

User's Guide for Mergic™ VPN

Version 1.1

Copyright Notice

Copyright © 2003 Mergic, Inc. All rights reserved. No part of this publication may be reproduced by any means, electronic or mechanical, for any purpose, without the express written permission of Mergic™, 23551 NE 29th St., Sammamish, Washington, 98074-5447, U.S.A.

Trademarks

Mergic, and the Mergic logo are trademarks or registered trademarks of Mergic, Inc.

HotSync and Palm OS are registered trademarks of PalmSource, Inc.

Handspring and Treo are trademarks or registered trademarks of PalmOne, Inc.

Microsoft, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe, Acrobat and Reader are trademarks of Adobe Systems Incorporated or its subsidiaries and may be registered in certain jurisdictions.

Other brand and product names are trademarks or registered trademarks of their respective holders.

Disclaimer and Limitation of Liability

The entire risk of the use or the result of the use of this documentation remains with the user.

Important: Please read the End User License Agreement with this product before using the accompanying software program(s). Using any part of the software indicates that you accept the terms of the End User Software License Agreement.

Contents

Introduction.....	4
Features.....	4
System Requirements.....	5
Installation.....	6
Uninstalling Mergic VPN from a Palm OS device.....	6
Configuration.....	7
Starting Mergic VPN for the first time.....	7
Main VPN configuration.....	8
Naming a VPN configuration.....	8
Entering a user name.....	8
Saving a password.....	8
Auto Connect configuration.....	9
Entering a VPN server name or address.....	11
Changing detailed VPN configuration information.....	12
Changing the Connect Via setting (Palm OS 3.3 – 4.1, except Treo).....	12
Changing the Idle Timeout setting.....	13
Changing Show Status In Command Bar setting.....	14
Changing the Send All To Private Net setting.....	15
Changing the DNS Suffix for Private Net setting.....	15
Modifying advanced VPN configuration information.....	17
Setting the Encryption Required checkbox.....	17
Defining primary and secondary DNS servers for the private network.....	18
Defining the IP address to be used on the private network.....	19
Multiple VPN configurations.....	20
Creating a new VPN configuration.....	20
Duplicating a VPN configuration.....	20
Selecting the current VPN configuration.....	21
Deleting the current VPN configuration.....	21
Using Mergic VPN.....	22
Manually establishing a VPN connection.....	22
Manually disconnecting.....	22
Using Auto Connect.....	23
Determining whether or not a VPN connection is active.....	24
Password Prompting.....	25
Troubleshooting.....	26
Using Mergic VPN's log.....	26
Opening the log.....	26
Saving the log to Memo Pad.....	26
Backing up the log.....	27
Customer Support.....	27
Appendix A: Modifying an existing Network Service for VPN (Palm OS 3.3 – 4.1, except Treo).....	28
Step 1 – Create an MVPN connection configuration.....	28
Step 2 – Modify the network service.....	29
Appendix B: Determining your Internet connection configuration (Palm OS 3.3 - 4.1, except Treo).....	30
Appendix C: Determining the correct Connect Via setting (Palm OS 3.3 - 4.1, except Treo).....	31
Index.....	33

Introduction

Mergic VPN is a Virtual Private Network (VPN) client for Palm OS® devices. A VPN client connects to a VPN server using a public network, such as the Internet, to provide secure network access to a private network, such as your corporate or home Local Area Network (LAN). This means that through a connection to the Internet¹ you can access resources on your LAN just as if you were directly connected to it.

For a VPN connection to work, the VPN client and server must agree on how to communicate. In this context communicating means a common understanding of many things such as how to manage the connection, how to identify that you are authorized to connect to the private network and how to keep the data that's passed through the Internet private. For computers, the common understanding of how to communicate is called a protocol. Just as there are many different languages used for human communication there are several different protocols used for VPNs. In addition, most VPN protocols also use several other specialized protocols to carry out specific tasks.

Mergic VPN communicates to a VPN server across a public TCP/IP network, such as the Internet, using a protocol called the Point-to-Point Tunneling Protocol (PPTP). PPTP uses another protocol called the Point-to-Point Protocol (PPP) to negotiate many of the connection properties between the client and server. Two of the most important properties negotiated for a VPN connection are authentication and encryption. The process of identifying who you are so that the server can make sure you are authorized to connect to the private network is called authentication. PPP negotiation is used to agree on a common authentication protocol that can be used for this purpose. Mergic VPN supports several different authentication protocols. Encryption is the process of obfuscating the transmitted data so that only the VPN client and the VPN server are able to read it. PPP is used to negotiate the use of yet another protocol that defines how encryption will take place. Mergic VPN supports the Microsoft Point-to-Point Encryption (MPPE) protocol to keep the data private. PPTP with MPPE is such a common combination that it's often collectively referred to as simply PPTP.

Microsoft, 3Com, and a consortium of other vendors developed PPTP. Its popularity is largely a result of its availability and easy implementation. Microsoft has provided a PPTP client in the Windows® operating system since Windows® 95 and a PPTP server has been included with Windows servers since Windows NT® 4.0. This integration makes PPTP available to any organization using Windows and, because PPTP is integrated with Windows it's relatively easy for an organization to implement. The popularity of Windows has also resulted in a high degree of support from other VPN server and client vendors.

Features

Mergic VPN provides the following features:

- Runs on Palm OS Devices with an English version of Palm OS 3.1 or higher (including OS 5).
- Supports the Point-to-Point Tunneling Protocol (PPTP).
- Auto Connect. Allows user selected Palm OS applications to automatically connect/disconnect to/from the VPN server as needed without requiring the user to launch the Mergic VPN application.
- Client-side split tunneling. Allows simultaneous access of the Internet and the private network without sending all traffic through the private network.
- Multiple VPN configurations.
- Compatible with TCP/IP based network connections, including connections using wireline and wireless modems, smartphones, 802.11b (Wi-Fi) wireless LANs, mobile phones connected to handholds using Bluetooth, infrared or cable, and GSM, GPRS, TDMA, CDMA, CDMA2000 and CDPD networks.

¹ Although a VPN client can be used to establish a private connection across any public network, the most common use is across the Internet. To simplify explanations, this document is written using the Internet in all descriptions of the public network.

- Support for 40, 56 and 128-bit Microsoft Point-to-Point Encryption (MPPE) in both stateless and stateful modes. Mergic VPN attempts to connect with the server using the strongest (128-bit, stateless) encryption available. If the server doesn't support that level of encryption Mergic VPN will try to connect with the next strongest level of encryption. This negotiation process continues until the weakest (40-bit, stateful) level of encryption is tried.
- Supports the PAP, CHAP, MS-CHAPv1, and MS-CHAPv2 authentication protocols. For security reasons, PAP authentication is disabled by default and, also by default, if the VPN server attempts to negotiate MS-CHAPv1, NT type responses are enabled and LAN Manager type responses are disabled. PAP authentication and LAN Manager type responses can be enabled by turning off the Encryption Required setting in Mergic VPN.
- Highly optimized encryption and authentication routines provide fast authentication and good performance over all network types, including 3G wireless networks and 802.11b wireless LANs.
- Automatic and/or manual configuration of the Domain Name Service (DNS) server addresses to be used on the private network. A custom Domain Name can also be entered as an automatic suffix to be used when connected to the private network.
- Automatic and/or manual configuration of the IP address to be used on the private network.
- Connection status icon on all Palm OS devices that support the command toolbar. An icon on the command toolbar indicates when a network connection exists, when a secure private network connection exists and the signal strength on smartphones that support this feature.
- Continuous VPN connection indicator on non-color Palm OS devices. A small flashing vertical bar in the upper right hand corner of the screen indicates an active network connection on a Palm OS device. When a connection with a VPN server is active this bar is replaced with a small flashing square.
- Separate user configurable idle timeout setting for VPN connections.
- Detailed diagnostic logging.

System Requirements

To install and run Mergic VPN you will need the following:

- A Palm OS device with an English version of Palm OS 3.1 or higher.
- 320 KB of available space on the Palm OS device. (Requires 220 KB after installation.)
- Some way to obtain a TCP/IP network connection. Supported methods include IEEE 802.11 wireless LAN modules, wireline and wireless modems, smartphones, and mobile phones connected to handhelds using Bluetooth, infrared or cable.
- An account with an Internet Service Provider (ISP) or wireless data provider.
- Access to a VPN (PPTP) Server.
- Adobe® Acrobat® Reader® for viewing the User's Guide.



Installation

To install or upgrade Mergic VPN double click on the MVPNInstall.prc file, follow any instructions given and then HotSync. After the HotSync operation completes launch the MVPN Install program on your handheld. Depending on the device and whether you are upgrading or installing Mergic VPN for the first time, the MVPN Install program may require a reset to complete the installation. Simply follow the on screen instructions.


Uninstalling Mergic VPN from a Palm OS device

To delete Mergic VPN you need to make sure that no part the program is active on the Palm OS device. The simplest way to ensure this is to reset your handheld and if you are prompted to Enable VPN Auto Connect then tap the Cancel button. After the reset perform the following procedures before making any network connections.



To Delete the Mergic VPN program from your device:

1. Tap the Applications icon .
2. Tap the Menu icon .
3. Tap App, and then tap Delete.
4. Select Mergic PPTP.
5. Tap the Delete button and then tap Yes to confirm the deletion.
6. Select Mergic VPN.
7. Tap the Delete button and then tap Yes to confirm the deletion.
8. Select MergicVPNDrvr and then tap the Delete button.
9. Tap the Delete button and then tap Yes to confirm the deletion.
10. Tap Done.

To Remove Mergic VPN Network Services (Palm OS 3.3 – 4.1, except Treo):


1. Tap the Applications icon .
2. Tap the Preferences icon .
3. Select Network.
4. Select the VPN network service (named Mergic VPN by default) that you no longer want.
5. Select Delete from the Service menu and then tap OK to confirm the deletion.
6. Repeat steps 4-5 for any remaining unwanted services.

To Remove Mergic VPN Connection configurations (Palm OS 3.3 – 4.1):

1. Tap the Applications icon .
2. Tap the Preferences icon .
3. Select Connection.
4. Select the MVPN configuration (named Mergic VPN by default) that you no longer want.
5. Tap Delete and then tap OK to confirm the deletion.
6. Repeat steps 5-7 for any remaining unwanted configurations.

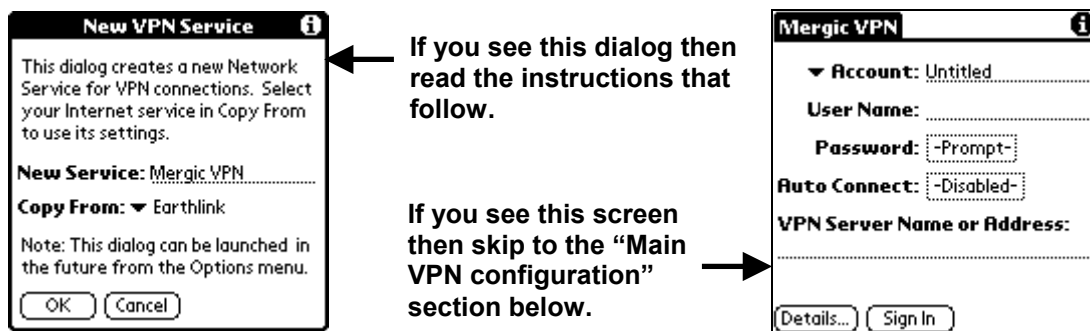
Configuration

Starting Mergic VPN for the first time

You can launch Mergic VPN by tapping the Applications icon  and then the Mergic VPN icon. When Mergic VPN is launched for the first time an End User License Agreement (EULA) dialog is displayed. Please read the agreement carefully. You must agree to the EULA before using Mergic VPN.

If you agree to the EULA then after the agreement is accepted, Mergic VPN will automatically determine your Palm OS connectivity requirements. With the exception of the palmOne (formerly Handspring) Treo, Palm OS 3.3 - 4.1 devices require some manual configuration of Palm OS connectivity options in order to use Mergic VPN. Manual configuration is not required on the Treo and devices with Palm OS 3.1, 3.2 and 5.x.

If manual configuration is required then you will be presented with a New VPN Service dialog that can be used to create a new Network Preferences service with all of the connectivity options required to make VPN connections. If no manual configuration is required then Mergic VPN's main configuration screen will be displayed.



Using the New VPN Service dialog:

1. The New Service name can be set to any name that you would like to call the new VPN network service. The default name is Mergic VPN.
2. If Copy From is not set to the network service that you use to connect to the Internet then select the correct service.
3. Tap OK.

The New VPN Service dialog does a lot of work behind the scenes to create the right settings. Normally you don't need to be concerned about how it does its job but if you want to understand what modifications are made then here's a description of what happens when OK is tapped: A new network service named Mergic VPN is created using a copy of the selected Internet service's settings and replacing the Connection with a Mergic VPN connection configuration. The Mergic VPN connection configuration is created by copying settings from the connection configuration that the selected Internet service uses. This new connection configuration is then modified by replacing the connection type with an "MVPN" connection type that allows Mergic VPN to intercept and encrypt network traffic. Finally, Mergic VPN's Connect Via option is set to the replaced connection type so that Mergic VPN knows how to connect to the Internet.

If you would prefer to modify an existing network service to use a VPN connection configuration, rather than creating a new service, that is also possible. To do this you should examine Appendix A: Modifying an existing Network Service for VPN (Palm OS 3.3 – 4.1, except Treo).

If you want to use the New VPN Service dialog after the first time Mergic VPN is launched then it can be accessed from the New VPN Service menu item in Mergic VPN's Options menu.

Main VPN configuration

All of the commonly required VPN settings are displayed on Mergic VPN's main screen. In most cases this screen contains all of the settings you need in order to make VPN connections.

Naming a VPN configuration

In case you need to connect to more than one VPN server, Mergic VPN allows you to create multiple VPN configurations. To allow you to distinguish one VPN configuration from another you can give each configuration a descriptive name.

To name a VPN configuration:

1. Tap the Account field.
2. Replace the "Untitled" string with a name that describes the VPN configuration.

A screenshot of the Mergic VPN application interface. At the top, there is a header bar with the text "Mergic VPN" and an information icon. Below the header, there are several settings fields: "Account: Untitled", "User Name:", "Password: -Prompt-", "Auto Connect: -Disabled-", and "VPN Server Name or Address:". At the bottom, there are two buttons: "Details..." and "Sign In".

Replace "Untitled" with a descriptive name here

Entering a user name

The User Name setting identifies the name you use when you log into your private network. Normally you just enter the same user name that you use for local area network access but on some Windows Domain based networks you need to enter the Windows domain name followed by a '/' character before your user name; for example, "MYDOM/dorenes" instead of just "dorenes". If you are unsure if you need to enter the Windows domain name then attempt to connect without it first and if you get an authentication error then try again, this time using the Windows domain name.

To enter a user name:

1. Tap the User Name field.
2. Enter your user name.

A screenshot of the Mergic VPN application interface, similar to the previous one. The "Account" field is now set to "ABCCompany". The "User Name" field is currently empty and is the focus of the instruction. The "Password" field is set to "-Prompt-", "Auto Connect" is "-Disabled-", and the "VPN Server Name or Address" field is empty. The "Details..." and "Sign In" buttons are at the bottom.

Enter your user name here

Saving a password

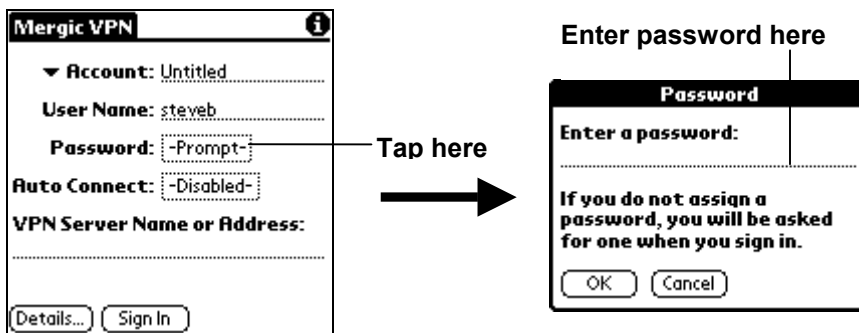
The Password box identifies the password that you use when you sign into your private network. Your entry in this field determines whether Mergic VPN prompts you to enter a password when you connect to your private network or whether a saved password is automatically used.

- If you do not enter a password, Mergic VPN displays the word “Prompt” in this field and asks you to enter a password when you sign into your private network. By default the prompt will occur each time you sign in but there are also settings to allow the password to be temporarily saved to avoid frequent prompting (See Password Prompting). The prompt occurs immediately after the connection to your Internet service is complete.
- If you enter a password, it is saved and Mergic VPN displays the word “Assigned” in this field and does not prompt you to enter a password during the VPN sign in procedure.

Note: The prompt option is more secure than saving the password. If you save a password and your Palm OS device is lost or stolen then you should immediately contact your system administrator and change your password.

To save a password:

1. Tap the Password field.
2. Enter the password you use to sign into your private network.



3. Tap OK.

Note: If you entered text before tapping OK then the password is saved and the password field will display “Assigned.” If you tap OK without entering any text then the Password field will display “Prompt” and any saved password will be destroyed.

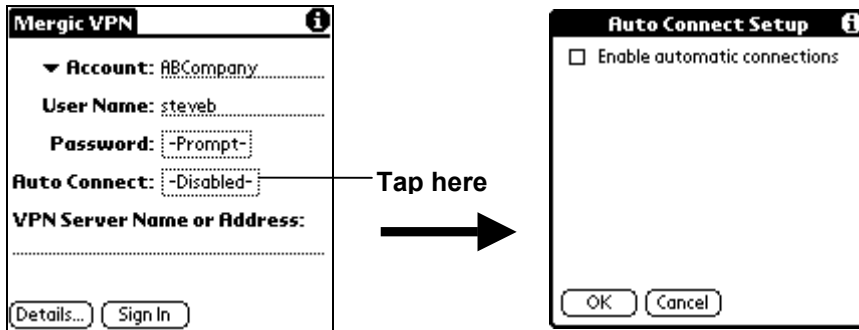
Auto Connect configuration

The Auto Connect feature allows selected Palm OS applications to automatically establish and release VPN connections as needed. Once Auto Connect is configured you save time and can focus on performing tasks rather than on VPN connectivity because you don’t need to launch Mergic VPN to connect to and disconnect from your private network. For example, if HotSync is configured for Auto Connect then when you start a network based HotSync the VPN connection will automatically take place as needed.

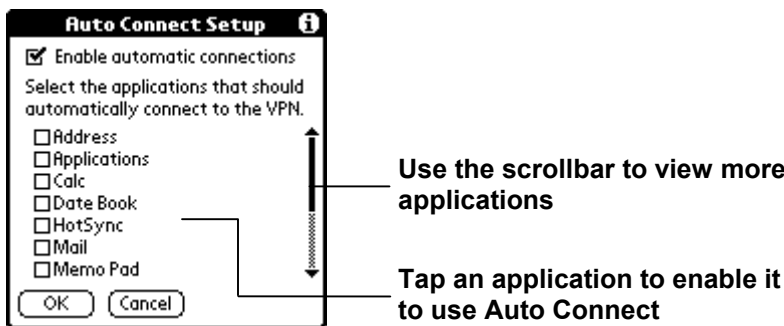
Note: More detailed information about how the Auto Connect feature decides when to connect and disconnect from your private network can be found in the section titled “Using Auto Connect”.

To enable applications to use Auto Connect:

1. Tap the Auto Connect field.



2. Tap the Enable automatic connections checkbox.



3. Tap OK.

Note: For Palm OS 3.3 - 4.1 devices, other than the Treo, automatic connections only take place if the current service in Network Preferences is a Mergic VPN service or another service that is configured to use a connection that uses the MVPN connection type.

If you reset your device while the Auto Connect feature is active then you will be prompted with the option of re-enabling the feature. This is simply a courtesy so that you have the option of resetting your device without starting any Mergic VPN code. Normally you will want to enable the feature unless you suspect it is causing a problem with the operation of your device. This prompt is similar to the prompts of other applications, such as HackMaster, that manage system modifications.

Technical Note: HackMaster manages third party code (called Hacks) that extend the Palm OS by replacing built-in system traps with their own code. The Mergic VPN Auto Connect doesn't use the HackMaster interface because it doesn't work by changing system traps.

Entering a VPN server name or address

Since Mergic VPN is a network client, it needs to know the Domain Name Service (DNS) name or IP address of a VPN server that provides access to your private network. Your system administrator should be able to provide you with the name or address of your VPN server. A DNS name looks like a web address without the “www.”, for example ABCCompany.com. An IP address consists of four numbers separated by dots, for example 189.22.229.124. If you would like general information about IP addresses and DNS names read the section titled “Defining primary and secondary DNS servers for the private network”.

Note: Some system administrators may use the term “VPN gateway” instead of “VPN server”.

To enter a VPN server name or address:

1. Tap the VPN Server Name or Address field.
2. Enter the VPN server’s DNS name or IP address.

The screenshot shows the Mergic VPN configuration interface. At the top, there is a title bar with 'Mergic VPN' and an information icon. Below the title bar, there are several fields: 'Account: ABCCompany', 'User Name: steveb', 'Password: -Prompt-', and 'Auto Connect: -Enabled-'. The 'VPN Server Name or Address:' field is highlighted with a red box, and a red arrow points from the text 'Enter the VPN server's DNS name or IP address here' to this field. At the bottom of the screen, there are two buttons: 'Details...' and 'Sign In'.

Enter the VPN server’s DNS name or IP address here

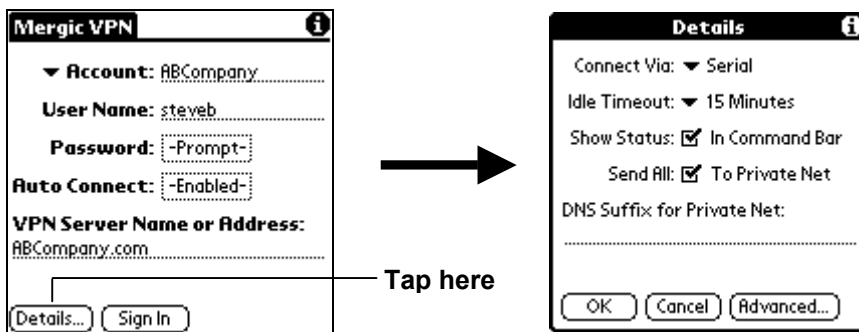
Changing detailed VPN configuration information

Under some circumstances you may also want to change the default Mergic VPN behavior by using its Details settings. You will need to change the detailed settings if any one of the following applies to your VPN connection:

- You're using Palm OS 3.3 – 4.1 on a non-Treo device and the current connection to the Internet doesn't use the same connection type as the connection method that you copied settings from when you used the New VPN Service or the New MVPN Connection dialog. (If you are not sure which connection type you use to access the Internet see "Appendix C: Determining the correct Connect Via setting (Palm OS 3.3 - 4.1, except Treo)".)
- You want to adjust the amount of time that needs to elapse before the VPN connection disconnects due to inactivity.
- You do not want the network and VPN status icon to be displayed in the command bar.
- You need to use the Internet and the private network simultaneously without disconnecting from the private network first.
- You need or would like to be able to find network resources by their short network name (i.e. "mypc") instead of their full network name (i.e. "mypc.mydomain.com").

To use the Details configuration dialog:

1. Tap Details.



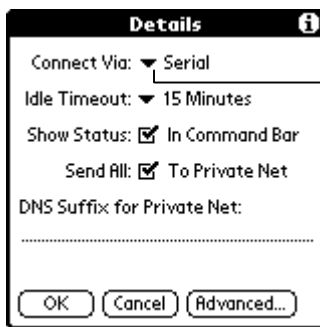
Changing the Connect Via setting (Palm OS 3.3 – 4.1, except Treo)

This setting is only available on devices that require it. If it is required then by default Mergic VPN will attempt to connect to your Internet service by using the same port as the last connection method that settings were copy from when the New VPN Service or New MVPN Connection dialogs were used. If another connection type is used for Internet access then you will need to change the "Connect Via" setting. For example, if you are using two different types of connections to the Internet but have only created one VPN configuration then you'll need to change the "Connect Via" setting when you switch between the two connections.

Note: If you are not sure whether or not you need to change this setting then see "Appendix C: Determining the correct Connect Via setting (Palm OS 3.3 - 4.1, except Treo)".

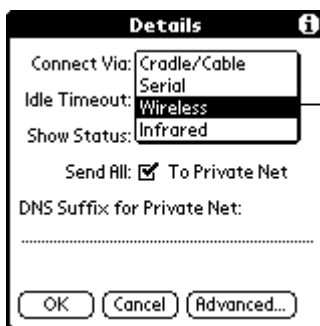
To change the Connect Via setting:

1. Tap the Connect Via pick list.



Tap to show the available connection types

2. Tap the connection type that Mergic VPN should use for this configuration.



Tap the connection type to use

3. Tap OK.

Changing the Idle Timeout setting

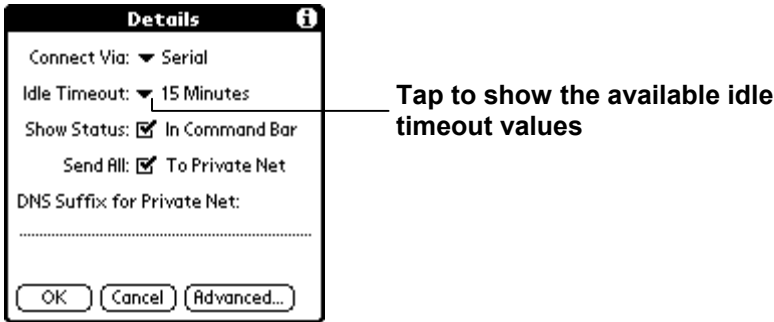
The Palm OS has two settings that extend battery life by automatically shutting down the network connection due to inactivity: (1) the Auto-off After setting in General Preferences and (2) the Idle Timeout setting for the network service which is available in Network Preferences for some connection types. These settings don't work with VPN connections because the Palm OS device drivers that detect the idle condition interpret VPN connection maintenance packets as network activity. If Mergic VPN did nothing about this then result would be that the handheld would never disconnects or power off when there is a VPN connection. To address this problem Mergic VPN provides its own Idle Timeout setting that is used when a VPN connection is established. If this Idle Timeout period expires without network activity other than VPN connection maintenance activity then the network is disconnected. After the network is disconnected then, if there is no user activity, the device will power off after the system's Auto-off After timer period elapses.

The best value for VPN Idle Timeout is really just a matter of personal preference. Some users prefer a short timeout to optimize battery life without having to remember whether a VPN connection was left up. Other users don't want the timeout to occur at all so they don't have to wait for the connection to be reestablished just because they set down their device for a few minutes. By default Mergic VPN allows the connection to stay up without activity for 15 minutes before disconnecting. This avoids frequent reconnects but eventually times out to let the device power-off if the connection is forgotten.

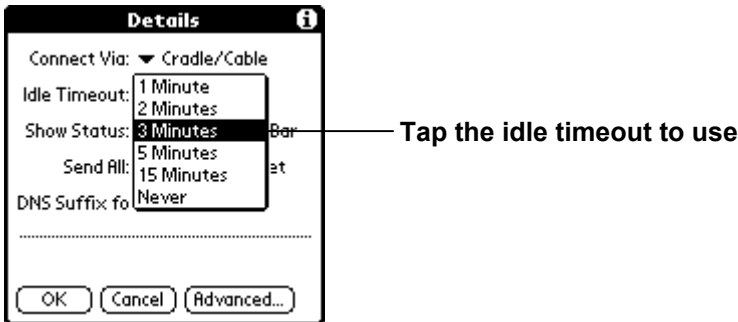
Note: Some VPN servers have their own inactivity timeout. This is independent of Mergic VPN's setting and when it exists, inactivity disconnects will happen at the shorter of Mergic VPN's setting or the server's setting.

To change the Idle Timeout setting for the VPN:

1. Tap the Idle Timeout pick list.



2. Tap the idle timeout value that Mergic VPN should use for this configuration.



3. Tap OK.

Changing Show Status In Command Bar setting

Beginning with Palm OS 3.5 many Palm OS devices added support for the display of a command toolbar when the command key (✓) or command stroke is entered. The command bar allows small icons that typically represent short cuts to be displayed. By default Mergic VPN uses the command bar to display connection status. If you tap on the icon then you can also see some statistics for the current connection. For a more detailed description of how Mergic VPN uses the command bar see the section titled "Determining whether or not a VPN connection is active".

Normally this feature is very desirable since it lets you check connection status without having to launch Mergic VPN or Network Preferences. However, if you do not want the extra icon in the command bar or if you believe Mergic VPN's command bar use is incompatible with the command bar use by another application then you can disable the feature in Mergic VPN.

To disable connection status indicator

1. Tap the Send All To Private Net checkbox to deselect it.



Tap here to disable the connection status indicator

2. Tap OK.

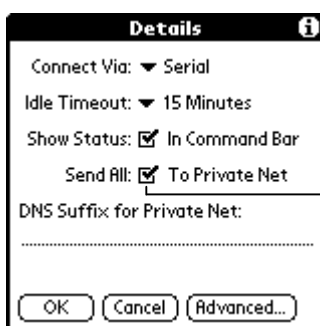
Note: Changes to this setting will not take effect until the next network connection.

Changing the Send All To Private Net setting

When you connect to a private network then by default Mergic VPN will pass all network traffic to the private network. This makes the VPN connection behave as if you are directly connected to the private network. This behavior, especially in combination with the connecting/disconnecting feature of the Using Auto Connect feature, is typically the most desirable way for the VPN connection to work. However, under some circumstances you may want to be able to directly communicate over the local Internet connection without disconnecting from the VPN first. For example, you may wish to access information that is only available from the local Internet without disconnecting from the remote private network, or you may have a background application such as an Instant Messaging application that only works when using the local Internet connection, or you may want to retrieve email from both a Internet email account and a private network account but the Internet account is inaccessible from the private network. Unchecking the “Send all to private net” option on the Details dialog enables a split tunneling feature that makes it possible to use the Internet and the private network simultaneously.

To change the Send all to private net setting:

3. Tap the Send All To Private Net checkbox to deselect it.



Tap here to toggle the split tunnel option

4. Tap OK.

Changing the DNS Suffix for Private Net setting

On many networks when you connect to your private network over the LAN a DNS suffix is automatically assigned to your PC. This suffix is then automatically appended to every DNS name query that is sent on the network. Typically the value of the setting is a domain name such as “abcompany.com”. This allows you to find servers and other machines on your network by just typing in a short name such as “abcmail”

instead of typing in the full DNS name “abcmail.abcompany.com”. When you connect via VPN, the BOOTP/DHCP traffic that is used on the LAN to assign the DNS suffix is not exchanged. This means that you must specify the full DNS name when finding network resources. Usually this is just an inconvenience but sometimes resources on your private network such as intranet websites depend on the ability to use the short DNS name. The DNS Suffix in Mergic VPN’s Advanced dialog allows you to manually set the suffix to be automatically appended when connected to the private network. When you use this option the suffix is added to all network name queries. If the query fails then the suffix is removed and another search is done.

To change the DNS Suffix setting:

1. Tap the DNS Suffix field.
2. Enter the suffix you wish to have automatically appended to name queries.



Enter a DNS Suffix to use for network name queries here

3. Tap OK.

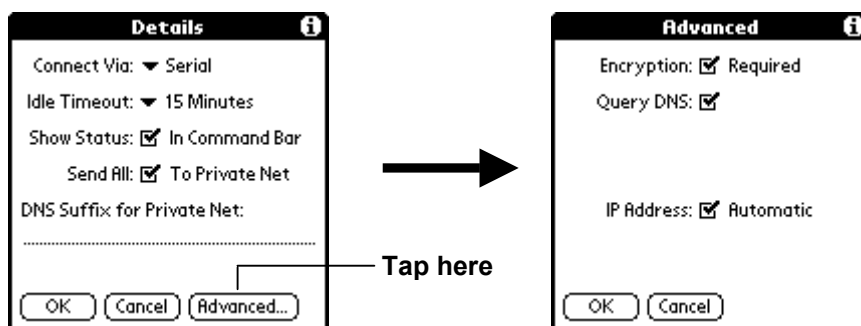
Modifying advanced VPN configuration information

Most VPN servers provide encryption, fairly recent versions of the PPTP protocol and automatically IP address information. By default Mergic VPN expects these features to be available, however, if your server doesn't provide one or more of these services then you will need to use Mergic VPN's advanced settings. Specifically, you will need to change the advanced settings if any one of the following applies to your VPN server:

- The VPN server doesn't provide encrypted connections or it only provides LAN Manager style authentication.
- The VPN server does not automatically provide the primary and/or secondary Domain Name Service (DNS) server addresses for the private network.
- The VPN server does not automatically provide the Palm OS device's IP address for the private network.

To use the advanced settings:

1. Tap Details.
2. Tap Advanced.



Setting the Encryption Required checkbox

The Encryption Required setting is used to control whether or not a secure connection to the private network is required. By default a secure connection is required. There are two types of security features that are affected by this setting: authentication and encryption.

Normally you should leave Encryption Required checked but if either of the following two exceptions applies to your VPN server then you will need to clear the setting:

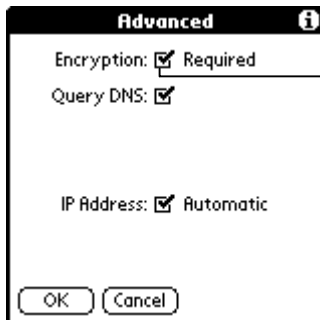
- The VPN server doesn't allow a secure connection.
- The VPN server only supports an older style of authentication referred to as MS-CHAPv1 with LAN Manager type authentication.

Note: Even if you disable Encryption Required, Mergic VPN will still attempt to acquire the most secure connection possible. The difference is that with this setting disabled the server will be allowed to:

- request and receive authentication using an unencrypted style of authentication called Password Authentication Protocol (PAP),
- negotiate for an unencrypted data connection,
- and, if the server requests the older MS-CHAPv1 style of authentication, a LAN Manager type response will be sent along with the NT type response.

To change the Encryption Required setting:

1. Tap the Encryption Required check box to toggle the setting. A checkmark indicates that encryption is required. Clearing the checkbox indicates that encryption is not required.



Tap here to toggle the Encryption Required setting

2. Tap OK.

Defining primary and secondary DNS servers for the private network

All connections between computers on a TCP/IP network take place using a unique identifier called an IP addresses. These addresses are hard for humans to remember so names are also given to computers that need to be found on the network. The Domain Name Service (DNS) provides a mechanism for translating computer names into IP addresses. For example, when you enter the name of a web site in a web browser then part of the name you enter (i.e. “www.Mergic.com”) is the DNS name for the web server. The browser then asks one of the configured DNS servers for the IP address of the web server corresponding to name you entered. If the DNS server knows or can find the IP address for the web server, it is returned to the browser. The browser then connects to the web server using its IP address and retrieves the web page that you requested.

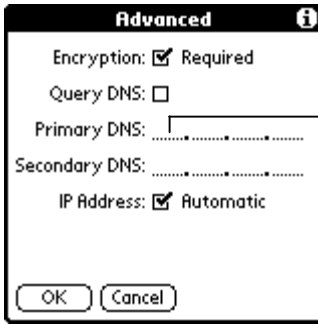
So, how does a computer that wants to find another computer know where the DNS servers are? On the Palm OS device, the DNS servers are typically configured in the Details dialog box of the Network Preferences settings. So, for example, in the case of your Internet service, the Details dialog for the service either contains the IP addresses of the DNS server(s) to be used or the “Query DNS” checkbox will be checked. If the “Query DNS” checkbox is checked then the DNS server addresses are provided to the Palm OS device by the computer that you connect to when you first establish a connection to your Internet service. If the “Query DNS” checkbox is not checked then the DNS server IP addresses were entered and they are labeled “Primary DNS” for the first server to try and “Secondary DNS” for an optional server to use if the first server is unavailable. Querying simplifies configuration, but not all Internet services provide the capability to query for DNS servers.

When a VPN connection is established you may run an application that needs to find computers on the private network but the computers on the private network are unknown to the DNS server(s) provided by your Internet service. This situation would occur, for example, if you tried to access a web page that’s only available on your private network’s intranet server. To provide for DNS capabilities on your private network you need to configure the private network’s DNS server(s) in the Mergic VPN Advanced dialog box. If the “Query DNS” checkbox is checked, as it is by default, then Mergic VPN will ask the VPN server for the addresses of the private network’s DNS server(s). If the VPN server doesn’t support the option to query for DNS servers then you’ll need to configure the IP addresses of the DNS server(s) to be used on the private network.

To configure the primary and secondary DNS servers to be used on the private network:

1. Tap the Query DNS checkbox to deselect it.
2. Tap the space to the left of the first dot in the Primary DNS server field.

3. Enter the correct part of the IP address.



Tap here and then enter the first part of the primary DNS server address

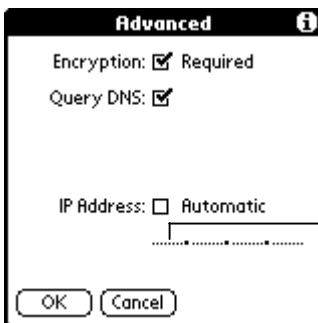
4. Enter a space or a period to move to the next field of the IP address.
5. Repeat steps 3 and 4 until all four fields of the IP address are complete.
6. Repeat steps 2 through 5 for the Secondary DNS server field.
7. Tap OK.

Defining the IP address to be used on the private network

When the Palm OS device establishes a VPN connection to the private network it needs an IP address that is unique within the private network. This IP address is different from the IP address used for your Internet service connection because the address is not necessarily unique or valid for use outside of the private network. If automatic IP addressing is enabled, as it is by default, then Mergic VPN will ask the VPN server for a private network IP address to be assigned to your device. If the VPN server doesn't support this option then you will need to configure the IP address to be used on the private network.

To configure the IP address to be used on the private network:

1. Tap the IP Address checkbox to deselect it.
2. Tap the space to the left of the first dot.
3. Enter the correct part of the IP address.



Tap here and then enter the first part of the IP address

4. Enter a space or a period to move to the next field of the IP address.
5. Repeat steps 3 and 4 until all four fields of the IP address are complete.
6. Tap OK.


Multiple VPN configurations

For situations where you need to connect to more than one VPN server, Mergic VPN allows you to create and manage multiple VPN configurations. In Mergic VPN configurations are called VPN Accounts.

Creating a new VPN configuration

VPN configurations can be created, deleted or duplicated by using the Account menu on the main Mergic VPN screen. The name of a new configuration is set to Untitled by default but it can be edited to give the configuration a meaningful name. See the section titled “Naming a VPN configuration” for instructions on how to change the name of a configuration.

To create a new VPN configuration:

1. Tap the Menu icon .
2. Tap the Account menu and then tap New.



The screenshot shows a menu with three options: 'New', 'Delete...', and 'Duplicate'. Each option has a checkmark and a letter: 'New' has a checkmark and 'F', 'Delete...' has a checkmark and 'E', and 'Duplicate' has a checkmark and 'T'. Below the menu, there are fields for 'Password' (set to '-Prompt-'), 'Auto Connect' (set to '-Enabled-'), and 'VPN Server Name or Address' (set to 'ABCompany.com'). At the bottom, there are two buttons: 'Details...' and 'Sign In'.


Tap New to create a new Untitled configuration

3. Change the Account name from Untitled to something meaningful (see “Naming a VPN configuration”).

Duplicating a VPN configuration

You can also create a new configuration by copying all of the settings from the current configuration to a new configuration.

To duplicate an existing VPN configuration:

1. Tap the Menu icon .
2. Tap the Account menu and then tap Duplicate.



The screenshot shows a menu with three options: 'New', 'Delete...', and 'Duplicate'. Each option has a checkmark and a letter: 'New' has a checkmark and 'F', 'Delete...' has a checkmark and 'E', and 'Duplicate' has a checkmark and 'T'. Below the menu, there are fields for 'Password' (set to '-Prompt-'), 'Auto Connect' (set to '-Enabled-'), and 'VPN Server Name or Address' (set to 'ABCompany.com'). At the bottom, there are two buttons: 'Details...' and 'Sign In'.

Tap Duplicate to copy the current configuration

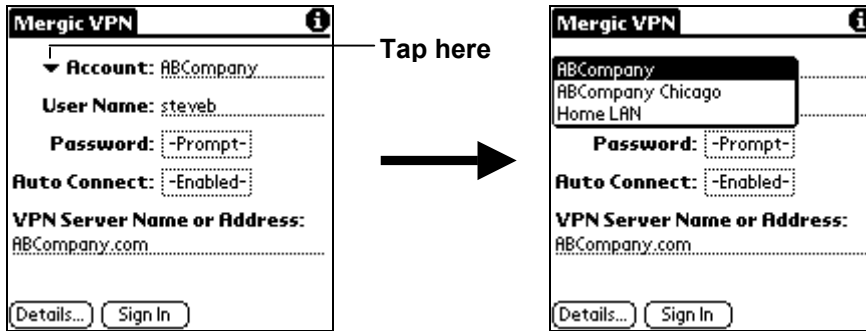
3. Change the Account name to something meaningful (see “Naming a VPN configuration”) for the new configuration.

Selecting the current VPN configuration

The Account pick list is used to select a VPN configuration. Although multiple VPN configurations are allowed, simultaneous VPN connections are not supported. The VPN configuration selected in the Account pick list becomes the current configuration and will be used for all VPN connections until a different configuration is selected.

To select a VPN configuration:

1. Tap the Account pick list.



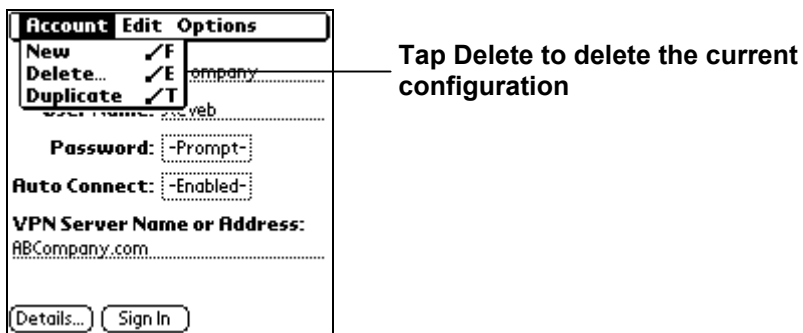
2. Tap the name of the configuration that should become the current configuration.

Deleting the current VPN configuration

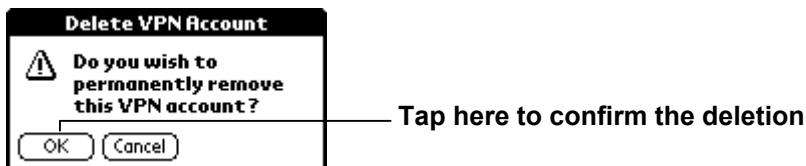
VPN configurations that are no longer needed can be deleted using the Account menu.

To delete a VPN configuration:

1. Use the VPN Name pick list to select the VPN configuration that you want to delete.
2. Tap the Menu icon (☰).
3. Tap the Account menu and then tap Delete.



4. Tap OK to confirm the delete.




Using Mergic VPN

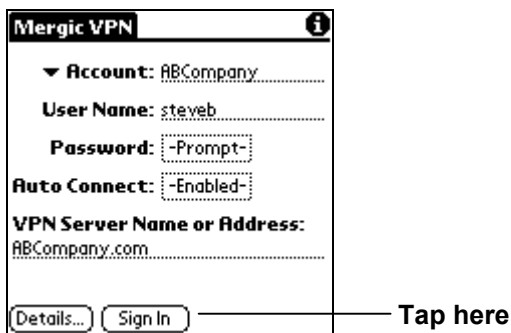
Using Mergic VPN consists of connecting to VPN server that provides access to a private network, using Palm OS applications that access the private network and then disconnecting from the VPN server when you're done accessing the private network. Connecting to and disconnecting from the VPN server can be handled manually or automatically with the Auto Connect feature.

Manually establishing a VPN connection

A VPN connection can be manually established from the main Mergic VPN screen. Once the VPN connection is manually established all communications will go through the private network until the connection is manually disconnected or the connection is lost.

To manually establish a VPN connection:

1. Tap the Applications icon .
2. Tap Mergic VPN.
3. Tap Sign In.




The Internet service connection will be established (if necessary) followed by a connection to the VPN server. If the VPN configuration uses the Password Prompting option then you will be prompted to enter the password before the VPN connection takes place.

After the VPN connection is complete the “Sign In” button will be replaced with a “Sign Out” button. At this point you can tap the Applications icon and run other networking applications that access the private network.

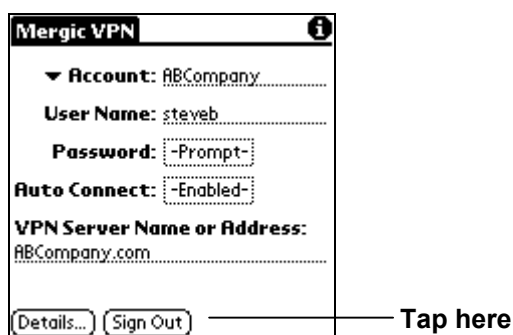
Manually disconnecting

VPN and Internet service connections can be manually disconnected by using the Mergic VPN application. You can disconnect the VPN connection and leave the connection to your Internet service active or you can disconnect from both your private network and your Internet service.

To manually disconnect:

1. Tap the Applications icon .
2. Tap Mergic VPN.

3. Tap Sign Out.





4. You will be asked if you would also like to disconnect from the Internet. Tap Yes if you want to completely disconnect your network connection. Tap No if you want to Sign Out of your private network but want to keep your device connected to the Internet.

If you do not disconnect from the Internet and the “Idle timeout” is not set to “Immediate” in the Network Preferences settings then the connection to the Internet service will continue to exist after you disconnect from the VPN server. This allows you to use applications that need Internet access without having to reestablish a connection.

To completely disconnect from your Internet service

If you have already signed out of your private network connection and want to disconnect from the Internet do the following:

1. Tap the Applications icon .
2. Tap Mergic VPN.
3. Tap the Menu icon .
4. Tap Options, and then tap Disconnect.

Using Auto Connect

Note: This section describes how to use the Auto Connect, see the section titled “Auto Connect configuration” for information on how to configure the feature.

The Auto Connect feature allows you to establish a VPN connection without having to open the Mergic VPN application each time you want to connect to a private network. Once the Auto Connect feature is configured no special action is required to connect or disconnect from the private network. When an application that is configured to use Auto Connect connects to the Internet service a VPN connection to the private network using the current VPN configuration automatically take place.

Tip: If you have a device other than a Treo with Palm OS 3.3 – 4.1 and Auto Connect doesn't seem to be working then make sure that the current network service is configured to use a Mergic VPN connection.

An automatic VPN connection is also disconnected automatically when it is no longer needed. For example, assume you have an e-mail application that uses Auto Connect to establish a connection to the VPN server. If you close the mail application then the VPN connection will still exist (unless the e-mail application forced a network disconnect) so that if the next application you use, for example HotSync, is also configured for Auto Connect then the connection doesn't need to be reestablished. But, if the next application you start is not configured for Auto Connect, for example a web browser, then the VPN connection will be disconnected when the web browser first accesses the Internet.

If you want to disable the Auto Connect feature then you can uncheck the “Enable Automatic Connections” checkbox in the Auto Connect dialog. See “Auto Connect configuration” for information on opening the Auto Connect dialog. If you have a device other than a Treo with Palm OS 3.3 – 4.1 then selecting a non-Mergic VPN connection configuration in Network Preferences settings also prevents automatic connections from taking place.

Determining whether or not a VPN connection is active

Like any network connection a VPN connection can unexpectedly disconnect. This can happen for a variety of reasons such as an unreliable phone line or wireless connection, a connection time limit may be reached on the VPN server, or the Auto Connect feature may need to disconnect from the server to allow a non-VPN application to access the Internet directly. Because the connection status can be so fluid it’s often useful to be able to determine the current connection status.

Beginning with Palm OS 3.5 many devices added support for the display of a command toolbar when the command key (⌘) or command stroke is entered. The command bar allows small icons that represent short cuts to be displayed. Mergic VPN uses this feature to display connection status as shown below.



On most devices arrows are used to indicate that a network connection exists. On devices that support signal strength, a signal strength indicator with arrows over the indicator is used. A small lock is displayed if there is an active VPN connection. If you tap on the icon then a current connection status pop-up form is displayed for a few seconds.

Note: If you want to disable the connection status icon see “Changing Show Status In Command Bar setting”.

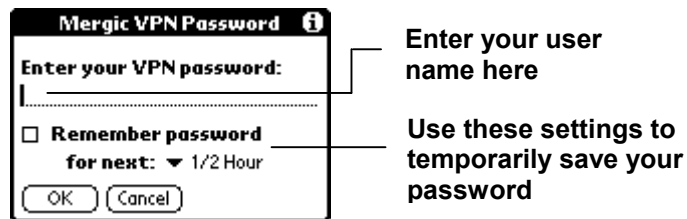
On non-color Palm OS devices the existence of an active VPN connection is also indicated by a small square flashing cursor in the upper right hand corner of the screen. This square replaces the flashing vertical bar that the Palm OS uses to indicate a network connection. If the VPN connection is lost but the network connection to the Internet service still exists, then the flashing square is replaced with the flashing vertical bar.



On color Palm OS devices that do not support the command bar there is no continuous indication of a VPN connection. To find out if a VPN connection exists you need to launch Mergic VPN and look at the right hand button on the bottom of the screen. If the button is titled “Sign Out” then the connection to the private network still exists. If the button is titled “Sign In” then there is an active VPN connection.

Password Prompting

If a password for the VPN connection has not been saved (see Saving a password) then Mergic VPN will prompt you for your VPN password after the network connection is established. Being prompted for a password is more secure than saving a password but frequent password prompting makes using VPN more tedious so password saving is frequently used. To provide a compromise Mergic VPN offers a prompt option to save the password for up to three hours. This feature is made available from the standard password prompt and can be seen below.



When a password is temporarily saved you will not be prompted for the password again for the period selected. The temporarily saved password will be deleted if there is a VPN connection error or if you tap the Password trigger in Mergic VPN and respond with OK to the saved prompt.

Mergic VPN's temporary password saving feature is more secure than saving the password but less secure than allowing the prompt for the password on every connection.

Troubleshooting



Using Mergic VPN's log

Mergic VPN provides a detailed logging capability. The log contains information for the current active connection. If there is no current connection the log contains information for the last completed connection. The log is very useful for diagnosing connection problems but it's also very technical. Understanding the log requires an understanding of the Point-to-Point Protocol (PPP) and the Point-to-Point Tunneling Protocol (PPTP). It's intended for use by system administrators and Mergic support personnel.

If you experience a problem then you can save the log for later examination. There are two ways that the log can be saved. (1) You can open the log and save its contents to the built-in Memo Pad application. (2) The log can be backed up to a file on the desktop computer. This file can then be sent to the appropriate support staff.

Opening the log

To open the log:


1. Tap the Applications icon .
2. Tap Mergic VPN.
3. Tap the Menu icon .
4. Tap Options, and then tap View Log.

Note: The Palm OS Select and Copy operations are supported to allow portions of the log to be copied. These features can be accessed from the Log dialog's Edit menu.

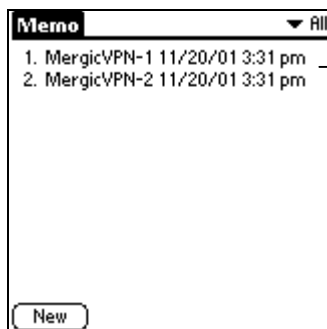
Saving the log to Memo Pad

The contents of the log can be copied to the built-in Memo Pad application. If log exceeds size 4,000 characters then multiple Memo Pad messages will be created.

To save the log to Memo Pad:

1. Open the log.
2. Tap the Menu icon .
3. Tap Record, and then tap Copy to Memo Pad.
4. Tap Done.

Note: The first line of each message will contain "MergicVPN", the message index for the current log, and the date and time of the connection that was logged.



A log that required two messages

Backing up the log

The Mergic VPN log is backed up each time you HotSync. The log database is stored in the "Mergic_VPN_Log.PDB" file in the HotSync backup directory. You can use your desktop computer to send this log database file to the appropriate support staff.

Note: To examine the log database it needs to be installed in a Palm OS device and then opened.

Customer Support

If you have any problems with Mergic VPN, or if you have questions or comments regarding the product you can reach Mergic support via the Internet at <http://www.mergic.com/support.php>.

Appendix A: Modifying an existing Network Service for VPN (Palm OS 3.3 – 4.1, except Treo)

If you have a device where the Palm OS connectivity options need to be configured to allow VPN access then the simplest way to set up the connectivity is to use Mergic VPN's New VPN Service dialog to set-up a VPN service in a single step. The New VPN Service dialog is presented when you start Mergic VPN for the first time (see *Starting Mergic VPN for the first time*) and can be accessed after that by using the Options menu in Mergic VPN. If you would prefer to modify an existing service to use VPN then this appendix describes how to create a VPN connection configuration and modify a network service to use it.

Note: On some smartphones if you modify the Connection used by the default wireless provider's network service then the device will overwrite your modification with the default setting after you HotSync, reset or disconnect from the network. If your device does this then you should create a new network service for VPN instead of modifying the wireless provider's default network service.

Step 1 – Create an MVPN connection configuration

The first step is to use the New MVPN Connection dialog to create a new Palm OS connection configuration that uses the settings of the connection configuration that you use to access the Internet. This dialog will replace the connection type in your Internet connection configuration with the MVPN connection type to allow Mergic VPN to intercept and encrypt network traffic.

Note: Although you can manually create an MVPN connection configuration by using Connect Prefs you should always use the New MVPN Connection dialog. There are two reasons for this:

- 1. In Palm OS devices with 4.1 ROMs some connection configurations, for example those connecting via Bluetooth, contain hidden settings that are needed to make a VPN connection. The New MVPN Connection dialog will copy the hidden settings.*
- 2. When you create a connection configuration by using the New MVPN Connection dialog then the Connect Via setting on the Mergic VPN Details dialog will automatically be modified to use the same connection method as the last Internet connection configuration that you choose to copy the settings from.*

To create an MVPN connection configuration:

1. Tap the Applications icon .
2. Tap Mergic VPN.
3. Tap the Menu icon .
4. Tap Options, and then tap New MVPN Connection to bring up the dialog.




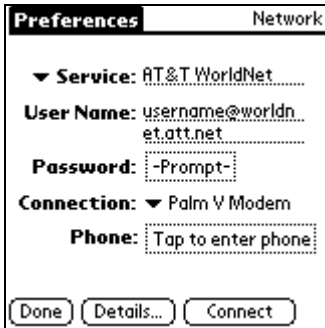
5. Tap the connection you use to connect to the Internet. (If you are not sure which connection you use for connecting to the Internet then stop here and follow the instructions in "Appendix B: Determining your Internet connection configuration (Palm OS 3.3 - 4.1, except Treo)".)

6. Tap OK.

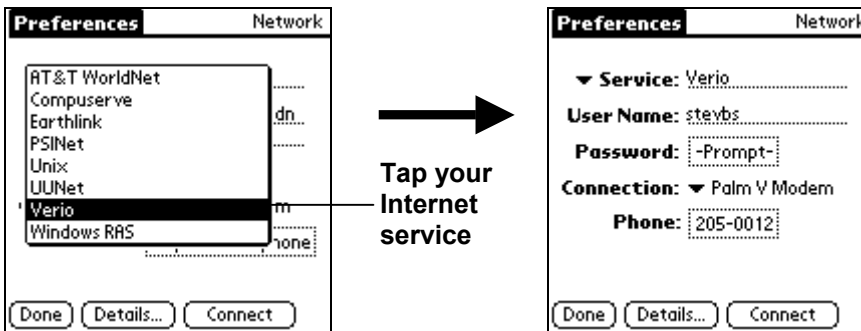
Step 2 – Modify the network service

Next you need to modify the network service that you want to use for VPN access to use the connection configuration that you created in Step 1.

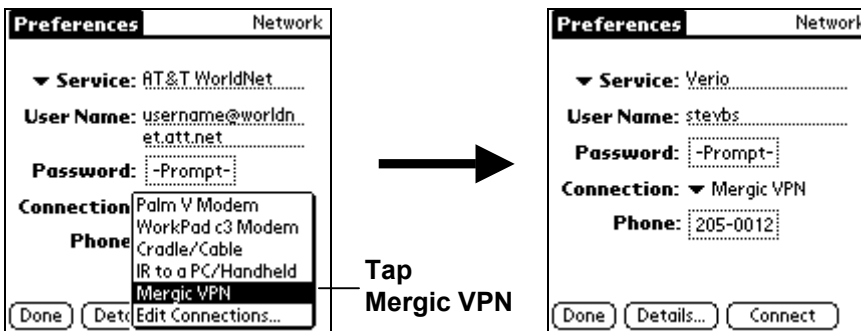
1. Tap the Menu icon .
2. Tap Options, and then tap Network Prefs.



3. If the service displayed is not the Internet service you want to use then tap the Service pick list and the service that you use to connect to the Internet.



4. Tap the Connection pick list and then select the connection configuration that you created for Mergic VPN in step 1 (named "Mergic VPN" by default).





5. Tap Done.

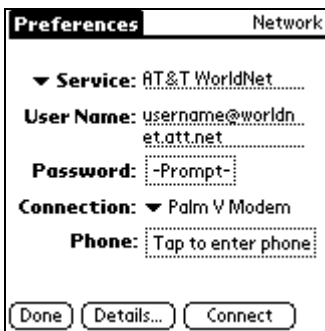
The Palm OS connectivity options are now set-up for VPN access.

Appendix B: Determining your Internet connection configuration (Palm OS 3.3 - 4.1, except Treo)

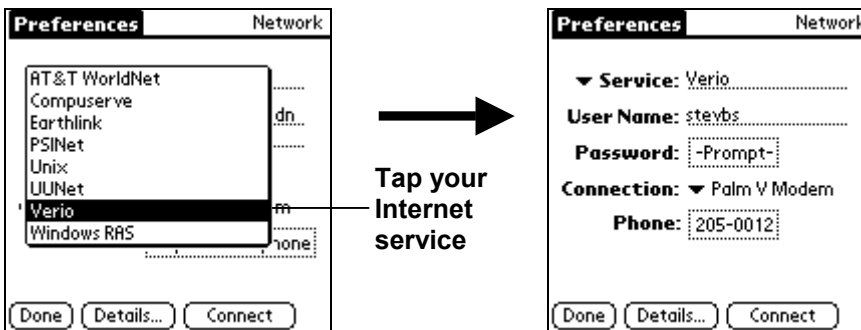
Manually setting up the Palm OS connectivity to use Mergic VPN using the New MVPN Connection dialog requires you to know which connection configuration you use for accessing the Internet. However, you may have forgotten this information, or the connectivity may have been set up for you by an administrator or automatically when your Internet provider software was installed. This appendix will help you determine which connection configuration has the settings you need to use as the basis for the Mergic VPN connection configuration.

To determine your Internet connection configuration:

1. Tap the Applications icon .
2. Tap Mergic VPN.
3. Tap the Menu icon .
4. Tap the Options menu and then tap Network Setup.



5. If the service displayed is not your Internet service then tap the Service pick list and the service that you use to connect to the Internet.



6. Make a note of the Connection setting. (Palm V Modem in the sample screen.)
7. Tap Done.



The connection setting that you made a note of in step 6 is your Internet connection configuration. You should copy settings from this connection configuration when you create an MVPN connection configuration.

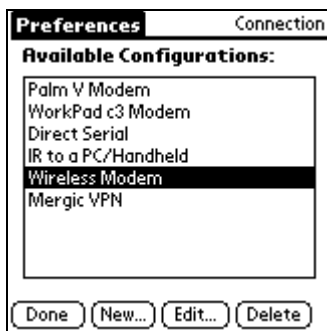
Appendix C: Determining the correct Connect Via setting (Palm OS 3.3 - 4.1, except Treo)

When you create an MVPN connection configuration using the New MVPN Connection dialog, the Connect Via setting on the Mergic VPN Details dialog is automatically modified to use the connection method that you copied the settings from. If you create a new VPN configuration or accidentally modify the Connect Via setting then you need to set it to the correct value. You can determine the correct value for this setting by examining your Internet connection configuration.

Note: If you are not sure of the name of your Internet connection configuration then see “Appendix B: Determining your Internet connection configuration (Palm OS 3.3 - 4.1, except Treo)” before proceeding with following instructions. If you have a Mergic VPN network service then be sure to switch back to this service before attempting a VPN connection.

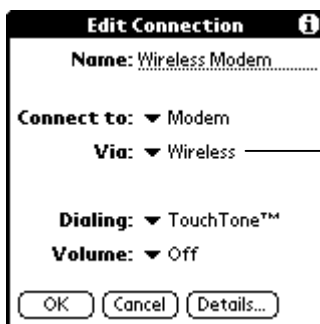
To determine your Internet service connection type:

1. Tap the Applications icon .
2. Tap Mergic VPN.
3. Tap the Menu icon .
4. Tap Options, and then tap Connection Prefs.
5. Tap your Internet connection configuration. .



Tap the connection configuration that was used in the Internet service

6. Tap Edit.
7. If the Palm OS device contains Palm OS 4.1, make a note of Via setting



Note the Via setting

If the device contains Palm OS 3.3 to 3.5x, make a note of the left side of the Connection Method setting (Wireless in the sample).



Note the left side of the Connection Method setting.

8. Tap Cancel to return to Connection Preferences.
9. Tap Done to return to the main Mergic VPN screen.

The setting you made a note of in step 7 is the value you need in Mergic VPN's "Connect Via" setting on the Details dialog.

Index

3

3Com · 4

A

Acrobat Reader · 5

Adobe · 5

Advanced dialog · 12

 accessing · 12, 17

 DNS settings · 18

 IP address setting · 19

Advanced Dialog · 17

applications

 using after manual connect · 22

 using with Auto Connect · 23

assigned password · 9

authentication

 changes by Encryption Required setting · 17

 described · 4

 LAN Manager · 17

 negotiation · 4

 protocols · 4, 5

Auto Connect · 15, 22, 24

 configuration · 9, 23, 24

 disabling · 24

 feature · 4

 required Palm OS connectivity settings · 10, 23

 reset · 10

 using · 23

Auto-off After setting · 13

B

Bluetooth · 28

BOOTP · 16

C

Challenge-Handshake Authentication Protocol ·
 See CHAP

CHAP · 5

client

 VPN · 4

command bar · 14, 24

command toolbar · See connection indicator

configuration

 copying a VPN configuration · 20

 creating a new VPN configuration · 20

 deleting a VPN configuration · 21

 overview · 7

 selecting a VPN configuration · 21

Connect Via setting · 12, 13, 31.

connecting

 to a VPN server · 22

connection configuration · 24, 31

 creating · 28

 Internet · 28, 30

 MVPN · 30

connection indicator · 5, 24

Connection Method setting · 32

Connection pick list · 29

connection status indicator

 disabling · 15

connection type

 Internet service · 31

 MVPN · 6, 30

Connectivity Wizard

 Step 2 · 29

consortium

 PPTP · 4

Customer Support · 27

D

Details dialog

 Connect Via setting · 32

DHCP · 16

disconnecting

 from a VPN server · 22, 23

DNS

 described · 18

 full name · 16

 primary server · 17, 18

 querying for · 18

 secondary server · 18

 secondary server · 17

 server configuration · 5, 18

 server settings · 18

 short name · 15

 VPN server name · 11

DNS suffix setting · 16

DNS Suffix setting · 15

domain name

 Windows · 8

E

encryption
 changes by Encryption Required setting · 17
 described · 4
 MPPE · 4, 5
 negotiation · 4, 5
Encryption Required setting · 5, 17, 18
End User License Agreement · 7
EULA · *See* End User License Agreement

F

features · 4
flashing square · *See* connection indicator

G

gateway
 VPN · 11

H

HackMaster · 10
Hacks · 10

I

Idle timeout · 23
Idle Timeout · 14
Idle Timeout setting · 13
Installation · 6
Internet · 4
Internet service · 29
Internet Service Provider · *See* ISP
IP
 address · 11
IP address
 described · 18
 for Palm OS device · 5, 17, 19
 from VPN server · 19
ISP · 5

L

LAN · 4
LAN Manager type response · *See* MS-CHAPv1
Local Area Network · *See* LAN
log · 5, 26
 backing up · 27
 saving to Memo Pad · 26

M

Memo Pad · 26
Mergic VPN Details dialog · 28
Microsoft · 4
 Windows · 4
Microsoft Point-to-Point Encryption · *See* MPPE
MPPE · 4, 17
 feature · 5
 negotiation · 5
 stateful mode · 5
 stateless mode · 5
MS-CHAPv1
 feature · 5
 LAN Manager type response · 5, 17
 LAN Manager type response · 17
 NT type response · 5, 17
MS-CHAPv2
 feature · 5
multiple
 VPN configurations · 20
 VPN connections · 20
multiple configurations
 feature · 4
MVPN · 6, 30
MVPN Install · 6
MVPNInstall.prc · 6

N

negotiation
 authentication · 4
 encryption · 5
 PPP · 4
network preferences · 18
network service
 modifying · 29
 Modifying · 7, 28
New MVPN Connection dialog · 12, 28, 31
New VPN Service · 7, 12
newer ROM · 28
NT type response · *See* MS-CHAPv1

P

Palm V Modem · 30
PAP
 and the Encryption Required setting · 17
 feature · 5
password
 prompt · 9, 22, 25
 saving · 8, 9
Password Authentication Protocol · *See* PAP
Point-to-Point Protocol · *See* PPP

Point-to-Point Tunneling Protocol · See PPTP
PPP · 26
 described · 4
PPTP · 4, 26
 consortium · 4
 server · 5
primary DNS server · 17
private network · 4
prompt
 password · 9, 25
protocol · 4
public network · 4

R

RAM requirements · 5
Requirements · 5
reset
 Auto Connect · 10
ROM
 newer · 28

S

saving
 password · 9
secondary DNS server · 17
selecting
 VPN configuration · 21
Send all to private net setting · 13, 15
server
 DNS · 5
 VPN · 4, 5
 VPN DNS name · 11
 VPN IP address · 11
Service pick list · 30
Show Status In Command Bar setting · 14
Sign Out button · 22, 24
split tunneling · 4, 15

T

Troubleshooting · 26

U

unexpected disconnect · 24
uninstalling · 6
 connection configurations · 6
 from Palm OS · 6
 Mergic VPN from Palm OS · 6
 network service configurations · 6
user name · 8

V

Via setting · 31
VPN
 client · 4
 configuration name · 8
 connection · 4
 current configuration · 21
 described · 4
 gateway · 11
 main configuration screen · 8
 protocol · 4
 server · 4, 5
 server address · 11
 server name · 11

W

Windows
 use of PPTP · 4
Windows domain name · 8
wireless
 data provider · 5
 PPP connection · 24