

Instruction Manual

PENTAGRAM horNET Wi-Fi USB 9dBi (P 6122-20)



For the latest versions of manuals, drivers and software, visit www.pentagram.eu .

NOTE: All information and technical specifications provided in this manual are subject to change without notice and/or indication.

© **2008 PENTAGRAM**

All rights reserved. Unauthorized duplication and copying prohibited.

INDEX

INTRODUCTION	5
PACKAGE CONTENTS	5
REQUIREMENTS	5
INSTALLING THE ADAPTER AND SOFTWARE	6
WIRELESS ADAPTER CONFIGURATION	7
RAUI APPLICATION	7
PROFILE TAB	8
NETWORK TAB	15
ADVANCED TAB	18
STATISTICS TAB	19
WMM TAB	20
WPS TAB	21
RADIO ON/OFF TAB	23
ABOUT TAB	23
HELP TAB	23
TROUBLESHOOTING	24





Introduction

PENTAGRAM horNET Wi-Fi USB 9dBi (P 6122-20) is a high-performance, easy-to-install 32-bit wireless network adapter attached via USB. The adapter can be used in ad hoc mode to establish peer-to-peer connections with other adapters for file sharing, or in infrastructure mode to provide Internet access on home or office networks using an access point or a router. PENTAGRAM horNET USB supports 802.11g connectivity with a maximum data rate of up to 54 Mbps! With a rich feature set, it can also interoperate with 802.11b (11 Mbps) products in home or office environments, and with public hotspots. Regardless of the mode, your data remain secure thanks to robust WPA encryption.

Package contents

1. PENTAGRAM horNET Wi-Fi USB 9dBi (P 6122-20) network adapter
2. External 9dBi antenna with RP-SMA connector
3. CD with drivers, software and manuals
4. Quick installation instructions

If any of the package contents are missing, please contact your vendor.

Requirements

- PC with an available USB port
- Windows 98SE, ME, 2000, XP, 2003 or Vista operating system
- CD-ROM drive
- 802.11g/802.11b-compliant access point (for infrastructure mode) or 802.11g/802.11b-compliant wireless adapter (for ad hoc/peer-to-peer mode)



Installing the adapter and software

Note: Do not connect the adapter to your PC before installing drivers!




1. Screw the supplied 9dBi antenna into the adapter's RP-SMA connector.



2. Insert the driver and utility CD into the CD-ROM drive. The setup wizard will launch automatically (under Windows Vista, you may additionally need to select **Run: Autorun.exe** in the Autorun window). If the CD-ROM autorun feature is disabled, run **Autorun.exe** in the CD's root directory.
3. Select **driver and utility**, to start driver installation.
4. Select **I accept the terms of the license agreement** and click **Next >**.
5. If you want to use attached application software (recommended), select **Ralink Configuration Tool** and click **Next >**. If you want to use application software built in operation system, select **Microsoft Zero Configuration Tool** and click **Next >**.
6. Select **Optimize for WiFi mode** and click **Next >** for compatibility. Select **Optimize for performance mode** and click **Next >** for performance. Second option may cause incompatibilities with some wireless devices – if that's the case, uncheck **Enable Tx Burst** option on **Advanced** Tab in attached application software.
7. Click **Install**, to install drivers and application.
8. In some cases there is a need to restart computer after driver installation. Select **Yes, I want to restart my computer now.**, to restart computer after installation or **No, I will restart my computer later.** if you plan to restart computer at later time.
9. Click **Finish**, to complete installation process.
10. Plug the adapter into an USB port.

Wireless adapter configuration

A configuration application is installed with adapter drivers. The application's icon is displayed in the system tray (next to the clock), and its appearance depends on the adapter and/or connection status.

		
The adapter is not attached to the PC or RF is off.	The adapter is not connected to a wireless network.	The adapter is connected to a wireless network.

To launch the adapter's configuration application, double-click the application's icon (**RaUI**).

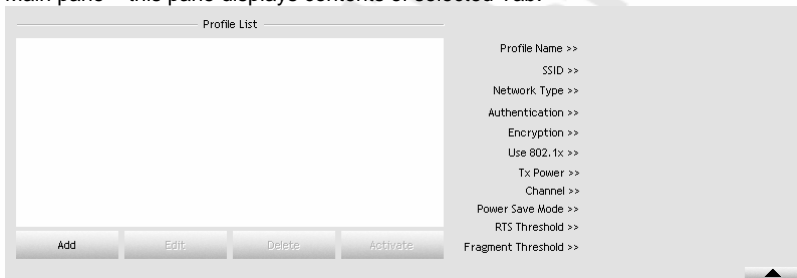
RaUI application

RaUI application window is divided into three parts:

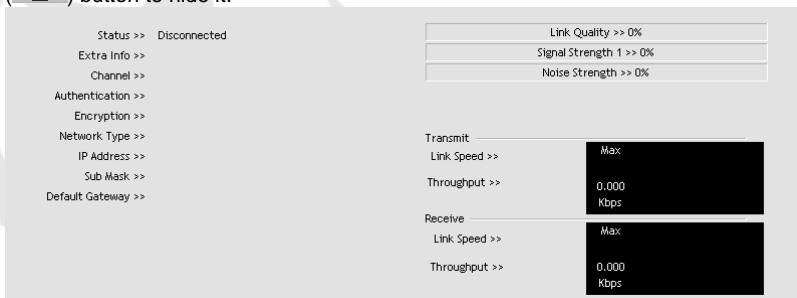
1. Tab bar – click on Tab to display its contents in the main pane. Active Tab is highlighted. Use arrow buttons to scroll Tab bar.



2. Main pane – this pane displays contents of selected Tab.



3. Secondary pane – this pane contains connection information or additional options for selected in main pane option. Click **More** (▼) button to show secondary pane or **Less** (▲) button to hide it.



Connection information contains:

Status – Connection status:

- **RF OFF** – Adapter disconnected or RF is turned off.

- **Disconnected** – Wireless connection not established.
 - **[SSID] <--> [BSSID]** – Connection established to network with displayed ID's.
- Extra Info** – Additional information about connection.
Channel – Channel (frequency) used by wireless network.
Authentication – Authentication method used by wireless network.
Encryption – Encryption method used by wireless network.
Network Type:
- **Ad hoc** – Connection point-point (peer-to-peer) with other wireless adapter.
 - **Infrastructure** – Connection with wireless network via AP (Access Point) or wireless router.
- Status** – Wireless connection status.
IP Address – IP Address configured or obtained from DHCP server.
Sub Mask – Subnet Mask configured or obtained from DHCP server.
Default Gateway – Gateway IP address configured or obtained from DHCP server.
- Link Quality:** Shows link quality as a percentage bar (0-100%).
Signal Strength: Shows signal strength as a percentage bar (0-100%).
Noise Level: Shows noise level as a percentage bar (0-100%).
- Transmit / Receive** – Transmit / receive parameters for active network.

Profile Tab

This Tab allows you to create profiles for the most frequently used wireless networks, i.e. home network, company network or public hotspots. The profiles can be activated as required.



Profile List – This list contains configured profiles. First column contains profile name, second – network SSID and third – additional network information. Icons on the list means:

	Connection with activated profile established successfully
	Connection with activated profile not established
	Infrastructure Type network
	Ad hoc Type network
	Secured network

Selected profile information is displayed on the right side of the list.

Add: Click **Add** to create a new profile. Profile configuration is opened in secondary pane.

Edit: Click **Edit** to change settings for the selected profile. Profile configuration is opened in secondary pane.

Delete: Click **Delete** to delete the selected profile.

Activate: Click **Activate** to activate the selected profile.

Profile configuration – System Config Tab

This Tab allows configuration of basic connection parameters.

The screenshot shows the 'System Config' window with the following settings:

- Profile Name: PROF1
- SSID: (empty dropdown)
- Network Type: Infrastructure
- Tx Power: Auto
- Preamble: Auto
- Power Save Mode: CAM (selected), PSM (selected)
- RTS Threshold: 2347
- Fragment Threshold: 2346

Profile Name – Enter a name to identify your profile. Default PROFx.

SSID – Enter a network service set identifier (SSID) or select from a list of active networks. If SSID Broadcast function of AP is disabled, SSID must be entered by hand. SSID is case sensitive, which means that *pentagram* and *Pentagram* are two different networks.

Network Type – You can select two wireless network types.

- The **Infrastructure** mode supports communications between a wireless network and a wired network using an access point.
- The **Ad hoc** mode supports peer-to-peer communications between two wireless network devices (without using an access point).

TX Power – Set the signal transmit power to be used by the radio transmitter. Choose the appropriate value from the drop-down list.

Preamble – Select the preamble length, i.e. **Auto**, **Long** or **Short**.

Channel – Select the channel to be used when establishing an Ad hoc network.

PSM – Select the power saving mode.

- Using **CAM** (Constantly Awake Mode), the network adapter will operate at full power when connected to mains.
- Using **PSM** (Power Saving Mode), the network adapter will enter power saving mode.

RTS Threshold – Use the slider or enter a value for the RTS threshold in the field provided. Default value: **2347**.

Fragment Threshold – Use the slider or enter a value for the fragment threshold in the field provided. Default value: **2346**.

OK – Closes profile configuration and saves settings.

Cancel – Closes profile configuration without saving settings.

Profile configuration – Auth. \ Encry. Tab

This Tab contains all Authentication and Encryption settings

Authentication:

- **Open** – With the **Open** method, every wireless station can request authentication.
- **Shared** – With **Shared** authentication, the station requesting authentication must provide a secret key (which can be obtained from the network administrator) using a secure channel (independent of the 802.11 wireless communications channel).
- **LEAP** – (Light Extensible Authentication Protocol) is an EAP authentication method used primarily on Cisco Aironet wireless networks. This protocol encrypts transmitted data using dynamically generated WEP keys, and supports two-way authentication.
- **WPA** and **WPA2** – IEEE 802.1x protocol is used for authentication and AES or TKIP for encryption.
- **WPA PSK** and **WPA2 PSK** – Station requesting authentication must provide a WPA Preshared Key. AES or TKIP are used for encryption.
- **Authentication: Open and Shared**

The screenshot shows the 'Auth. \ Encry.' tab with the '802.1X' sub-tab selected. The 'Authentication' dropdown is set to 'Open', and the 'Encryption' dropdown is set to 'None'. There is a checkbox for '802.1X' which is currently unchecked. Below these are fields for 'WPA Preshared Key' and 'Wep Key'. The 'Wep Key' section contains four entries: Key#1, Key#2, Key#3, and Key#4. Each entry has a radio button, a 'Hexadecimal' dropdown menu, and an input field. A 'Show Password' checkbox is located to the right of the input fields. At the bottom of the window are 'OK' and 'Cancel' buttons.

Authentication – Change authentication method.

Encryption – Select **None** or **WEP**.

802.1X – Check this option to use IEEE 802.1x for authentication. IEEE 802.1x supports full user authentication and control. This will also enable 8021X Tab, where 802.1x can be configured.

WEP Key / Key#1 ... 4 – When you select **WEP** encryption or **Shared** authentication without **802.1x**, you need to enter a correct WEP key.

- If a 64-bit WEP key is used, enter 10 **Hexadecimal** characters or 5 **ASCII** characters.
- If a 128-bit WEP key is used, enter 26 **Hexadecimal** characters or 13 **ASCII** characters.

Show Password – Select this box if you do not want key characters to be replaced with asterisks.

OK – Closes profile configuration and saves settings.

Cancel – Closes profile configuration without saving settings.

● **Authentication: LEAP**

Authentication – Change authentication method.

Identity – Enter your identity for the LEAP authentication service.

Password – Enter your password for the LEAP authentication service.

Domain Name – Enter your domain name for the LEAP authentication service.

Show Password – Select this box if you do not want key characters to be replaced with asterisks.

OK – Closes profile configuration and saves settings.

Cancel – Closes profile configuration without saving settings.

● **Authentication: WPA and WPA2**

Authentication – Change authentication method.

Encryption – Select the encryption method to be used.

- **AES** (Advanced Encryption System) uses symmetrical 128-bit data block encryption.

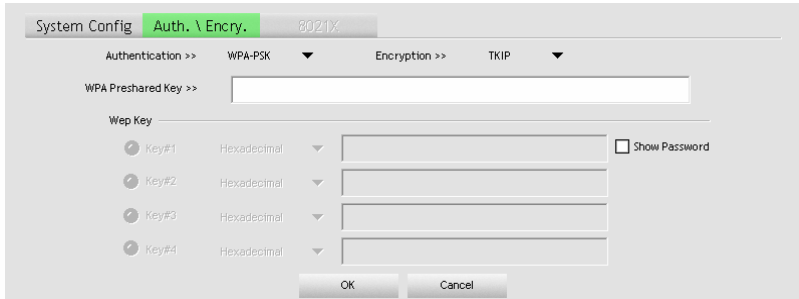
- **TKIP** (Temporal Key Integrity Protocol) uses stronger encryption algorithms and MIC (Message Integrity Check) to provide security against hackers.

WPA and WPA2 use IEEE 802.1x protocol for authentication. After selecting encryption method go to 8021X Tab, where 802.1x settings can be configured.

OK – Closes profile configuration and saves settings.

Cancel – Closes profile configuration without saving settings.

● **Authentication: WPA PSK and WPA2 PSK**



Authentication – Change authentication method.

Encryption – Select the encryption method to be used.

- **AES** (Advanced Encryption System) uses symmetrical 128-bit data block encryption.
- **TKIP** (Temporal Key Integrity Protocol) uses stronger encryption algorithms and MIC (Message Integrity Check) to provide security against hackers.

WPA Preshared Key – Enter the WPA preshared key (WPA-PSK and WPA2-PSK only). The key should be 8 to 32 characters in length.

Show Password – Select this box if you do not want key characters to be replaced with asterisks.

OK – Closes profile configuration and saves settings.

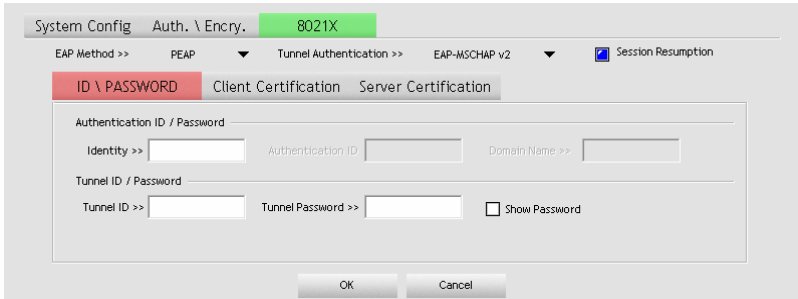
Cancel – Closes profile configuration without saving settings.

Profile configuration – 8021X Tab

Settings on this Tab allow configuring IEEE 802.1x protocol. All information can be obtained from wireless network administrator. Appearance of this Tab depends on options selected from **EAP Method** and **Tunnel Authentication** lists.

- **PEAP** – Protect Extensible Authentication Protocol. PEAP transport securely authentication data by using tunneling between PEAP clients and an authentication server. PEAP can authenticate wireless LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure wireless LAN.
- **TLS/Smart Card** – Transport Layer Security. Provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point.
- **TTLS** – Tunneled Transport Layer Security. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
- **EAP-FAST** – Flexible Authentication via Secure Tunneling. It was developed by Cisco. Instead of using a certificate, mutual authentication is achieved by means of a PAC (Protected Access Credential) which can be managed dynamically by the authentication server. The PAC can be provisioned (distributed one time) to the client either manually or automatically. Manual provisioning is delivery to the client via disk or a secured network distribution method. Automatic provisioning is an in-band, over the air, distribution. For tunnel authentication, only support "Generic Token Card" authentication now.
- **MD5-Challenge** – Message Digest Challenge. Challenge is an EAP authentication type that provides base-level EAP support. It provides for only one-way authentication - there is no mutual authentication of wireless client and the network.

• **ID \ PASSWORD Tab**



EAP Method – Change EAP authentication method.

Tunnel Authentication – Change tunnel authentication method.

Session Resumption – Enable / disable session resumption.

Authentication ID / Password – **Identity**, **Password** and **Domain Name** for server. Only **EAP-FAST** authentication can key in domain name. Domain name can be keyed in blank space.

Tunnel ID / Password:

- **Identity** – Identity for tunnel.
- **Password** – Password for tunnel.

Show Password – Select this box if you do not want key characters to be replaced with asterisks.

OK – Closes profile configuration and saves settings.

Cancel – Closes profile configuration without saving settings.

• **Client Certification Tab**

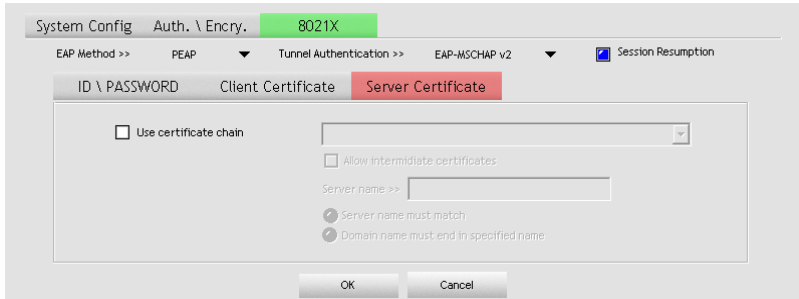


Use Client certificate – Enable this option to use Client certificate for server authentication and then select certificate from drop-down list. You can find detailed information on certificate below this list.

OK – Closes profile configuration and saves settings.

Cancel – Closes profile configuration without saving settings.

• **Server Certification Tab**



Use certificate chain – Enable this option, to enable the certification feature and select the certificate issuer.

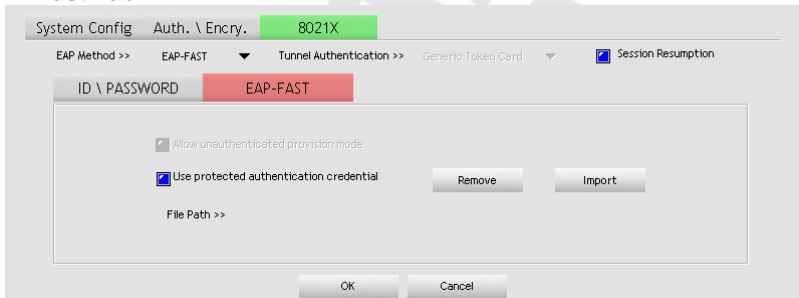
Allow intermediate certificates – Select this option to allow the use of intermediate certificates. These certificates must be located on the certification chain between the server certificate and the server selected from list.

Server name – Enter the name of the authentication server.

OK – Closes profile configuration and saves settings.

Cancel – Closes profile configuration without saving settings.

• **EAP Fast Tab**



Allow unauthenticated provision mode – During the PAC can be provisioned (distributed one time) to the client automatically. It only supported **Allow unauthenticated provision mode** and use **EAP-MSCHAP v2** authentication to authenticate now. It causes to continue with the establishment of the inner tunnel even though it is made with an unknown server.

Use protected authentication credential – During the PAC can be provisioned to the client manually via disk or a secured network distribution method. Click **Import**, to browse for PAC settings file or click **Remove**, to stop using current file.

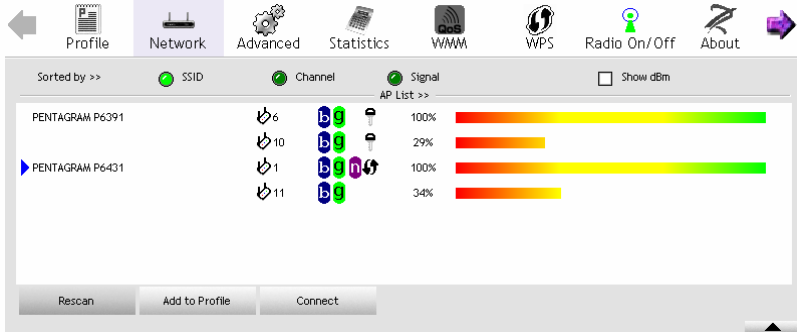
File Path – Path, where PAC settings file is located.

OK – Closes profile configuration and saves settings.

Cancel – Closes profile configuration without saving settings.

Network Tab

This Tab enables searching for and connecting to active wireless networks.



Icons on list means:

	Connection to this network established successfully
	Connection to this network not established
	Infrastructure type network
	Ad hoc type network
	802.11 standards supported by wireless station
	Access Point supports WPS function and it's enabled
	Secured network

Show dBm – Select this box, to show signal Strength on **AP List** as dBm instead of percentages. This also applies to **Signal Strength** and **Noise Strength** in secondary pane.

AP List – List of wireless networks in range. Columns contains as follows: SSID (hidden when SSID Broadcast on AP is disabled), network type icon (Infrastructure or Ad hoc) and used channel, supported 802.11 standards (i.e. 802.11g), security and signal strength. Double-click on network, to display Detailed network information in secondary pane.

Rescan – Click this button to rescan for available wireless networks.

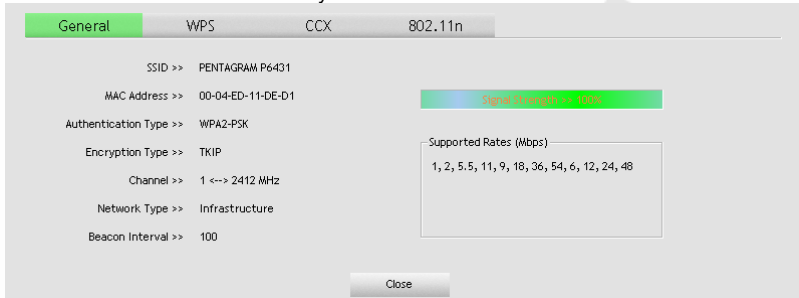
Add to Profile – Click to create a profile for selected network. You can find detailed information on profile configuration in previous section.

Connect – Click to connect do selected network without creating a profile. Connection configuration will be displayed in secondary pane. Options correspond to options from profile configuration. You can find detailed information on profile configuration in previous section. If selected network doesn't broadcast SSID, after clicking **Connect** button you will be asked to enter SSID. Enter SSID in **Please enter SSID** field in secondary pane and click **OK**, to continue connection configuration.

Detailed network information

- **General Tab**

General info on network and security.



SSID – Network SSID or **Hidden** if AP doesn't broadcast SSID.

MAC Address – MAC address of AP.

Authentication Type – Authentication used by this network.

Encryption Type – Encryption used by this network.

Channel – Channel and frequency used by this network.

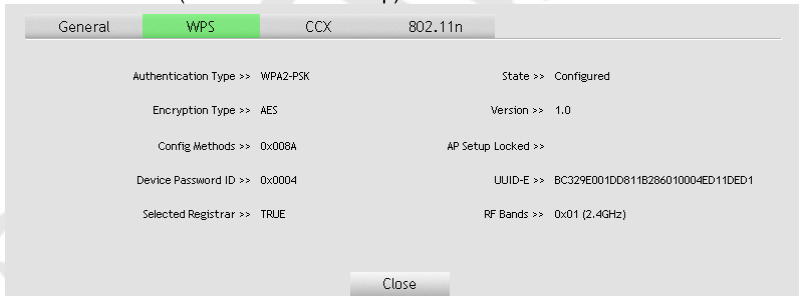
Network Type – Infrastructure or Ad hoc.

Beacon Interval – Interval for sending beacon to sustain connection.

Close – Close information.

- **WPS Tab**

Information on WPS (Wi-Fi Protected Setup).



Authentication Type – There are three types of authentication modes supported by RaConfig. They are open, Shared, WPA-PSK and WPA system.

Encryption Type – For open and shared authentication mode, the selection of encryption type are None and WEP. For WPA, WPA2, WPA-PSK and WPA2-PSK authentication mode, the encryption type supports both TKIP and AES.

Config Methods – Correspond to the methods the AP supports as an Enrollee for adding external Registrars. (a bitwise OR of values)

Value	Hardware Interface
0x0001	USBA (Flash Drive)
0x0002	Ethernet
0x0004	Label
0x0008	Display

horNET Wi-Fi USB 9dBi (P 6122-20)

0x0010	External NFC Token
0x0020	Integrated NFC Token
0x0040	NFC Interface
0x0080	Push Button
0x0100	Keypad

Device Password ID – Indicate the method or identifies the specific password that the selected Registrar intends to use. AP in PBC mode must indicate 0x0004 within two-minute Walk Time.

Value	Description
0x0000	Default (PIN)
0x0001	User-specified
0x0002	Rekey
0x0003	Display
0x0004	PushButton (PBC)
0x0005	Registrar-specified
0x0006-0x000F	Reserved

Selected Registrar – Indicate if the user has recently activated a Registrar to add an Enrollee. The values are **TRUE** and **FALSE**.

State – The current configuration state on AP. The values are **Unconfigured** and **Configured**.

Version – WPS specified version.

AP Setup Locked – Indicate if AP has entered a setup locked state.

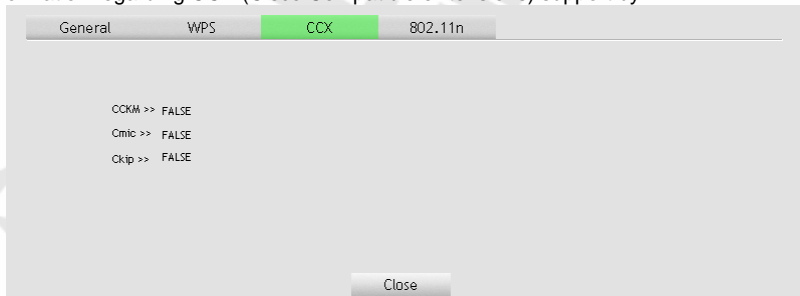
UUID-E – The universally unique identifier (UUID) element generated by the Enrollee. There is a value. It is 16 bytes.

RF Bands – Indicate all RF bands available on the AP. A dual-band AP must provide it. The values are **2.4GHz** and **5GHz**.

Close – Close information.

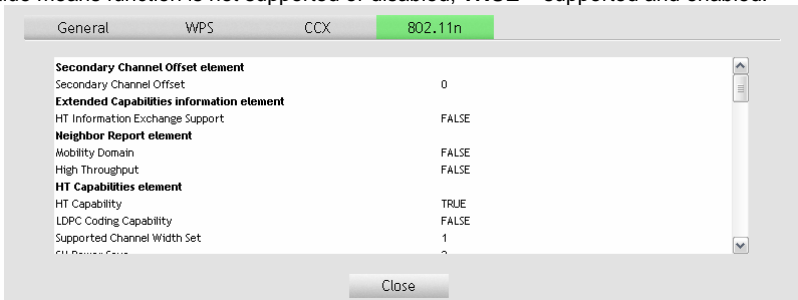
- **CCX Tab**

Information regarding CCX (Cisco Compatible eXtensions) support by AP.



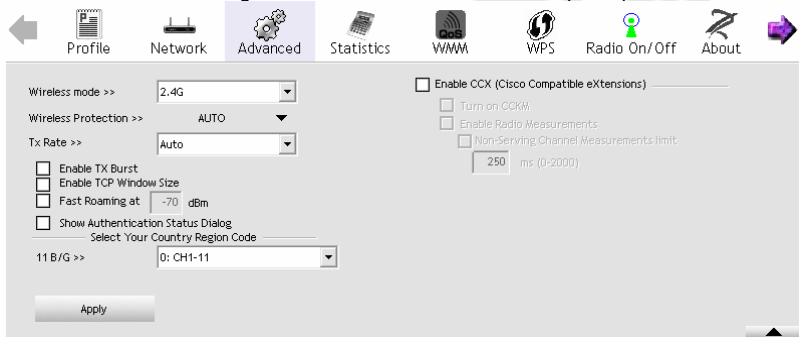
● **802.11n Tab**

Detailed information about APs support of 802.11n protocol and its functions. **FALSE** value means function is not supported or disabled, **TRUE** – supported and enabled.



Advanced Tab

This Tab can be used to change advanced wireless network adapter options.



Wireless mode – Select wireless mode in which adapter will work.

Wireless Protection – **AUTO** (STA will dynamically change as AP announcement), **ON** (Always send frame with protection) or **OFF** (Always send frame without protection).

TxRate – Allows the transmit rate to be changed manually. Default value: **Auto**.

Enable TX BURST – Selecting this mode may accelerate frame transmission.

Enable TCP Window Size – Selecting this feature may improve TCP performance on wireless connections.

Fast Roaming – Switchover between access points will occur when the current access point's minimum signal strength threshold set in this field is exceeded.

Show Authentication Status Dialog – When you connect AP with authentication, choose whether show **Authentication Status Dialog** or not. Authentication Status Dialog displays the process about 802.1x authentication.

Select Your Country Region Code – The item selected in this field determines the channels (frequencies) available. In some cases driver will select region based on regional settings of operating system – in those cases it's not possible to change this value.

Enable CCX (Cisco Compatible eXtensions) – This enables support for Cisco Compatible Extensions.:

- **Turn on CCKM** – Using LEAP allows taking advantage of CCKM (Cisco Centralized Key Management).
- **Enable Radio Measurement** – Enables support for the Radio Measurement feature used in Cisco network hardware.

Apply – Applies changes.

Statistics Tab

This Tab shows **Transmit** and **Receive** statistics.

The screenshot shows the 'Statistics' tab selected in the top navigation bar. The 'Transmit' sub-tab is active, displaying a table of statistics. A 'Reset Counter' button is located at the bottom left of the table area.

Statistic	Value
Frames Transmitted Successfully	0
Frames Retransmitted Successfully	0
Frames Fail To Receive ACK After All Retries	0
RTS Frames Successfully Receive CTS	0
RTS Frames Fail To Receive CTS	0

Frames Transmitted Successfully – shows the number of frames transmitted without errors.
Frames Retransmitted Successfully – shows the number of frames transmitted successfully after retrying.

Frames Fail To Receive ACK After All Retries – shows the number of frames which did not receive acknowledgement after all retries.

RTS Frames Successfully Receive CTS – shows the number of RTS (Request To Send) frames which received responses in the form of CTS (Clear To Send) frames.

RTS Frames Fail To Receive CTS – shows the number of RTS (Request To Send) frames which did not receive responses in the form of CTS (Clear To Send) frames.

Reset Counter – Click this button to reset all Transmit statistics.

The screenshot shows the 'Statistics' tab selected in the top navigation bar. The 'Receive' sub-tab is active, displaying a table of statistics. A 'Reset Counter' button is located at the bottom left of the table area.

Statistic	Value
Frames Received Successfully	0
Frames Received With CRC Error	0
Frames Dropped Due To Out-of-Resource	0
Duplicate Frames Received	0

Frames Received Successfully – shows the number of frames received without errors.

Frames Received with CRC Error – shows the number of frames received with CRC errors.

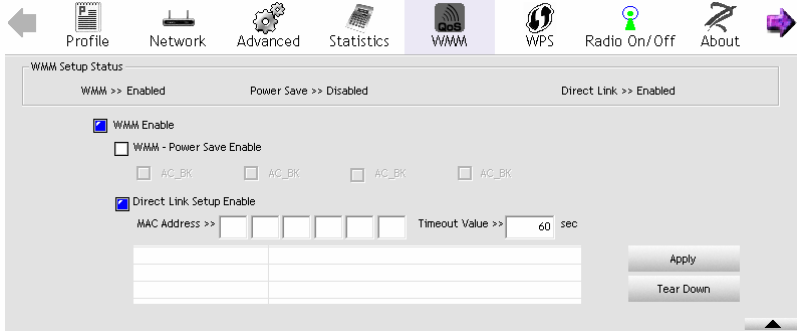
Frames Dropped Due To Out-of-Resource – shows the number of frames dropped due to resource issue.

Duplication Frames Receive – shows the number of received duplicate frames.

Reset Counter – Click this button to reset all Receive statistics.

WMM Tab

This Tab contains settings for WMM (Wi-Fi Multimedia), which provide basic QoS (Quality of Service) for 802.11 networks. WMM prioritize traffic based on four Access Categories (AC): voice, video, best effort and background. WMM doesn't guarantee throughput for ACs and can be used for VoIP applications. To use WMM functions WMM must be also supported by AP.



WMM Setup Status – Status of WMM options: **Disabled** or **Enabled**.

WMM Enable – Enable Wi-Fi Multi-Media.

WMM – Power Save Enable – Enable WMM Power Save and select ACs: AC_BK (background), AC_BE (best effort), AC_VI (video), AC_VO (voice).

Direct Link Setup Enabled – Enable DLS (Direct Link Setup).

MAC Address – MAC Address of remote STA (must conform to two conditions: connect with the same AP that support DLS features and have to enable DLS).

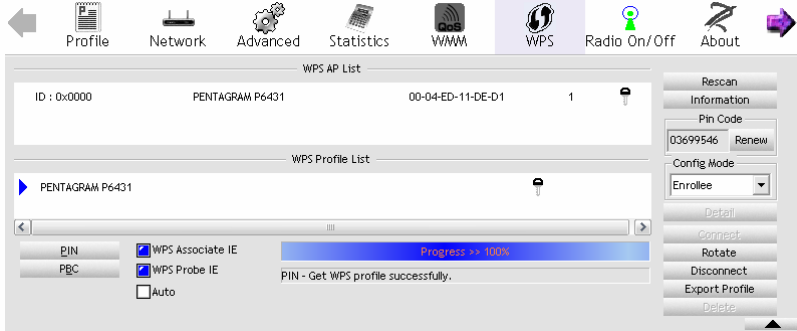
Timeout Value – represents that it disconnect automatically after some seconds. The value is integer. The integer must be between 0~65535. It represents that it always connects if the value is zero. Default value of Timeout Value is 60 seconds.

Apply – Click, to save DLS and add it to the list.

Tear Down – Select DLS from list and click this button, to remove it.

WPS Tab

The primary goal of Wi-Fi Protected Setup (Wi-Fi Simple Configuration) is to simplify the security setup and management of Wi-Fi networks. Ralink STA as an Enrollee or external Registrar supports the configuration setup using PIN configuration method or PBC configuration method through an internal or external Registrar.



WPS AP List – Display the information of surrounding APs with WPS IE from last scan result. List information includes SSID, BSSID, Channel, ID (Device Password ID), Security-Enabled.

Rescan – Issue a rescan command to wireless NIC to update information on surrounding wireless network.

Information – Display the information about WPS IE on the selected network. List information includes Authentication Type, Encryption Type, Config Methods, Device Password ID, Selected Registrar, State, Version, AP Setup Locked, UUID-E and RF Bands. Details can be found in **Detailed network information** section.

PIN Code – 8-digit numbers. It is required to enter PIN Code into Registrar using PIN method. When STA is Enrollee, you can use **Renew** button to re-generate new PIN Code.

Config Mode – Our station role-playing as an **Enrollee** or an external **Registrar**.

WPS Profile List – Display all of credentials got from the Registrar. List information includes SSID, MAC Address, Authentication and Encryption Type. If STA Enrollee, credentials are created as soon as each WPS success. If STA Registrar, RaUI creates a new credential with WPA2-PSK/AES/64Hex-Key and doesn't change until next switching to STA Registrar.

Detail – Displays Credential information in secondary pane.

Connect – Command to connect to the selected network inside credentials. The active selected credential is as like as the active selected Profile.

Rotate – Command to rotate to connect to the next network inside credentials.

Disconnect – Stop WPS action and disconnect this active link. And then select the last profile at the Profile Page of RaUI if exist. If there is an empty profile page, the driver will select any non-security AP.

Export Profile – Export all credentials to Profile.

Delete – Delete an existing credential. And then select the next credential if exist. If there is an empty credential, the driver will select any non-security AP.

PIN – Start to add to Registrar using PIN configuration method. If STA Registrar, remember that enter PIN Code read from your Enrollee before starting PIN.

PBC – Start to add to AP using PBC configuration method.

Caution: When you click **PIN** or **PBC**, please don't do any rescan within two-minute connection. If you want to abort this setup within the interval, restart **PIN/PBC** or press **Disconnect** to stop WPS action.

WPS associate IE – Send the association request with WPS IE during WPS setup. It is optional for STA.

WPS probe IE – Send the probe request with WPS IE during WPS setup. It is optional for STA.

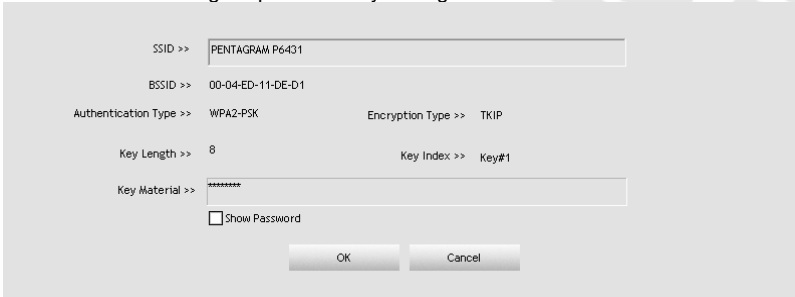
Progress Bar – Display rate of progress from Start to Connected status.

Status Bar – Display currently WPS Status.

Automatically select the AP – Start to add to AP by using to select the AP automatically in PIN method.

Credential information

Modification of these settings is possible only in Registrar mode.



SSID >> PENTAGRAM P6431

BSSID >> 00-04-ED-11-DE-D1

Authentication Type >> WPA2-PSK Encryption Type >> TKIP

Key Length >> 8 Key Index >> Key#1

Key Material >> *****

Show Password

OK Cancel

SSID – Network SSID in credential.

BSSID – Network BSSID in credential.

Authentication Type – Authentication used by network in credential.

Encryption Type – Encryption used by network in credential.

Key Length – Encryption key length.

Key Index – Encryption key index.

Key Material – Encryption key.

Show Password – Select this box if you do not want key characters to be replaced with asterisks.

OK – Closes credential information and saves settings.

Cancel – Closes credential information without saving settings.

Radio On/Off Tab

Click this Tab to enable or disable radio transmission. Green icon – RF ON, red icon – RF off.

About Tab

The About Tab contains driver, application and network adapter information.



RaConfig Version – Shows the version of the RaConfig application.

Driver Version – Shows the current driver version.

Date – Shows the application/driver release date.

EEPROM Version – Shows the current EEPROM revision.

Firmware Version – Shows the current firmware revision.

Phy_Address – Shows the adapter's physical address (MAC).

Help Tab

Click this Tab to display help file.

Troubleshooting

This section describes methods that can be used to solve problems, which may appear during the installation and operation of the wireless network adapter. Please read the description below for troubleshooting.

The application does not detect the wireless network adapter.

- Make sure the adapter has been installed correctly.
- Make sure drivers and the application have been installed correctly, and are compatible with your hardware.

Cannot connect to a wireless network.

- Make sure the access device (access point, router, etc.) is in range.
- Make sure connection settings (e.g. SSID or authentication settings) are configured correctly.
- Make sure that no equipment which may cause radio frequency interference is located in the vicinity. Equipment such as mobile phones, microwave ovens, etc. may degrade wireless connection quality.

If problems which are not addressed in this section occur, please look for a solution at www.pentagram.eu or contact an authorized PENTAGRAM service dealer.

