



QUICK GUIDE

Guida configurazione dell'Access Point Mod.SEAPIN152

Con la seguente guida si vuole evidenziare i requisiti minini di configurazione dell'Access Point SEAPIN152



1- Configurazione scheda PC

Il dispositivo SEAPIN152, ha come IP default: 192.168.0.1 SUBNET MASK: 255.255.255.0. Per accedere alla Web Page di setup è necessario pertanto inserire nella scheda di rete del proprio PC un IP della stessa famiglia ad esempio: 192.168.0.100 (Fig.1) e collegare il PC alla porta **ETH0**.

le	Condivisione		ategor
P	roprietà - Protocollo Internet ve	rsione 4 (TCP/IPv4)	8
	Generale		
	È possibile ottenere l'assegnazior rete supporta tale caratteristica. richiedere all'amministratore di re Ottieni automaticamente un	e automatica delle imposta: In caso contrario, sarà nec te le impostazioni IP corrett indirizzo IP	zioni IP se la essario e.
	Otilizza il seguente indirizzo	IP:	
	Indirizzo IP:	192.168.0.1	100
	Subnet mask:	þ55 . 255 . 255 .	0
	Gateway predefinito:		
	 Ottieni indirizzo server DNS Ottilizza i seguenti indirizzi se 	automaticamente	
	Server DNS preferito:	a a (4)	
	Server DNS alternativo:	(i) i) ii)	1
1.100		A	vanzate

Fig.1 Inserimento IP scheda rete PC



Supporto tecnico:



1



2- Accesso alla WebPage di SETUP

Per accedere alla pagina di setup aprire il proprio Browser e digitare l'indirizzo IP: 192.168.0.1, l'accesso è protetto da una finestra di login con nome utente "admin" e password "admin" (Fig.2)

Sat.	Modifica	Visualizza	Preferiti	Strumenti	?		
					User authenticat	ion required. Login p	lease.
					Username:	admin	
					Password:	••••	Ŷ
					Language:	English 💙	
					Please enter your	login username and pas	sword.
						Log	in
							97.75

Fig.2 Finestra di Login

3- Accesso alla WebPage di SETUP

La Fig.3 mostra la WebPage di Diagnostica e di configurazione

	×	Kouter-index	zza Preferiti Strumenti ?
Save • Reboot • Logout • English Logged in as: adm		System	Robustel Status
		LEDs Information	System
		RUN: GREEN/BLINK	Network
		WIFI: OFF	Route
		USR: OFF	VPN
			Services
		Router Information	Event/Log
	R3000-NU	Device Model:	Configuration
	00302114030008	Serial Number:	configuration
	Cellular Router	Device Name:	Link Management
	1.01.01	Firmware Version:	Ethernet
	1.02.01	Hardware Version:	WiFi
	2.6.39-7	Kernel Version:	Serial
	0 day 00:12:07	Uptime:	DI/DO
	00.90%	CPU Load:	USB
	123.03MB/73.91MB(60.07%)	RAM Total/Free:	NAT/DMZ
	1970-01-01 08:12:07	System Time:	Firewall
		Current WAN Link	QoS
	Ethernot	Current WAN Link:	IP Routing
	102 168 0 1	ID Addrose:	DynDNS
	102 168 0 1	Gateway:	IPsec
		Gateway.	OpenVPN
Manual Refresh V Refresh			COL

Fg.3 Web page Setup





a Visualizza	Preferiti Strumenti ?	
	Robuste	• Save • Repoor • Logout • English
		Logged in as: admin
	Status	Basic MAC Filter Status
	System	WiFi Basic Settings
	Network	² Enable WiFi
	Route	Mode: AP
	VPN	Channel: Auto V
	Services	SSID: 3 Router AP
	Event/Log	Hide SSID:
	Configuration	Security Mode: Open 🗸
	Link Management	WiFi Network Settings
	Ethernet	*WIFI interface bridged with eth1, network settings please refer to this page.
	1 WiFi	
	Serial	
	DI/DO	
	USB	
	NAT/DMZ	
	Firewall	
	QoS	
	IP Routing	
	DynDNS	
	IPsec	
	OpenVPN	
	GRE	Apply Cancel

4- Configurazione AP - Abilitazione modulo Radio e assegnazione nome Rete SSID

Fig.4 Setup Configuration -Sezione" WiFi"

Per accedere alla configurazione dei parametri di Setup dell'Acess Point, andiamo nella sezione *Configuration* (Fig.4) e selezioniamo la voce WiFi(1), mettiamo il segno di spunta su *Enable WiFi* (2) e, se vogliamo, assegniamo un nome diverso alla rete *SSID* (3).

Nota: tutte le modifiche effettuate all'interno di ogni schermata vanno salvate con il tasto "Apply" e "Save"

5- Configurazione AP – Assegnazione parametri di sicurezza (Crittografia)

Robuste Status	Basic MA	C Filter Status	• Save • Reboot • Logout • Logge	English sed in as: admi
System	WiFi Basic Settings			
Network	Enable WiFi			
Route	Mode:	AP 🗸		
VPN	Channel:	Auto 🗸		
Services	SSID:	Router AP	Open	
Event/Log	Hide SSID:		WPA	
Configuration	Security Mode: Encryption:		WPA2	
Link Management	Passphrase:		CCMP(AES)	
Ethernet	Key Renewal Interval(s):	3600		
WIFI Control	WiFi Network Settings			
Senal	THUE Interface bridged wi	ik ath t - naturali antitinan alanan m	afan ta thia anna	
01/00	wirri internace bridded wi	n enii, network settings piedse re	erer to this bage.	
USB				
NAT/DMZ				
Firewall				
QoS				
IP Routing				









ù

Per garantire una protezione nella comunicazione dati è importante creare un profilo di sicurezza, selezionando il tipo di sicurezza (WPA o WPA2), la crittografia: TKIP o CCMP(AES) e la chiave di sicurezza "Passphrase" (Fig.5).

Una volta compilati i parametri nella sezione WiFi premere il tasto "Apply" e "Save"

6- Configurazione indirizzo SERVER DHCP

L'Access Point ha una configurazione DHCP Server il cui indirizzo, di default, appartiene alla stessa famiglia della Porta Ethenet1: 192.168.1.1, con un pool di indirizzi che va da IP:192.168.1.2 a IP:192.168.1.100. Questo vuol dire che tutti i dispositivi Client che si collegheranno all'Access Point, assumeranno come indirizzo IP in valore in DHCP della famiglia 192.168.1.XX. E' comunque possibile cambiare tale famiglia di indirizzi attraverso La sezione WiFi Network Setting (Fig.6)

Robuste	Radic MAC	Ciltor Statuc	• Save • Rebo	iot • Logout • English Logged in as: ai
System	WiEl Pacie Sottinge	June June June June June June June June		
Network				
Route	Made	40.		
VPN	Mode:			
Services	Cranner:	Auto •		
Event/Log	SIU:			
	Hide SSID:	MDAD .		
Configuration	Security Mode.			
Link Management	Encryption:			
Ethernet	Passpillase.	2000		
WiFi	Key Kenewai Interval(s):	3000		
Serial	WiFi Network Settings			
DI/DO	*WIFI Interface bridged with e	th1,network settings please refer	to this page.	
USB	h.			
NAT/DMZ				
Firewall				
QoS				
IP Routing	-			
DynDNS	-			
IPsec				
OpenVPN				
GRE				
L2TP				Apply Car
PPTP				

Fig.6 Assegnazione Indirizzi WiFi Network Setting





Fig.7 Assegnazione Pool indirizzi DHCP Server

Una volta eseguito le modifiche necessarie premere il pulsante "Apply" e "Save" per confermare le impostazioni.

Una volta terninato la configurazione base dell'Access Point è necessario effettuare un Rebbot del dispositivo selezionando con il Mouse la voce "Reboot" (Fig.8) e attendere circa 30 Secondi al riavvio del dispositivo.

Router-index ×			
· → C 🗋 192.168.0	0.1/index.asp		
Robuste			Save • Reboot • Logout • English • Logged in as: admin
Status	 Basic MAC 	Filter Sta	tus
System	WiFi Basic Settings		
Network	C Enable WiFi		La pagina all'indirizzo 192.168.0.1 dice:
Route	Mode:	AP 🔻	Annual sector and a sector and a sector
VPN	Channel:	Auto 💌	Are you sure to reboot the device:
Services	SSID:	Router AP	OK Annulla
Event/Log	Hide SSID:		
Configuration	Security Mode:	WPA2 •	
Link Management	Encryption:	TKIP •	
Ethernet	Passphrase:		
WiFi	Key Renewal Interval(s):	3600	

Fig.8 Riavvio dispositivo







Una terminato il reboot dell'Acces Point il Led Wlan, posto sul prontale del dispositivo sarà acceso, a conferma del modulo radio attivo.

7- Collegamento di un Notebook all'Access Point



Fig.9 Connessione con client (PC)

Una volta configurato l'Access Point è possibile associare i dispositivi "Client" , nel caso in esempio un Notebook (Fig.9)

8- Connessone Rete WiFi Notebook



Fig.10 Connessione Rete WiFi su Notebook

Attraverso la schedaq di rete Wifi del Notebook selezioniamo l'accessPoint corrispondente al profilo SSID di rete "Router_AP" (Fig.10)





ROBUSTEL SEAPIN152

	Connessione a una rete	
Digita	are la chiave di protezione di rete o la passphrase per Rout	er_AP
La pers	ona che ha configurato la rete può comunicare la chiave o la passphrase.	
Chiave	o passphrase di protezione:	
••••	••••	
Visu	alizza caratteri	
Ø	Se si dispone di un' <u>unità memoria flash USB</u> con le impostazioni di rete pe Router_AP, inserirla ora.	er
	Con	Annulla

Fig.11 Inserimento dati di crittografia

Inseriamo la Password precedentemente impostata nell'AccessPoint (Fig.11).

Contrast of	1000		A DECK DOOR OF
Disconne	ttersi o connette	rsi a un'altra rete	
Mostra	Tutte	•	
Connessio	ne rete wireless		· · ·
💐 R	outer_AP	Connesso	liter -
Je a	irel_guest	Rete protetta	liter
💐 Т	eleTu_f0842f0e8d81	Rete protetta	
Configura u	na connessione o un	a rete	
Apri Centro	connessioni di rete e	condivisione	

Fig.12 Associazione PC - Acess Point

Una volta terminata la procedura di Associazione del Notebook all'Access Point sarà visibile lo stato di connessione (Fig.12)





9- Verifica Status Connessioni Access Point

→ C 192.168.0	.1/index.asp			
Robuste Status	Basic	MACE	iter Status	• Save • Reboot • Logout • English • Logged in as: admi
System	Status			
Network	BSSID		00:23:a7:46:54:bb	
Route	SSID.		Pouter AD	
VPN	Mode:			
Services	Koy Manage	mont	WDAD DSK	
Event/Log	Cipher Pain	vise:	TKID	
Configuration	Cipher Grou	p:	TKIP	
connguration	WPA State:		Completed	
Link Management	Address:		00:23:a7:46:54:bb	
Ethernet				
WiFi	Associated Clie	nts		
Serial	Index	BSSID	IP Address	
DI/DO	1	00:22 fa:d4:30:18	192.168.1.2	
USB				
NAT/DMZ				
Firewall				

Fig.13 Associazione Client - Access Point

Nelle impostazioni di configurazione WiFi dell'Access Point, nella sezione "Status", è possibile verificare la presenza dei dispositivi associati e il relativo indirizzo IP acquisito (Fig.13)

10- Utilizzo del dispositivo SEAPin152 come Client WiFi

E' possibile utilizzare il dispositivo SEAPIN152 in modalità Client WiFi

🖹 Router-index 🛛 🗙		
← → C 🗋 192.168.0.1	1/index.asp	
Robustel		Save • Reboot • Logout • English • Logged in as: admin
Status 🔺	Link Management	
System	Link Management Settings	Eth0 WiFi
Network	Primary Interface:	WiFi •
Route	Backup Interface:	None T
VPN	ICMP Detection Primary Server:	8.8.8.8
Services	ICMP Detection Secondary Server:	8.8.4.4
Event/Log	ICMP Detection Interval (s):	30
Configuration	ICMP Detection Timeout (s):	3
Link Management	ICMP Detection Retries:	3
WiFi	*It is recommended to use an ICMP detec	tion server to keep router always online.
Serial	*The ICMP detection increases the reliabil	ty and also cost data traffic.
DI/DO	*DNS example: Google DNS Server 8.8.8.	3 and 8.8.4.4
USB		
NAT/DMZ		
Firewall		
QoS		



Supporto tecnico:



tecnico@direl.it

8



Attraverso la sezione di configurazione "Link Management Setting", alla voce "Primary Interface", tramite il menù a tenda selezionare l'opzione "WiFi" e confermare la scelta premendo i tasti "Apply", "Save" e "Reboot" (Fig.14)

11- Configurazione connessione Client

lobuste	1		• Save • Reboot • Logout •	English
tatus	A Basic	Status	Logge	d in as: ad
System	WiFi Basic Settings			
Network	Enable WiFi			
Route	Mode:	Client V		
/PN	Chappel	Auto		
ervices	SSID:	Router AP	n	
event/Log	Hide SSID:			
onfiguration	Security Mode:	Open 🔻		
.ink Management	WiFi Network Settings			
Ethernet	IP Configuration:	DHCP Client •		
WiFi	Use Peer DNS			
Serial	Override DHCP Server	Values:		
DI/DO	Netmask:			
JSB	Gateway:			
AT/DMZ				
irewall				
2oS				
P Routing				
OvnDNS			Apply	Cancel

Fig.15 Scansione reti WiFi disponibili

Una volta effettuato il Reboot del dispositivo torniamo nella sezione di configurazione "WiFi" e selezioniami il pulsante "Scan" (Fig.15)

Robuste Status	Basic	Status			• Save • Reboot • Logout • Englis Logged in as:
System	Status		_		
Network	BSSID:				
Route	SSID:				
VPN	Mode:				
Services	Key Management:				
Event/Log	Cipher Pairwise:				
Configuration	Cipher Group:				
Link Management	WPA State:	Scann	ing		
Ethernet	Address:	00:23	:a7:46:54:t	ob	
Lenernee	Scan Results				
WiFi		0070	Channel	Signal Level	Flags
WiFi Serial	BSSID	5510			
WiFi Serial DI/DO	BSSID 00:a0:a2:62:90:64	direl_guest	7	-65	[WPA2-PSK-1KIP+CCMP][ESS]
WiFi Serial DI/DO USB	BSSID 00:a0:a2:62:90:64 00:01:36:e3:63:98	direl_guest FASTWEB-1-N3koz(7	-65	[WPA2-PSK-TKIP][ESS] [WPA-PSK-TKIP][WPS][ESS]
WiFi Serial DI/DO USB NAT/DMZ	BSSID 00:a0:a2:62:90:64 00:01:36:e3:63:98	direl_guest FASTWEB-1-N3koz(7	-65 -76	[WPA2-PSK-TKIP][WPS][ESS] [WPA-PSK-TKIP][WPS][ESS]
WiFi Serial DI/DO USB NAT/DMZ Firewall	BSSID 00:a0:a2:62:90.64 00:01:36:e3:63:98	direl_guest FASTWEB-1-N3koz(7 1	-65 -76	[WPA2:PSK-TKIP+CCMP][ESS] [WPA-PSK-TKIP][WPS][ESS]
WiFi Serial DI/DO USB NAT/DMZ Firewall QoS	BSSID 00:a0:a2:62:90:64 00:01:36:a3:63:98	direl_guest	7 1	-65	[WPA2+3K-1KIP+CCMP][ESS] [WPA-PSK-TKIP][WPS][ESS]
WiFi Serial DI/DO USB NAT/DMZ Firewall QoS IP Routing	BSSID 00:a0:a2:62:90.64 00:01:36:e3:63:98	direl_guest FASTWEB-1-N3koz(7	-65	[WPA2+3K-1KIP+CCMP][ESS] [WPA-PSK-TKIP][WPS][ESS]



Supporto tecnico:

9



Attraverso la sezione "Status" è possibile vedere le reti WiFi disponibili (Fig.16)

12- Connessione ad una rete

lobuste			Save • Reboot • Logout • English
tatus	A Basic S	tatus	Logycum as. u
System	WiFi Basic Settings		
Vetwork	Enable WiFi		
toute	Mode:	Client V	
PN	Channel	Auto T	
ervices	SSID	diral quest	an
vent/Log	Hide SSID:		
nfiguration	Security Mode:	WPA2 V	
omiguration	Encryption:	TKIP	
ink Management	Passnbrase		
Ethernet	Passpinase.		
ViFi	WiFi Network Settings		
Serial	IP Configuration:	DHCP Client •	
DI/DO	Use Peer DNS		
JSB	Override DHCP Server V	alues:	
IAT/DMZ	Netmask:		
irewall	Gateway:		
QoS .			
P Routing			
DynDNS			
Psec			
penVPN			
RE			
2TP			
PTP	1		
SNMP			Apply Cancel
/RRD			2 <u></u>

Fig.17 Inserimento dati Rete e crittografia

A titolo di esempio è possibile effettuare una connessione ad una rete visualizzata (fig.16), ad esempio: direl_guest.

Per collegare il dispositivo all'Access Point con SSID: direl_guest è necessario inserire nella sezione di configurazione "WiFi Basic Setting" il nome della rete SSID corretto (1) e, ove richiesto, i dati di crittografia (2), visualizzati nella sezione di Status (Fig.16), relativi all'access point "direl_guest" (Fig.17).

Procedere poi alla conferma e alla memorizzazione dei dati in modo permanente dei dati inseriti tramite il tasto "Apply", "Save".

Per associare correttamente il Client alla rete SSID "direl_guest" è necessario procedere ad un "Reboot" del dispositivo.





Al riavvio del dispositivo dovremo attendere la fase di associazione con l'Access Point, questa operazione potrebbe impiegare un tempo piu' o meno lungo, a seconda del modello di Access Point in uso. E' possibile verificare la corretta associazione tramite la sezione "WiFi" alla voce "WPA State".

Robuste	Basic	Status			 Save • Reboot • Logout • English Logged in as: at
System	Status				
Network	BSSID:	00:a0	:a2:62:90:6	54	
Route	SSID:	direl	quest		
VPN	Mode:	client			
Services	Key Managemen	Key Management: W/DA3-DSK			
Event/Log	Cipher Pairwise:	ткір			
onfiguration ink Management	Cipher Group: WPA State:	TKIP Comp	leted 🔫	ab	
Ethernet	Addressi	00125	10714010410		
WiFi	Scan Results				
Serial	BSSID	SSID	Channel	Signal Level	Flags
DI/DO	00:a0:a2:62:90:64	direl_guest	7	-59	[WPA2-PSK-TKIP+CCMP][ESS]
JSB	f0:84:2f:0e:8d:81	TeleTu_f0842f0e8d81	1	-77	[WPA-PSK-CCMP][WPA2-PSK-CCMP][ESS]
AT/DMZ					
irewall					
QoS					
P Routing	1				
	-				

Fig.19 Associazione client con Access Point

Nella sezione "Status/System", sara' possibile vedere lo status della connessione e l'eventuale indirizzo IP acquisito dall'access Point (Fig.19)

			Save • Reboot • Logout • English
lobuste	• /		
tatus	System		Logged in as: adm
System	LEDs Information		
Network	BUN: GREEN/BLINK		
Route	WIEI: GREEN/BLINK		
VPN	USR: OFF		
Services			
Event/Log	Router Information		
and the second the second	Device Model:	R3000-NU	
onliguration	Serial Number:	00302114030018	
Link Management	Device Name:	Cellular Router	
Ethernet	Firmware Version:	1.01.01-sub-140125	
WiFi	Hardware Version:	1.02.01	
Serial	Kernel Version:	2.6.39-7	
DI/DO	Uptime:	0 day 00:16:06	
USB	CPU Load:	03.57%	
NAT/DMZ	RAM Total/Free:	123.03MB/70.97MB(57.68%)	
Firewall	System Time:	1970-01-01 08:16:06	
QoS	Current WAN Link		
IP Routing	Current WAN Link:	wiEi	
DynDNS	IP Address:	192 168 123 102	
IPsec	Gataway	102 168 123 254	
OpenVPN	NetMask:	255 255 255 0	
GRE	DNS Server	102 168 122 254	
L2TP	Keepplive PING IP Address:	000000010	
PPTP	Keepaive PING IP Address:	0.0.0.0, 0.0.4.4	
SNMP	Reepaive Pino interval:	30	

Fig.19 System status Connessione Rete "direl_guest"







13-Note per il Troubleshooting

→ C 192.168.0	0.1/index.asp		
Robuste Status	2 Link Management	• Save • I	Reboot • Logout • English • Logged in as: adm
System	Link Management Settings		
Network	Primary Interface:	Eth0 •	
Route	Backup Interface:	None 🔻	
VPN	ICMP Detection Primary Server:	8.8.8.8	
Services	ICMP Detection Secondary Server:	8.8.4.4	
Event/Log	ICMP Detection Interval (s):	30	
Configuration	ICMP Detection Timeout (s):	3	
	ICMP Detection Retries:	3	
Link Management	Reset The Interface		
Eulemet	*It is recommended to use an ICMP detect	on server to keep router always online.	
Forial	*The ICMP detection increases the reliabilit	y and also cost data traffic.	
	*DNS example: Google DNS Server 8.8.8.8	and 8.8.4.4	
LISB			
NAT/DMZ			
	-		

L'Access Point è dotato di funzione ICMP Detection per il controllo dello stato connessione verso un indirizzo IP, al fine dell'utilizzo come Access Point tale funzione non è necessaria in quanto potrebbe comportare delle disconnessioni dell'Access Point verso i Client ritenute erroneamente anomali, si suggerisce pertanto di verificare che la voce "Reset the interface", presente alla sezione "Configuration", non sia presente il segno di spunta (Fig.20).

14-Reset

E' possibile ripristinare il dispositivo con le impostazioni di base attraverso il pulsante "Reset", posto sul frontale del dispositivo, tenendolo premuto per circa 30 secondi fino a vedere i LED di status eseguire una serie di lampeggi, terminata questa fase il dispositivo tornerà con le impostazioni di fabbrica.



Supporto tecnico:

12

tecnico@direl.it