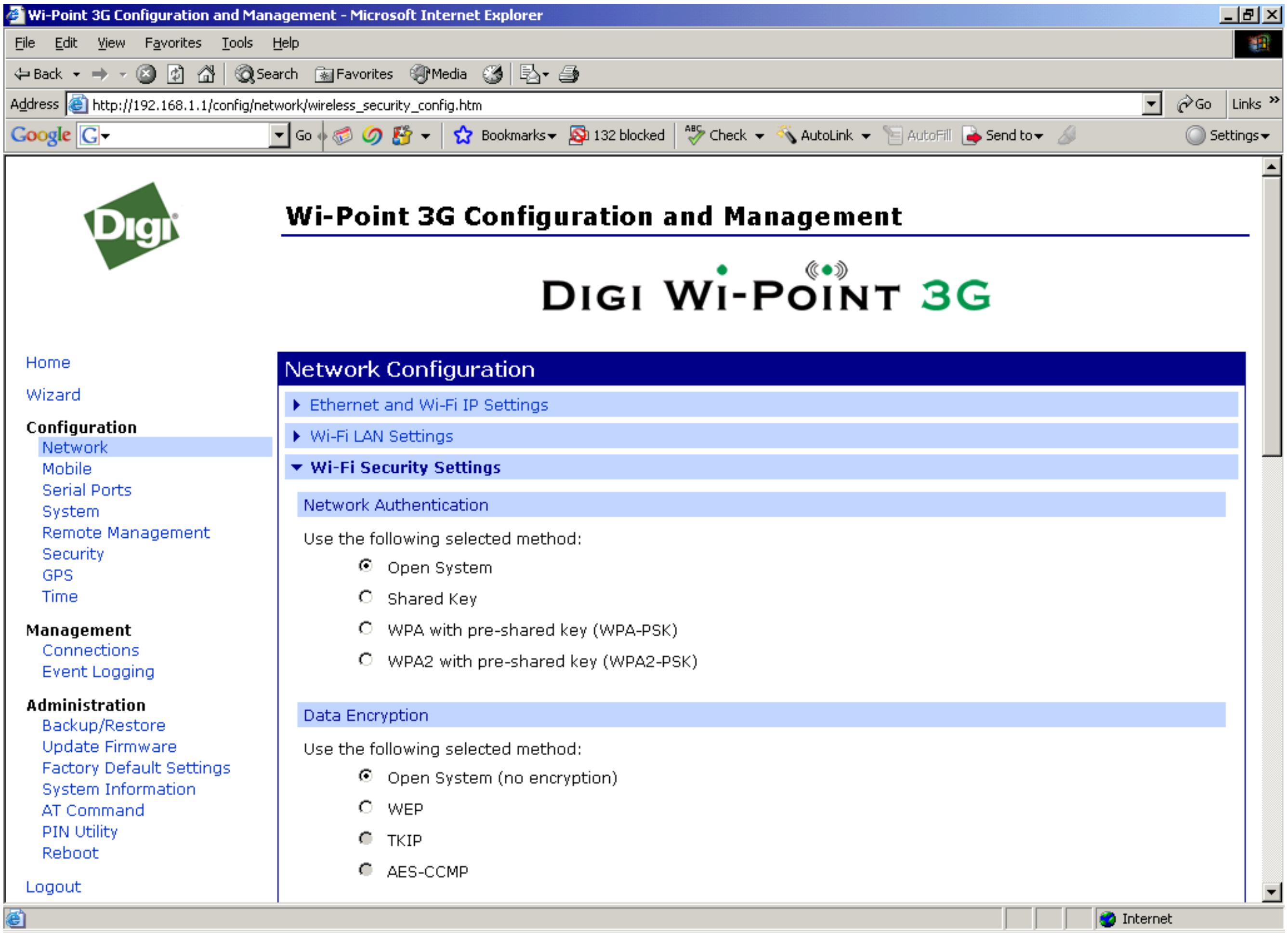
WLAN Authentication and Data Privacy

Digi Wi-Point 3G supports various Wi-Fi security options, including WEP-40/WEP-104 and WPA-PSK and WPA2-PSK. To configure WLAN security on DIGI WI-POINT 3G, you may login to its WEBUI by going to the default, the IP address of 192.168.1.1.

Open System authentication.

When using *Open System* authentication, a wireless station will be able to associate with DIGI WI-POINT 3G without authentication. When using *Open System* authentication, all wireless stations (clients) can associate with DIGI WI-POINT 3G and access the network through DIGI WI-POINT 3G if no other access control be applied. And the traffic data between the DIGI WI-POINT 3G and all of the wireless stations are unencrypted. To configure DIGI WI-POINT 3G to work in this mode, open "**Configuration →Network→Wi-Fi Security Settings** ".
Then under **Network Authentication** select **Open System** and set the **Data Encryption** to **Open system** (no encryption).


Wi-Point 3G Configuration and Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1/config/network/wireless_security_config.htm
Go Links
Google G Go Bookmarks 132 blocked Check AutoLink AutoFill Send to Settings
Digi
Wi-Point 3G Configuration and Management
DIGI WI-POINT 3G
Home
Wizard
Configuration
Network
Mobile
Serial Ports
System
Remote Management
Security
GPS
Time
Management
Connections
Event Logging
Administration
Backup/Restore
Update Firmware
Factory Default Settings
System Information
AT Command
PIN Utility
Reboot
Logout
Internet

Network Configuration

▸ Ethernet and Wi-Fi IP Settings

▸ Wi-Fi LAN Settings

▾ **Wi-Fi Security Settings**

Network Authentication

Use the following selected method:

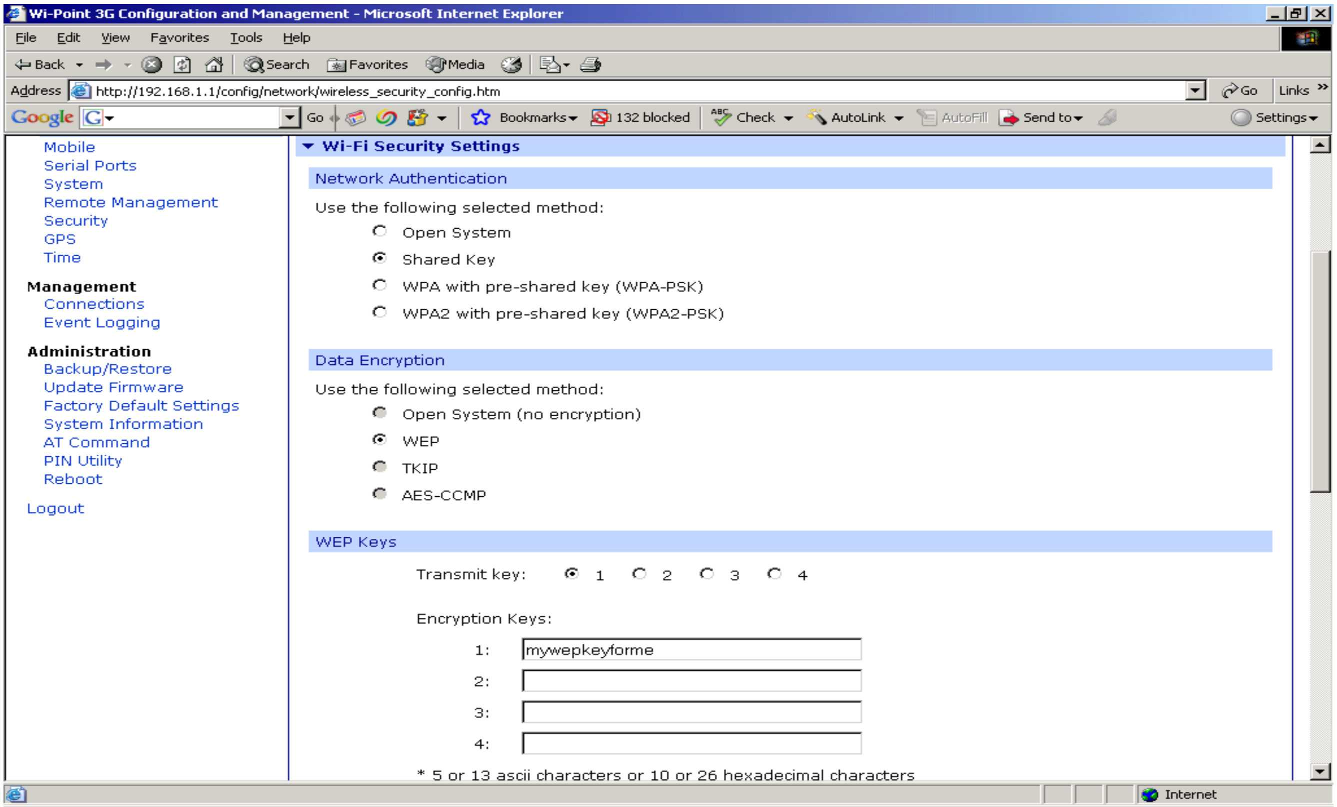
- ● Open System
- ○ Shared Key
- ○ WPA with pre-shared key (WPA-PSK)
- ○ WPA2 with pre-shared key (WPA2-PSK)

Data Encryption

Use the following selected method:

- ● Open System (no encryption)
- ○ WEP
- ○ TKIP
- ○ AES-CCMP

Shared Key authentication and WEP encryption


Wi-Point 3G Configuration and Management - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.1.1/config/network/wireless_security_config.htm
Go Links
Google Go Bookmarks 132 blocked Check AutoLink AutoFill Send to Settings
Mobile
Serial Ports
System
Remote Management
Security
GPS
Time
Management
Connections
Event Logging
Administration
Backup/Restore
Update Firmware
Factory Default Settings
System Information
AT Command
PIN Utility
Reboot
Logout
Internet

Wi-Fi Security Settings

Network Authentication

Use the following selected method:

- ○ Open System
- ● Shared Key
- ○ WPA with pre-shared key (WPA-PSK)
- ○ WPA2 with pre-shared key (WPA2-PSK)

Data Encryption

Use the following selected method:

- ○ Open System (no encryption)
- ● WEP
- ○ TKIP
- ○ AES-CCMP

WEP Keys

Transmit key: ● 1 ○ 2 ○ 3 ○ 4

Encryption Keys:

1: mywepkeyforme

2:

3:

4:

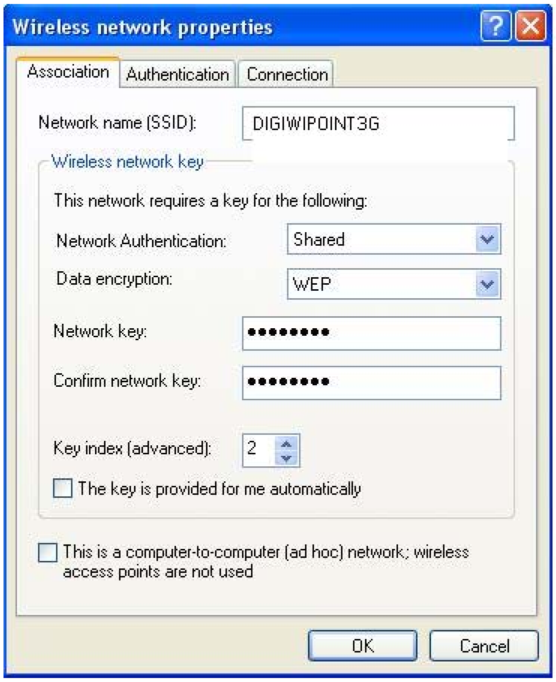
* 5 or 13 ascii characters or 10 or 26 hexadecimal characters

To prevent the unauthenticated users from accessing the network, you may use “Shared Key Authentication”, which is defined by IEEE 802.11. The IEEE 802.11 defines 4 WEP keys (with index 1 to 4) for WEP encryption and distinguishes WEP encryption to WEP-40 and WEP-104 according to the length of the keys.

Set the “*Network Authentication*” mode to “*Shared key*” to indicate DIGI WI-POINT 3G to use shared key authentication. When this option is selected, DIGI WI-POINT 3G will authenticate the wireless stations with the pre-configured WEP key. Only the wireless stations that hold the exact WEP keys can associate with DIGI WI-POINT 3G and access the network and the traffic data between them are encrypted by WEP.
“*Data Encryption*” field indicates the data encryption algorithm that DIGI WI-POINT 3G uses. There is only one option “*WEP*” available when shared key authentication is selected. All of the 4 WEP keys should be configured to either 5 ASCII characters or 10 hexadecimal (0~9, a~f) characters (WEP-40). You can also either configure 13 ASCII characters or 26 hexadecimal characters for the 4 WEP keys (WEP-104). The 4 WEP keys should be configured to the fields of “Encryption Key 1” to “Encryption *Key4*” respectively. One of the 4 keys should be specified as the default WEP key to encrypt the traffic data in the field of “Transmit key”.

Windows Wireless Client Setup

You should also configure the corresponding parameters into the wireless client. The figure below shows the configuration of a Microsoft Windows XP (with SP2) **Wireless Network Properties** dialog box with the above configuration. The “Key index” field here should match the corresponding setting in DIGIWIPOINT 3G.



Wireless network properties

Network name (SSID): DIGIWIPOINT3G

Wireless network key

This network requires a key for the following:

Network Authentication: Shared

Data encryption: WEP

Network key: ●●●●●●●●●

Confirm network key: ●●●●●●●●●

Key index (advanced): 2

□ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

There may be a little difference in appearance of the **Wireless Network Properties** dialog box between the Windows XP service pack 1 and service pack 2, but the setup is the same.

WPA-PSK

WPA (Wi-Fi Protected Access) is a specification of standard-based, interoperable security enhancements that strongly increase the level of data protection and access control for existing and future WiFi systems. WPA utilizes the TKIP (Temporal Key Integrity Protocol) to improve data encryption. The user authentication using 802.1X is called enterprise mode in WPA, which requires a backend authentication service such as RADIUS. For small enterprises that do not have RADIUS deployed and home users, WPA also provides a home mode authentication using the Pre-Shared Key (PSK).

TopGlobal DIGI WI-POINT 3G supports WPA-PSK to strengthen WLAN security. You may set the “Network Authentication” type to “WPA-PSK” on the “Wireless LAN” page. When using WPA-PSK to authenticate the users, one of three privacy methods can be applied: TKIP, AES, and TKIP+AES. When “WPA-PSK” is selected, you should also configure a passphrase in the “PSK (Only for WPA-PSK)” field. The passphrase should be 8 to 63 characters in length. Figures below show a typical settings for WPA-PSK on DIGI WI-POINT 3G and the configuration on a Windows XP.

www.digi.com