

## **Security tips for T-KD 318 W 2 port & 4 port MTNL wireless routers**

Dear Customer,

Thank you for choosing wireless router from MTNL, which provides Internet Access from your home or office forgetting the problem of cables. But please remember that before using the wireless, ensure that your wireless network is completely protected so that no one from outside can access your router and get into Internet. This guide provides you simple steps to secure your wireless router

### **Securing Ways**

There are 3 ways to protect your router. These are independent protection ways so that it is always better to use all three.

- I. Disabling SSID Broadcast
- II. Secured Access through data encryption
- III. Restricted Access based on MAC Address

#### **I. Disable SSID**

The SSID is a unique name to identify the ADSL Router in the wireless LAN. If SSID is enabled, then anyone will get this SSID information through passive scanning from his PC/Laptop. So please disable this SSID broadcast so that SSID can not be accessed through passive scanning. One has to manually put this SSID if he wants to access the router.

For this, Open the router homepage <http://192.168.1.1>

go to **Interface Setup --> Wireless**

Click **Access Point 'Activated'**

Put your SSID as you wish (Please put such SSID which can not be easily guessed by anyone)

Click **Broadcast SSID** option **No**



Interface

- Quick Start
  - Interface Setup
  - Advanced Setup
  - Access Management
  - Maintenance
  - Status
  - Help
- Internet | LAN | Wireless

Wireless LAN

Access Point :  Activated  Deactivated

SSID : myname

Broadcast SSID :  Yes  No

Channel ID : Channel06 2437MHz

Authentication Type : WPA2-PSK

WPA-PSK

Encryption : AES

Pre-Shared Key : passpass (8-64 characters)

Advanced Setting

Beacon Interval : 100 (range: 20~1000)

RTS/CTS Threshold : 2347 (range: 1500~2347)

Fragmentation Threshold : 2346 (range: 256~2346, even numbers only)

DTIM : 3 (range: 1~255)

802.11 b/g : 802.11b-g

Wireless MAC Address Filter

Active :  Activated  Deactivated

Action : Allow Association the follow Wireless LAN station(s) association.

Mac Address #1 : 00:00:00:00:00:00

## **II)Secured Access through data encryption**

For secure data transmission between wireless client and router, different encryption standards are available. You can select any of the encryption standards but both sides (On wireless router and Client) this encryption standard should be the same.

For eg: WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network. Select Disable to allow all wireless computers to communicate with the access points without any data encryption. Select 64-bit WEP or 128-bit WEP to use data encryption.

Key#1~Key#4 --> The WEP keys are used to encrypt data. Both the ADSL Router and the wireless clients must use the same WEP key for data transmission. If you chose 64-bit WEP, then enter any 10 hexadecimal digits ("0-9", "A-F") preceded by 0x for each key (1-4). If you chose 128-bit WEP, then enter 26 hexadecimal digits ("0-9", "AF") preceded by 0x for each key (1-4). The values must be set up exactly the same on the Access Points as they are on the wireless client stations. The same value must be assigned to Key 1 on both the access point (your ADSL Router) and the client adapters, the same value must be assigned to Key 2 on both the access point and the client stations and so on, for all four WEP keys.

**If client supports, please use strong encryption standard WPA2-PSK (Authentication type) and Encryption AES as shown below**

http://192.168.1.1/ - Microsoft Internet Explorer provided by Wipro Limited

http://192.168.1.1/

File Edit View Favorites Tools Help

MTNL ADSL Router

**Interface** Quick Start **Interface Setup** Advanced Setup Access Management Maintenance Status Help

Internet LAN **Wireless**

**Wireless LAN**

Access Point :  Activated  Deactivated  
SSID : RT2561\_6  
Broadcast SSID :  Yes  No  
Channel ID : Channel06 2437MHz  
Authentication Type : WPA2-PSK

**WPA-PSK**

Encryption : AES  
Pre-Shared Key : mysecretkey (8~64 characters)

**Advanced Setting**

Beacon Interval : 100 (range: 20~1000)  
RTS/CTS Threshold : 2347 (range: 1500~2347)  
Fragmentation Threshold : 2346 (range: 256~2346, even numbers only)  
DTIM : 3 (range: 1~255)  
802.11 b/g : 802.11b+g

**Wireless MAC Address Filter**

Active :  Activated  Deactivated  
Action : Allow Association the follow Wireless LAN station(s) association.  
Mac Address #1 : 00:00:00:00:00:00

Done Internet 100%

### III)Restricted Access based on MAC Address

For restricting access to Wireless router (thus Internet also) can be done by putting MAC Address of NIC Cards from which access to be allowed in the wireless set up as explained below.

Open the router homepage <http://192.168.1.1>

go to **Interface Setup --> Wireless**

Under **Wireless MAC Address filter** heading , select 'Active' as **Activated**

Select 'Action' as **Allow Dissociation** and type MAC Addresses of NIC Cards from which access to be allowed.

For eg: If a PC which has an NIC card having a MAC Address 00:E0:4C:69:10:C7 has to be allowed to access the wireless router, settings should be made as shown below ..

The screenshot shows the configuration page for the MTNL ADSL Router, specifically the 'Wireless' tab under 'Interface Setup'. The 'Wireless MAC Address Filter' section is expanded, showing the following settings:

- Access Point:  Activated  Deactivated
- SSID: RT2561\_6
- Broadcast SSID:  Yes  No
- Channel ID: Channel06 2437MHz
- Authentication Type: Disabled

Under 'Advanced Setting':

- Beacon Interval: 100 (range: 20~1000)
- RTS/CTS Threshold: 2347 (range: 1500~2347)
- Fragmentation Threshold: 2346 (range: 256~2346, even numbers only)
- DTIM: 3 (range: 1~255)
- 802.11 b/g: 802.11b+g

Under 'Wireless MAC Address Filter':

- Active:  Activated  Deactivated
- Action: Allow Association (dropdown menu)
- Mac Address #1: 00:E0:4C:69:10:C7
- Mac Address #2: 00:00:00:00:00:00
- Mac Address #3: 00:00:00:00:00:00
- Mac Address #4: 00:00:00:00:00:00
- Mac Address #5: 00:00:00:00:00:00
- Mac Address #6: 00:00:00:00:00:00
- Mac Address #7: 00:00:00:00:00:00
- Mac Address #8: 00:00:00:00:00:00

Red arrows point to the 'Active' radio button, the 'Action' dropdown menu, and the first 'Mac Address' field.

**Note: After making changes, do remember to save your configuration by clicking the save button.**

