New Wi-Fi features in Windows 7

Along with a lot of advanced improvements to the Network and Sharing Center, there are also many new Wi-Fi features added in Windows 7 and Windows Server 2008 R2.

In this article we will introduce you to the new Wi-Fi features in Windows 7 like Wi-Fi Protected Setup (WPS), Wireless Router Configuration, Wireless Hosted Networks and advanced 802.1X settings. .

Along with a lot of advanced improvements to the Network and Sharing Center, there are also many new Wi-Fi features added in Windows 7 and Windows Server 2008 R2. The support of the Wi-Fi Protected Setup (WPS) feature allows administrators and users to easily set up wireless routers or access points and wireless clients. The Wireless Hosted Networks feature also allows users to create virtual Wi-Fi networks. Meanwhile, advanced 802.1X settings allow for better control of authentication settings when using the Enterprise mode of WPA or WPA2 security. In this article, we will discuss those features together.

Support for Wi-Fi Protected Setup (WPS) and configuring the wireless router

Wi-Fi Protected Setup (WPS), developed by the Wi-Fi Alliance, this feature can help users quickly and easily configure WPA / WPA2-Personal (PSK) security on routers and clients cord. Some carriers use one or two or both other WPS configuration methods: Personal Information Number (PIN) and Push Button Configuration (PBC).

The PIN method usually requires entering the wireless adapter PIN into the router's web interface. This PIN code can be printed on the adapter or displayed via client software.

The Push Button Configuration (PBC) method requires pressing a button on the wireless router and then pressing the button on the wireless adapter or computer (WPS supported) within a minute or something. Most wireless adapters do not have physical buttons, but they may still have a button on the client software if you have it installed. Similarly, wireless routers will have WPS settings available on the web-based console.

Specific WPS jobs can be very different between software and hardware vendors. However, generally WPS works like this: It will create a WPA / WPA2 password on the first WPS attempt when the wireless router still uses the factory default settings. Other clients participating in WPS attempts for the first time or after that will automatically be configured with the same WPA / WPA2 password. However, if some settings on the wireless router (such as SSID) have been changed (not the default settings) before attempting to WPS for the first time, security will not be enabled by WPS. If WPA / WPA2 security has been set up through other methods, WPS will still help configure client devices with an existing WPA / WPA2 password.

Microsoft began introducing WPS implementation in the Windows Vista operating system under the Windows Connect Now feature. The use of WPS PINs has been supported but requires you to initiate the connection via Ethernet. Later Windows Vista SP2 also added support for Push Button Configuration (PBC). However, here we will discuss the WPS feature in Windows 7.

Windows 7 supports the PBC method. The first time you connect to a wireless router with WPS, Windows 7 will prompt you to enter the security key or the most buttons, as shown in Figure 1.

Figure 1: Prompt to enter the PSK key or press WPS on the router.

If you press the WPS button on the router, the security setting will automatically be transferred to Windows 7, it will connect and a profile will be created and saved for connections to the router later.

Windows 7 also supports the PIN method, but only when setting up the router for the first time. If Windows 7 detects that the router is using the factory default settings when connected, it will prompt you to set up the router, as shown in Figure 2.

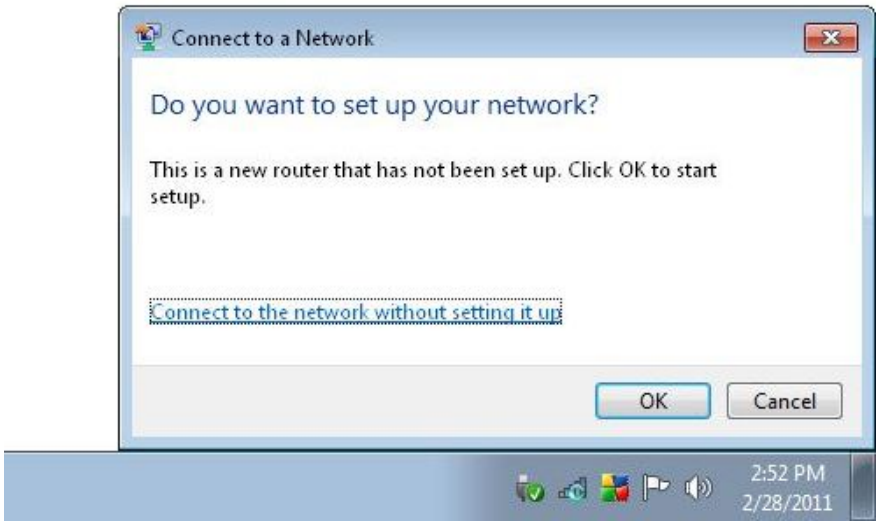

Figure 2: Reminder to set up a new wireless router

You can proceed to connect to an insecure signal or you can set up a router right in Windows 7. If you choose to set up the router, you will see a prompt for the router's PIN (see Figure 3).

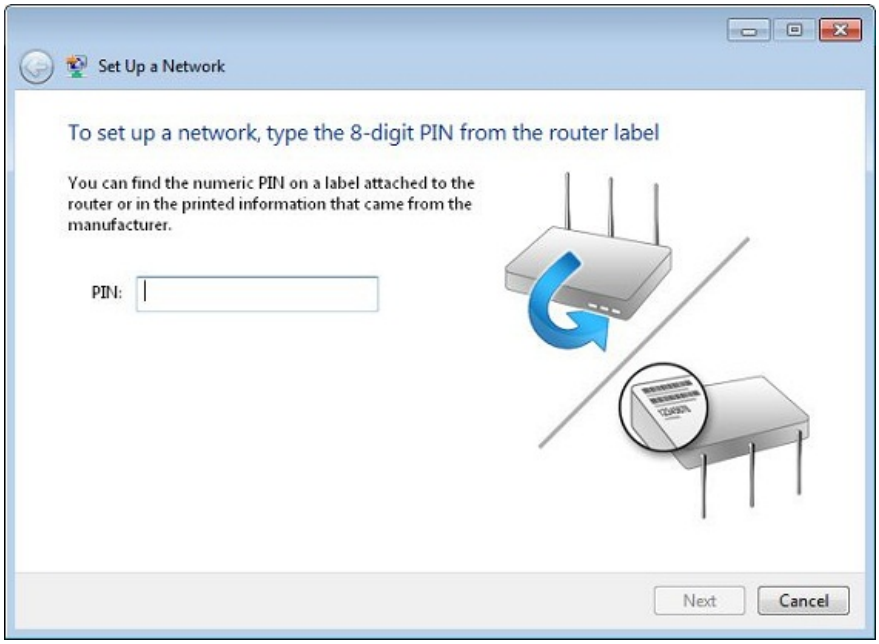

Figure 3: Enter the WPS PIN code to install the new wireless router.

You will then be prompted to enter Network Name (SSID) and customize the security settings, as shown in Figure 4.

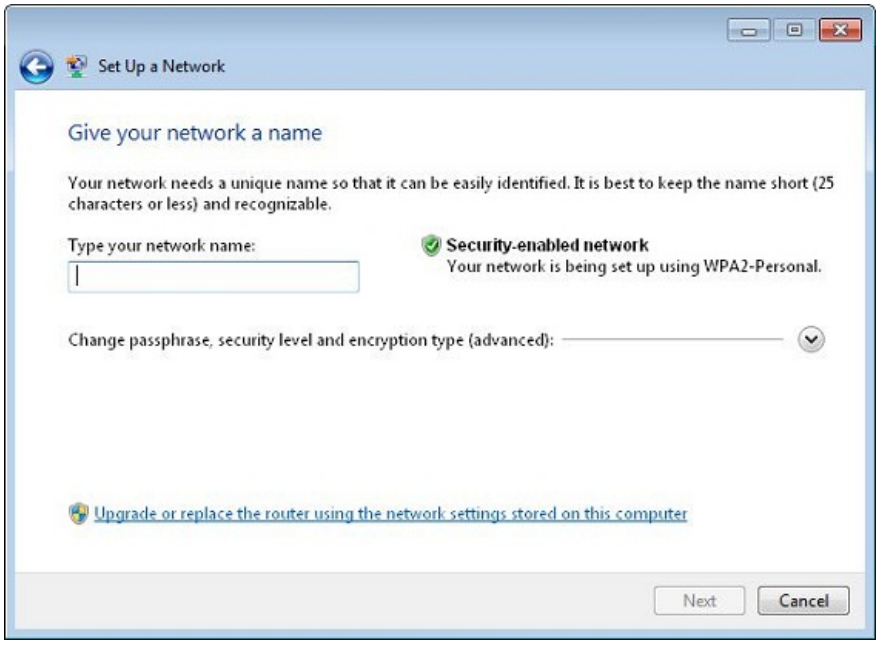

Figure 4: Enter the wireless settings.

When configuring, you will see encryption keys used for older Wi-Fi devices that do not support WPS. If you have Windows XP computers, you can even insert a USB drive to copy the configuration.

Wireless Hosted Networks feature

Part of a previous project called Virtual Wi-Fi, the Wireless Hosted Network feature allows users to create a virtual wireless router with a wireless adapter supported in Windows 7 or Windows Server 2008 R2. You can even configure a virtual wireless network while connecting to a normal wireless network using the same physical adapter.

You can use the Wireless Hosted Network to set up a temporary Wi-Fi network for the purpose of securely sharing files outside the office and home networks. It can also be used to expand or share a wired or wireless network connection. This is basically an advanced version of an ad-hoc network connection.

If the Windows 7 or Windows Server 2008 R2 operating system detects an adapter that it supports, you should see the *Microsoft Virtual Wi-Fi Miniport Adapter* in the Network Connections window, as shown in Figure 5.

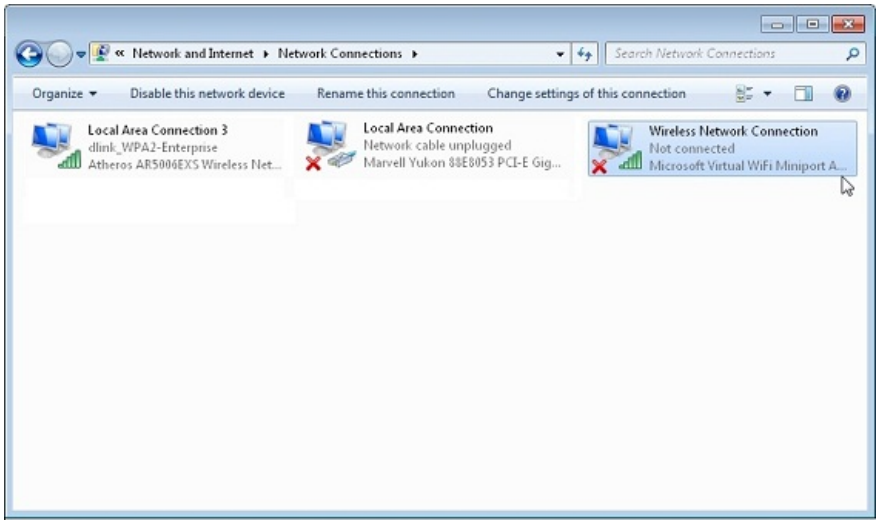

Figure 5: Virtual adapter for Wireless Hosted Networks.

To begin, make sure you want to enable Internet Connection Sharing (ICS) to have an Internet connection on the host network. In the Network Connections window, right-click on the network adapter connected to the Internet through a regular network and select Properties. Select the Sharing tab, check the *Allow other network users to connect through Internet connection this computer* , select *Hosted Network Connection* from the drop-down checkbox list and click OK.

Next, configure the host network via Command Prompt:

Netsh wlan set hostednetwork mode = cho phép ssid = YourVirtualNetworkName key = YourNetworkPassword

Launch host network:

Netsh wlan start hostednetwork

To stop the host network:

netshwlan stop hostednetwork

Figure 6 shows an example of these commands.

Figure 6: Configure, launch, stop Wireless Hosted Network

Wireless Hosted Networks are very useful and get much attention from technicians, but they are also very easy to cause security vulnerabilities on corporate networks. Employees can create a Wireless Hosted Network, thereby opening an uncontrolled wireless access to the corporate network. Although secured with WPA2 / AES encryption, all are not controlled by administrators. If you are using a Windows Server, you can prevent users from creating Wireless Hosted Networks by using Wireless Network (IEEE 802.11) Policies.

Advanced 802.1X settings

Microsoft introduced advanced settings for 802.1X authentication in Group Vista Group Policy settings. Now most of those settings are available on the Windows 7 GUI. Users can access them by clicking the Advanced Settings button on the *Security* tab in the *Wireless Network Properties* dialog box (Figure 7) and the *Authentication* tab on the dialog box. *Local Area Connection Properties* (Figure 8).

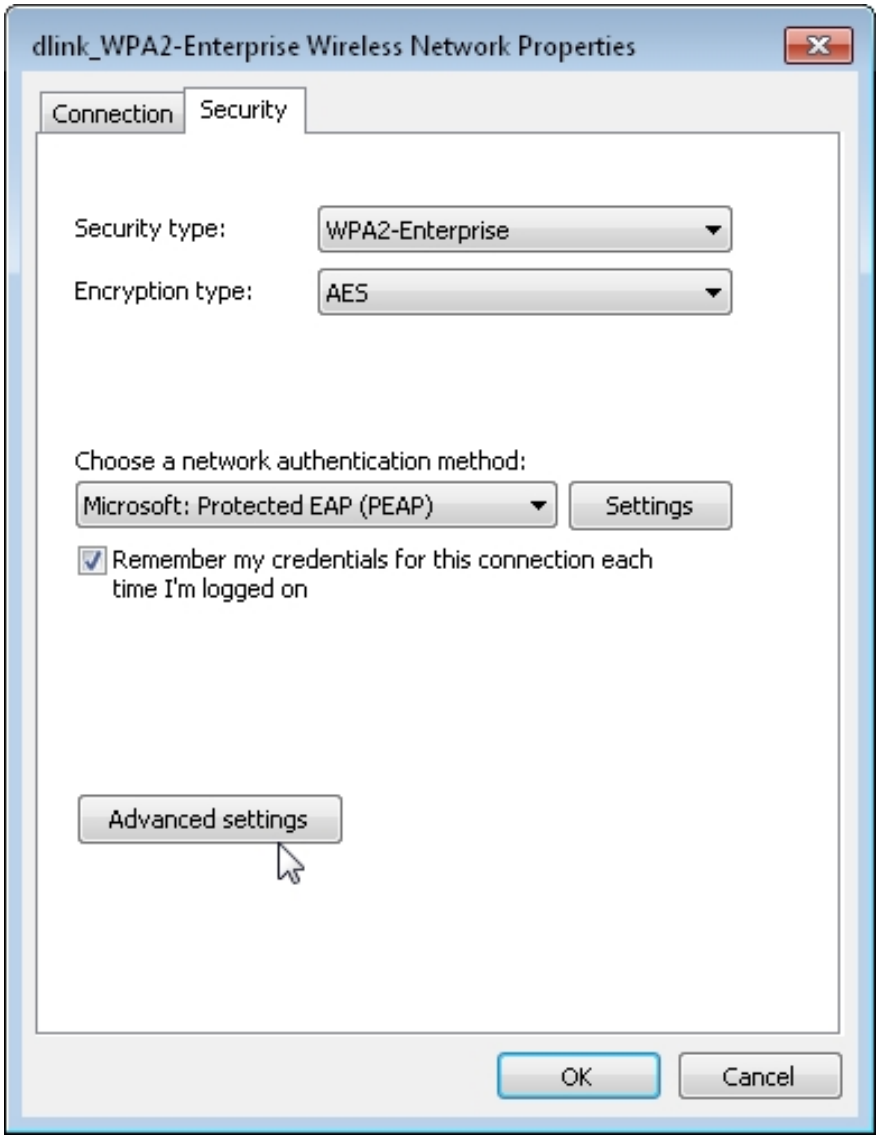

Figure 7: Tab Security on the Wireless Network Properties dialog box

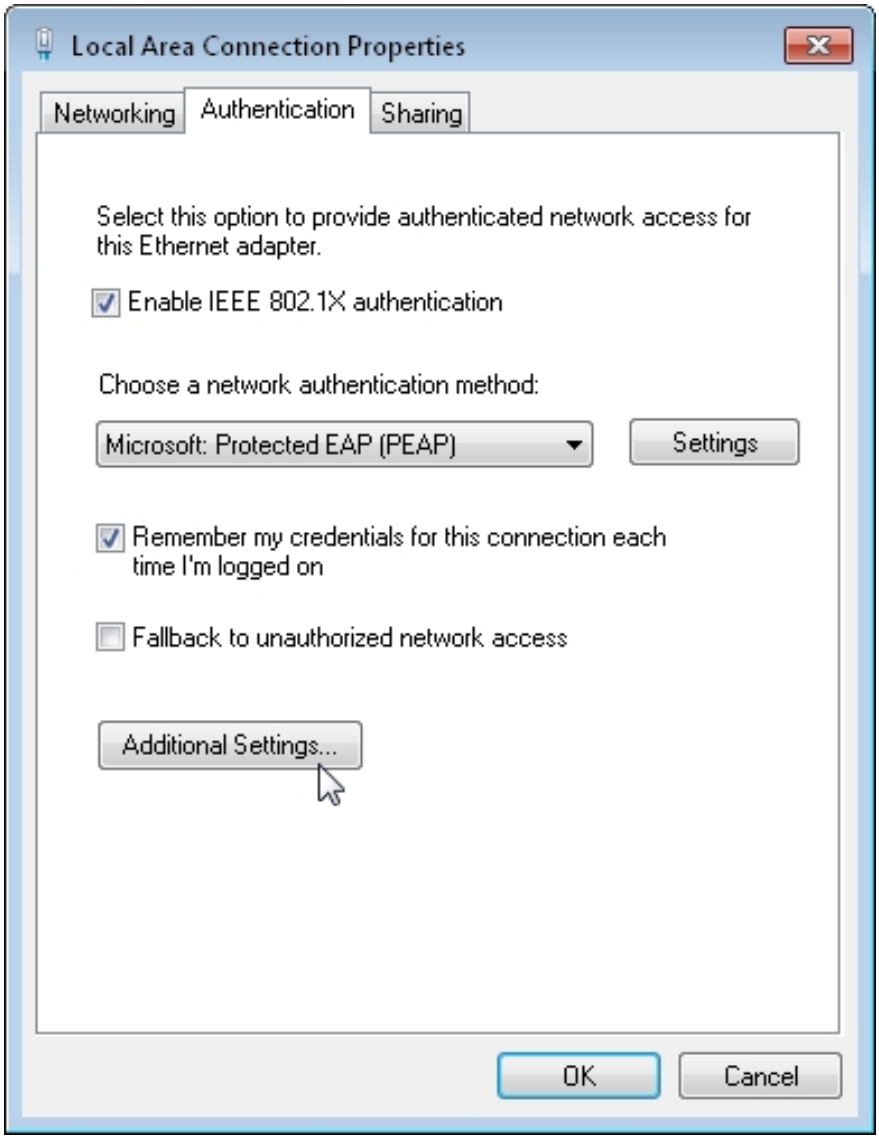

Figure 8: Authentication Tab on the Local Area Connection Properties dialog box

Figure 9 shows the Advanced Settings dialog box.

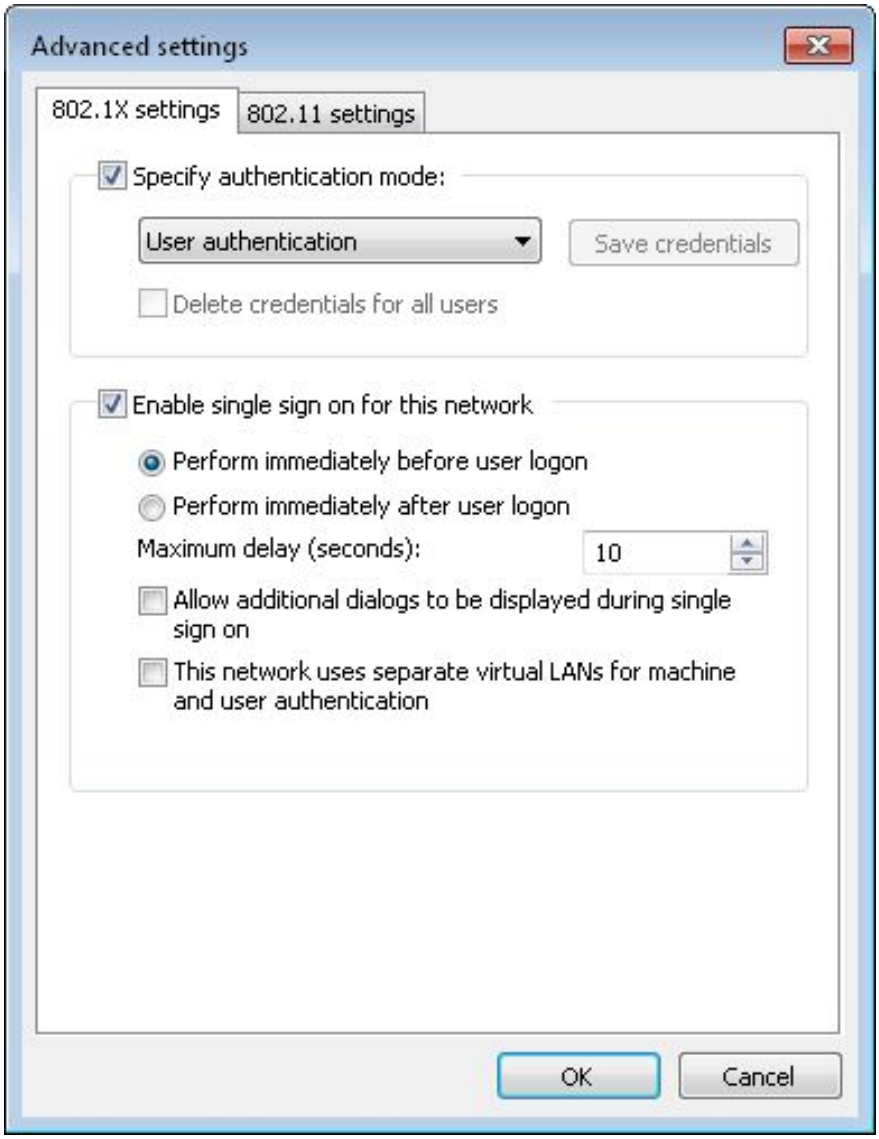

Figure 9: Advanced 802.1X settings dialog

The first part is where you can specify authentication mode: User, Computer or Guest. When using User authentication, you can click the Save Credentials button to enter the username and password. In addition, you can remove saved certificates by checking the checkbox below.

The second part of the dialog box allows you to enable and configure the single sign-on feature. If supported by the system and the network, configuring these settings will limit the need to provide separate login credentials. Windows will use Windows account certificates in 802.1X authentication.

With wireless connections, you'll find the *802.11 Settings* tab as shown in Figure 10 below.

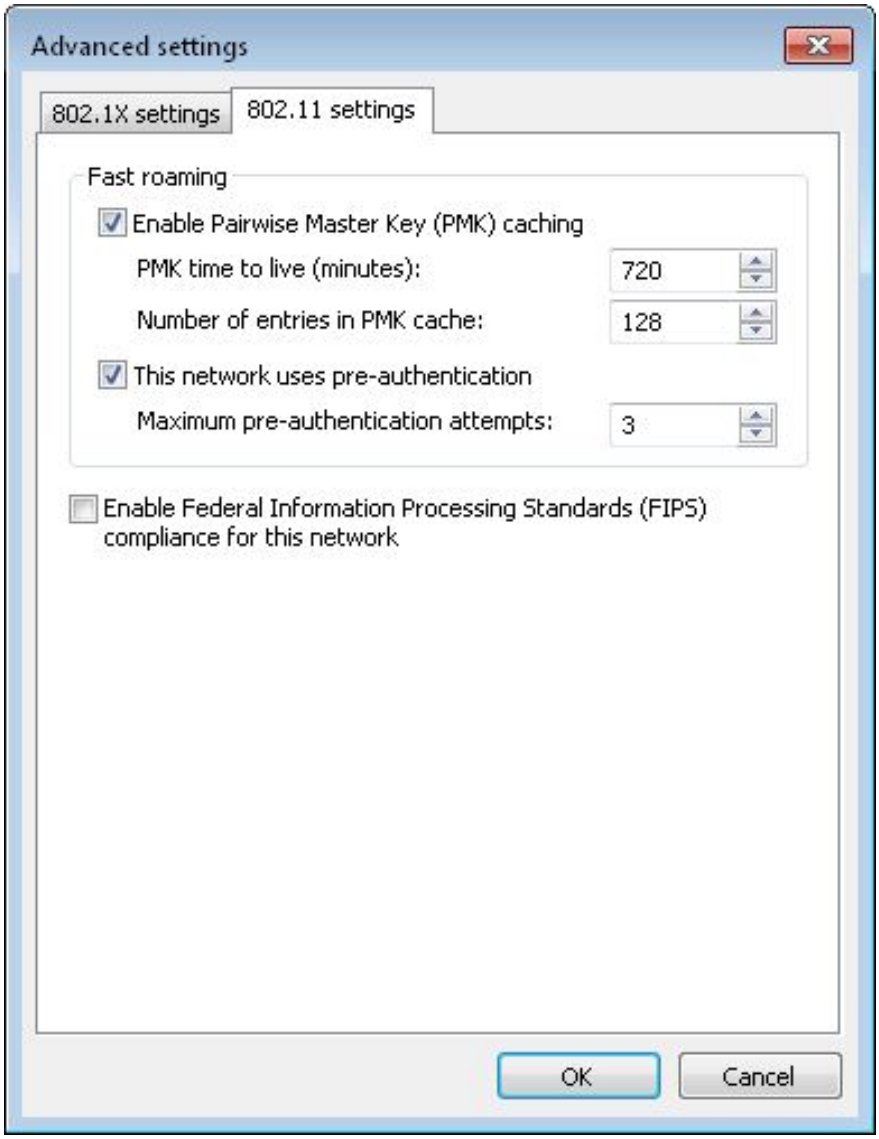

Figure 10: Advanced Settings dialog box

Here you can activate and configure the save Pairwise Master Key (PMK). This allows you to quickly roam between multiple wireless access points. When enabled and supported by APs, APs will share PMKs together so that clients do not have to perform 802.1X authentication before roaming to another AP - speeding up roaming.

When PMK caching is enabled, you can also enable and configure pre-authentication mode to prevent PMK caching from being supported by a particular AP. Pre-authentication mode eliminates the need for clients to perform full 802.1X authentication when roaming to another AP - speeding up roaming.

On this tab, you can also enable Federal Information Processing Standards (FIPS), which is used by non-US military organizations.