the root manager Password and click the "Save" button.

This will download a copy of the current settings from the gateway to your PC.

 Please note: The following conditions apply:

- It is NOT possible to edit the contents of the file downloaded; if you modify the contents of the configuration file in any way you will not be able to restore it later.
- You may change the name of the file if you wish but the filename extension must remain ".cfg"

To restore a copy of the gateway's configuration

1. Click the "Browse..." button under the "Restore Saved settings:" section.
2. Select the previously saved configuration file that you wish to restore to the gateway.
3. Click the "Restore" button.

To restore the gateway's configuration to the factory defaults

Click the "Restore" button under the "Restore Factory Defaults" section to restore the gateway to factory default settings.

The gateway will then restart with the factory default configuration loaded.

Upload

The Upload page enables you to upload and install firmware files or user created application packages to the Telstra Outdoor Gateway.

File Name	Date	Size	Action
ntc_30ww_1.9.27.0.cdi	Jan 1 1970	19.0M	Install Delete

Figure 58 - Upload Page



Please note: In order to perform an update, you must be logged into the gateway as the root user (see the Remote Administration section for more details).

Firmware upgrade

The firmware update process has two steps. The first step is to upload and install the system recovery image onto the gateway.

You can do this by clicking on the browse button and then to navigate to where the recovery image upgrade file is located on your computer.

Once you have selected the system recovery image file to use, click Upload to upload the file. You will then see a progress bar as shown in the screenshot below. The upload has finished when the status bar reaches 100%.

Phase:	Upload
Percent Complete:	12 %
Current Position:	2288 / 19508 KBytes
Elapsed time:	00:00:03
Est Time Left:	00:00:13
Est Speed:	1315 KB/s.

Figure 59 - Local Firmware Upgrade - Upload Firmware

When the upload has completed, the screen should refresh and list the system recovery file you have just uploaded. Click on the “Install” link to the right of this.

Once you see “Done” shown as per the screenshot below, you can then boot into the system recovery mode to install the main system software.

```
Done
Done
Done
Firmware update successful!
```

Figure 60 - Local Firmware Upgrade - Firmware Update

Press and hold the reset button for approximately 5 – 10 seconds until the LEDs on the front of the gateway start to flash in an ON / OFF sequence and then release it. The gateway will now boot into the system recovery mode.

The second step is to upload and install the main system software image. To do this, open your web browser (e.g. Internet Explorer/Firefox/Safari) and navigate to <http://192.168.1.1/>

Click “Login” and type `root` in the Username and `admin` in the Password fields then click on “Submit”.

The banner at the top of the page should change to show that the gateway is currently in recovery console mode.



Figure 61 - Recovery Console Banner

To upload the main system software, click on “Application Installer” from the menu at the top of the page and then click on the browse button and navigate to where the main system image upgrade file is located on your computer.

Once you have selected the recovery image file to use, click Upload to upload the file. You will then see a progress bar as shown in the screenshot below. The upload has finished when the status bar reaches 100%.

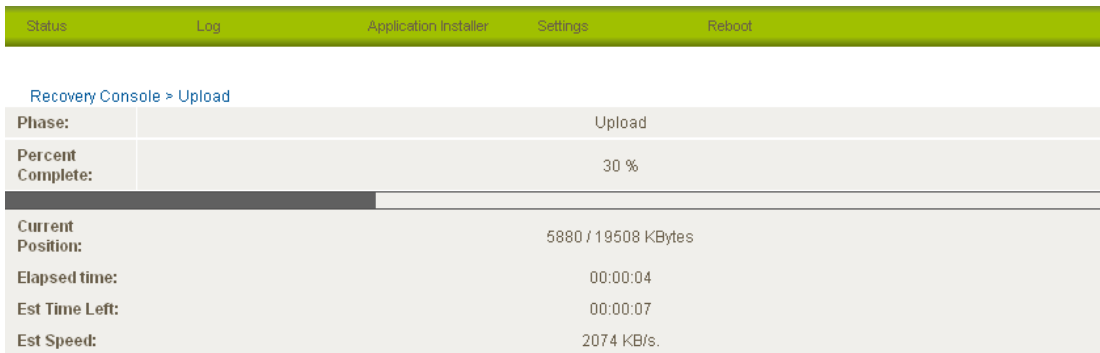


Figure 62 - Recovery Console - Upload Firmware

When the upload has completed, the screen should refresh and show the file you have just uploaded. Click on the “Install” link to the right of this.

Once you see “Done” shown as per the screenshot below, click on “Reboot” at the top of the page and then click the “Reboot” button to restart the gateway.

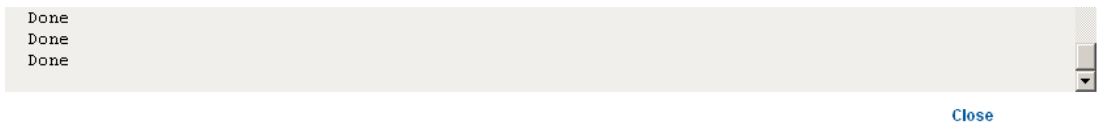
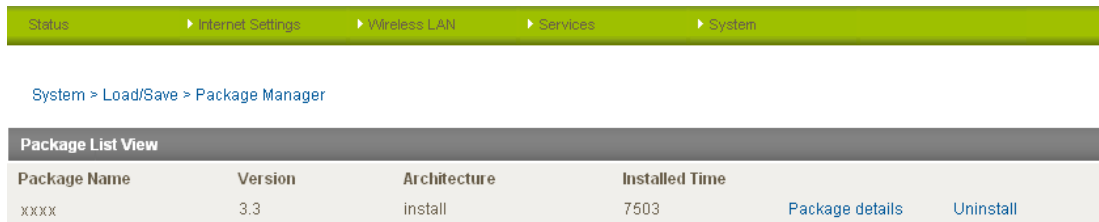


Figure 63 - Recovery Console - Firmware Update

The gateway will confirm you want to restart and then start up with the new system software loaded.

Package Manager

The Package Manager page is used to provide details of any user installed packages on the gateway.



The screenshot shows a navigation bar with the following items: Status, Internet Settings, Wireless LAN, Services, and System. Below the navigation bar is a breadcrumb trail: System > Load/Save > Package Manager. The main content area is titled "Package List View" and contains a table with the following data:

Package Name	Version	Architecture	Installed Time		
XXXX	3.3	install	7503	Package details	Uninstall

Figure 64 - Package Manager Items

The Package Name, Version, Architecture, and Install time are shown and the package content details are available by clicking on the blue "Package Details" link.

Alternatively, if you want to remove a package, click the blue "Uninstall" link.

 Please note: For more information on creating software packages for the gateway, please refer to the SDK document available from the NetComm Wireless website.

Administration

The Administration page is used to enable or disable the firewall, remote administration, telnet access and ping responses.

The screenshot shows the Administration configuration page with the following sections:

- System > Administration** breadcrumb.
- Firewall** section:
 - Firewall: Enable Disable
 - Enable HTTP: Port (1 - 65534)
 - Enable Telnet:
 - Enable Ping:
- Web User Interface Account** section:
 - User Name:
 - Admin Password:
 - Confirm Password:
- Telnet Account** section:
 - User Name:
 - Admin Password:
 - Confirm Password:
- Save** button.

Figure 65 - Administration Configuration Items

OPTION	DEFINITION
Firewall	Enable or disable the in-built firewall on the gateway.
Enable HTTP	Enable or disable remote HTTP access to the gateway. You can also set the port you would like remote HTTP access to be available on.
Enable Telnet	Enable or disable telnet (command line) access to the gateway.
Enable Ping	Enable or disable ping responses on the WWAN connection.
Web User Interface Account	
Username	Select the username you would like to change the password for. Root users have write permissions for both the root and admin accounts. Admin users can only update the admin password.
Password	Enter the new password for the selected user account.
Confirm Password	Re-enter the new password for the selected user account.
Telnet Account	
User Name	The Telnet Account settings are only available when logged into the gateway as the 'root' user.
Password	Enter the new password for the root telnet user account.
Confirm Password	Re-enter the new password for the root telnet user account.

Table 31 - Administration Configuration Items

 Please note: The password will only be changed if you enter two matching passwords. It is not necessary to change the password if you are only changing the incoming port number.

To access the gateway's configuration pages remotely, perform the following steps:


1. Open a new browser window (e.g. Internet Explorer, Firefox, Safari ...).
2. In the address bar, enter the gateway's WAN IP address and assigned port number, e.g. "10.10.10.10:8080".

 Please note: You can find the gateway's WAN IP address by clicking on the "Status" menu. The Local field in the WWAN section shows the gateway's WAN IP address.

3. Click "Login" and type admin or root in the Username and admin in the Password fields. Then click on "Submit".

System Configuration

The System configuration page is used to specify an external syslog server and the TCP Keepalive settings.

 Please note: the Load/Save menu is only available to users logged in to the gateway using the user name root. To perform Firmware upgrade, device configuration backup and reset the gateway to factory defaults, you need to login as the root user.

The TCP Keepalive function can be used to ensure the WWAN connection does not disconnect due to inactivity.




Figure 66 - System Configuration Items

OPTION	DEFINITION
IP / Hostname [PORT]	The IP address and port of the external syslog server you would like logging information sent to.
Keepalive	Enable or Disable the TCP Keepalive function.
Keepalive Time	The interval between the last packet sent and the first TCP keepalive packet being sent.
Keepalive Interval	The time between subsequent TCP Keepalive packets.
Keepalive Probes	The number of TCP Keepalive packets to send.

Table 32 - System Configuration Items

TR-069

The TR-069 (Technical Report 069) protocol is a technical specification also known as CPE WAN Management Protocol (CWMP). It is a framework for remote management and auto-configuration of end-user devices such as customer-premises equipment (CPE) and Auto Configuration Servers (ACS). It is particularly efficient in applying configuration updates across networks to multiple CPEs.

It uses a bi-directional SOAP/HTTP-based protocol based on the application layer protocol.

The screenshot shows a web-based configuration interface for TR-069. At the top, there is a navigation bar with links for Status, Internet Settings, Wireless Settings, Services, and System. Below this, the page title is 'Services > TR-069'. The main content is divided into two sections:

- TR-069 Configuration:** This section contains several fields:
 - 'Enable TR-069 Service' with radio buttons for 'Enable' and 'Disable' (selected).
 - 'ACS URL' with an empty text input field.
 - 'ACS Username' with a text input field containing 'acs'.
 - 'ACS Password' and 'Verify ACS Password' with masked password input fields (represented by dots).
 - 'Enable Periodic ACS Informs' with radio buttons for 'Enable' (selected) and 'Disable'.
 - 'Inform Period' with a text input field containing '600' and a label '(30-2592000) second'.
- TR-069 Connection Request:** This section contains:
 - 'Connection Request Username' with a text input field containing 'cpe'.
 - 'Connection Request Password' and 'Verify Password' with masked password input fields.

Each section has a 'Save' button at the bottom.

Figure 67 - System - TR-069

OPTION	DEFINITION
Enable TR069 Service	This field provides the option to switch on or off the TR069 feature. ..
ACS URL	This field can be used to enter the domain name or IP address of the Auto Configuration Server (ACS) you wish to use.
ACS Password/Verify ACS Password	This field can be used to enter the password that the Auto Configuration Server (ACS) uses
Enable Periodic ACS Informs	Each session begins with the transmission of an Inform message from the ACS server. If able to the CPE device responds with an Inform Response message. A periodic Inform message verifies that each CPE device is capable of communicating and receiving updates from the ACS server
Keepalive Probes	The number of TCP Keepalive packets to send.
Inform Period	Enter the time in seconds between periodic Inform messages. The maximum time span possible is equivalent to more than 68 years.
Connection Request Username	Enter the TR-069 connection request username here.
Connection Request Password	Enter the TR-069 connection request password here.
Verify Password	Re-enter the TR-069 connection request password here and press the Save button.

Table 33 - System - TR-069 Details

Logoff

The logoff item will log you out of your web configuration session.

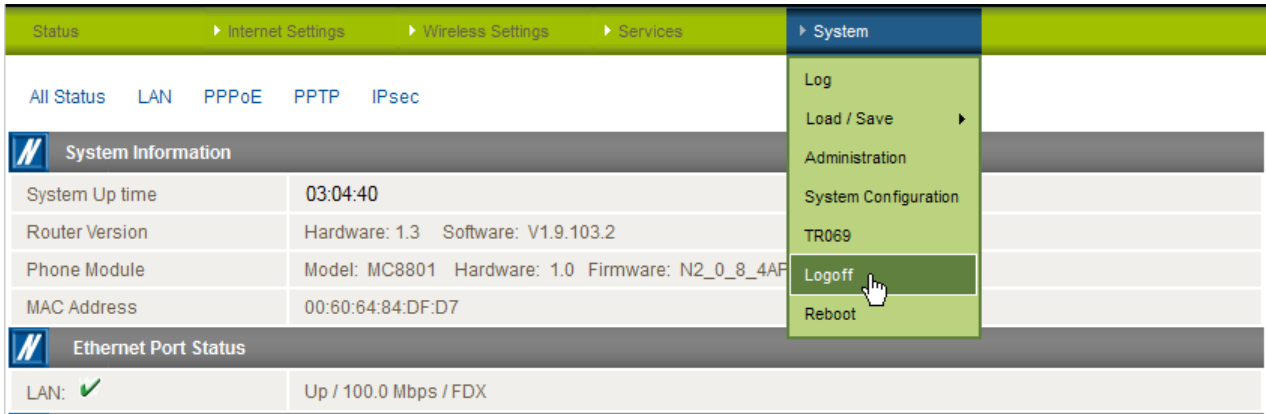


Figure 68 - Logoff

Reboot

The reboot item will reboot the gateway. This can be useful if you have made configuration changes you want to implement or want to reboot the gateway.

 Please Note: the Load/Save menu is only available to users logged in to the gateway using the user name root. To perform Firmware upgrade, device configuration backup and reset the gateway to factory defaults, you need to login as the root user.

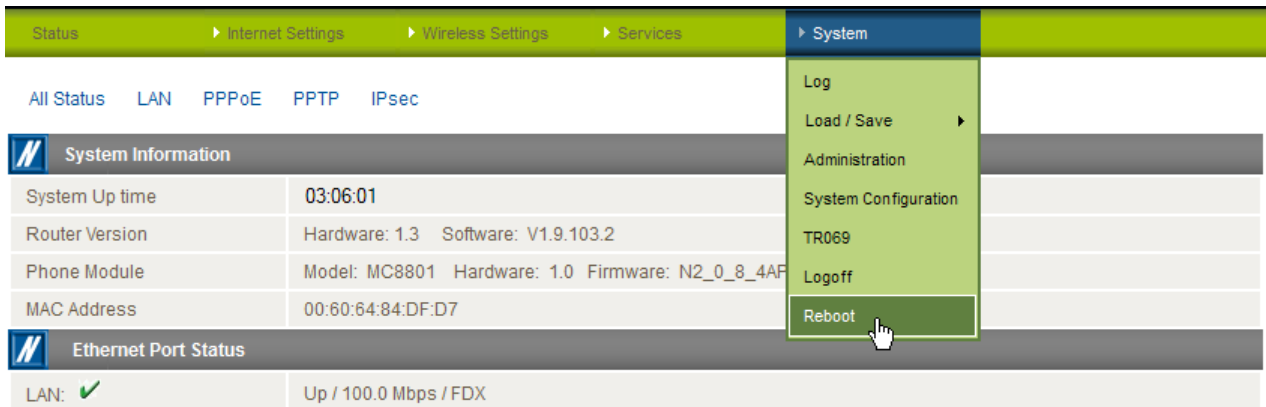


Figure 69 - Reboot Gateway

Configuration of the Indoor WiFi Access Point

Installing the WiFi Access Point

Please refer to the Telstra Outdoor Quick Start Guide for information on connecting the WiFi Access Point.

Configuring the Indoor Access Point

To log in to the management console, view the status and make changes to your indoor access point, please follow the steps below:

1. Open your web browser (e.g. Internet Explorer/Firefox/Safari) and navigate to <http://192.168.1.2>
2. Enter the username and password configured during the first time setup and click the Submit button. The default username and password is "admin" if the details haven't been customized. Click the Submit button to continue.

The screenshot shows a web interface with a dark header containing 'Status' and 'Login' tabs. Below the header is a 'Login' form with two input fields: 'Username' and 'Password'. At the bottom of the form are two buttons: 'Submit' and 'Clear'.

Figure 70 - Login prompt for Indoor Access Point web interface

After logging in, the Status page should then be displayed.

Status

The status page provides a summary of the wireless settings on both radio bands and is displayed when you login to the access point console.

The screenshot shows a web interface with a dark header containing 'Status', 'Network Setup', and 'Toolbox' tabs. Below the header is a 'Wireless 2.4GHz Status' table and a 'Wireless 5GHz Status' table. Both tables have columns for 'Item', 'WLAN Status', and 'Sidenote'. A 'Refresh' button is located below the tables, and the device time is displayed at the bottom.

Wireless 2.4GHz Status		
Item	WLAN Status	Sidenote
Wireless 2.4GHz mode	Enable	(B/G/N Mixed)
SSID	Telstra 2204	
Channel	Auto	
Security	WPA-PSK / WPA2-PSK	(TKIP/AES)

Wireless 5GHz Status		
Item	WLAN Status	Sidenote
Wireless 5GHz mode	Enable	(A/N Mixed)
SSID	Telstra 5GHz 1353	
Channel	Auto	
Security	WPA-PSK / WPA2-PSK	(TKIP/AES)

Device Time: Thu, 01 Jan 2009 10:20:50 +1000

Figure 71 - Status page of the Indoor Access Point

DHCP Server

The Indoor WiFi Access Point is equipped with a DHCP Server but it is disabled by default as the most common scenario is to have DHCP configured on the outdoor gateway. The DHCP Server page allows you to configure DHCP settings on the indoor access point. You can manually set the DHCP Start and End range, the DHCP Lease time, the default Domain name suffix, Primary and Secondary DNS Server, the Primary and Secondary WINS Server, and an optional Gateway address.

Item	Setting
DHCP Server	DHCP <input checked="" type="radio"/> Disable <input type="radio"/> Enable
LAN IP Address	<input type="text" value="192.168.1.2"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
IP Pool Starting Address	<input type="text" value="100"/>
IP Pool Ending Address	<input type="text" value="200"/>
Lease Time	<input type="text" value="86400"/> Seconds
Domain Name	<input type="text"/>
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
Primary WINS	<input type="text"/>
Secondary WINS	<input type="text"/>
Gateway	<input type="text"/> (optional)

Figure 72 - DHCP Server Settings page

Wireless 2.4GHz and 5GHz

These pages let you configure settings for the 2.4GHz or 5GHz wireless modules. You can enable or disable the module, configure the SSID, wireless channel, wireless mode, authentication type, enable or disable 802.1X, select encryption type and modify the Pre-Shared Key.

Item	Setting
Wireless Module (2.4GHz)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network ID (SSID)	<input type="text" value="Telstra 2204"/>
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	<input type="text" value="Auto"/>
Wireless Mode	<input type="text" value="B/G/N mixed"/>
Authentication	<input type="text" value="WPA-PSK / WPA2-PSK"/>
802.1X	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Encryption	<input type="text" value="TKIP / AES"/>
Pre-shared Key	<input type="text" value="Dayumahoju"/>

Figure 73 - Wireless 2.4GHz Settings page

Item	Setting
Wireless Module (5GHz)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network ID (SSID)	<input type="text" value="Telstra 5GHz 1353"/>
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Channel	<input type="text" value="Auto"/>
Wireless Mode	<input type="text" value="A/N mixed"/>
Authentication	<input type="text" value="WPA-PSK / WPA2-PSK"/>
802.1X	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Encryption	<input type="text" value="TKIP / AES"/>
Pre-shared Key	<input type="text" value="zoquxevuzo"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="WDS Setting..."/> <input type="button" value="WPS Setup..."/> <input type="button" value="Wireless Client List..."/>	

Figure 74 - Wireless 5GHz Settings page

WDS Setting

This screen allows you to enable or disable wireless bridging. Enter the MAC address of the remote access points to use this feature. Click Save when you are done.

Item	Setting
Wireless Bridging	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Remote AP MAC 1	<input type="text"/>
Remote AP MAC 2	<input type="text"/>
Remote AP MAC 3	<input type="text"/>
Remote AP MAC 4	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Back"/>	

Figure 75 - WDS Settings screen

WPS Setting

The WPS Setting page allows you to connect WPS certified equipment to the Indoor WiFi Access Point. Use this page to generate a new PIN, configure the mode of operation, view the WPS status and change the WPS method. You can also use the Trigger button to begin the WPS connection process.

Item	Setting
WPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP PIN	<input type="button" value="Generate New PIN"/>
Config Mode	<input type="text" value="Registrar"/>
Config Status	CONFIGURED <input type="button" value="Release"/>
Config Method	<input type="text" value="Push Button"/>
WPS status	IDLE
<input type="button" value="Save"/> <input type="button" value="Trigger"/> <input type="button" value="Cancel"/>	

Figure 76 - WPS Settings page

Wireless Client List

The Wireless Client list shows the ID and MAC Address of the connected devices.

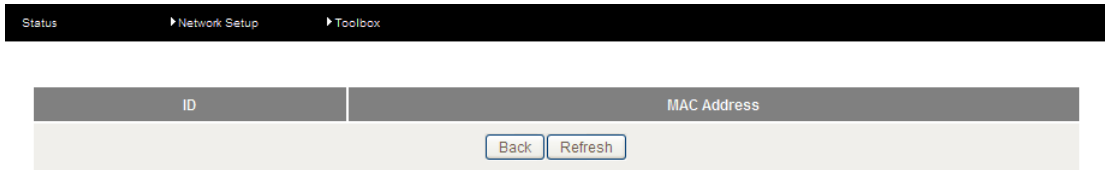


Figure 77 - Wireless Client List

Change Password

Use this page to change the default password for the access point. It is highly recommended that you change the administrator password for security reasons.

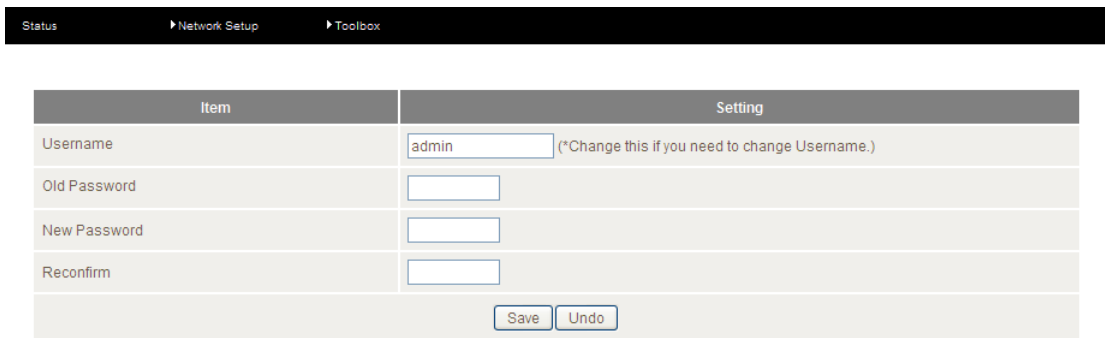


Figure 78 - Change Password screen

System Time

The System Time page allows you to synchronise the time on the access point with the time on your computer. Click the button and the time will synchronise immediately.

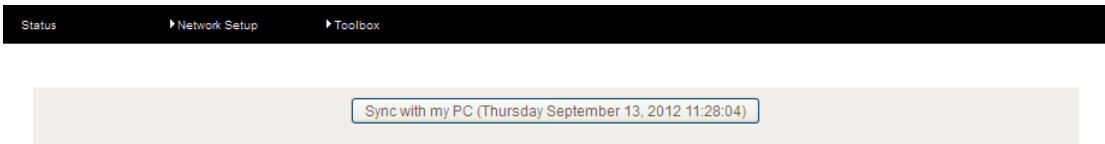


Figure 79 - System time page

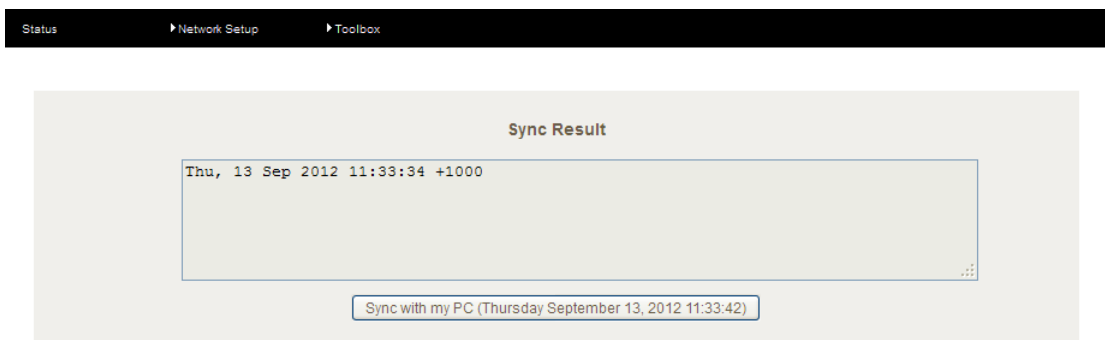


Figure 80 - System Time - Sync Result

Restore Settings

The restore settings screen allows you to restore system settings that you have previously backed up. This is useful in the event that you have performed a factory reset of the access point and want to quickly restore the previous configuration.

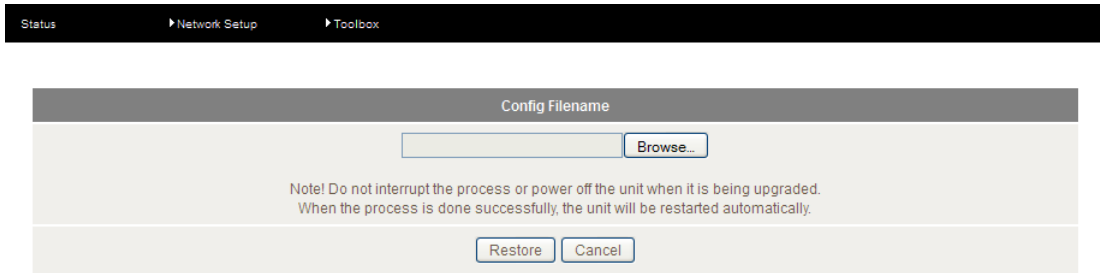


Figure 81 - Restore Settings screen

Firmware Upgrade

The firmware upgrade page enables you to upgrade the firmware of the Indoor WiFi Access Point. Occasionally, updates to the firmware are released which can offer new features and fix bugs. Click the Browse button and locate the firmware file on your local hard drive then click Upgrade to begin the process.

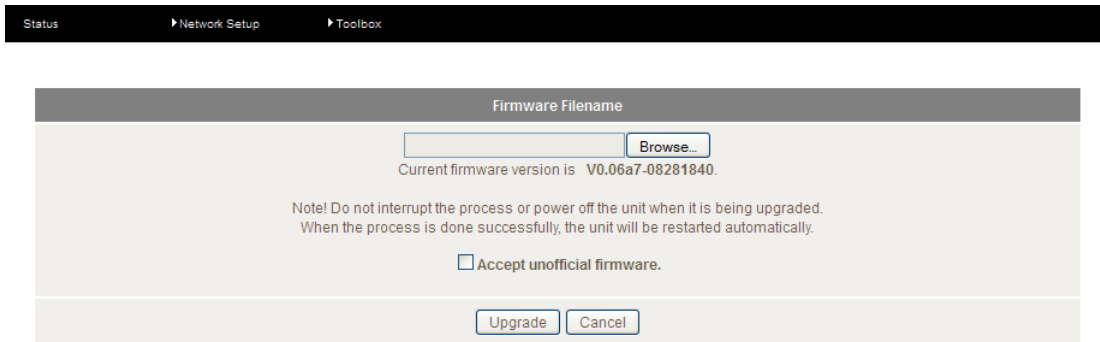


Figure 82 - Firmware upgrade screen

Backup Settings

To backup the configuration of the access point, move your mouse over Toolbox then click Backup Settings. Your browser will prompt you to save the configuration file.

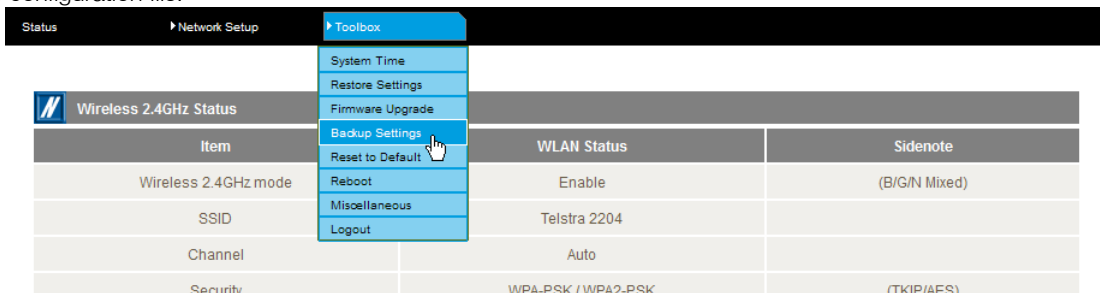


Figure 83 - Backup Settings screen

Reset to Default

This option allows you to reset the access point to factory default settings. Click the Reset to Default option and then select OK to proceed with the factory default reset.

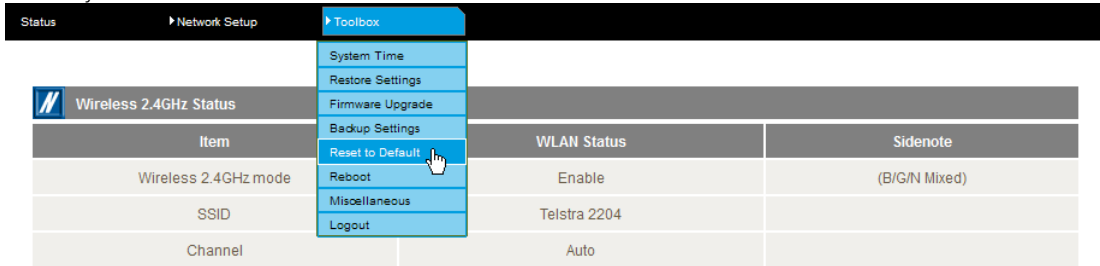


Figure 84 - Reset to default option

Reboot

You can use this option to perform a soft reboot. After clicking on Reboot, choose OK to reboot the access point.

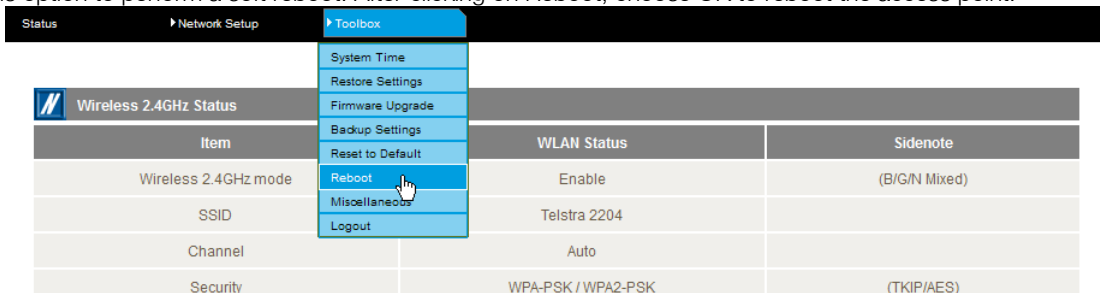


Figure 85 - Reboot option

Miscellaneous

The miscellaneous screen provides the option to configure the Administrator time out setting. When logged in and no activity has been performed on the access point, the administrator will be automatically logged out after the specified number of seconds. If you do not want to be automatically logged out, set this to 0. Ensure you click Save to save your changes.

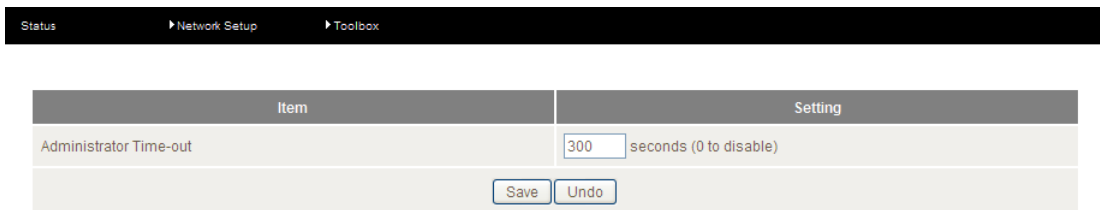
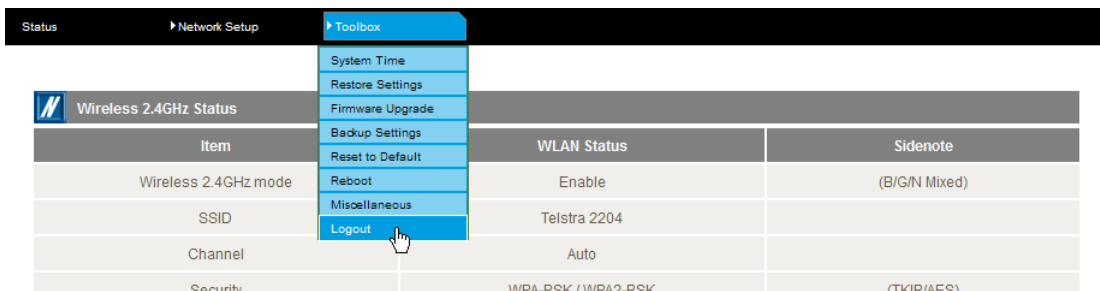


Figure 86 - Miscellaneous screen

Logout

The logout option will log you out of your web configuration session.



Technical Data

The following table lists the hardware specifications of the Telstra Outdoor Gateway.

MODEL	TELSTRA OUTDOOR GATEWAY
Modem Module/Chipset	Sierra Wireless MC8801
Wireless LAN	Ralink RT3072 (IEEE 802.11b/g/n – 2T2R)
Memory	RAM: 64MB DRAM Storage: 256MB Flash
Operating System	Embedded Linux 2.6
UMTS bands	Quad-Band: 850/900/1900/2100Mhz
GSM bands	Quad-Band: 850/900/1800/1900Mhz
Maximum Data Throughput / 3G Radio interface	Downlink: 42 Mbps (HSDPA Cat. 8); Uplink: 5.76 Mbps (HSUPA Cat. 6); EDGE MS Class 12: 236 kbps
Wireless Frequency	2.4 – 2.438Ghz
Peak Data Rate (Wireless)	300 Mbps (MIMO)
Wireless Security	WEP, WPA, WPA-PSK, WPA2-PSK, Mixed WPA-PSK/WPA2-PSK, TKIP, AES
Connectivity	1 x RJ-45 Fast Ethernet 10/100Base-TX w/ Auto MDIX 1 x Optional Circular IP67 Power Connection (When PoE not used)
SIM Card Reader	1 x Lockable SIM Card Tray Reader, Push to Release
Antenna connectors	Cellular: 2 x detachable TNC (1 x Main and 1 x Rx Diversity) WLAN: 2 x detachable TNC (1 x Main and 1 x Rx Diversity)
LED Indicators	7 LEDs: Power, Tx/Rx Data Traffic, 5 x Signal Strength
Operating Temperature	Normal Operating Temperature: -25°C ~+60°C , Extended Operating Temperature: -25°C ~+75°C (with Performance Deviations),
Power input	DC-in Port: 8 ~ 28V PoE (IEEE 802.3af): 48V DC AC/DC Power Adapter: 100-240V AC to 12V DC/1.5A
Power Consumption	Standby Input Current: 110mA @ 12V DC 3G Active Current: 300mA @ 12V DC Maximum Input Current: 560mA @ 12V DC
Dimensions & Weight	Telstra Outdoor Gateway (NTC-30WT): 255mm X 240mm X 80mm / 1750g Mounting Bracket: 290mm X 110mm X 12mm / 410g Antennas: length = 180mm; diameter = 20mm / 60g
Regulatory Compliancy	A-Tick (Australia), CE (Europe), FCC (USA), RoHS, Emark, IP67 Rating

Table 34 - Technical Specifications for the Telstra Outdoor Gateway

The following table lists the hardware specifications of the Indoor Access Point.

MODEL	INDOOR ACCESS POINT
Connectivity	4 x 10/100Mbps LAN port
LED Indicators	WPS/LAN Ports 1-4/WiFi/Power
Wireless Security	WEP/WPA/WPA-PSK/WPA2/WPA2-PSK
Wireless Frequency	2.4GHz and 5GHz
Wireless Standard	IEEE 802.11n. Backwards compatible with IEEE 802.11b/g/a
Antennas	2 x 3 internal WiFi antennas, 1 x external WiFi antenna
Power Input	DC Input Voltage 12V/1.5A
Operating Temperature	0-40°C, Humidity: 10%-90% non-condensing
Dimensions & Weight	133 mm (L) x 190 mm (H) x 34 mm (W) / 322g (with antenna attached)
Regulatory Compliance	C-Tick

Table 35 - Technical Specifications for the Indoor Access Point

Captive Power Terminal Block

The following table displays the pin outs for the Locking Power Block on the PoE Injector.



Figure 87 - Locking Power Terminal Block

PIN	SIGNAL	DESCRIPTION
1	V+	Voltage+
2	GND	Ground
3	V-	Voltage-

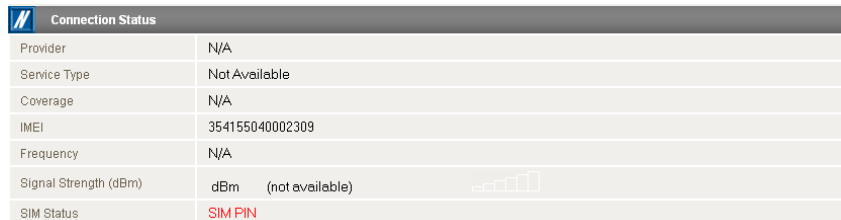
Table 36 - Locking Power Block Pin Outs

Additional Product Information

Unlocking the SIM

If the SIM card is locked you will need to unlock it with the appropriate PIN code.

You can find out if the SIM is locked by viewing the SIM Status at the bottom of the Status page.





Connection Status	
Provider	N/A
Service Type	Not Available
Coverage	N/A
IMEI	354155040002309
Frequency	N/A
Signal Strength (dBm)	dBm (not available) 
SIM Status	SIM PIN

Figure 88 - Checking the SIM PIN Status

If the SIM Status is “SIM PIN” as shown above then the SIM card requires a PIN code to be entered before use. To enter the PIN code:

- d) Click on the “Internet Settings” menu at the top of the page and then the “SIM Security” item from the WWAN (3G) menu item on the right.



Internet Settings > WWAN (3G) > SIM Security

PIN Settings	
SIM Status	SIM PIN
Number of Retries Remaining	
PIN	<input type="text"/>
Confirm PIN	<input type="text"/>
Remember PIN: Disabled	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
PIN Protection: Enabled	Disable PIN ▼

Figure 89 - Entering the SIM PIN

- e) Enter the PIN code in the “PIN” field and then enter it again in the “Confirm PIN” field to confirm the PIN code.



Please note: You can also select to “Remember PIN” so that entering the PIN code each time the SIM is inserted is not required. Alternatively you can also disable SIM PIN protection by selecting to “Disable PIN” from the “PIN Protection” drop down menu.

- f) Click the “Save” button.

Appendix A: Tables

Table 1 - Document Revision History	2
Table 2 - LED Indicators	7
Table 3 - Device Dimensions	9
Table 4 - Mounting Bracket Dimensions	9
Table 5 - Antenna Dimensions	10
Table 6 - Bottom Mounted Interfaces	11
Table 7 - Top Mounted Integrated Interfaces	11
Table 8 - LAN Management Default Settings	12
Table 9 - WiFi Default Settings	12
Table 10 - System Management Accounts	12
Table 11 - Status page items	17
Table 12 - Status Page - LAN Details	18
Table 13 - Status Page - PPPoE Details	18
Table 14 - Status Page - PPTP Details	18
Table 15 - Status Page - IPSec Details	18
Table 16: Advanced Status Settings	20
Table 17 - NAT Configuration Items	31
Table 18 - IPsec Configuration Items	35
Table 19 - OpenVPN Configuration Items	37
Table 20 - PPTP Configuration Items	39
Table 21 - GRE VPN Settings	40
Table 22 - Wireless Configuration - Basic Configuration Items	42
Table 23 - Wireless Settings - Advanced Configuration Items	45
Table 24 - SNMP Configuration Options	50
Table 25 - SMS Setup Configuration Items	51
Table 26 - SMS Diagnostic Command Syntax	58
Table 27 - List of Valid SMS Diagnostic Commands	59
Table 28 - List of SMS Diagnostics Variables	59
Table 29 - SMS Diagnostics - Example Commands	60
Table 30 - System Log Detail Levels	61
Table 31 - Administration Configuration Items	66
Table 32 - System Configuration Items	67
Table 33 - System - TR-069 Details	68
Table 34 - Technical Specifications for the Telstra Outdoor Gateway	76
Table 35 - Technical Specifications for the Indoor Access Point	77
Table 36 - Locking Power Block Pin Outs	77

Legal and Regulatory

Intellectual Property Rights

All intellectual property rights (including copyright and trade mark rights) subsisting in, relating to or arising out of this Manual are owned by and vest in NetComm Wireless Limited (ACN 002490486) (**NetComm Wireless Limited**) (or its licensors). This Manual does not transfer any right, title or interest in NetComm Wireless Limited (or its licensors) intellectual property rights to you.

You are permitted to use this Manual for the sole purpose of using the NetComm Wireless product to which it relates. Otherwise no part of this Manual 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 Wireless Limited.

NetComm is a trademark of NetComm. All other trademarks are acknowledged to be the property of their respective owners.

Customer Information

The Australian Communications & Media Authority (**ACMA**) requires you to be aware of the following information and warnings:

1. This unit may be connected to the Telecommunication Network through a line cord which meets the requirements of the AS/CA S008-2011 Standard.
2. This equipment has been tested and found to comply with the Standards for C-Tick and or A-Tick as set by the ACMA. These standards are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio noise and, if not installed and used in accordance with the instructions detailed within this manual, may cause interference to radio communications. However, there is no guarantee that interference will not occur with the installation of this product in your home or office. If this equipment does cause some degree of interference to radio or television reception, which can be determined by turning the equipment off and on, we encourage the user to try to correct the interference by one or more of the following measures:
 - i. Change the direction or relocate the receiving antenna.
 - ii. Increase the separation between this equipment and the receiver.
 - iii. Connect the equipment to an alternate power outlet on a different power circuit from that to which the receiver/TV is connected.
 - iv. Consult an experienced radio/TV technician for help.
3. The power supply that is provided with this unit is only intended for use with this product. Do not use this power supply with any other product or do not use any other power supply that is not approved for use with this product by NetComm. Failure to do so may cause damage to this product, fire or result in personal injury.

Consumer Protection Laws

Australian and New Zealand consumer law in certain circumstances implies mandatory guarantees, conditions and warranties which cannot be excluded by NetComm and legislation of another country's Government may have a similar effect (together these are the **Consumer Protection Laws**). Any warranty or representation provided by NetComm is in addition to, and not in replacement of, your rights under such Consumer Protection Laws.

If you purchased our goods in Australia and you are a consumer, you are entitled to a replacement or refund for a major failure and for compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure. If you purchased our goods in New Zealand and are a consumer you will also be entitled to similar statutory guarantees.

Product Warranty

All NetComm products have a standard one (1) year warranty from date of purchase, however, some products have an extended warranty option (refer to packaging and the warranty card) (each a **Product Warranty**). To be eligible for the extended warranty option you must supply the requested warranty information to NetComm Wireless Limited within 30 days of the original purchase by registering online via the NetComm Wireless Limited web site at www.netcommwireless.com. For all Product Warranty claims you will require proof of purchase. All Product Warranties are in addition to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see [Section 3](#) above).

Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see [Section 3](#) above), the Product Warranty is granted on the following conditions:

1. the Product Warranty extends to the original purchaser (you / the customer) and is not transferable;
2. the Product Warranty shall not apply to software programs, batteries, power supplies, cables or other accessories supplied in or with the product;
3. the customer complies with all of the terms of any relevant agreement with NetComm Wireless Limited and any other reasonable requirements of NetComm Wireless Limited including producing such evidence of purchase as NetComm Wireless Limited may require;
4. the cost of transporting the product to and from NetComm Wireless Limited's nominated premises is your responsibility;
5. NetComm Wireless Limited does not have any liability or responsibility under the Product Warranty where any cost, loss, injury or damage of any kind, whether direct, indirect, consequential, incidental or otherwise arises out of events beyond NetComm Wireless Limited's reasonable control. This includes but is not limited to: acts of God, war, riot, embargoes, acts of civil or military authorities, fire, floods, electricity outages, lightning, power surges, or shortages of materials or labour; and the customer is responsible for the security of their computer and network at all times. Security features may be disabled within the factory default settings. NetComm Wireless Limited recommends that you enable these features to enhance your security.

Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see [Section 3](#) above), the Product Warranty is automatically voided if:

1. you, or someone else, use the product, or attempt to use it, other than as specified by NetComm Wireless Limited;
2. the fault or defect in your product is the result of a voltage surge subjected to the product either by the way of power supply or communication line, whether caused by thunderstorm activity or any other cause(s);
3. the fault is the result of accidental damage or damage in transit, including but not limited to liquid spillage;
4. your product has been used for any purposes other than that for which it is sold, or in any way other than in strict accordance with the user manual supplied;
5. your product has been repaired or modified or attempted to be repaired or modified, other than by a qualified person at a service centre authorised by NetComm Wireless Limited; or
6. the serial number has been defaced or altered in any way or if the serial number plate has been removed.

Limitation of Liability

This clause does not apply to New Zealand consumers.

Subject to your rights and remedies under applicable Consumer Protection Laws which cannot be excluded (see [Section 3](#) above), NetComm Wireless Limited accepts no liability or responsibility, for consequences arising from the use of this product. NetComm Wireless Limited reserves the right to change the specifications and operating details of this product without notice.

If any law implies a guarantee, condition or warranty in respect of goods or services supplied, and NetComm Wireless Limited's liability for breach of that condition or warranty may not be excluded but may be limited, then subject to your rights and remedies under any applicable Consumer Protection Laws which cannot be excluded, NetComm Wireless Limited's liability for any breach of that guarantee, condition or warranty is limited to: (i) in the case of a supply of goods, NetComm Wireless Limited doing any one or more of the following: replacing the goods or supplying equivalent goods; repairing the goods; paying the cost of replacing the goods or of acquiring equivalent goods; or paying the cost of having the goods repaired; or (ii) in the case of a supply of services, NetComm Wireless Limited doing either or both of the following: supplying the services again; or paying the cost of having the services supplied again.

To the extent NetComm is unable to limit its liability as set out above, NetComm Wireless Limited limits its liability to the extent such liability is lawfully able to be limited.

Contact

Address: NETCOMM WIRELESS LIMITED

PO Box 1200, Lane Cove NSW 2066 Australia

Phone: +61(0)2 9424 2070 Fax: +61(0)2 9424 2010

Website: www.netcommwireless.com

Email: sales@netcommwireless.com , Technical.Support@netcommwireless.com