

Introduction

Some implementations of RFgen as a thin client require connectivity beyond the Wi-Fi coverage area. One method of connecting is to utilize a GSM (global system for mobile [communications]) or GPRS (general packet radio service) modem connection. GSM/GPRS connections are via cellular carriers across the Internet and by themselves are not secure.

A VPN (virtual private network) tunnel provides the necessary security to allow a TCP connection from RFgen through the GSM/GPRS tower across the Internet and into the corporate network. Virtual private networks essentially provide a global, secure connection to a private network via the Internet. A VPN uses authentication and encryption to ensure that only authorized users are accessing a private network via a secure channel which allows for the safe transmission of sensitive data. Windows achieves VPN security via Point-to-Point Tunneling Protocol (PPTP) or Layer Two Tunneling Protocol (L2TP). The VPN connection across the Internet logically operates as a dedicated wide area network (WAN) link. Internet connections should use a dedicated line such as T1, Fractional T1, or Frame Relay.

This paper is intended to outline how this connection can be accomplished using the Windows Mobile 2005 VPN client to connect via the Internet to the corporate VPN endpoint. This paper will also discuss the necessary configuration settings of the RFgen client, the Connection Manager settings in Windows Mobile 2005, and the VPN endpoint requirements and settings.

Overview

RFgen requires TCP connectivity to successfully establish a connection from the RFgen Client to the Communication Server.

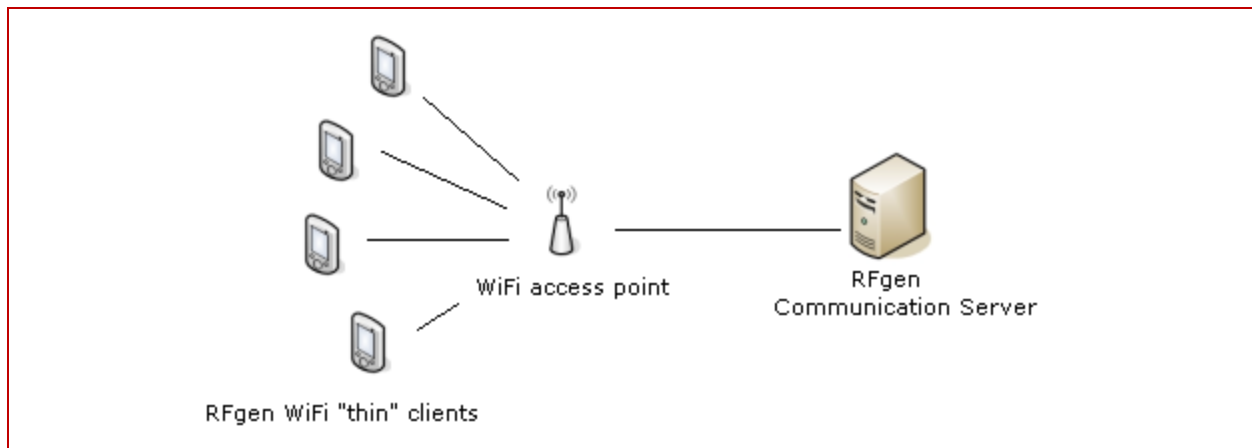


Diagram 1 – A typical connectivity scenario employing Wi-Fi technology.

Some implementations of RFgen require the “thin” client be able to connect from outside Wi-Fi coverage. This connectivity can be accomplished via a GSM/GPRS connection.

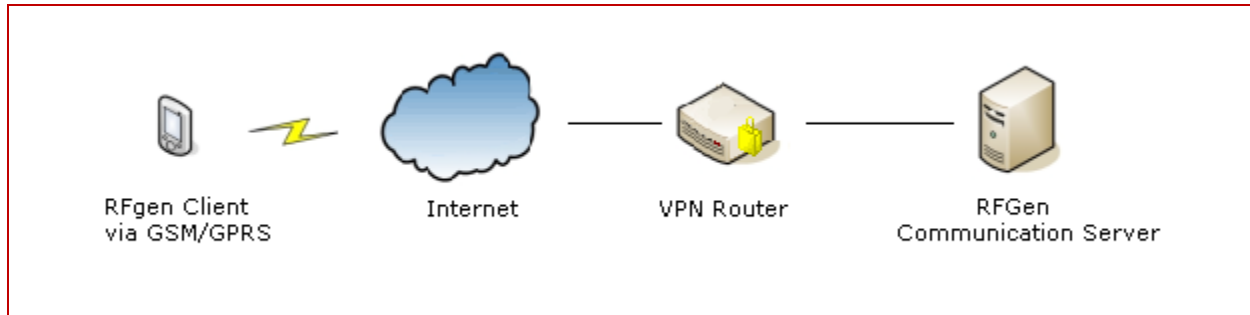


Diagram 2 – A connectivity scenario that relies upon GSM/GPRS and VPN technologies.

In other implementations a mix of Wi-Fi and GSM/GPRS connections are needed. RFgen supports this scenario as well. RFgen also supports the ability for a single device to operate using a Wi-Fi connection, travel out of the Wi-Fi coverage area and switch from Wi-Fi to GSM/GPRS coverage.

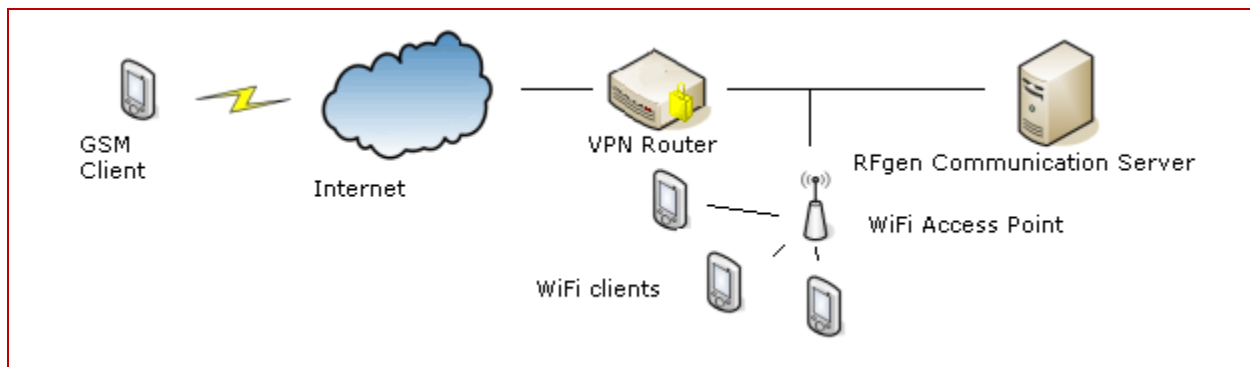


Diagram 3 – A hybrid connectivity scenario that consists of GSM/GPRS, VPN, and Wi-Fi technologies.

RFgen Client

RFgen client connectivity can be configured to connect via Wi-Fi radio or a GSM/GPRS modem. When RFgen starts, if configured for GSM/GPRS, it will attempt to establish a GSM/GPRS connection and, if configured, attempt to establish a VPN connection. If Wi-Fi is selected, then the device will attempt to communicate to the RFgen Communication Server over the established Wi-Fi connection.

To configure the RFgen client to connect via GSM/GPRS/VPN or Wi-Fi connection follow these steps:

1. Create a new text file (gprs.ini) and save it as follows: \program files\rfgence\gpris.ini
2. Add the following lines of text for the GSM/GPRS and VPN connections:

```
[GPRS]
Enabled = False
```

Name = GPRS

User =

Pwd =

[VPN]

Enabled = True

Name = My Work Network

User =

Pwd =

Enabled – when set to `True`, enables the connection; when set to `False`, disables the connection. Depending upon the version of the CE operating system, the GSM/GPRS connection may be automatically activated when attempting to connect to a VPN.

Name – the identifying name given to the connection.

User – an authorized user name that is able to utilize this connection. This setting is also dependent upon the version of the CE operating system. Some versions of the CE operating system save the user name as part of the connection configuration. This field can be utilized to save the user name for those versions that do not retain this information.

Pwd – the password of the authorized user to authenticate the connection. This setting is also dependent upon the version of the CE operating system. Some versions of the CE operating system save the password as part of the connection configuration. This field can be utilized to save the password for those versions that do not retain this information.

3. Click “Start” > “Programs” > “RFgenCFG”
4. Ensure that the “Configure” field is set to “Connection Settings”. In the “Phonebook” field, select either “WiFi” or “GSM/GPRS”, depending upon the connection type desired. “GSM/GPRS” will only appear as a valid selection if the INI file was correctly created and saved.

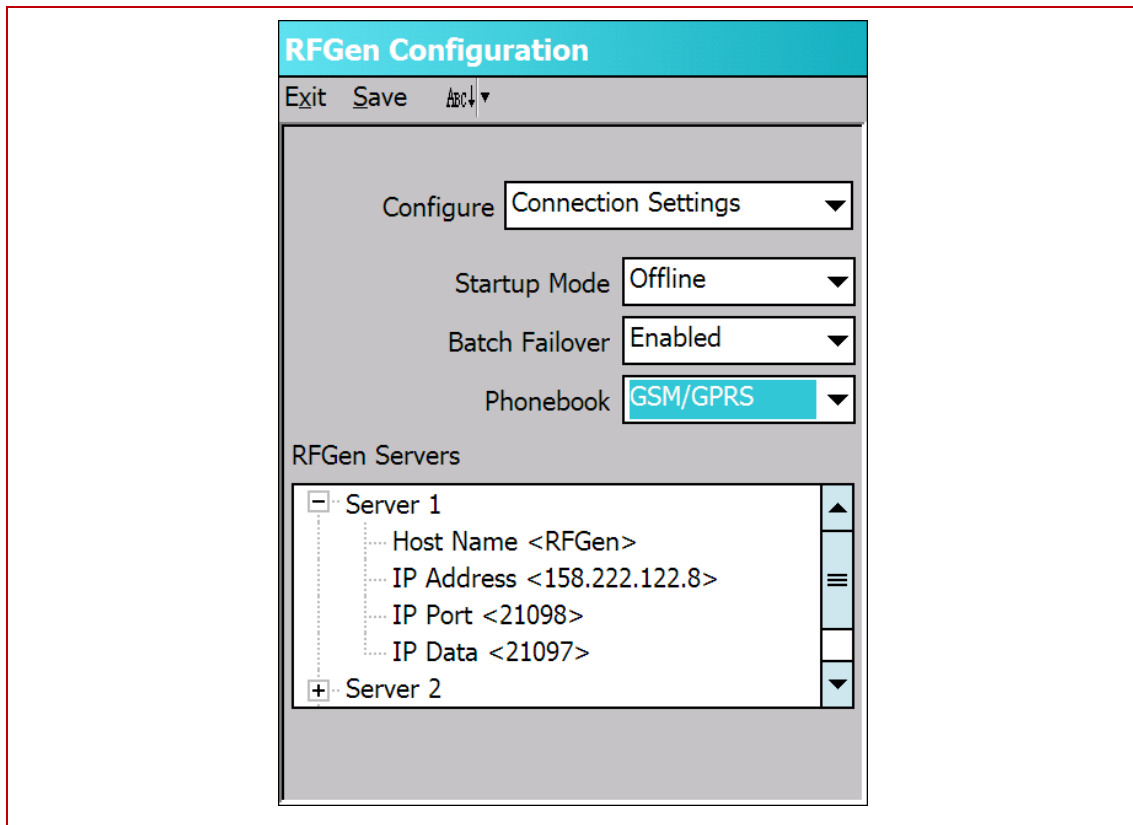


Diagram 4 – A hybrid connectivity scenario that consists of GSM/GPRS, VPN, and Wi-Fi technologies.

Windows Mobile: GSM/GPRS

If you wish to configure your Windows Mobile device for a dial-up connection you must enter proper configuration parameters. If you wish to have a VPN tunnel established, you would also need to configure this as well. The following sections explain how to properly configure a network connection as well as a VPN tunnel.

Internet Connection (Dial-Up)

When configuring a GSM/GPRS connection to the Internet you will need the modem and carrier information that your wireless carrier and/or network administrator should provide. The instructions that follow are for configuring a GSM/GPRS connection to the Internet using AT&T/Cingular as the cellular provider; your settings may differ.

To setup and configure an Internet Connection on an RFGen client, follow these steps:

1. Click “Start” > “Settings” > “Connections” and select the “Connections” entry.
2. Select “Add a new modem connection”.

3. Enter a name for the connection and select “Cellular Line (GPRS)” as the modem.
4. Click “Next”.

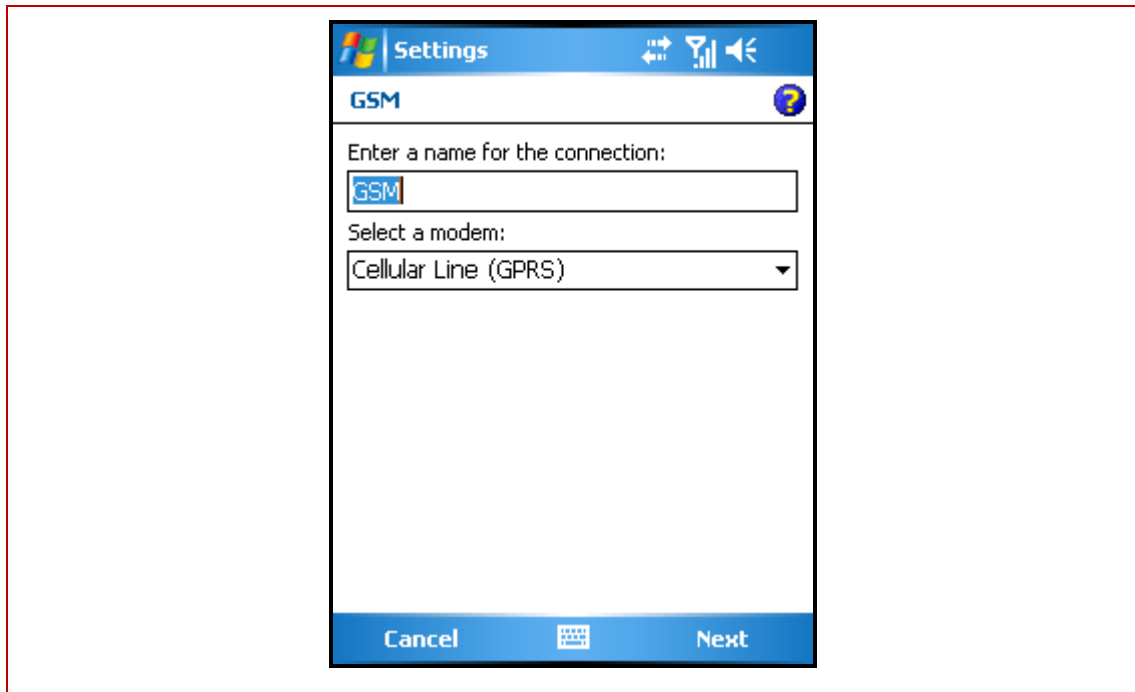


Diagram 5 – Name the connection and provide information about the modem.

5. Enter the name of the access point (provided by your cellular carrier).
6. Click “Next”

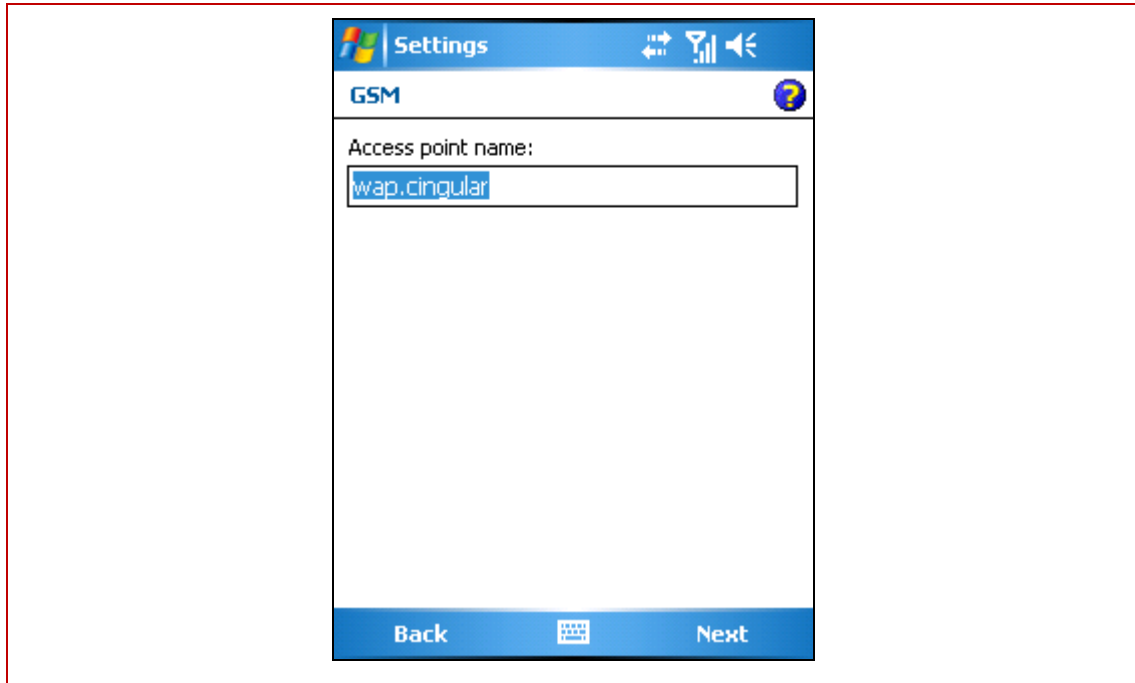


Diagram 6 – Provide a name for the access point.

7. Enter a user name, password, and domain (provided by your cellular carrier). Generally, these fields can be left blank.
8. Click the “Advanced...” button to set up IP address information. This is usually left as the default “Server Assigned”.
9. Finally, click “Finish” to complete the connection setup process.

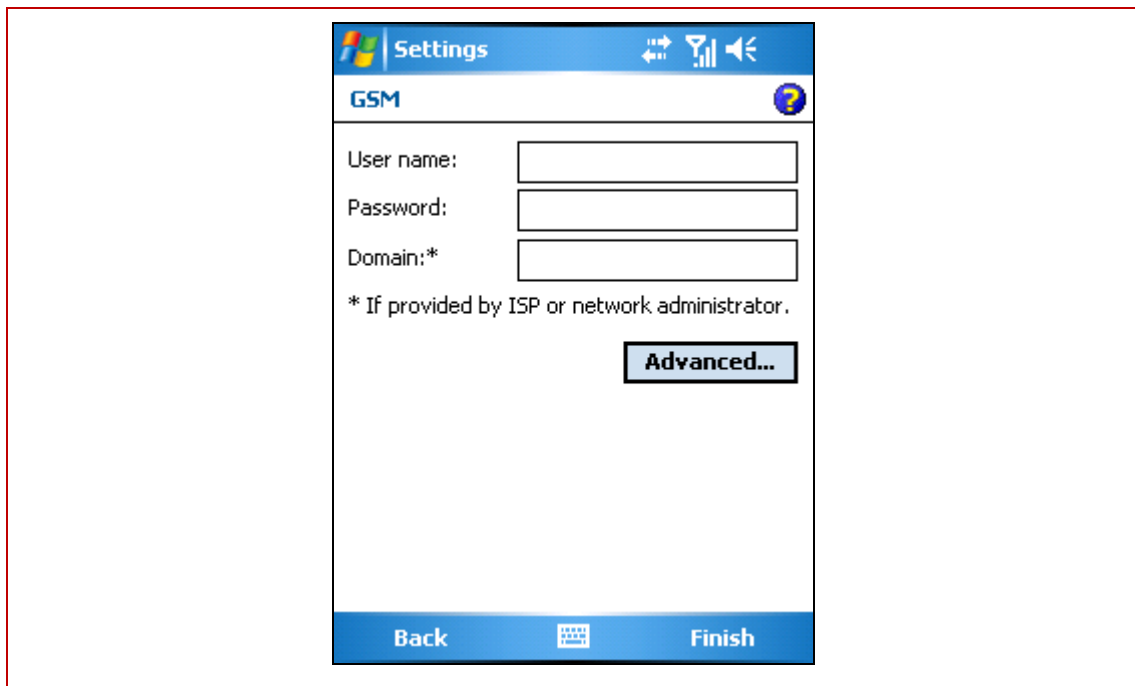


Diagram 7 – The fields user name, password, and domain can be left blank in most instances.

Windows Mobile: VPN Connection

A VPN connection is optional when establishing a connection from the RFgen client to the Communication Server. The necessity of a VPN connection is dependent upon corporate network configuration and you should, therefore, consult a network administrator to begin implementing a VPN connection. In the following example, the VPN uses the Internet Connection to tunnel through a secure data connection.

To configure setup and configure VPN Connection, follow these steps:

1. Click “Start” > “Settings” > “Connections” and select the “Connections” entry.
2. Select “Add a new VPN server connection”.
3. Enter a name for the connection, a host name or IP address, and select the VPN type.

4. Click “Next”

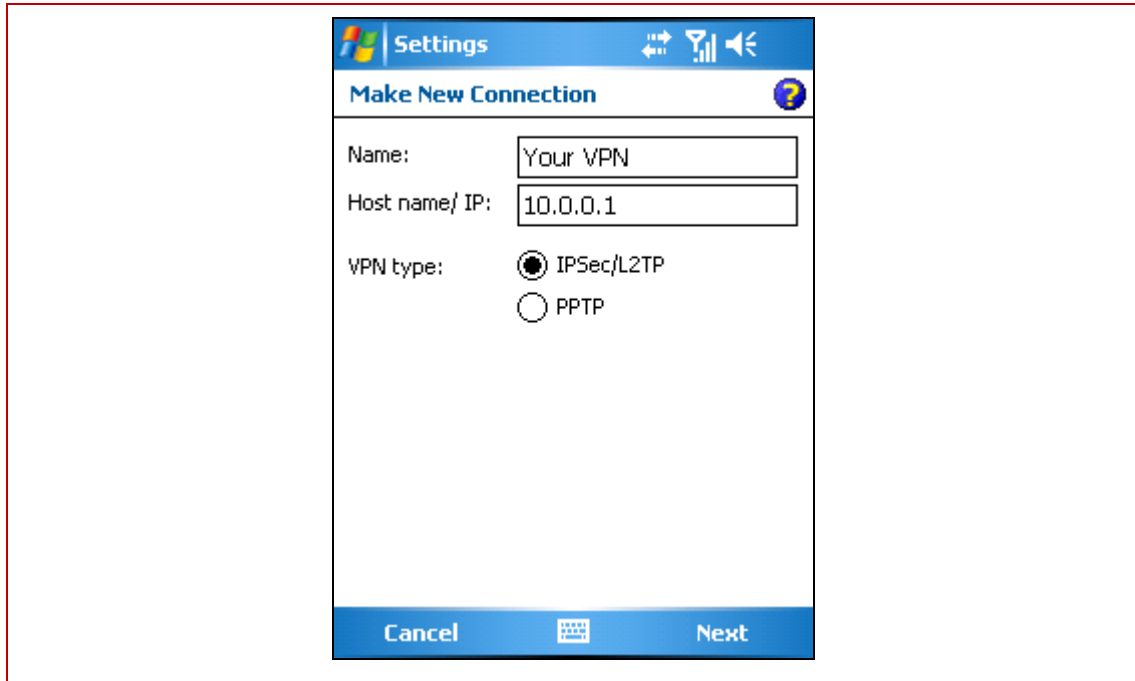


Diagram 8 – The Name the connection and provide host information along with a VPN type.

5. Provide either a certificate or a pre-shared key to authenticate the VPN tunnel. This key must match the key configured on the IPSec/L2TP or PPTP endpoint located in the corporate network.
6. Click “Next”

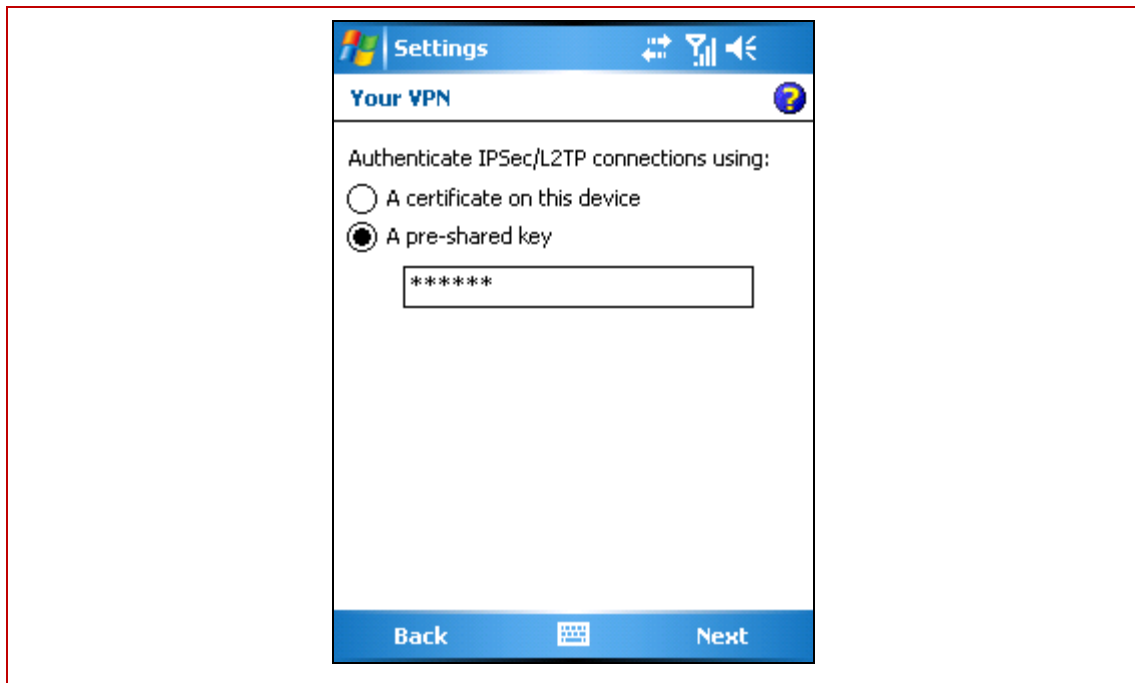


Diagram 9 – Enter authentication data.

7. If the VPN endpoint has user name and password enabled, enter the correct user name and password. Enter the domain, if it has been provided by the ISP or network administrator.
8. Click the “Advanced...” key to configure TCP settings for the VPN connection.
9. Click “Finish”.

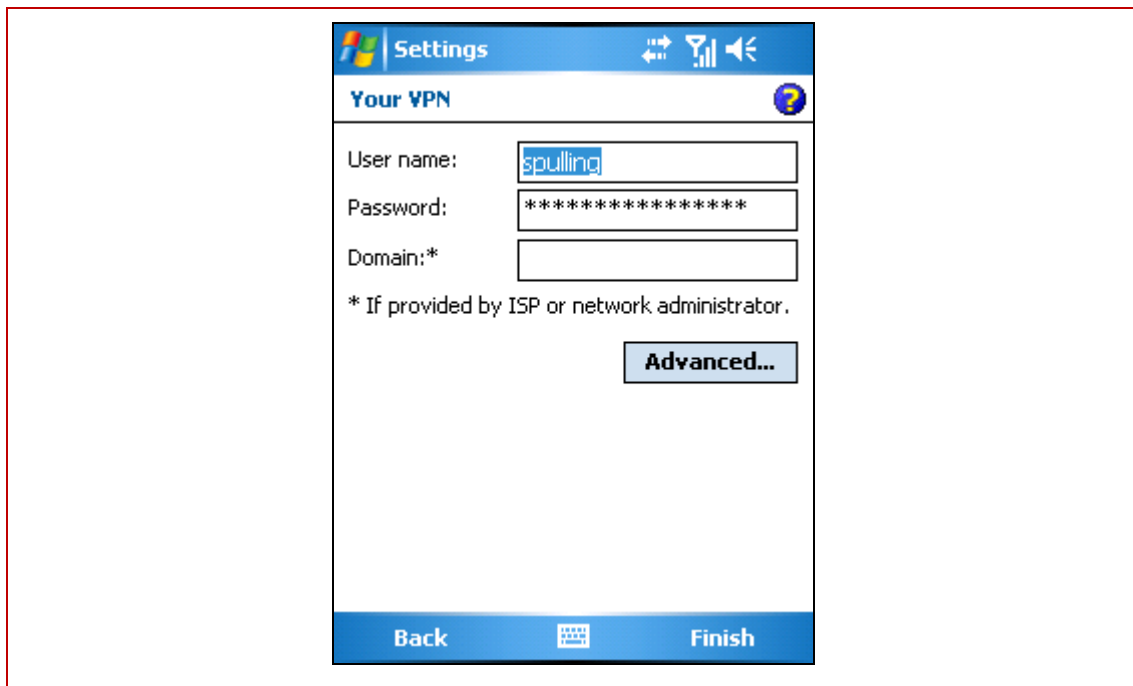


Diagram 10 – Enter authentication data.

Microsoft VPN Server: Install and Enable VPN

The VPN tunnel router endpoint must support IPSec/L2TP to connect with the Mobile VPN client. There are numerous hardware vendors that provide IPSec/L2TP hardware. Windows 2000 and Windows XP support the ability to become a VPN tunnel endpoint. This enables the computer to become a remote access server. A Windows VPN consists of a VPN server, a VPN client, a VPN connection (data encryption), and VPN tunnel (data encapsulation).

To install and enable VPN, follow these steps:

1. Confirm that both the connection to the Internet and the connection to the local area network (LAN) are correctly configured.
2. “Start” > “Control Panel” > “Administrative Tools” > “Routing and Remote Access”

3. Locate and click the server name in the tree, then “Action” > “Enable Routing and Remote Access”.
4. Click “Next”.
5. “Common Configurations” dialog box: click “Virtual private network (VPN server)”.
6. Click “Next”.
7. “Remote Client Protocols” dialog box: confirm that “TCP/IP” is included in the list, and select “Yes, all of the available protocols are on this list.”
8. Click “Next”.
9. “Internet Connection” dialog box: select the Internet connection that will connect to the Internet.
10. Click “Next”.
11. “IP Address Assignment” dialog box: select “Automatically” in order to use the DHCP server on the subnet to assign IP addresses to dial-up clients and to the server.
12. Click “Next”.
13. “Managing Multiple Remote Access Servers” dialog box: confirm that the checkbox for “No, I don’t want to set up this server to use RADIUS now” is checked.
14. Click “Next”.
15. Click “Finish”.
16. Right-click the “Ports” node and select “Properties”
17. “Ports Properties” dialog box: click the WAN miniport (PPTP) device and click “Configure”.
18. “Configure Device – WAN Miniport (PPTP)” dialog box:
 - a. Check the “Demand-Dial Routing Connections (Inbound and Outbound)” check box to enable direct user dial-up VPN to modems installed on the server or uncheck the check box to disable direct user dial-up VPN to modems installed on the server.
 - b. Enter the maximum number of simultaneous PPTP connections allowed in the “Maximum Ports” field. (This may depend upon the number of available IP addresses.)

19. Repeat steps 17 and 18 for the L2TP device.

20. Click “OK”.

Microsoft VPN Server: Configuration as a Router

For the remote access server to forward traffic properly inside a network, it must be first configured as a router with either static routes or routing protocols. This allows all of the locations within the intranet to be accessible from the remote access server.

To configure the remote access server as a router, follow these steps:

1. “Start” > “Control Panel” > “Administrative Tools” > “Routing and Remote Access”
2. Right-click the server name, and select “Properties”.
3. In the “General” tab, select “Enable this Computer as a Router”
4. Select either “Local area network (LAN) routing only” or “LAN and demand-dial routing”
5. Click “OK”

Microsoft VPN Server: PPTP Port Configuration

As a precursor, confirm the number of PPTP ports that will be necessary before performing this procedure.

To configure PPTP ports, follow these steps:

1. “Start” > “Control Panel” > “Administrative Tools” > “Routing and Remote Access”
2. Expand “Routing and Remote Access”
3. Expand the server name
4. Select “Ports”
5. Right-click “Ports” and select “Properties:
6. “Ports Properties” dialog box: select “WAN Miniport (PPTP)” and click “Configure”

7. “Configure Device” dialog box: select the maximum number of ports for the device and select the options to specify whether the device accepts incoming connections only, or both incoming and outgoing connections.

Microsoft VPN Server: Managing Addresses and Name Servers

The VPN server must have IP addresses available in order to assign them to the VPN server’s virtual interface and to VPN clients during the IP Control Protocol (IPCP) negotiation phase of the connection process. The IP address assigned to the VPN client is assigned to the virtual interface of the VPN client.

For Windows 2000 based VPN servers, the IP addresses assigned to VPN clients are obtained through DHCP, by default. A static IP address pool can also be configured. The VPN server must also be configured with the name resolution servers, typically DNS and WINS server addresses, to assign to the VPN client during IPCP negotiation.

Microsoft VPN Server: Managing Access

Configure the dial-in properties on user accounts and remote access policies to manage access for dial-up networking and VPN connections.

Note: By default, users are denied access to dial-up.

Access by User Account

For managing remote access by user basis, click “Allow Access” on the “Dial-In” tab of the user’s “Properties” dialog box for those user accounts that are allowed to create VPN connections. If the VPN server is allowing only VPN connections, delete the default remote access policy “Allow Access If Dial-In Permission Is Enabled”. Then, create a new remote access with a descriptive name. For more information consult the Windows Help.

Caution: After the default policy has been deleted, any dial-up client that does not match at least one of the existing policy configurations will be denied access.

If the VPN server is also allowing dial-up remote access services, do not delete the default policy, but move it so that it is the last policy to be evaluated.

Access by Group Membership

To manage remote access on a group basis, select the “Control access through remote access policy” radio button option on all user accounts by using the Active Directory Users and Computer Console in Administrator Tools or MMC snap-in. Create a Windows group with members that are allowed to create VPN connections. If the VPN server allows only VPN connections, delete the default remote access policy “Allow Access If Dial-In Permission Is Enabled”. Next, create a new remote access policy with a descriptive name such as “VPN Access If Member of VPN-Allowed Group”, and assign the Windows group to the policy.



5049 R.J. Mathews Parkway #100
El Dorado Hills, California 95762
(916) 939-4065 | www.rfgen.com

Technical Memo

June 2, 2009

Re: Windows Mobile VPN Connectivity

If the VPN server is also allowing dial-up remote access services, do not delete the default policy, but move it so that it is the last policy to be evaluated.