

# Dual Band WiFi Data and VoIP Gateway NF3ADV



USER GUIDE

## 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.

## Save Our Environment

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:

NetComm Wireless Limited NF3ADV

DOCUMENT VERSION	DATE
1.0 - Initial document release	29/06/2012

*Table 1 - Document Revision History*

# Table of Contents

<b>Overview</b> .....	<b>4</b>
Introduction .....	4
Target Users.....	4
Prerequisites.....	4
Notation .....	4
<b>Product Introduction</b> .....	<b>5</b>
Product Overview .....	5
Package Contents .....	5
Product Features.....	5
<b>Physical Dimensions and Indicators</b> .....	<b>6</b>
LED Indicators.....	6
Integrated Interfaces .....	7
NF3ADV Default Settings .....	8
<b>Safety and Product Care</b> .....	<b>9</b>
<b>Transport and Handling</b> .....	<b>9</b>
<b>Installation and Configuration of the NF3ADV</b> .....	<b>10</b>
Placement of your NF3ADV.....	10
Avoid obstacles and interference.....	10
Cordless Phones .....	10
Choose the “Quietest” Channel for your Wireless Network .....	10
Hardware installation.....	11
Connecting via an Ethernet cable .....	11
Connecting wirelessly .....	11
First Time Simple Configuration Wizard.....	12
<b>Management Console Login Procedure</b> .....	<b>17</b>
Basic View - Status.....	18
<b>Advanced Features</b> .....	<b>23</b>
Network Setup .....	24
Forwarding Rules.....	35
Security Settings.....	37
Advanced Settings.....	41
Toolbox.....	51
<b>VOIP/NAS View</b> .....	<b>57</b>
Phone Setting .....	58
SIP Settings.....	64
Other VoIP Settings .....	68
<b>NAS Settings</b> .....	<b>70</b>
Disk Utility .....	70
File Sharing.....	70
Access Control.....	71
iTunes Server .....	72
Download Assistant.....	73
Web HDD.....	75
<b>Additional Product Information</b> .....	<b>76</b>
Establishing a wireless connection.....	76
Troubleshooting.....	77
Using the indicator lights (LEDs) to Diagnose Problems.....	77
Using the NF3ADV to make and receive telephone calls.....	78
Accessing voicemail.....	78
Call Feature Codes .....	79
<b>Technical Data</b> .....	<b>81</b>
Electrical Specifications.....	81
Environmental Specifications / Tolerances .....	81
<b>FAQ</b> .....	<b>82</b>
<b>Appendix A: Tables</b> .....	<b>84</b>
<b>Appendix B: Samba Server</b> .....	<b>86</b>
<b>Legal &amp; Regulatory Information</b> .....	<b>87</b>
Intellectual Property Rights.....	87
Customer Information .....	87
Consumer Protection Laws.....	87
Product Warranty .....	88
Limitation of Liability.....	88
<b>Contact</b> .....	<b>89</b>

## Overview

### Introduction

This manual provides information related to the installation, operation, and utilization of the NF3ADV.

### Target Users

The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

### Prerequisites

Before continuing with the installation of your NF3ADV, please confirm that you comply with the minimum system requirements below.

- Computer with Windows, Macintosh, or Linux-based operating systems with a working Ethernet adapter with TCP/IP Protocol installed.
- A Web Browser such as Internet Explorer, Netscape Navigator, Mozilla Firefox, Opera, Safari etc.
- Wireless Computer System Requirements:
  - Computer with a working 802.11b, 802.11g or 802.11n wireless adapter.

### Notation

The following symbols are utilised in this user manual:



The following note requires attention.



The following note provides a warning.



The following note provides relevant information.

# Product Introduction

## Product Overview

- ADSL 2/2+ Integrated Modem.
- 1 x 10/100/1000 Gigabit WAN port.
- 3 x 10/100/1000 Gigabit LAN Ethernet port.
- 1 x FXS Voice port (circuit-switched).
- 1 x FXO port for PSTN calling.
- IPv6 Support – Dual Stack IPv6, Static IPv6, DHCPv6, PPPoE, 6 to 4, IPv6 to IPv4 tunnel
- 802.11n up to 900Mbps Wireless<sup>1</sup> (Backward compatible with 802.11b/g).
- 2.4GHz and 5.0GHz Concurrent WiFi
- DECT base station with DECT association button.
- 2 x USB host ports supporting 3G/4G USB, mass storage file sharing.
- WiFi Protected Setup (WPS) for simple setup of your wireless network.
- VPN pass-through (PPTP, L2TP, IPSec).
- Browser based interface for configuration and management.
- Multiple power saving features – time of day LED dimming, WiFi power save features, green/power down functions.

1. Speeds are dependent on network coverage. See your Mobile Broadband (MBB) provider coverage maps for more details. The total number of WiFi users can also affect data speeds. The maximum wireless signal rate and coverage values are derived from IEEE Standard 802.11g and 802.11n specifications. The actual wireless speed and coverage are dependent on network and environmental conditions including but not limited to the volume of network traffic, building materials and construction/layout.

## Package Contents

The NF3ADV package consists of:

- 1 x NF3ADV Dual Band WiFi Data and VoIP Gateway
- 1 x 12VDC~2.0A Power Adapter.
- 1 x RJ-45 Ethernet LAN Cable.
- 1 x RJ-11 phone Cable.
- Quick Setup Guide.
- Wireless Security Card.

If any of these items are missing or damaged, please contact NetComm customer care.

## Product Features

Congratulations on your purchase of a NetComm NF3ADV Wireless Router. This router is compliant with 802.11n WiFi while still being compatible with 802.11g & 802.11b devices. The NF3ADV is not only a Wireless Access Point, but features a built-in ADSL modem, has a Gigabit speed WAN port and doubles as a 3-port full-duplex Ethernet Switch, connecting your wired-Ethernet devices together at incredible speeds.

With speeds of up to 900Mbps, the NetComm NF3ADV Wireless Router uses Dual Band WiFi, advanced MIMO (Multi-Input, Multi-Output) technology to transmit multiple streams of data in a single wireless channel giving you seamless access to multimedia content under Robust RF signal travels farther, eliminates dead spots and extends network range. For data protection and privacy, the NF3ADV encodes all wireless transmissions with WEP, WPA, or WPA2 encryption.

With inbuilt DHCP Server & powerful SPI firewall the NF3ADV protects your computers against intruders and most known Internet attacks but provides safe VPN pass-through. With incredible speed and QoS function of 802.11n, NF3ADV is ideal for media-centric applications like streaming video, gaming, and VoIP telephony allowing you to run multiple media-intense data streams through the network at the same time, with no degradation in performance.

The NetComm NF3ADV creates a secure WiFi network router incorporating a WLAN 802.11b/g/n access point, which can provide Internet access for up to 15 users and simultaneous phone service using your VoIP Service Provider's network. It incorporates a DECT base station for use with cordless phones, three 10/100/1000 Mbps Ethernet ports, one 10/100/1000 Mbps Ethernet WAN port, an FXO port for PSTN calling and an FXS phone port for making and receiving telephone calls. It features the latest security options such as WPA and WPA2 data encryption, SPI (Stateful Packet Inspection) Firewall and VPN pass through.

# Physical Dimensions and Indicators

## LED Indicators

The NF3ADV has been designed to be placed on a desktop. All of the cables exit from the rear for better organization. The display is visible on the front of the NF3ADV to provide you with information about network activity and the device status. See below for an explanation of each of the indicator lights.

LED INDICATOR	ICON	STATE	DESCRIPTION
Power		Blue Off	Powered Off
		Blue Flashing	Powering Up.
		Blue On	Powered On
Ethernet 1 - 3		Blue On	Ethernet Link Up
		Blue Blinking	Traffic on Ethernet Port
		Blue Off	Ethernet Link Down
WiFi		Blue On	WiFi Enabled
		Blue Flashing	WPS PBC connection window open
		Blue Off	WiFi Disabled
DECT		Blue On	Device is in Register Mode
		Blue Off	Device is not in Register Mode
		Blue flashing	Device is in Paging Mode
VoIP		Blue On	VoIP Settings are Registered
		Blue Off	VoIP Settings have not Registered
		Blue Flashing	VoIP Connecting
ADSL Sync		Blue On	ADSL is in Sync
		Blue Off	ADSL is not in Sync
		Blue Flashing	ADSL is Training
WWW/ Internet Connection		Blue On	Connected via ADSL
		Blue Flashing	ADSL Data Traffic
		Red On	Connected via 3G
		Red Flashing	3G Data Traffic
		Purple On	Connected via WAN Ethernet port (e.g. PPPoE up / DHCP lease received / Static IP Configured )
		Purple Flashing	WAN Port Data Traffic
		Off	Internet connection not Configured
WAN		Blue On	Ethernet Link Up
		Blue Off	Ethernet Link Down
3G/4G Signal		Blue On	Connected to 3G/4G Network
		Blue Off	3G/4G not configured (no dongle connected)
		Blue Flashing	Connecting

Table 2 - LED Indicators

## Integrated Interfaces

The following integrated interfaces are available on the rear of the NF3ADV:



Figure 1: Rear Panel

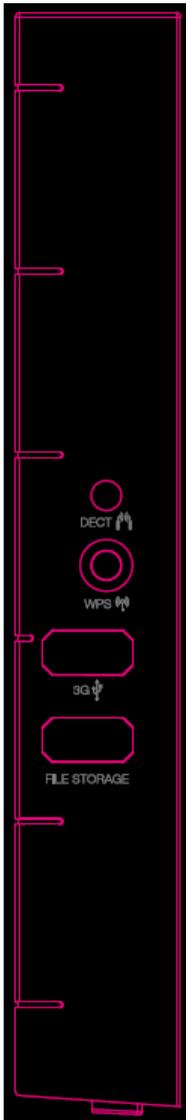


Figure 2: Side Panel

INTERFACE	FUNCTION
DSL	The ADSL port for xDSL connectivity.
Line	The RJ-11 port provides a connection to your PSTN phone line for PSTN pass through calling.
Phone	The RJ-11 phone port provides a connection to a standard analogue telephone.
WiFi	Wireless Distribution System push-button-connect function. <ul style="list-style-type: none"> <li>• Hold this button in for 1-3 seconds to enable the 2.4 Ghz WDS function</li> <li>• Hold this button in for 4-6 seconds to enable the 5.0 Ghz WDS function.</li> </ul>
Reset	Hold this button down for over 10 seconds to reset the router to factory default settings.
WAN	The WAN Ethernet port for a Fixed Line (ADSL/Cable/Satellite) connection to the internet.
LAN 3	A LAN Port for wired Ethernet clients (Computers, Laptops, etc.).
LAN 2	A LAN Port for wired Ethernet clients (Computers, Laptops, etc.).
LAN 1	A LAN Port for wired Ethernet clients (Computers, Laptops, etc.).
On/Off	This switch can be used to power up or down the NF3ADV.
Power	The power connector designed for use with a DC 12V 3.0A Power Adapter
DECT	Press the button to connect a cordless phone and use the NF3ADV as a DECT base station.
WPS	WiFi Protected System (WPS) push-button-connect function <ul style="list-style-type: none"> <li>• Hold this button in for 1-3 seconds before releasing to trigger the 2.4 GHz WPS.</li> <li>• Hold this button in for 4-6 seconds before releasing to trigger the 5 GHz WPS.</li> </ul>
3G	Insert a 3G/4G USB dongle into this port for Mobile Broadband connectivity.
File Storage	Insert a USB Hard Disk Drive and the NF3ADV on board file server will make files on the drive available across all networked connections.

Table 3: Rear and Side Panel Interface Connectors

## NF3ADV Default Settings

The following tables list the default settings for the NF3ADV.

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

Table 4 - LAN Management Default Settings

WAN (INTERNET)	
WAN mode:	DHCP

Table 5 - WAN Port Default Settings

WIRELESS (WIFI)	
SSID:	(Refer to the included wireless security card)
Security:	WPA-PSK/WPA2-PSK
Security Key:	(Refer to the included wireless security card)

Table 6 - WiFi Default Settings



For security purposes, each NF3ADV comes with a unique SSID that varies by a 4 digit number at the end. e.g. SSID: "NetComm Wireless XXXX"

NF3ADV WEB INTERFACE ACCESS	
Username:	admin
Password:	admin

Table 7 - Web Interface Default Settings

# Safety and Product Care

With reference to unpacking, installation, use and maintenance of your electronic device, the following basic guidelines are recommended:

- To avoid fire or shock hazard do not use or install this product near water. For example, near a bathtub, kitchen sink, laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).
- Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on or mistreat the cord.
- To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are unobstructed.



## WARNING

Disconnect the power line from the device before servicing.

# Transport and Handling

When transporting the NF3ADV, it is recommended to return the product in the original packaging. This ensures the product will not be damaged.



In the event the product needs to be returned, ensure it is securely packaged with appropriate padding to prevent damage during courier transport.

# Installation and Configuration of the NF3ADV

## Placement of your NF3ADV

The wireless connection between your NF3ADV and your WiFi devices will be stronger the closer your connected devices are to your NF3ADV. Your wireless connection and performance will degrade as the distance between your NF3ADV and connected devices increases. This may or may not be directly noticeable, and is greatly affected by the individual installation environment.

If you have concerns about your network's performance that might be related to range or obstruction factors, try moving the computer to a position between three to five meters from the NF3ADV in order to see if distance is the problem.



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

If you experience difficulties connecting wirelessly between your WiFi Devices and your NF3ADV, please try the following steps:

- If the wireless network adapters of your wireless devices support 5GHz bandwidth try changing from the 2.4GHz wireless band to the 5GHz band on the router.
- In multi-storey homes, place the NF3ADV on a floor that is as close to the centre of the home as possible. This may mean placing the NF3ADV on an upper floor.
- Try not to place the NF3ADV near a cordless telephone that operates at the same radio frequency as the NF3ADV (2.4GHz).

## Avoid obstacles and interference

Avoid placing your NF3ADV near devices that may emit radio “noise”, such as microwave ovens. Dense objects that can inhibit wireless communication include:

- Refrigerators.
- Washers and/or dryers.
- Metal cabinets.
- Large aquariums.
- Metallic-based, UV-tinted windows.
- If your wireless signal seems weak in some spots, make sure that objects such as those listed above are not blocking the signal's path (between your wireless devices and the NF3ADV).

## Cordless Phones

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

- Try moving cordless phones away from your NF3ADV and your wireless-enabled computers.
- Unplug and remove the battery from any cordless phone that operates on the 2.4GHz band (check manufacturer's information). If this fixes the problem, your phone may be interfering with the NF3ADV.
- If your phone supports channel selection, change the channel on the phone to the farthest channel from your wireless network. For example, change the phone to channel 1 and move your NF3ADV to channel 11. See your phone's user manual for detailed instructions.
- If necessary, consider switching to a 900MHz or 5GHz cordless phone.

## Choose the “Quietest” Channel for your Wireless Network

In locations where homes or offices are close together, such as apartment buildings or office complexes, there may be wireless networks nearby that can conflict with your wireless network. Use the Site Survey capabilities found in the Wireless Utility of your wireless adapter to locate any other wireless networks that are available (see your wireless adapter's user manual), and switch your Router and computers to a channel as far away from other networks as possible. Alternately try using a different wireless band.

Experiment with more than one of the available channels and bands, in order to find the clearest connection and avoid interference from neighbouring cordless phones or other wireless devices.

## Hardware installation

1. Insert an Ethernet LAN cable from the WAN port of the NF3ADV to a LAN port on your modem/switch/hub.
2. For VoIP functionality, connect a standard analogue telephone to the FXS port using the RJ-11 Cable provided.
3. For PSTN pass-through connect an RJ-11 cable from any wall jack to the FXO Line port of the NF3ADV.
4. Connect the power adapter to the Power socket on the back of the NF3ADV.
5. Plug the power adapter into the wall socket and switch on the power.
6. Wait approximately 60 seconds for the NF3ADV to power up.

## Connecting via an Ethernet cable

1. Connect the Ethernet cable provided to the port marked LAN at the back of the NF3ADV.
2. Connect the other end of the yellow Ethernet cable to your computer.
3. Wait approximately 30 seconds for the connection to establish.
4. Open your Web browser and type `http://192.168.1.1` into the address bar and press enter.
5. Enter "admin" (without quotations) for both the Username and Password and click on the Login button.
6. Follow the steps of the start-up wizard to set up your NF3ADV.
7. After the setup process is completed, you will be connected to the Internet.

## Connecting wirelessly

1. Ensure WiFi is enabled on your device (computer/laptop/Smartphone).
2. Scan for wireless networks in your area and connect to the network name that matches the Wireless network name found on the Wireless Security Card (included in the box).



Figure 3 - Included Security Card



Please note: For security purposes, each NF3ADV has a unique SSID (such as NetComm Wireless XXXX) and Wireless Security Key. The included Wireless Security Card lists these fields instead of the xxxxx's as shown in the screenshot above.

3. When prompted for your wireless security settings, enter the wireless security key listed on your Wireless Security Card.
4. Wait approximately 30 seconds for the connection to be established.
5. Open your Web browser and type `http://192.168.1.1` into the address bar and press enter.
6. Enter "admin" (without quotations) as both the Username and Password and press the Login button.
7. Follow the steps to set up your NF3ADV.
8. After the setup process is completed, you will be connected to the Internet.
9. To connect additional devices via WiFi, repeat steps 1 through 4.

## First Time Simple Configuration Wizard

When you log in to your NF3ADV for the first time, you will be presented with the NF3ADV “Set-up Wizard” as shown in the screenshot below. This wizard can be skipped by clicking on the link “No thanks, take me to the Basic Interface”, shown on the screenshot below. You can re-run the Setup Wizard again anytime after first use by selecting the “Startup Wizard” option under the “Toolbox” menu in the Advanced View of the management console.

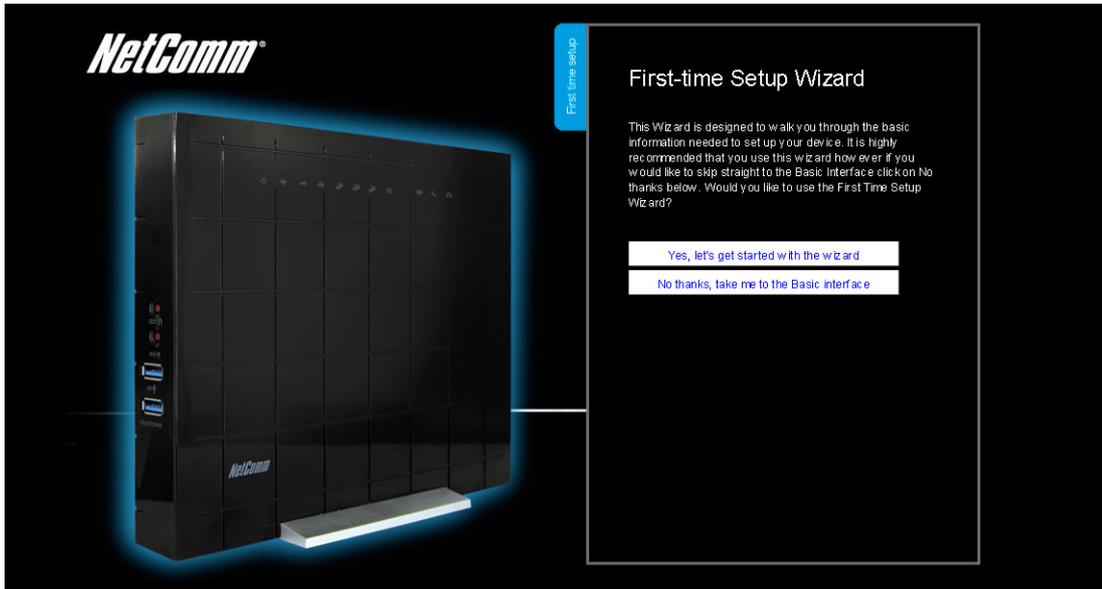


Figure 2: Setup Wizard - Start

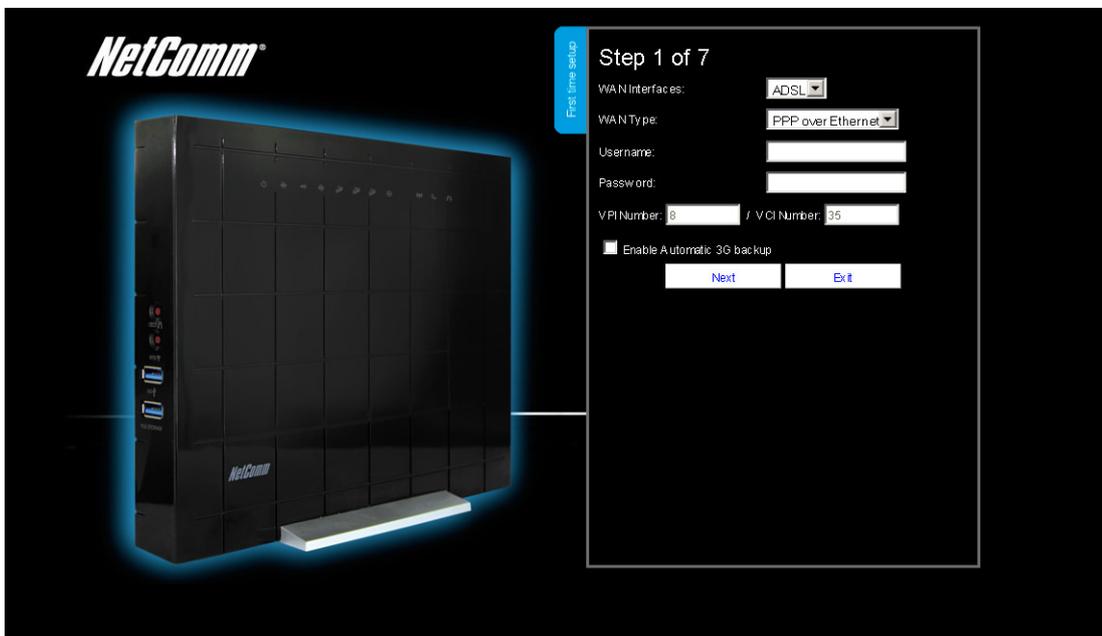


Figure 4: Setup Wizard Step 1 - WAN Interface - ADSL

Select your WAN interface – WAN, ADSL or 3G. The example above shows the WAN Interface as an ADSL connection. Press the Next button to continue the setup wizard.

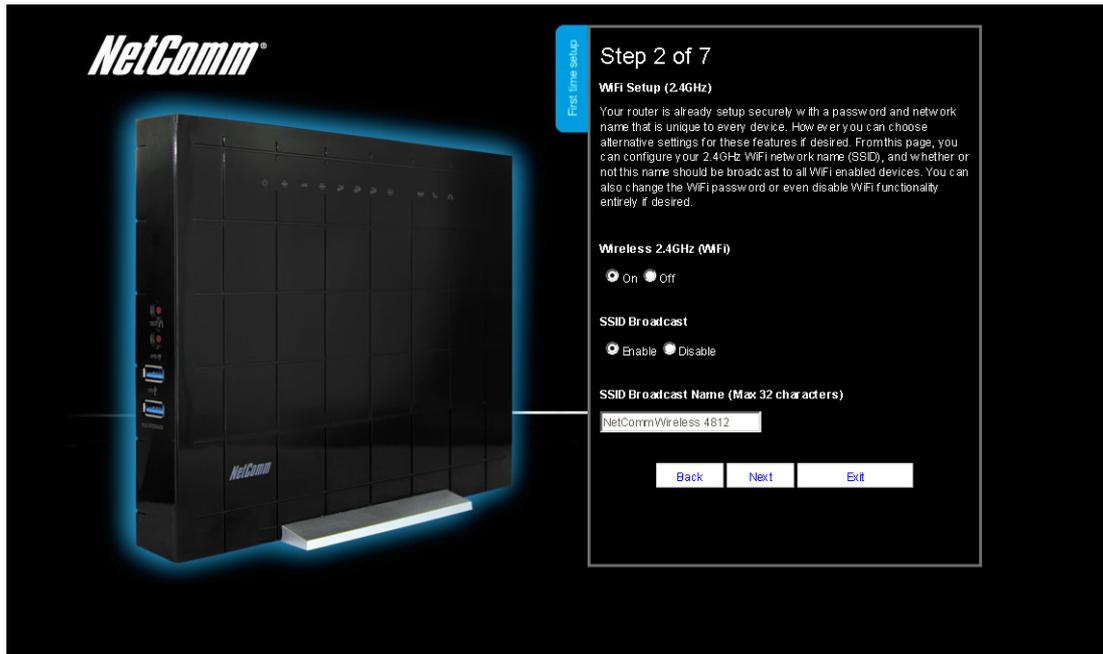


Figure 5: Setup Wizard Step 2 - 2.4 GHz WiFi Setup

This page allows you to customize the 2.4GHz wireless settings of the NF3ADV.

### Wireless (WiFi):

WiFi is set to “On” by default. Changing this option to “Off” will turn off the wireless feature and you will not be able to connect to your NF3ADV via 2.4 GHz WiFi.

### SSID Broadcast:

Select ‘Disable’ to hide the SSID of the NF3ADV. If disabled, other people will not be able scan and detect your NF3ADV’s SSID.

### SSID Broadcast Name (Max 32 Characters):

The SSID (Service Set Identifier) is the name of your wireless network. Use a unique name to identify your wireless network so that you can easily connect from your wireless clients. This field is case sensitive and can be up to 32 characters. You should change the default SSID for added security.

Click “Next” to continue.

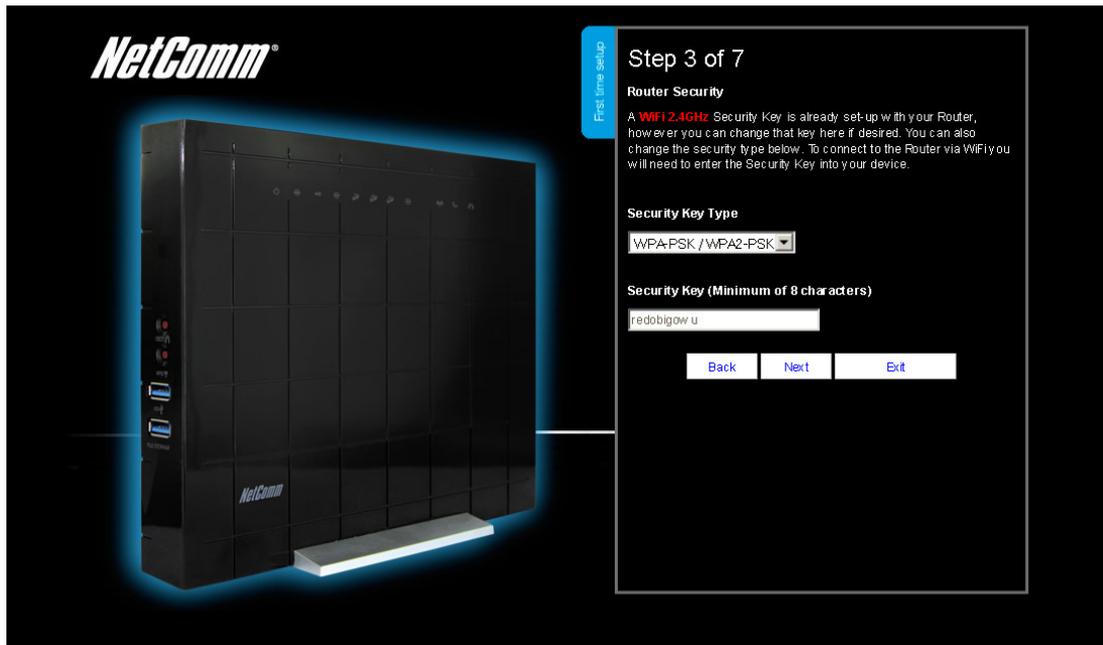


Figure 6 - Setup Wizard Step 3 – 2.4 GHz WiFi Security Settings

This page allows you to configure the 2.4 GHz WiFi security settings for the NF3ADV. Setting a strong wireless security level (such as WPA-PSK - AES) can prevent unauthorized access to your wireless network. Please enter the Security Key that you wish to use, or leave this field unchanged to use the default Security Key. Click “Next” to continue.



Figure 7: Setup Wizard Step 4 - 5.0 GHz WiFi Setup

This page allows you to customize the 5.0 GHz wireless setting of the NF3ADV.

#### Wireless (WiFi):

WiFi is set to “On” by default. Changing this option to “Off” will turn off the wireless feature and you will not be able to connect to your NF3ADV via 5.0 GHz WiFi.

#### SSID Broadcast:

Select ‘Disable’ to hide the SSID of the NF3ADV. If disabled, other people will not be able scan and detect your NF3ADV’s SSID.

## SSID Broadcast Name (Max 32 Characters):

The SSID (Service Set Identifier) is the name of your wireless network. Use a unique name to identify your wireless network so that you can easily connect from your wireless clients. This field is case sensitive and can be up to 32 characters. You should change the default SSID for added security.

Click "Next" to continue.

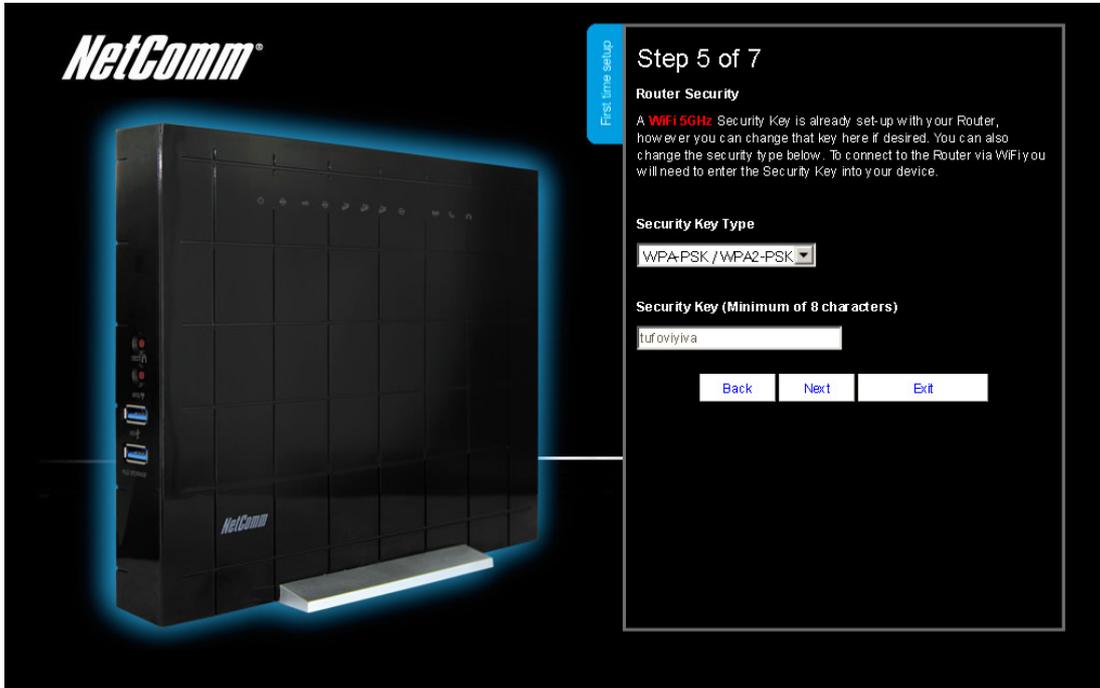


Figure 7: Setup Wizard Step 5 - 5.0 GHz Wireless Security Setup

This page allows you to configure the 5.0 GHz WiFi security settings for the NF3ADV. Setting a strong wireless security level (such as WPA-PSK - AES) can prevent unauthorized access to your wireless network. Please enter the Security Key that you wish to use, or leave this field unchanged to use the default Security Key. Click "Next" to continue.

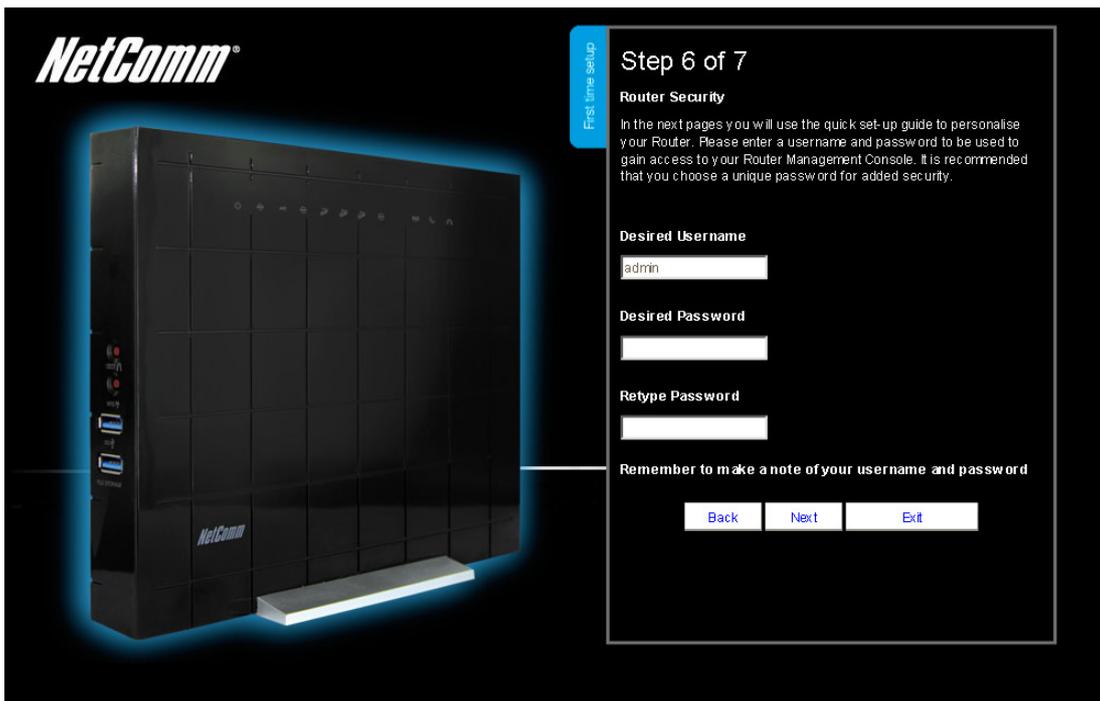


Figure 8: Setup Wizard Step 6 - Router Security Settings

# NF3ADV – Dual Band WiFi Data and VoIP Gateway

In Step 6 of the NF3ADV Setup Wizard the administration password for the router can be set to prevent unauthorized access to the router management page. Enter the Desired Username and Desired Password, retyping the desired Password in the Retype Password field to confirm the new password. Click Next to continue the setup wizard.



Figure 9: Setup Wizard Step 7 - Summary

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

After clicking Finish, the NF3ADV will save your configuration and reboot. Please wait as this process takes about 2 minutes. You will be guided back to the management console once the process is complete.

# Management Console Login Procedure

After first time setup, the management console will be password protected to prevent unauthorized access to the configuration settings of your NetComm NF3ADV.

To log in to the management console, view the status and make changes to your NF3ADV, please follow the steps below:

1. Open your 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. Use the default username and password "admin" if these details have not been customized. Click "Login" to continue.



Please note: If you forget the username and password you selected during the NF3ADV set-up process, holding the reset button for over 10 seconds will restart the unit with the original settings (username: admin / password: admin).



Please note: In the event that your Internet connection becomes unavailable and no fail over service has been configured, the NetComm NF3ADV Management console page will display when attempting to browse to an Internet site.

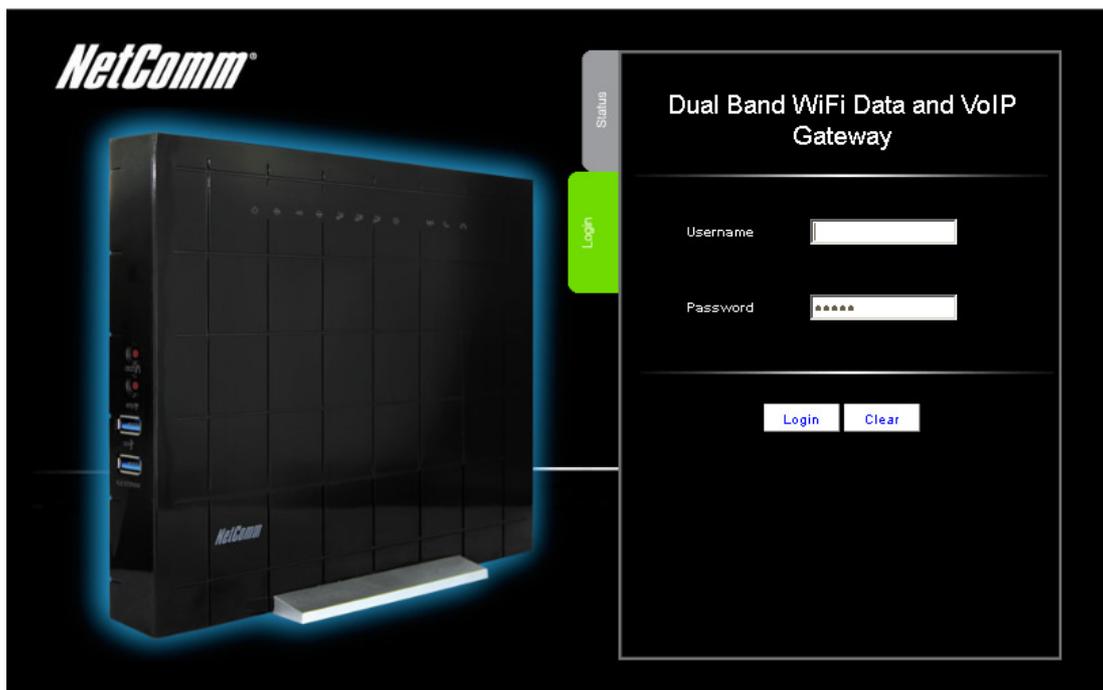


Figure 10: Basic View – Login

## Basic View - Status

The basic status page provides basic system related information. It can be accessed by clicking on the “Switch to Basic view” button from the top of the status page.

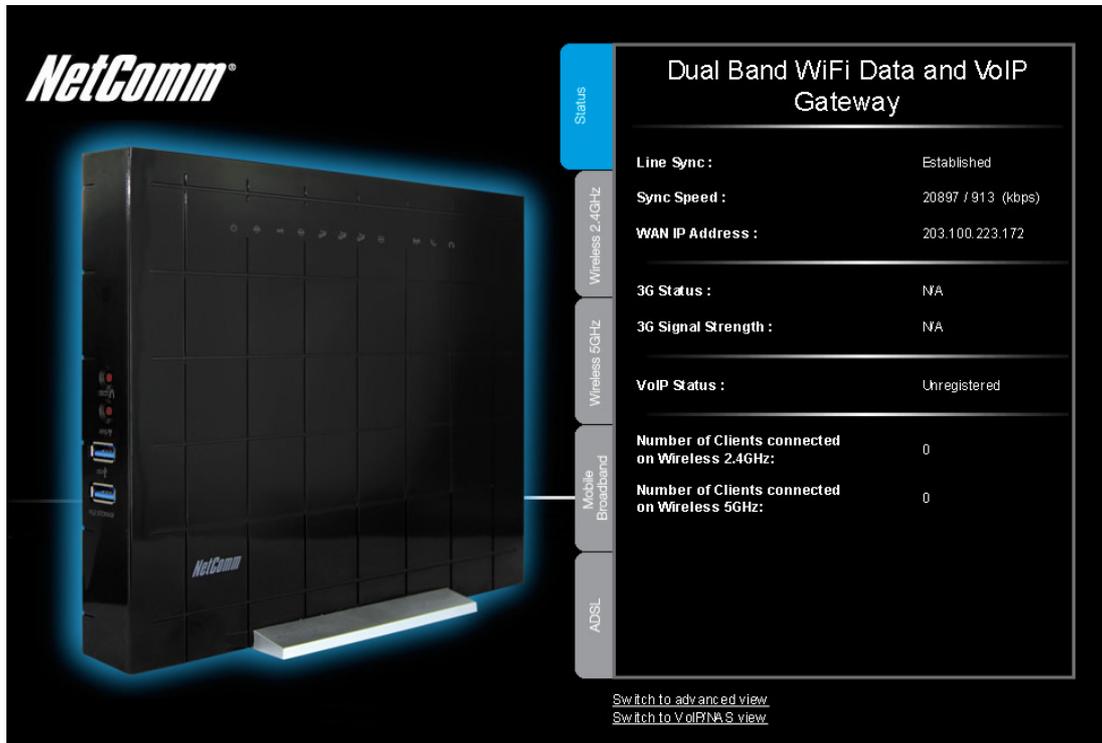


Figure 11: Basic View – Status

The status page shows the current primary Internet connection, WAN/LAN status, MBB connection status, current Signal Strength (dBm), VoIP Status and number of wireless clients currently connected.

OPTION	DEFINITION
Line Sync	The line sync status of the current ADSL WAN type set on the NF3ADV.
Sync Speed	The current downstream and upstream speed of the ADSL WAN type.
WAN IP Address	The current IP Address that has been assigned to the WAN interface.
3G Status	The current status of the 3G connectivity is listed here.
3G Signal Strength	The current signal strength of the MBB (Mobile Broadband) service connection.
VoIP Status	An indication as to whether the SIP settings have registered successfully.
Number of Clients connected on Wireless 2.4 Ghz	This field indicates how many wireless devices are connected on the NF3ADV's 2.4 GHz wireless frequency.
Number of Clients connected on Wireless 5 GHz	This field indicates how many wireless devices are connected on the NF3ADV's 5 GHz wireless frequency.

Table 8: Basic View - Status Settings

## Basic View - 2.4 GHz Wireless



Figure 12: Basic View - Wireless 2.4GHz

This page allows you to configure basic 2.4 GHz WiFi settings for this device such as enabling/disabling the 2.4 GHz WiFi functionality, changing the 2.4 GHz Wireless Network Name (SSID) or the 2.4 GHz Wireless Security key. If you make any changes to the settings, click the “Save and apply changes” button to make these changes active.

OPTION	DEFINITION
Wireless (WiFi)	Changing this option to Off will turn off the WiFi feature on the NF3ADV and you will not be able to connect to your NF3ADV wirelessly.
SSID Broadcast	Select whether the NF3ADV will broadcast the SSID (Network Name) for any wireless device in range to detect.
WiFi network Name	The SSID (Service Set Identifier) is the name of your wireless network. Use a unique name to identify your wireless device so that you can easily connect to it from your wireless clients. This field is case sensitive and can be up to 32 characters long.
Security Key:	Enter your chosen Wireless Security key here. The default WPA-PSK key is printed on the wireless security card and on the Product ID on the bottom of the NF3ADV. Please note that whilst the key can be customized on this page, the key will revert to the default if the NF3ADV is reset to factory default settings.

Table 9: Basic View - 2.4GHz Wireless Settings

## Basic View - 5.0 GHz Wireless



Figure 13: Basic View - 5.0 GHz Wireless

This page allows you to configure basic 5.0 GHz WiFi settings for this device such as enabling/disabling the 5.0 GHz WiFi functionality, changing the 5.0 GHz Wireless Network Name (SSID) or the 5.0 GHz Wireless Security key. If you make any changes to the settings, click the “Save and apply changes” button to make these changes active.

OPTION	DEFINITION
Wireless (WiFi) ON/ OFF:	Changing this option to Off will turn off the WiFi feature on the NF3ADV and you will not be able to connect to your NF3ADV wirelessly.
SSID Broadcast	Select whether the NF3ADV will broadcast the SSID (Network Name) for any wireless device in range to detect.
WiFi Network Name (SSID):	The SSID (Service Set Identifier) is the name of your wireless network. Use a unique name to identify your wireless device so that you can easily connect to it from your wireless clients. This field is case sensitive and can be up to 32 characters long.
Security key:	Enter your chosen Wireless Security key here. The default WPA-PSK key is printed on the wireless security card and on the Product ID on the bottom of the NF3ADV. Please note that whilst the key can be customized on this page, the key will revert to the default if the NF3ADV is reset to factory default settings.

Table 10: Basic View - 5.0 GHz Wireless Settings

## Basic View - Mobile Broadband

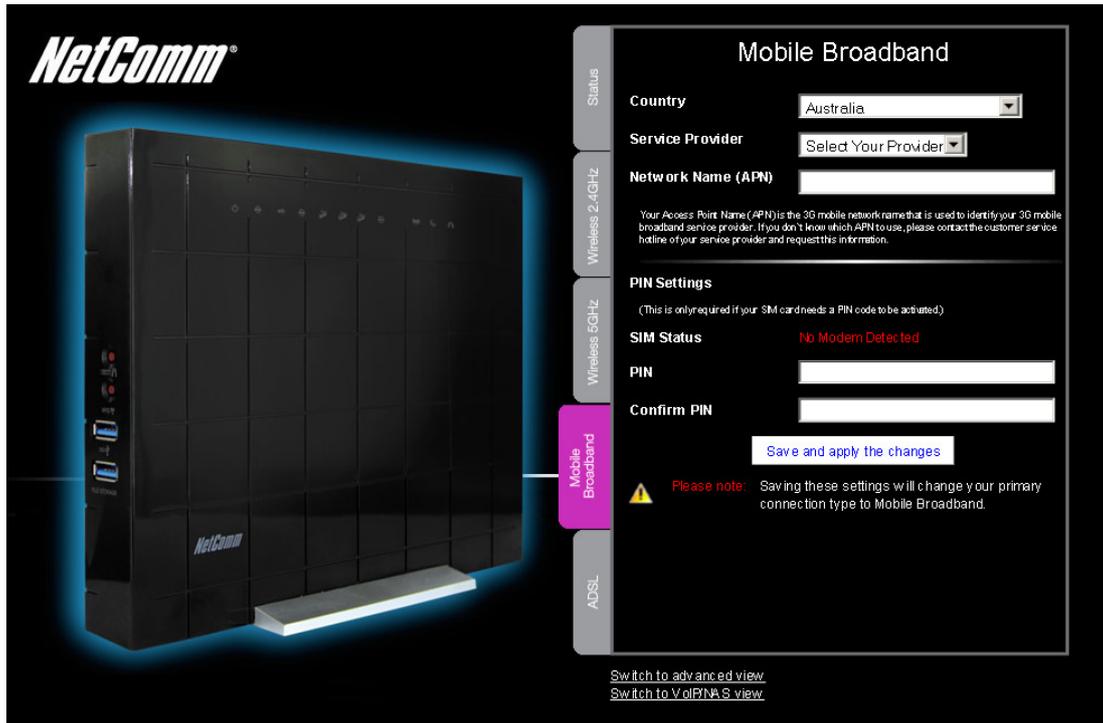


Figure 14: Basic View - Mobile Broadband

This page allows you to configure the MBB (Mobile Broadband) WAN connection settings for the NF3ADV.



Please note: Entering and saving Mobile Broadband settings on this page will change the primary (WAN) connection type to Mobile Broadband. To set the Mobile Broadband connection as a back-up connection to Ethernet or ADSL WAN select the “Enable Automatic 3G Backup” option in Step 1 of the Startup Wizard.

OPTION	DEFINITION
Country	Select the country that your MBB (Mobile Broadband) provider is situated in.
Service Provider	Select the MBB provider for your 3G/4G dongle and/or SIM card.
Network Name (APN)	Enter the Access Point Name (APN) of your MBB provider.
SIM Status	This field indicates whether the SIM card has been detected and is functioning correctly.
PIN	If the SIM card requires a PIN to operate enter the PIN into this field.
Confirm PIN	If the SIM card requires a PIN to operate enter the PIN into this field also.

Table 11: Basic View - Mobile Broadband Settings

## Basic View - ADSL

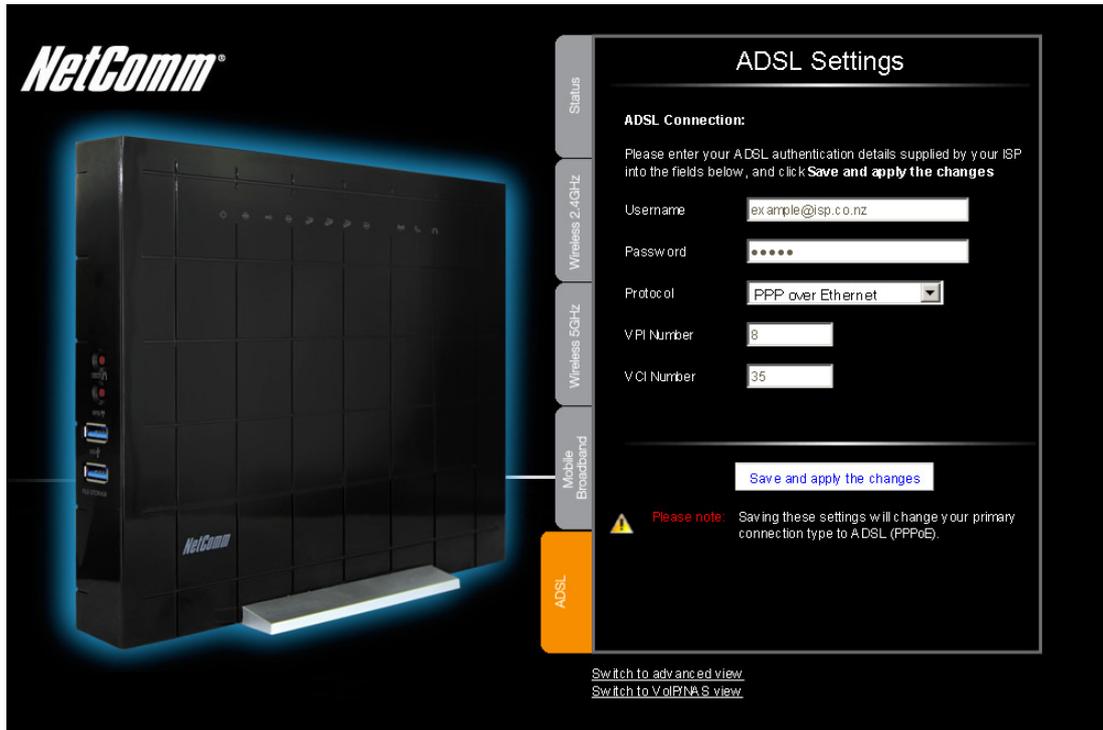


Figure 15: Basic View - ADSL

The ADSL page allows a network administrator to configure ADSL as the primary WAN connection type.



Please note: Entering and saving ADSL settings on this page will change the primary (WAN) connection type to ADSL.

OPTION	DEFINITION
User Name	Enter the broadband user name supplied to you by your Internet Service Provider (ISP).
Password	Enter the broadband password supplied to you by your Internet Service Provider (ISP).
Protocol	Select the protocol used for your fixed line ADSL connection.
VPI Number	Enter the VPI (Virtual Path Identifier). For most users in Australia the VPI will be 8. For most users in New Zealand the VPI will be 0.
VCI Number	Enter the VCI (Virtual Channel Identifier). For most users in Australia the VCI will be 35. For most users in new Zealand the VCI will be 100.

Table 12: Basic View - ADSL Settings

# Advanced Features

The basic configuration interface is intended to provide access to all the settings that most people will want to use on their NetComm NF3ADV. There are advanced settings available if desired which are accessible by viewing the advanced settings pages. Click on the “Switch to Advanced View” option to view and configure the advanced features of your NF3ADV.

## Status

The status page provides system related information and is displayed when you login to the NetComm NF3ADV management console and switch to the Advanced View. By default, the status page will show IPv4 System Status, IPv6 System Status, Wireless 2.4 GHz Status, Wireless 5.0 GHz Status, VoIP Status and Statistics Information.

In addition there are buttons that can be pressed to view ADSL Modem Status, View System Logs, Clients List, NAT Status and to Refresh the status page.

Status   [▶ Network Setup](#)   [▶ Forwarding Rules](#)   [▶ Security Settings](#)   [▶ Advanced Settings](#)   [▶ Toolbox](#)

IPv4 System Status		
Item	WAN Status	Sidenote
IP Address	203.100.223.172	PPPoA
Subnet Mask	255.255.255.255	
Gateway	202.180.81.32	
Domain Name Server	202.180.64.10 , 202.180.64.11	
Connection Time	02:59:09	<a href="#">Disconnect</a>
ADSL Connection (Down Stream/Up Stream)	20897 / 913 (kbps)	

IPv6 System Status		
Item	WAN Status	Sidenote
WAN Link Local Address		Dynamic IPv6
Global IPv6 Address	/64	
LAN IPv6 Link Local Address	fe80::260:64ff:fe59:17eb	
Link Status		Connecting...

Wireless 2.4GHz Status		
Item	WLAN Status	Sidenote
Wireless 2.4GHz mode	Enable	(B/G/N Mixed)
SSID	NetCommWireless 4812	
Channel	Auto	
Security	WPA-PSK / WPA2-PSK	(TKIP/AES)

Wireless 5GHz Status		
Item	WLAN Status	Sidenote
Wireless 5GHz mode	Enable	(A/N Mixed)
SSID	NetCommWireless 9370	
Channel	Auto	
Security	WPA-PSK / WPA2-PSK	(TKIP/AES)

VoIP Status		
Item	Status	Sidenote
Phone	Unregistered	
DECT 1	Unregistered	
DECT 2	Unregistered	

Statistics Information		
Statistics of WAN	Inbound	Outbound
Octets	3881251	810557
Unicast packets	6703	6525
Multicast packets	0	0

[ADSL Modem Status](#)   [View Log...](#)   [Clients List...](#)   [NAT Status...](#)   [Refresh](#)

Device Time: Wed, 13 Jun 2012 14:13:20 +1000

Figure 16: Advanced View - Status

## Network Setup

### Network Setup - Ethernet WAN

This page allows you to setup the Ethernet WAN (Wide Area Network) interface of the NF3ADV router. This is for an internet connection through the WAN port of the router instead of using a Mobile Broadband (MBB) WWAN connection.

Item	Setting
WAN Interface	Ethernet WAN
WAN Type	PPP over Ethernet
Automatic 3G Backup	<input type="checkbox"/> Enable Remote Host for keep alive: <input type="text"/>
IPv6 Dualstack	<input type="checkbox"/> Enable
Username	<input type="text"/>
Password	<input type="text"/>
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
Connection Control	Connect-on-Demand
Maximum Idle Time	600 seconds
Service Name	<input type="text"/> (optional)
Assigned IP Address	<input type="text"/> (optional)
MTU	0 (0 is auto)
NAT	<input checked="" type="checkbox"/> Enable
Multicast	Disable
IGMP Snooping	<input type="checkbox"/> Enable
VLAN TAG	<input type="checkbox"/> Enable <input type="text"/> (range: 1~4094)

Save Undo

Figure 17: Advanced - Network Setup - Ethernet WAN

OPTION	DEFINITION
WAN Interface	Enter the WAN interface required. Options are Ethernet WAN, ADSL or Wireless WAN (3G/4G Mobile Broadband).
WAN Type	Enter the WAN type of the WAN interface; Options include Dynamic IP Address (default), Static IP address, PPP over Ethernet (PPPoE), PPTP and L2TP.
Automatic 3G Backup	Select the Enable checkbox to enable automatic MBB backup of the Ethernet WAN interface. Enter an IP address or domain name into the Remote Host for Keep Alive field for the router to periodically check the status of the connection.
IPv6 Dualstack	Select this option if an IPv6 TCP stack is required along with the IPv4 TCP stack.
User Name	If you have a modem attached to the WAN port of the router and it is in bridge mode enter your broadband username as supplied by your Internet Service Provider here.
Password	If you have a modem attached to the WAN port of the router and it is in bridge mode enter your broadband password as supplied by your Internet Service Provider here.
Primary DNS	Enter the preferred primary DNS address here if different to the automatically assigned primary DNS address.
Secondary DNS	Enter the secondary DNS address here if different to the automatically assigned secondary DNS address.
Connection Control	Select the means to connect via the Ethernet WAN. Options include Connect On-demand, Auto-reconnect (always on) or connecting manually.
Maximum Idle Time	Enter the time seconds before the Ethernet WAN connection will time out if the connection becomes idle.
Service Name	Enter the service name for the Ethernet WAN connection. This is an optional field.
Assigned IP Address	Enter an assigned IP address if your Internet Service Provider has assigned a static IP address for your connection. This field is optional.
MTU	Enter the Maximum Transmission Unit (MTU), the largest data packet size that the router can transmit. The default MTU size is 0 (for automatic).

NAT	Select this option if NAT (Network Address Translation) is required. In most cases NAT will be required. Therefore NAT is enabled by default.
Multicast	Select whether which version IGMP (Internet Group management Protocol) is required for your WAN connection. In most cases the Auto connection will suffice.
IGMP Snooping	Select whether you wish IGMP enabled on the WAN connection. IGMP snooping is the process of listening to (IGMP) network traffic. IGMP snooping, as implied by the name, allows the router to listen in on the IGMP conversation between computers and the routers. By listening to these conversations the router maintains a map of which links need which IP multicast streams.
VLAN TAG	Select this item to tag the data from this Ethernet WAN connection for the purpose of creating a Virtual LAN. This can be used for setting up separate logical networks for data separation and security purposes.

Table 13: Advanced - Network Setup - Ethernet WAN setting

## Network Setup - Wireless WAN

This page allows you to setup the Wireless WAN (Wide Area Network) interface of the NF3ADV router. This is for an internet connection through a 3G or 4G USB dongle connected to the USB port of the router instead of using an ADSL or Ethernet WAN connection. The Wireless WAN connection can also be configured as a backup or failover connection to either an ADSL or Ethernet WAN connection. To do this select the Automatic 3G Backup option when configuring the ADSL or Ethernet WAN connection type.

▶ Status
▶ Network Setup
▶ Forwarding Rules
▶ Security Settings
▶ Advanced Settings
▶ Toolbox

Item	Setting
WAN Interface	Wireless WAN ▼
Country	Australia ▼
Service Provider	Select Your Provider ▼
APN	<input type="text"/>
PIN Code	<input type="text"/> (optional)
Dial Number	<input type="text"/>
Username	<input type="text"/> (optional)
Password	<input type="text"/> (optional)
Authentication Type	<input checked="" type="radio"/> Auto <input type="radio"/> PAP <input type="radio"/> CHAP
Primary DNS	<input type="text"/> (optional)
Secondary DNS	<input type="text"/> (optional)
Connection Control	Auto Reconnect (always-on) ▼
Allowed Connection Time	<input checked="" type="radio"/> Always <input type="radio"/> By Schedule
MTU	1500 (0 is auto)
Keep Alive	<input checked="" type="radio"/> Disable <input type="radio"/> LCP Echo Request Interval <input type="text" value="10"/> seconds Max. Failure Time <input type="text" value="3"/> times <input type="radio"/> Ping Remote Host Host IP <input type="text"/> Interval <input type="text" value="60"/> seconds
Multicast	Disable ▼
IGMP Snooping	<input type="checkbox"/> Enable

Figure 18: Advanced - Network Setup - Wireless WAN

OPTION	DEFINITION
WAN Interface	Enter the WAN interface required. Options are Ethernet WAN, ADSL or Wireless WAN (Mobile Broadband).
Country	Enter the Country where the Mobile Broadband (MBB) Internet Provider is operating. This field affected such settings as dial and ring tones, and the prefixes that need to be entered before making a call.
Service Provider	Enter your MBB (Mobile Broadband) provider here. Enter the Access Point Name that your MBB (Mobile Broadband) provider has recommended you use.
APN	Enter the Access Point Name that your MBB (Mobile Broadband) provider has recommended you use.
PIN Code	If your SIM card requires a PIN code, enter it in here.
Dial Number	The string value that needs to be dialed to make a mobile broadband (MBB) connection. *99# is the default string.
Username	If your Mobile Broadband connection requires a username enter it in here.
Password	If your Mobile Broadband connection requires a password enter it in here.
Authentication Type	Select the authentication type used by the MBB connection. If you are unsure what this is select the default Auto option.
Primary DNS	Enter the Primary Domain Name Server address to be used by the MBB connection. This is an optional field.
Secondary DNS	Enter the Secondary Domain Name Server address to be used by the MBB connection. This is an optional field.
Connection Control	Select from the connection control options: Connect on Demand – Connect when a MBB WAN interface is attempting to make a connection. Auto Reconnect (always on) – Assume the MBB connection is always on and try to connect if the MBB connection is dropped. Manually – Connect the Wireless WAN interface only when a manual attempt is made.
MTU	Enter the Maximum Transmission Unit, the size of the largest packet that a network protocol can transmit.
Keep Alive	A mechanism for testing whether the MBB connection is active or not by periodically pinging a remote host.
Multicast	Select whether which version IGMP (Internet Group management Protocol) is required for your WAN connection. In most cases the Auto connection will suffice.
IGMP Snooping	Select whether you wish IGMP enabled on the WAN connection. IGMP snooping is the process of listening to (IGMP) network traffic. IGMP snooping, as implied by the name, allows the router to listen in on the IGMP conversation between computers and the routers. By listening to these conversations the router maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them.

Table 14: Advanced - Network Setup - Wireless WAN

## Network Setup – ADSL WAN

This page allows you to setup the WAN (Wide Area Network) interface of the NF3ADV router through a fixed line ADSL connection. Ensure you have plugged an RJ11 cable from the ADSL port of your ADSL splitter and have a solid DSL light lit on the front of the router before configuring this interface type.

Item	Setting
WAN Interface	ADSL   PVC0   <input checked="" type="radio"/> Active <input type="radio"/> Inactive   <a href="#">PVCs Summary</a>
WAN Type	PPP over Ethernet
Automatic 3G Backup	<input type="checkbox"/> Enable Remote Host for keep alive: <input type="text"/>
IPv6 Dualstack	<input type="checkbox"/> Enable
Username	<input type="text" value="example@isp.com.au"/>
Password	<input type="password" value="....."/>
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
Connection Control	Auto Reconnect (always-on)
Service Name	<input type="text"/> (optional)
Assigned IP Address	<input type="text"/> (optional)
MTU	<input type="text" value="0"/> (0 is auto)
NAT	<input checked="" type="checkbox"/> Enable
Data Encapsulation	LLC
VPI Number	<input type="text" value="0"/> (range: 0-255)
VCI Number	<input type="text" value="100"/> (range: 1-65535)
Schedule type	UBR
Multicast	Disable
IGMP Snooping	<input type="checkbox"/> Enable
VLAN TAG	<input type="checkbox"/> Enable   <input type="text" value="1"/> (range: 1-4094)
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

Figure 19: Advanced - Network Setup - ADSL

If the DSL LED is not solid try an isolation test by unplugging all devices plugged into the phone sockets on the premises. In this way you may identify a device – be it a faulty cable, phone, ADSL filter, monitored alarm or multimedia device that may be causing interference with the broadband signal. You may require ADSL filters on all phone jacks before the DSL signal becomes usable.

OPTION	DEFINITION
WAN Interface	Enter the WAN interface required. Options are Ethernet WAN, ADSL or Wireless WAN (3G/4G Mobile Broadband).
WAN Type	Enter the WAN type of the WAN interface; Options include Ethernet over ATM (RFC 1483 Bridged) with NAT, IP over ATM (RFC 1483 Routed), PPP over Ethernet (PPPoE), PPP over ATM or RFC 1483 Bridged.
Automatic 3G Backup	Select this option if you wish to use a Mobile Broadband connection as a failover (back up) connection to the ADSL connection. Enter a public IP address for the router to ping to so that the router can monitor whether the ADSL connection is still alive.
IPv6 Dualstack	Select this option if an IPv6 TCP stack is required along with the IPv4 TCP stack.
Username	If your Mobile Broadband connection requires a username enter it in here.
Password	If your Mobile Broadband connection requires a password enter it in here.
Primary DNS	Enter the Primary Domain Name Server address to be used by the MBB connection. This is an optional field.
Secondary DNS	Enter the Secondary Domain Name Server address to be used by the MBB connection. This is an optional field.
Connection Control	Select from the connection control options: Connect on Demand – Connect when a MBB WAN interface is attempting to make a connection. Auto Reconnect (always on) – Assume the MBB connection is always on and try to connect if the MBB connection is dropped. Manually – Connect the Wireless WAN interface only when a manual attempt is made.
Service Name	Enter the service name for the ADSL connection. This is an optional field.
Assigned IP Address	Enter an assigned IP address if your Internet Service Provider has assigned a static IP address for your connection. This field is optional.
MTU	Enter the Maximum Transmission Unit, the size of the largest packet that a network protocol can transmit.
NAT	Select this option to enable NAT.
Data Encapsulation	Select the data encapsulation method. Options include LLC and VC-Mux.
VPI	Enter the Virtual path Identifier (VPI) number. For most users in Australia the VPI will be 8. For most users in new Zealand the VPI will be 0.
VCI	Enter the Virtual Channel Identifier (VCI). For most users in Australia the VCI will be 35. For most users in New Zealand the VCI will be 100.
Schedule Type	Select the schedule type. Options include UBR, CBR, VBR and GFR
Multicast	Select whether which version IGMP (Internet Group management Protocol) is required for your WAN connection. In most cases the Auto connection will suffice.
IGMP Snooping	Select whether you wish IGMP enabled on the WAN connection. IGMP snooping is the process of listening to (IGMP) network traffic. IGMP snooping, as implied by the name, allows the router to listen in on the IGMP conversation between computers and the routers. By listening to these conversations the router maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them.
VLAN TAG	Select this item to tag the data from this ADSL connection for the purpose of creating a Virtual LAN. This can be used for setting up separate logical networks for data separation and security purposes.

Table 15: Advanced - Network Setup - ADSL WAN

# DHCP

DHCP is the means used so that all computers connected to the router can be assigned an IP address dynamically. Generally it is recommended to leave DHCP as default (enabled) unless instructed otherwise by your Internet Service Provider.

Item	Setting
DHCP Server	DHCP <input type="radio"/> Disable <input checked="" type="radio"/> Enable
LAN IP Address	192.168.1.1
Subnet Mask	255.255.255.0
IP Pool Starting Address	100
IP Pool Ending Address	200
Lease Time	86400 Seconds
Domain Name	
Primary DNS	
Secondary DNS	
Primary WINS	
Secondary WINS	
Gateway	(optional)

Figure 20: Advanced - Network Setup – DHCP

OPTION	DEFINITION
DHCP Server	The option to disable or enable the DHCP function.
LAN IP Address	The LAN IP address of the DHCP server/router.
Subnet Mask	The subnet mask used by the DHCP server.
IP Pool Starting Address	The starting IP address for the DHCP pool, in the above example is 192.168.1.100
IP Pool Ending Address	The ending IP address for the DHCP pool, in the above example is 192.168.1.200
Lease Time	The time in seconds that an IP address is leased for.
Domain Name	The domain of the DHCP server.
Primary DNS	Enter the Primary Domain Name Server address used by the DHCP server.
Secondary DNS	Enter the Secondary Domain Name Server address used by the DHCP server.
Primary WINS	Enter the Primary WINS (Windows Internet Name Server) address used by the DHCP server.
Secondary WINS	Enter the Secondary WINS (Windows Internet Name Server) address used by the DHCP server.
Gateway	Enter the gateway address for the router. This field is optional.

Table 16: Advanced - Network Setup – DHCP

## Clients List

The clients list page provides a list of all the devices currently connected to the router using DHCP.

IP Address	Host Name	MAC Address	Type	Lease Time	Select
192.168.1.100	techsupport-laptop	00-0F-B0-FA-92-57	Wired	23:03:33	<input type="checkbox"/>

Figure 21: Advanced - Network Setup - DHCP - Clients List

ITEM	DEFINITION
IP Address	The current IP address of the connected device.
Host Name	The name of the device connected via DHCP.
MAC Address	A unique identifying code of 12 characters assigned to all networking devices.
Type	The type of connection - wired or wireless.
Lease Time	The amount of time remaining before the DHCP lease will need to be renewed.

Table 17: Advanced - network Setup - DHCP - Clients List Settings

## Fixed Mapping

This page allows an IP address to be reserved to one particular network interface device. Enter the MAC address and corresponding IP address you wish the device to use, enter a tick in the Enable checkbox and press the Save button.

DHCP clients: -- select one --
Copy to ID: --

ID	MAC Address	IP Address	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Figure 22: Advanced - Network Setup - DHCP - Fixed Mapping

## Wireless 2.4 GHz

This page allows the user to configure the 2.4 GHz wireless settings on the NetComm NF3ADV including the wireless security types, wireless encryption, WDS (Wireless Distributed System) settings and WPS (Wireless Protected Setup) setup.

Figure 23: Advanced - Network Setup - Wireless 2.4 GHz

OPTION	DEFINITION
Wireless Module (2.4GHz)	The option to disable or enable the 2.4 GHz Wireless function.
Network ID (SSID)	The SSID (Service Set Identifier) is the name of your wireless network. Use a unique name to identify your wireless device so that you can easily connect to it from your wireless clients. This field is case sensitive and can be up to 32 characters in length. It is recommended that the default SSID be changed for added security.
SSID Broadcast	Enabled by default, this field enables or disables the SSID broadcast, deciding whether the SSID will be hidden to all wireless clients, requiring a manual configuration to connect to the network or whether the SSID can be detected by wireless clients.
Channel	The wireless frequency used by the 2.4 GHz connection. Recommended channels to use include 1, 6 and 11.
Wireless Mode: There are 6 modes to select from:	
802.11b/g mixed mode:	Both 802.11b and 802.11g wireless devices can connect to the NetComm NF3ADV.
802.11b only:	Select this if all of your wireless clients use the 802.11b wireless protocol.
802.11g only:	Select this if all of your wireless clients use the 802.11g wireless protocol.
802.11n only:	Select this if all of your wireless clients use the 802.11n wireless protocol.
802.11g/n Mixed mode:	Select this if 802.11g and 802.11n wireless devices access your network.
802.11b/g/n Mixed mode:	Select this if 802.11b and 802.11g and 802.11n wireless devices access your network.
Authentication	This field allows you to select the authentication type of the wireless security for the 2.4 GHz wireless network connection.
802.1x	This field gives the option to enable or disable the 802.1x authentication protocol.
Encryption	With this field the encryption that the wireless security will use on the 2.4 GHz wireless network can be selected.
Pre-shared Key	The wireless security password for the 2.4 GHz wireless network connection.

Table 18: Advanced - Network Setup - Wireless 2.4 GHz Settings

## WDS Settings

WDS (Wireless Distribution System) is a system that enables the wireless interconnection of access points, and allows a wireless network to be expanded using multiple access points without using a wired backbone to link them. To successfully link each WDS Access Point needs to be set with the same channel, SSID, encryption type and encryption key. Please note that wireless clients will not be able to access the Access Points as the wireless functionality is used to create the wireless bridge. Network access for clients will only be possible through wired Ethernet cable.

Item	Setting
Wireless Bridging	<input checked="" type="radio"/> Enable <input 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"/>

Figure 24: Advanced - Network Setup - Wireless – WDS

Enter the MAC address of each Remote Access Point and press the Save button.

## WPS Setup

WiFi Protected Setup is a computer standard that offers a quick and easy alternative to setting up a wireless network. WPS can be configured using a push button method or by using a PIN code.

Item	Setting
WPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP PIN	58388297 <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

Figure 25: Advanced - Network Setup - Wireless - WPS

OPTION	DEFINITION
WPS	Enable or disable WPS with this field.
AP PIN	Set the Access Point PIN by pressing the Generate New PIN button.
Config Mode	Select from being an enrollee or registrar. In most cases the router will be the registrar.
Config Status	This field gives the current WPS status. Press either the Release button to release a configured WPS setting or the Set button to configure the current WPS settings
Config Method	Select whether WPS should use Push button or PIN Code mode for its configuration.
WPS Status	This field advises the current WPS status.

Table 19: Advanced - Network Setup - Wireless - WPS Settings

## Wireless 5.0 GHz

This page allows the user to configure the 5.0 GHz wireless settings on the NetComm NF3ADV including the wireless security types, wireless encryption, WDS (Wireless Distributed System) settings and WPS (Wireless Protected Setup) setup.

Figure 26: Advanced - Network Setup - 5.0 GHz Wireless

OPTION	DEFINITION
Wireless Module (5.0GHz)	The option to disable or enable the wireless 5.0 GHz function.
Network ID (SSID)	The SSID (Service Set Identifier) is the name of your wireless network. Use a unique name to identify your wireless device so that you can easily connect to it from your wireless clients. This field is case sensitive and can be up to 32 characters in length. It is recommended that the default SSID be changed for added security.
SSID Broadcast	Enabled by default, this field enables or disables the SSID broadcast, deciding whether the SSID will be hidden to all wireless clients, requiring a manual configuration to connect to the network or whether the SSID can be detected by wireless clients.
Channel	The wireless frequency used by the 5.0 GHz connection. Recommended channels to use include 1, 6 and 11.
Wireless Mode: There are 3 modes to select from using the 5 GHz frequency: A, N or mixed A/N mode	
802.11 A only:	Select this if all of your wireless clients use 802.11A wireless protocol.
802.11 N only:	Select this if all of your wireless clients are 802.11N wireless protocol.
802.11 A/N Mixed mode:	Select this if both 802.11A and 802.11N wireless devices access your network.
Authentication	This field allows you to select the authentication type of the wireless security for the 5.0 GHz wireless network connection.
802.1x	This field gives the option to enable or disable the 802.1x authentication protocol.
Encryption	With this field the encryption that the wireless security will use on the 5.0 GHz wireless network can be selected.
Pre-shared Key	The wireless security password for the 5.0 GHz wireless network connection.

Table 20: Advanced - Network Setup - 5.0 GHz Wireless Settings

## Change Password

This page allows you to change the administrator username and password to secure the NetComm NF3ADV management console against unauthorized access.

Item	Setting
Username	<input type="text" value="admin"/> (*Change this if you need to change Username.)
Old Password	<input type="password"/>
New Password	<input type="password"/>
Reconfirm	<input type="password"/>

Figure 27: Advanced - Network Setup - Change Password

# Forwarding Rules

The forwarding rules section deals with NAT traversal. Using the Virtual Server settings port forwarding can be configured. Special AP settings can be used to configure port triggering. In the Miscellaneous section a DMZ host can be configured and UPnP can be enabled or disabled.

## Virtual Server

The Virtual Server page allows you to direct incoming traffic from the Internet side (identified by Protocol and External port) to the internal server with a private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 20 entries can be configured. In addition a series of pre-configured commonly used ports can be selected for easy setup.

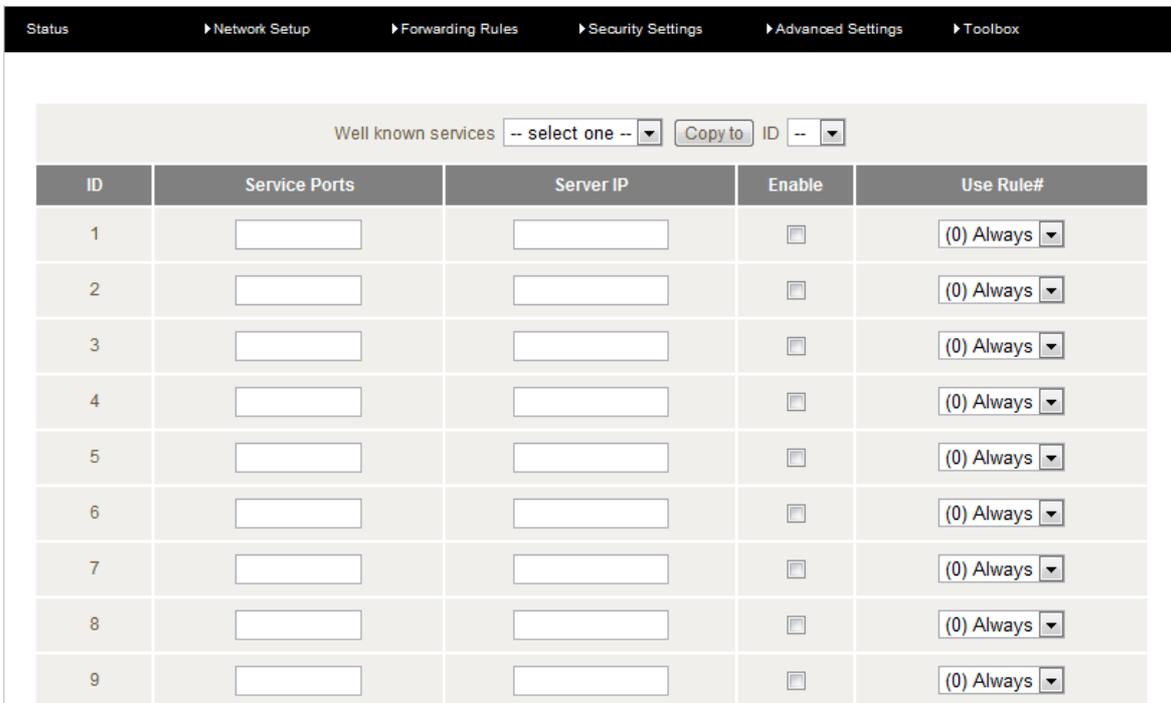


Figure 28: Advanced - Forwarding Rules - Virtual Server

OPTION	DEFINITION
Service Ports	Enter the port number or port range to be used with the Server IP address. For a port range entry use the format shown in the following example (81-90).
Server IP	Enter the local IP address of the device you wish to port forward to.
Enable	Select this option to enable the port forwarding rule.
Use Rule	Select when the port forwarding rule should be used. The default option is Always.

Table 21: Advanced - Forwarding Rules - Virtual Server Settings

## Port Triggering

Port triggering allows a client device connected to the router to dynamically and automatically forward a specific port back to itself. Port triggering opens an incoming port when your computer is using a specified outgoing port for specified traffic. A selection of common port triggering settings come preconfigured on the NF3ADV for easy setup and are listed in Popular Applications checkbox.

ID	Trigger	Incoming Ports	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Figure 29: Advanced - Forwarding Rules – Port Triggering

OPTION	DEFINITION
Trigger	Enter the outgoing trigger port be opened by a device connected to the router.
Incoming Ports	Enter the incoming port number or port ranges. For a port range use a dash (-) between the lower and upper range numbers; e.g. 5000-6000. Use a comma between multiple numbers.
Enable	Select this option to enable or disable the port triggering rule.

Table 22: Advanced - Forwarding Rules - Special AP settings

## Miscellaneous

The miscellaneous page gives the user the option of enabling or disabling UPnP protocol or the option to assign a device connected to the router as a DMZ host. A DMZ host is a host on the internal network that has all ports exposed to a WAN connection, except those ports otherwise forwarded.

Item	Setting	Enable
DMZ Mode	Multi Mode   PVC0	
IP Address of DMZ Host	<input type="text"/>	<input type="checkbox"/>
UPnP setting		<input checked="" type="checkbox"/>

Figure 30: Advanced - Forwarding Rules - Miscellaneous

# Security Settings

The security settings menu has such configuration options for the NetComm NF3ADV as Packet Filtering, Domain Filtering, URL Blocking, MAC Control and Remote Administration settings.

## Status

The Security Settings Status page provides an overview of the current IP filter and domain filter rules in place on the NF3ADV.

<a href="#">Status</a> <a href="#">▶ Network Setup</a> <a href="#">▶ Forwarding Rules</a> <a href="#">▶ Security Settings</a> <a href="#">▶ Advanced Settings</a> <a href="#">▶ Toolbox</a>			
Item		Status	
Outbound Filter		Disable	
Local Client	Only Deny Remote Host	Service	Working Time
Item		Status	
Inbound Filter		Disable	
Remote Host	Deny Remote Host to access	Service	Working Time
Item		Status	
Domain Filter		Disable	
Domain		Access	
All other Domains		Yes	
<input type="button" value="Refresh"/>			

Figure 31: Advanced - Security Settings - Status

## Packet Filtering

The inbound and outbound packet filtering function gives the network administrator the option of denying or allowing data packets to be transmitted through to the WAN interface when any of the specified rules are met. Conversely any other data packets not matching these rules will be denied or allowed access through the network as specified by the network administrator.

<a href="#">Status</a> <a href="#">▶ Network Setup</a> <a href="#">▶ Forwarding Rules</a> <a href="#">▶ Security Settings</a> <a href="#">▶ Advanced Settings</a> <a href="#">▶ Toolbox</a>				
Item		Setting		
Outbound Packet Filter		<input type="checkbox"/> Enable		
<input checked="" type="radio"/> Allow all data through the router except data that matches the specified rules. <input type="radio"/> Deny all data through the router except data that matches the specified rules.				
ID	Source IP	Destination IP : Ports	Enable	Use rule#
1	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
2	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
3	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
4	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
5	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
6	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
7	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
8	<input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="checkbox"/>	(0) Always ▾
<input type="button" value="First page"/> <input type="button" value="Previous page"/> <input type="button" value="Next page"/> <input type="button" value="Last page"/> <input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Inbound Filter..."/> <input type="button" value="MAC Level..."/>				

Figure 32: Advanced – Security Settings - Packet Filtering

OPTION	DEFINITION
Source IP	Enter the local source IP address where the packet originates from for an outgoing packet filter rule or is being sent to for an incoming packet filter rule.
Destination IP: Ports	Enter the WAN IP address and port number or range where the packet is directed to or from.
Enable	Select this option to make the packet filter rule active.
Use Rule#	Select when the rule is to be used. The default value is Always.

Table 23: Advanced Security Settings - Packet Filtering Settings

## Domain Filter

Domain Filtering can be used to monitor and or deny access to specified domain names.

Status
▶ Network Setup
▶ Forwarding Rules
▶ Security Settings
▶ Advanced Settings
▶ Toolbox

Item	Setting
Domain Filter	<input type="checkbox"/> Enable
Log DNS Query	<input type="checkbox"/> Enable
Privilege IP Addresses Range	From <input type="text"/> To <input type="text"/>

ID	Domain Suffix	Action	Enable
1	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
8	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
9	<input type="text"/>	<input type="checkbox"/> Drop <input type="checkbox"/> Log	<input type="checkbox"/>
10	* (all others)	<input type="checkbox"/> Drop <input type="checkbox"/> Log	-

Figure 33: Advanced – Security Settings - Domain Filter

OPTION	DEFINITION
Domain Filter	Select this option to enable Domain Filtering
Log DNS Query	Select this option to log DNS Queries for all specified domain names.
Privilege IP Addresses Range	Enter the range of IP addresses that will not be filtered.
Domain Suffix	Enter the domain name you wish to deny or have logged.
Drop	Select drop if you wish to deny access to the specified domain name
Log	Select Log if you wish to log any attempts to access the specified domain name.
Enable	Select this option to enable the domain filter rule.

Table 24: Advanced - Security Settings - Domain Filter settings

# MAC Control

The MAC filter function can be used to restrict access to the NF3ADV for both wired and wireless clients. Using Connection Control wired and wireless clients can connect to the router and either allow or deny any unspecified MAC addresses connection access. Using association control wireless clients can associate to the wireless LAN. All other unspecified wireless clients can be allowed or denied association rights.

Status   ▶ Network Setup   ▶ Forwarding Rules   ▶ Security Settings   ▶ Advanced Settings   ▶ Toolbox

Item	Setting		
MAC Address Control	<input type="checkbox"/> Enable		
<input type="checkbox"/> Connection control	Wireless and wired clients with <b>C</b> checked can connect to this device; and <span style="border: 1px solid black; padding: 0 2px;">allow</span> unspecified MAC addresses to connect.		
<input type="checkbox"/> Association control	Wireless clients with <b>A</b> checked can associate to the wireless LAN; and <span style="border: 1px solid black; padding: 0 2px;">allow</span> unspecified MAC addresses to associate.		
DHCP clients <span style="border: 1px solid black; padding: 0 10px;">- select one -</span> <span style="border: 1px solid black; padding: 0 2px;">Copy to</span> ID <span style="border: 1px solid black; padding: 0 5px;">-</span>			
ID	MAC Address	C	A
1	<input style="width: 100%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input style="width: 100%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input style="width: 100%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input style="width: 100%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input style="width: 100%;" type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
<span style="border: 1px solid black; padding: 2px 5px;">&lt;&lt; Previous</span> <span style="border: 1px solid black; padding: 2px 5px;">Next &gt;&gt;</span> <span style="border: 1px solid black; padding: 2px 5px;">Save</span> <span style="border: 1px solid black; padding: 2px 5px;">Undo</span>			

Figure 34: Advanced - Security Settings - MAC Control

## URL Blocking

The URL blocking function can deny access to specified URL addresses.

Item		Setting
URL Blocking		<input type="checkbox"/> Enable
ID	URL	Enable
1	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="checkbox"/>

Save Undo

Figure 35: Advanced - Security Settings - URL Blocking

## Miscellaneous

The Security Settings Miscellaneous section provides access to remote administration settings, administrator time out and DoS (Denial of Service) Attack Detection amongst other things.

Item	Setting	Enable
Administrator Time-out	300 seconds (0 to disable)	
Remote Administration	<input type="text"/> / <input type="text"/> : <input type="text"/>	<input type="checkbox"/>
Discard PING from WAN side		<input type="checkbox"/>
DoS Attack Detection		<input checked="" type="checkbox"/>
Keep WAN in stealth mode		<input checked="" type="checkbox"/>

Save Undo

Figure 36: Advanced - Security Settings - Miscellaneous

# Advanced Settings

The Advanced Settings menu has System log, Dynamic DNS, QoS (Quality of Service), SNMP (Simple Network Management Protocol), Routing, System Time, Scheduling, IPv6, TR-069 and VLAN options.

## Status

The status page shows the current status of the Advanced Settings on the NF3ADV.

Status				
Item	Status			
SystemTime	Wed, 13 Jun 2012 16:37:23 +1000			
Item	Status			
DDNS	Disable			
Provider	-			
Item	Status			
Dynamic Routing	Disable			
Static Routing	Disable			
Destination	Subnet Mask	Gateway	Hop	
Item	Status			
QoS Control	Disable			
Local Client	Remote Host	Service	Priority	Working Time

Refresh

Figure 37: Advanced - Advanced Settings – Status

## System Log

As well as viewing the system log entries locally the System Log page allows a network administrator to configure the router’s system log to be sent to a remote system log server or to be emailed to nominated email addresses of the administrator’s choice.

Item	Setting	Enable
IP address for syslog server	<input type="text"/>	<input type="checkbox"/>
Email address to send syslog to		<input type="checkbox"/>
• SMTP Server : port	<input type="text"/> : <input type="text"/>	
• SMTP Username	<input type="text"/>	
• SMTP Password	<input type="text"/>	
• E-mail addresses	<input type="text"/>	
• E-mail subject	<input type="text"/>	

Figure 38: Advanced - Advanced Settings - System Log

OPTION	DEFINITION
IP Address for Syslog Server	For sending the system log information to a remote server, enter the IP address of your System Log server.
Email Address to Send Syslog to	If you would like to send the system log details via email select this option and enter the appropriate details.
SMTP Server: port	Enter the name of the outgoing mail server to use in sending out the system log server.
SMTP Username	If a username is required for the outgoing mail server, enter it into this field.
SMTP Password	If a password is required for the outgoing mail server, enter it into this field.
Email Addressees	Enter the email addresses of where you wish the system log details to be sent to.
Email Subject	Enter a Subject for the System Log Email.
View Log	View the System Log entries locally.
Email Log Now	If the email settings are correct the emails containing the system log will be sent on pressing this button.

Table 25: Advanced - Advanced Settings - System Log Settings

## Dynamic DNS

Dynamic DNS or DDNS is used for the updating in real time of Domain Name System (DNS) name servers to keep the active DNS configuration of their hostnames, addresses and other information up to date. To use these settings you will need a dynamic DNS account with DynDNS.org, No-IP.com, TZO.com or dhs.org.

Figure 39: Advanced – Advanced Settings – Dynamic DNS

OPTION	DEFINITION
DDNS	The option to disable or enable the Dynamic DNS function.
Provider	Select your dynamic DNS provider.
Host Name	Enter the hostname / host domain name / host IP address.
Username / Email	Enter the dynamic DNS account username.
Password / Key	Enter the dynamic DNS account password.

Table 26: Advanced - Advanced Settings - Dynamic DNS Settings

# QoS (Quality of Service)

Quality of Service (QoS) refers to resource reservation control mechanisms with the ability to provide a different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. For example, a required packet transfer rate or delay may be guaranteed.

Item	Setting
QoS	Disable
WAN Interface	PVC0
QoS Mode	Smart-QoS
Bandwidth of Upstream	<input type="text"/> Kbps (Kilobits per second)
Bandwidth of Downstream	<input type="text"/> Kbps (Kilobits per second)
Flexible Bandwidth Management	Disable

Item	Select	Setting
Game	<input type="checkbox"/>	<input type="text" value="0"/> %
Chat	<input type="checkbox"/>	<input type="text" value="0"/> %
VoIP	<input type="checkbox"/>	<input type="text" value="0"/> %
P2P	<input type="checkbox"/>	<input type="text" value="0"/> %
Video	<input type="checkbox"/>	<input type="text" value="0"/> %
Web	<input type="checkbox"/>	<input type="text" value="0"/> %

Figure 40: Advanced - Advanced Settings - QoS

OPTION	DEFINITION
QoS	Select the Enable option to enable Quality of Service (QoS).
WAN Interface	Select the WAN interface you wish to configure QoS for.
QoS Mode	Select the QoS Mode to use.
Bandwidth of Upstream	Set the Upstream limit in Kilobits per second (Kbps).
Bandwidth of Downstream	Set the Downstream limit in Kilobits per second (Kbps).
Flexible Bandwidth Management	Select this option to Enable to allow the router to assign the QoS percentage rates or set this option to disable and manually enter the QoS percentage rates for the Item fields.

Table 27: Advanced - Advanced Settings - QoS Settings

## SNMP

SNMP, short for Simple Network Management Protocol is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

Item	Setting
Enable SNMP	<input type="checkbox"/> Local <input type="checkbox"/> Remote
Get Community	<input type="text"/>
Set Community	<input type="text"/>
IP 1	<input type="text"/>
IP 2	<input type="text"/>
IP 3	<input type="text"/>
IP 4	<input type="text"/>
SNMP Version	<input checked="" type="radio"/> V1 <input type="radio"/> V2c
WAN Access IP Address	<input type="text"/>

Save Undo

Figure 41: Advanced – Advanced Settings – SNMP

OPTION	DEFINITION
Enable SNMP	The options to disable or enable the SNMP function for local or remote use.
Get Community	An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent. The Get Community field gets the current community name and is used to identify the group. A SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities. SNMP default communities are: Write – private; Read – public.
Set Community	An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent. The Set Community field sets the new community name used to identify the group. A SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities. SNMP default communities are: Write – private; Read – public.
IP 1	Enter the IP address for one of the local clients connected to router. SNMP will then gather and transmit the network information that you have specified.
IP 2	Enter the IP address for the second of the local clients connected to router. SNMP will then gather and transmit the network information specified.
IP 3	Enter the IP address for the third of the local clients connected to router. SNMP will then gather and transmit the network information specified.
IP 4	Enter the IP address for the fourth of the local clients connected to router. SNMP will then gather and transmit the network information specified.
SNMP Version	Select the version SNMP you wish to use with the NF3ADV.
WAN Access IP Address	Enter the WAN Access IP Address used to provide (WAN) Wide Area Network connectivity to the internet.

Table 28: Advanced - Advanced Settings - SNMP Settings

# Routing

The Routing page in the Advanced Settings section of the NF3ADV provides a network administrator with the means to configure the routing method that the NF3ADV will use, with either dynamic or static routing. Routes are called static if they do not change over time. Thus a static routing table is loaded with values when the system starts and the routes do not change unless an error is detected. Dynamic routing refers to a system that can change its routing table information over time. With dynamic routing, software known as RIP (Routing Information Protocol) interacts with network devices and learns the optimal route to each location. Then RIP updates the local routing table to ensure datagrams follow the optimal routes.

Status   ▶ Network Setup   ▶ Forwarding Rules   ▶ Security Settings   ▶ **Advanced Settings**   ▶ Toolbox

Item	Setting				
Dynamic Routing	<input checked="" type="radio"/> Disable <input type="radio"/> RIPv1 <input type="radio"/> RIPv2				
Static Routing	<input checked="" type="radio"/> Disable <input type="radio"/> Enable				
ID	Destination	Subnet Mask	Gateway	Hop	Enable
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Figure 42: Advanced - Advanced Settings - Routing

**Dynamic Routing:** Routing Information Protocol (RIP) will exchange information about different host destinations for working out routes throughout the network.



Please note: Only select RIPv2 if you have a different subnet in your network. Otherwise, select RIPv1.

**Static Routing:** For static routing, you can specify up to 8 routing rules. You need to enter the destination IP address; subnet mask, gateway, and hop for each routing rule, then enable the rule by clicking the Enable checkbox.

Click on "Save" to store your setting or "Undo" to discard your changes.

## System Time

The NF3ADV router time can be synchronized either to a local PC or using NTP (Network Time Protocol) settings to a standard global internet time. These settings will affect functions such as System Log statistics, scheduling and Firewall settings.

Item	Setting															
Time Zone	(GMT+10:00) Canberra, Melbourne, Sydney															
Auto-Synchronization	<input checked="" type="checkbox"/> Enable Time Server (RFC-868): 0.netcomm.pool.ntp.org															
Enable Daylight Saving	<input checked="" type="radio"/> Disable <input type="radio"/> Enable															
Daylight Saving Dates	<table border="0"> <tr> <td></td> <td>Month</td> <td>Week</td> <td>Day of Week</td> <td>Time</td> </tr> <tr> <td>DTS Start</td> <td>Jan</td> <td>1st</td> <td>Sun</td> <td>1am</td> </tr> <tr> <td>DTS End</td> <td>Jan</td> <td>1st</td> <td>Sun</td> <td>1am</td> </tr> </table>		Month	Week	Day of Week	Time	DTS Start	Jan	1st	Sun	1am	DTS End	Jan	1st	Sun	1am
	Month	Week	Day of Week	Time												
DTS Start	Jan	1st	Sun	1am												
DTS End	Jan	1st	Sun	1am												

Save Undo

Sync Result

Sync with Time Server    Sync with my PC (Wed June 13, 2012 18:40:50)

Figure 43: Advanced - Advanced Settings - System Time

OPTION	DEFINITION
Time Zone	Select the GMT offset for your location.
Auto-Synchronization	Select an NTP (Network Time Protocol) time server to synchronize to the global internet time with.
Enable Daylight Saving	Enable or disable this option to allow for daylight saving.
Daylight Saving Dates	The daylight saving start and end dates can be set with this option.
Sync with Time Server	Select this button to initiate the router time synchronization to the specified network time server above.
Sync with my PC	Select this button to initiate the router time synchronization to the computer you are currently logged into the router with.

Table 29: Advanced - Advanced Settings - System Time Settings

# Scheduling

The NF3ADV has built in scheduling, allowing the router to be switched on or off. This offers a means of parental control. To create a schedule, ensure the enable Schedule option is selected and press the Add New button.

Figure 44: Advanced - Advanced Settings – Scheduling

## Adding a Schedule

Figure 45: Advanced - Advanced Settings - Adding a Schedule

OPTION	DEFINITION
Name of Rule	Enter a name for the Schedule.
Policy	Use the Policy option to set each rule defined to Activate or Deactivate the router except the selected days and hours below.
Week Day	Select the day(s) of the week you wish the rule to be used on.
Start Time (hh:mm)	Enter the Start time for the rule to begin.
End Time (hh:mm)	Enter the End time for the rule to end.

Table 30: Advanced - Advanced Settings - Adding a Schedule

## IPv6

The NF3ADV router can be configured to use IPV6 routing configuration.

Item	Setting
IPv6	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
IPv6 Connection	DHCPv6
DNS Setting	<input checked="" type="radio"/> Obtain DNS Server address Automatically <input type="radio"/> Use the following DNS address
Primary DNS Address	
Secondary DNS Address	
LAN IPv6 Address	
LAN IPv6 Link Local Address	fe80::260:64ff:fe59:17eb
Auto configuration	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Auto configuration Type	Stateless
Router Advertisement Lifetime	200 Seconds

Figure 46: Advanced - Advanced Settings - IPv6

OPTION	DEFINITION
IPv6	The option to enable or disable IPv6.
IPv6 Connection	Select the type of IPv6 for the router to use. Options include : <ul style="list-style-type: none"> <li>DHCPv6 - an IPv6 address is assigned by the router automatically,</li> <li>Static IPv6 - a static IPv6 address assigned by an Internet Service Provider can be assigned to the router.</li> <li>6 to 4 – This option converts an IPv6 address to an IP v4 address.</li> <li>IPv6 in IPv4 tunnel – This option uses an IPv6 address through an IPv4 tunnel.</li> <li>PPPoA – for using an IPv6 address over PPPoA.</li> </ul>
DNS Setting	Select Obtain a DNS Server address automatically assigned by the router or assign your own static Primary and Secondary DNS addresses.
Primary/Secondary DNS Address	Primary and secondary DNS addresses can be added here.
LAN IPv6 Address	Enter the local IPv6 address in this field.
Auto-configuration	Select to enable auto configuration of the IPv6 address.
Auto-configuration Type	Select either Stateless or Stateful IPv6 auto configuration. Stateless Address Auto configuration (or SLAAC) can be used by devices connecting to a routed network using Internet Control Message Protocol version 6 (ICMPv6) router discovery messages. This is generally streamlined and simplified compared to Stateful Auto-configuration. Stateful IPv6 also known as DHCPv6 uses a dedicated configuration mechanism that is more comprehensive than Stateless Auto configuration catering to all the information needs in the form of required parameters to the network devices
Router Advertisement lifetime	When a computer host first connects to the NF3ADV router using IPv6 it sends a link-local router solicitation multicast request for its configuration parameters. If the NF3ADV router is configured correctly it will respond with a router advertisement packet that contains network-layer configuration parameters. The Router advertisement lifetime is the amount of time that the router advertisement is broadcast as a multicast after receiving the request.

Table 31: Advanced - Advanced Settings - IPv6 Settings

## TR-069

The TR-069 (technical report 069) protocol uses a SOAP/HTTP protocol to provide communications between Customer-Premises Equipment (CPE) and an Auto-Configuration Server (ACS) for the purpose of automated configuration of the CPE devices. This can be useful in updating multiple units across a network concurrently.

Item	Setting
TR-069	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
ACS URL	<input type="text"/>
ACS Username	<input type="text"/>
ACS Password	<input type="text"/>
Connection Request Port	<input type="text" value="8099"/>
Connection Request Username	<input type="text"/>
Connection Request Password	<input type="text"/>
Inform	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Interval	<input type="text" value="900"/> seconds

Figure 47: Advanced - Advanced Settings - TR-069

OPTION	DEFINITION
TR-069	Select the enable option to enable the TR-069 protocol on the NF3ADV.
ACS URL	Enter the URL of the Auto-Configuration Server in this field.
ACS UserName	Enter the user name of the Auto-Configuration Server here.
ACS Password	Enter the password of the Auto-Configuration Server here.
Connection Request Port	Enter the port number to be used by a CPE in sending an Inform message to the ACS server to initialize a connection.
Connection Request UserName	Enter the Connection Request username to be used by each of the CPE devices to authenticate with the ACS server.
Connection Request Password	Enter the Connection Request password to be used by each of the CPE devices to authenticate with the ACS server.
Inform	Set the Inform to enable or disable to accept or deny an inform message from a CPE device to the ACS server.
Interval	Enter the interval in seconds between Inform messages being sent to the ACS server.

Table 32: Advanced - Advanced Settings - TR-069 Settings

## VLAN

The VLAN section of the NF3ADV allows for the creation of a virtual LAN across one or more of the Ethernet and wireless interfaces

Ethernet	WAN/LAN	VID	Tx TAG
Port1	LAN1	1	<input type="checkbox"/>
Port2	LAN2	1	<input type="checkbox"/>
Port3	LAN3	1	<input type="checkbox"/>
Port4	LAN4	1	<input type="checkbox"/>

VLAN ID on LAN	LAN/Wireless LAN Interface	Tag	Type	Internet or ISP map WAN (VLAN ID)
1	Port1, Port2, Port3, Port4	No	NAT	0
2	AP-1, AP2-1	No	NAT	0

Save Undo WAN VLAN Settings

Figure 48: Advanced - Advanced Settings - VLAN

Enter the Virtual ID for each Ethernet port and tick whether the data transmitted needs to be tagged, a part of VLAN tagging. For WAN VLAN settings press the WAN VLAN Settings button.

Item	Setting
VID	1
Routing Type	NAT
DHCP Setting	DHCP

Save Undo Back

Figure 49: Advanced - Advanced Settings - WAN VLAN Settings

# Toolbox

The Toolbox menu provides access to maintenance settings of the NF3ADV. Menu options include System Info, Routing Table, Restore Settings, Firmware Upgrade, Backup Settings, Reset to Default, Reboot, Startup Wizard, Miscellaneous and Logout.

## System Info

The System Info section provides access to the system log entries of the NF3ADV. The system log entries can be saved to a file by pressing the Download button at the bottom of the page.

Status   ▶ Network Setup   ▶ Forwarding Rules   ▶ Security Settings   ▶ Advanced Settings   ▶ Toolbox

Item	Setting
WAN Type	
Display time	Thu, 14 Jun 2012 09:12:23 +1000
Time	Log
Jun 14 08:28:10	kernel: klogd started: BusyBox v1.3.2 (2012-06-04 09:46:21 CST)
Jun 14 08:28:11	BEID: BEID STATUS : 0 , STATUS OK!
Jun 14 08:28:13	commander: NETWORK Initialization finished. Result: 0
Jun 14 08:28:14	syslog: Failure parsing line 12 of /etc/udhcpd.conf
Jun 14 08:28:14	syslog: server_config.pool_check = 1
Jun 14 08:28:14	syslog: start = 192.168.1, end = 192.168.1, lan_ip = 192.168.1, interface=br0, ifindex=0
Jun 14 08:28:14	syslog: Unable to open /var/run/udhcpd.leases for reading
Jun 14 08:28:14	udhcpd[1247]: udhcpd (v0.9.9-pre) started
Jun 14 08:28:14	udhcpd[1247]: Unable to open /var/run/udhcpd.leases for reading
Jun 14 08:28:17	nat: Using the packet filter which support IP range
Jun 14 08:28:17	commander: SPA PI
Jun 14 08:28:17	commander: DDNS!
Jun 14 08:28:17	commander: SNMP!
Jun 14 08:28:17	commander: ROUTING!
Jun 14 08:28:17	commander: disable Day light saving..

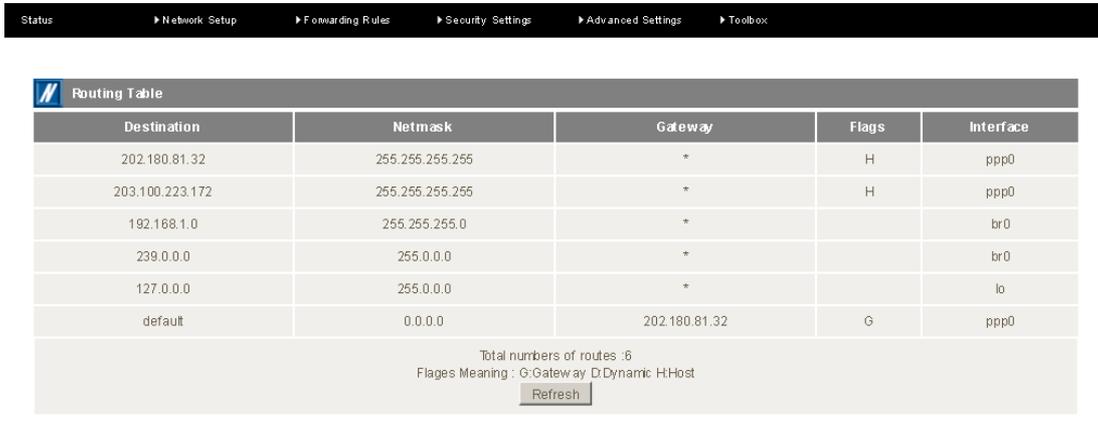
**Page: 1/9 (Log Number: 132)**

<< Previous   Next >>   First Page   Last Page  
Refresh   Download   Clear logs

Figure 50: Advanced - Toolbox - System Info

## Routing Table

The routing table lists all static and dynamic routes currently set for all router interfaces.



The screenshot shows the 'Routing Table' interface within the 'Toolbox' menu. It features a navigation bar at the top with options: Status, Network Setup, Forwarding Rules, Security Settings, Advanced Settings, and Toolbox. The main content area is titled 'Routing Table' and contains a table with the following data:

Destination	Netmask	Gateway	Flags	Interface
202.180.81.32	255.255.255.255	*	H	ppp0
203.100.223.172	255.255.255.255	*	H	ppp0
192.168.1.0	255.255.255.0	*		br0
239.0.0.0	255.0.0.0	*		br0
127.0.0.0	255.0.0.0	*		lo
default	0.0.0.0	202.180.81.32	G	ppp0

Below the table, it states: 'Total numbers of routes :6' and 'Flags Meaning : G:Gateway D:Dynamic H:Host'. A 'Refresh' button is located at the bottom of the table area.

Figure 51: Toolbox - Routing Table

## Restore Settings

The restore settings page can be used to load a previously saved router configuration. It is recommended using an Ethernet cable connection to upload any configuration settings. Do not power off the router until the configuration settings are successfully updated and the router has automatically restarted.



The screenshot shows the 'Restore Settings' page within the 'Advanced' section of the 'Toolbox' menu. It features a navigation bar at the top with options: Status, Network Setup, Forwarding Rules, Security Settings, Advanced Settings, and Toolbox. The main content area is titled 'Config Filename' and contains a text input field with a 'Browse...' button next to it. Below the input field, there is a note: 'Note! Do not interrupt the process or power off the unit when it is being upgraded. When the process is done successfully, the unit will be restarted automatically.' At the bottom of the form, there are 'Restore' and 'Cancel' buttons.

Figure 52: Advanced - Toolbox - Restore Settings

## Firmware Upgrade

This page can be used to upload the latest firmware version for the NF3ADV as it becomes available.

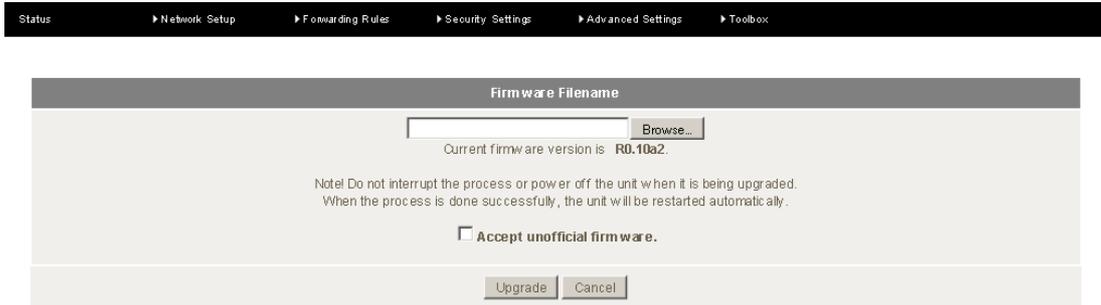


Figure 53: Advanced - Toolbox - Firmware Upgrade

Click the "Browse" button and navigate to the location where you have saved the firmware update file. You can then upgrade the firmware by clicking the "Upgrade" button. Do not power off the device until the firmware upgrade has completed and the router has automatically restarted.

## Backup Settings

This option allows the network administrator to save the configuration settings of the NF3ADV to a file that can be uploaded to another NF3ADV or uploaded into the NF3ADV at a later date. The name of the file can be changed but it is recommended to leave the suffix of the file name as .bin.

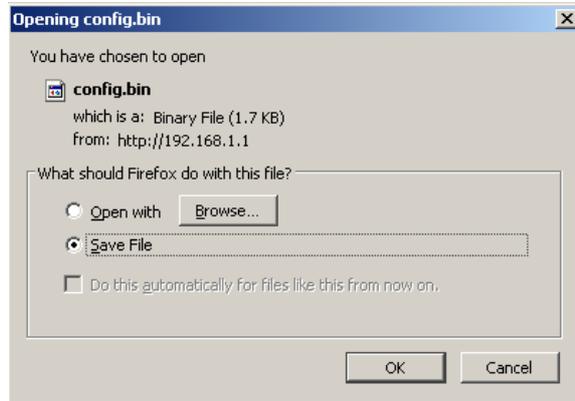


Figure 54: Advanced - Toolbox - Backup Settings

## Reset to Default

This option can be used to reset all settings on the NF3ADV to factory default settings. It is recommended to reset the router to factory default settings after a firmware upgrade.

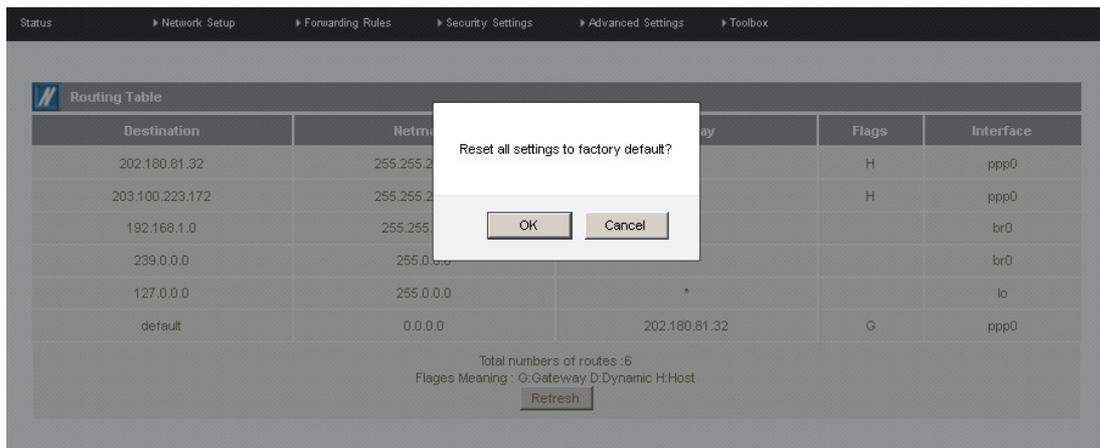


Figure 55: Advanced - Toolbox - Reset to Default

## Reboot

Use this option to reboot the router after making any changes to the configuration settings.

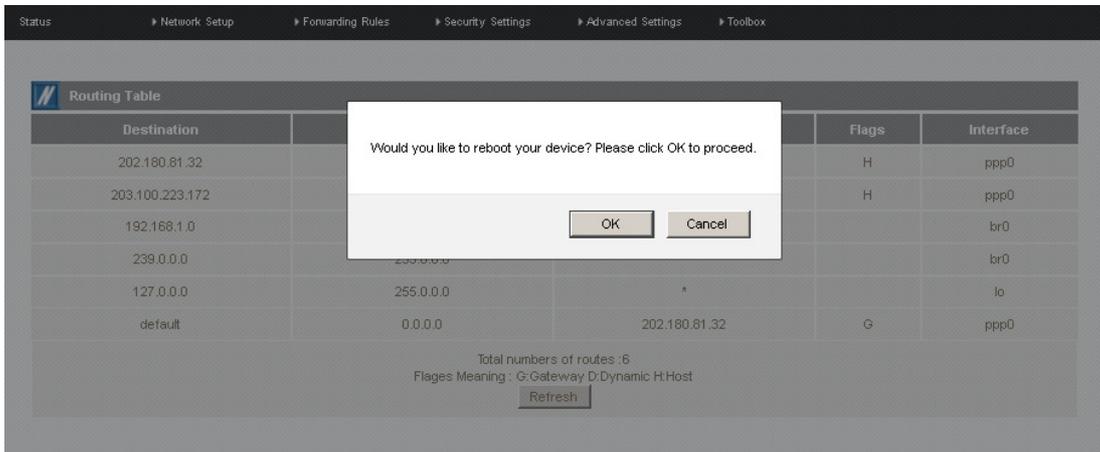


Figure 56: Advanced - Toolbox - Reboot

## Startup Wizard

The Startup Wizard option will return the user to the NF3ADV Startup wizard so that the router can be reconfigured.

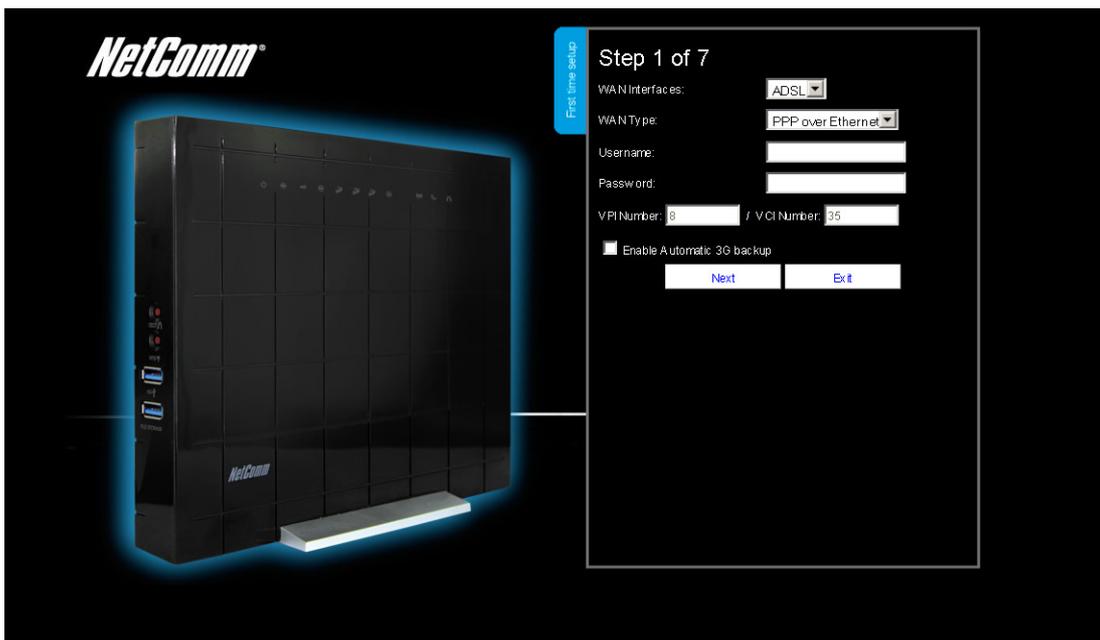


Figure 57: Advanced - Toolbox - Startup Wizard

## Miscellaneous

The Miscellaneous page provides settings for Wake on LAN, has provision for ping tests, and has the option to DIM the LEDs on the front of the unit. Wake-on-LAN enables the router to start-up a computer or device (if the computer supports it) when a WOL packet is detected on the network going to the client MAC you have entered.

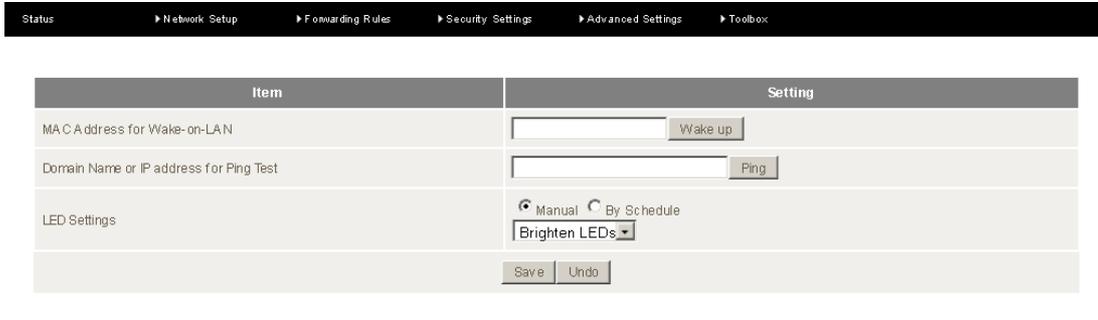


Figure 58: Advanced - Toolbox - Miscellaneous

OPTION	DEFINITION
MAC Address for Wake on LAN	Enter the MAC address of the computer you would like to wake up from stand-by mode.
Domain Name or IP Address for PING Test	Enter the domain name or IP address you wish to attempt to ping to.
LED Settings	Select the manually control the LED brightness.

Table 33: Advanced - Toolbox - Miscellaneous

## Logout

The logout option gives the user the option to logout of the NF3ADV Graphical User Interface.

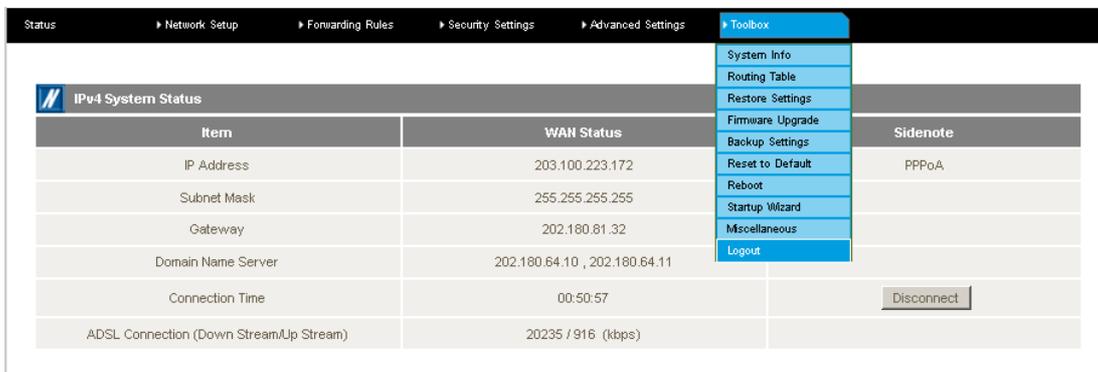


Figure 59: Advanced - Toolbox - Logout

# VOIP/NAS View

To access the VOIP configuration options of your NF3ADV, you need to login to the web configuration and click on the VOIP menu at the top of the page.

Open your web browser (e.g. Internet Explorer/Firefox/Safari) and type "http://192.168.1.1" (without quotations) into the address bar at the top of the window.

At the login screen, type "admin" (without quotes) in the System Password field. Then click on Login.



Please note: "admin" is the default login password for the unit.

Click on the 'Switch to VoIP/NAS View' link at the bottom of the page.

## Status

For more information on the details displayed on the status page, please refer to the [Status](#) page field information on page 24.

## Phone Book

The phone book page provides a list of contact names and phone numbers for easy retrieval when making PSTN and VoIP phone calls. Listing a phone number to a name in the phone book is also used by the Caller ID feature to help identify a caller making an incoming call. (Caller ID must be supported by your VOIP service and telephone handset to work.)

ID	Name	Phone	Enable
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Figure 60: VoIP/NAS View - Phone Book

The phone book can store up to 140 names and phone numbers. On entering a new phone book entry select the Enable checkbox and press the Save button. To remove an incorrect phone book entry, press the Undo button.

## Phone Setting

The Phone Settings menu enables you to configure settings for features such as call waiting, call forwarding and caller ID, Flash Time, Hot Line and DECT Settings. Click on any of the menu items on the left to access the respective page.

### Call Forward

The Call Forward page enables you to configure the type of call forwarding you would like to use and the SIP address to forward any such calls to.

Figure 61: VoIP/NAS Settings - Call Forward

You can select from the following call forwarding conditions:

- Always
- Busy
- No Answer
- Disable

OPTION	DEFINITION
Phone Set	Select either a standard handset or select a cordless phone.
Type	Select the type of Call Forwarding you would like to use.
URL	Enter the phone number or IP address to forward VoIP calls to.

Table 34: VoIP/NAS Settings - Call Forward Settings

## DND Setting

The DND Setting page enables you to configure Do Not Disturb (DND) mode. When DND mode is enabled calls are prevented from being routed through the router to your phone.



Figure 62: VoIP/NAS View - Phone Settings - DND

OPTION	DEFINITION
Phone Set	Select either a standard phone handset or your cordless digital DECT (Digital Enhanced Cordless Telecommunications) phone.
DND Always	Use this option to enable the Do Not Disturb feature.

Table 35: VoIP/NAS View - Phone Settings - DND Settings

## Caller ID

The Caller ID feature provides a means of identification of incoming calls. Unknown calls originating from unrestricted phone lines will output the phone line number. Calls from phone lines listed in the NF3ADV phone book will output the name and number of the phone line.

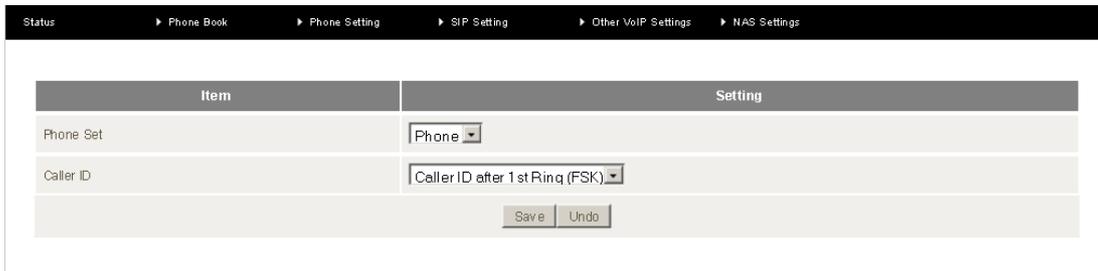


Figure 63: VoIP/NAS View - Phone Settings - Caller ID

OPTION	DEFINITION	
Phone Set	Select either a standard phone handset or a cordless DECT (Digital Enhanced Cordless Telecommunications) phone that is connected to the router.	
Caller ID	Don't Show Caller ID	Caller ID will be disabled.
	Caller ID after 1- Ring (FSK)	Caller ID displays after the first ring of an incoming phone call using Frequency Shift Keying to identify the incoming phone line.

Table 36: VoIP/NAS View - Phone Settings - Caller ID Settings

## Flash Time

The Flash Time page can be used to configure the minimum and maximum time a hook flash signal can occur. A hook flash is a quick off-hook/on-hook/off-hook cycle used to switch to another incoming call using a call waiting service on the NF3ADV.

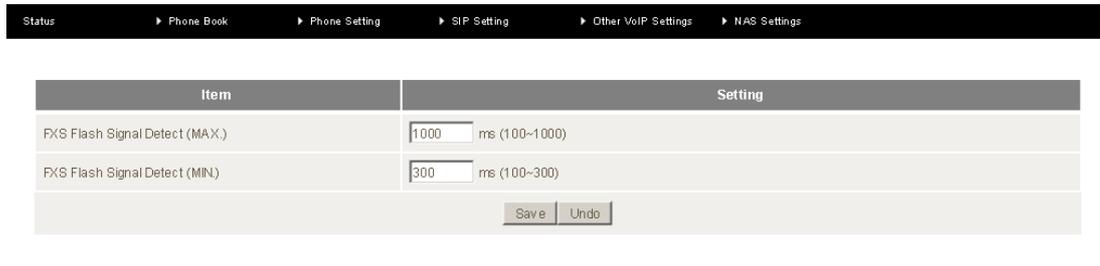


Figure 64: Advanced - VoIP/NAS View - Phone Settings - Flash Time

These settings should not need to be changed unless you have been directed to do so. Click 'Save' to save your settings or 'Undo' to discard any incorrect settings entered.

OPTION	DEFINITION
FXS Flash Signal Detect (MAX)	Enter the maximum time (in milliseconds) for the router to detect a hook flash.
FXS Flash Signal Detect (MIN)	Enter the minimum time (in milliseconds) for the router to detect a hook flash.

Table 37: Advanced - VoIP/NAS View - Phone Settings - Flash Time Settings

## Call Waiting

The Call Waiting feature negates the need for a second phone line by enabling a user to engage two incoming calls simultaneously. When an incoming phone call is placed and the user is already engaged with an existing phone call the user can temporarily suspend the current phone call and switch to the new incoming call (using the hook flash function mentioned above). The user can then negotiate with both parties the optimal outcome to accommodate all parties. Please note to use the NF3ADV Call Waiting feature Call Waiting must be enabled over your VoIP line by your VOIP Service Provider.



Figure 65: VoIP/NAS View - Phone Settings - Call Waiting

OPTION	DEFINITION
Phone Set	Select either a standard phone handset or your cordless digital DECT (Digital Enhanced Cordless Telecommunications) phone.
Call Waiting	Enable or Disable the Call Waiting feature on the NF3ADV.

Figure 66: VoIP/NAS View - Phone Settings - Call Waiting Settings

# Hot Line

The Hot Line page enables you to configure a telephone number which can be called without dialing any numbers at all (simply pick up the telephone handset) after the specified wait time.

Item	Setting
Phone Set	Phone
Use Hot Line	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Hot Line Number	<input type="text"/>
Waiting time before starting Hot Line	3 second (1~9)

Figure 67: VoIP/NAS View - Phone Settings -Hot Line

OPTION	DEFINITION
Phone Set	Select the phone you wish to use as the Hot Line phone.
Use Hot Line	Select to Enable or Disable the Hot Line feature.
Hot Line Number	Enter the number to forward Hot Line calls to.
Waiting time before starting Hot Line	Enter the amount of time (in seconds) to wait after the handset is off hook before forwarding a call to the Hot Line number.

Table 38: VoIP/NAS View - Phone Settings - Hot Line Settings

# Call Features

The Call Features page enables you to configure dialing codes that can be used to activate or deactivate additional features on your VOIP service. Please note each call feature listed will only function if your VoIP Service Provider has enabled them on your VoIP line.

Item	Setting
Blind Call Transfer	*98
Attended Call Transfer	*02
Anonymous Call Enable	*67
Anonymous Call Disable	*67#
Anonymous Call Per Call Basis	*81
DND Enable	*78
DND Disable	*78#
Call Forwarding Enable	*72
Call Forwarding Disable	*72#
Call Return	*69

Figure 68: VoIP/NAS View - Phone Settings - Call Features

You can change the dial codes on the following VOIP service features:

- Blind Call Transfer
- Anonymous Call Enable
- Anonymous Call Disable
- Anonymous Call per Call Basis
- DND Enable
- DND Disable
- Call Forwarding Enable
- Call Forwarding Disable
- Call Return

Click 'Save' to save your settings or 'Undo' to discard any incorrect settings entered.

## DECT Settings

The DECT (Digital Enhanced Cordless Telecommunications) Settings page allows for the configuration of the router's built in DECT base station. Up to four cordless DECT handsets can be connected to the DECT base station at one time and can be used with both VoIP (FXS) and PSTN (FXO) phone call types.

### DECT Settings

This section allows a registered DECT handset to be defined into or deregistered from a DECT Phone Group.

Figure 69: VoIP/NAS View - Phone Setting - DECT Handset Settings

OPTION	DEFINITION
Base Station Status	This field give a basic description of the DECT base station's current state.
DECT	Enable or disable the DECT base station with this field.
Handset Setting	This section allows a registered DECT handset to be defined into or deregistered from a DECT Phone Group.

Table 39: Advanced - Phone Setting - DECT Handset Settings

## Handset Page

This page allows the DECT handset page to be enabled or disabled.

Item	Setting
Base Station status	Normal
DECT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Handset Page	
Handset Page	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

Figure 70: VoIP/NAS View - Phone Setting - DECT Settings - Handset Page

## DECT Handset Registration Page

This page allows the DECT handset registration function to be enabled or disabled.

Item	Setting
Base Station status	Normal
DECT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Registration	
Registration	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

Figure 71: VoIP/NAS View - Phone Setting - DECT Settings - Registration Page

## DECT Handset PIN Code Page

This page allows the PIN code for a DECT handset to be set.

Item	Setting
Base Station status	Normal
DECT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
PIN Code	
PIN Code	<input type="text" value="0000"/>
<input type="button" value="Save"/> <input type="button" value="Undo"/>	

Figure 72: VoIP/NAS View - Phone Setting - DECT Settings - PIN Code Page

## SIP Settings

The SIP (Session Initiation Protocol) Settings section of the NF3ADV can be used to configure your VoIP service with the VoIP account settings provided by your VoIP Service provider.

### Service Domain

The Service Domain page can be used to successfully register the SIP settings of your VoIP account. If you are unsure about any specific setting or have not been supplied information for a particular field, please contact your VOIP service provider to verify if this setting is needed or not.

Item	Setting
SIP Account	1 SIP Account
Phone Set	Phone
WAN Interface	PVC0
Item	Setting
Display Name	
UserName	
Register Name	
Register Password	
Realm	
Domain	
Proxy Server	
Registrar	
Use Outbound Server	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Outbound Proxy	
Status	Unregistered

Figure 73: VoIP/NAS View - SIP Settings - Service Domain

OPTION	DEFINITION
SIP Account	Select whether you wish to configure a single VoIP account or multiple VoIP accounts.
Phone Set	Select which handset to use.
WAN Interface	Select which method of connection configuration to use.
Display Name	Enter the display name for your VOIP service.
User Name	Enter the User Name for your VOIP service.
Register Name	Enter the Register Name (May be called the Auth ID ) for your VOIP service.
Register Password	Enter the Register Password (May be called the Auth Password) for your VOIP service.
Realm	Enter the Realm in use for your VOIP service.
Domain	Enter the Domain for your VOIP service.
Proxy Server	Enter the Proxy Server address in use for your VOIP service.
Registrar	Enter the Registrar for your VOIP service.
Use Outbound server	Enable or Disable the use of an Outbound Proxy for VOIP calls depending on whether your VoIP account is capable of outbound calls.
Outbound Proxy	Enter the Outbound Proxy server address to use if required.
Status	The current status of your VOIP service.

Table 40: VoIP/NAS View - SIP Settings - Service Domain Settings

## Port Setting

The Port Setting page enables you to specify a different SIP (Session Initiation Protocol) Port or RTP (Real Time Protocol) Port number to connect to your VOIP service on.

Item	Setting
SIP Port	5000 (0-65533) if set 0, it will be assigned by the system
RTP Port	5000 (0-65533) if set 0, it will be assigned by the system

Save Undo

Figure 74: VoIP/NAS View - SIP Setting - Port setting

Generally the SIP and RTP port numbers will not need to be changed from their default values. It is recommended to only change the port number of these protocols if advised by your VoIP Service or Internet Service Provider.

## Codec Setting

The Codec Setting page enables you to select which audio codec to use with your VOIP service. This information will usually be supplied by your VOIP service provider and should not need to be changed unless you are experiencing issues with VOIP call sound quality.

Item	Setting
Codec Priority 1	G.711 a-law
Codec Priority 2	G.729
Codec Priority 3	G.726 - 32
Codec Priority 4	G.711 u-law
Item	Setting
SIP Packet Length (G.711 & G.729)	10 ms
Item	Setting
Voice VAD	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
The packet length for Comfort noise packet	30 ms(10-50ms)

Save Undo

Figure 75: VoIP/NAS View - SIP Setting - Codec Setting

The following codecs are available for use:

- G.729
- G.711 a-law
- G.711 u-law
- G.726 -32

OPTION	DEFINITION
Codec Priority 1	Set the audio codec you would like to try first with your VOIP service.
Codec Priority 2	Set the audio codec you would like to try second with your VOIP service.
Codec Priority 3	Set the audio codec you would like to try third with your VOIP service.
Codec Priority 4	Set the audio codec you would like to try fourth with your VOIP service.
G.711 & G.729 Packet Length	Adjust the packet length size. This can reduce or increase the bandwidth required for a VOIP call.
Voice VAD	Adjustment of the 'Voice Activity Detection' (VAD) interval can be done here but should not be adjusted unless the words in your conversation are being cut off. (This setting should not need to be changed.)
The Packet Length for Comfort Noise Level	To minimise jarring, stop-start transmissions between the silence and speech periods of a call comfort noise is used, filling the silent periods of a call with ambient noise. Do not change this value unless advised to by your VoIP Service Provider.

Table 41: VoIP/NAS View - SIP Setting - Codec Settings

Click 'Save' to save your settings or 'Undo' to discard the settings entered.

## DTMF Setting

The DTMF Setting page enables you to specify which DTMF standard to use on your VOIP service. DTMF or Dual-tone multi-frequency signaling is used for signaling in telecommunications over analog telephone lines in the voice-frequency band between telephone handsets and other communications devices. Many people use DTMF settings daily when making a number selection when dialing a phone number on a standard handset and producing a tone.



Figure 76: VoIP/NAS View - SIP Setting - DTMF Setting

The following DTMF standards are available for use:

- RFC 2833.
- Inband DTMF.
- Send DTMF SIP Info.

This information will usually be supplied by your VOIP service provider and should not need to be changed unless you are experiencing issues with DTMF based services such as automated telephone services and answering machines.

Click 'Save' to save your settings or 'Undo' to discard the settings entered.

## Other Settings

The Other Settings page enables you to specify a different SIP expire time and select to enable the DNS SRV function. This information will usually be supplied by your VOIP service provider and should not need to be changed unless you are experiencing issues with VoIP calls or with successfully registering the SIP settings of your VoIP service.

Item	Setting
SIP Expire Time	500 (15--96400 sec)
Use DNS SRV	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
SIP ALG	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Rport	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Save Undo

Figure 77: VoIP/NAS View - SIP Setting - Other Settings

OPTION	DEFINITION
SIP Expire Time	Select to length of time in seconds between the NF3ADV re-registering the SIP settings on your VoIP Service Provider's network.
Use DNS SRV	Select enable or disable the DNS SRV function. This is a DNS service record of the IP addresses and port number of the servers used by your specified VoIP service. Press the Save button to save any settings changes.
SIP ALG	The SIP ALG (Application Layer Gateway) is basically a VoIP firewall. It checks and modifies SIP traffic where necessary to pass through a NAT firewall. Press the Save button to save any settings changes.
Rport	Select to enable or disable Rport function.

Table 42: VoIP/NAS View - SIP Setting - Other Settings

## Other VoIP Settings

The Other VoIP settings page enables you to configure settings for connecting the NF3ADV to a STUN server. Click on the menu item on the left to access the configuration page.

### STUN Settings

The STUN Settings page enables you to configure settings related to utilizing a STUN server with your VOIP service. This information will usually be supplied by your VOIP service provider and should not be needed unless you are experiencing issues with VOIP calls or signing into your VOIP service.

Item	Setting
SIP ALG	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
STUN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
STUN Server	<input type="text"/>
STUN Port	<input type="text"/> (80-65535)

Save Undo

Figure 78: VoIP/NAS View - Other VoIP Settings - STUN Settings

OPTION	DEFINITION
SIP ALG	The SIP ALG (Application Layer Gateway) is basically a VoIP firewall. It checks and modifies SIP traffic where necessary to pass through a NAT firewall.
STUN	Select to enable or disable STUN functionality.
STUN Server	Enter the IP address of the STUN server.
STUN Port	Enter port number that the STUN server uses.

Table 43: VoIP/NAS View - Other VoIP Settings - STUN Settings

Press the Save button to save any settings changes you make.

## Telephony Profile

The Telephony Profile page enables you to configure the way the FXS phone port (RJ-11) operates.

Item	Setting
FXS Port	Australia

Save Undo

Figure 79: VoIP/NAS View - Other VoIP Settings - Telephony Profile

Generally this setting should not need to be changed. Currently the Australia and United States Profile are available for use.

Click 'Save' to save any changes to your settings or 'Undo' to discard the settings you have entered.

## NAS Settings

The NAS Settings page enables you to configure the network area storage (NAS) function of the NF3ADV. This function can be used to remotely access files stored on an attached USB hard drive. Click on any of the menu items to access the respective configuration page.

### Disk Utility

The Disk Utility function enables you to check any attached USB storage for errors. The NF3ADV will scan the attached storage and determine if there are any file system errors present. File System errors can prevent you being able to access stored content. You can also format (erase) any attached storage if needed. Simply click the appropriate button to perform either task.

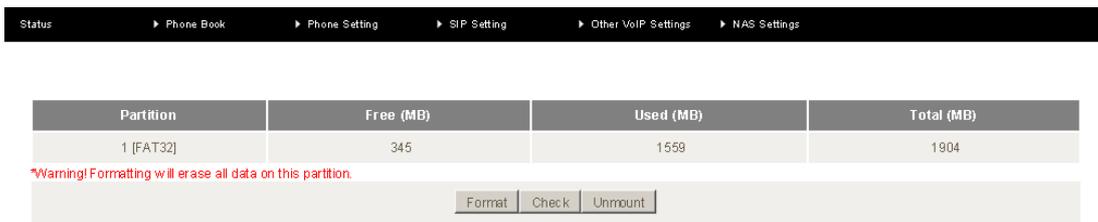


Figure 80: VoIP/NAS View - NAS Settings - Disk utility

### File Sharing

The File Sharing function enables the NBF3ADV to take part in a Windows networking environment. Once configured, the attached USB Storage can be viewed from Windows Explorer by typing:

\\<Configured Name of the NF3ADV>\Storage\ or as for the example below \\NAS\Storage.

Files can then be dragged and dropped onto the attached USB storage.

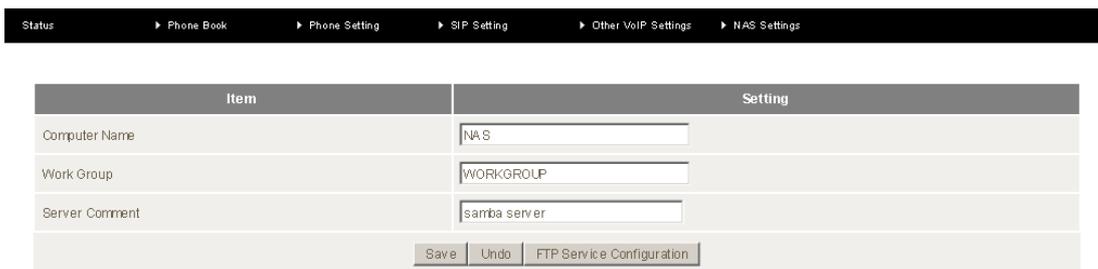


Figure 81: VoIP/NAS View - NAS Settings - File Sharing

OPTION	DEFINITION
Computer Name	Enter the computer name the NF3ADV is to use on the network.
Work Group	Enter the network workgroup the NF3ADV is to be a member of.
Server Comment	Enter the comment to be displayed when a list of network hosts is shown. This can be useful to help identify the device and its purpose.

Table 44: VoIP/NAS View - NAS Settings - File Sharing Settings

The File Sharing configuration also enables you to enable the built-in FTP server function and the associated settings:

Figure 82: VoIP/NAS View - NAS Settings - FTP Configuration

OPTION	DEFINITION
FTP	Select to enable or disable the FTP server function.
FTP Port	Enter the network port the FTP server should run on.
FTP Max Connections per IP	Enter the maximum number of concurrent connections which can be used by a particular IP address.
FTP Max Clients	Enter the maximum number of clients which can connect to the FTP concurrently.
Client Support UTF8	Enable Unicode support for connected clients.

Table 45: VoIP/NAS view - NAS Settings - FTP Settings

## Access Control

The Access Control function enables control over which users can access any attached USB Storage. By default, the NF3ADV is in 'Guest Mode' which means anyone can access the attached hard drive.

Figure 83: VoIP/NAS View - NAS Settings - Access Control

Enabling 'Authorization Mode' allows the creation of specific user accounts with a password to further control access permissions. To enable this, click on the 'Authorization Mode' radio button and click 'Save'. You can then click on the 'User Configuration' button in order to create the required user accounts.

Figure 84: VoIP/NAS View - NAS Settings - Access Control - Security Level

Add the user name and password and then click the 'Add' button. Alternatively, to remove a user, click on the radio button to the right of the username and then click the 'Delete' button.

## iTunes Server

The iTunes Server function enables any applicable media on any attached USB storage to be directly accessed from within iTunes. To enable this function, click on the 'Enable' radio button in the 'Service' section. Click the 'Save' button to save any configuration changes you have made.

Item	Setting
Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
iTunes Shared Library Name	<input type="text"/>
iTunes Shared Library Password (required)	<input type="text"/>
Service Port (default = 3689)	<input type="text" value="3689"/>

Save Undo

Figure 85: VoIP/NAS View - NAS Settings - iTunes Server

OPTION	DEFINITION
Service	Select to Enable or Disable the iTunes server service.
iTunes Shared Library Name	Enter the name that will show up in the iTunes library list.
iTunes Shared Library Password (required)	Enter the password that will show up in the iTunes library list
Service Port	Enter the port number to run your iTunes server on (This will usually be left as the default value 3369).

Table 46: VoIP/NAS View - NAS Settings - iTunes Server Settings

# Download Assistant

The Download Assistant enables you to schedule the NF3ADV to perform a download from an Internet host.

You are able to select from two download types:

- FTP
- HTTP

Each type of download job requires different configuration options.

## FTP

Item	Setting
Download Type	<input checked="" type="radio"/> FTP <input type="radio"/> HTTP
Job Name	<input type="text"/>
URL	<input type="text"/> Port <input type="text" value="21"/>
Save To	<input type="text" value="/QDownloads/FTP"/>
Login method	<input checked="" type="radio"/> Anonymous <input type="radio"/> Account
Username	<input type="text"/>
Password	<input type="text"/>
Start Time	<input type="radio"/> Schedule <input checked="" type="radio"/> At Once
	Time <input type="text" value="2012"/> / <input type="text" value="Jun"/> / <input type="text" value="14"/> - <input type="text" value="15"/> : <input type="text" value="42"/>
<small>*Please make sure the files that you download are legal before proceeding to download them.</small>	
<input type="button" value="E-mail Alert Configuration"/> <input type="button" value="Save"/> <input type="button" value="Undo"/>	

Figure 86: VoIP/NAS View - NAS Settings - Download Assistant – FTP

OPTION	DEFINITION
Job Name	A name to identify the download job.
URL	The address to download the file from using the FTP protocol.
Port	The port required for the FTP server (This would usually be left as 21).
Save To	The location of the device on the NF3ADV network to save the downloaded file to.
Login Method	Select the type of authentication required by the FTP server (Selecting anonymous means a username and password are not required).
Username	The username required to access the FTP server.
Password	The password required to access the FTP server.
Start Time	Select to either schedule a time for the download to begin or start the download immediately.

Table 47: VoIP/NAS Settings - NAS Settings - Download Assistant - FTP

## HTTP

Item	Setting
Download Type	<input type="radio"/> FTP <input checked="" type="radio"/> HTTP
Job Name	<input type="text"/>
URL	<input type="text"/>
Save To	<input type="text" value="/Downloads/HTTP"/>
Start Time	<input type="radio"/> Schedule <input checked="" type="radio"/> At Once
	Time: 2012 Jun 14 15:44
*Please make sure the files that you download are legal before proceeding to download them.	
<input type="button" value="E-mail Alert Configuration"/> <input type="button" value="Save"/> <input type="button" value="Undo"/>	

Figure 87: VoIP/NAS Settings - NAS Settings - Download Assistant - HTTP

OPTION	DEFINITION
Job Name	A name to identify the download job.
URL	The address to download the target files from.
Save To	The location on the NF3ADV to save the downloaded files to.
Start Time	Select to either schedule a time for the download to begin or start the download immediately.

Table 48: VoIP/NAS View - NAS Settings - Download Assistant – HTTP

You can also configure the NF3ADV to send an e-mail on completion of a scheduled download. Click on the 'E-mail Alert Configuration' button to setup this option.

Item	Setting
HTTP download alert	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
FTP download alert	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
SMTP Server Address	<input type="text"/>
SMTP Server Port	<input type="text"/>
SMTP UserName	<input type="text"/>
SMTP Password	<input type="text"/>
Email Address	<input type="text"/>
Email Subject	<input type="text"/>
Reservation Diskspace	200 MB
<input type="button" value="Back"/> <input type="button" value="Save"/> <input type="button" value="Undo"/> <input type="button" value="Test E-mail"/>	

Figure 88: VoIP/NAS View - NAS Settings - Download Assistant - Email Alert Settings

OPTION	DEFINITION
HTTP Download Alert	Select to enable or disable an alert to be sent for a completed HTTP download.
FTP Download Alert	Select to enable or disable an alert to be sent for a completed FTP download.
SMTP Server Address	Enter the address of the email server to be used to send the alerts.
SMTP Server Port	Enter the port which the email server is running on.
SMTP User Name	Enter the username required to login to the email server.
SMTP Password	Enter the password required to login to the email server.
Email Address	Enter the email address any alerts are to be sent to.
Email Subject	Enter the subject to be used on any email alerts sent out.
Reservation Disk Space	Enter the amount of disk space to reserve on the NF3ADV for the specified download.

Table 49: VoIP/NAS Settings - NAS Settings - Download Assistant Settings

## Download Status

The Download Status page enables you to monitor previously scheduled Download Assistant jobs. From this page you are able to Start, Pause, Resume or Delete any Download Assistant jobs.

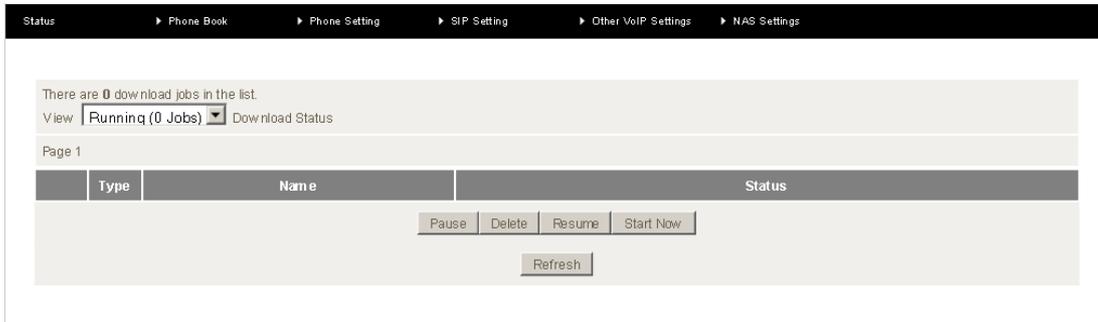


Figure 89: VoIP/NAS View - NAS Settings - Download Status

The View drop-down menu enables you to select whether currently running jobs, waiting jobs or scheduled jobs are displayed. Once listed, click on the checkbox on the left hand side of the listed jobs and then click the appropriate function button.

## Web HDD

The Web HDD function provides a web page based Windows Explorer type view of the content of any attached USB storage. Using this interface you are able to upload, download or delete files and folders as well as create directories. Click through the displayed folders to show any stored files.



Figure 90: VoIP/NAS view - NAS Setting - Web HDD

Select any item and click the appropriate operation button at the bottom of the page. Alternatively double click folders to view any content.

To upload files to your Web HDD click the Upload button. You can then click the 'Browse' button and then navigate to the file you would like to upload. Once selected, this file will be copied to the Web HDD and become available to download by connected devices.

## Additional Product Information

### Establishing a wireless connection

#### Windows XP (Service Pack 2)

1. Open the Network Connections control panel (Start -> Control Panel -> Network Connections).
2. Right-click on your Wireless Network Connection and select View Available Wireless Networks.
3. Select the wireless network listed on your included wireless security card and click Connect.
4. Enter the network key (refer to the included wireless security card for the default wireless network key).
5. The connection will show Connected.

#### Windows Vista

1. Open the Network and Sharing Center (Start > Control Panel > Network and Sharing center).
2. Click on "Connect to a network".
3. Choose "Connect to the Internet" and click on "Next".
4. Select the wireless network listed on your included wireless security card and click Connect.
5. Enter the network key (refer to the included wireless security card for the default wireless network key).
6. Select the appropriate location. This will affect the firewall settings on the computer.
7. Click on both "Save this network" and "Start this connection automatically" and click "Next".

#### Windows 7

1. Open the Network and Sharing Center (Start > Control Panel > Network and Sharing Center).
2. Click on "Change Adapter settings" on the left-hand side.
3. Right-click on "Wireless Network Connection" and select "Connect / Disconnect".
4. Select the wireless network listed on your included wireless security card and click Connect.
5. Enter the network key (refer to the included wireless security card for the default wireless network key).
6. You may then see a window that asks you to "Select a location for the 'wireless' network". Please select the "Home" location.
7. You may then see a window prompting you to setup a "HomeGroup". Click "Cancel" on this.
8. You can verify your wireless connection by clicking the "Wireless Signal" indicator in your system tray.
9. After clicking on this, you should see an entry matching the SSID of your NF3ADV with "Connected" next to it.

#### Mac OSX 10.6

1. Click on the Airport icon on the top right menu.
2. Select the wireless network listed on your included wireless security card and click Connect.
3. On the new window, select "Show Password", type in the network key (refer to the included wireless security card for the default wireless network key) in the Password field and then click on OK.
4. To check the connection, click on the Airport icon and there should be a tick on the wireless network name.



Please note: For any other operating system (Windows 98SE, Windows ME, Windows 2000 etc.) or if you use a wireless adaptor utility to configure your wireless connection, please consult the wireless adaptor documentation for additional information.

## Troubleshooting

### Using the indicator lights (LEDs) to Diagnose Problems

The LEDs are useful aides for finding possible problem causes.

#### Power LED

The Power LED does not light up.

STEP	CORRECTIVE ACTION
1	Make sure that the NF3ADV power adaptor is connected to the device and plugged in to an appropriate power source. Use only the supplied power adaptor.
2	Check that the NF3ADV and the power source are both turned on and device is receiving sufficient power.
3	Turn the NF3ADV off and on.
4	If the error persists, you may have a hardware problem. In this case, you should contact technical support.

#### Web Configuration

I cannot access the web configuration pages.

STEP	CORRECTIVE ACTION
1	Make sure you are using the correct IP address of the NF3ADV. You can check the IP address of the device from the Network Setup configuration page.
2	Check that you have enabled remote administration access. If you have configured an inbound packet filter, ensure your computer's IP address matches it.
3	Your computer's and the NF3ADV's IP addresses must be on the same subnet for LAN access. You can check the subnet in use by the router on the Network Setup page.
4	If you have changed the devices IP address, then enter the new one as the URL you enter into the address bar of your web browser.

The web configuration does not display properly.

STEP	CORRECTIVE ACTION
1	Delete the temporary web files and log in again. In Internet Explorer, click Tools, Internet Options and then click the Delete Files ... button. When a Delete Files window displays, select Delete all offline content and click OK. (Steps may vary depending on the version of your Internet browser.)

#### Login Username and Password

I forgot my login username and/or password.

STEP	CORRECTIVE ACTION
1	Press the Reset button for ten seconds, and then release it. When the Power LED begins to blink, the defaults have been restored and the NF3ADV restarts. You can now login with the factory default username and password "admin" (without the quotes)
2	It is highly recommended to change the default username and password. Make sure you store the username and password in a safe place.

#### WLAN Interface

I cannot access the NF3ADV from the WLAN or ping any computer on the WLAN.

STEP	CORRECT ACTION
1	If you are using a static IP address for the WLAN connection, make sure that the IP address and the subnet mask of the NF3ADV and your computer(s) are on the same subnet. You can check the routers configuration from the Network Setup page.

## Using the NF3ADV to make and receive telephone calls

The NF3ADV provides circuit switched voice services via a telephony line interface offering the ability to make and receive telephone calls via a regular analogue telephone using the local voice network.



Please note: Please refer to your mobile service provider for activation of your voice service and information about the call charges that apply.

### Handset requirements

The NF3ADV allows you to make telephone calls over the VoIP network using a standard analogue telephone via the built in RJ-11 Phone port and up to 5 cordless phones using the built in DECT module . Please refer to the documentation provided by the manufacturer of your analogue or cordless telephone for assistance with the operation of your telephone handset.

### Maximum REN Loading

Please note that the line interface on the NF3ADV is capable of supporting multiple analogue telephones connected via splitters. The ringer equivalence number (REN) for each line is 5. Therefore, a maximum of 5 handsets each with a REN number of 1 can be connected to each line port.

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

1. You have a WAN connection to the internet.
2. Your NF3ADV is powered on and in running condition.
3. Your SIP settings have successfully registered to your VoIP provider's network.
4. A working analogue telephone connected into the Phone port.
5. You hear the dial tone and the Phone LED on the front of your NF3ADV should light up after lifting the handset.

### How to place a call

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

### How to receive a call

When an incoming call is received, the Line light will start flashing and any phones connected to the NF3ADV will ring. Answer the telephone following the instructions provided by your telephone handset manufacturer to conduct the call.

If there is no phone connected to the NF3ADV, all incoming calls will be transferred to Voicemail (if enabled on the device).

### Answering an incoming call when on a call

Call waiting enables a 2nd incoming call to be received while you are on a call. To answer a call waiting call, perform a hook-flash (briefly depressing the hook button). The incoming call should then be answered. Upon hanging up or performing another hook-flash, you will be returned to the original telephone call.

### Accessing voicemail

To access your voicemail, please dial \*98 and follow the voice prompts.

# Call Feature Codes

## Quick Reference Table

The NF3ADV supports a number of call feature codes for supplementary services.

FEATURE	ACTIVATION	DEACTIVATION	STATUS
Caller ID	#31# (to block an individual call)	*31# (to unblock an individual call)	N/A
Call Waiting	*43#	#43#	*#43#
Call Forwarding	*72<Directory Number>#	*72#	*#72#

Table 50: Additional Product Information - Call Feature Codes Quick Reference

### Caller ID

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

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

### Call Waiting

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

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

### Call forwarding

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



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

### Call Forwarding Unconditional

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

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

### Call Forwarding No Answer

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

- To enable Call Forwarding No Answer, dial \*72<Directory Number>#  
(Where directory number is the number you wish to forward calls to)
- Hang up after you hear 2 low pitch beeps.
- To disable Call Forwarding No Answer, dial #72#
- Hang up after you hear 2 high pitch beeps.
- To check the status of Call Forwarding No Answer, dial \*#61# or view the advanced status page of the management console.
  - Call Forwarding No Answer is disabled if you hear 2 high pitch beeps.
  - Call Forwarding No Answer is enabled if you hear 2 low pitch beeps.

## Call Forwarding Busy

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

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

## Call Forwarding Not Reachable

Call forwarding busy will divert all incoming calls to a phone number that you desire only if your telephone is unreachable by the network.

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

## Conference Call

A conference call can be achieved by performing a hook-flash and then by dialing the third party. Wait for the third party to answer your call and then perform another hook-flash to conference all the parties together.



Please note: In order to activate a conference call, you will need to have originated both calls.

## Troubleshooting

What do I do if I have no dial tone?

Please follow the procedure listed below:

1. Check to make sure the phone is plugged into your NF3ADV into the RJ-11 port marked with a phone.
2. Check to make sure you are using the correct cable (Cat-3 UTP Telephone Cable with RJ-11 plugs).
3. Check to make sure the line light on the front panel of the NF3ADV turns solid blue if you lift the handset.
4. Check to make sure the blue MBB indication light on the front of the NF3ADV is blinking.
5. Check to make sure your MBB SIM card is activated and inserted into your NF3ADV properly.
6. Check and see if you get the dial tone after rebooting your NF3ADV.

I have noise interference during telephone calls. How can I fix this?

To resolve this issue, try the following:

- Verify that the RJ-11 cable is securely connected and not damaged.
- Try to remove any telephone splitters from the connection between your phone and the NF3ADV.
- Try rebooting your NF3ADV.

# Technical Data

The following table lists the hardware specifications of the NF3ADV.

MODEL	NF3ADV
<b>Connectivity</b>	10/100/1000 Ethernet LAN x 3, 10/100/1000 Ethernet WAN x 1, WLAN, RJ-11 x 3, ADSL modem
<b>Antenna connector</b>	Onboard
<b>LED Indicators</b>	Power, ADSL, 3G, WWW, LAN 1-3, WAN, WiFi, Voice, DECT
<b>Operating Temperature</b>	0 ~ 50 degrees Celsius (operating temperature)
<b>Power input</b>	12VDC – 2.0A
<b>Dimensions &amp; Weight</b>	189 mm (L) x 240 mm (H) x 34 mm (W) 250 grams
<b>Voice</b>	1 x FXO port, 1 x FXS ports, 1 x DECT module
<b>Storage/ Print Server</b>	2 x USB 2.0 ports
<b>Regulatory Compliancy</b>	A-Tick

Table 51: NF3ADV Technical Specifications

## Electrical Specifications

A suitable power supply is available on request or via direct purchase from the NetComm Online shop. It is recommended that the NF3ADV be powered using the 12VDC/2.0A power supply which is included with the device.

## Environmental Specifications / Tolerances

The NF3ADV is able to operate over a wide variety of temperatures from 0°C ~ 50°C (ambient).

## FAQ

1. I cannot seem to access the web page interface.

The default IP address of the unit is 192.168.1.1, so first try to open a web browser to this address. Also check that your laptop/ PC is using the same subnet as the router's Ethernet port. I.e. An IP address has been assigned to your computer in the range of 192.168.1.x where x can equal 2 – 254.

2. The router has a connection but cannot access the internet.

Check that DNS Proxy is enabled by clicking on the DHCP Server link on the Advanced > Network Setup menu. Make sure that the DHCP DNS server address 1 IP address is set to the same address as that of the Ethernet port.

3. Can I make PSTN calls from the NF3ADV?

Yes. By connecting a regular landline (Analogue) telephone to the port Phone using the RJ-11 Cable provided or by connecting a cordless DECT phone to the iQ DECT base station onboard the NF3ADV. To activate the phone jacks in your home or office connect an RJ-11 Cable from the port labeled "Line" to any wall jack. When you lift the receiver you will hear a dial tone and can place your call. Dial ## before the number you wish to be connected to, and the PSTN call will be placed.

4. Is the NF3ADV secure; can other people access my wireless network?

The NF3ADV comes configured with WPA2-PSK WiFi security enabled. When you first access the Internet, enter 192.168.1.1 into the address bar of a web browser. The wizard will pop up to configure your computer to connect with the wireless security settings of your choice (please see the Quick Start Guide for more information on connecting your data devices to the NF3ADV). Only people you allow access to, will be able to connect to the NF3ADV ensuring your connection is secure and safe.

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

Yes. You can change your NF3ADV settings from the browser user interface by typing 192.168.1.1 into the address bar of your Web browser. You can change the WiFi network name or SSID (Service Set Identifier), WiFi security standard (WPA, WPA2, WEP) and your WiFi password.

6. How do I share my Internet connection, using the NF3ADV, with other users?

Provide the SSID (Service Set Identifier) and WiFi network password of your NF3ADV for any users you want to share your WiFi Internet connection with. Each user will need to select the NF3ADV's SSID, on their WiFi enabled computer or device and enter the network password you provide.

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

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

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

No. The NF3ADV comes equipped with an onboard WLAN antenna.

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

If you have lost your security card, and forgotten the wireless security details (SSID and WiFi network password), there is a label attached to the base of your NF3ADV with all your original security details. If the label is unreadable or has been removed, the WiFi network password can be viewed or reset by logging in to the Management Console using an Ethernet Cable connected to the LAN port of the NF3ADV.

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

If you have forgotten your Management Console password and cannot access the Web user interface, you will need to reset your NF3ADV back to factory default settings. To reset your device press and hold the reset button on the back of your NF3ADV for 10-15 seconds until all the indicator lights on the unit flash to indicate the device is reset. After a reset, use the default WiFi settings (SSID and WPA key) which can be found on the base of your NF3ADV. (Note - this will also reset any custom settings and passwords you may have already set up).

11. Can I use the NF3ADV overseas?

Yes. The NF3ADV is equipped for most overseas xDSL services and connections.

# Appendix A: Tables

Table 1 - Document Revision History .....	2
Table 2 - LED Indicators .....	6
Table 3: Rear and Side Panel Interface Connectors .....	7
Table 4 - LAN Management Default Settings .....	8
Table 5 - WAN Port Default Settings .....	8
Table 6 – WiFi Default Settings.....	8
Table 7 - Web Interface Default Settings.....	8
Table 8: Basic View - Status Settings .....	18
Table 9: Basic View - 2.4GHz Wireless Settings .....	19
Table 10: Basic View - 5.0 GHz Wireless Settings .....	20
Table 11: Basic View - Mobile Broadband Settings .....	21
Table 12: Basic View - ADSL Settings .....	22
Table 13: Advanced - Network Setup - Ethernet WAN setting.....	25
Table 14: Advanced - Network Setup - Wireless WAN.....	26
Table 15: Advanced - Network Setup - ADSL WAN .....	28
Table 16: Advanced - Network Setup – DHCP .....	29
Table 17: Advanced - network Setup - DHCP - Clients List Settings .....	30
Table 18: Advanced - Network Setup - Wireless 2.4 GHz Settings.....	31
Table 19: Advanced - Network Setup - Wireless - WPS Settings.....	32
Table 20: Advanced - Network Setup - 5.0 GHz Wireless Settings.....	33
Table 21: Advanced - Forwarding Rules - Virtual Server Settings .....	35
Table 22: Advanced - Forwarding Rules - Special AP settings .....	36
Table 23: Advanced Security Settings - Packet Filtering Settings.....	38
Table 24: Advanced - Security Settings - Domain Filter settings.....	38
Table 25: Advanced - Advanced Settings - System Log Settings .....	42
Table 26: Advanced - Advanced Settings - Dynamic DNS Settings.....	42
Table 27: Advanced - Advanced Settings - QoS Settings .....	43
Table 28: Advanced - Advanced Settings - SNMP Settings.....	44
Table 29: Advanced - Advanced Settings - System Time Settings.....	46
Table 30: Advanced - Advanced Settings - Adding a Schedule.....	47
Table 31: Advanced - Advanced Settings - IPv6 Settings.....	48
Table 32: Advanced - Advanced Settings - TR-069 Settings .....	49
Table 33: Advanced - Toolbox - Miscellaneous .....	56
Table 35: VoIP/NAS Settings - Call Forward Settings.....	58
Table 36: VoIP/NAS View - Phone Settings - DND Settings .....	59
Table 37: VoIP/NAS View - Phone Settings - Caller ID Settings .....	59
Table 38: Advanced - VoIP/NAS View - Phone Settings - Flash Time Settings.....	60
Table 39: VoIP/NAS View - Phone Settings - Hot Line Settings .....	61
Table 40: Advanced - Phone Setting - DECT Handset Settings .....	62
Table 41: VoIP/NAS View - SIP Settings - Service Domain Settings.....	64
Table 42: VoIP/NAS View - SIP Setting - Codec Settings.....	66
Table 43: VoIP/NAS View - SIP Setting - Other Settings .....	67
Table 44: VoIP/NAS View - Other VoIP Settings - STUN Settings .....	68

Table 45: VoIP/NAS View - NAS Settings - File Sharing Settings.....70

Table 46: VoIP/NAS view - NAS Settings - FTP Settings .....71

Table 47: VoIP/NAS View - NAS Settings - iTunes Server Settings .....72

Table 48: VoIP/NAS Settings - NAS Settings - Download Assistant - FTP .....73

Table 49: VoIP/NAS View - NAS Settings - Download Assistant – HTTP .....74

Table 50: VoIP/NAS Settings - NAS Settings - Download Assistant Settings .....74

Table 51: Additional Product Information - Call Feature Codes Quick Reference .....79

Table 52: NF3ADV Technical Specifications.....81

## Appendix B: Samba Server

For Windows Vista/7

1. Open a web-browser (such as internet Explorer, Firefox or Safari).
2. Type in the address \\ "NetbiosName" "DirectoryName" \ (eg [\\Nas\Storage](#)).

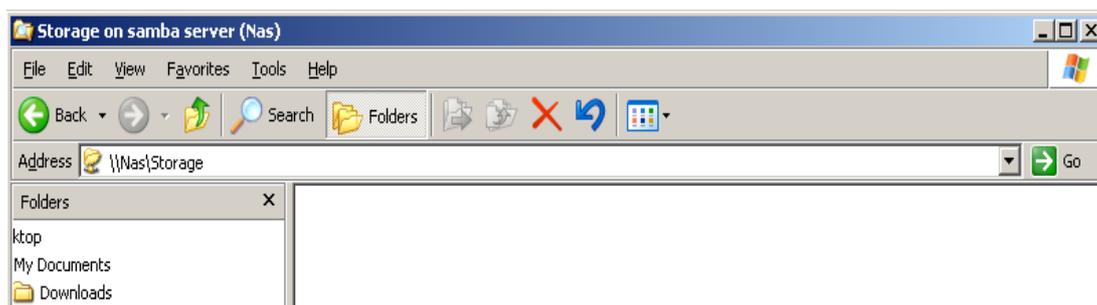


Figure 91: Accessing the USB Drive

Note: When the Access Control Security Level is in Guest mode there is no username and password required to access the USB drive, the user will be able to read/write the folder/files in the USB drive. To secure the access to the drive change the Access Control Security Level to Authorization Mode and configure a username and password.

For MAC OSX

1. Click the finder icon in the Dock.
2. Choose **Connect to Server** from the **Go** menu.
3. In the address field of the Connect to Server dialog, type in the URL Smb:// "NetbiosName"/"DirectoryName" (eg smb://ntc-cpe/ntc-cpe) .

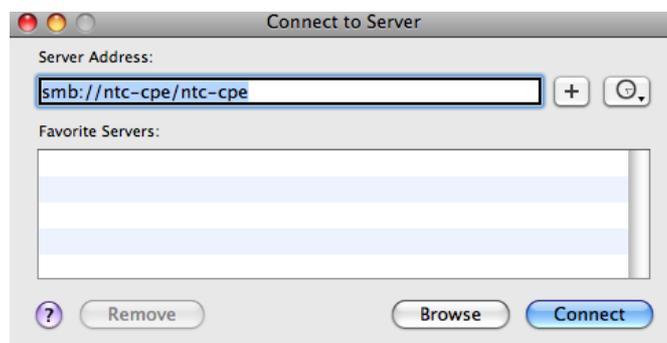


Figure 92: USB Drive Access with Mac

4. Select the Connect button to connect your USB driver.

# Legal & Regulatory Information

## 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 vested in NetComm Wireless Limited (ACN 002490486) (**NetComm**) (or its licensors). This Manual does not transfer any right, title or interest in NetComm Wireless Limited's (or its licensors') intellectual property rights to you.

You are permitted to use this Manual for the sole purpose of using the NetComm Wireless Limited 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 Wireless Limited. 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 incorporates a radio transmitting device, in normal use a separation distance of 20cm will ensure radio frequency exposure levels complies with Australian and New Zealand standards.
3. 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:
  - Change the direction or relocate the receiving antenna.
  - Increase the separation between this equipment and the receiver.
  - Connect the equipment to an alternate power outlet on a different power circuit from that to which the receiver/TV is connected.
  - Consult an experienced radio/TV technician for help.
4. 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 Wireless Limited. 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 Wireless Limited 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 Wireless Limited 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 Wireless 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](http://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.

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 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
6. 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 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 Consumer Protection Laws Section 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 Consumer Protection Laws Section 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 Wireless Limited 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 Head Office  
PO Box 1200, Lane Cove NSW 2066 Australia  
P: +61(0)2 9424 2070 F: +61(0)2 9424 2010  
E: [sales@netcommwireless.com](mailto:sales@netcommwireless.com)  
W: [www.netcommwireless.com](http://www.netcommwireless.com)