First Data™

FD Wi-Fi Terminals

FD100Ti/200Ti/300Ti Quick Set-Up Guide

Thanks for choosing a First Data™ Wi-Fi terminal.

You just purchased a terminal that is Wi-Fi capable — allowing you the most flexibility when using your terminal. This guide is in addition to the specific terminal guide found in the box and is intended to help you set up the Wi-Fi portion of your terminal.

What else will you need to connect through Wi-Fi?

- Wireless access point, modem or router supporting 802.11b/g/n
- Broadband Internet service

FD100Ti

FD200Ti

FD300Ti

Let’s get started...

Typical set-up time: 20–30 minutes

Where to put the FD terminal

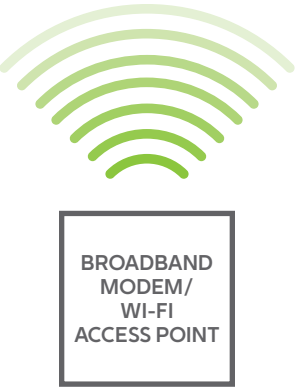
Place the terminal on a desk or tabletop. Avoid areas with direct sunlight, objects that radiate heat, excessive dust and other electrical devices that can cause excessive voltage.

Wi-Fi signal strength

There are certain environmental factors, such as concrete walls and other devices that use the same frequency. These can have an impact on the signal quality of the Wi-Fi network. If possible, place your wireless access point in the center of the area you wish to cover. Also, consider mounting Wi-Fi access points high on a wall or ceiling, avoiding any obstructions that can impede Wi-Fi signals. For best Wi-Fi performance, follow the access point manufacturer’s recommendations regarding location and positioning.

Two common Wi-Fi configurations

Option 1



Option 2

Ethernet Cable

Wireless Signal

Wi-Fi settings on the terminal

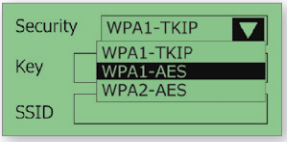
Network settings

1. On the initial screen, touch the option **SYSTEM** if it is displayed; otherwise press the "**0**" key.

2. Touch **SETUP**

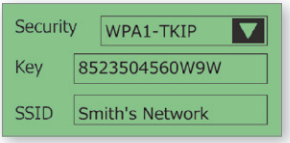
3. Touch **WIFI**

4. Touch **SECURITY** or **WIFI SECURITY**



5. Verify the security mode matches the access point's setting (i.e., WPA1-TKIP, WPA1-AES or WPA2-AES)

Note: To change, touch the drop-down arrow and select a new option.



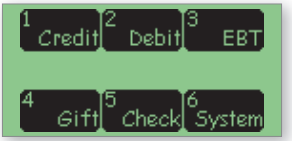
6. After setting the security mode, verify that the key and SSID match the access point's settings

(**Note:** both are case-sensitive). A USB keyboard may be connected to the terminal for entering this information.

Testing the wireless signal strength

Because environmental factors can impact the quality of wireless signals, you may want to test the strength of the signal that is reaching the terminal. You may improve your wireless signal strength by placing the Wi-Fi access point nearest to the terminal with the highest -db number (= weakest signal strength) and, as much as possible, avoiding obstructions such as walls, ceilings, appliances and fixtures.

To test the strength of the signal reaching your terminal, follow these steps.



1. On the initial screen, touch the option **SYSTEM** if it is displayed; otherwise press the "**0**" key.

2. Touch **SETUP**

3. Touch **WIFI**

4. Touch **VIEW STATUS**

Note: Signal strength "-xxdB" appears on the first line following the Wi-Fi 'mode/ connection status' ("DHCP Connect" in this example). Anything within the range of -70db to -20db indicates a strong signal strength.

You may also be able to obtain better performance by setting up the Wi-Fi access point in some of the following ways:

- Set the Wi-Fi access point to use a non-default wireless channel (such as 1, 6 or 11), and avoid any channel already being used by any other Wi-Fi network within the same coverage area.
- If using more than one access point in the Wi-Fi network, ensure that each access point is assigned a unique channel number.
- If the Wi-Fi access point has an option for "Auto Frequency," disable it.
- Set the b/g/n/mixed mode for the 802.11 (2.4 GHz range) to use either g or n only, and not mixed if possible, depending upon which terminals you have and what other devices are sharing the access point. If all your devices support n, then use only n; but if the devices only support different modes, then mixed is the only option.

Note: The First Data™ FD100^{Ti}, FD200^{Ti} and FD300^{Ti} terminals support all of 802.11b/g/n, while older FD100, FD200 and FD300 terminals support 802.11b/g. If all your Wi-Fi devices support 802.11n, then setting the access point to use n only will provide the best performance and range. However, if there is a mixture of g-capable and n-capable devices, then mixed mode must be selected.

- WPA2-AES/personal security mode can also provide better performance, and therefore it is recommended, if available and supported by all the devices in the Wi-Fi network.
- MAC filtering can also provide better performance, but such options are normally set up only by advanced Wi-Fi users.

Wi-Fi settings on the Access Point

Network settings

All Wi-Fi access points (also known as Wi-Fi modems or routers) must be configured by the network administrator with a Service Set Identifier (SSID), a wireless security mode and a security key (as well as various other optional settings).

The SSID (the name of the Wi-Fi network), the security mode and the security key (not passphrase) must be configured in the FD terminal and must exactly match the corresponding settings in the access point (including any upper- and lower-case letters).

This operation may be more easily accomplished by connecting a Windows-PC USB keyboard, which you may connect to any one of the terminal's USB connectors.

Network security

The First Data™ FD100Ti, FD200Ti and FD300Ti terminals make several types of wireless security modes available:

→ None

Not recommended (not PCI compliant)

→ WEP (Wired Equivalent Privacy)

Not recommended (not PCI compliant)

→ WPA1-TKIP

Wi-Fi Protected Access 1st generation — Temporal Key Integrity Protocol (may also be called 'WPA Personal' or WPS-PSK on some access points)

→ WPA1-AES

Wi-Fi Protected Access 1st generation — Advanced Encryption Standard

→ WPA2-AES

Wi-Fi Protected Access 2nd generation — Advanced Encryption Standard (may also be called WPA2 Personal on some Access Points)

Note: The FD100Ti, FD200Ti and FD300Ti terminals do not support WPA or WPA2 Enterprise modes.

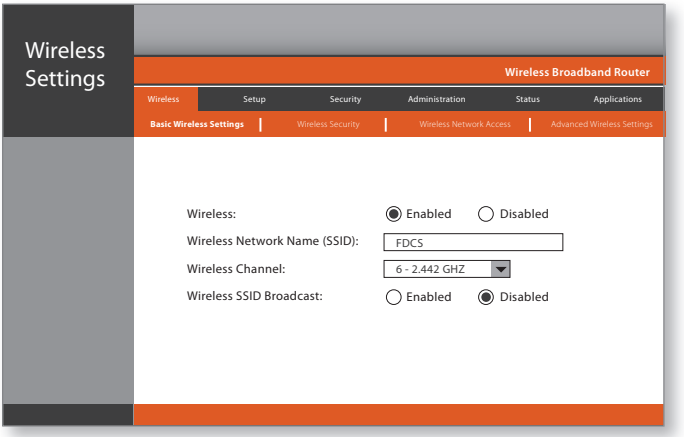
The IP address mode (DHCP or Static) set in the terminal must also match the configuration of the Wi-Fi access point. Most small, non-enterprise Wi-Fi networks use DHCP, and in this case, the FD terminal's mode should also be set to DHCP. This setting enables the terminal to automatically acquire a dynamic IP address assigned to it by the access point. Ensure that the access point's DHCP setup permits enough IP addresses to be allocated for all devices that will share the Wi-Fi network.

Certain more sophisticated Wi-Fi networks may require the FD terminal to use a Static IP address, rather than a dynamically assigned address. In this case, the network administrator must provide the IP address, subnet mask, gateway address and DNS server address that the terminal must use. In this event, the terminal's Wi-Fi setup 'Set Mode' function must be used to select the Static mode, and the 'Set IP Addr' option must be used to configure all IP parameters to match the network's requirements.

Please note

The following examples are representative of a typical network settings interface. Individual settings may differ based on the Access Point and the model being used. However, all systems will have security settings similar to the examples provided.

The screen below shows a typical example of the security settings for a wireless Access Point.



The screen below displays the option of WPA Pre-Shared Key in the Wireless Security settings of the Access Point.