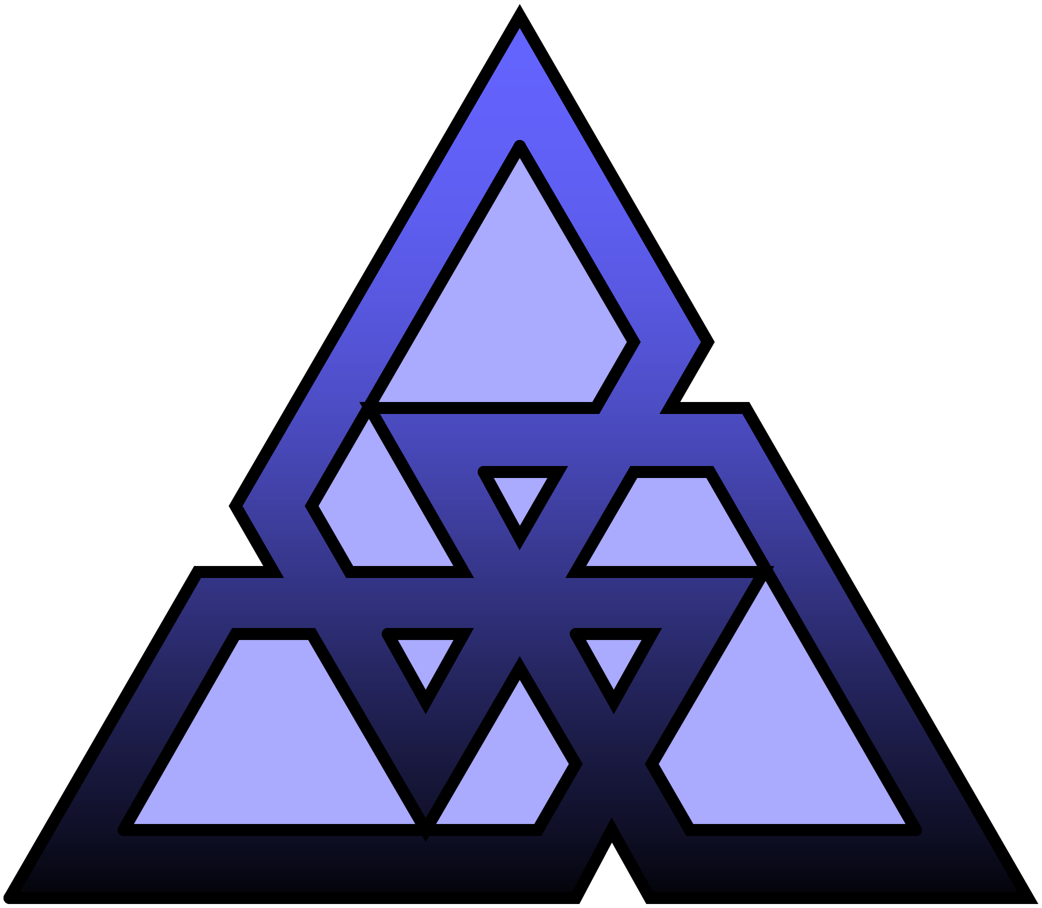


TRIO SECURITY

TRIO VAULT™ VERSION 3.0

User Guide

TRIO VAULT™

User Guide (Version 3.0)

1250 Academy Park Loop, Suite 235
Colorado Springs, CO 80910-3708
http://www.TrioSecurity.com

Copyright

Disclaimer and Limitation of Liability

Trio Security, Inc. assumes no responsibility for any damage or loss resulting from the use of this guide.

Trio Security, Inc. assumes no responsibility for any loss or claims by third parties which may arise through the use of this software. Trio Security, Inc. assumes no responsibility for any damage or loss caused by deletion of data as a result of malfunction, dead battery, or repairs. Be sure to make backup copies of all important data on other media to protect against data loss.

Important: Please read the End User Software 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.

Table of Contents

Introduction and Overview

Trio Vault™ has been developed to directly address the specific needs of the corporate office environment by providing a single-sign-on solution with 3-factor authentication. Trio Vault™ is designed to provide a fast, simple and highly reliable way to verify a user's identity before granting access to protected resources. Once the user's identity has been verified, Trio Vault™ automates access to all information resources granted to the user without any further authentication inconvenience. Trio Vault™ reduces the risks of e-business and increases the productivity of the workforce.

Trio Vault Basics

What is Single-Sign-On?

The Trio Vault™ Single Sign-On (SSO) solution improves overall security by automating access to all authorized workstations, web services and enterprise-wide applications through a single login. The Trio Vault solution eliminates the need to remember multiple sign-on processes, user IDs, or passwords. As a result, Trio Vault™ increases productivity and profitability by providing users and customers instant access to their own personalized resources and reducing demands on help desks to reset lost passwords. Trio Vault™ greatly increases network security while also increasing user convenience.

What is Three-factor Authentication?

Authentication security solutions use one or more of three fundamental factors to authenticate the identity of network users:

- **What You Know** – such as passwords, mother's maiden name, or social security number
- **What You Have** – car keys, ATM card, hardware token
- **Who You Are** – biometrics such as an iris scan, fingerprint, or a signature

However, each of these factors is vulnerable to attack if used alone or in pairs. For example, policies for ensuring secure passwords result in greater inconvenience for users, in turn causing users to write down the passwords or use passwords that can be easily memorized. In addition, typical users use the same password for multiple accounts, further degrading security. Password cracking tools (tools that allow an attacker to automate the process of guessing user passwords) are readily available for download from the Internet, making it relatively easy to crack the average password. Furthermore, many successful attacks are accomplished using passwords obtained from social engineering (an attacker's use of clever manipulation to trick trusting users into divulging password information), a problem that even the best of corporate password policies find difficult to address.

Consider the combination of a password and hardware token, such as that used in the RSA SecurID system. Systems using this form of two-factor authentication are vulnerable to attacks through theft of the hardware token coupled with the use of social engineering to obtain the user's password.

By using all three factors of authentication, along with automated password generation and management, Trio Vault™ virtually eliminates the vulnerabilities of single-factor and two-factor authentication systems.

Enhanced Security with Ease of Use: A Use Case

The Trio Vault™ Single-Sign-On solution requires users to authenticate themselves to a PDA using ALL THREE factors of authentication. The PDA then authenticates the user to the rest of the world. Because the PDA manages the creation and use of passwords for each account, users no longer have a need to remember passwords for individual accounts. For example, to log into a corporate LAN users must be in possession of their PDA with a unique device key loaded into memory (What You Have), they must enter their password into the PDA (What You Know), and then sign a password or draw a symbol on the screen (Who You Are). The rhythm, speed, and velocity of the user's handwriting are the biometrics. The PDA then uses the existing LAN security infrastructure to authenticate the user to the network.

The PDA creates and manages longer, more secure passwords for each account on behalf of the user. In addition, the passwords for individual accounts can be automatically changed by the PDA on EVERY login, providing additional security. By changing the password on every login, concerns of password compromise are virtually eliminated. In addition, users never know the passwords for ANY of their accounts, greatly reducing the opportunity for social engineering.

Because Trio Vault uses all three factors of authentication rather than just two, the authentication system is less vulnerable to attacks using theft and social engineering techniques.

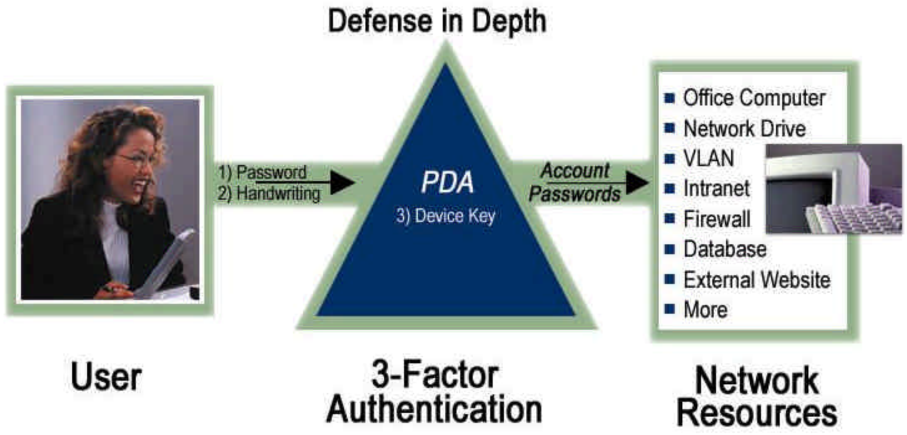
In addition, Trio Vault™ mitigates the problems traditionally associated with the use of biometrics in two ways. First, it is difficult for attackers to digitally copy the biometrics profile of a written password. Even if the biometrics profile is compromised, the user can simply change the password to generate a new profile (something that is not easily done with a fingerprint or iris). Secondly, the user's biometrics profile is NOT stored in a central database. The biometrics profile is stored (in encrypted format) only in the PDA. This provides increased privacy for the user and increased security for the corporation.

Trio Vault: Defense in Depth

In the Trio Vault™ solution, the user is given a PDA that contains the Trio Vault™ software and an encrypted listing of user accounts that can only be accessed after the user successfully completes authentication. The process of authentication is as follows:

1) **Factor 1: What You Have** - The user must be in possession of a PDA with the correct device-specific key.
2) **Factor 2: What You Know** – Upon launching the Trio Vault software, the user is prompted to enter a password.
3) **Factor 3: Who You Are** – After successfully entering the password, the Trio Vault software prompts the user to write or draw a password or symbol on the screen of the PDA. The rhythm, speed, and velocity associated with the handwriting are the biometrics. (This step also provides an additional layer of "What You Know" protection in that the user must know the correct password or symbol to write or draw on the screen.).

Once authenticated, the user chooses an account from the given list, and then presses a "Logon" button on the PDA screen. The PDA authenticates the user to the chosen computer via infrared communications or cradle. The Trio Vault solution is not vulnerable to the same attacks that can penetrate two-factor systems. It is not enough for an attacker to steal the PDA and to know the Trio Vault password. An attacker would also need to know the word or symbol the user writes or draws on the screen of the PDA and be able to write or draw it in precisely the same way.



The PDA authenticates the user to all network resources through infrared or serial connection with the computer.

Installation and Setup

System Requirements

Palm Pilot Information

- Palm OS 3.5 or greater
- 2MB memory minimum with 70K free space
- Palm Desktop 3.0 or greater for Serial COM Port connectivity
- Palm Desktop 4.0 or greater for USB connectivity

PC Information

- IBM-Compatible 486 PC or higher
- Windows 95/98/ME/NT 4.0/2000/XP
- 8M RAM minimum (64MB recommended for Windows 2000 or later)
- One available serial port for Serial Cradles
- USB port for USB Cradles
- 20MB available hard disk space
- CD-ROM Drive
- Optional
    - Infrared hardware and drivers for IR connectivity

Installation Process

The installation process is based on familiar InstallShield processes. The installation includes all the components of Trio Vault™ and a few support and information files.

Trio Vault Components

Trio Vault: PDA Application

The PDA application provides 3-factor user authentication and manages a database of user accounts and passwords. After successful authentication, the user may select a specific account to access from the listing of accounts in the account database. The application then communicates with the Trio Launch component to automate the process of logging into the selected account resource. Three modes of communication are supported: USB, Direct Serial, and Infrared.

Trio Vault: PC Components

Trio Launch

The Trio Launch component accepts from the PDA a request to login to a specific user account. Once a request is received, Trio Launch automates the process of launching the required application (e.g., Internet Explorer, Microsoft Outlook, Dial-Up Networking, etc.) and entering the username and password associated with the requested information resource (e.g., website, password protected document, virtual private network, etc.).

Desktop Logon

This Desktop Logon component of Trio Vault replaces the default logon system in Windows NT-based operating systems. In conjunction with the Trio Vault™ PDA software, this component creates a highly secure entry system that requires 3-factor authentication before granting access to the computer desktop. After successful user authentication on the PDA, the user may logon to the user's computer desktop by selecting the associated account from the account database on the PDA.

Installation

This section describes the process for installing all Trio Vault software components.

There are 3 software components of Trio Vault that get installed:

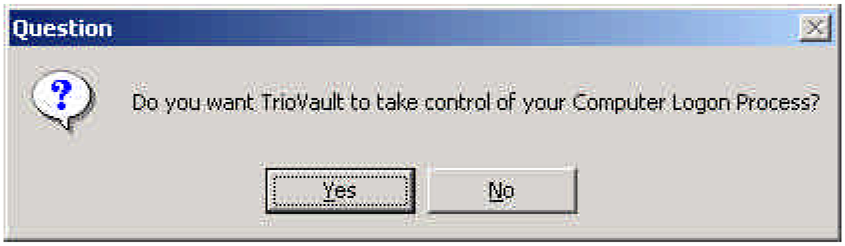
- Trio Vault™ PDA Application (installed on the PDA)
- Trio Vault™ Trio Launch (runs in the background on the user's Desktop)
- Trio Vault™ Desktop Logon (Windows NT/2000/XP only)

The installation process will automatically detect on which version of Windows the installation kit is currently running and will perform the appropriate installation. The Desktop Logon component will not be installed on Windows 9x Operating Systems.

Important Windows NT/2000/XP Installation Notes

For Windows NT 4.0 SP5 or greater, Windows 2000 Professional and Advanced Server with all service packs, and Windows XP Home and Professional Editions, Trio Vault™ can enhance the Desktop Logon process by replacing the normal Windows logon process with a more secure process that requires 3-factor user authentication before granting access to the user's desktop.

During the installation process, the user will be asked if the default Windows Desktop Logon process should be replaced with the more secure Trio Desktop Logon component.



Question

Do you want TrioVault to take control of your Computer Logon Process?

If the user selects NO, then the normal Windows Desktop Logon process will remain as the default. If YES is selected, the installation kit will install the Trio Vault™ Desktop Logon component.

IMPORTANT NOTE: If the Desktop Logon component was installed, before restarting the computer create a user account in the Trio Vault application on the PDA for the user desktop (The Trio Vault PDA Application section of this manual provides instructions for creating new accounts). This account will be used to logon to the user desktop after rebooting the computer.

Starting the Installation Kit

IMPORTANT NOTE: If installing on Windows NT/2000/XP, create a user account with administrator privileges and a strong password. The password for this account should be stored in a secure location. If the information on the Palm device is erased or otherwise lost, it may become necessary to use this account to restore the information to the device.

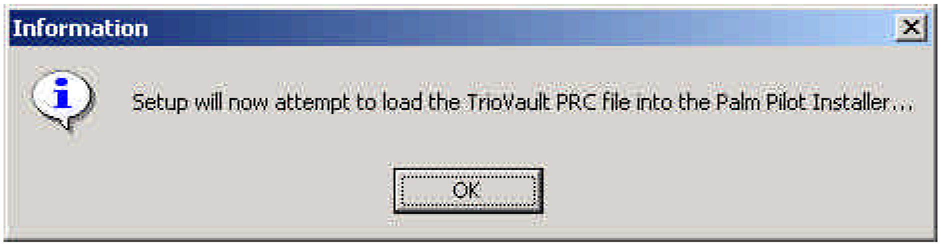
1. Verify the Palm Desktop software has been installed. You should be able to use the Hotsync® function to back up the data on the Palm device before beginning the installation process for Trio Vault.

2. Exit any open programs, including those that run automatically at startup (such as Microsoft Office) and virus-scanning software.

3. Insert the Trio Vault Installation CD-ROM into the CD-ROM drive. **Note:** If installation does not begin, click the Windows Start button, choose Run, enter "D:\Trio Vault Office Edition.exe", and then click OK. If necessary, replace D: with the drive letter assigned to your CD-ROM drive.

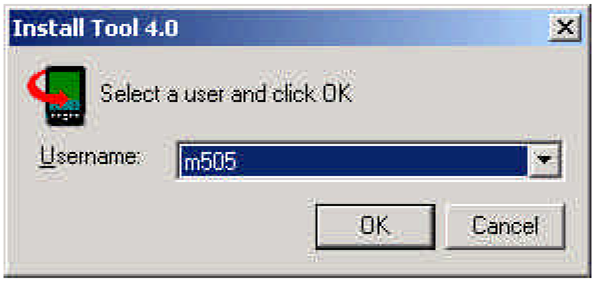
4. Follow the onscreen instructions to complete the installation. During installation, you will be asked to use the Hotsync® function to install the Trio Vault PDA application on the Pam device.

As part of the installation process, for user convenience and proper installation of all components of Trio Vault, the installation process will install the Trio Vault PDA Application onto the PDA.



Setup will now attempt to load the TrioVault PRC file into the Palm Pilot Installer…

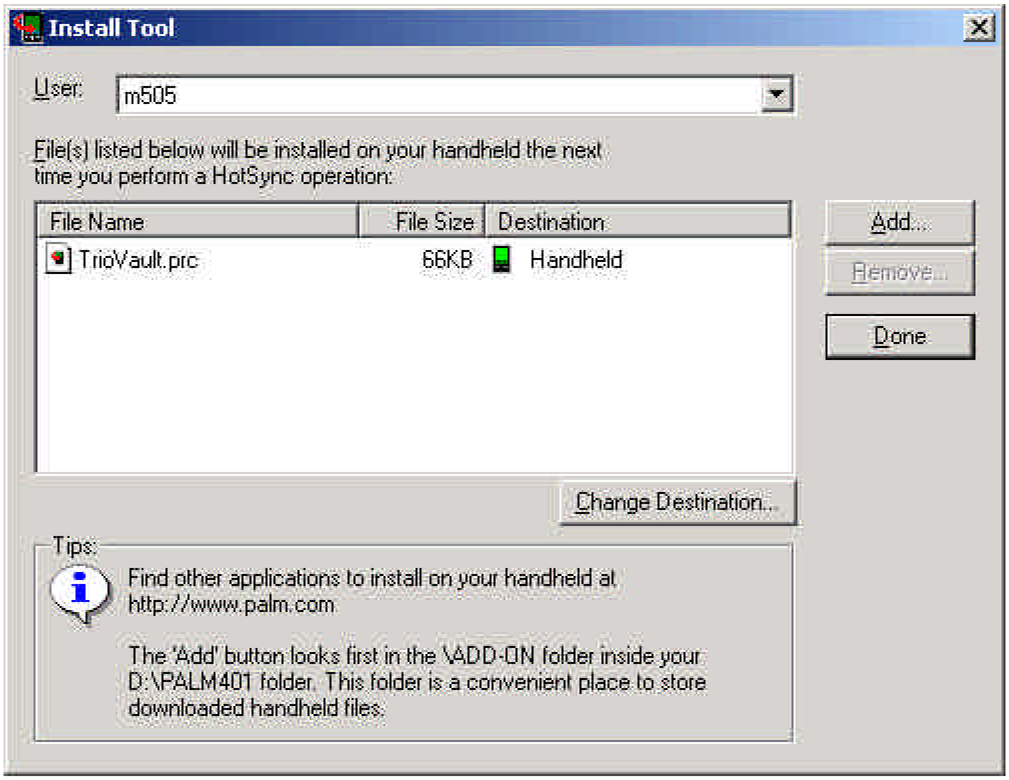
If there are multiple PDA users on the computer, you will see this dialog box first:



Select a user and click OK

Username: m505

Select the correct PDA username and press OK to continue.



User: m505

File(s) listed below will be installed on your handheld the next time you perform a HotSync operation:

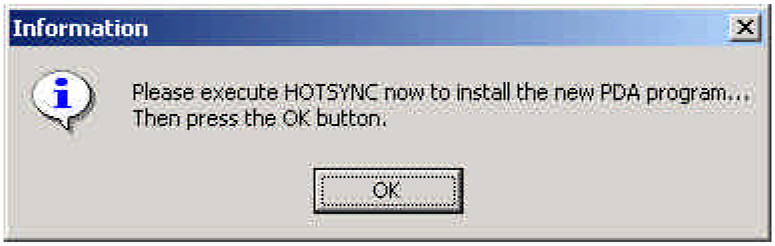
File Name	File Size	Destination
TrioVault.prc	66KB	Handheld

Find other applications to install on your handheld at http://www.palm.com

The 'Add' button looks first in the \ADD-ON folder inside your D:\PALM401 folder. This folder is a convenient place to store downloaded handheld files.

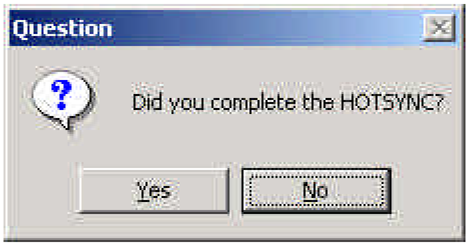
Press DONE in order to complete the PDA installation setup.

The Trio Vault™ Installation process will require the use of the Hotsync® function to install the Trio Vault software on the PDA.



Please execute HOTSYNC now to install the new PDA program...
Then press the OK button.

When the Hotsync® function is complete, the user can press the OK button to continue.



Did you complete the HOTSYNC?

The Hotsync® function is so important to a successful Trio Vault™ installation, the installation kit requires explicit confirmation that the user completed the Hotsync® function successfully.

Trio Vault: PDA Application

Setting up the PDA software

The Initial Launch of Trio Vault

When the Trio Vault™ software is launched for the first time, it creates a 40 digit Emergency Passphrase and displays that code to the user. It is vitally important to copy the Emergency Passphrase and place the copy in a secure location. The Emergency Passphrase may be required to recover account information and/or gain access to some components of the software in some circumstances.

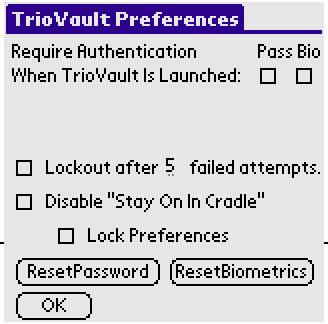
Once you have copied the Emergency Passphrase from the screen of the PDA, click the **Continue** button to proceed to the **Account List** screen. Before creating accounts, we recommend that you verify that you correctly copied the Emergency Passphrase. To do this, simply select the **Verify Emergency Pwd** menu item from the **Options** menu. Enter the Emergency Passphrase when prompted and tap **OK.** You will be alerted if the Emergency Passphrase is incorrect. If you do not have the correct Emergency Passphrase, you should delete the Trio Vault™ software from the PDA and reinstall. When you launch the Trio Vault™ software for the first time after a clean reinstall, a new Emergency Passphrase will be generated and displayed.

If you received your PDA with the Trio Vault™ software already loaded then it may be the case that your system administrator has the Emergency Passphrase for your PDA.

Trio Vault Preferences

From the **Account List** screen, select **Preferences** in the **Options** menu to access the **Trio Vault Preferences** screen.

Trio Vault Preferences:



TrioVault Preferences

Require Authentication When TrioVault Is Launched: Pass ☐ Bio ☐

☐ Lockout after 5 failed attempts.

☐ Disable "Stay On In Cradle"

☐ Lock Preferences

1. **Require Authentication When Trio Vault is Launched –** To require user authentication anytime the Trio Vault™ software is launched, select either the **Pass** checkbox, indicating that a Graffiti® password will be required, and/or the **Bio** checkbox, indicating that a handwritten word or symbol will be required.

2. **Lockout after X failed attempts –** This option will limit the number of authentication attempts that may be made before the Device Key is deleted. Once the Device Key is deleted, the Emergency Passphrase is required to gain access to the Trio Vault™ account database.

3. **Disable "Stay On In Cradle" -** Users of Palm OS devices that have rechargeable batteries can configure their PDAs to stay on while placed in the cradle. This option disables that feature. When selected, the PDA will automatically turn the power off after a user-defined time interval of inactivity. The time interval is defined in the ***Preferences*** application on the PDA.

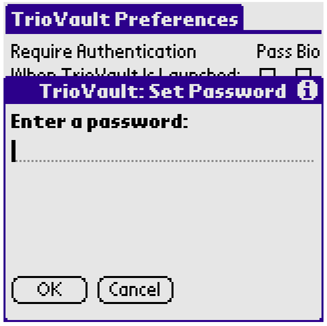
4. **Lock Preferences –** When this checkbox is selected, the user will be required to enter the Emergency Passphrase to gain access to the Trio Vault™ Preferences screen.

5. **Reset Password –** Used to change the Graffiti® password required for authentication.

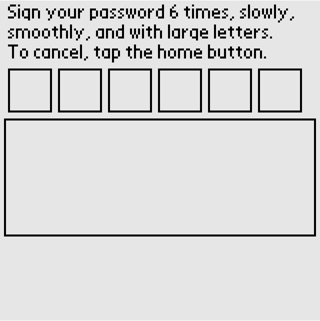
6. **Reset Biometrics –** Used to change the handwritten word or symbol required for authentication.

Creating a Graffiti® Password

When the **Pass** checkbox is selected in the **Trio Vault Preferences** screen, the user will be prompted to create the Graffiti password that will be required when launching the Trio Vault software.



Creating a Biometrics Profile



Sign your password 6 times, slowly, smoothly, and with large letters.
To cancel, tap the home button.

When the **Bio** checkbox is selected, you will be prompted to write a word or draw a symbol on the screen of the PDA six times. The screen will contain six small boxes and one large box. Write the same word or symbol in the large box six times. Each time you write the word or draw the symbol one of the six smaller boxes will be darkened. **IMPORTANT**: Sign the word or draw the symbol smoothly, slowly and with large letters. You may use multiple pen strokes when writing the word (e.g., dotting an *i* or crossing a *t*). If the six instances of the word or symbol are not very similar, the software will notify you and give you a choice to accept the handwriting profile created based on those six writing samples, or you to enter a new set of six samples.

The Trio Vault™ handwriting recognition software works by measuring the differences in the six writing samples and remembering the maximum difference between any two samples. That maximum difference is then used as a benchmark during authentication. When a user is prompted to enter the word or symbol during authentication, the software measures the difference between the authentication sample and an average sample created from the six samples given during the training process. If the difference between the authentication sample and the average sample is greater than the maximum difference between any two of the six original samples, then the user is not allowed entry. **Bottom Line: The more dissimilar the user writes the six samples during the training process, the less secure the handwriting recognition will be.**

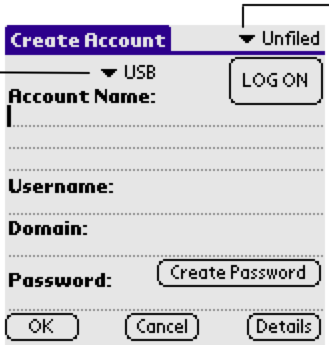
Technical Note*: Trio Vault™ actually keeps two copies of the handwriting profile: 1) the average of the six original samples, and 2) an average of the six original samples that is updated each time the user successfully authenticates. Each time the user authenticates, the authentication sample is compared against both handwriting profiles. If the authentication sample closely matches either profile, the user is allowed access. In this way, the user is granted access even if the user's handwriting changes slightly over time.*

Any word or symbol may be used when creating the biometrics profile. However, it is suggested that you NOT use your name. This represents a security hazard in that that average user may compromise digital copies of their signature on a routine basis. (When is the last time you signed an electronic pad when accepting a package from UPS?)

Creating Accounts

From the **Account List** screen, select the **New Account** menu entry in the **Options** menu. The **Create Account** screen will appear:

Tap arrow to select appropriate communications mode with PC



Tap arrow to select a category for this account

Enter the account name, username, domain name (if appropriate), and initial password in the appropriate fields.

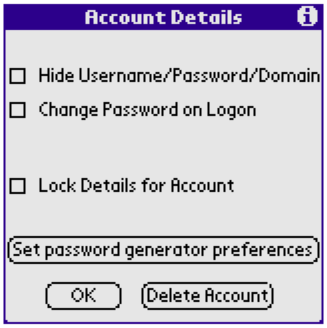
Once the appropriate information has been entered into the Username, Domain name (if appropriate), and Password fields, and once a corresponding account has been created in the Trio Launch application on the PC, then place the PDA in the cradle or point the PDA at the infrared port on the PC and tap the **Log On** button to test the account information with the PC.

Tap the **Create Password** button to have Trio Vault™ automatically create a password for you.

Tap the **Details** button to configure the preferences for the new account.

Setting Preferences for Individual Accounts

1. **Hide Username/Password/Domain** – When selected, the user will only see the account name, a logon button, and the communications mode associated with the given account.

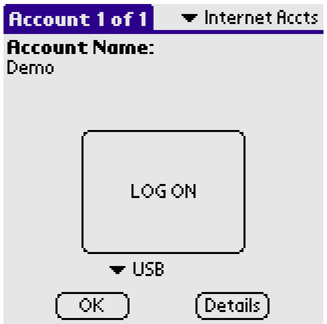


Account Details

☐ Hide Username/Password/Domain

☐ Change Password on Logon

☐ Lock Details for Account



Account 1 of 1

▾ Internet Accts

Account Name: Demo

▾ USB

2. **Change Password on Logon –** When selected, the Trio Vault™ software will attempt to change the password after a successful login to a Windows NT based operating systems (Windows NT 4.0 and later, Windows 2000, and Windows XP). This feature does not work with applications or websites.

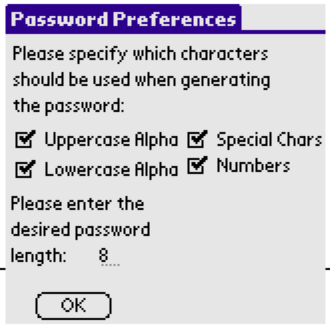
3. **Lock Details for Account** – When this checkbox is selected, the user will be required to enter the Emergency Passphrase to gain access to the **Account Details** screen for the account.

4. **Set password generator preferences –** The Trio Vault™ software can be configured to automatically generate passwords for each account. Tap this button to configure how passwords will be created (i.e., character set and length) for the account.

5. **Delete Account –** Tap this button to delete the account.

Setting Password Generator Preferences For An Account

Select which character sets should be used when generating passwords, and enter the length of the passwords (in number of characters) to be generated.



Password Preferences

Please specify which characters should be used when generating the password:

☑ Uppercase Alpha ☑ Special Chars

☑ Lowercase Alpha ☑ Numbers

Please enter the desired password length: 8

Deleting Accounts

From the **Account List** screen:

1) Select the account to be deleted by tapping the account from the list.

2) Select the **Delete** menu item from the **Options** menu for the account.

Alternatively,

3) Tap the **Details** button if available to enter the **Account Details** screen for the account.

4) Tap the **Delete Account** button.

What To Do If The Account Database Is Lost

There are several different reasons why you may need to recover an account database:

1) The batteries in your PDA run out and the memory contents of the PDA are lost.

2) The PDA is lost or stolen.

3) The Trio Vault™ software is accidentally deleted.

In all cases, the procedure for recovering the account database is the same.

1) After recharging or installing new batteries, or after purchasing a new PDA, use the Hotsync® function to recover your PDA information. The Trio Vault™ software and account database will be reloaded onto your PDA.

   NOTE: If you are using Trio Vault™ with Windows NT, Windows 2000, or Windows XP, you may be required to enter a username and password to get access to your desktop. In this case, press the **Enter** button on the PC keyboard when the Trio Vault logon screen is shown immediately after booting the PC. If the username and password for your user account is available, use these to log into the PC. If these aren't available, log in to the PC using the Administrator account, or other user account with administrator privileges created prior to Trio Vault™ installation. Using an account with administrator privileges, you should be able to gain access to the backup information for the PDA.

2) After the Trio Vault™ software and account information has been restored to the PDA, tap the Trio Vault™ icon on the screen of the PDA to launch the software. You will be required to enter the Emergency Passphrase to gain access to the account database in Trio Vault™. When the correct Emergency Passphrase is entered, a new Device Key will be generated for the PDA, and a new Emergency Passphrase will be created and displayed on the screen of the PDA. It is critical that you copy the new Emergency Passphrase and verify its validity following the procedure outlined in the section of this document entitled "Setting Up The PDA Software".

3) In some cases you may need to reset the password for your user accounts on both the PC and the PDA. For example, if

    a. you have an account on the PDA called *OfficePC* that is used to log into your user account on your office PC, and

    b. the *OfficePC* account on the PDA is configured to change the password for your user account on the PC during each login, and

    c. you did not backup the contents of the PDA after your last successful login, then

    d. the password for the *OfficePC* account restored from the last successful backup will not be the most recent password.

Therefore, both the PC user account and the PDA *OfficePC* account will need to be reset to a common password before the Trio Vault software can again be used to successfully login.

Trio Vault: Trio Launch

Setting up the Software

Trio Launch will be automatically installed during the installation process. On initial use, the communications server must be configured. When prompted, select the communication channel(s) appropriate for the PC/Cradle on which Trio Launch is installed. In most cases, the selected communication channel(s) will be identical to those that are used by the Palm Hotsync® software. For example, if the Palm Hotsync software uses USB for communicating with the Palm device, then Trio Launch should be configured to use USB as well.

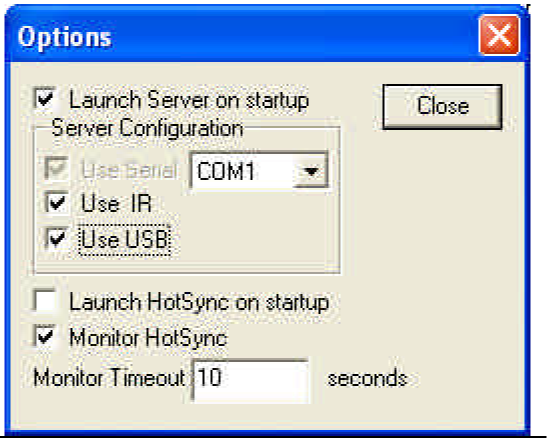
For every account in the PDA application for which you would like to automate the logon process, there must be a matching account within Trio Launch with an identical name.

The Initial Launch of Trio Launch

When the Trio Launch software is launched for the first time on a PC, the **Options** dialog will be displayed so communication options can be chosen. If no communication mode is configured, this dialog will be displayed on the next launch. Trio Launch is configured to start automatically at user logon. However, the communication server (the portion of the Trio Launch software that "listens" for a logon request from the PDA) can be set to start automatically at user logon or it can be started manually.

Trio Launch Options

To access the Trio Launch Options, right-click the Trio Launch icon located in the system tray (normally in the lower right corner of the user desktop). From the Trio Launch menu select **Options**.



☑ Launch Server on startup

Server Configuration

☑ Use Serial COM1

☑ Use IR

☑ Use USB

☐ Launch HotSync on startup

☑ Monitor HotSync

Monitor Timeout 10 seconds

Trio Launch Options:

1. **Launch Server on startup** - If this option is set the communication server will be automatically started when Trio Launch is started. If this option is not set the communication server will need to be started manually from the Trio Launch menu..

2. **Server Configuration** - This section configures the communication channels that Trio Launch will use. One or more communication channels must be selected in order for Trio Launch to communicate with the PDA. The USB option will only be available if a version of the Palm Desktop software with USB support is installed.

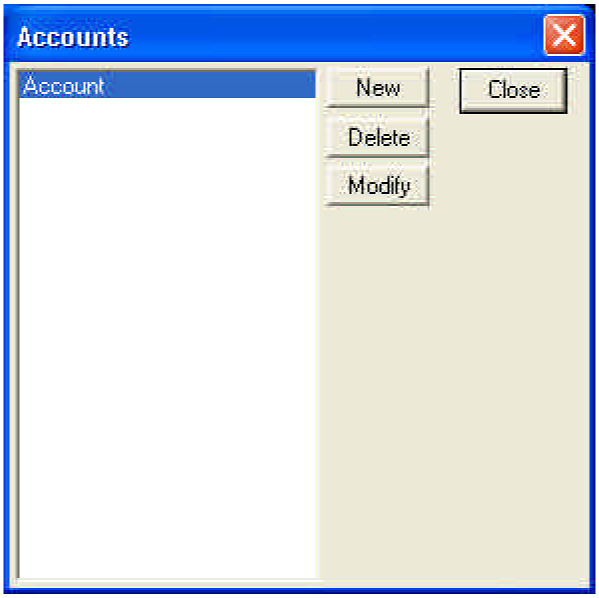
3. **Launch HotSync on startup** - This option will launch the HotSync® software once Trio Launch is running.

4. **Monitor HotSync** - This option can be used to increase security by minimizing the time HotSync is allowed to be active. This option is only available if **Launch HotSync on startup** is disabled. If this option is enabled, the user must manually launch the Hotsync software by right-clicking the Trio Launch icon and selecting "Start Hotsync". The HotSync software will only be allowed to be active for the duration of the synchronize operation or until the timeout has expired. This option is particularly useful when not using the Trio Desktop Logon software. This prevents the possibility of an attacker being able to perform a Hotsync when the workstation is locked.

Administrator Note: *The Trio Launch options can be made read only by moving them from the HKEY_CURRENT_USER\Software\TrioSecurity\Trio Launcher\Options registry key to the HKEY_CURRENT_USER\Software\TrioSecurity\Trio Launcher\Settings registry key. To prevent the user from modifying these settings by directly editing the registry, the settings key can by made readonly by changing the permissions.*

Accounts

To automate the logon process for user accounts, each account in the Trio Vault PDA application must have a parallel account within Trio Launch. The account name used in the Trio Vault PDA application must be identical to the account name used in Trio Launch.



1. To create a new account or modify an existing account in Trio Launch, right-click the Trio Launch icon in the system tray and select **Accounts** from the popup menu.

2. To add a new account, press the **New** button. To modify an existing account, select the account name and press the **Modify** button.

3. When creating a new account or modifying an existing account the **Account Name** must match the account name in Trio Vault™ on the PDA.

4. Select the **Executable** file associated with the user account by entering the path directly or by using the browse (...) button to select the file to launch. A typical example might be
   "C:\Program Files\Internet Explorer\IEXPLORE.EXE"
   to launch Internet Explorer, if the account in Trio Launch is to be used to automatically login to a password protected website.

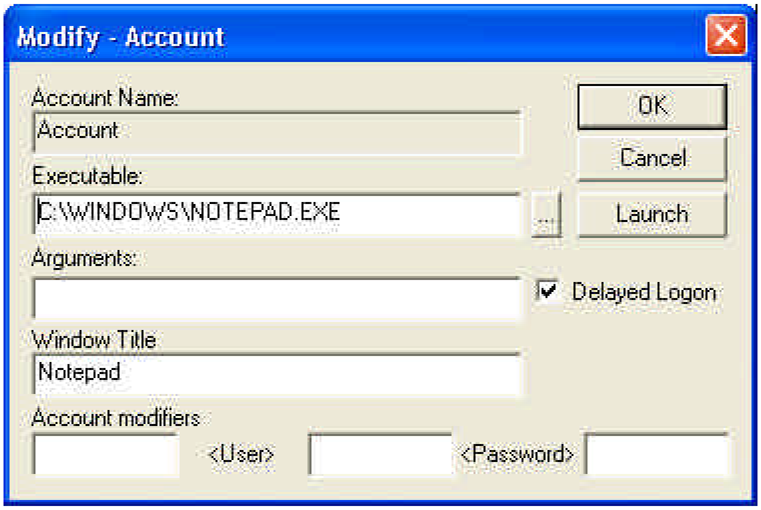
   The **Launch** button can be used to test that the correct file is being launched and to verify the Window Title.

5. Enter any arguments to be passed to the application in the **Arguments** field. For example, if the executable file is Internet Explorer (C:\Program Files\Internet Explorer\IEXPLORE.EXE) then the URL for the user account login page would be passed as an argument (http://www.ETrade.com).

6. The **Delayed Logon** checkbox should be used anytime the logon screen associated with an application may take an extended period of time to load. For example, when logging into a user account through a webpage, the login page for the website may take several seconds to fully load in the web browser. In this case, the **Delayed Logon** checkbox must be selected. This will enable the user to complete the automated logon process by clicking a "Logon" button once the web page has finished fully loading.

7. In the **Window Title** field, enter the application window title for the window that contains the username/password fields.

   Each application window on the user desktop has a title. The window title for an application window may change as a result of a change in the state of the application. For example, if Internet Explorer is used to browse to the E*Trade home page, the window title will be *E*TRADE Financial*. However, if the same browser window is then used to browse to the CNN.com home page, the window title will change to *CNN.com*. In the picture below, the window title is "Modify – Account".



Account Name: Account

Executable: C:\WINDOWS\NOTEPAD.EXE

Arguments:

☑ Delayed Logon

Window Title: Notepad

Account modifiers <User> <Password>

8. The **Account Modifiers** tell the Trio Launch software how to move the cursor inside the Window to the fields in which the username and password should be entered.

   For example, to sign in to the Mail2Web (http://www.mail2web.com), the account modifiers would be as follows:

   - The first account modifier would be **&2t**. The Trio Launch software should execute two tabs which will position the cursor in the "Your Email Address" field of the Mail2Web webpage.
   - The Trio Launch software would then enter the username.
   - The second account modifier would be **&t**. A single tab will reposition the cursor to the "Password" field.
   - The Trio Launch software would then enter the password into the "Password" field.
   - An **&r** is entered in the final account modifiers field. This will cause the "Check Mail" button to be pressed, completing the login sequence.

   Any combination of key codes may be entered in the Account Modifiers fields. In addition, a digit, N, entered between the & and the key code will cause that key code to be executed N times. As in the example above, **&2t** causes the Trio Launch software to "type" the tab key twice. See "**Appendix B: Key Codes Listing**" for a list of valid key codes that may be used.

Trio Vault: Desktop Logon

Once the components of Trio Vault™ are installed and the computer is restarted, the Trio Vault Desktop Logon system will take over the normal computer logon sequence (if the user selected this option during installation). The Desktop Logon system listens for a logon request from the PDA and will determine if the account information (username, password, and optionally a domain) that is passed to the Logon system is valid. If so, the Logon system will start the user's application desktop. If the account information is not valid, the Logon system will remain at the startup screen and will continue to listen for another request from the PDA.

The Trio Vault™ Desktop Logon utility is only available on Window NT-based operating systems (Windows NT, 2000, and XP). This utility replaces the normal default logon system that is provided in Windows. The Trio Vault™ Desktop Logon utility adds more security to the computer by requiring use of the PDA to authenticate the user, and then use of the PDA to logon to the particular computer system.

Communication Types

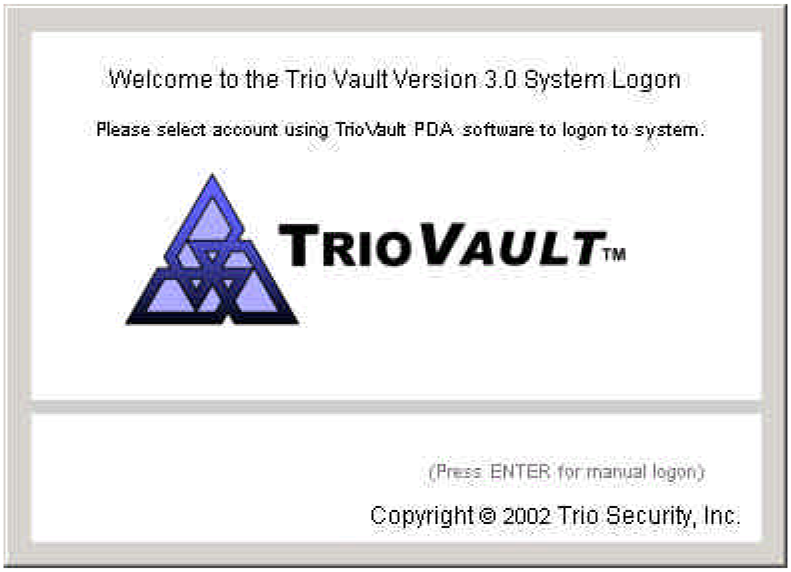
There are 3 communication modes that the Desktop Logon utility supports:

- Serial Port (COM1 – COM4 only)
    - Windows NT 4.0
    - Windows 2000
    - Windows XP
- USB (Universal Serial Bus)
    - Windows 2000
    - Windows XP
- Infrared
    - Windows NT (with the appropriate IR drivers)
    - Windows 2000 (drivers default in OS)
    - Windows XP (drivers default in OS)

Both the Serial Port and USB connections require a PDA cradle. For infrared communications, the computer must have an infrared transceiver and the operating system must support the IR drivers for that communication mode.

User Logon After Computer Boot

The Desktop Logon system will display the following screen after booting of the computer:



Welcome to the Trio Vault Version 3.0 System Logon

Please select account using TrioVault PDA software to logon to system.

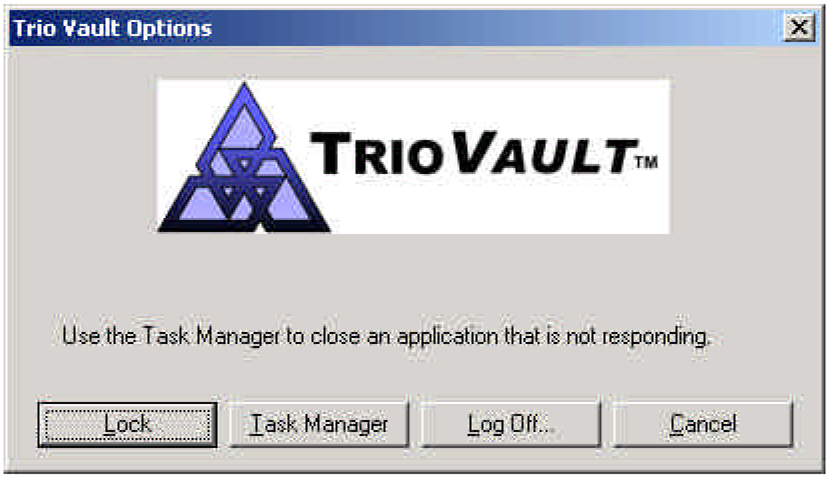
(Press ENTER for manual logon)

Copyright © 2002 Trio Security, Inc.

If the account information sent from the PDA is valid, the Desktop Logon system will start the user's application desktop and the user may begin using the computer as normal. If the account information sent from the PDA is invalid, the user will see a momentary "blink" of the screen indicating that the information was invalid and the Desktop Logon system has returned to the "listening state", waiting for another logon request from the PDA.

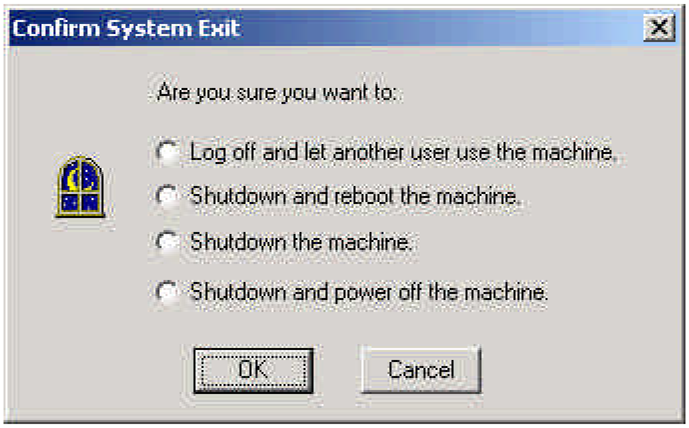
Logon after Logoff

The user may log off from the current application desktop by executing the standard Ctrl-Alt-Del key sequence. This will bring up the **Trio Vault Options** dialog.



Use the Task Manager to close an application that is not responding.

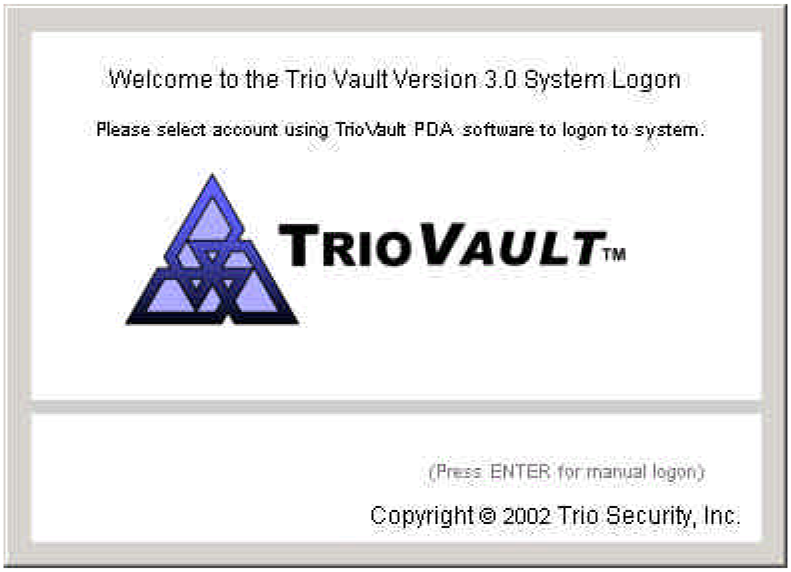
If the user selects **Log Off…**, the following dialog appears to give the standard log off options available.



Are you sure you want to:

○ Log off and let another user use the machine.
○ Shutdown and reboot the machine.
○ Shutdown the machine.
○ Shutdown and power off the machine.

If the user chooses **Log off and let another user use the machine**, the current user's application desktop will close and the Logon system will display the Desktop Logon screen.



Welcome to the Trio Vault Version 3.0 System Logon

Please select account using TrioVault PDA software to logon to system.

(Press ENTER for manual logon)

Copyright © 2002 Trio Security, Inc.

Workstation Lock / Unlock

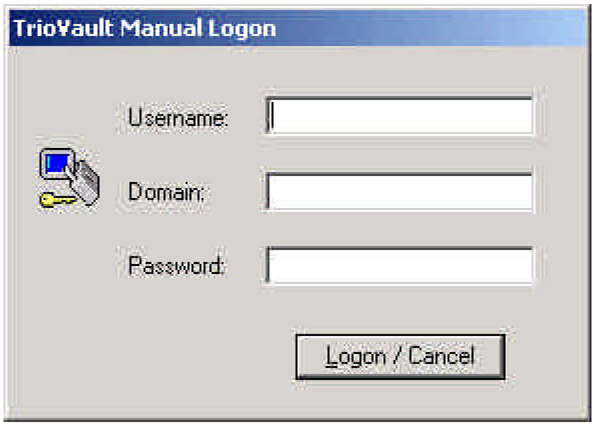
Again, by executing the standard Ctrl-Alt-Del key sequence, Trio Vault allows the user to take advantage of the standard Windows Workstation Lock system to disable the current application desktop while continuing to allow programs to run in the background. This is useful if the user wishes to leave the area where the computer is located, but does not wish to logoff or turn off the computer.

Screen Saver Mode

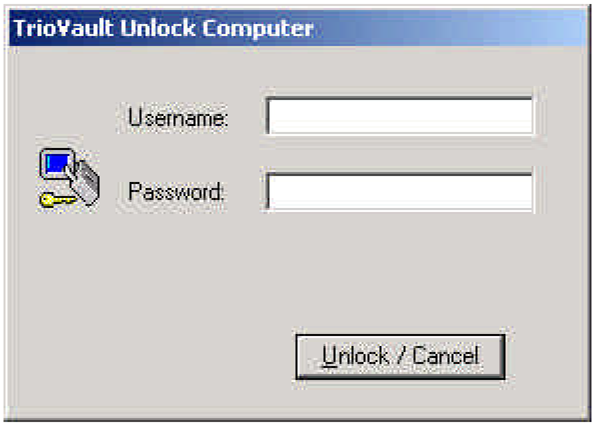
If the user has set up a password protected screen saver, the Desktop Logon system will become active after the user presses a key or moves the mouse to get back into the computer.

Manual Logon and Unlock

Trio Vault™ does allow a manual process to logon to the computer. The manual process is similar to the default Windows Desktop Logon sequence; however, instead of using "Ctrl-Alt-Del", the Trio Desktop Logon system requires the use of the "Enter" key. The Logon system will listen for the Enter Key and will display the following dialog:



If the user has the computer locked and depresses the Enter Key, the following dialog appears:



Notice that in this case, the “Domain” is not required (same as the default Windows version).

Trio Vault FAQ

Q: "Use USB" is not selectable in the Trio Launch software.

A: Make sure that a USB compatible version of the Palm Desktop software is installed. If you are using Windows NT, Windows 2000, or Windows XP then the Palm Desktop software must be installed separately for each user account.

Q: How do I turn off Windows from automatically entering data into edit boxes on web forms?

A: Microsoft Windows can optionally fill in usernames on forms (e.g., web forms). This feature interferes with Trio Launch, and must be turned off. To turn it off:

- go to the "Start" menu
- click on "Control Panel"
- click on "Internet Options"
- click on "Content"
- click on "AutoComplete..." button
- make sure this checkbox is not checked: "User names and passwords on forms"

Troubleshooting Guide

Known Issues

1. **Disable "Stay On In Cradle"** option does not work on Kyocera 6035.

PDA Application

1. **The software indicates that it will not work with a Palm OS version earlier than version 3.5.**

    a. You must upgrade your Palm OS version to 3.5 or later. To check your current Palm OS version, select Menu|Info|Version on your PDA device.

Trio Launch

1. **My Internet browser automatically completes my username and or password.**

    b. The AutoComplete settings should be disabled. To disable AutoComplete in Internet Explorer, choose **Tools->Internet Options**. Choose the **Content** tab. Under Personal Information, click the **AutoComplete** button. Deselect "Username and passwords on forms". Click **Clear Forms** and **Clear Passwords** under Clear AutoComplete History. NOTE: The exact procedure will vary by Internet browser version and vendor. The procedure above is meant to be representative of the steps that should be followed.

2. **I cannot get the PDA to communicate with the PC. The PDA always returns the error "The PDA could not communicate with the PC."**

   c. The Trio® server may not be started, or may need to be reset. Right-click on the Trio® icon in the system tray next to the time in the lower right corner of the screen. Select "Start Server" if available in the popup menu. If not, select "Stop Server" and then restart the server by selecting "Start Server" in the popup menu.

Miscellaneous

1. **The communications mode "IR to a PC" does not work. The PDA always returns the error "The PDA could not communicate with the PC."**

   a. Make sure that the latest version of Palm Desktop is installed on the PC. Early versions of the Palm Desktop did not include support for infrared communications.

   b. Attempt to perform a Hotsync® operation using the infrared port. If this is unsuccessful, consult the Palm Desktop documentation describing how to complete an infrared Hotsync® operation.

2. **I cannot get the PDA to communicate with the PC and I am using the PalmConnect USB Adapter.**

   c. The Trio Vault™ software does not support the PalmConnect USB Adapter at this time.

Appendix A: Key Codes Listing

This is the list of key codes that can be used when setting up the Application Launch program.

&&	Enters a '&'
&t	Enters a tab
&r	Enters a RETURN
\\	Enters a '\'
\109	Shift-Tab
\209	Ctrl-Tab
08	BACKSPACE key
09	TAB key
0C	CLEAR key
0D	ENTER key
13	PAUSE key
14	CAPS LOCK key
1B	ESC key
20	SPACEBAR
21	PAGE UP key
22	PAGE DOWN key
23	END key
24	HOME key
25	LEFT ARROW key
26	UP ARROW key
27	RIGHT ARROW key
28	DOWN ARROW key
29	SELECT key
2A	PRINT key
2B	EXECUTE key

2C	PRINT SCREEN key
2D	INS key
2E	DEL key
2F	HELP key
30	0 key
31	1 key
32	2 key
33	3 key
34	4 key
35	5 key
36	6 key
37	7 key
38	8 key
39	9 key
41	A key
42	B key
43	C key
44	D key
45	E key
46	F key
47	G key
48	H key
49	I key
4A	J key
4B	K key
4C	L key
4D	M key
4E	N key
4F	O key
50	P key

51	Q key
52	R key
53	S key
54	T key
55	U key
56	V key
57	W key
58	X key
59	Y key
5A	Z key
5B	Left Windows key (Microsoft® Natural® keyboard)
5C	Right Windows key (Natural keyboard)
5D	Applications key (Natural keyboard)
6A	Multiply key
6B	Add key
6C	Separator key
6D	Subtract key
6E	Decimal key
6F	Divide key
70	F1 key
71	F2 key
72	F3 key
73	F4 key
74	F5 key
75	F6 key
76	F7 key
77	F8 key
78	F9 key
79	F10 key

7A	F11 key
7B	F12 key
7C	F13 key
7D	F14 key
7E	F15 key
7F	F16 key
80H	F17 key
81H	F18 key
82H	F19 key
83H	F20 key
84H	F21 key
85H	F22 key
86H	F23 key
87H	F24 key
90	NUM LOCK key
91	SCROLL LOCK key