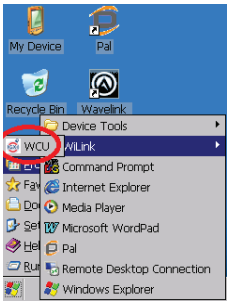
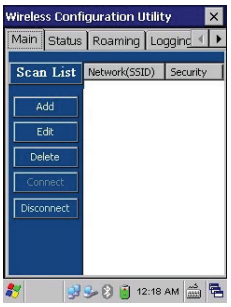
WCU (Wireless Configuration Utility)

Wireless Configuration Utility (WCU) is a user-mode application that provides an interface for configuring and operating an installed wireless network interface card (wireless adapter).

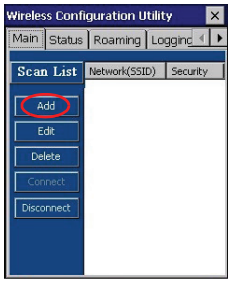
Tap **Start** > **Programs** > **WLink** > **WCU** to open the **WCU** screen:





Create a New Profile

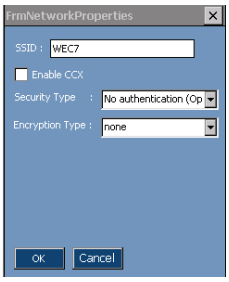
Select **Add** from the menu bar and enter information for the **SSID**, **Security Type** and **Encryption Type**:





Security Type: No Authentication (Open)

Open authentication allows any device to authenticate and then attempt to communicate with the access point. Using open authentication, any wireless device can authenticate with the access point, but the device can communicate only if its Wired Equivalent Privacy (WEP) keys match the access point's WEP keys.

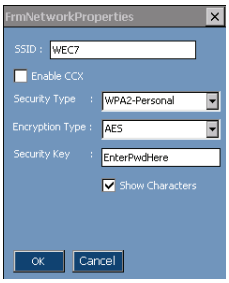


Security Type: WPA2-Personal

In case of pre-shared key (PSK) authentication, the access point sends an unencrypted challenge text string to any device that is attempting to communicate with the access point. The device that is requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate.

To create a profile with PSK authentication, follow the steps below:

1. Select the **Security Type** as **WPA2-Personal**
2. Select the **Encryption Type**
3. Enter the password in the **Security Key** field.

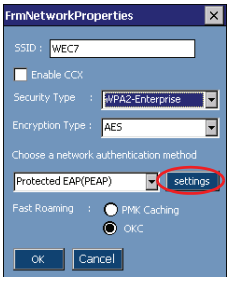


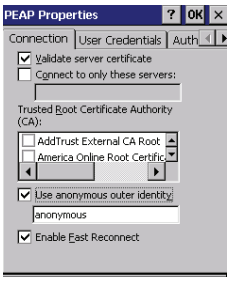
Security Type: WPA2-Enterprise

This authentication type provides the highest level of security for your wireless network. By using the Extensible Authentication Protocol (EAP) to interact with an EAP-compatible RADIUS server, the access point helps a wireless client device and the RADIUS server to perform mutual authentication and derive a dynamic unicast WEP key. The RADIUS server sends the WEP key to the access point, which uses the key for all unicast data signals that the server sends to or receives from the client. The access point also encrypts its broadcast WEP key (which is entered in the access point's WEP key slot 1) with the client's unicast key and sends it to the client.

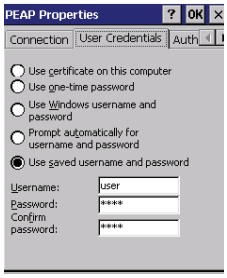
To create a profile with EAP authentication, follow the steps below:

1. Select the **Security Type** as **WPA2-Enterprise**
2. Select the **Encryption Type**
3. Tap **settings**. The **PEAP Properties** screen appears, where you can configure connection properties, source of user credentials and authentication properties (inner method) to be used:

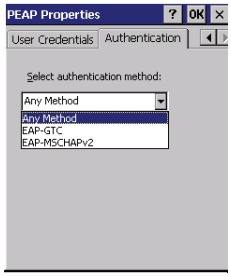




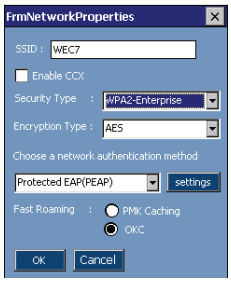
4. Tap the **User Credentials** tab to enter the EAP methods user credentials:



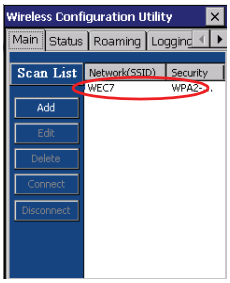
5. Tap the **Authentication** tab to select the EAP inner method:



Tap OK to complete:



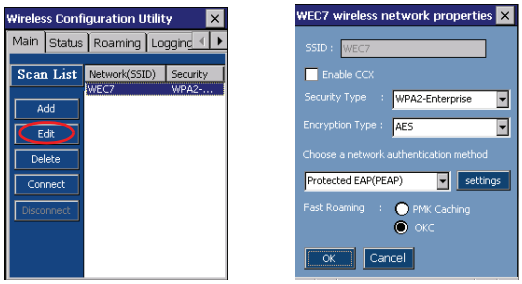
The new profile now appears in the WCU profile list:



Each EAP profile can be either "Pairwise Master Key Caching (PMK)" or Opportunistic Key Caching (OKC). By default, OKC radio button is enabled for each of WLAN profile.

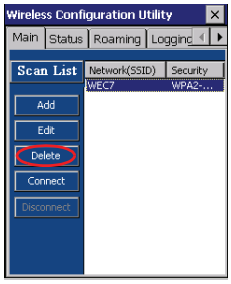
Edit a Profile

Select a profile in WCU profile list and tap **Edit** on the navigation menu bar:



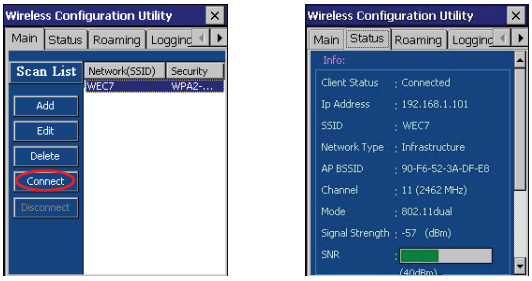
Delete a Profile

Select a profile in WCU profile list and tap **Delete** on the navigation menu bar:



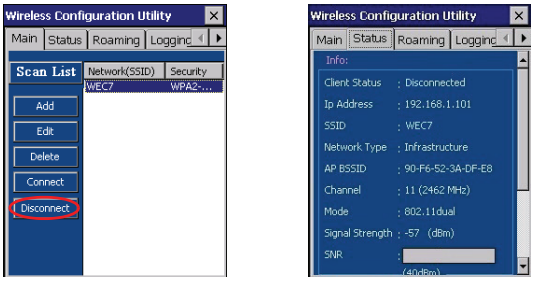
Connect to a Profile

Select a profile in WCU profile list and tap **Connect** on the navigation menu bar. Tap the **Status** tab to display the connection status:



Disconnect from a Profile

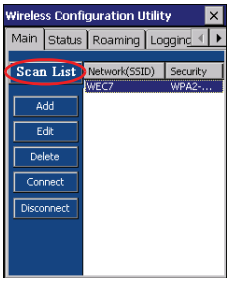
Select a connected profile in WCU profile list and tap **Disconnect** on the navigation menu bar. Tap the **Status** tab to display the connection status:

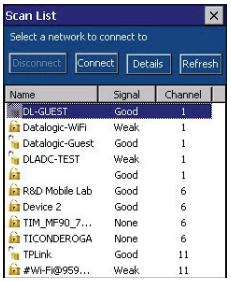


Browse Nearby Wireless Networks

The **Browse Nearby Wireless Networks** window shows the scan list entries of the WLAN driver. It is automatically refreshed periodically, without sending an explicit scan request to driver.

Tap **Scan List** in the Options menu. A window appears, that shows all the detected networks.





Connect to/Disconnect from a Network

1. Select a network from the list. Depending on whether or not the adapter network is connected to that network, the **Connect** or **Disconnect** button on the menu bar will be enabled.
2. Tap **Connect** or **Disconnect**.
3. WCU initiates the **Create New Profile** dialog box if the profile doesn't exist already.
4. Enter a profile name or leave the default name.
5. Select **Security Type** and **Encryption Type** settings for the new profile (see Create a New Profile on page 56).
6. Tap **OK** to save the profile and connect the adapter to the network, or **Cancel** to return to the current view without saving the profile.

Refresh

Tap Refresh to manually refresh the scan list. Each click on this button triggers a scan request to driver.