Wi-Fi WPA, WPA2-Enterprise

What is WPA/WPA2?

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2) are security and security certification programs developed to protect wireless computer networks by the Wi-Fi Alliance. They were developed to address the weaknesses found in the previous system, Wired Equivalent Privacy (WEP).

The WPA protocol implements many IEEE 802.11i standards. It is similar to the WEP protocol, but provides improvements in handling security keys and authorized users. For an encrypted data transfer to work, both system on the beginning and end of a data transfer must use the same encryption/decryption key. While WEP provides each authorized system with the same key, WPA uses the temporal key integrity protocol(TKIP), which employs a per-packet key and dynamically changes the 128-bit key for each packet.

WPA2 protocol includes mandatory support for CCMP (AES-based encryption mode). It provides a high level of assurance for corporate and customer Wi-Fi users that only authorized users can access their networks. There are two versions of WPA2: WPA2 Personal Edition and WPA2 Enterprise Edition. WPA2-Personal protects unauthorized network access by using a setup password. WPA2-Enterprise authenticates network users through the server.

WPA2-Enterprise

Comparing to WPA2-Personal, WPA2-Enterprise requires a RADIUS server in order to handle the task of authenticating network users access. The actual authentication process is based on the IEEE 802.1x policy and comes in several different system labeled EAP. Since each device has been authenticated before connecting, it is possible to effectively create a personal encrypted tunnel between the device and the network.

The following protocols are primarily used in WPA2-Enterprise.

- EAP-TLS: EAP-TLS is considered as the most secure EAP standard as it eliminates the risk of over-the-air credential theft. It also eliminates the password related disconnections due to password-change policies, which provides the great user experience.

- EAP-TTLS/PAP: EAP-TTLS/PAP is a credential based protocol which only needs the server to be authenticated and the user authentication is optional.

- PEAP-MSCHAPv2: PEAP-MSCHAPv2 is initially designed by Microsoft as a credential-based protocol for the Active Directory environment. Although

PEAP-MSCHAPv2 is one of the most popular methods of WPA2-Enterprise authentication, it does not need to configure server certificate authentication, making the device vulnerable to wireless certificate theft attacks. When left to end-users, device configuration errors are relatively common, which is why most organizations rely on Onboarding Software to configure devices for PEAP-MSCHAPv2.

How the WPA/WPA2-Enterprise is used in AXM-WEB2?

AXM-WEB2 communication module has a WiFi antenna which allows users to access the meter and its data through the wireless communication. The default Wi-Fi mode is Access Point(AP) mode. Under AP mode, the AXM-WEB2 will act as a wireless access point and will allow other wireless devices to connect and access the AXM-WEB2. The other mode is Station mode. Under station mode, the AXM-WEB2 will behave like a wireless client and bridge to another wireless net work that is available. AXM-WEB2 supports both WPA and WPA2-Enterprise under station mode, where users can connect using an enterprise level Wi-Fi network which is common in many colleges/universities, hospitals, etc. When attempting to connect to an enterprise level Wi-Fi network the interface will show options to connect to the network with a username and password.