

NETCOMM INFRASTRUCTURE SERIES  
In-wall Wireless Access Point

*NetComm*<sup>®</sup>



USER GUIDE

# Table of Contents

<b>1. Introduction.....</b>	<b>4</b>
1.1 Overview .....	4
1.2 Product Features .....	4
1.3 Deployment Topology Diagram .....	5
1.4 Document Conventions .....	5
<b>2. System Overview .....</b>	<b>6</b>
2.1 Package Contents .....	6
2.2 Specification.....	7
<b>3. Installation .....</b>	<b>10</b>
3.1 Panel Function Description .....	10
3.2 Hardware Installation .....	12
3.3 Basic Configuration.....	15
<b>4. Web Interface Configuration.....</b>	<b>26</b>
4.1 System Configuration.....	27
4.1.1 System Information .....	27
4.1.2 Network Settings .....	29
4.1.3 Management Services .....	30
4.2 Wireless .....	31
4.2.1 Virtual AP Overview.....	31
4.2.2 General Settings.....	33
4.2.3 VAP Configuration.....	35
4.2.4 Security Settings .....	36
4.2.5 Repeater Settings .....	39
4.2.6 Advanced Wireless Settings.....	41
4.2.7 Access Control Settings .....	40
4.2.8 Site Survey.....	42
4.3 Firewall .....	44
4.3.1 Layer 2 Firewall Settings.....	44
4.3.2 Firewall Service .....	52
4.3.3 Advanced Firewall Settings .....	50
4.4 Utilities .....	51
4.3.1 Change Password.....	51
4.3.2 Network Utilities .....	52
4.3.3 Configuration Save & Restore .....	53
4.3.4 System Upgrade.....	54
4.3.5 Reboot.....	55
4.5 Status .....	56
4.5.1 System Overview.....	56
4.5.2 Associated Client Status .....	61

4.5.3 Repeater Information .....	62
4.5.4 Event Log .....	61
4.6 Online Help .....	62

# ***1. Introduction***

## **1.1 Overview**

The NP727 In-wall Wireless Access Point is an in-the-wall Wi-Fi IEEE 802.11b/g AP, designed to blend with any office or home interior architecture and furnishings effortlessly.

The compact NP727, with its small form factor can fit in a standard wall outlet box, and hides the wall cutout with its faceplate. Its front panel features LED status indicators and an RJ45 wall jack. It has the interfaces to serve both wireless and wired LAN access. The simplistic yet stylish design of NP727 allows it to blend into a working or a living environment seamlessly.

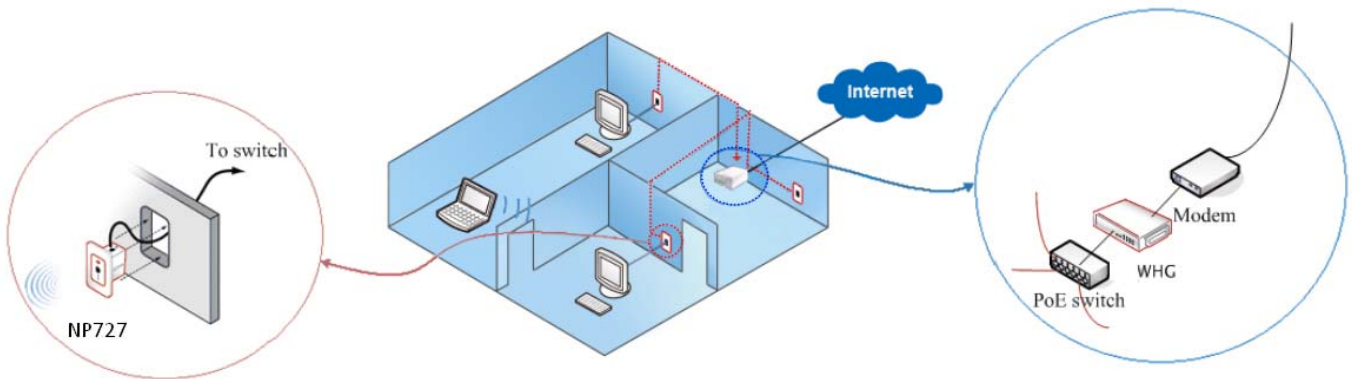
By utilizing Power over Ethernet (PoE), the NP727 comes with an advantage of running fewer cables in the duct. The Power over Ethernet (PoE) LAN port on the NP727 serves as the power feed as well as the wired network feed. Alternatively, it can also be powered via an AC adapter when a PoE switch is not available.

The NP727 is an easy-to-install and cost-effective solution for most indoor wireless deployments, including hotel rooms, apartments, offices, classrooms, libraries, private homes and public kiosks etc.

## **1.2 Product Features**

- Installation friendly housing design for seamless blending into deployed environment
- High speed IEEE 802.11g and backward compatible with 802.11b
- Supporting IEEE 802.3af Power over Ethernet (PoE)
- WDS for extending wireless coverage
- Supporting QoS & 802.11e WMM
- Multiple virtual APs & capable of client isolation
- Business-class WLAN security & client authentication
- Layer 2 firewall for security enhancement

## 1.3 Deployment Topology Diagram



This above deployment scenario illustrates a deployment example.

- Hidden in-the-wall behind faceplate, blending into most interior/architectural designs.
- Keep the style of a simple LAN wall jack while being able to serve both LAN and WLAN devices.
- When managed under a NetComm Internet Access Controller, the combination has been pre-integrated to provide solutions for many applications.

## 1.4 Document Conventions

	Represents essential steps, actions, or messages that should not be ignored.
<b>» Note:</b>	Contains related information that corresponds to a topic.
	Indicates that clicking this button will save the changes you made, but you must reboot the system upon the completion of all configuration settings for the changes to take effect.
	Indicates that clicking this button will clear what you have set before the settings are applied.

## ***2. System Overview***

### **2.1 Package Contents**

The standard package of the NP727 includes:

- NP727 x 1
- Screws & Face Plate Kit x 1
- Product CD-ROM x 1

## 2.2 Specification

### Standard Conformance

- Wireless:
  - (1) IEEE 802.11g (up to 54Mbps)
  - (2) IEEE 802.11b (up to 11Mbps)
- Ethernet:
  - (1) 802.3
  - (2) 802.3u

### Wireless Radio

- Frequency band: 2.4 GHz
- Wireless architecture:
  - (1) AP mode
  - (2) Repeater mode (WDS/Universal Repeater)
- Modulation:
  - (1) 802.11b: DSSS (CCK, DBPSK, DQPSK)
  - (2) 802.11g: OFDM (64-QAM, 16-QAM, QPSK, BPSK)
- Channels:
  - (1) Australia (Channel 1~13)
- Data rate with auto fallback: 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, and 1 Mbps
- Receiver Sensitivity:
  - (1) 802.11g: 54Mbps@-74dBm
  - (2) 802.11b: 11Mbps@-89dBm
- RF output power:
  - (1) EU/AU: 100mW EIRP

\*Note: EIRP= Transmit Power + Antenna Gain
- Antenna: Built-in chip antenna

### Wireless Signal Management

- Max number of ESSIDs (Virtual APs): 8
- Max number of associated clients per AP: 32
- Setting for maximum number of associated clients
- Network policy based on ESSID

### QoS & WMM

- DiffServ / TOS
- IEEE 802.1p/ COS
- IEEE 802.1Q Tag VLAN priority control
- IEEE 802.11e WMM

### Handover & Roaming

- IEEE 802.11f IAPP
- IEEE 802.11i pre-auth (PMKSA cache)
- L2 Roaming

**System Management**

- Web-based administration
- SNMP v1/v2c
- Provides Event Log
- Syslog information support
- Statistics
- Configuration backup and restore
- One-button-click to restore factory default setting
- Firmware upgrade
- Capable of performing RADIUS Accounting and Accounting Update

**Security**

- WEP (64/128/152 bits)
- EAP-TLS + Dynamic WEP
- EAP-TTLS + Dynamic WEP
- PEAP / MS-PEAP + Dynamic WEP
- WPA (PSK + TKIP)
- WPA (802.1X certification + TKIP)
- 802.11i WPA2 (PSK + CCMP / AES)
- 802.11i WPA2 (802.1X certification + CCMP / AES)
- Setting for TKIP / CCMP / AES key's refreshing period
- Hidden ESSID support
- MAC Address filtering (MAC ACL)
- MAC authentication with RADIUS servers
- Maximum number of registered RADIUS servers: 2

**Built-in Servers & Client Interfaces to Other Services**

- DHCP client
- DNS client
- Syslog client
- RADIUS client
- SNMP v1/v2c read & write client

**Physical and Power**

- Form factor: In-Wall type
- Dimensions (W x H x D):
  - Center unit: 1.88" x 3.07" x 3.07" (48mm x 78 mm x 78 mm)
  - Faceplate: 2.95" x 4.72" x 0.35" (75mm x 120 mm x 9 mm)
- Weight: 0.42 lbs (0.19 kg)
- PoE port: IEEE 802.3af
- Power adaptor (Optional, not included in the package):
  - AC Input: 100~240 VAC, 50~60 Hz
  - DC Output: 12VDC, 1.5A

**Connectors and Display**

- LAN Port: 1 x 10/100 Base-T Ethernet



- PoE Port: 1 × 10/100 Base-T Ethernet
- LED Indicators: 1 × Power, 1 × LAN, 1 × WLAN

**Environment**

- Operation Temperature: -20 ~ 50 °C
- Storage Temperature: -20 ~ 70 °C
- Operation Humidity: 10% ~ 80% Non-condensing
- Storage Humidity: 5% ~ 90% Non-condensing

**Certifications**

- FCC, CE
- RoHS compliant

## 3. Installation

### 3.1 Panel Function Description

On the front panel of the NP727, there are three LEDs that are used to indicate the **POWER** status, the **WLAN** status, and the link status of the **LAN** port. On the front panel, there are: one **RESET** button and one **LAN** port. The antenna is built-in chip antenna.

#### Front Panel



#### 1. RESET Button:

- Press the button to restart the system.
- Press the button for more than 30 seconds to reset the system to default settings.

#### 2. LAN:

- The LAN port is for connection with wired networks.

#### LED status indication:

#### 3. LAN

- OFF indicates no connection; ON indicates connection; BLINKING indicates transmitting data.

#### 4. WLAN

- Green LED ON indicates system ready.

#### 5. Power

- Green LED On indicates power on; OFF indicates power off.

**In-Wall Panel****1. POWER SOCKET:**

- Attach the power adapter here, it accepts 12VDC 1.5A.

**2. PoE (LAN):**

- The LAN port is for connection with wired networks or PoE Switch.

## 3.2 Hardware Installation

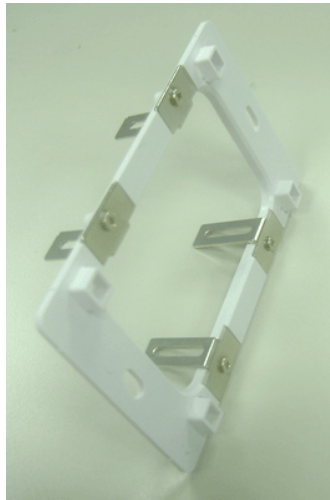
Please follow the steps mentioned below to install the hardware of the NP727:

Before the installation, assemble the following parts accordingly for the in-wall placement.

**Step 1:** Unpack the box and remove the cover and the frame.



**Step 2:** Lock the screw correctly to the frame.



**Step 3:** Slide the frame from the two sides to the front until locked to the fixed point.



**Step 4:** Cover it with faceplate.



**1. Place the NP727 in the best location.**

The best location for the NP727 is usually at the center of your wireless network.

**2. Connect the NP727 to your network device.**

Connect one end of an Ethernet cable to the LAN port of THE NP727 and the other end of the cable to a switch, a router or a hub. The NP727 is then connected to your existing wired LAN network.

**3. There are two ways to supply power over to THE NP727.**

(1) Connect the power adapter to the NP727 power socket.

(2) THE NP727 PoE (LAN) port is capable of transmitting DC currents via its PoE (LAN) port. Connect an IEEE 802.3af-compliant PSE device, e.g. a PoE switch, to the PoE (LAN) port of THE NP727 with the Ethernet cable.

Now, the hardware installation is completed.

### 3.3 Basic Configuration

The NP727 supports web-based configuration. Upon the completion of the hardware installation, the NP727 can be configured through a PC by using its web browser such as Mozilla Firefox 2.0 or Internet Explorer version 6.0 and the above.

The default values of the LAN IP address and subnet mask of the NP727 are:

*IP Address: 192.168.27.1*

*Subnet Mask: 255.255.255.0*

- To access the web management interface, connect the administrator PC to the LAN port of the NP727 via an Ethernet cable. Then, set a static IP address on the same subnet mask as the NP727 in the TCP/IP of your PC, such as the following example (Please note that the IP address used shall not be duplicated with the IP address of other devices within the same network.):

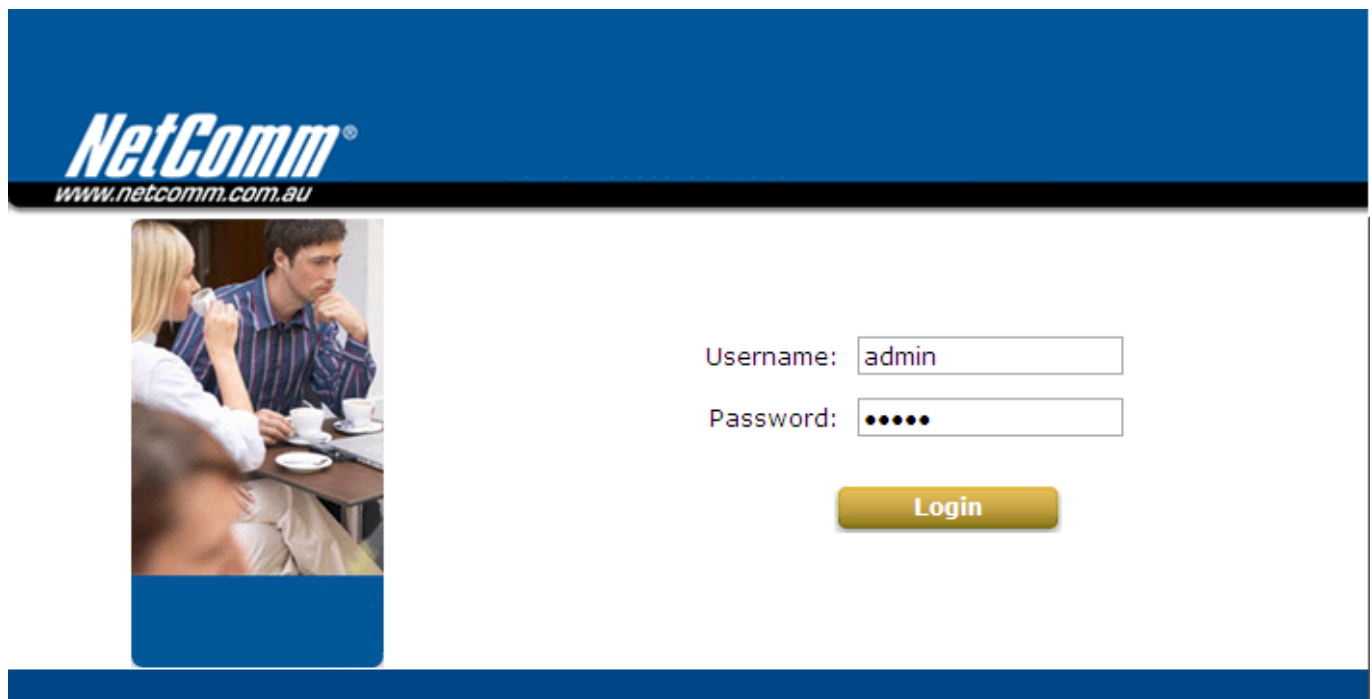
*IP Address: 192.168.1.100*

*Subnet Mask: 255.255.255.0*

- Launch the web browser on your PC by entering the IP address of the NP727 (**http://192.168.27.1**) in the address field, and then press **Enter**. The following Administrator Login Page will then appear. Enter "**admin**" for both the *User name* and *Password* fields, and then click **Login** to log in.

*User name: "admin"*

*Password: "admin"*



**NetComm**  
www.netcomm.com.au

Username:

Password:

**Login**

- After a successful login into the NP727, a **System Overview** page of the web management interface will appear. To logout, simply click on the **Logout** button in the upper right hand corner of the interface to return to the Administrator Login Page.

The screenshot displays the NetComm NP727 web interface. At the top, the NetComm logo and website URL (www.netcomm.com.au) are on the left, and the page title "NP727 - In-wall Wireless Access Point" is in the center. On the right, there are navigation links for Home, Logout, and Help. Below the header is a main menu with buttons for System, Wireless, Firewall, Utilities, and Status. The Status button is highlighted. Underneath, there are sub-tabs for Overview, Clients, Repeater, and Event Log. The main content area shows the breadcrumb "Home > Status > System Overview" and the title "System Overview".

The System Overview page is divided into four main sections:

- System:** A table listing system details:
 

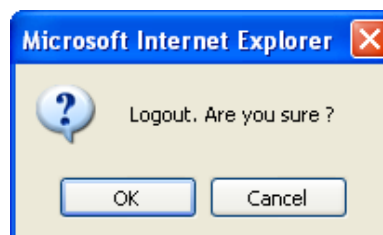
System Name	NP727
Firmware Version	1.00.00
Build Number	1.5-1.2418
Location	Sydney, Australia
Site	EN-AU
Device Time	2000/01/01 11:05:40
System Up Time	0 days, 0:05:40
- Radio Status:** A table listing radio configuration:
 

MAC Address	00:60:64:2D:B6:44
Band	802.11b+g
Channel	6
TX Power	Highest
- LAN Interface:** A table listing network interface details:
 

MAC Address	00:60:64:2D:B6:43
IP Address	192.168.27.1
Subnet Mask	255.255.255.0
Gateway	192.168.27.254
- AP Status:** A table listing active profiles:
 

Profile Name	BSSID	ESSID	Security Type	Online Clients
VAP-1	00:60:64:2D:B6:..	NetComm Wirele..	None	0

- To logout, simply click on the **Logout** button at the upper right hand corner of the interface to return to the Administrator Login Page.





Please refer to the following steps to complete the basic configuration:

**Step 1. Change Administrator's Password:**

The screenshot shows the web interface for changing the administrator password. At the top, there are navigation buttons for System, Wireless, Firewall, Utilities (highlighted with a red box), and Status. Below these is a sub-menu with 'Change Password' (highlighted with a red box), Network Utilities, Config Save & Restore, System Upgrade, and Reboot. The main content area has a breadcrumb trail: Home > Utilities > Change Password. The title is 'Change Password'. The form contains the following fields:

- Name : admin
- Old Password : [masked]
- New Password : [masked] \*up to 32 characters
- Re-enter New Password : [masked]

At the bottom of the form are two buttons: 'SAVE' and 'CLEAR'.

- Click on the **Utilities** button, and then select the **Admin Password** tab.
- Enter a new password with length up to 32 characters, and then click **SAVE** to save the new password.

---

➤ **Note:** Click **SAVE** to save the changes, but you must reboot the system upon the completion of all configuration settings for the changes to take effect. When clicking **SAVE**, the following message will appear: **“Some modifications have been saved and will take effect after Reboot.”**

---

**Step 2. Configure Wireless Settings**

System Wireless Firewall Utilities Status

VAP Overview General VAP Config Security Repeater Advanced Access Control Site Survey

Home > Wireless > General

### General Settings

**Band**: 802.11b+802.11g

**Super G**:  Bursting  Fast Frames  Dynamic Turbo

**Short Preamble**:  Disable  Enable

**Channel**: 1

**Max Transmit Rate**: Auto

**Transmit Power**: Auto

**ACK Timeout**: 0 \*(0 - 255, 0:Auto, Unit:4 micro seconds)

SAVE CLEAR

- Click on the **Wireless** button, and then select the **General** tab.
- Determine the *Band* and *Channel* settings:  
Select your preferred *Band* and *Channel* for your wireless connection. For example, select *802.11b+802.11g* for the band and *Auto* for the channel.

**Step 3. Configure VAP (Virtual Access Point) Profile Settings**

Home > Wireless > VAP Config

### VAP Configuration

Profile Name :

VAP :  Disable  Enable

Profile Name :

ESSID :

VLAN ID :  Disable  Enable

VLAN ID :  \*( 1 - 4094 )

The NP727 Supports up to 8 virtual APs. By default, only 1 VAP is enabled.

- Configure VAP profile settings:
  - (a) Select the **VAP Config** tab to configure the settings for each VAP.
  - (b) An administrator can enable or disable specific VAP from the drop-down list box of *Profile Name*.
- Check VAP status :
 

After finishing the above settings, the status of enabled Virtual APs shall be reflected on the **Virtual AP Overview** page.

Home > Wireless > VAP Overview

### VAP Overview

VAP No.	ESSID	State	Security Type	MAC ACL	Advanced Settings
1	VAP-1	Enabled	None	Disabled	Edit
2	VAP-2	Disabled	None	Disabled	Edit
3	VAP-3	Disabled	None	Disabled	Edit
4	VAP-4	Disabled	None	Disabled	Edit
5	VAP-5	Disabled	None	Disabled	Edit
6	VAP-6	Disabled	None	Disabled	Edit
7	VAP-7	Disabled	None	Disabled	Edit
8	VAP-8	Disabled	None	Disabled	Edit

**Step 4 (Advanced Optional). Choose Security Type**

The screenshot displays the NP727 user interface. At the top, there are five main navigation buttons: System, Wireless, Firewall, Utilities, and Status. The Wireless button is highlighted with a red border. Below these are several sub-tabs: VAP Overview, General, VAP Config, Security, Repeater, Advanced, Access Control, and Site Survey. The Security tab is also highlighted with a red border. The breadcrumb trail shows 'Home > Wireless > Security'. The main heading is 'Security Settings'. Below this, there is a 'Profile Name' dropdown menu set to 'VAP-1'. The 'Security Type' dropdown menu is open, showing a list of options: None, WEP, 802.1X, WPA-PSK, and WPA-RADIUS. The 'None' option is currently selected. There are two yellow buttons at the bottom: one is partially obscured by the dropdown menu, and the other is labeled 'CLEAR'.

- Click on the **Wireless** button.
- Select the **Security** tab to configure your preferred security types:  
*(The following uses “VAP-1” security configuration as an example.)*

1. Choose "WEP" as its *Security Type*:

When **WEP** is selected, provide the desired **Authentication**, **key length**, **format**, **index** and **values**.

VAP Overview   General   VAP Config   **Security**   Repeater   Advanced   Access Control   Site Survey

Home > Wireless > Security

## Security Settings

Profile Name : VAP-1 ▼

Security Type : WEP ▼

Note! The WEP keys are global setting for all virtual APs. The key value will apply to all VAPs.

802.11 Authentication:  Open System    Shared Key    Auto

WEP Key Length :  64 bits    128 bits    152 bits

WEP Key Format :  ASCII    Hex

WEP Key Index : 1 ▼

WEP Keys :

1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>

2. Choose "802.1X" as its *Security Type*:

When **802.1X** authentication is selected, provide the desired **WEP key length** and the corresponding settings of RADIUS server.

VAP Overview General VAP Config Security Repeater Advanced Access Control Site Survey

Home > Wireless > Security

## Security Settings

Profile Name : VAP-1

Security Type : 802.1X

Dynamic WEP :  Disable  Enable

WEP Key Length :  64 bits  128 bits

Rekeying Period : 300 second(s)

**Primary RADIUS Server :**

Host :  \*( Domain Name / IP Address )

Authentication Port : 1812 \*

Secret Key :

Accounting Service :  Disable  Enable

Accounting Port : 1813 \*

Accounting Interim Update Interval : 60 second(s)\*

**Secondary RADIUS Server :**

Host:  ( Domain Name / IP Address )

Authentication Port: 1812

Secret Key:

Accounting Service:  Disable  Enable

Accounting Port: 1813

Accounting Interim Update Interval: 60 second(s)

3. Choose “WPA-PSK” as its *Security Type*:

When **WPA-PSK** is selected, provide the desired **pre-shared key** and **Cipher Suite**.

VAP Overview | General | VAP Config | **Security** | Repeater | Advanced | Access Control | Site Survey

Home > Wireless > Security

### Security Settings

Profile Name : VAP-1

Security Type : WPA-PSK

Cipher Suite : TKIP (WPA)

Pre-shared Key Type :  PSK(Hex)\*( 64 chars )  Passphrase\*( 8 - 63 chars )

Pre-shared Key :

Group Key Update Period: 600 second(s)

4. Choose “WPA-RADIUS” as its *Security Type*:

When **WPA-RADIUS** is selected, provide the **Cipher** type and the corresponding settings of RADIUS server.

VAP Overview | General | VAP Config | **Security** | Repeater | Advanced | Access Control | Site Survey

Home > Wireless > Security

### Security Settings

Profile Name : VAP-1

Security Type : WPA-RADIUS

Cipher Suite : TKIP (WPA)

Group Key Update Period: 600 second(s)

**Primary RADIUS Server :**

Host :  \*( Domain Name / IP Address )

Authentication Port : 1812 \*

Secret Key :

Accounting Service :  Disable  Enable

Accounting Port : 1813 \*

Accounting Interim Update Interval : 60 second(s) \*

**Secondary RADIUS Server :**

Host:  ( Domain Name / IP Address )

Authentication Port: 1812

Secret Key:

Accounting Service:  Disable  Enable

Accounting Port: 1813

Accounting Interim Update Interval: 60 second(s)

**Step 5. Configure WDS (Wireless Distribution System) Settings**

Home > Wireless > Repeater Config

## Repeater Settings

Repeater Type :

Security type :

MAC Address :

Item	MAC Address	Enable	<input type="button" value="Delete"/>
1			
2			
3			
4			

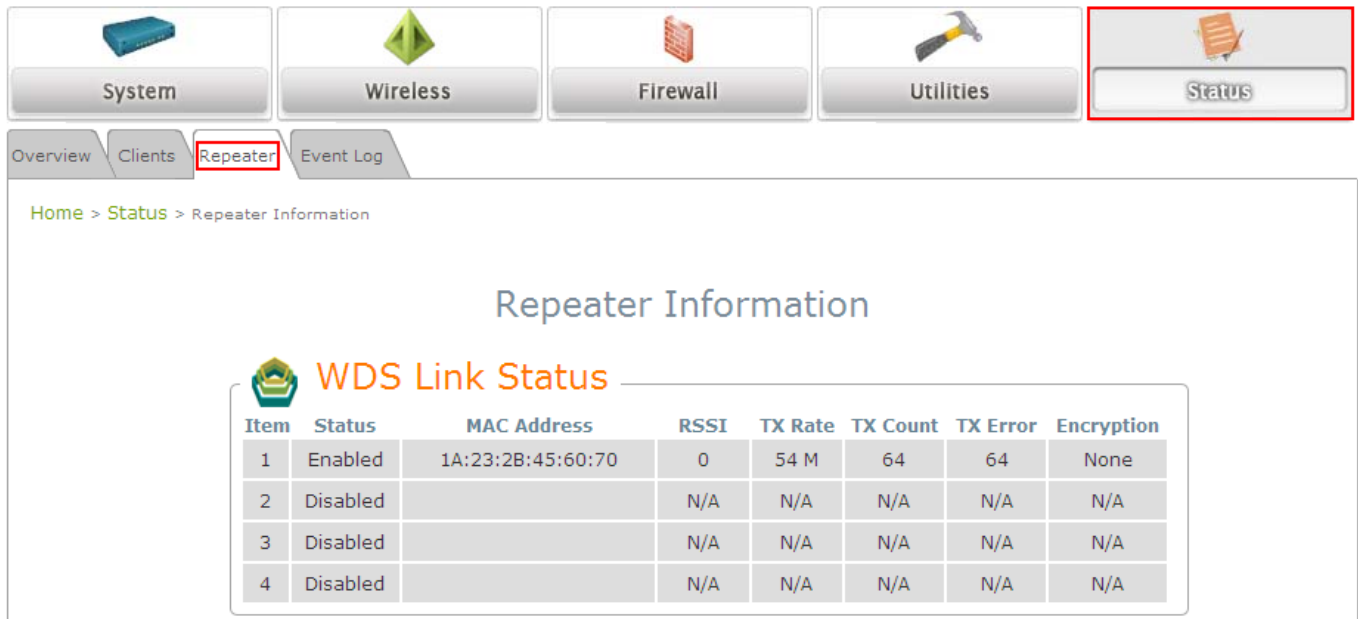
To extend its wireless coverage, the NP727 is capable of creating WDS links for connection to other WDS-capable APs (peer APs). The NP727 supports up to 4 WDS links; by default, all WDS profiles are disabled.

- Click on the **Repeater** tab.
- Select **WDS** from the drop-down list of Repeater Type.
- Configure WDS link parameters:
  - (a) Select preferred *Security Type*
  - (b) *Enter MAC Address of Remote AP* (peer AP) and click Add
- To configure peer AP(s):

After completing the WDS settings for the NP727 (functioning as a “primary WDS station”), you must also configure the settings of its peer AP(s).

If you use another NP727 as the peer AP, simply repeat the above-mentioned steps with the MAC Address of the primary WDS station for setting WDS link parameters of the peer AP(s).



**Step 5 (CONT). Check WDS Link Status**


Home > Status > Repeater Information

### Repeater Information

#### WDS Link Status

Item	Status	MAC Address	RSSI	TX Rate	TX Count	TX Error	Encryption
1	Enabled	1A:23:2B:45:60:70	0	54 M	64	64	None
2	Disabled		N/A	N/A	N/A	N/A	N/A
3	Disabled		N/A	N/A	N/A	N/A	N/A
4	Disabled		N/A	N/A	N/A	N/A	N/A

- Click on the **Status** button.
- Select the **Repeater** tab.
- Check the signal strength of WDS link(s) :

Upon the completion of Step 5, there shall be *RSSI* displayed on the **WDS Link Status**. If the RSSI is shown as *N/A*, check if the wiring is properly connected and please ensure the accurate execution of Step 5 as described above.

**Congratulations!**

The NP727 is now installed and configured successfully.



- *It is strongly recommended to make a backup copy of configuration settings.*
- *After the NP727's network configuration is completed, please remember to change the IP Address of your PC Connection Properties back to its original settings in order to ensure that your PC functions properly in its real network environments.*

### 3. Web Interface Configuration

This chapter will guide you through further detailed settings. The following table shows all the UI functions of the NP727 In-wall Wireless Access Point. In the web management interface, there are two main interface areas: **Main Menu** and **Working Area**. The **Working Area** occupies the largest area of the web management interface, displayed in the center of the interface. It is also referred as **the configuration page**. The web management interface is the page where status is displayed, control is issued and parameters are configured. The **Main Menu**, on the top of the web management interface, allows the administrator to traverse to various management functions of this system. The management functions are grouped into branches: **System**, **Wireless**, **Firewall**, **Utilities**, and **Status**.

OPTION	FUNCTION
<b>System</b>	System Information
	Network Settings
	Management Services
<b>Wireless</b>	Virtual AP Overview
	General Settings
	VAP Configuration
	Security Settings
	Repeater Settings
	Advanced Wireless Settings
	Access Control Settings
	Site Survey
<b>Firewall</b>	Layer 2 Firewall Settings
	Firewall Service
	Advanced Firewall Settings
<b>Utilities</b>	Change Password
	Network Utilities
	Configuration Save & Restore
	System Upgrade
<b>Status</b>	Reboot
	System Overview
	Associated Client Status
	Repeater Information
	Event Log

---

On each and every configuration page, you may click **SAVE** to save the changes, but you must reboot the system upon the completion of all configuration settings for the changes to take effect.

- **Note:** When clicking **SAVE**, the following message will appear: **“Some modifications have been saved and will take effect after Reboot.” <All on-line users will be disconnected during reboot/restart.>**
-

## 4.1 System Configuration

This section includes the following functions: **System Information**, **Network Settings** and **Management Services**.

### 4.1.1 System Information

System Information   Network   Management

Home > System > General

### System Information

**Name :**  \*

**Description :**

**Location :**

### Time

**Device Time :** 2000/01/01 11:22:19

**Time Zone :**

**Time :**  Enable NTP    Manually set up

**Set Date :**  Year  Month  Day

**Set Time :**  Hour  Min  Sec

- **System Information**

For the purpose of maintenance, it is required to specify the system name, its location and corresponding basic parameters. Fields such as *Name*, *Description* and *Location* are used for mnemonic purpose. It is recommended to have different values in each AP.

- *Name*: The system name used to identify this system
- *Description*: Further information about this installation
- *Location*: The geographic location

- **Time**

Synchronize the system time either by using NTP server or by manual setup. When NTP server is used, the information of at least one NTP server must be provided. If FQDN (full qualified domain name) is used as the IP address of NTP server, the DNS server must also be activated (please refer to **4.1.2 Network Settings**).

- *Device Time*: Current system time
- *Time Zone*: Select a time zone from the drop-down list box

- *Synchronization*: There are two options of setting system time

1) *Enable NTP*:

By selecting *Enable NTP*, the NP727 can synchronize its system time with the NTP server automatically. While this method is chosen, at least one NTP server's IP address should be provided. It is recommended to provide the IP address of both NET Server 1 and 2 in case of any NTP service failure.

### Time

Device Time : 2000/01/01 11:22:19

Time Zone : (GMT+10:00)Canberra,Melbourne,Sydney ▼

Time :  Enable NTP     Manually set up

NTP Server 1 : 0.netcomm.pool.ntp.org \*\*

NTP Server 2 : 1.netcomm.pool.ntp.org

2) *Manually set up*:

By selecting *manually set up*, the administrator can manually set the system date and time.

### Time

Device Time : 2000/01/01 11:22:19

Time Zone : (GMT+10:00)Canberra,Melbourne,Sydney ▼

Time :  Enable NTP     Manually set up

Set Date : ---- ▼ Year -- ▼ Month -- ▼ Day

Set Time : -- ▼ Hour -- ▼ Min -- ▼ Sec



Unless the Internet connection is unavailable, it is recommended to use NTP server for time synchronization.

## 4.1.2 Network Settings

System Information | Network | Management

Home > System > Network Interface

### Network Settings

**Mode :**  Static  DHCP

IP Address :  \*

Netmask :  \*

Default Gateway :  \*

Primary DNS Server :  \*

Alternate DNS Server :

**Layer2 STP :**  Disable  Enable

**SAVE** **CLEAR**

This page is for setting up the wired internet connections. There are two methods of IP configuration available with the NP727. LAN interface configuration determines the way to obtain the IP address, either by DHCP or by manual setup.

- **Mode:** Determine the way to obtain the IP address, by DHCP or Static.
  - *DHCP client:* This option can be selected when there is a DHCP server located on your wired/wireless network. Please make sure the network connection settings are correct and the network connection is active.
  - *Static setting:* When this option is selected, the administrator can set the parameters manually. Enter the *IP Address, Netmask* and *Gateway* provided by your ISP.
- **Primary and Secondary DNS Server:** If any host information is given in FQDN format (full qualified domain name), ensure at least one of these DNS (Domain Name Service) server IP is correct.
- **Layer 2 STP:** When the system is configured to bridge several networks (WDS mode), this STP (Spanning Tree Protocol) function must be enabled to avoid a loop condition and to obtain the best data path for network communication optimization purpose.

Broadcasting storm may occur in a multi-switch environment where broadcast packets are forwarded in an endless loop between switches. A broadcast storm can consume up all available CPU resources and the Internet and Ethernet bandwidth. Enabling the STP function can prevent the system from encountering such chaos.

### 4.1.3 Management Services

System Information Network Management

Home > System > Management Services

## Management Services

**VLAN for Management:**  Disable  Enable  
 VLAN ID :  \*( 1 - 4094 )

**SNMP Configuration :**  Disable  Enable  
 Community String :  
 Read :   
 Write :   
 Trap :  Disable  Enable  
 Server IP :

**System Log :**  Disable  Enable  
 SYSLOG Server IP :   
 Server Port :   
 SYSLOG Level :

**Auto Reboot :**  Disable  Enable  
 Reboot Time :

**SAVE** **CLEAR**

For the purpose of easy maintenance, SNMP (Simple Network Management Protocol) and remote syslog services are provided in the NP727. The system will be managed remotely in a centralized manner.

- **VLAN for Management:** The management traffic from the device can be tagged with VLAN ID. If the option is enabled, the VLAN ID can be chosen from 1 to 4094.
- **SNMP Configuration:** By enabling SNMP service, the remote SNMP manager can obtain the NP727's system status.
  - *Community String:* Specify the password for *Read* and *Write*.
  - *Trap:* Enable or Disable the feature. When enabled, events on Cold Start, Interface Up & Down and Association & Disassociation can be reported to an assigned management station with specified *Server IP Address*.
- **System Log:** By enabling this service, specify an external syslog server to accept syslog messages from the NP727 remotely. Thus, by reading the syslog message in the remote server, the administrator can review activities of all installed the NP727s in the network.
  - *Server Port:* The port number of the server.
  - *Log Level:* Select the desired level of received events from the drop-down list box.

## 4.2 Wireless

This section includes the following functions: **VAP Overview**, **General**, **VAP Configuration**, **Security**, **Repeater**, **Advanced**, **Access Control**, and **Site Survey**. The NP727 supports up to eight Virtual Access Points (VAPs). Each VAP can have its own settings including ESSID, VLAN ID, security settings, etc. Such VAP capability enables different levels of service to meet actual requirements.

### 4.2.1 Virtual AP Overview

An overall status is collected in this page, including *Enable/Disable State*, *Security Type*, *MAC ACL* state, and *Advanced Settings*. The NP727 has 8 VAPs; each has its own settings. In this table, please click on the hyperlink for further configuration of each VAP respectively.

VAP No.	ESSID	State	Security Type	MAC ACL	Advanced Settings
1	VAP-1	<a href="#">Enabled</a>	<a href="#">None</a>	<a href="#">Disabled</a>	<a href="#">Edit</a>
2	VAP-2	<a href="#">Disabled</a>	<a href="#">None</a>	<a href="#">Disabled</a>	<a href="#">Edit</a>
3	VAP-3	<a href="#">Disabled</a>	<a href="#">None</a>	<a href="#">Disabled</a>	<a href="#">Edit</a>
4	VAP-4	<a href="#">Disabled</a>	<a href="#">None</a>	<a href="#">Disabled</a>	<a href="#">Edit</a>
5	VAP-5	<a href="#">Disabled</a>	<a href="#">None</a>	<a href="#">Disabled</a>	<a href="#">Edit</a>
6	VAP-6	<a href="#">Disabled</a>	<a href="#">None</a>	<a href="#">Disabled</a>	<a href="#">Edit</a>
7	VAP-7	<a href="#">Disabled</a>	<a href="#">None</a>	<a href="#">Disabled</a>	<a href="#">Edit</a>
8	VAP-8	<a href="#">Disabled</a>	<a href="#">None</a>	<a href="#">Disabled</a>	<a href="#">Edit</a>

- **State:** The hyperlink showing *Enable* or *Disable* connects to the screen of **VAP Configuration**.

VAP Overview	General	VAP Config	Security	Repeater	Advanced	Access Control	Site Survey
Home > Wireless > VAP Config							
<h3>VAP Configuration</h3>							
Profile Name : <input type="text" value="VAP-1"/>							
VAP : <input type="radio"/> Disable <input checked="" type="radio"/> Enable							
Profile Name : <input type="text" value="VAP-1"/>							
ESSID : <input type="text" value="VAP-1"/>							
VLAN ID : <input checked="" type="radio"/> Disable <input type="radio"/> Enable							
VLAN ID : <input type="text"/> *( 1 - 4094 )							

- **Security Type:** The hyperlink showing security type connects to the screen of Security Settings.

VAP Overview General VAP Config Security Repeater Advanced Access Control Site Survey

Home > Wireless > Security

## Security Settings

Profile Name : VAP-1 ▼

Security Type : None ▼

- **MAC ACL:** The hyperlink showing *Allow* or *Disable* connects to the screen of **Access Control Settings**.

VAP Overview General VAP Config Security Repeater Advanced Access Control Site Survey

Home > Wireless > Access Control

## Access Control Settings

Profile Name : VAP-1 ▼

Maximum Number of Clients : 32 \*( Range: 1 ~ 32 )

Access Control Type : Disable Access Control ▼

- **Advanced Settings:** The hyperlink of advanced settings connects to the screen of **Advanced Wireless Settings**.

VAP Overview General VAP Config Security Repeater Advanced Access Control Site Survey

Home > Wireless > Advanced

## Advanced Wireless Settings

Profile Name : VAP-1 ▼

Beacon Interval : 100 \*(100 - 500ms )

RTS Threshold : 2346 \*(1 - 2346)

Fragment Threshold : 2346 \*(256 - 2346)

Broadcast SSID :  Disable  Enable

Wireless Station Isolation :  Disable  Enable

WMM :  Disable  Enable

IAPP :  Disable  Enable

802.11g Protection :  Disable  Enable



## 4.2.2 General Settings

Home > Wireless > General

### General Settings

Band :

Super G :  Bursting  Fast Frames  Dynamic Turbo

Short Preamble :  Disable  Enable

Channel :

Max Transmit Rate :

Transmit Power :

ACK Timeout :  \*(0 - 255, 0:Auto, Unit:4 micro seconds)

- **Band:** The operating wireless frequency band of this system. Select one frequency band from *Disable*, *802.11b*, *802.11g* or mixed mode *802.11b+802.11g*.
- **Super G:** Options of Bursting, Fast Frames, and Dynamic Turbo can be selected to boost wireless throughput.
- **Short Preamble:** This option can be turned on to enable Short-Preamble frames.
- **Channel:** Select the appropriate channel from the drop-down list box to correspond with your network settings, for example, Channel 1-13 in Australia, or choose the default *Auto*.
- **Max Transmit Rate:** Select transmit rate from *1 M* to *54 M* or *Auto*.
- **Transmit Power:** Select from the lowest to highest power level or choose *Auto*.
- **ACK Timeout:** When packet loss is increasing over longer distance, ACK Timeout can be used to alleviate this issue.

The RF settings in this page will be applied to all VAPs.

Under normal circumstances, the available RF configurations are illustrated as below:

<b>Mode</b>	<b>Channel</b>	<b>Rate</b>	<b>Power</b>
<i>Disable</i>	<i>NA</i>	<i>NA</i>	<i>NA</i>
<i>802.11b</i>	<i>1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13</i>	<i>Auto, 1M, 2M, 5.5M, 11M</i>	<i>Auto, Lowest, Low, Medium, High, Highest</i>
<i>802.11g</i>	<i>1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13</i>	<i>Auto, 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M</i>	
<i>802.11b+802.11g</i>	<i>1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13</i>	<i>Auto, 1M, 2M, 5.5M, 11M, 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M</i>	

## 4.2.3 VAP Configuration

VAP Overview | General | **VAP Config** | Security | Repeater | Advanced | Access Control | Site Survey

Home > Wireless > VAP Config

### VAP Configuration

Profile Name :

VAP :  Disable  Enable

Profile Name :

ESSID :

VLAN ID :  Disable  Enable

VLAN ID :  \*( 1 - 4094 )

To enable each VAP in the NP727, the administrator must configure each VAP manually. The settings of each VAP are collected as its profile.

- **Enable VAP:** Enable or disable VAP function.
- **Profile Name:** The profile name of each VAP for identity/management purpose.
- **ESSID:** ESSID (Extended Service Set ID) indicates a unique SSID used by a client device to associate with a specified VAP. ESSID determines the service level assigned to a client.
- **VLAN ID:** The NP727 supports tagged VLANs (virtual LANs). To enable VLAN function, each VAP must have a unique VLAN ID; valid values are ranged from 1 to 4094.

## 4.2.4 Security Settings

The NP727 supports various user authentication and data encryption methods in each VAP profile. Thus the administrator can depend on the need to provide different service levels to clients. The security type includes **None**, **WEP**, **802.1X**, **WPA-PSK**, and **WPA-RADIUS**.

- **None:** No authentication required. This is the default setting as shown in the following figure.

The screenshot shows the 'Security Settings' page for profile 'VAP-1'. The 'Security Type' is set to 'None'. The breadcrumb trail is 'Home > Wireless > Security'.

- **WEP:** Support key length of 64/128/152 bits.

The screenshot shows the 'Security Settings' page for profile 'VAP-1' with 'Security Type' set to 'WEP'. The '802.11 Authentication' is set to 'Open System', 'WEP Key Length' is '64 bits', and 'WEP Key Format' is 'ASCII'. A note states: 'Note! The WEP keys are global setting for all virtual APs. The key value will apply to all VAPs.' There are four input fields for 'WEP Keys' numbered 1 through 4.

- **802.1X:** Provide RADIUS authentication and enhanced WEP.

VAP Overview General VAP Config **Security** Repeater Advanced Access Control Site Survey

Home > Wireless > Security

## Security Settings

Profile Name : VAP-1

Security Type : 802.1X

Dynamic WEP :  Disable  Enable

WEP Key Length :  64 bits  128 bits

Rekeying Period : 300 second(s)

Primary RADIUS Server :

Host :  \*( Domain Name / IP Address )

Authentication Port : 1812 \*

Secret Key :

Accounting Service :  Disable  Enable

Accounting Port : 1813 \*

Accounting Interim Update Interval : 60 second(s)\*

Secondary RADIUS Server :

Host:  ( Domain Name / IP Address )

Authentication Port: 1812

Secret Key:

Accounting Service:  Disable  Enable

Accounting Port: 1813

Accounting Interim Update Interval: 60 second(s)

- **WPA-PSK:** Provide shared key authentication in WPA data encryption.

VAP Overview General VAP Config **Security** Repeater Advanced Access Control Site Survey

Home > Wireless > Security

## Security Settings

Profile Name : VAP-1

Security Type : WPA-PSK

Cipher Suite : TKIP (WPA)

Pre-shared Key Type :  PSK(Hex)\*( 64 chars )  Passphrase\*( 8 - 63 chars )

Pre-shared Key :

Group Key Update Period: 600 second(s)

- **WPA-RADIUS:** Authenticate users by RADIUS and provide WPA data encryption.

VAP Overview   General   VAP Config   **Security**   Repeater   Advanced   Access Control   Site Survey

Home > Wireless > Security

## Security Settings

**Profile Name :** VAP-1 ▼

**Security Type :** WPA-RADIUS ▼

**Cipher Suite :** TKIP (WPA) ▼

**Group Key Update Period:** 600 second(s)

**Primary RADIUS Server :**

Host :  \*( Domain Name / IP Address )

Authentication Port : 1812 \*

Secret Key :

Accounting Service :  Disable    Enable

Accounting Port : 1813 \*

Accounting Interim Update Interval : 60 second(s)\*

**Secondary RADIUS Server :**

Host:  ( Domain Name / IP Address )

Authentication Port: 1812

Secret Key:

Accounting Service:  Disable    Enable

Accounting Port: 1813

Accounting Interim Update Interval: 60 second(s)

## 4.2.5 Repeater Settings

VAP Overview General VAP Config Security Repeater Advanced Access Control Site Survey

Home > Wireless > Repeater Config

### Repeater Settings

Repeater Type :

None  
WDS  
Universal Repeater

The NP727 supports either WDS or Universal Repeater as options of repeater types; selecting None will turn off this function.

### ◆ WDS

VAP Overview General VAP Config Security Repeater Advanced Access Control Site Survey

Home > Wireless > Repeater Config

### Repeater Settings

Repeater Type :

Security type :

MAC Address :

Item	MAC Address	Enable	Delete
1	1A:23:2B:45:60:70	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2			
3			
4			

If WDS is chosen, the NP727 will support 4 WDS links to its peer APs. Security Type (None, WEP, or TKIP/AES) can be configured to decide which encryption is to be used for WDS connections respectively. Please fill in remote peer's MAC address and click Add to add this peer into WDS list. After the settings have been configured, please click SAVE to proceed; CLEAR button is used to clear the contents in the above WDS connection list.

## ◆ Universal Repeater

VAP Overview   General   VAP Config   Security   Repeater   Advanced   Access Control   Site Survey

Home > Wireless > Repeater Config

## Repeater Settings

Repeater Type :

The SSID of Upper-Bound AP : \*

Security Type :

Current wireless channel of the system is set at 1. Repeater connection may fail if the system is set to connect to upper AP with different channels

If Universal Repeater is chosen, please provide the SSID of upper-bound AP for uplink connection; Security Type (None, WEP, or WPA-PSK) can be configured for this Repeater connection. Please note the security type configured here needs to be the same as upper-bound AP to be connected.



## 4.2.6 Advanced Wireless Settings

VAP Overview General VAP Config Security Repeater **Advanced** Access Control Site Survey

Home > Wireless > Advanced

### Advanced Wireless Settings

Profile Name : VAP-1

Beacon Interval : 100 \*(100 - 500ms )

RTS Threshold : 2346 \*(1 - 2346)

Fragment Threshold : 2346 \*(256 - 2346)

Broadcast SSID :  Disable  Enable

Wireless Station Isolation :  Disable  Enable

WMM :  Disable  Enable

IAPP :  Disable  Enable

802.11g Protection :  Disable  Enable

The advanced wireless settings for the NP727's VAP (Virtual Access Point) profiles allow customization of data transmission settings. The administrator can tune the following parameters to improve network communication performance if a poor connection occurs.

- **Beacon Interval:** Enter a value between 25 and 500 ms. The default is 100 milliseconds. The specified value represents the amount of time between access point beacon signal transmissions.
- **RTS Threshold:** Enter a value between 1 and 2346. The default is 2346. RTS (Request to Send) Threshold determines the packet size at which the access point (the NP727) issues a request to send (RTS) before sending the packet to prevent the hidden node problem. The RTS mechanism will be activated if the data size exceeds the value you set. A lower RTS Threshold setting can be useful in areas where many client devices are associating with the NP727 or in areas where the clients are far apart and can detect only the NP727 and not each other.

**Fragment Threshold:** Enter a value between 256 and 2346. The default is 2346. A packet size larger than this threshold will be fragmented (sent in several pieces instead of one block) before transmission. A smaller value results in smaller packets but allows a larger number of packets in transmission. A lower Fragment Threshold setting can be useful in areas where communication is poor or disturbed by a serious amount of radio interference.

- **Broadcast SSID:** The default is *Enable*. Disabling this function will prevent the NP727 from broadcasting its SSID, where only devices that have the correct SSID can connect.
- **Station Isolation:** The default is *Disable*. By enabling this function, all stations associated with the NP727 can only communicate with the NP727.
- **WMM:** The default is *Disable*. Wi-Fi Multimedia (WMM) is a Quality of Service (QoS) feature that prioritizes wireless data packets based on four access categories: voice, video, best effort, and background. Applications without WMM and applications that do not require QoS are assigned to the best-effort category, which receives a lower priority than voice and video. In short, WMM decides which data streams are the most important and assign them a higher traffic priority.

#### < To receive the benefits of WMM QoS >

- The application must support WMM.

- You must enable WMM in the NP727.
- You must enable WMM in the wireless adapter in your computer.
- **IAPP:** The default is *Disable*. IAPP (Inter Access Point Protocol) is a protocol by which access points share information about the stations that are connected to them. By enabling this function, the NP727 will automatically broadcast information of associated wireless stations to its peer access points. This will help wireless stations roam smoothly among IAPP-enabled access points in the same wireless LAN.
- **802.11g Protection:** When enabled, the associated 802.11g stations will benefit from this function since their transmission speed will not be affected by the surrounding 802.11b stations.

## 4.2.7 Access Control Settings

VAP Overview General VAP Config Security Repeater Advanced Access Control Site Survey

Home > Wireless > Access Control

### Access Control Settings

Profile Name : VAP-1

Maximum Number of Clients : 32 \*( Range: 1 ~ 32 )

Access Control Type : Disable Access Control

- **Maximum Number of Clients**

The NP727 supports various methods of authenticating clients for using wireless LAN. The default policy is unlimited access without any authentication required. To restrict the station number of wireless connections, simply change the **Maximum Number of Stations** to a desired number. For example, while the number of stations is set to 20, only 20 stations are allowed to connect to the specified VAP.

- **Access Control Type**

The selected **Access Control Type** will be the activated policy while the rest will be omitted. The following is a list of the supported methods for MAC ACL control:

- (1) **Disable Access Control**

No MAC address check required.

- (2) **MAC ACL Allow List**

Deny all except those in the Allow List. When selecting *MAC ACL Allow List*, all wireless connections to the specified VAP will be denied except the MAC addresses listed in the Allow List ("allowed MAC addresses"). The administrator can disable any allowed MAC address to connect to the VAP temporarily by checking *Disable*. For example, 11:22:33:44:55:66 is in the Allow List; to temporarily deny its access, check *Disable* in the **State** section.

VAP Overview General VAP Config Security Repeater Advanced Access Control Site Survey

Home > Wireless > Access Control

### Access Control Settings

Profile Name : VAP-1

Maximum Number of Clients : 32 \*( Range: 1 ~ 32 )

Access Control Type : MAC ACL Allow List

No.	MAC Address	State
1	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
2	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

- (3) **MAC ACL Deny List**

Allow all except those in the Deny List. When selecting *MAC ACL Deny List*, all wireless connections to the specified VAP will be allowed except the MAC addresses listed in the Deny List ("denied MAC addresses"). The administrator can allow any denied MAC address to connect to the VAP temporarily by

checking *Enable*.

VAP Overview | General | VAP Config | Security | Repeater | Advanced | Access Control | Site Survey

Home > Wireless > Access Control

### Access Control Settings

Profile Name : VAP-1

Maximum Number of Clients :  \*( Range: 1 ~ 32 )

Access Control Type : MAC ACL Deny List

No.	MAC Address	State
1	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
2	<input type="text"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

(4) **RADIUS ACL**

Authenticate incoming MAC addresses by RADIUS. When selecting *RADIUS ACL*, all incoming MAC addresses will be authenticated by RADIUS. Please note that each VAP's MAC ACL and its security type (showing on the **Security Settings** page) share the same RADIUS configuration.

VAP Overview | General | VAP Config | Security | Repeater | Advanced | Access Control | Site Survey

Home > Wireless > Access Control

### Access Control Settings

Profile Name : VAP-1

Maximum Number of Clients :  \*( Range: 1 ~ 32 )

Access Control Type : RADIUS ACL

Primary RADIUS Server :

Note!!! These settings will also apply to security settings which use RADIUS Server for this VAP.

Host:  \*( Domain Name / IP Address )

Authentication Port:  \*( 1 - 65535 )

Secret Key:  \*

Secondary RADIUS Server :

Host:

Authentication Port:

Secret Key:

## 4.2.8 Site Survey

Home > Wireless > Site Survey

### Scan Result

[Scan Again!](#)

SSID	MAC Address	Channel	Rate	Signal	Security	Setup / Connect
NP727-1	00:60:64:00:2E:56	1	54	43	None	<a href="#">Connect</a>
NP727-2	00:60:64:00:2E:55	1	54	49	None	<a href="#">Connect</a>

If **Universal Repeater** function is enabled, the system can scan and display all surrounding available access points (APs). The administrator can then select an AP to be connected to extend its wireless service coverage on this page.

- **SSID:** The SSID (Service Set ID) of the AP found in the system's coverage area.
- **MAC Address:** The MAC address of the respective AP.
- **Channel:** The channel number currently used by the respective AP or repeater.
- **Rate:** The transmitting rate of the respective AP.
- **Signal:** The signal strength of the respective AP.
- **Security:** The encryption type used by the respective AP
- **Setup/ Connect:**
  - **Connect:** Click **Connect** to associate with the respective AP directly; no further configuration is required.

893	00:0E:2E:7C:AA:6E	1	54	4	None	<a href="#">Connect</a>
-----	-------------------	---	----	---	------	-------------------------

- **Setup:** Click **Setup** to configure security settings for associating with the respective AP.
  - **WEP:** Click **Setup** to configure the WEP setting for associating with the target AP.

wep	00:11:A3:08:09:56	6	54	40	WEP	<a href="#">Setup</a>
-----	-------------------	---	----	----	-----	-----------------------

The following configuration box will then appear at the bottom of the screen. Security settings configured here must be the same as the target AP.

Note!!! If you set WEP security for Universal Repeater the security of AP will also change to WEP and use the same settings.

WEP Key Type :  Open  Shared  Auto

WEP Key Length :  64 bits  128 bits  152 bits

WEP Key Format :  ASCII  Hex

WEP Key Index :

WEP Keys :

1

2

3

4

- **WPA-PSK:** Click **Setup** to configure the WPA-PSK setting for associating with the target AP.

psk	0A:1F:D4:39:10:74	11	54	52	WPA-PSK	<input type="button" value="Setup"/>
-----	-------------------	----	----	----	---------	--------------------------------------

The following configuration box will then appear at the bottom of the screen. Information provided here must be consistent with the security settings of the target AP.

Pre-shared Cipher :

Pre-shared Key Type :  PSK(Hex) \*( 64 chars )

Passphrase \*( 8 - 63 chars )

Pre-shared Key :

## 4.3 Firewall

The system provides an added security feature, L2 firewall, in addition to typical AP security. Layer-2 firewall offers a firewall function that is tailored specifically for layer 2 traffics, providing another choice of shield against possible security threats coming from/going to WLAN (AP interfaces); hence, besides firewall policies configured on gateways, this extra security feature will assist to mitigate possible security breach.

### 4.3.1 Layer 2 Firewall Settings

It provides an overview of firewall rules in the system; 6 default rules with up to total 20 firewall rules are available for configuration.

Home > Firewall > Firewall List

### Layer 2 Firewall Settings

Enable Layer 2 Firewall  Disable  Enable

No.	State	Action	Name	EtherType	Remark	Setting
1	<input type="checkbox"/>	DROP	CDP and VTP	IEEE_8023		<a href="#">Del</a> <a href="#">Ed</a> <a href="#">In</a> <a href="#">Mv</a>
2	<input type="checkbox"/>	DROP	STP/BPDU	IEEE_8023		<a href="#">Del</a> <a href="#">Ed</a> <a href="#">In</a> <a href="#">Mv</a>
3	<input type="checkbox"/>	DROP	GARP	IEEE_8023		<a href="#">Del</a> <a href="#">Ed</a> <a href="#">In</a> <a href="#">Mv</a>
4	<input type="checkbox"/>	DROP	RIP	IPv4		<a href="#">Del</a> <a href="#">Ed</a> <a href="#">In</a> <a href="#">Mv</a>
5	<input type="checkbox"/>	DROP	HSRP	IPv4		<a href="#">Del</a> <a href="#">Ed</a> <a href="#">In</a> <a href="#">Mv</a>
6	<input type="checkbox"/>	DROP	OSPF	IPv4		<a href="#">Del</a> <a href="#">Ed</a> <a href="#">In</a> <a href="#">Mv</a>
7	<input type="checkbox"/>					<a href="#">Del</a> <a href="#">Ed</a> <a href="#">In</a> <a href="#">Mv</a>
8	<input type="checkbox"/>					<a href="#">Del</a> <a href="#">Ed</a> <a href="#">In</a> <a href="#">Mv</a>
9	<input type="checkbox"/>					<a href="#">Del</a> <a href="#">Ed</a> <a href="#">In</a> <a href="#">Mv</a>
10	<input type="checkbox"/>					<a href="#">Del</a> <a href="#">Ed</a> <a href="#">In</a> <a href="#">Mv</a>

[First](#) [Prev](#) [Next](#) [Last](#) ( total: 20 )

#### Layer 2 Firewall Overview

From the overview table, each rule is designated with the following fields:

- ◆ **No.:** The numbering will decide the priority to let the system carry out the available firewall rules in the table.
- ◆ **State:** The check marks will enable the respective rules.
- ◆ **Action:** “DROP” denotes a block rule; “ACCEPT” denotes a pass rule.
- ◆ **Name:** It shows the name of the rule.
- ◆ **EtherType:** It denotes the type of traffics subject to this rule.

- ◆ **Remark:** It shows the note of this rule.
- ◆ **Setting:** 4 actions are available; “Del” denotes to delete the rule, “Ed” denotes to edit the rule, “In” denotes to insert a rule, and “Mv” denotes to move the rule.

**>>To delete a specific rule,**

“Del” in “Setting” column of firewall list will lead to the following page for removal confirmation. After “SAVE” button is clicked and system reboot, the rule will be removed.

The screenshot shows the 'Layer 2 Firewall Settings' page. At the top, there are tabs for 'Firewall List', 'Service', and 'Advanced'. Below the tabs, a breadcrumb trail reads 'Home > Firewall > Firewall List'. The main heading is 'Layer 2 Firewall Settings'. Underneath, it says 'Remove rule | 1'. At the bottom, there are two yellow buttons: 'SAVE' and 'CLEAR'.

*Layer 2 Firewall Settings Screen (Remove rule)*

**>>To edit a specific rule,**

“Ed” in “Setting” column of firewall list will lead to the following page for detail configuration. From this page, the rule can be edited from scratch or from an existing rule for revision.

The screenshot shows the 'Layer 2 Firewall Configuration' page. At the top, there are tabs for 'Firewall List', 'Service', and 'Advanced'. Below the tabs, a breadcrumb trail reads 'Home > Firewall List > Rule Config'. The main heading is 'Layer 2 Firewall Configuration'. The form contains the following fields:

- Rule ID :** 1
- Rule name :** CDP and VTP \*
- EtherType :** IEEE802.3
- Interface :** From (selected) To
- Interface :** VAP1
- DSAP/SSAP :** aa
- Type :** 2000 (ie IPv4: 0800)
- Source :** MAC Address: [ ] Mask: [ ]
- Destination :** MAC Address: 01:00:0C:CC:CC:CC Mask: [ ]
- Action :** Block (selected) Pass
- Remark :** [ ]

At the bottom, there are two yellow buttons: 'SAVE' and 'CLEAR'.

*Layer 2 Firewall Configuration Screen (Edit)*

- ◆ **Rule ID:** The numbering of this specific rule will decide its priority among available firewall rules in the table.
- ◆ **Rule name:** The rule name can be specified here.



- ◆ **EtherType:** The drop-down list will provide the available types of traffics (ALL, IPv4, IEEE802.3, 802.1Q, ARP, and RARP) subject to this rule.
- ◆ **Interface:** It can indicate inbound/outbound direction with desired interfaces (VAP1~VAP8)
- ◆ **Service (when EtherType is IPv4):** Select the available upper layer protocols/services from the drop-down list.
- ◆ **DSAP/SSAP (when EtherType is IEEE802.3):** The value can be further specified for the fields in 802.2 LLC frame header.
- ◆ **Type (when EtherType is IEEE802.3):** The field can be used to indicate the type of encapsulated traffics.
- ◆ **Vlan ID (when EtherType is 802.1Q):** The Vlan ID is provided to associate with certain VLAN-tagging traffics.
- ◆ **Priority (when EtherType is 802.1Q):** It denotes the priority level with associated VLAN traffics.
- ◆ **Encapsulated Type (when EtherType is 802.1Q):** It can be used to indicate the type of encapsulated traffics.
- ◆ **Opcode (when EtherType is ARP/RARP):** This list can be used to specify the ARP Opcode in ARP header.
- ◆ **Source:** MAC Address/Mask indicates the source MAC; IP Address/Mask indicates the source IP address (when EtherType is IPv4); ARP IP/MAC & MASK indicate the ARP payload fields.
- ◆ **Destination:** MAC Address/Mask indicates the destination MAC; IP Address/Mask indicates the destination IP address (when EtherType is IPv4); ARP IP/MAC & MASK indicate the ARP payload fields.
- ◆ **Action:** The rule can be chosen to be "Block" or "Pass".
- ◆ **Remark:** The note of this rule can be specified here.

When the configuration for firewall rules is provided, please click "**SAVE**" and reboot system to let the firewall rules take effect.

**>>To insert a specific rule,**

"In" in "Setting" column of firewall list will lead to the following page for detail configuration with rule ID for the current inserted rule.

From this page, the rule can be edited from scratch or from an existing rule for revision.

Firewall List Service Advanced

Home > Firewall List > Rule Config

### Layer 2 Firewall Configuration

Rule ID : 1

Rule name : CDP and VTP \*

EtherType : IEEE802.3

Interface :  From  To  
VAP1

DSAP/SSAP : aa

Type : 2000 (ie IPv4: 0800)

Source : MAC Address:  Mask:

Destination : MAC Address: 01:00:0C:CC:CC:CC Mask:

Action :  Block  Pass

Remark :

SAVE CLEAR

*Layer 2 Firewall Configuration Screen (Insert)*

**>>To move a specific rule,**

“Mv” in “Setting” column of firewall list will lead to the following page for re-ordering confirmation. After “**SAVE**” button is clicked and system reboot, the order of rules will be updated.

Firewall List Service Advanced

Home > Firewall > Move rule

### Move Rule

ID : 1

Move to :  Before  After ID :  \*( 1 - 20 )

SAVE CLEAR

*Move Rule Screen*

Please make sure all desired rules (state of rule) are **checked** and **saved** in overview page; the rule will be enforced upon system reboot.

### Layer 2 Firewall Settings

Enable Layer 2 Firewall  Disable  Enable

No.	State	Action	Name	EtherType	Remark	Setting
1	<input checked="" type="checkbox"/>	DROP	CDP and VTP	IEEE_8023		<a href="#">Del</a> <a href="#">Ed</a> <a href="#">In</a> <a href="#">Mv</a>
2	<input type="checkbox"/>	DROP	STP/BPDU	IEEE_8023		<a href="#">Del</a> <a href="#">Ed</a> <a href="#">In</a> <a href="#">Mv</a>
3	<input type="checkbox"/>	DROP	GARP	IEEE_8023		<a href="#">Del</a> <a href="#">Ed</a> <a href="#">In</a> <a href="#">Mv</a>
4	<input type="checkbox"/>	DROP	RIP	IPv4		<a href="#">Del</a> <a href="#">Ed</a> <a href="#">In</a> <a href="#">Mv</a>
5	<input type="checkbox"/>	DROP	HSRP	IPv4		<a href="#">Del</a> <a href="#">Ed</a> <a href="#">In</a> <a href="#">Mv</a>
6	<input type="checkbox"/>	DROP	OSPF	IPv4		<a href="#">Del</a> <a href="#">Ed</a> <a href="#">In</a> <a href="#">Mv</a>
7	<input type="checkbox"/>					<a href="#">Del</a> <a href="#">Ed</a> <a href="#">In</a> <a href="#">Mv</a>
8	<input type="checkbox"/>					<a href="#">Del</a> <a href="#">Ed</a> <a href="#">In</a> <a href="#">Mv</a>
9	<input type="checkbox"/>					<a href="#">Del</a> <a href="#">Ed</a> <a href="#">In</a> <a href="#">Mv</a>
10	<input type="checkbox"/>					<a href="#">Del</a> <a href="#">Ed</a> <a href="#">In</a> <a href="#">Mv</a>

[First](#) [Prev](#) [Next](#) [Last](#) ( total: 20 )

**SAVE**

**CLEAR**

*Layer 2 Firewall Overview (Check State)*

## 4.3.2 Firewall Service

The administrator can add or delete firewall service here; the services in this list will become options to choose in firewall rule (when EtherType is IPv4).

Home > Firewall > Service Config

### Firewall Service

No.	Name	Description	Delete
1	ALL	ALL	<input type="checkbox"/>
2	ALL TCP	TCP, Source Port: 0~65535, Destination Port: 0~65535	<input type="checkbox"/>
3	ALL UDP	UDP, Source Port: 0~65535, Destination Port: 0~65535	<input type="checkbox"/>
4	ALL ICMP	ICMP	<input type="checkbox"/>
5	FTP	TCP/UDP, Destination Port: 20~21	<input type="checkbox"/>
6	HTTP	TCP/UDP, Destination Port: 80	<input type="checkbox"/>
7	HTTPS	TCP/UDP, Destination Port: 443	<input type="checkbox"/>
8	POP3	TCP, Destination Port: 110	<input type="checkbox"/>
9	SMTP	TCP, Destination Port: 25	<input type="checkbox"/>
10	DHCP	UDP, Destination Port: 67~68	<input type="checkbox"/>

First Prev Next Last ( total: 28 )

Add

SAVE CLEAR

### Overview of Firewall Services

There are 28 firewall services available in default settings; these default services cannot be deleted but can be disabled. If changes are made, please click SAVE to save the settings before leaving this page.

### 4.3.3 Advanced Firewall Settings

Advanced firewall settings are used to supplement the firewall rules, providing extra security enhancement against DHCP and ARP traffics traversing the available interfaces of system.

Home > Firewall > Advanced

### Advanced Firewall Settings

**Trust Interface :**

VAP1    VAP2    VAP3    VAP4    VAP5    VAP6    VAP7    VAP8

WDS1    WDS2    WDS3    WDS4

LAN

**DHCP Snooping :**    Disable    Enable

**ARP Inspection :**    Disable    Enable

Trust List Broadcast :  Disable    Enable

Static Trust List :    Disable    Enable

**SAVE**   **CLEAR**

#### *Advanced Firewall Settings*

- ◆ **Trust Interface:** Each interface can be checked individually to mark as trusted interfaces; security enforcements on DHCP/ARP like DHCP snooping and ARP inspection will be carried out on non-trusted interfaces.
- ◆ **DHCP Snooping:** When enabled, DHCP packets will be validated against possible threats like DHCP starvation attack; in addition, the trusted DHCP server (IP/MAC) can be specified to prevent rogue DHCP server.
- ◆ **ARP Inspection:** When enabled, ARP packets will be validated against ARP spoofing. **Trust List Broadcast** can be enabled to let other NP727 (with L2 firewall feature) learn the trusted MAC/IP pairs to issue ARP requests. **Static Trust List** can be used to add MAC or MAC/IP pairs to issue ARP request. Other network nodes can still send their ARP requests; however, if their IP appears in the static list (with different MAC), their ARP requests will be dropped to prevent eavesdropping.

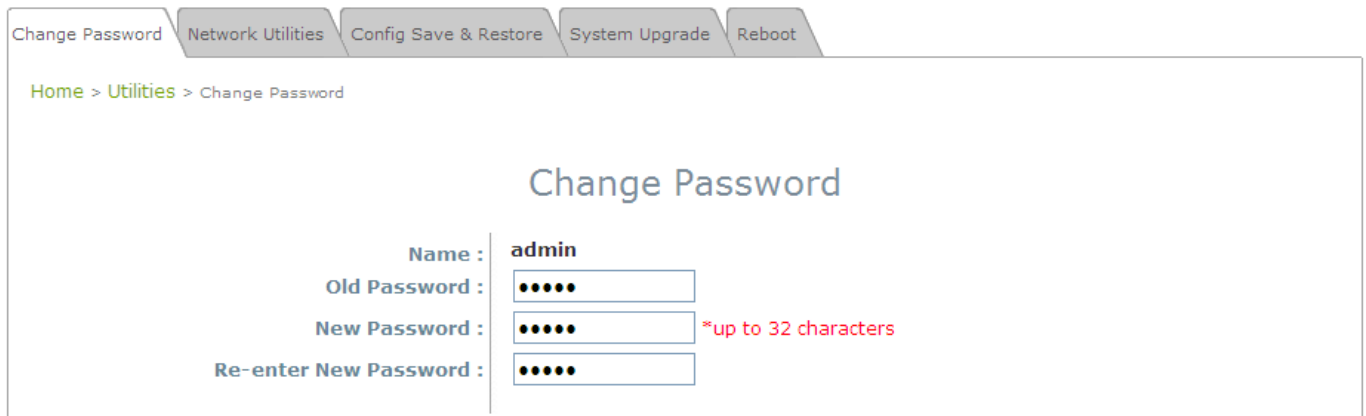
If any settings are made, please click **SAVE** to save the configuration before leaving this page.

## 4.4 Utilities

This section includes five utilities used for customizing and maintaining the system, including **Change Password**, **Network Utilities**, **Config Save & Restore**, **System Upgrade** and **Reboot**.

### 4.3.1 Change Password

To protect the management web site from unauthorized access, it is strongly recommended to change the default administrator's password to a secure password. Only alpha-numeric characters pattern is allowed, and it is strongly recommended to take a combination of both numeric and alphabetic characters.

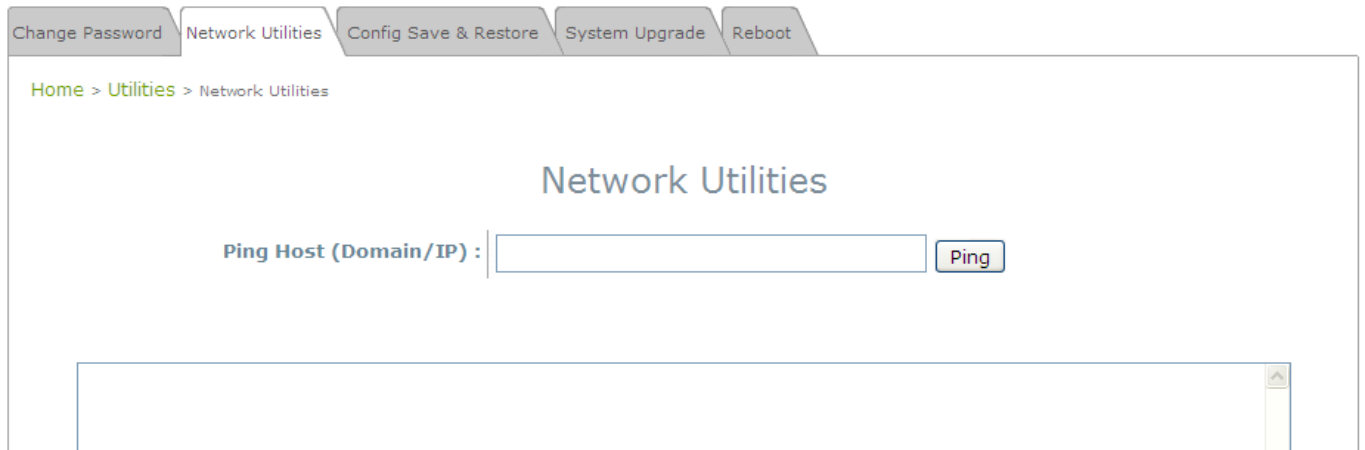


The screenshot shows the 'Change Password' utility interface. At the top, there are five tabs: 'Change Password', 'Network Utilities', 'Config Save & Restore', 'System Upgrade', and 'Reboot'. Below the tabs, a breadcrumb trail reads 'Home > Utilities > Change Password'. The main heading is 'Change Password'. The form contains the following fields:

- Name :** admin
- Old Password :** [password field with 5 dots]
- New Password :** [password field with 5 dots] \*up to 32 characters
- Re-enter New Password :** [password field with 5 dots]

The administrator can change the password of the system. The login account for the administrator is *admin*, and the default admin password of the system is "**admin**". The admin password can be changed here by entering the new password. Click **SAVE** to save the new password.

## 4.3.2 Network Utilities



The screenshot shows a web interface with a navigation bar at the top containing five tabs: "Change Password", "Network Utilities", "Config Save & Restore", "System Upgrade", and "Reboot". The "Network Utilities" tab is selected. Below the navigation bar, a breadcrumb trail reads "Home > Utilities > Network Utilities". The main content area is titled "Network Utilities" and features a form with the label "Ping Host (Domain/IP) :". To the right of the text input field is a "Ping" button. Below the form is a large empty rectangular area, likely for displaying the results of the ping command.

THE NP727 provides a PING utility for possible network trouble shooting.

### 4.3.3 Configuration Save & Restore

This function is used to backup and to restore the THE NP727 settings. The THE NP727 can also be restored to the factory default settings using this function. It can be used to duplicate settings to other access points (backup settings of this system and then restore on another AP).

Change Password | Network Utilities | **Config Save & Restore** | System Upgrade | Reboot

Home > Utilities > Config Save & Restore

## Configuration Backup & Restore

**Reset to Default:**

**Backup System Settings:**

**Restore System Settings:**

- **Reset to Default:** Click **Reset** to load the factory default settings of THE NP727. Then, reboot the system to let the default settings take effect.
- **Backup Settings:** Click **Save** to save the current system configurations to a backup file on a local disk. It is recommended to make a backup before any configuration changes are made.
- **Restore Settings:** Click **Browse** to select a configuration file to restore, and then, press **Upload** to proceed. The configuration file will replace the active configuration file currently running on the system. Reboot the system to let the parameter changes take effect.



*After network parameters have been reset/restored, the network settings of the administrator PC may need to be changed to ensure that the IP address of the administrator PC is on the same subnet mask as THE NP727.*



### 4.3.4 System Upgrade

THE NP727 provides Web firmware upload/upgrade feature. The administrator can download the latest firmware from the website and save it on the administrator PC. To upgrade the system firmware, click **Browse** to choose the new firmware file you downloaded onto the temporary directory of your PC and then click **Upload** to execute the process. There will be a prompt confirmation message appearing to notify the administrator to restart the system after a successful firmware upgrade. Please restart the system after upgrading the firmware.

System Upgrade

Current Version: 1.00.00  
 Current Build Number: 1.5-1.2418  
 File Name:

►► **Note:**

- It is recommended to check the firmware version number before proceeding further. Please make sure you have the correct firmware file.
- Firmware upgrade may sometimes result in loss of some data. Please ensure that all necessary settings are written down before upgrading the firmware.
- During firmware upgrade, please do not turn off the power. This may permanent damage this system.

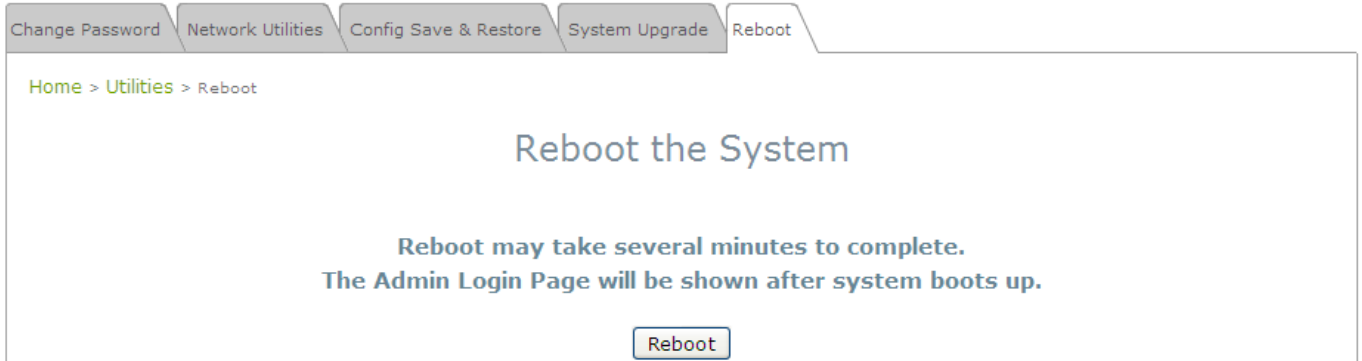


*For further information of available firmware version, please contact your local dealers.*

### 4.3.5 Reboot

This function allows the administrator to restart the THE NP727 safely. The process shall take about three minutes. Click **Reboot** to restart the system. Please wait for the blinking timer to complete its countdown before accessing the system web management interface again.

Occasionally, it is necessary to reboot THE NP727 to ensure parameter changes being submitted.



## 4.5 Status

This section includes the following functions: **Overview**, **Clients**, **Repeater** and **Event Log**.

### 4.5.1 System Overview

The **System Overview** page provides an overview of the system status for the administrator.

NetComm®  
www.netcomm.com.au

NP727 – In-wall Wireless Access Point

Home Logout Help

System Wireless Firewall Utilities Status

Overview Clients Repeater Event Log

Home > Status > System Overview

### System Overview

**System**

System Name	NP727
Firmware Version	1.00.00
Build Number	1.5-1.2418
Location	Sydney, Australia
Site	EN-AU
Device Time	2000/01/01 11:05:40
System Up Time	0 days, 0:05:40

**Radio Status**

MAC Address	00:60:64:2D:B6:44
Band	802.11b+g
Channel	6
TX Power	Highest

**LAN Interface**

MAC Address	00:60:64:2D:B6:43
IP Address	192.168.27.1
Subnet Mask	255.255.255.0
Gateway	192.168.27.254

**AP Status**

Profile Name	BSSID	ESSID	Security Type	Online Clients
VAP-1	00:60:64:2D:B6:...	NetComm Wirele..	None	0

The description of the table is as the following:

	<b>ITEM</b>	<b>DESCRIPTION</b>
<b>System</b>	<b>System Name</b>	The system name of THE NP727.
	<b>Firmware Version</b>	The present firmware version of THE NP727.
	<b>Device Time</b>	The system time of THE NP727.
	<b>System Up Time</b>	The time that the system has been in operation
<b>LAN Interface</b>	<b>MAC Address</b>	The MAC address of LAN Interface
	<b>IP Address</b>	The IP address of the LAN Interface
	<b>Subnet Mask</b>	The Subnet Mask of the LAN Interface
	<b>Gateway</b>	The Gateway of the LAN Interface
<b>Radio Status</b>	<b>MAC Address</b>	The MAC address of RF Card
	<b>Band</b>	The RF band (b or g) used
	<b>Channel</b>	The channel specified
	<b>Tx Power</b>	Transmit Power level of RF card
<b>Virtual AP Profiles</b>	<b>BSSID</b>	Basic Service Set ID
	<b>ESSID</b>	Extended Service Set ID
	<b>Security Type</b>	Security type of the Virtual AP
	<b>Online Clients</b>	The number of online clients

## 4.5.2 Associated Client Status

[Home](#) > [Status](#) > [Wireless Clients](#)

### Associated Client Status

#### Client List

Associated VAP	ESSID	MAC Address	SNR (dB)	Idle Time (secs)	Disconnect
VAP-1	NetComm Wireless-1	00:16:ea:c8:ec:d6	55	17	<input type="button" value="Kick"/>

This page lists all associated clients of all VAPs to allow administrator to remotely oversee the status of the clients. When a low SNR is found here, the administrator can tune the corresponding parameters or investigate the settings of network devices to improve network communication performance.

- **Associated VAP:** The name of an associated VAP (Virtual Access Point)
- **ESSID:** Extended Service Set ID
- **MAC Address:** The MAC Address of associated clients
- **SNR:** Signal to Noise Ratio
- **Idle Time:** Time of no activity of associated clients in seconds
- **Disconnect:** When clicking **Kick**, the clients will disconnect with the system.

### 4.5.3 Repeater Information

The administrator can review detailed information of the repeater function on this page. Information of repeater's status, mode and encryption is provided

- **Repeater Status:** The table will be displayed when Repeater mode is selected.
  - **Status:** The status of the repeater function either *Enabled* or *Disabled*.
  - **Mode:** The mode selected for the repeater function, either *Universal Repeater* or *WDS*.
  - **Encryption:** The encryption type used: *None*, *WEP*, or *WPA-PSK*.
- **WDS Link Status:** The table will be displayed when WDS mode is selected. For more information on the repeater type, please refer to **Section 4.2.5 Repeater Settings**.
  - **MAC Address:** The MAC Address of the WDS peer.
  - **RSSI:** Received Signal Strength Indication, a measurement of received radio signal over WDS link.
  - **Tx Rate:** The transmit rate of the Repeater.
  - **Tx Count:** The accumulative number of transmission counts.
  - **Tx Error:** The accumulative number of transmission errors.

Overview Clients Repeater Event Log

Home > Status > Repeater Information

## Repeater Information

### Repeater Status

Status	Enabled
Mode	WDS
Encryption	None

### WDS Link Status

Item	MAC Address	RSSI	Tx Rate	Tx Count	Tx Error
1	00:1F:D4:00:08:1F	0	54 M	19	19
2		N/A	N/A	N/A	N/A
3		N/A	N/A	N/A	N/A
4		N/A	N/A	N/A	N/A

< Fig. 4.5.3-1 Repeater Information: WDS Page >

- **Universal Repeater:** The table will be displayed when Universal Repeater mode is selected. For more information on the repeater type, please refer to **Section 4.2.5 Repeater Settings**.
  - **SSID:** SSID of the upper-bound AP to be associated with.
  - **Tx Rate:** The transmit rate of the Repeater.
  - **SNR:** The SNR (Signal to Noise Ratio) indicates the relative signal strength between the upper-bound AP and the system.
  - **Tx Count:** The accumulative number of transmission counts.
  - **Tx Error:** The accumulative number of transmission errors.

Overview Clients Repeater Event Log

Home > Status > Repeater Information

## Repeater Information

### Repeater Status

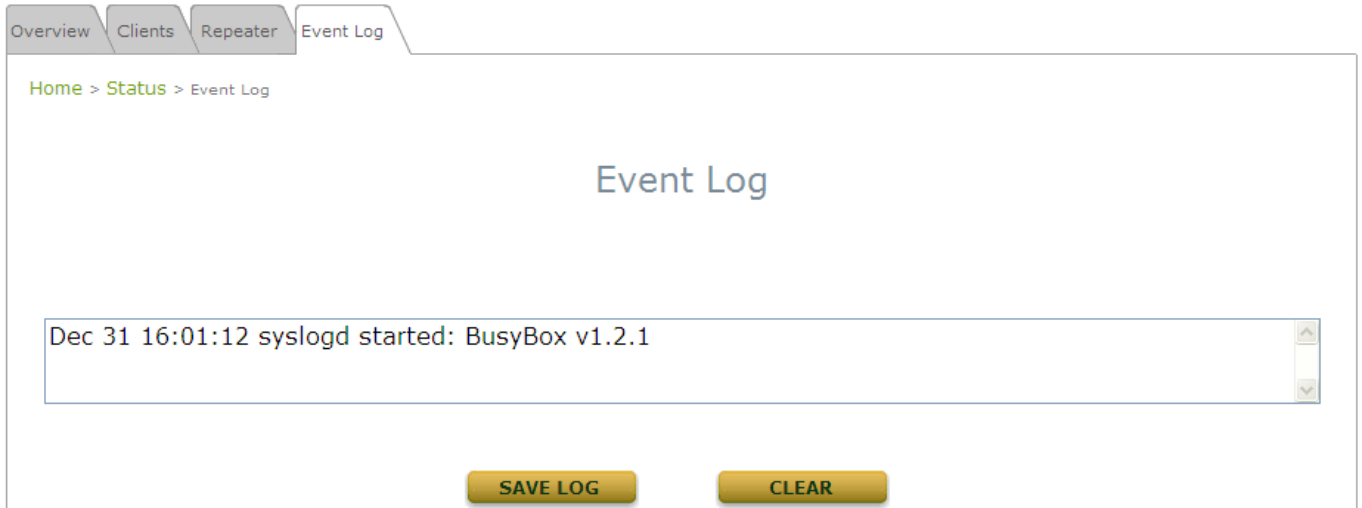
Status	Enabled
Mode	Universal Repeater
Encryption	None

### Universal Repeater

SSID	AP
TX Rate	54 Mbits
SNR	15
TX Count	393 Bytes
TX Error	17 Packets

<Fig 4.5.3-2 Repeater Information: Universal Repeater Page>

## 4.5.4 Event Log



The Event Log provides the system activities records. The administrator can monitor the system status by checking this log. Please enable system Sys-log to view the system log messages.

In the log, normally, each line represents an event record; in each line, there are 4 fields:

- **Date/Time:** The time & date when the event happened
- **Hostname:** Indicate which host records this event. Note that all events in this page are local event, so the hostname in this field are all the same. However, in remote syslog service, this field will help the administrator identify which event is from this THE NP727. Please refer to section *4.1.3 Management Services*.
- **Process name:** Indicate the event generated by the running instance.
- **Description:** Description of this event.

To save the file locally, click **SAVE LOG**; to clear all the records, click **CLEAR**.



## 4.6 Online Help

The **Help** button is at the upper right hand corner of the display screen.

Click **Help** for the **Online Help** window, and then click the hyperlink of the relevant information required.

### Online Help

#### Organization of the Configuration Web:

<u><a href="#">System</a></u>	<u><a href="#">Wireless</a></u>	<u><a href="#">Firewall</a></u>	<u><a href="#">Utilities</a></u>	<u><a href="#">Status</a></u>
<u><a href="#">System Information</a></u>	<u><a href="#">VAP Overview</a></u>	<u><a href="#">Firewall List</a></u>	<u><a href="#">Password</a></u>	<u><a href="#">System Overview</a></u>
<u><a href="#">Network</a></u>	<u><a href="#">General</a></u>	<u><a href="#">Service</a></u>	<u><a href="#">Network Utilities</a></u>	<u><a href="#">Clients</a></u>
<u><a href="#">Management Services</a></u>	<u><a href="#">VAP Config</a></u>	<u><a href="#">Advanced</a></u>	<u><a href="#">Config Save Restore</a></u>	<u><a href="#">Repeater</a></u>
	<u><a href="#">Security</a></u>		<u><a href="#">System Upgrade</a></u>	<u><a href="#">Event Log</a></u>
	<u><a href="#">Repeater</a></u>		<u><a href="#">Reboot</a></u>	
	<u><a href="#">Advanced</a></u>			
	<u><a href="#">Access Control</a></u>			
	<u><a href="#">Site Survey</a></u>			

# NetComm

# Dynalink

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

**DYNALINK NZ** 12c Tea Kea Place, Albany, Auckland,  
New Zealand  
**P:** 09 448 5548  
**F:** 09 448 5549  
**E:** [sales@dynalink.co.nz](mailto:sales@dynalink.co.nz)  
**W:** [www.dynalink.co.nz](http://www.dynalink.co.nz)

## Product Warranty

NetComm products have a standard 12 months warranty from date of purchase. However some products have an extended warranty option, via registering your product online at the NetComm website [www.netcommlimited.com](http://www.netcommlimited.com).

## Technical Support

If you have any technical difficulties with your product, please refer to the support section of our website.

[www.netcomm.com.au/support](http://www.netcomm.com.au/support)

Note: NetComm Technical Support for this product only covers the basic installation and features outlined in the Quick Start Guide. For further information regarding the advanced features of this product, please refer to the configuring sections in the User Guide or contact a Network Specialist.