SHD69A

Surveillance transmission system

User Guide

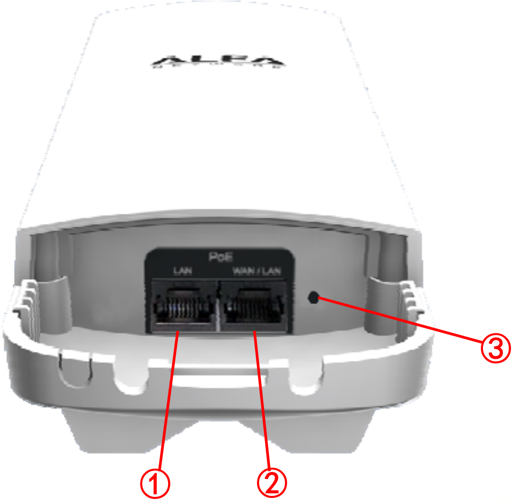
Table of Contents

INTRODUCTION

The SHD69A is a 2x2 MIMO IEEE Surveillance transmission system which support high through-put up to 300Mbps. It is rain and splash proof when install in upright position. SHD69A also integrated 11dBi patch antenna and passive PoE for simplify installation.

HARDWARE DESCRIPTION

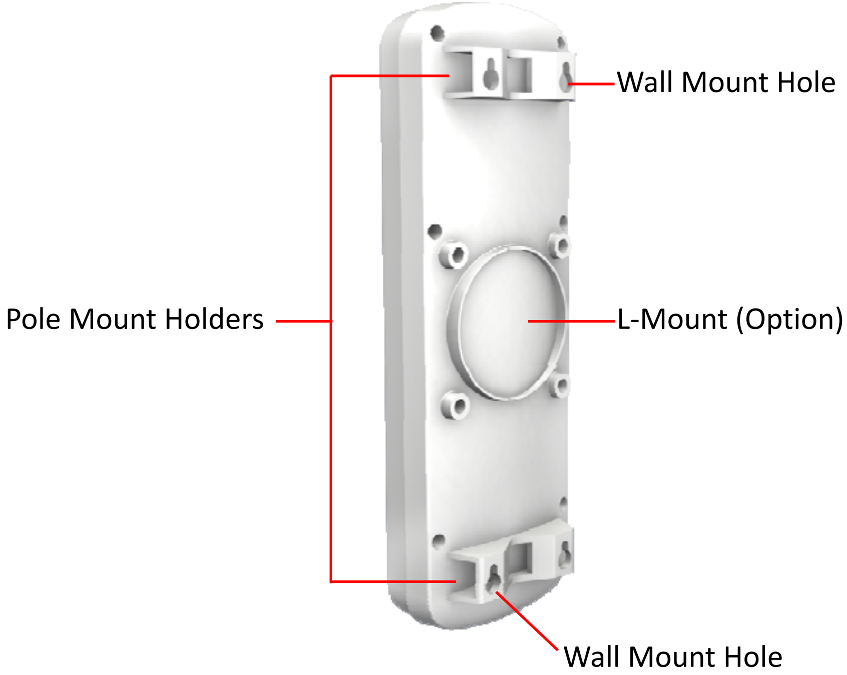
Below are SHD69A hardware descriptions

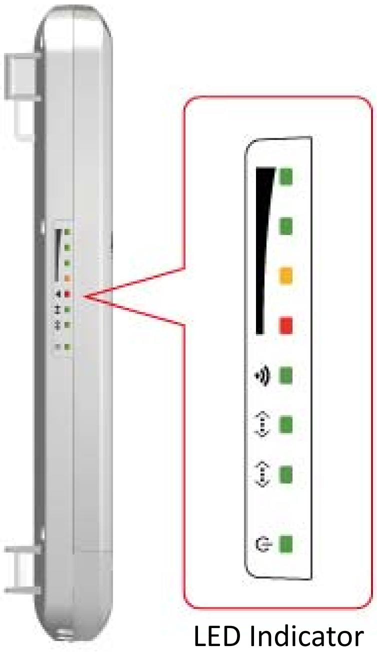


① PoE LAN

② PoE WAN (in Rouer mode)
PoE LAN (in Bridge Mode)

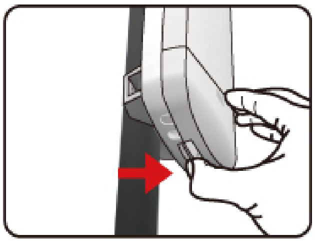
③ Reset



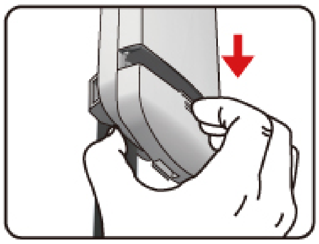


Hardware Installation

◆ How to open the sliding door

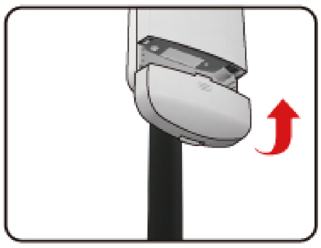


Unlatch the weatherproof sliding door from the rear of the base to open.

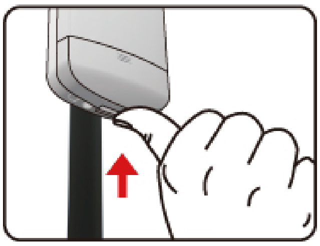


Slide the weatherproof sliding door downwards by griping onto the indented surface of the weatherproof sliding door and the rear.

◆ How to close the sliding door

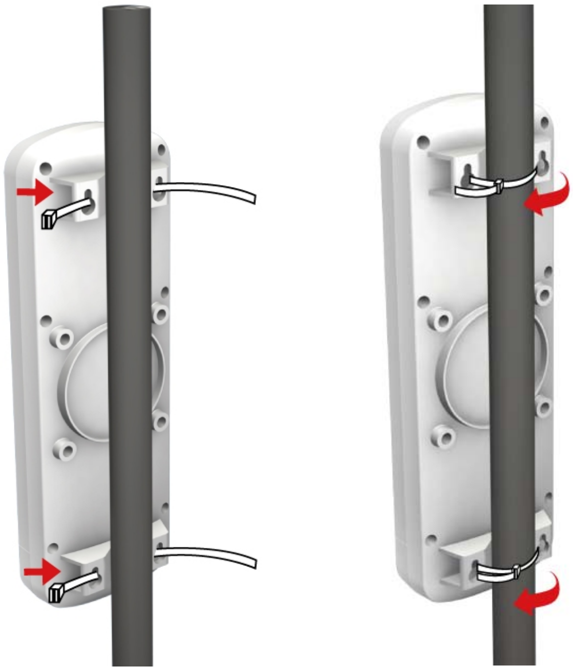


Align the base with the weatherproof sliding door.

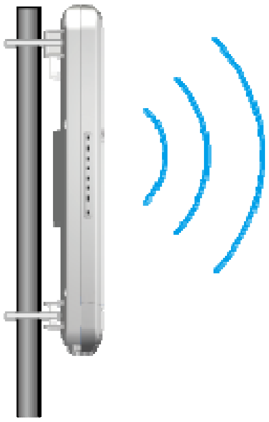


Slide the weatherproof sliding door upwards until it clicks into place.

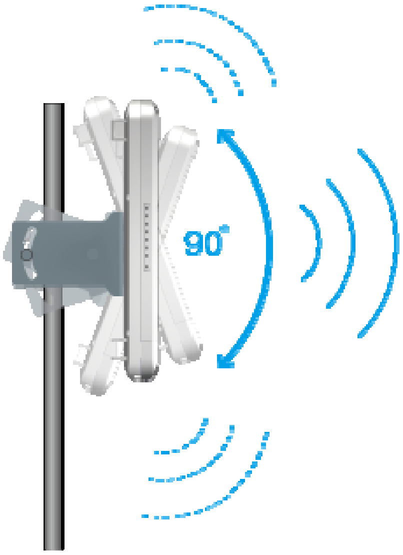
◆ How to tie the strap on the pole



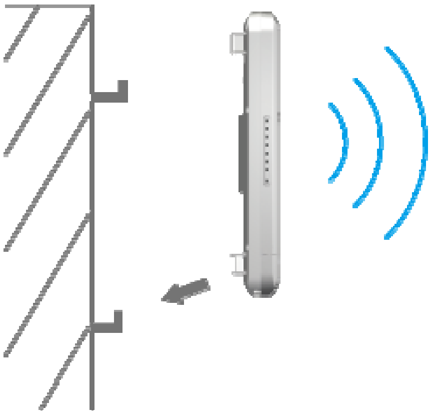
- Mounting and Radio forward Diagram



Standard Pole Mount



*Option Adjust Antenna L- Mount



*Option Wall Mount

INITIAL CONFIGURATION

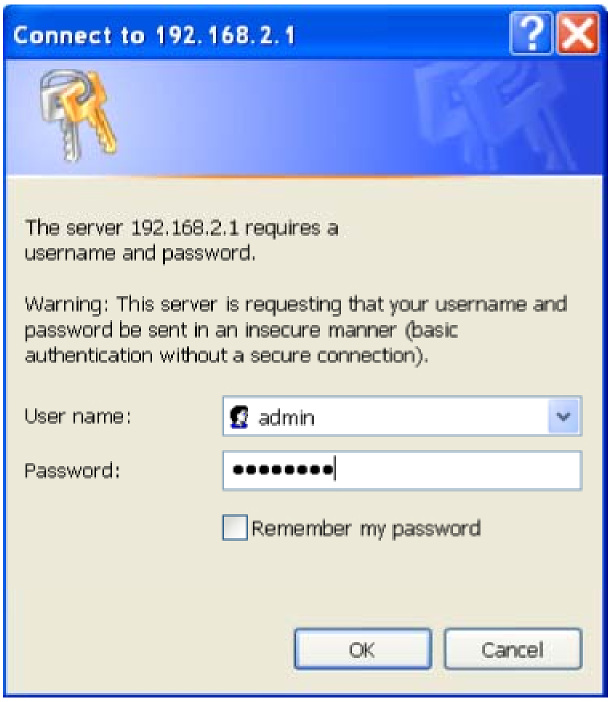
The SHD69A, 5GHz AP/CPE offers a user-friendly web-based management interface for the configuration of all the unit's features. Any PC directly attached to the unit can access the management interface using a web browser, such as Internet Explorer (version 6.0 or above).

CONNECTING TO THE LOGIN PAGE

It is recommended to make initial configuration changes by connecting a PC directly to the SHD69A's LAN port. The N5 has a default IP address of 192.168.2.1 and a subnet mask of 255.255.255.0. You must set your PC IP address to be on the same subnet as the SHD69A (that is, the PC and SHD69A addresses must both start 192.168.2.x). To access the SHD69A's management GUI interface, follow these steps:

1. Use your web browser to connect to the management interface using the default IP address of 192.168.2.1.

2. Log into the interface by entering the default username "admin" and password "admin," then click OK.



The server 192.168.2.1 requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

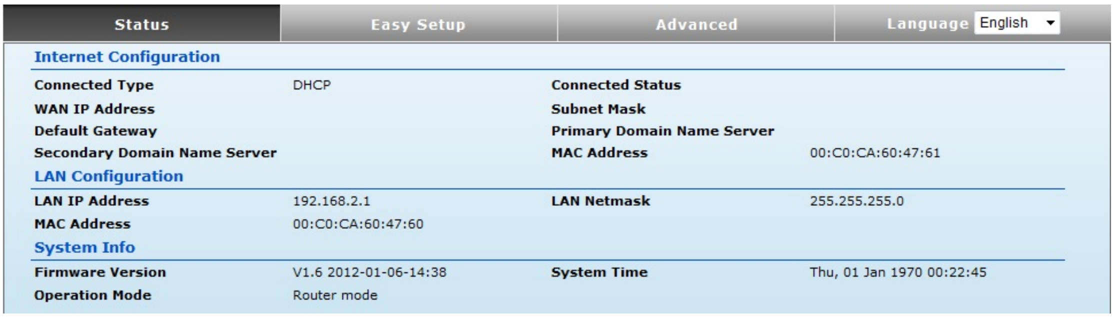
User name: admin

Password: •••••••••

□ Remember my password

STATUS PAGE

After logging in to the web interface, the Status page displays. The Home page top-menu-bar shows the Status, Easy Setup, Advanced and Language.



Internet Configuration

Connected Type	DHCP	Connected Status	
WAN IP Address		Subnet Mask	
Default Gateway		Primary Domain Name Server	
Secondary Domain Name Server		MAC Address	00:C0:CA:60:47:61

LAN Configuration

LAN IP Address	192.168.2.1	LAN Netmask	255.255.255.0
MAC Address	00:C0:CA:60:47:60		

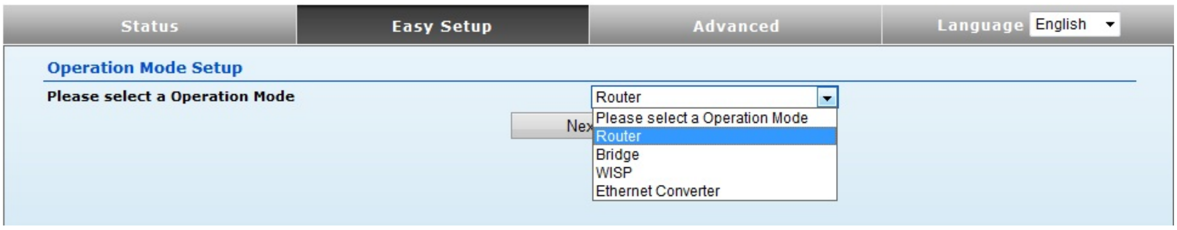
System Info

Firmware Version	V1.6 2012-01-06-14:38	System Time	Thu, 01 Jan 1970 00:22:45
Operation Mode	Router mode		

EASY SETUP

The Easy Setup is designed to help you configure the basic settings required to get the SHD69A up and running. There are only a few basic steps you need to set up the SHE69A to get the connection.

Click on Easy Setup to bring up the wizard

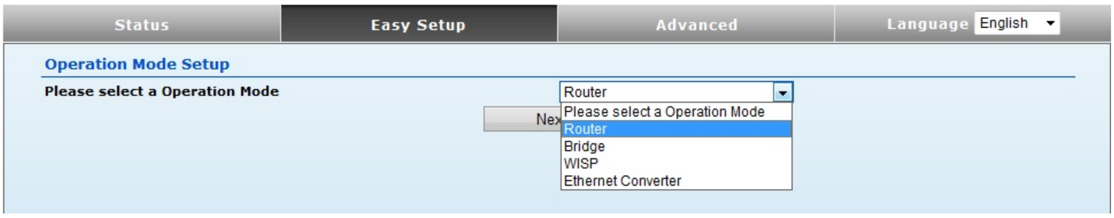


Operation Mode Setup

Please select a Operation Mode: Router

OPERATION MODE - ROUTER

In Router mode, the POE port of the SHD69A will turn into the WAN port. The wireless interface will become the LAN side. It will turn SHD69A into a wireless router. Since the Ethernet interface becomes WAN; if your PC is connected to the POE port, the management IP will change to the WAN IP (192.168.2.1). The remote management will be automatically turned on to allow you managing the device from the PoE WAN port..

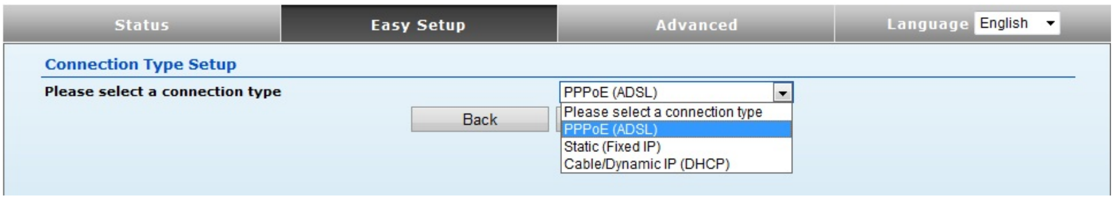


Operation Mode Setup

Please select a Operation Mode: Router

SETTINGS – PPPoE(ADSL)

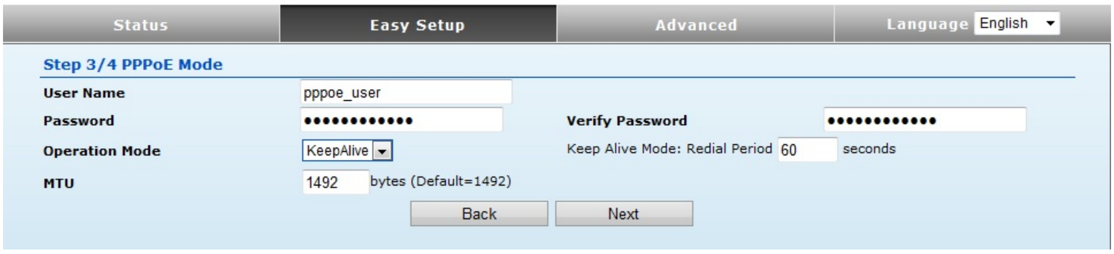
1) Select PPPoE to be assigned automatically from an Internet service provider (ISP) through a DSL modem using Point-to-Point Protocol over Ethernet (PPPoE).



Connection Type Setup

Please select a connection type: PPPoE (ADSL)

2)



Step 3/4 PPPoE Mode

User Name: pppoe_user

Password: ●●●●●●●●●●●● Verify Password: ●●●●●●●●●●●●

Operation Mode: KeepAlive Keep Alive Mode: Redial Period 60 seconds

MTU: 1492 bytes (Default=1492)

◆ **User Name** — Sets the PPPoE user name for the WAN port.

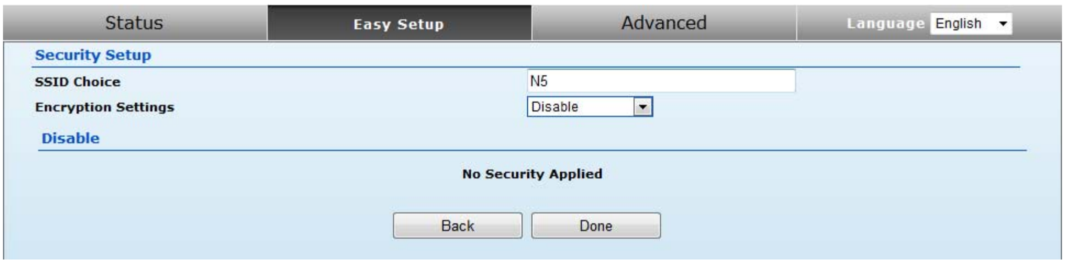
(Default: pppoe_user; Range: 1~32 characters)

◆ **Password** — Sets a PPPoE password for the WAN port.

(Default: pppoe_password; Range: 1~32 characters)

- **Verify Password** — Prompts you to re-enter your chosen password.
- **Operation Mode —** Enables and configures the keep alive time and configures the on-demand idle time.

3)



Security Setup

SSID Choice: N5

Encryption Settings: Disable

Disable

No Security Applied

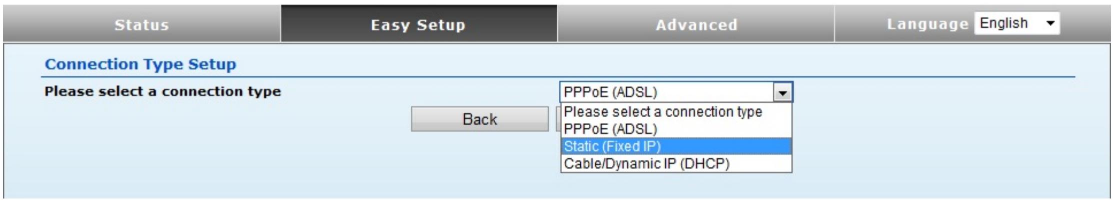
Security Setup

SSID Choice—The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security.

Security Mode — Select the security method and then configure the required parameters. (Options: Disabled, WEP-AUTO, WPA-PSK, WPA2-PSK, WPA-Auto-PSK, WPA, WPA2, WPA-Auto, 802.1X; Default: Disabled)

SETTINGS – STATIC (FIXED IP)

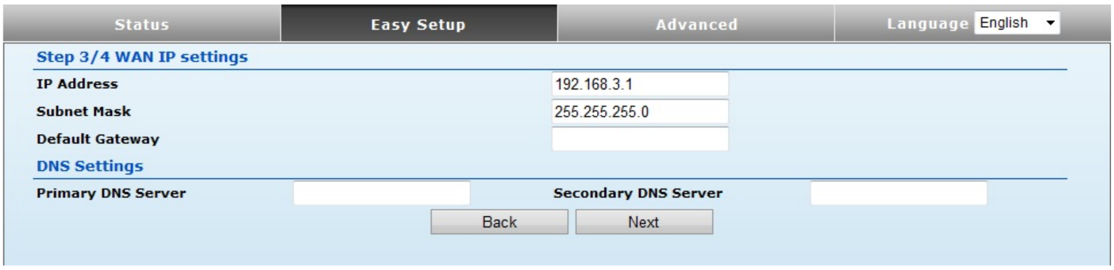
1) Select Static(Fixed IP), if your Internet service provider (ISP) to be permanent address on the Internet. A Static IP address is a number (in the form of a dotted quad)



Connection Type Setup

Please select a connection type: Static (Fixed IP)

2)



Step 3/4 WAN IP settings

IP Address: 192.168.3.1

Subnet Mask: 255.255.255.0

Default Gateway:

DNS Settings

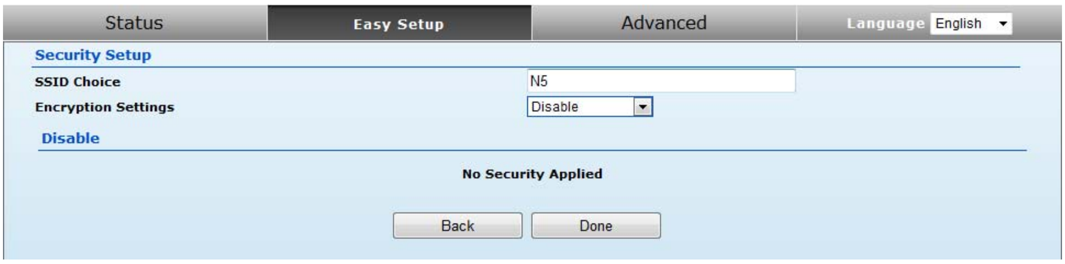
Primary DNS Server:

Secondary DNS Server:

- **IP Address** — Sets the static IP address.
- **Subnet Mask** — Sets the static IP subnet mask. (Default: 255.255.255.0)

- **Default Gateway** — The IP address of a router that is used when the requested destination IP address is not on the local subnet.
- **Primary DNS Server** — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.
- **Secondary DNS Server** — The IP address of the Secondary Domain Name Server.

3)



Security Setup

SSID Choice: N5

Encryption Settings: Disable

Disable

No Security Applied

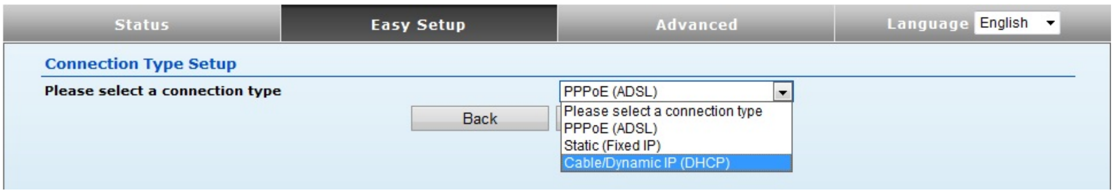
Security Setup

SSID Choice—The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security.

Security Mode — Select the security method and then configure the required parameters. (Options: Disabled, WEP-AUTO, WPA-PSK, WPA2-PSK, WPA-Auto-PSK, WPA, WPA2, WPA-Auto, 802.1X; Default: Disabled)

SETTINGS – CABLE/DYNAMIC IP (DHCP)

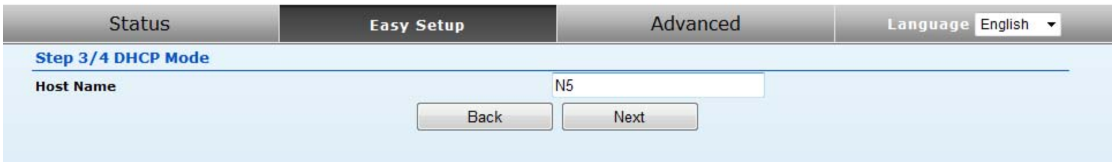
1) Select Cable/Dynamic IP (DHCP), if your Internet service provider (ISP) use a DHCP service to assign your Router an IP address when connecting to the Internet.



Connection Type Setup

Please select a connection type: Cable/Dynamic IP (DHCP)

2)

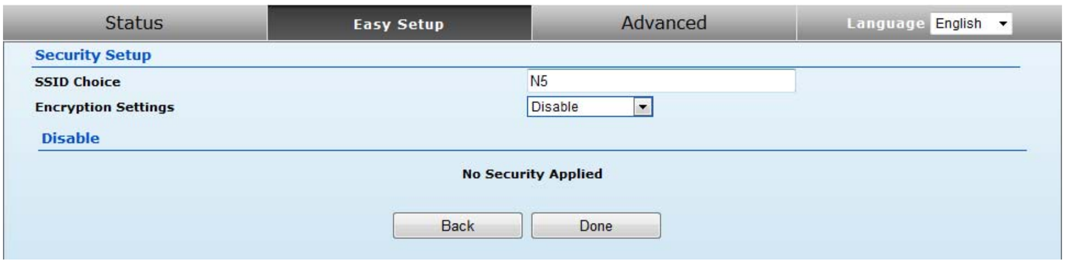


Step 3/4 DHCP Mode

Host Name: N5

The host name that you selected from the DDNS service provider.

3)



Security Setup

SSID Choice N5

Encryption Settings Disable

Disable

No Security Applied

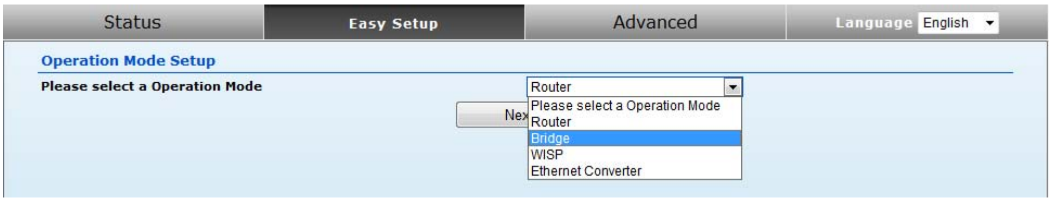
Security Setup

SSID Choice—The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security.

Security Mode — Select the security method and then configure the required parameters. (Options: Disabled, WEP-AUTO, WPA-PSK, WPA2-PSK, WPA-Auto-PSK, WPA, WPA2, WPA-Auto, 802.1X; Default: Disabled)

OPERATION MODE - BRIDGE

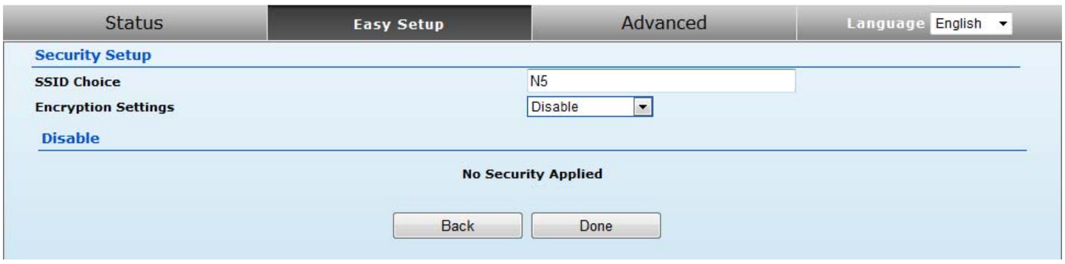
1) In this mode bridge your SHD69A to another Access Point.



Operation Mode Setup

Please select a Operation Mode Router

2)



Security Setup

SSID Choice N5

Encryption Settings Disable

Disable

No Security Applied

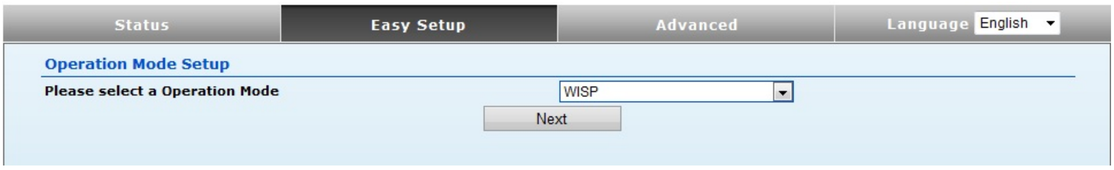
Security Setup

SSID Choice—The same name of SSID (Service Set Identification) must be assigned to all wireless devices in your network. Considering your wireless network security.

Security Mode — Select the security method and then configure the required parameters. (Options: Disabled, WEP-AUTO, WPA-PSK, WPA2-PSK, WPA-Auto-PSK, WPA, WPA2, WPA-Auto, 802.1X; Default: Disabled)

OPERATION MODE - WISP

In the WISP mode is also known as Client Router. The SHD69A wireless side is connected to the remote AP (Base-Station) as in Client Infrastructure mode. Between the wireless and LAN is the IP sharing router function. This is used to share WISP connection. The WAN is on the wireless side.

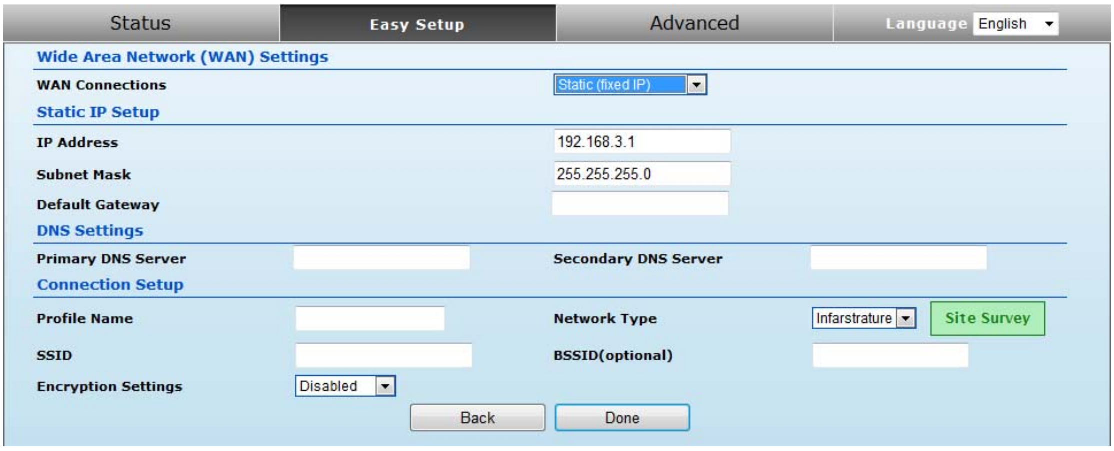


Operation Mode Setup

Please select a Operation Mode: WISP

SETTINGS – STATIC (FIXED IP)

1) Select this setting if the WAN connection uses a permanent, fixed (static) IP address that your ISP assigned.



Wide Area Network (WAN) Settings

WAN Connections: Static (fixed IP)

Static IP Setup

IP Address: 192.168.3.1

Subnet Mask: 255.255.255.0

Default Gateway:

DNS Settings

Primary DNS Server: Secondary DNS Server:

Connection Setup

Profile Name: Network Type: Infarstrature

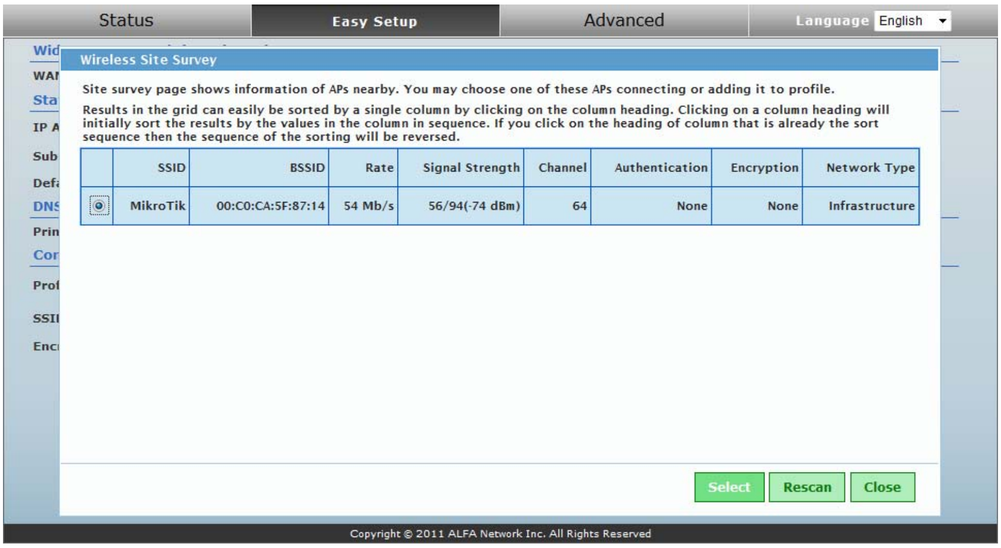
SSID: BSSID(optional):

Encryption Settings: Disabled

- **IP Address** — Sets the static IP address.
- **Subnet Mask** — Sets the static IP subnet mask. (Default: 255.255.255.0)
- **Default Gateway** — The IP address of a router that is used when the requested destination IP address is not on the local subnet.
- **Primary DNS Server** — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.
- **Secondary DNS Server** — The IP address of the Secondary Domain Name Server.

2) Press **Site Survey** button and look for available wireless network then click on the

SSID that you attempt to connect to it; MikroTik is the SSID that we are going to connect in this example. Press **Select** button when finished.



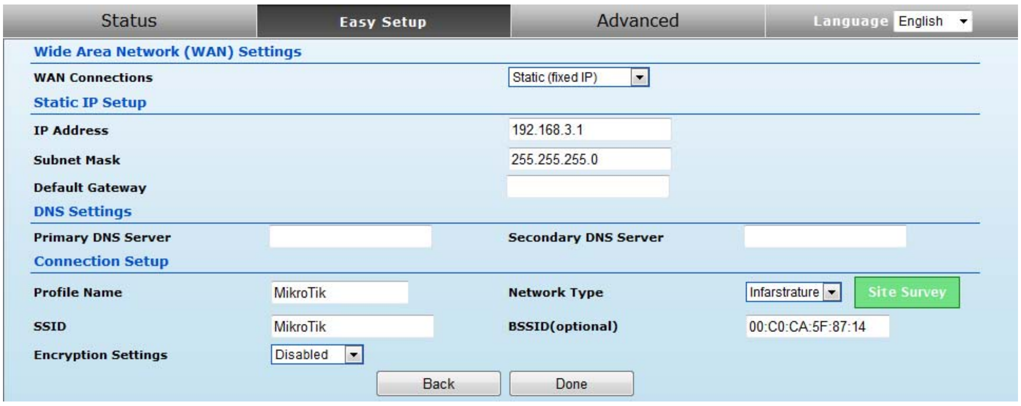
Wireless Site Survey

Site survey page shows information of APs nearby. You may choose one of these APs connecting or adding it to profile.

Results in the grid can easily be sorted by a single column by clicking on the column heading. Clicking on a column heading will initially sort the results by the values in the column in sequence. If you click on the heading of column that is already the sort sequence then the sequence of the sorting will be reversed.

	SSID	BSSID	Rate	Signal Strength	Channel	Authentication	Encryption	Network Type
●	MikroTik	00:C0:CA:5F:87:14	54 Mb/s	56/94(-74 dBm)	64	None	None	Infrastructure

3) Now, it shows the Profile Name, SSID, BSSID, and encryption type received from your target network and press **Done** button when is finished.



Wide Area Network (WAN) Settings

WAN Connections: Static (fixed IP)

Static IP Setup

IP Address: 192.168.3.1

Subnet Mask: 255.255.255.0

Default Gateway:

DNS Settings

Primary DNS Server: Secondary DNS Server:

Connection Setup

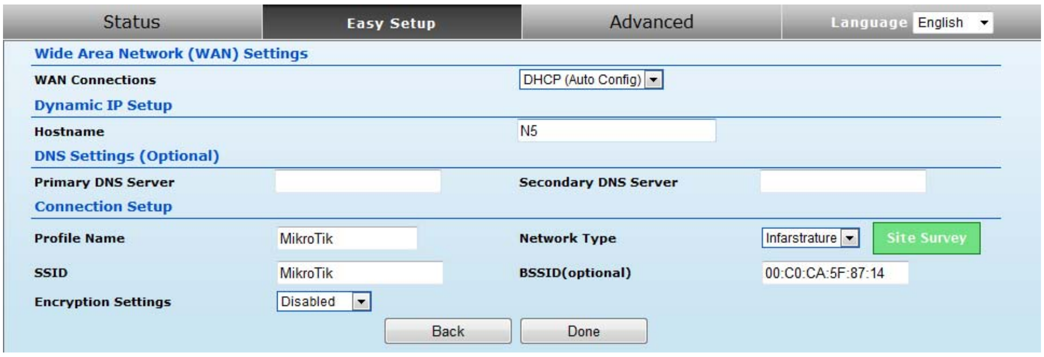
Profile Name: MikroTik Network Type: Infarstrature

SSID: MikroTik BSSID(optional): 00:C0:CA:5F:87:14

Encryption Settings: Disabled

SETTINGS – DHCP (AUTO CONFIG)

1) Select this setting if the WAN connection uses a DHCP service to assign your Router and IP address when connecting to Internet.



Wide Area Network (WAN) Settings

WAN Connections: DHCP (Auto Config)

Dynamic IP Setup

Hostname: N5

DNS Settings (Optional)

Primary DNS Server:
Secondary DNS Server:

Connection Setup

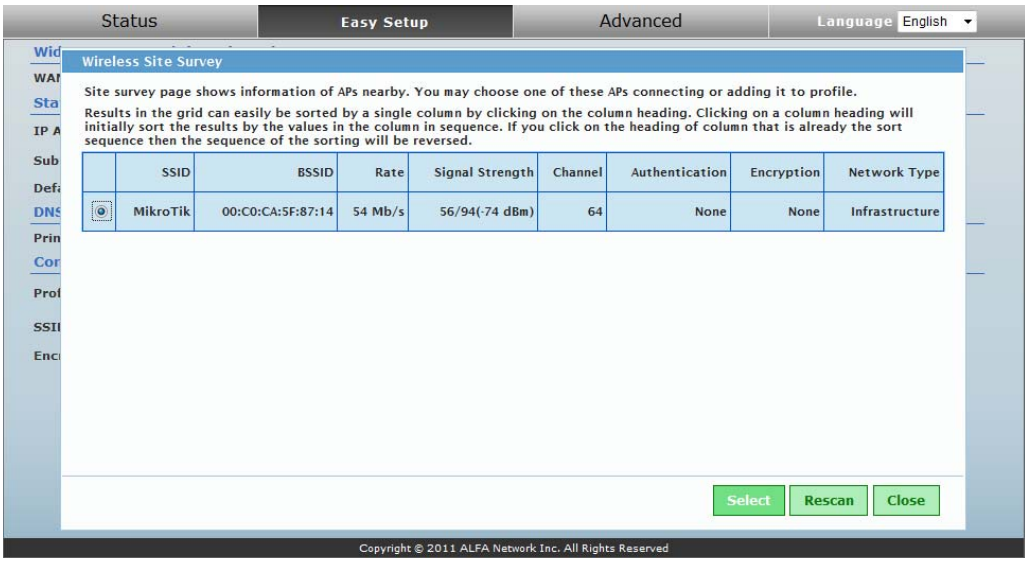
Profile Name: MikroTik
Network Type: Infarstrature

SSID: MikroTik
BSSID(optional): 00:C0:CA:5F:87:14

Encryption Settings: Disabled

- **IP Address** — Sets the static IP address.
- **Subnet Mask** — Sets the static IP subnet mask. (Default: 255.255.255.0)
- **Default Gateway** — The IP address of a router that is used when the requested destination IP address is not on the local subnet.
- **Primary DNS Server** — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.
- **Secondary DNS Server** — The IP address of the Secondary Domain Name Server.

2) Press **Site Survey** button and look for available wireless network then click on the SSID that you attempt to connect to it; MikroTik is the SSID that we are going to connect in this example. Press **Select** button when finished.



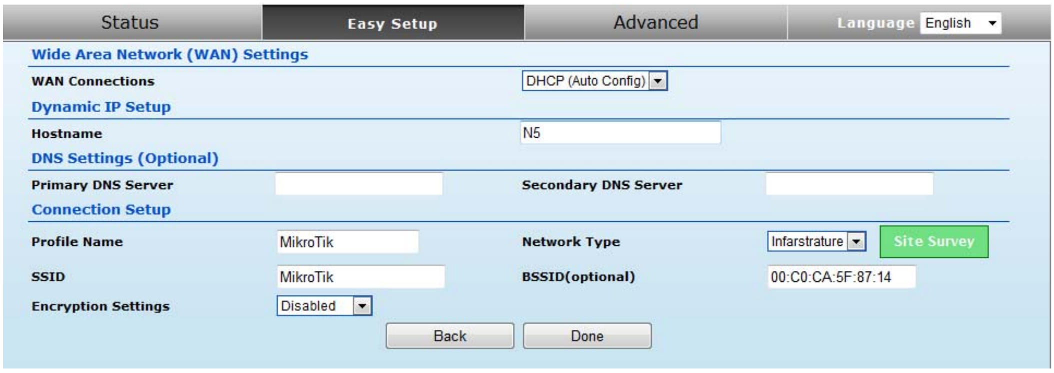
Wireless Site Survey

Site survey page shows information of APs nearby. You may choose one of these APs connecting or adding it to profile.

Results in the grid can easily be sorted by a single column by clicking on the column heading. Clicking on a column heading will initially sort the results by the values in the column in sequence. If you click on the heading of column that is already the sort sequence then the sequence of the sorting will be reversed.

	SSID	BSSID	Rate	Signal Strength	Channel	Authentication	Encryption	Network Type
◉	MikroTik	00:C0:CA:5F:87:14	54 Mb/s	56/94(-74 dBm)	64	None	None	Infrastructure

3) Now, it shows the Profile Name, SSID, BSSID, and encryption type received from your target network and press **Done** button when is finished.



Wide Area Network (WAN) Settings

WAN Connections: DHCP (Auto Config)

Dynamic IP Setup

Hostname: N5

DNS Settings (Optional)

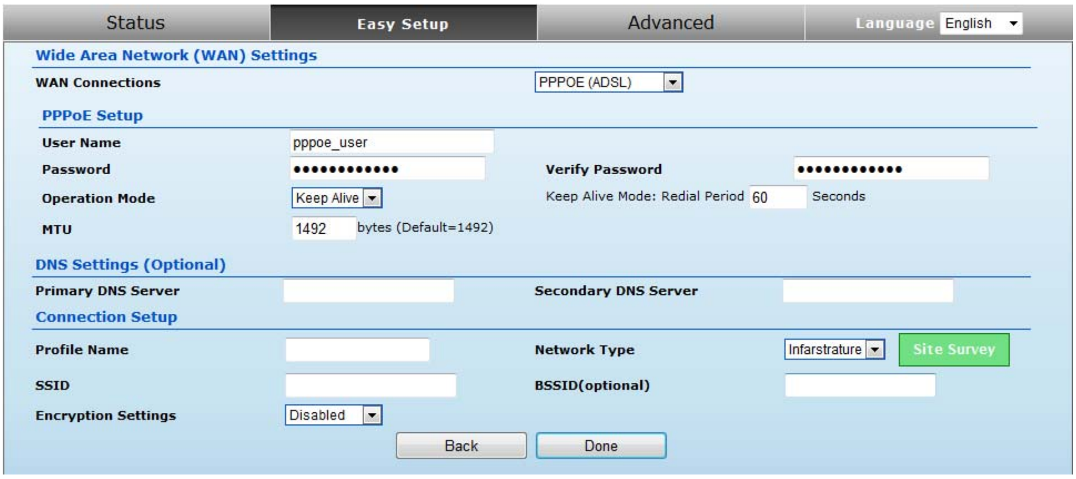
Primary DNS Server:
Secondary DNS Server:

Connection Setup

Profile Name: MikroTik
Network Type: Infarstrature
SSID: MikroTik
BSSID(optional): 00:C0:CA:5F:87:14
Encryption Settings: Disabled

SETTINGS – PPPOE(ADSL)

1) Select PPPoE to be assigned automatically from an Internet service provider (ISP) through a DSL modem using Point-to-Point Protocol over Ethernet (PPPoE).



Wide Area Network (WAN) Settings

WAN Connections: PPPOE (ADSL)

PPPoE Setup

User Name: pppoe_user
Password: ●●●●●●●●●●●●
Verify Password: ●●●●●●●●●●●●
Operation Mode: Keep Alive
Keep Alive Mode: Redial Period 60 Seconds
MTU: 1492 bytes (Default=1492)

DNS Settings (Optional)

Primary DNS Server:
Secondary DNS Server:

Connection Setup

Profile Name:
Network Type: Infarstrature
SSID:
BSSID(optional):
Encryption Settings: Disabled

- **User Name** — Sets the PPPoE user name for the WAN port.

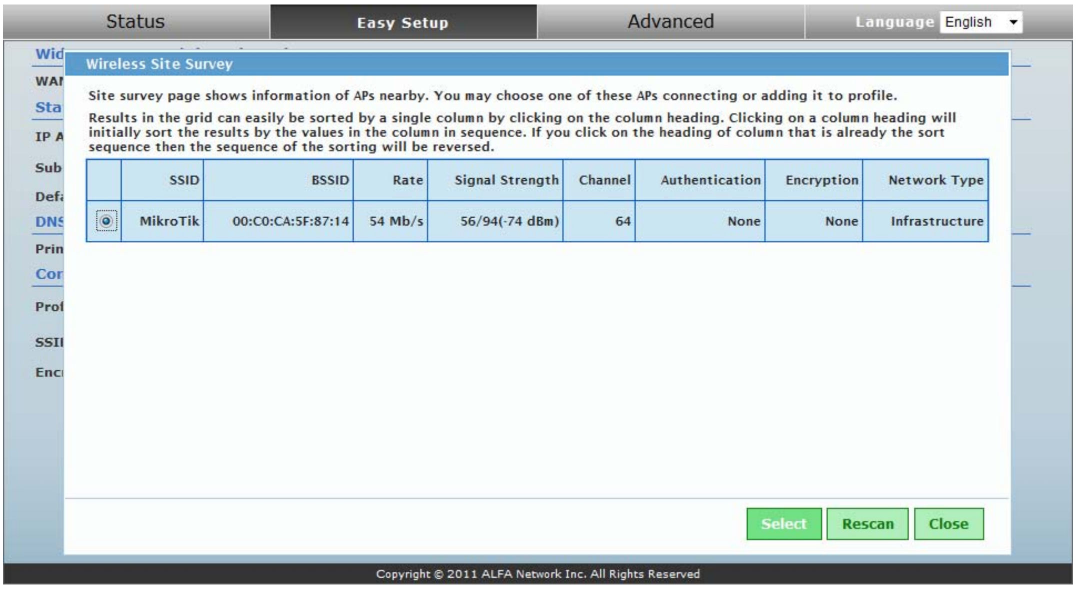
(Default: pppoe_user; Range: 1~32 characters)

- **Password** — Sets a PPPoE password for the WAN port.

(Default: pppoe_password; Range: 1~32 characters)

- **Verify Password** — Prompts you to re-enter your chosen password.
- **Operation Mode —** Enables and configures the keep alive time and configures the on-demand idle time

2) Press **Site Survey** button and look for available wireless network then click on the SSID that you attempt to connect to it; MikroTik is the SSID that we are going to connect in this example. Press **Select** button when finished.



Wireless Site Survey

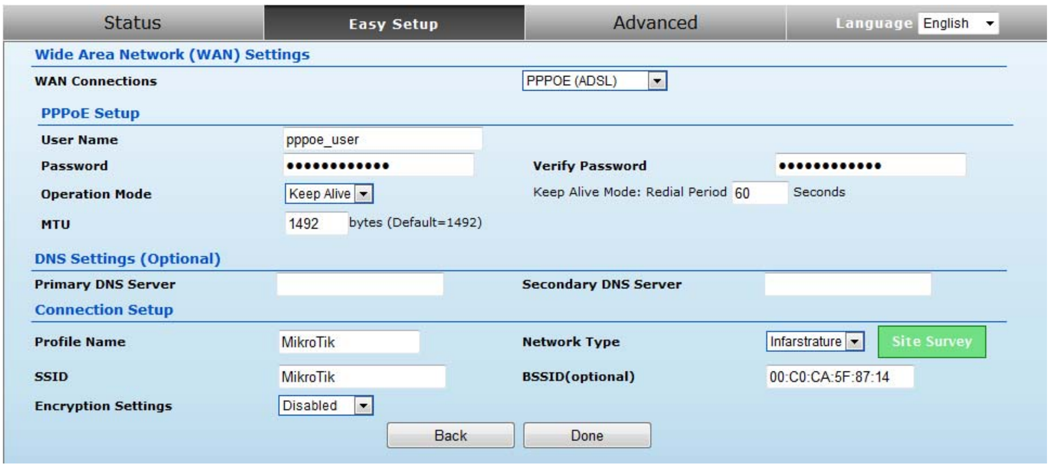
Site survey page shows information of APs nearby. You may choose one of these APs connecting or adding it to profile.

Results in the grid can easily be sorted by a single column by clicking on the column heading. Clicking on a column heading will initially sort the results by the values in the column in sequence. If you click on the heading of column that is already the sort sequence then the sequence of the sorting will be reversed.

	SSID	BSSID	Rate	Signal Strength	Channel	Authentication	Encryption	Network Type
●	MikroTik	00:C0:CA:5F:87:14	54 Mb/s	56/94(-74 dBm)	64	None	None	Infrastructure

Copyright © 2011 ALFA Network Inc. All Rights Reserved

3) Now, it shows the Profile Name, SSID, BSSID, and encryption type received from your target network and press **Done** button when is finished.



Wide Area Network (WAN) Settings

WAN Connections: PPPOE (ADSL)

PPPoE Setup

User Name: pppoe_user

Password: ●●●●●●●●●●●● Verify Password: ●●●●●●●●●●●●

Operation Mode: Keep Alive Keep Alive Mode: Redial Period 60 Seconds

MTU: 1492 bytes (Default=1492)

DNS Settings (Optional)

Primary DNS Server: Secondary DNS Server:

Connection Setup

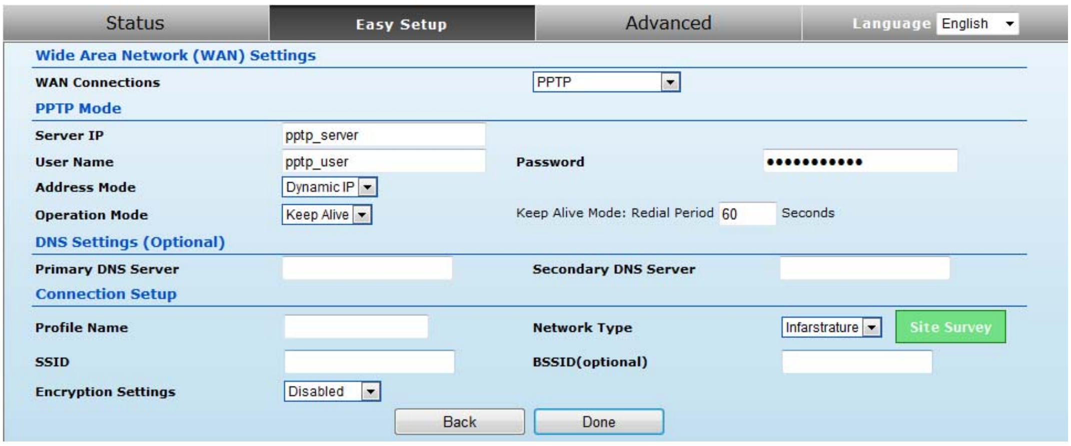
Profile Name: MikroTik Network Type: Infarstrature

SSID: MikroTik BSSID(optional): 00:C0:CA:5F:87:14

Encryption Settings: Disabled

SETTINGS – PPTP

1) Select PPTP if your ISP provides PPTP connection, please select **PPTP** option.



Wide Area Network (WAN) Settings

WAN Connections: PPTP

PPTP Mode

Server IP: pptp_server

User Name: pptp_user

Password: ●●●●●●●●●●●

Address Mode: Dynamic IP

Operation Mode: Keep Alive

Keep Alive Mode: Redial Period 60 Seconds

DNS Settings (Optional)

Primary DNS Server:

Secondary DNS Server:

Connection Setup

Profile Name:

Network Type: Infarstrature

SSID:

BSSID(optional):

Encryption Settings: Disabled

- **Server IP** — Sets the PPTP server IP Address. (Default: pptp_server)
- **User Name** — Sets the PPTP user name for the WAN port.

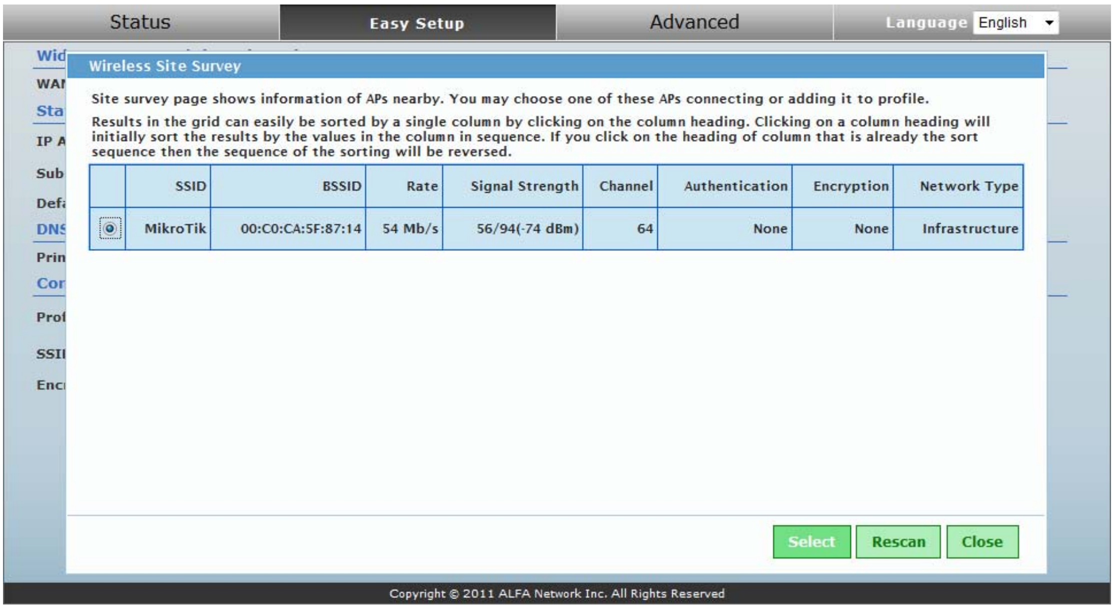
(Default: pptp_user; Range: 1~32 characters)

- **Password** — Sets a PPTP password for the WAN port. (Default:

pptp_password; Range: 1~32 characters)

- **Address Mode** — Sets a PPTP network mode. (Default: Dynamic)
- **Operation Mode —** Enables and configures the keep alive time.

2) Press **Site Survey** button and look for available wireless network then click on the SSID that you attempt to connect to it; MikroTik is the SSID that we are going to connect in this example. Press **Select** button when finished.



Wireless Site Survey

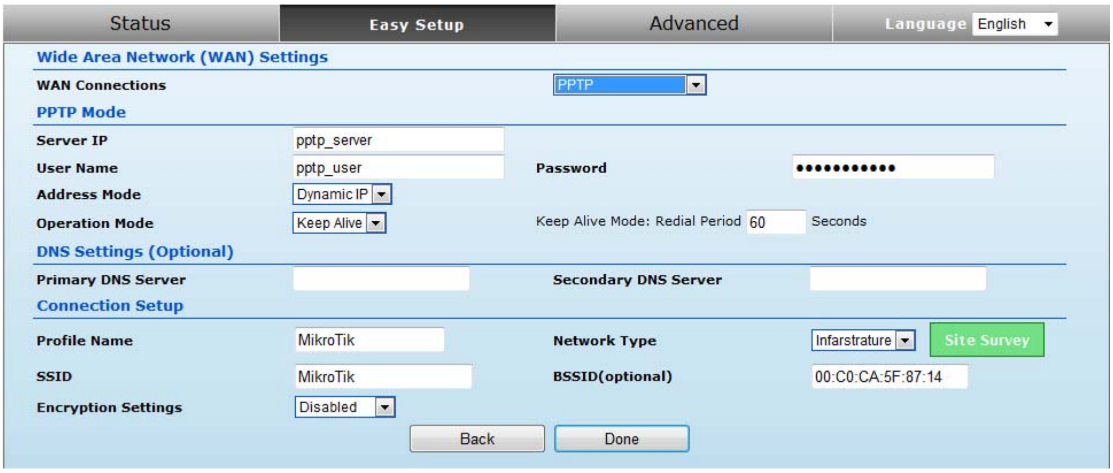
Site survey page shows information of APs nearby. You may choose one of these APs connecting or adding it to profile.

Results in the grid can easily be sorted by a single column by clicking on the column heading. Clicking on a column heading will initially sort the results by the values in the column in sequence. If you click on the heading of column that is already the sort sequence then the sequence of the sorting will be reversed.

	SSID	BSSID	Rate	Signal Strength	Channel	Authentication	Encryption	Network Type
◉	MikroTik	00:C0:CA:5F:87:14	54 Mb/s	56/94(-74 dBm)	64	None	None	Infrastructure

Copyright © 2011 ALFA Network Inc. All Rights Reserved

3) Now, it shows the Profile Name, SSID, BSSID, and encryption type received from your target network and press **Done** button when is finished.



Wide Area Network (WAN) Settings

WAN Connections	PPTP		

PPTP Mode

Server IP	pptp_server		
User Name	pptp_user	Password	●●●●●●●●●●●
Address Mode	Dynamic IP		
Operation Mode	Keep Alive	Keep Alive Mode: Redial Period	60 Seconds

DNS Settings (Optional)

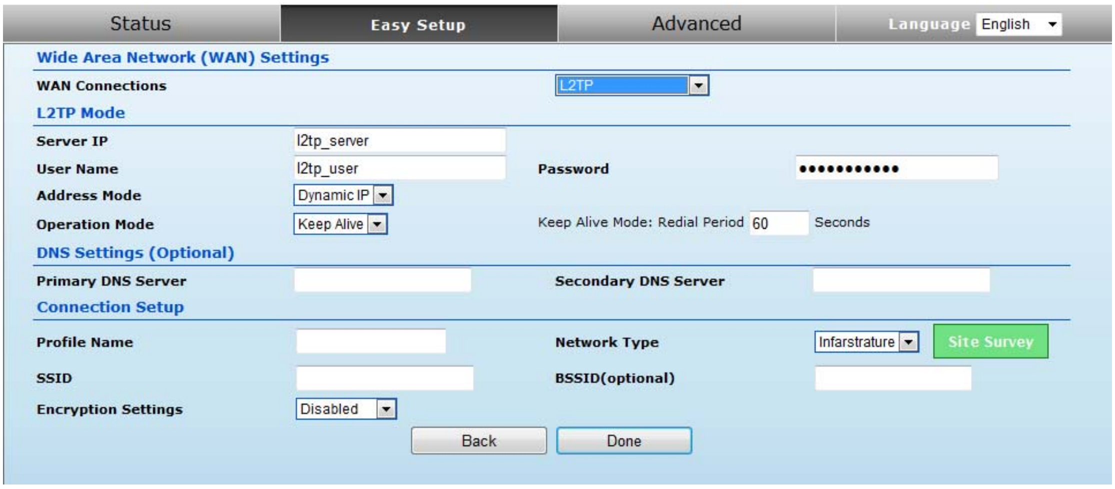
Primary DNS Server		Secondary DNS Server	

Connection Setup

Profile Name	MikroTik	Network Type	Infarstrature
SSID	MikroTik	BSSID(optional)	00:C0:CA:5F:87:14
Encryption Settings	Disabled		

SETTINGS –L2TP

1) Select L2TP if your ISP provides PPTP connection, please select **L2TP** option.



Wide Area Network (WAN) Settings

WAN Connections	L2TP		

L2TP Mode

Server IP	l2tp_server		
User Name	l2tp_user	Password	●●●●●●●●●●●
Address Mode	Dynamic IP		
Operation Mode	Keep Alive	Keep Alive Mode: Redial Period	60 Seconds

DNS Settings (Optional)

Primary DNS Server		Secondary DNS Server	

Connection Setup

Profile Name		Network Type	Infarstrature
SSID		BSSID(optional)	
Encryption Settings	Disabled		

- **Server IP** — Sets the L2TP server IP Address. (Default: l2tp_server)
- **User Name** — Sets the L2TP user name for the WAN port.

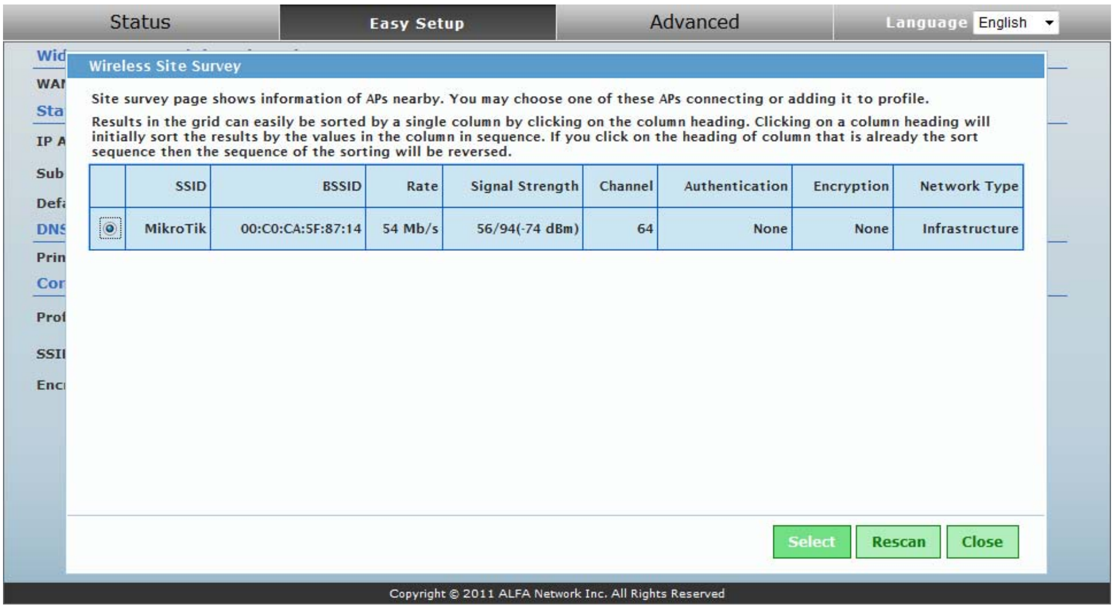
(Default: pptp_user; Range: 1~32 characters)

- **Password** — Sets a L2TP password for the WAN port. (Default:

pptp_password; Range: 1~32 characters)

- **Address Mode** — Sets a L2TP network mode. (Default: Dynamic)
- **Operation Mode —** Enables and configures the keep alive time.

2) Press **Site Survey** button and look for available wireless network then click on the SSID that you attempt to connect to it; MikroTik is the SSID that we are going to connect in this example. Press **Select** button when finished.



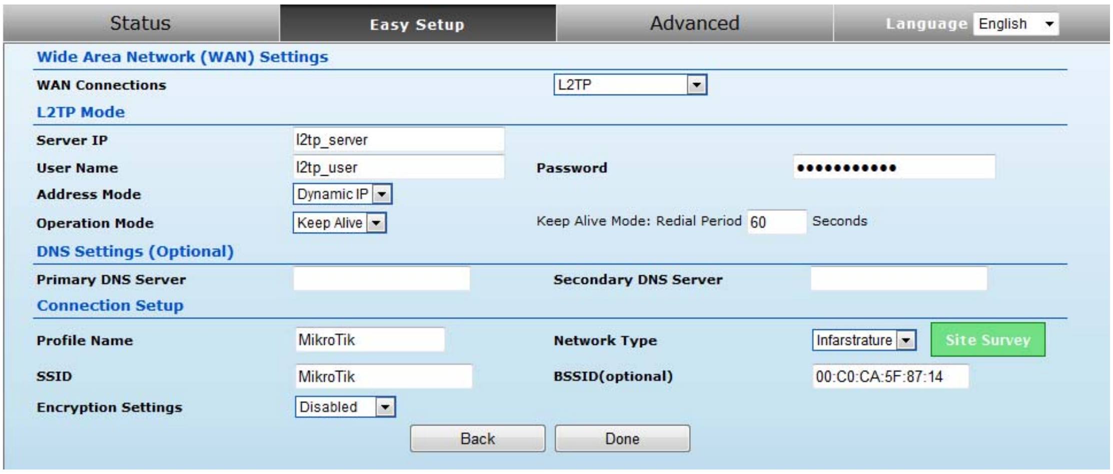
Wireless Site Survey

Site survey page shows information of APs nearby. You may choose one of these APs connecting or adding it to profile.

Results in the grid can easily be sorted by a single column by clicking on the column heading. Clicking on a column heading will initially sort the results by the values in the column in sequence. If you click on the heading of column that is already the sort sequence then the sequence of the sorting will be reversed.

	SSID	BSSID	Rate	Signal Strength	Channel	Authentication	Encryption	Network Type
◉	MikroTik	00:C0:CA:5F:87:14	54 Mb/s	56/94(-74 dBm)	64	None	None	Infrastructure

3) Now, it shows the Profile Name, SSID, BSSID, and encryption type received from your target network and press **Done** button when is finished.



Wide Area Network (WAN) Settings

WAN Connections		L2TP	

L2TP Mode

Server IP	l2tp_server		
User Name	l2tp_user	Password	●●●●●●●●●●●
Address Mode	Dynamic IP		
Operation Mode	Keep Alive	Keep Alive Mode: Redial Period	60 Seconds

DNS Settings (Optional)

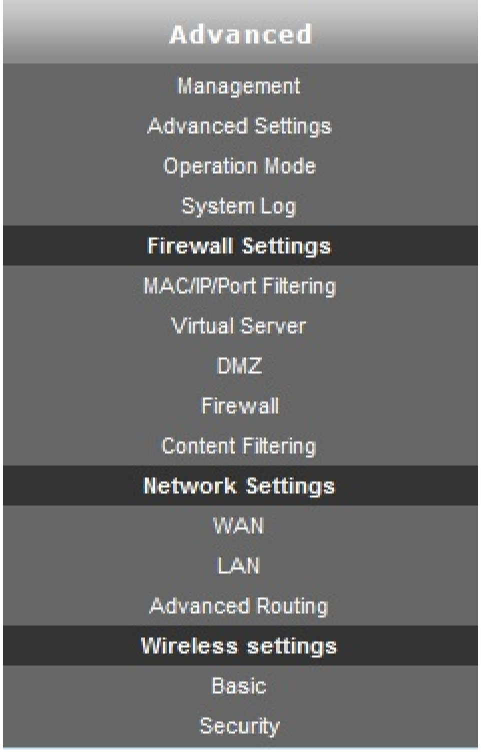
Primary DNS Server		Secondary DNS Server	

Connection Setup

Profile Name	MikroTik	Network Type	Infarstrature
SSID	MikroTik	BSSID(optional)	00:C0:CA:5F:87:14
Encryption Settings	Disabled		

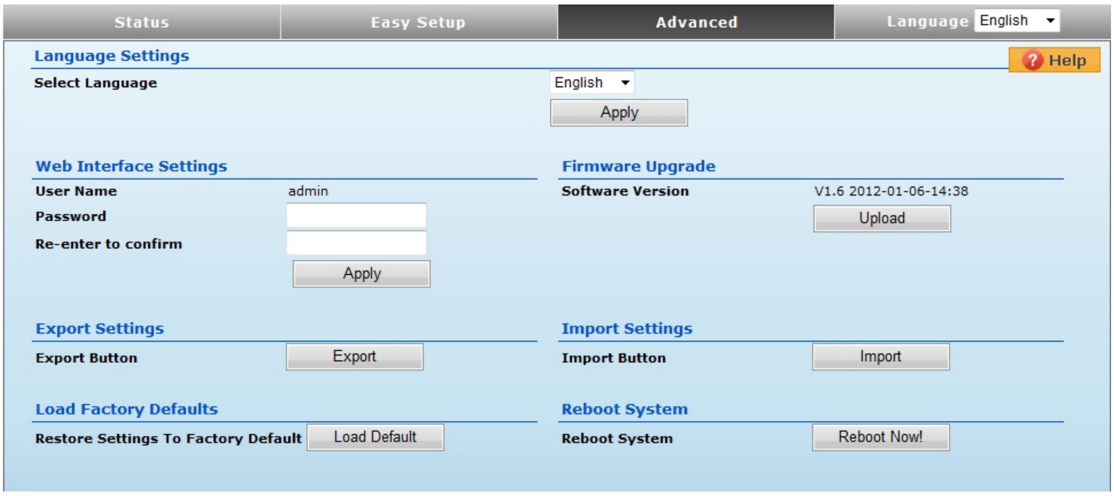
ADVANCED SETUP

In the Advanced Manual Bar, it includes all the settings such as firmware upgrade, LAN, WAN and wireless settings that change the RF behaviors. It is important to read through this section before attempting to make changes.



MANAGEMENT

The Management section is provided for configuration of administrative needs such as language type, user name / Password, firmware upgrade, export and import settings, load factory defaults and reboots system.



Language Settings
Select Language: English

Web Interface Settings
User Name: admin
Password
Re-enter to confirm

Firmware Upgrade
Software Version: V1.6 2012-01-06-14:38

Export Settings
Export Button

Import Settings
Import Button

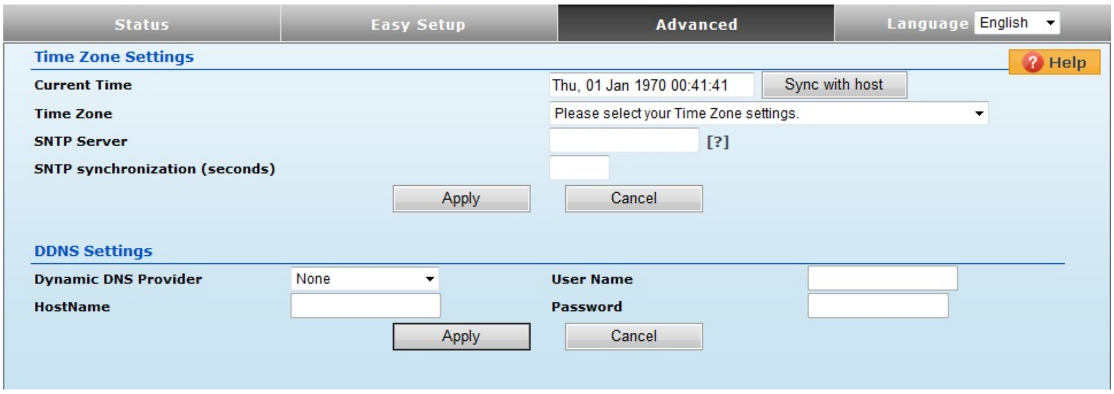
Load Factory Defaults
Restore Settings To Factory Default

Reboot System
Reboot System

- **Language Setting** — Select the Language.
- **Password** — The new password must not exceed 32 characters in length and must not include any spaces. Enter the new password a second time to confirm it.
- **Export Settings** — Click the Export Button to download current router configuration to your PC.
- **Import Settings** — Click the Import Button to browse for the configuration file that is currently saved on your PC. Click Import to overwrite all current configurations with the one in the configuration file.
- **Load Factory Defaults** — If you have problems with SHD69A, which might be a result from changing some settings, but you are unsure what settings exactly, you can restore the factory defaults by click the Load Default Button.
- **Reboot System** — If you want to reboot the SHD69A, click the Reboot Now Button.

ADVANCED SETTINGS

The Advanced Settings section is provided for configuration of Time Zone and DDNS.



Time Zone Settings

Current Time: Thu, 01 Jan 1970 00:41:41

Time Zone: Please select your Time Zone settings.

SNTP Server

SNTP synchronization (seconds)

DDNS Settings

Dynamic DNS Provider: None

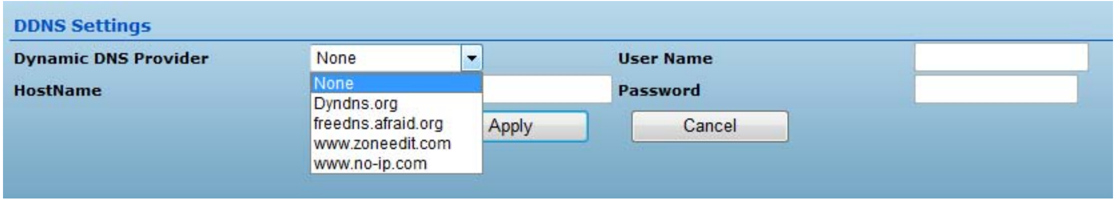
HostName

User Name

Password

Language: English

- **Time Zone Settings** — The Time Zone Settings allows you to configure, update and maintain the correct time on the SHD69A's internal system clock.
- **DDNS Settings** — DDNS lets you assign a fixed host and domain name to dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the SHD69A. Before using this feature, you need to sign up for DDNS service at www.dyndns.org , a DDNS service provider.
- **SNTP Server** — Enter the address of an SNTP server to receive time updates.
- **SNTP synchronization (seconds)** — Specify the interval between SNTP server updates.



DDNS Settings

Dynamic DNS Provider: None

HostName

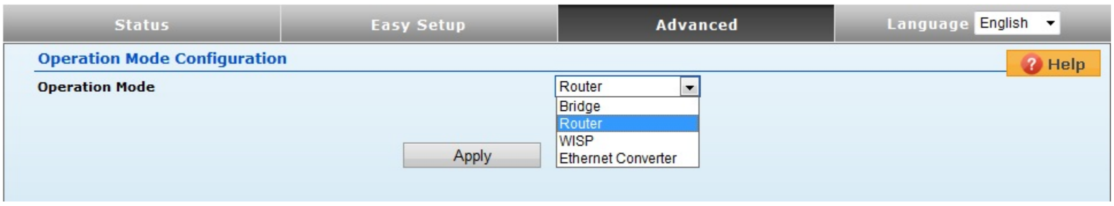
User Name

Password

- **User Name** — Sets the DDNS user name for the connection.
- **Password** — Sets a DDNS password for the connection.
- **HostName —** The host name that you selected from the DDNS service provider.

Operation Mode

The Operation Mode content four modes: Bridge, router, WISP and Ethernet converter.



Operation Mode Configuration

Operation Mode: Router

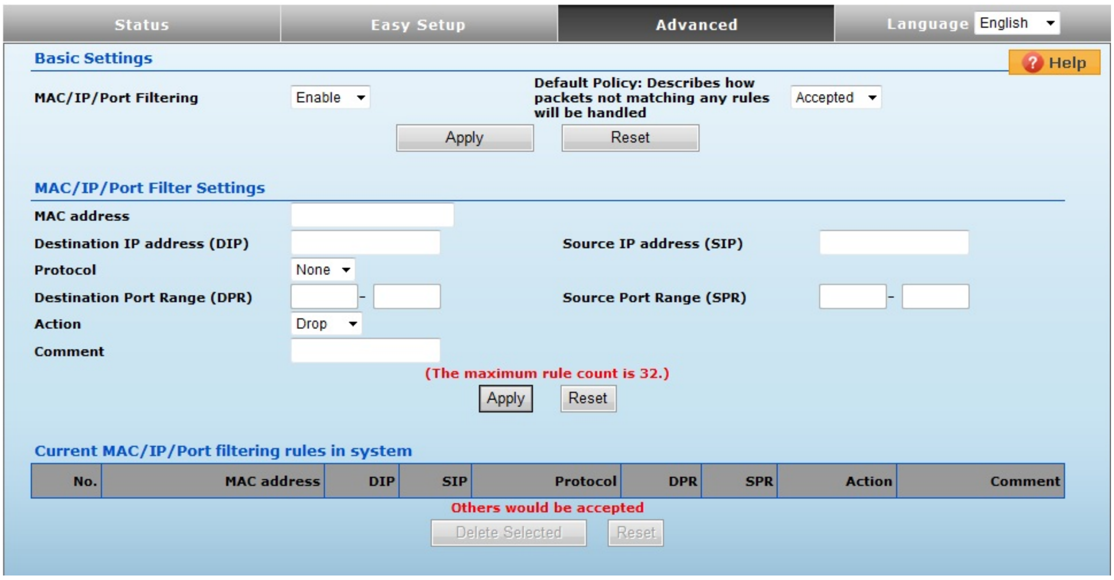
Bridge
Router
WISP
Ethernet Converter

- **Bridge** — The wired Ethernet and wireless are bridged together. Once the mode is selected, all WAN related functions will be disabled.
- **Router** — The WAN port is used to connect with ADSL/Cable modem and the wireless is used for your private WLAN. The NAT is existed between the 2 RJ45 ports and all wireless clients share the same public IP address through the WAN port to ISP. The default IP configuration for WAN port is DHCP client
- **WISP** — The SHD69A will behave just the same as the client mode for wireless function. However, router functions are added between the wireless WAN side and the Ethernet LAN side. Therefore, the WSIP subscriber can share the WISP connection without the extra router.
- **Ethernet Converter** — The wireless client interface is treated as WAN port, and the wireless interface and the Ethernet port are LAN ports.

Firewall Configuration

MAC/IP/Port Filtering

MAC/IP/Port filtering restricts connection parameters to limit the risk of intrusion and defends against a wide array of common hacker attacks. MAC/IP/Port filtering allows the unit to permit, deny or proxy traffic through its MAC addresses, IP addresses and ports. The SHD69A allows you define a sequential list of permit or deny filtering rules (up to 32). This device tests ingress packets against the filter rules one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the packet is either accepted or dropped depending on the default policy setting.



Basic Settings

MAC/IP/Port Filtering	Enable
Default Policy: Describes how packets not matching any rules will be handled	Accepted

MAC/IP/Port Filter Settings

MAC address			
Destination IP address (DIP)		Source IP address (SIP)	
Protocol	None		
Destination Port Range (DPR)	-	Source Port Range (SPR)	-
Action	Drop		
Comment			

(The maximum rule count is 32.)

Current MAC/IP/Port filtering rules in system

No.	MAC address	DIP	SIP	Protocol	DPR	SPR	Action	Comment

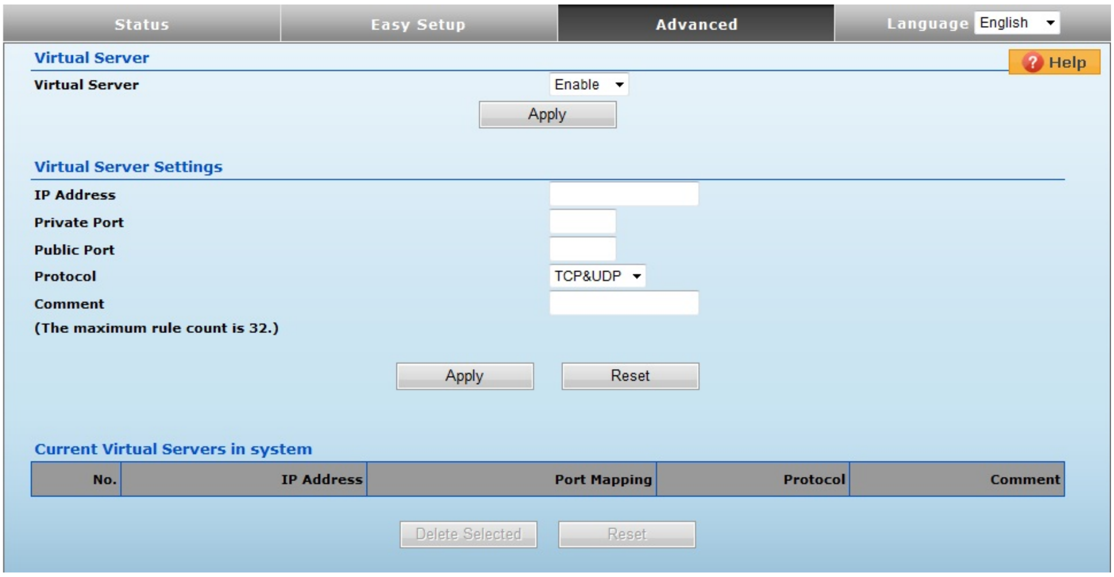
Others would be accepted

- **MAC/IP/Port Filtering** — Enables or disables MAC/IP/Port Filtering. (Default: Disable)
- **Default Policy** — When MAC/IP/Port Filtering is enabled, the default policy will be enabled. If you set the default policy to “Dropped”, all incoming packets that don’t match the rules will be dropped. If the policy is set to "Accepted," all incoming packets that don't match the rules are accepted. (Default: Dropped)
- **MAC Address** — Specifies the MAC address to block or allow traffic from.
- **Destination IP Address** — Specifies the destination IP address to block or allow traffic from.
- **Source IP Address** — Specifies the source IP address to block or allow traffic from.
- **Protocol** — Specifies the destination port type, TCP, UDP or ICMP. (Default: None).
- **Destination Port Range** — Specifies the range of destination port to block traffic from the specified LAN IP address from reaching.
- **Source Port Range** — Specifies the range of source port to block traffic from the specified LAN IP address from reaching.
- **Action** — Specifies if traffic should be accepted or dropped. (Default: Accept)
- **Comment** — Enter a useful comment to help identify the filtering rules.
- **Current Filtering rules** — The Current Filter Table displays the configured IP addresses and ports that are permitted or denied access to and from.
  - **No.** — The table entry number.
  - **MAC Address** — Displays a MAC address to filter.
  - **Destination IP Address (DIP)** — Displays the destination IP address.
  - **Source IP Address (SIP)** — Displays the source IP address.
  - **Protocol** — Displays the protocol type.
  - **Destination Port Range (DPR)** — Displays the destination port range.

- **Source Port Range (SPR)** — Displays the source port range.
- **Action** — Displays if the specified traffic is accepted or dropped.
- **Comment** — Displays a useful comment to identify the filter rules.

VIRTUAL SERVER SETTINGS

Virtual Server (sometimes referred to as Port Forwarding) is the act of forwarding traffic from one network node to another based on received protocol port number. This technique can allow an external user to reach a port on a private IP address (inside a LAN) from the outside through a NAT enabled router. (Maximum 32 entries are allowed.)



Virtual Server

Virtual Server: Enable

Virtual Server Settings

IP Address:
Private Port:
Public Port:
Protocol: TCP&UDP
Comment:
(The maximum rule count is 32.)

Current Virtual Servers in system

No.	IP Address	Port Mapping	Protocol	Comment

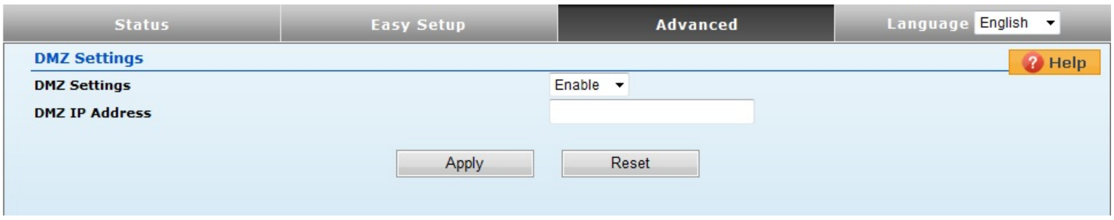
- ◆ **Virtual Server** — Selects between enabling or disabling port forwarding the virtual server. (Default: Disable)
- ◆ **IP Address** — Specifies the IP address of a server on the local network to allow external access.
- ◆ **Private Port** — The protocol port number on the local server.
- ◆ **Public Port** — The protocol port number on the router's WAN interface.
- ◆ **Protocol** — Specifies the protocol to forward, either TCP, UDP, or TCP&UDP.
- ◆ **Comment** — Enter a useful comment to help identify the port forwarding service on the network.
- ◆ **Current Virtual Servers in System** — The Current Port Forwarding Table displays the entries that are allowed to forward packets through the SHD69A's firewall.
    - **No.** — The table entry number.
    - **IP Address** — The IP address of a server on the local network to allow

external access.

- **Port Mapping** — displays the port mapping for the server.
- **Protocol** — Displays the protocol used for forwarding this port.
- **Comment** — Displays a useful comment to identify the nature of the port to be forwarded.

DMZ

DMZ is to specified host PC on the local network to access the Internet without any firewall protection. Some Internet applications, such as interactive games or video conferencing, may not function properly behind the firewall. By specifying a Demilitarized Zone (DMZ) host, the PC's TCP ports are completely exposed to the Internet, allowing open two-way communication. The host PC should be assigned a static IP address (which is mapped to its MAC address) and this must be configured as the DMZ IP address.



DMZ Settings

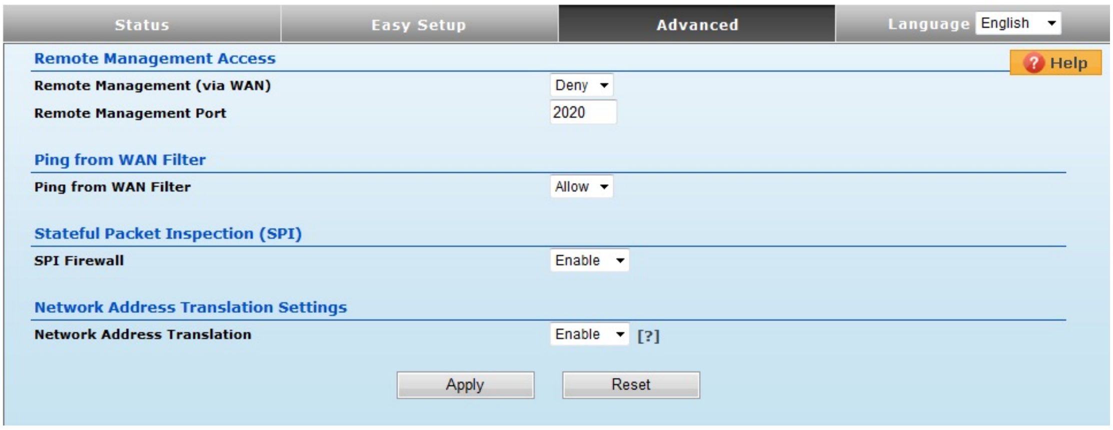
DMZ Settings: Enable

DMZ IP Address:

- **DMZ Settings** — Sets the DMZ status. (Default: Disable)
- **DMZ IP Address** — Specifies an IP address on the local network allowed unblocked access to the WAN.

FIREWALL

Firewall functions which will help to protect your network and computer. You can utilized firmware functions to protect your network from hackers and malicious intruders.



Remote Management Access

Remote Management (via WAN) Deny

Remote Management Port 2020

Ping from WAN Filter

Ping from WAN Filter Allow

Stateful Packet Inspection (SPI)

SPI Firewall Enable

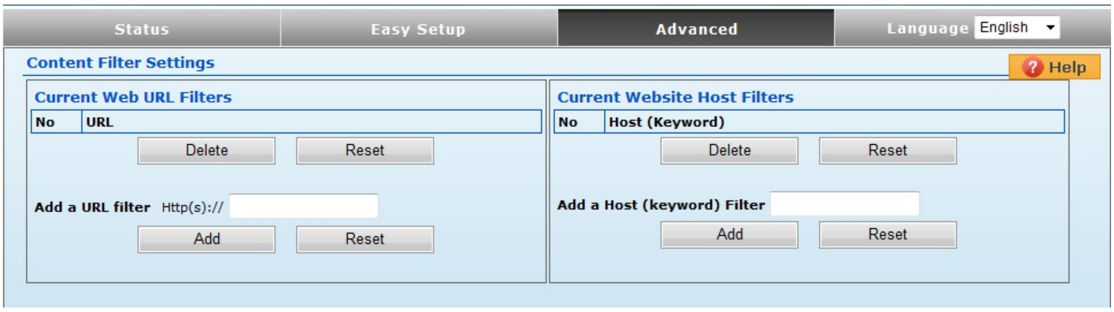
Network Address Translation Settings

Network Address Translation Enable [?]

- **Remote Management (via WAN)** — allow or deny to manage the router from anywhere on the Internet.
- **Remote Management Port** — The port that you will use to address the management from the Internet. For example, if you specify port 1080, then to access the SHD69A from Internet, you would use a URL of the form: http://xxx.xxx.xxx.xxx:1080/
- **Ping from WAN Filter** — When Allow, the SHD69A does not respond to ping packets received on the WAN port.
- **SPI Firewall** — SIP firewall help to keep track of the state of network connections (such as TCP streams, UDP communication) traveling across it. It is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known active connection will be allowed by the firewall; others will be rejected.
- **Network Address Translation** — NAT is the process of modifying IP address information in IP packet headers while in transit across a traffic routing device.

CONTENT FILTERING

The SHD69A provides a variety of options for blocking Internet access based on content, URL and host name.



- **Web URL Filter Settings** — By filtering inbound Uniform Resource Locators (URLs) the risk of compromising the network can be reduced. URLs are commonly used to point to websites. By specifying a URL or a keyword contained in a URL traffic from that site may be blocked.
- **Add a URL Filter** — Adds a URL filter to the settings.
- **Delete a URL Filter** — Deletes a URL filter entry from the list.

Web Host Filter Settings — Allows Internet content access to be restricted based on web address keywords and web domains. A domain name is the name of a particular web site. For example, for the address www.HOST.com, the domain name is HOST.com. Enter the Keyword then click “Add.”

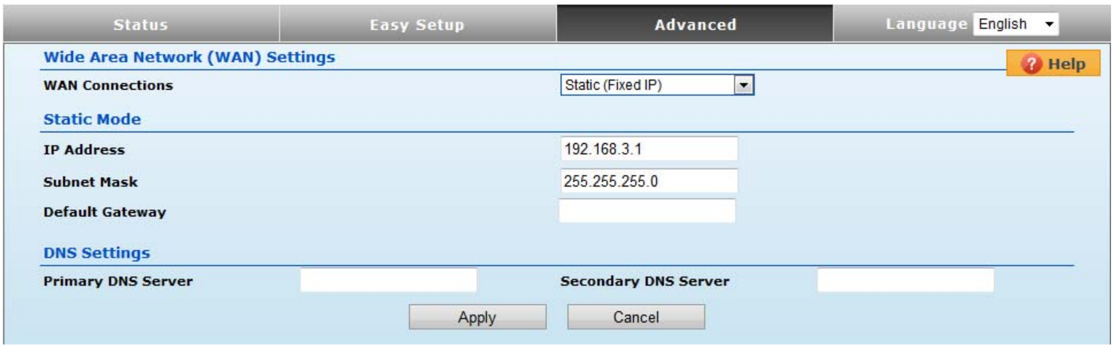
- **Current Host Filters** — Displays current Host filter.
- **Add a Host Filter** — Enters the keyword for a host filtering.
- **Delete a Host Filter** — Deletes a Host filter entry from the list.

NETWORK SETTINGS

WAN

In this section, there are several connection types to choose from; Static IP, DHCP, PPPoE, PPTP and L2TP. If you are unsure of your connection method, please contact your Internet Service Provider.

STATIC IP (FIXED IP)



Wide Area Network (WAN) Settings

WAN Connections: Static (Fixed IP)

Static Mode

IP Address: 192.168.3.1

Subnet Mask: 255.255.255.0

Default Gateway:

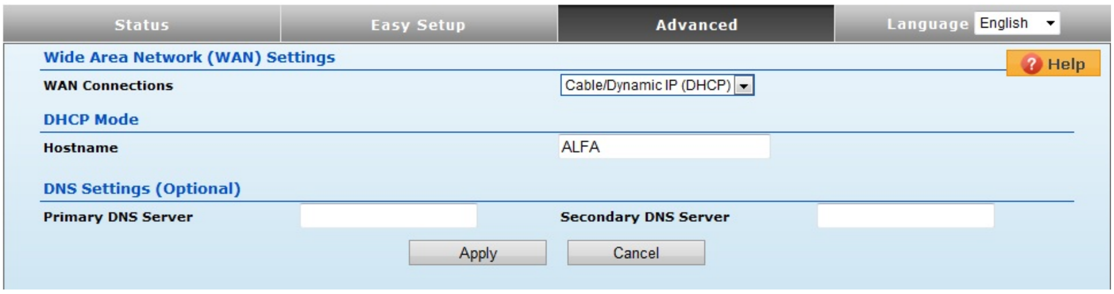
DNS Settings

Primary DNS Server:

Secondary DNS Server:

- **IP Address** — Sets the static IP address.
- **Subnet Mask** — Sets the static IP subnet mask. (Default: 255.255.255.0)
- **Default Gateway** — The IP address of a router that is used when the requested destination IP address is not on the local subnet.
- **Primary DNS Server** — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.
- **Secondary DNS Server** — The IP address of the Secondary Domain Name Server.

CABLE/DYNAMIC IP (DHCP)



Wide Area Network (WAN) Settings

WAN Connections: Cable/Dynamic IP (DHCP)

DHCP Mode

Hostname: ALFA

DNS Settings (Optional)

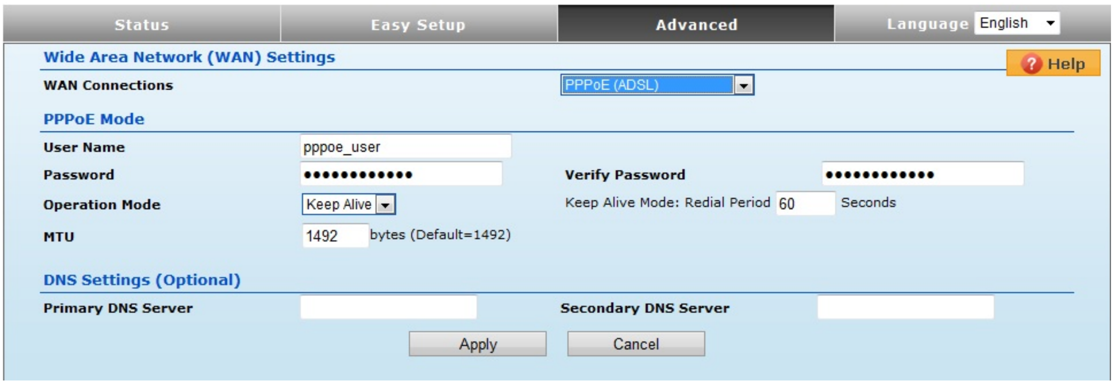
Primary DNS Server:

Secondary DNS Server:

- **Hostname** — Specifies the host name of the DHCP client.

- **Primary DNS Server** — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.
- **Secondary DNS Server** — The IP address of the Secondary Domain Name Server.

PPPoE (ADSL)



Wide Area Network (WAN) Settings

WAN Connections: PPPoE (ADSL)

PPPoE Mode

User Name: pppoe_user

Password: ●●●●●●●●●●●● Verify Password: ●●●●●●●●●●●●

Operation Mode: Keep Alive Keep Alive Mode: Redial Period 60 Seconds

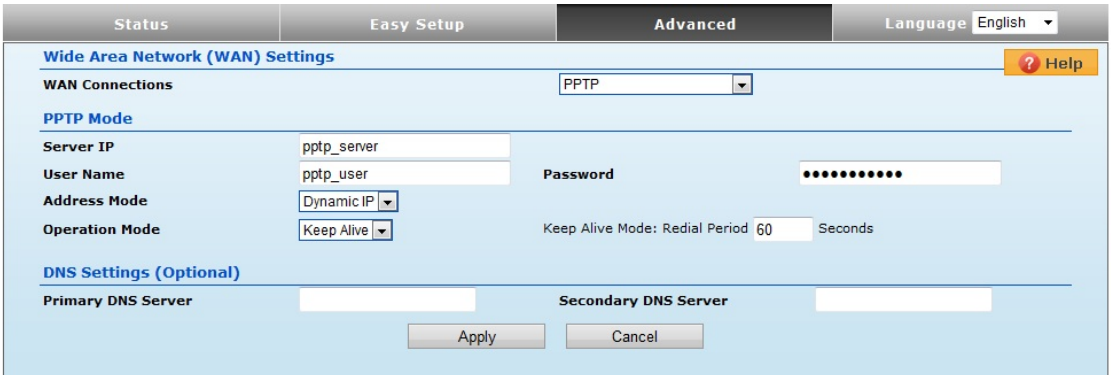
MTU: 1492 bytes (Default=1492)

DNS Settings (Optional)

Primary DNS Server: Secondary DNS Server:

- **User Name** — Sets the PPPoE user name for the WAN port. (Default: pppoe_user; Range: 1~32 characters)
- **Password** — Sets a PPPoE password for the WAN port. (Default: pppoe_password; Range: 1~32 characters)
- **Verify Password** — Prompts you to re-enter your chosen password.
- **Operation Mode —** Enables and configures the keep alive time and configures the on-demand idle time.

PPTP



Wide Area Network (WAN) Settings

WAN Connections: PPTP

PPTP Mode

Server IP: pptp_server

User Name: pptp_user Password: ●●●●●●●●●●●

Address Mode: Dynamic IP

Operation Mode: Keep Alive Keep Alive Mode: Redial Period 60 Seconds

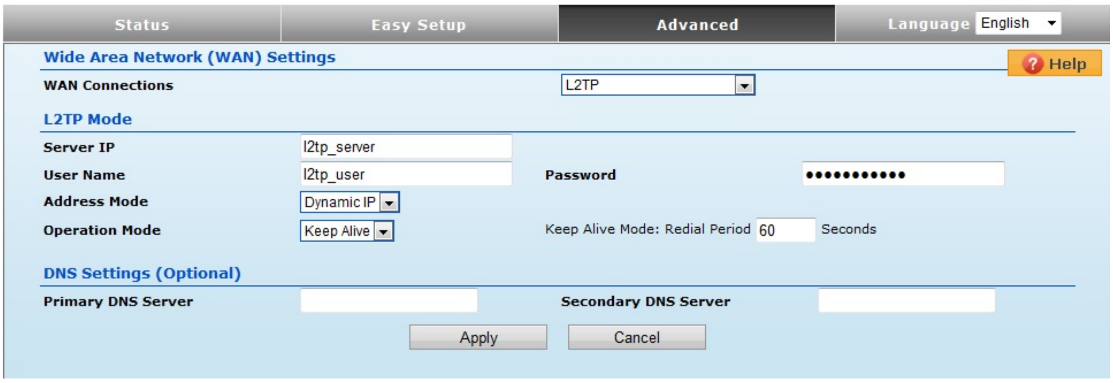
DNS Settings (Optional)

Primary DNS Server: Secondary DNS Server:

- **Server IP** — Sets the PPTP server IP Address. (Default: pptp_server)
- **User Name** — Sets the PPTP user name for the WAN port. (Default: pptp_user; Range: 1~32 characters)
- **Password** — Sets a PPTP password for the WAN port. (Default: pptp_password; Range: 1~32 characters)

- **Address Mode** — Sets a PPTP network mode. (Default: Dynamic IP)
- **Operation Mode —** Enables and configures the keep alive time.
- **Primary DNS Server** — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.
- **Secondary DNS Server** — The IP address of the Secondary Domain Name Server.

L2TP



Wide Area Network (WAN) Settings

WAN Connections	L2TP		

L2TP Mode

Server IP	l2tp_server		
User Name	l2tp_user	Password	●●●●●●●●●●●
Address Mode	Dynamic IP		
Operation Mode	Keep Alive	Keep Alive Mode: Redial Period	60 Seconds

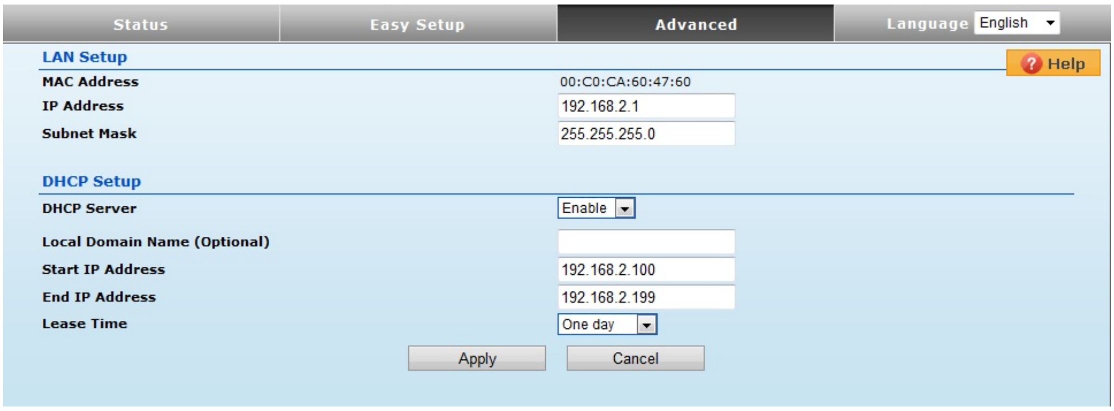
DNS Settings (Optional)

Primary DNS Server		Secondary DNS Server	

- **Server IP** — Sets the L2TP server IP Address. (Default: l2tp_server)
- **User Name** — Sets the L2TP user name for the WAN port. (Default: l2tp_user; Range: 1~32 characters)
- **Password** — Sets a L2TP password for the WAN port. (Default: l2tp_password; Range: 1~32 characters)
- **Address Mode** — Sets a L2TP network mode. (Default: Dynamic IP)
- **Operation Mode —** Enables and configures the keep alive time.
- **Primary DNS Server** — The IP address of the Primary Domain Name Server. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses. To specify a DNS server, type the IP addresses in the text field provided. Otherwise, leave the text field blank.
- **Secondary DNS Server** — The IP address of the Secondary Domain Name Server.

LAN

In this section, the LAN settings are configured based on the IP Address and Subnet Mask. The IP address is also used to access this Web-based management interface. It is recommended to use the default settings if you do not have an existing network.



LAN Setup

MAC Address	00:C0:CA:60:47:60
IP Address	192.168.2.1
Subnet Mask	255.255.255.0

DHCP Setup

DHCP Server	Enable
Local Domain Name (Optional)	
Start IP Address	192.168.2.100
End IP Address	192.168.2.199
Lease Time	One day

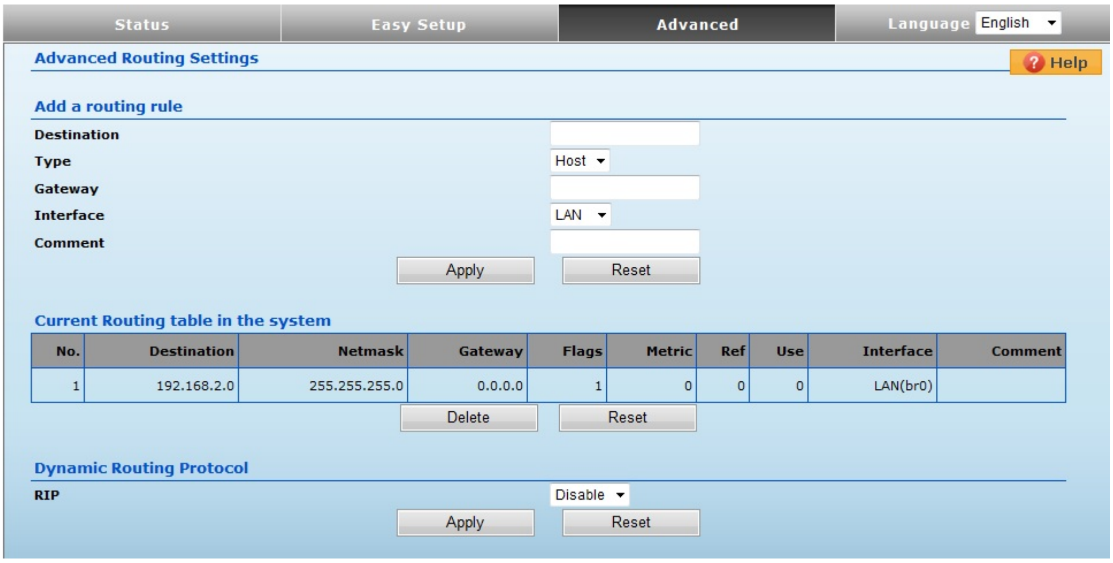
- **IP Address** — The IP address of SHD69A on the local area network.

(Default: 192.168.2.1)

- **Subnet Mask** — The subnet mask of SHD69A on the local area network
- **DHCP Server** — The DHCP Server is to assign private IP address to the SHD69A in your SHD local area network(LAN). The default LAN IP address is 192.168.2.1, changing IP address will also change the DHCP server's IP subnet.

Advanced Routing

In this section, allow to configure routing feature in the SHD69A.



Advanced Routing Settings

Add a routing rule

Destination	
Type	Host
Gateway	
Interface	LAN
Comment	

Current Routing table in the system

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	192.168.2.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN(br0)	

Dynamic Routing Protocol

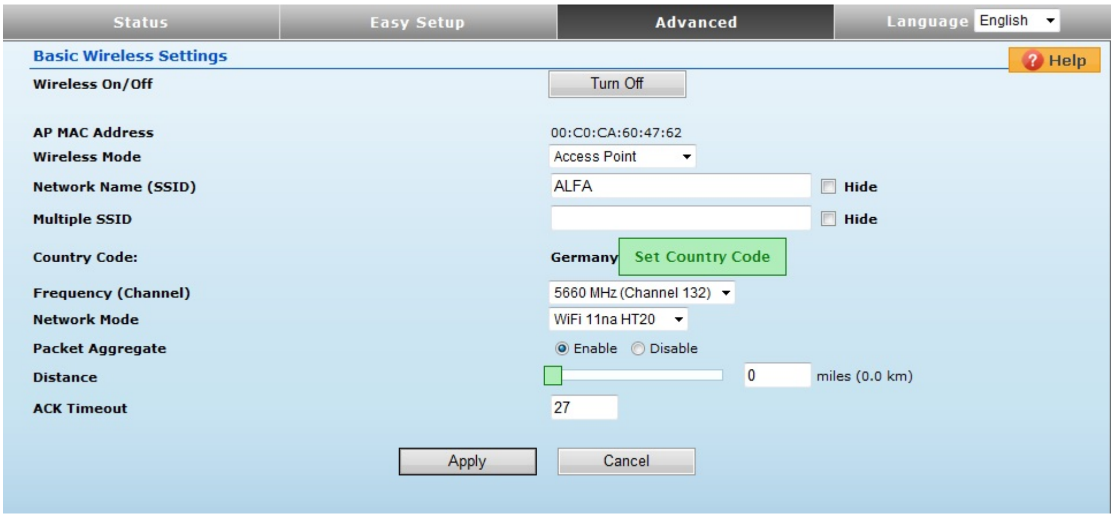
RIP	Disable

- **Destination** — The IP address of packets that can be routed.
- **Type** — Defines the type of destination. (Host: Signal IP address / Net: Portion of Network)
- **Netmask** — Displays the subnetwork associated with the destination.

- **Gateway** — Defines the packets destination next hop
- **Interface** — Select interface to which a static routing subnet is to be applied
- **Comment** — Help identify the routing
- **RIP** — Enable or disable the RIP(Routing Information Protocol) for the WAN or LAN interface.

WIRELESS SETTINGS

BASIC



Basic Wireless Settings

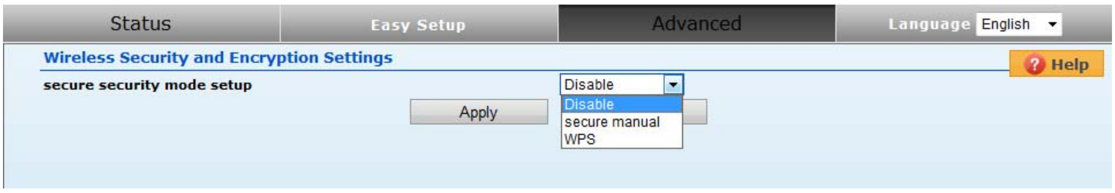
Wireless On/Off	Turn Off
AP MAC Address	00:C0:CA:60:47:62
Wireless Mode	Access Point
Network Name (SSID)	ALFA □ Hide
Multiple SSID	□ Hide
Country Code:	Germany Set Country Code
Frequency (Channel)	5660 MHz (Channel 132)
Network Mode	WiFi 11na HT20
Packet Aggregate	● Enable ○ Disable
Distance	0 miles (0.0 km)
ACK Timeout	27

- **Wireless On/Off** — Enables or Disable the radio. (Default: Turn On)
- **Wireless Mode** — There are 4 wireless mode, those are Access Point, WDS Access Point, WDS Repeater and WDS Client
- **Network Name (SSID)** — The name of the wireless network service provided by the SHD69A. Clients that want to connect to the network must set their SSID to the same as that of SHD69A. (Range: 1-32 characters)
- **Multiple SSID** — One additional VAP interface supported on the device. (Default: no name configured; Range: 1-32 characters)
- **Country Code** — Select the country on your location, after selected the country will automatically to change the channel frequency
- **Frequency (Channel)** — The radio channel that the SHD69A uses to communicate with wireless clients.
- **Network Mode** — Defines the radio operating mode.(Default: 11an HT20)
- **Packet Aggregate** — The process of joining multiple packets together into a single

transmission unit, in order to reduce the overhead associated with each transmission.

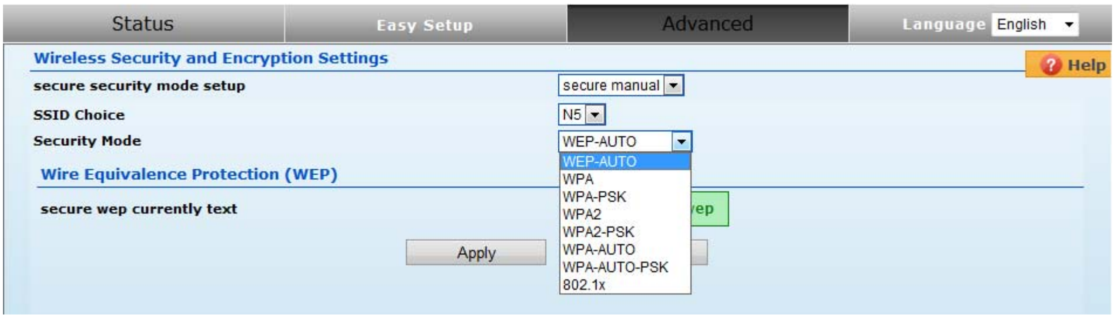
- **Distance** — Change the distance to fit into your network, when change the distance will automatically to change the ACK timeout.
- **ACK timeout** — The ACK timeout is shorter than the time it takes for the end of the last data packet to propagate to the receiver + the start of the ACK for that packet to propagate back to the sender, then the sending MAC will assume that the packet has been lost and will unnecessarily retransmit the data packet

SECURITY



Wireless Security and Encryption Settings

secure security mode setup: Disable



Wireless Security and Encryption Settings

secure security mode setup: secure manual

SSID Choice: N5

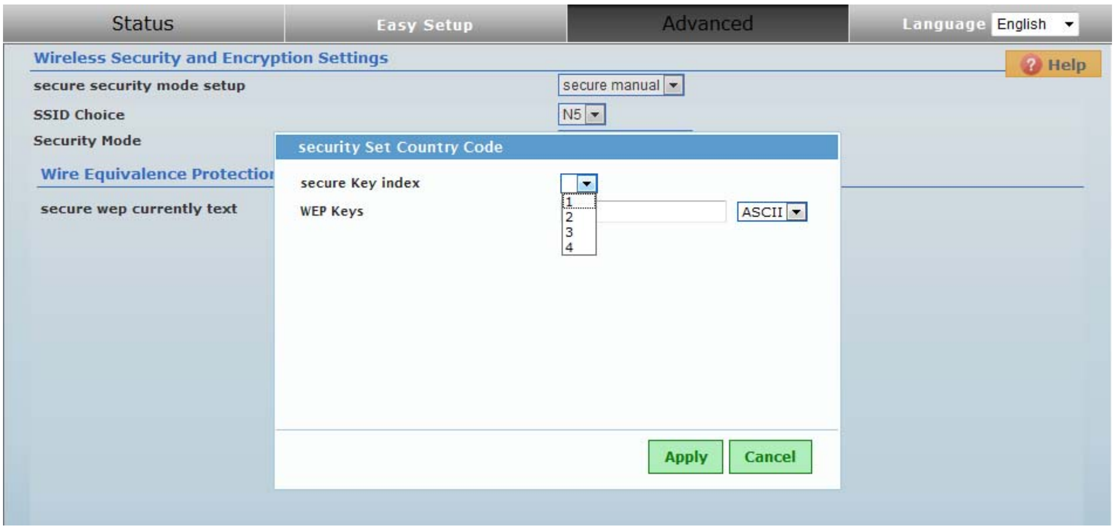
Security Mode: WEP-AUTO

Wire Equivalence Protection (WEP)

secure wep currently text

WIRED EQUIVALENT PRIVACY (WEP)

WEP provides a basic level of security, preventing unauthorized access to the network, and encrypting data transmitted between wireless clients and an access point. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network. When you select to use WEP, be sure to define at least one static WEP key for user authentication or data encryption. Also, be sure that the WEP shared keys are the same for each client in the wireless network.



Wireless Security and Encryption Settings

secure security mode setup: secure manual

SSID Choice: N5

Security Mode

Wire Equivalence Protectio

secure wep currently text

security Set Country Code

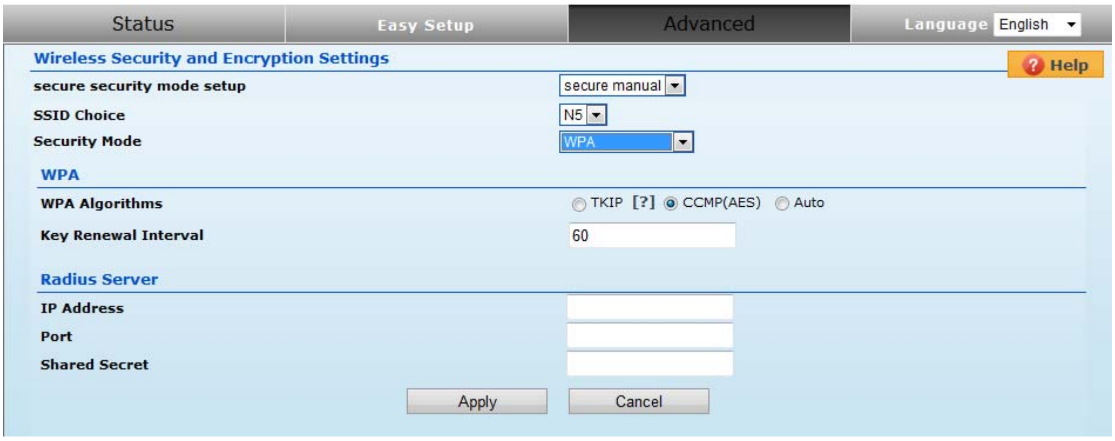
secure Key index: 1, 2, 3, 4

WEP Keys: ASCII

- **Encrypt Type** — Selects WEP for data encryption (OPEN mode only).
- **Security Key Index**— Selects the WEP key number to use for authentication or data encryption. If wireless clients have all four WEP keys configured to the same values, you can change the encryption key to any of the settings without having to update the client keys. (Default: 1; Range: 1~4)
- **WEP Keys** — Sets WEP key values. The user must first select ASCII or hexadecimal keys. Each WEP key has an index number. Enter key values that match the key type and length settings. Enter 5 alphanumeric characters or 10 hexadecimal digits for 64-bit keys, or enter 13 alphanumeric characters or 26 hexadecimal digits for 128-bit keys. (Default: Hex, no preset value)

WPA & WPA2

Wi-Fi Protected Access (WPA) was introduced as an interim solution for the vulnerability of WEP pending the adoption of a more robust wireless security standard. WPA2 includes the complete wireless security standard, but also offers backward compatibility with WPA.



Wireless Security and Encryption Settings

secure security mode setup: secure manual

SSID Choice: N5

Security Mode: WPA

WPA

WPA Algorithms: ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval: 60

Radius Server

IP Address

Port

Shared Secret

- **WPA** — Clients using WPA for authentication.
- **WPA2** — Clients using WPA2 for authentication.

◆ **WPA-Auto** — Clients using WPA or WPA2 for authentication.

◆ **WPA Algorithms** — Selects the data encryption type to use. (Default is determined by the Security Mode selected.)

▪ **TKIP** — Uses Temporal Key Integrity Protocol (TKIP) keys for encryption. WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.

▪ **AES** — Uses Advanced Encryption Standard (AES) keys for encryption. WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) for message integrity. The AES Counter-Mode/CBCMAC Protocol (AESCCMP) provides extremely robust data confidentiality using a 128- bit key. Use of AES-CCMP encryption is specified as a standard requirement for WPA2. Before implementing WPA2 in the network, be sure client devices are upgraded to WPA2-compliant hardware.

▪ **Auto** — Uses either TKIP or AES keys for encryption. WPA and WPA2 mixed modes allow both WPA and WPA2 clients to associate to a common SSID. In mixed mode, the unicast encryption type (TKIP or AES) is negotiated for each client.

◆ **Key Renewal Interval** — Sets the time period for automatically changing data encryption keys and redistributing them to all connected clients. (Default: 3600 seconds)

RADIUS Server — Configures RADIUS server settings.

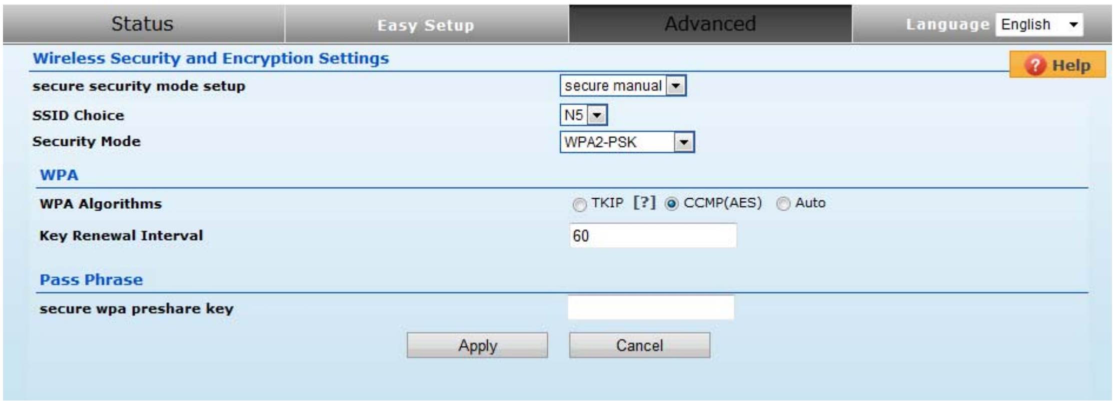
◆ **IP Address** — Specifies the IP address of the RADIUS server.

◆ **Port** — The User Datagram Protocol (UDP) port number used by the RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)

◆ **Shared Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Maximum length: 20 characters)

WPA-PSK & WPA2-PSK

Wi-Fi Protected Access (WPA) was introduced as an interim solution for the vulnerability of WEP pending the adoption of a more robust wireless security standard. WPA2 includes the complete wireless security standard, but also offers backward compatibility with WPA. Both WPA and WPA2 provide an “enterprise” and “personal” mode of operation. For small home or office networks, WPA and WPA2 provide a simple “personal” operating mode that uses just a pre-shared key for network access. The **WPA Pre-Shared Key (WPA-PSK)** mode uses a common password phrase for user authentication that is manually entered on the access point and all wireless clients. Data encryption keys are automatically generated by the access point and distributed to all clients connected to the network.



Wireless Security and Encryption Settings

secure security mode setup: secure manual

SSID Choice: N5

Security Mode: WPA2-PSK

WPA

WPA Algorithms: ○ TKIP [?] ● CCMP(AES) ○ Auto

Key Renewal Interval: 60

Pass Phrase

secure wpa preshare key:

◆ **WPA-PSK** — Clients using WPA with a Pre-shared Key are accepted for authentication. The default data encryption type for WPA is TKIP.

◆ **WPA2-PSK** — Clients using WPA2 with a Pre-shared Key are accepted for authentication. The default data encryption type for WPA is AES.

◆ **WPA- Auto-PSK** — Clients using WPA or WPA2 with a Preshared Key are accepted for authentication. The default data encryption type is TKIP/AES.

◆ **WPA Algorithms** — Selects the data encryption type to use. (Default is determined by the Security Mode selected.)

▪ **TKIP** — Uses Temporal Key Integrity Protocol (TKIP) keys for encryption. WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.

▪ **AES** — Uses Advanced Encryption Standard (AES) keys for encryption. WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) for message integrity. The AES Counter-Mode/CBCMAC Protocol (AESCCMP) provides extremely robust data confidentiality using a 128- bit key. Use of AES-CCMP encryption is specified as a standard requirement for WPA2. Before implementing WPA2 in the network, be sure client devices are upgraded to WPA2-compliant hardware.

▪ **Auto** — Uses either TKIP or AES keys for encryption. WPA and WPA2 mixed modes allow both WPA and WPA2 clients to associate to a common SSID. In mixed mode, the unicast encryption type (TKIP or AES) is negotiated for each client.

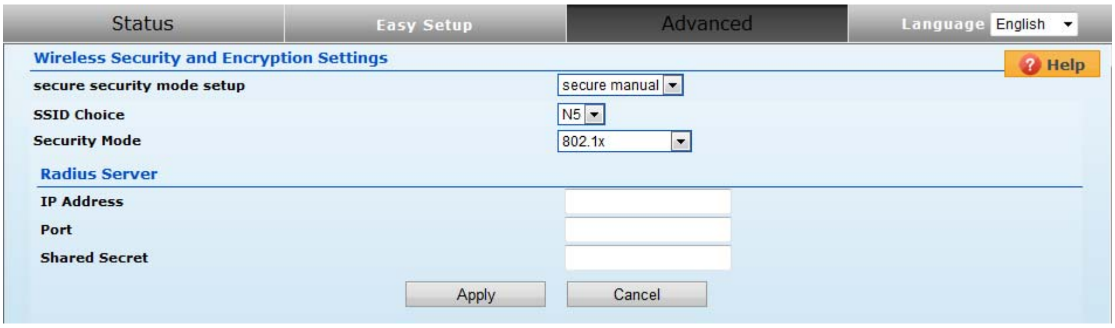
◆ **Pass Phrase** — The WPA Preshared Key can be input as an ASCII string (an easy-to-remember form of letters and numbers that can include spaces) or Hexadecimal format. (Range: 8~63 ASCII characters, or exactly 64 Hexadecimal digits)

- **Key Renewal Interval** — Sets the time period for automatically changing data encryption keys and redistributing them to all connected clients. (Default: 3600 seconds)

IEEE 802.1X AND RADIUS

IEEE 802.1X is a standard framework for network access control that uses a central RADIUS server for user authentication. This control feature prevents unauthorized access to the network by requiring an 802.1X client application to submit user credentials for authentication. The 802.1X standard uses the Extensible Authentication Protocol (EAP) to pass user credentials (either digital certificates, user names and passwords, or other) from the client to the RADIUS server. Client authentication is then verified on the RADIUS server before the client can access the network. Remote Authentication Dial-in User Service (RADIUS) is an authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of user credentials for each user that requires network access.

The WPA and WPA2 enterprise security modes use 802.1X as the method of user authentication. IEEE 802.1X can also be enabled on its own as a security mode for user authentication. When 802.1X is used, a RADIUS server must be configured and be available on the connected wired network.



Wireless Security and Encryption Settings

secure security mode setup: secure manual

SSID Choice: N5

Security Mode: 802.1x

Radius Server

IP Address

Port

Shared Secret

802.1X: Selects WEP keys for data encryption. When enabled, WEP encryption keys are automatically generated by the RADIUS server and distributed to all connected clients. (Default: Disabled)

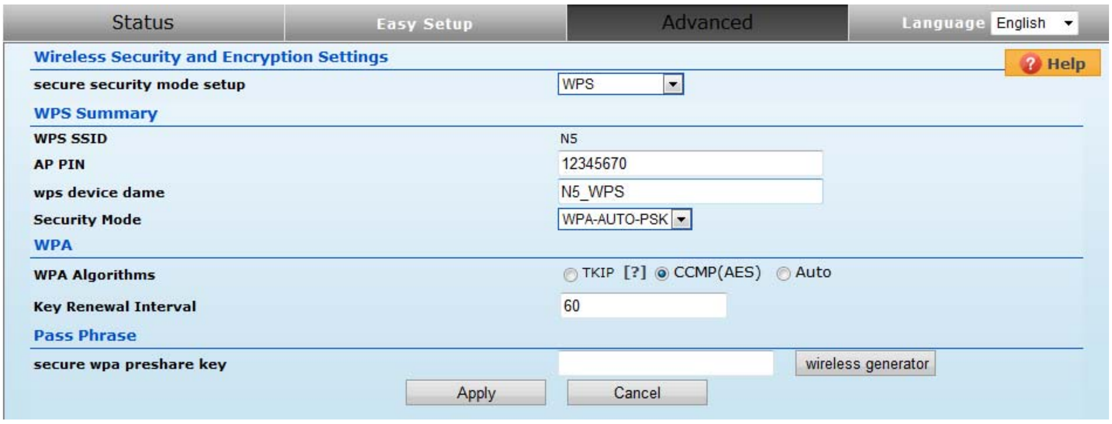
RADIUS Server — Configures RADIUS server settings.

- **IP Address** — Specifies the IP address of the RADIUS server.
- **Port** — The User Datagram Protocol (UDP) port number used by the RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)
- **Shared Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Maximum length: 20

characters)

WI-FI PROTECTED SETUP (WPS)

Wi-Fi Protected Setup (WPS) is designed to ease installation and activation of security features in wireless networks. WPS has two basic modes of operation, Push-button Configuration (PBC) and Personal Identification Number (PIN). The WPS PIN setup is optional to the PBC setup and provides more security. The WPS button on the 3G Mobile Wireless Router can be pressed at any time to allow a single device to easily join the network. The WPS Settings page includes configuration options for setting WPS device PIN codes and activating the virtual WPS button. Click on "Wireless Settings," followed by "WPS".



Wireless Security and Encryption Settings

secure security mode setup	WPS

WPS Summary

WPS SSID	N5
AP PIN	12345670
wps device dame	N5_WPS
Security Mode	WPA-AUTO-PSK

WPA

WPA Algorithms	○ TKIP [?] ● CCMP(AES) ○ Auto
Key Renewal Interval	60

Pass Phrase

secure wpa preshare key	

WPS Summary — Provides detailed WPS statistical information.

- **WPS SSID** — The service set identifier for the unit.
- **AP PIN** — Displays the PIN Code for the 3G Mobile Wireless Router. The default is exclusive for each unit. (Default: 64824901)
- **WPS Name** — WPS name for connecting to the device.
- **Security Mode** — Selects between methods of broadcasting the WPS beacon to network clients wanting to join the network:

WPA Algorithms — Selects the data encryption type to use. (Default is determined by the Security Mode selected.)

- **TKIP** — Uses Temporal Key Integrity Protocol (TKIP) keys for encryption. WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys.
- **AES** — Uses Advanced Encryption Standard (AES) keys for encryption. WPA2 uses AES Counter-Mode encryption with Cipher Block Chaining Message Authentication Code (CBC-MAC) for message integrity. The AES Counter-Mode/CBCMAC Protocol (AESCCMP) provides extremely robust data confidentiality using a 128- bit key. Use of AES-CCMP encryption is specified as a standard requirement for WPA2. Before implementing WPA2 in the network, be sure client devices are upgraded to

WPA2-compliant hardware.

◆ **TKIP/AES** — Uses either TKIP or AES keys for encryption. WPA and WPA2 mixed modes allow both WPA and WPA2 clients to associate to a common SSID. In mixed mode, the unicast encryption type (TKIP or AES) is negotiated for each client.

◆ **Key Renewal Interval** — Sets the time period for automatically changing data encryption keys and redistributing them to all connected clients. (Default: 3600 seconds)

◆ **Pass Phrase** — The WPA Preshared Key can be input as an ASCII string (an easy-to-remember form of letters and numbers that can include spaces) or Hexadecimal format. (Range: 8~63 ASCII characters, or exactly 64 Hexadecimal digits)

Warning:

This Product is only used in industry and SHD69A for indoor used

FCC Warning:

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Any Changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment .This equipment should be installed and operated with minimum distance 20cm between the radiator& your body.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.