Security Configuration using AT Command at WizFi630

Version 1.00

Document Revision History

Date	Revision	Changes
2013-03-21	V1.00	Official Release

WIZnet's Online Technical Support

If you have something to ask about WIZnet products, write down your question on Q&A Board in WIZnet website (www.wiznet.co.kr). WIZnet will give an answer as soon as possible.

COPYRIGHT NOTICE

Technical Support: support@wiznet.co.kr
Sales & Distribution: sales@wiznet.co.kr
For more information, visit our website at http://www.wiznet.co.kr

Table of Contents

1. Summary

Generally, security configuration is done by using web page. But depending on development environment, only AT Commands are allowed to configure. In that case, this document will be needed. Note that there are two configurations of 'DU'/'GU' and 'AU'/'PU' at AP-Client mode. 'DU'/'GU' is the security configuration of AP side, and how to configure is same with other 'DU'/'GU'. But 'AU'/'PU' is the security configuration of Client side which will be connected to Router, so is a bit different with 'DU'/'GU'.

2. 'DU' / 'GU' Command - AP, Gateway, AP-Client Mode

A. Format

1. 'GU' Input Format

Authentication Method	Format
None	<GU(1)_(2)>
WEP / PSK	<GU(1)_(2)_(3)_(4)_(5)_(6)>
Radius / 802.1x	<GU(1)_(2)_(3)_(4)_(5)_(6)_(7)_(8)_(9)>

2. 'DU' Response Format

Authentication Method	Format
None	<S(1)_(2)>
WEP / PSK	<S(1)_(2)_(3)_(4)_(5)_(6)>
Radius / 802.1x	<S(1)_(2)_(3)_(4)_(5)_(6)_(7)_(8)_(9)>

3. Format Details

■ (1) Authentication Mode:

1	Open	2	802.1x	3	Shared
4	WPA-Radius	5	WPA-PSK	6	WPA2-Radius
7	WPA2-PSK	8	WEPAUTO	9	WPA1/2-Radius
a	WPA1/2-PSK				

■ (2) Encryption Mode:

0	None	1	WEP	2	TKIP
3	AES	4	TKIP_AES		

■ (3) Default Key Index:

Range	1 ~ 4

■ (4) Key Length mode:

0	None	1	WEP64	2	WEP128

■ (5) Key/Passphrase Format:

0	ASCII	1	HEX		

- (6) Default-Key/Passphrase Value
- (7) Radius Password
- (8) Radius IP
- (9) Radius Port

* (3) ~ (4): Available only at WEP mode,
* (7) ~ (9): Available only at Radius(Enterprise) mode.

B. 'DU' Response Details

1. Response of each mode

Auth	Encr	Response
Open	None	<S1_0>
Open	WEP	<S1_1_(DefKeyIdx)_(KeyLenMod)_(ASCII/HEX)_(DefKeyVal)>
Shared	WEP	<S3_1_(DefKeyIdx)_(KeyLenMod)_(ASCII/HEX)_(DefKeyVal)>
WEPAUTO	-	<S8_1_(DefKeyIdx)_(KeyLenMod)_(ASCII/HEX)_(DefKeyVal)>
802.1x	None	<S2_0_(x)_(x)_(x)_(x)_(Password)_(RadiusIP)_(RadiusPort)>
802.1x	WEP	<S2_1_(x)_(x)_(x)_(x)_(Password)_(RadiusIP)_(RadiusPort)>
WPA-PSK	TKIP	<S5_2_(x)_(x)_(x)_(Passphrase)>
WPA-PSK	AES	<S5_3_(x)_(x)_(x)_(Passphrase)>
WPA2-PSK	TKIP	<S7_2_(x)_(x)_(x)_(Passphrase)>
WPA2-PSK	AES	<S7_3_(x)_(x)_(x)_(Passphrase)>
WPA1/2-PSK	TKIP	<Sa_2_(x)_(x)_(x)_(Passphrase)>
WPA1/2-PSK	AES	<Sa_3_(x)_(x)_(x)_(Passphrase)>
WPA-Radius	TKIP	<S4_2_(x)_(x)_(x)_(x)_(Password)_(RadiusIP)_(RadiusPort)>
WPA-Radius	AES	<S4_3_(x)_(x)_(x)_(x)_(Password)_(RadiusIP)_(RadiusPort)>
WPA2-Radius	TKIP	<S6_2_(x)_(x)_(x)_(x)_(Password)_(RadiusIP)_(RadiusPort)>
WPA2-Radius	AES	<S6_3_(x)_(x)_(x)_(x)_(Password)_(RadiusIP)_(RadiusPort)>
WPA1/2-Radius	TKIP	<S9_2_(x)_(x)_(x)_(x)_(Password)_(RadiusIP)_(RadiusPort)>
WPA1/2-Radius	AES	<S9_3_(x)_(x)_(x)_(x)_(Password)_(RadiusIP)_(RadiusPort)>

* (x): Don't Care
* Notice:
  - [Open] + [None] is the 'Disabled' mode in the web page.
  - [Open] + [WEP] is the 'OPENWEP' mode in the web page.
    64/128 Key length is determined by the key user input.
  - 'WEPAUTO' means [Open/Shared]

C. 'GU' Input Details

1. Input of each mode

Just change 'S' to 'GU' at the 'DU' Response Details

2. Examples of each mode input

Auth	Encr	Response
Open	None	<GU1_0>
Open	WEP	<GU1_1_1_1_0_12345> :ASCII <GU1_1_1_1_1_3132333435> :HEX <GU1_1_1_2_0_1234567890123> :ASCII <GU1_1_1_2_1_31323334353637383930313233> :HEX
Shared	WEP	Only GU1 -> GU3 is changed from [Open]+[WEP]
WEPAUTO	-	Only GU1 -> GU8 is changed from [Open]+[WEP]
802.1x	None	<GU2_0_0_0_0_0_12345_101.102.103.104_1812>
802.1x	WEP	<GU2_1_0_0_0_0_12345_101.102.103.104_1812>
WPA-PSK	TKIP	<GU5_2_0_0_0_12345678>
WPA-PSK	AES	<GU5_3_0_0_0_12345678>
WPA2-PSK	TKIP	<GU7_2_0_0_0_12345678>
WPA2-PSK	AES	<GU7_3_0_0_0_12345678>
WPA1/2-PSK	TKIP	<GUa_2_0_0_0_12345678>
WPA1/2-PSK	AES	<GUa_3_0_0_0_12345678>
WPA-Radius	TKIP	<GU4_2_0_0_0_0_12345_101.102.103.104_1812>
WPA-Radius	AES	<GU4_3_0_0_0_0_12345_101.102.103.104_1812>
WPA2-Radius	TKIP	<GU6_2_0_0_0_0_12345_101.102.103.104_1812>
WPA2-Radius	AES	<GU6_3_0_0_0_0_12345_101.102.103.104_1812>
WPA1/2-Radius	TKIP	<GU9_2_0_0_0_0_12345_101.102.103.104_1812>
WPA1/2-Radius	AES	<GU9_3_0_0_0_0_12345_101.102.103.104_1812>

* Reference:: 1812 is the Port number of Official Radius Protocol which is registered by IANA.

3. 'AU' / 'PU' Command - AP-Client Mode

A. Format

1. 'PU' Input Format

Authentication Method	Format
None	<PU(1)_(2)_(3)>
WEP / PSK	<PU(1)_(2)_(3)_(4)_(5)>

2. 'AU' Response Format

Authentication Method	Format
None	<S(1)_(2)_(3)>
WEP / PSK	<S(1)_(2)_(3)_(4)_(5)>

3. Format Details

■ (1) Authentication Mode:

1	Open	3	Shared	5	WPA-PSK	7	WPA2-PSK

■ (2) Encryption Mode:

0	None	1	WEP	2	TKIP	3	AES

■ (3) WiFi Channel

■ (4) Default Key Index:

Range	1 ~ 4

■ (4) Default-Key/Passphrase Value:

WEP	5(10), 13(26) characters
WPA-PSK	8-63 characters

* (4): Available only at WEP mode,

B. 'AU' Response Details

1. Response of each mode

Auth	Encr	Response
Open	None	<S1_0_(Channel)>
Open	WEP	<S1_1_(Channel)_(DefKeyIdx)_(DefKeyVal)>
Shared	None	<S1_0_(Channel)> : same with [Open]+[None]
Shared	WEP	<S3_1_(Channel)_(DefKeyIdx)_(DefKeyVal)>
WPA-PSK	TKIP	<S5_2_(Channel)_(x)_(Passphrase)>
WPA-PSK	AES	<S5_3_(Channel)_(x)_(Passphrase)>
WPA2-PSK	TKIP	<S7_2_(Channel)_(x)_(Passphrase)>
WPA2-PSK	AES	<S7_3_(Channel)_(x)_(Passphrase)>

* (x): Don't Care

* There is not a variable with which we can know the key is ASCII or HEX in the format, but HEX value displayed as HEX digit.

C. 'PU' Input Details

1. Input of each mode

Just change 'S' to 'PU' at the 'AU' Response Details

2. Examples of each mode input

Auth	Encr	Response
Open	None	<PU1_0_11>
Open	WEP	<PU1_1_11_1_12345> : WEP64 <PU1_1_11_1_1234567890123> : WEP128
Shared	None	Not Available
Shared	WEP	<PU3_1_11_1_12345> : WEP64 <PU3_1_11_1_1234567890123> : WEP128
WPA-PSK	TKIP	<PU5_2_11_0_12345678>
WPA-PSK	AES	<PU5_3_11_0_12345678>
WPA2-PSK	TKIP	<PU7_2_11_0_12345678>
WPA2-PSK	AES	<PU7_3_11_0_12345678>

* There is not a way to input key as HEX digit.