



SecureSuite™ XS

Advanced Authentication Software

Workstation Guide

Notices

Specifications may be changed without notice. This document is provided for informational purposes only. I/O Software, Inc. makes no warranties, either express or implied, as to the accuracy of this document. The entire risk of the use, or the results of the use, of this product remains with the user. This product may have a small possibility of granting access to persons other than those who have registered their security token. In no event shall I/O Software, Inc. or our representatives be liable for any incidental, consequential or special loss arising from granting an access to persons other than those who have registered their security token. In no event shall I/O Software, Inc., or our representatives, be liable for any incidental, consequential or special loss arising from any use, defect, malfunction, or fault of this product.

Version 4.0

I/O Software, Inc.

http://www.iosoftware.com

Table of Contents

Chapter 1: Welcome to SecureSuite

About the Guide

The SecureSuite XS User's Guide is designed to introduce and familiarize you with SecureSuite's many features and applications. It also provides the information necessary for you to customize SecureSuite to meet your specific needs and security requirements.

This manual has been divided into 12 chapters, providing an overview of SecureSuite as well as operating instructions for the various SecureSuite applications.

- *Chapter 1: Welcome to SecureSuite* introduces you to the *SecureSuite XS Workstation Guide*. It also defines the minimum system requirements for a SecureSuite XS installation, important naming conventions, and where to look when you need more information.

- *Chapter 2: SecureSuite Overview* provides an overview of SecureSuite and it's features.

- *Chapter 3: Installing SecureSuite XS Workstation* explains the SecureSuite installation process, including the initial logon procedure.

- *Chapter 4: SecureSuite Key Features* explains some important features of SecureSuite, such as credential caching, RAS support, system binary verification, and password randomization options.

- *Chapter 5: Using SecureSuite* describes the main functionality of SecureSuite, including detailed instructions and tips.

- *Chapter 6: Account Management* explains how to set up and maintain your own user account, including how to set your user-level policies and manage your authentication methods.

- *Chapter 7: System Administration* explains how to set up the SecureSuite

User Manager, add a new user account to SecureSuite, and make new methods of authentication available.

- *Chapter 8: SecureSuite System Settings* describes the various system properties, including system policies, device management, event logging, database management, SecureFolder policies, SecureSession policies, communication settings, and logon settings for identification devices. It also covers the basics of how to secure applications with SecureLaunch.

- *Chapter 9: SecureSession* explains how to use the "password bank" and account management functionality of SecureSession for Internet Explorer for web sites and SecureSession for Applications for Windows applications.

- *Chapter 10: SecureFolder* explains how to use SecureFolder, a SecureSuite application that provides security for files and folders.

- *Chapter 11: SecureLaunch* explains how to set and remove restrictions in order to prevent unauthorized users from running Windows applications.

- *Chapter 12: SecureSuite Program Maintenance* explains how to modify, repair, or uninstall SecureSuite.

- The Appendices include supplemental material that provides quick access to important information. Appendix 1 lists common user problems and troubleshooting techniques. Appendix 2 contains a glossary, which covers important terms used in SecureSuite. Appendix 3 contains a table of SecureSuite policies.

Naming Conventions and Typefaces

Information within this guide is clearly structured with descriptive instructions as well as many step-by-step examples on how to implement or configure a particular feature. These are supplemented with graphics that make the instructions easy to follow.

Note: Notes generally represent information that requires special attention. Notes in the manual will be displayed in this typeface.

More Info: References to other books and sources of information are offered throughout the manual.

Important: These notes contain important warnings about the subject at hand – critical information about the security of your system.

Specific names and instructions (as they appear on your computer screen) are displayed in this typeface.

System Requirements

Requirements	Recommendations
Windows 2000 w/ SP1 Windows XP Professional or Windows XP Home Edition	Windows 2000 w/ SP2 Windows XP Professional
For SecureSession for Internet Explorer, IE 4.x or above	Internet Explorer 6.0 or above
At least one network client service installed, with TCP/IP available	MS client for MS networks and TCP/IP
Pentium II-350 or better	Pentium III-700 or better
128 MB of RAM	256 MB of RAM
30 MB of free hard disk space	30 MB of free hard disk space
For client/server functionality, the domain must have DNS capability	

Table 1: System Requirements

Additional Information

Refer to the **SecureSuite Release Notes** for the most current information and general issues. The **Release Notes** are available during installation. To view the **Release Notes** after installation, from the **Start** menu, select **Programs**, **SecureSuite** and click **SecureSuite Release Notes**.

Chapter 2: SecureSuite Overview

SecureSuite is an enhanced security software solution that seamlessly integrates with the Windows 2000 and Windows XP operating systems to provide biometrically enabled user authentication services and additional functionality. SecureSuite supports stand-alone workstation installations, as well as full client/server functionality. SecureSuite is the most comprehensive biometric security solution available on the market today, supporting the largest number and widest variety of biometric and non-biometric authentication devices.

Computer security has traditionally been based on two authentication methods: Something you know (e.g., passwords) and something you have (e.g., smart cards, tokens). In recent years, a third method of security has emerged: Something you are, known as biometrics. With biometrics, users can verify their identity via unique physical characteristics, such as their fingerprint, iris, retina, hand, face, or voice.

SecureSuite XS is an integrated 4-in-1 software package that provides a suite of security applications for Windows 2000 and Windows XP. SecureSuite's scalable authentication infrastructure improves security, enhances user convenience, reduces costs and increases productivity. SecureSuite is unique in that it allows users to utilize a wide range of powerful and secure authentication methods such as passwords, biometrics, smart cards, token devices, and any combination of these. These advanced authentication methods can be used to control access to sensitive files and applications. In addition to enhancing standard logon procedures, SecureSuite includes SecureSession, SecureLaunch, and SecureFolder, providing powerful tools that are necessary for the security and productivity of your PC.

SecureSuite Highlights

SecureSuite provides system administrators with a complete set of tools for managing user accounts and controlling access to information via an intuitive and easy-to-use software package. SecureSuite also addresses the need for a robust and rich set of security services users once they are logged on to a domain. SecureSuite's functionality includes:

- SecureSuite enables deployment of a wide range of biometric and non-biometric authentication technologies through single-factor and multi-factor authentication.
- SecureSuite seamlessly supports the Windows 2000, Windows XP Professional and Windows XP Home platforms.
- SecureSuite is highly scalable, supporting a single user in one location to members of an enterprise scattered around the globe.

- User-friendly wizards facilitate the installation and enrollment of authentication methods including smart cards, tokens or biometric devices.

- SecureSuite provides efficient administrator tools, such as the **SecureSuite User Manager**, which enables full user management, from system policies to biometric enrollment.

- SecureSession captures and stores information for application windows and web sites, and releases the information upon authentication.

- SecureFolder allows you to easily protect files with strong encryption. The locking/unlocking of directories and the encryption/decryption of files can be activated by a SecureSuite-compatible authentication device.

- With SecureLaunch, Windows-based applications can easily be secured to prevent unauthorized use.

- Credential caching allows credentials from the last successful logon to a remote domain to be stored on the client computer. This allows users to log on to client computers in the event that they are disconnected from the network or if all the domain controllers are down.

- SecureSuite supports Remote Access Service (RAS) connections. Using a RAS connection via a modem, a client computer can operate as if it were physically connected to a LAN.

- Administration is easy and powerful using the native MMC-style snap-ins for system policy and user account management.

- Password randomization options allow system administrators to enable or disable SecureSuite management of user passwords. This feature is invisible to the user and, when enabled, enhances system security. Refer to *Chapter 4: SecureSuite Key Features* for a detailed explanation of this feature.

- SecureSuite administrators can quickly and easily view event-logging details. An administrator can use **Event Viewer** to view and manage system security and application event logs.

- One-Touch Logon Support provides users with single sign-on capabilities with all SecureSuite applications.

- SecureSuite is BAPI (Biometric Application Programming Interface) compliant.

This sophisticated and empowering suite of security features and applications offers advanced security via a wide range of authentication methods. Following is a list of the security applications available with SecureSuite:

SecureLogon: SecureLogon enhances the normal logon procedure for Windows, enabling you to log on to your system securely and easily using one or multiple authentication methods and devices supported by SecureSuite.

SecureSession: SecureSession is composed of two applications:

- SecureSession for Applications (SecureSession/Apps) stores passwords and other text-based information for application windows, and enters the information for you.

- SecureSession for Internet Explorer (SecureSession/IE) stores authentication information, such as user names and passwords for web sites, and enters it for you.

SecureFolder: SecureFolder is a powerful, fast and convenient way to protect data. With a right-click you can secure folders, allowing only authorized users to view the contents. SecureFolder also encrypts individual files. Secured folders look and function like other Windows folders: You can "drag and drop" files into and out of the secured folder. All of the security functions in SecureFolder take place quickly and transparently. SecureFolder also includes an emergency data recovery utility for use in the event that some or all data encryption/decryption keys are lost.

SecureLaunch: SecureLaunch prevents unauthorized users from running Windows applications. Administrators can secure most programs, and set access permissions for individual users or groups of users. This application is very convenient for accounting software and databases that contain sensitive or confidential information, or for controlling usage of games and entertainment software.

Architecture

This section provides an overview of product operation, including details about SecureSuite XS Server, SecureSuite XS Workstation, and SecureSuite user roles.

SecureSuite XS Workstation vs. SecureSuite XS Server

SecureSuite XS Workstation: SecureSuite XS Workstation is a complete package that can operate with or without SecureSuite XS Server installed. SecureSuite XS Workstation provides all the user applications and authentication software for a stand-alone workstation. It automatically detects the SecureSuite XS Server (if installed) and then acts as a client.

SecureSuite XS Server: SecureSuite XS Server is a server application designed to support an Active Directory domain. As in the Windows domain model, SecureSuite XS Server provides centralized user management and authentication services. Many of these services are also accessible from domain clients. In addition, the standard functionality of the domain model is also supported including user roaming and server fail-over protection.

SecureSuite User Roles

SecureSuite defines two distinct user roles that are equivalent to the corresponding Windows user groups:

- **Administrator** – Installs and maintains software on systems, manages user accounts, manages authentication methods and associated devices, and manages security and related policies.

- **User** – A standard resource user. No special privileges or abilities.

Refer to Microsoft Windows documentation for more information on group memberships.

Chapter 3: Installing SecureSuite XS Workstation

Prior to running the installer, please verify that you have at least one network client installed on the target system. This can be verified by viewing the properties of any available connection in **Network Neighborhood** or **My Network Places** by right-clicking the connection icon and selecting **Properties**. If **Client for Microsoft Networks** (or something similar) is not listed, click the **Install** or **Add** button, then select **Client** and press **OK**. The list of available clients will then be available. We highly recommend that you select **Client for Microsoft Networks**. If no connection is available or established, please contact your system administrator.

Installation

Important: Software installation requires local administrator privileges in the case of a workstation-only setup, or domain administrator privileges for domain installations. Before installing SecureSuite, close all applications and disable your virus detection software.

Important: Please refer to the Sony® Puppy® installation guide ("Training Your Puppy Unit") included in your package or on the CD-ROM for specific instructions on the installation and use of your fingerprint identity device.

To install SecureSuite:

1. Insert the SecureSuite CD into your CD-ROM drive. Wait for the installation to start automatically.
2. If the software does not auto-initiate, select **Start** from the taskbar and then click **Run**. In the **Run** dialog, type **D:\Setup.exe** (where **D** is the drive letter for your CD-ROM drive or other source media).
3. Follow the onscreen instructions, which are outlined below.

Welcome: Click **Next** to continue.

License Agreement: You must accept the terms of this license agreement by checking the **I accept the terms in the license agreement** check box to proceed with the installation. Click **Next** to continue.

Product License Key: Enter the product license key provided on a label on the SecureSuite CD envelope. Click **Next** to continue. If the product license key entered is invalid or already in use, you will be prompted to enter a new one after restarting your system.

Release Notes: Select the **Yes** check box to review the **Release Notes** for important information about installing and using SecureSuite. If you deselect this check box, you may view the **Release Notes** at a later time. Click **Next** to continue.

Customer Information: Enter your name and company information. Click **Next** to continue.

Complete or Custom Setup: Choose the type of setup that best suits your needs. If you select Custom Setup, you can select the program features that you want installed. You can accept the default destination, or click the **Change** button to select an alternate path, to which SecureSuite files will be installed. Complete Setup will not allow for any modifications. Click **Next** to continue.

Shortcut Icon: Select the **Create a SecureSuite desktop icon** check box to have a SecureSuite shortcut group icon placed on your desktop, from which you can access all SecureSuite functionality. Click **Next** to continue.

Install: Click **Install** to initiate the installation process.

Device Setup: If you are installing an authentication device module at this time, you will be instructed to connect your authentication device. Refer to the *Installing OEM Device Modules* section in Chapter 12 of this manual for more information.

Restart: Click **Yes** to restart your machine.

You have completed your software installation. Once your machine restarts, any user who previously existed on the system will have now become “SecureSuite enabled”. To log on to your system, supply your Windows password, which existed before installing SecureSuite.

Initial Logon Procedure

To log on to your system after installation:

1. Press **Ctrl + Alt + Delete** as prompted by the **SecureSuite Authentication** dialog.
2. Enter your user name and password.
3. Click **Options** to change the target domain on which to authenticate. Select the **Authentication Details** check box to view instructions specific to your account.
4. Click **OK** or press **Enter** when finished.

Note: On some systems running Windows 2000 and XP, it is not necessary to press **Ctrl+Alt+Delete** as it may be disabled. Consult your Windows documentation for more information.

The SecureSuite Welcome Screen

Upon successful authentication, your desktop will appear and you will see the **SecureSuite Welcome Screen**. From this screen, you can register your SecureSuite software, create a new user account, or exit to the desktop.

Register SecureSuite: Click this tab to register SecureSuite and take advantage of product update notifications and technical support. Your Internet connection must be active in order to register SecureSuite.

Manage Users: Click this tab to create a new user account. You will be taken directly to the **Local Users and Groups** dialog, from which you can enroll new SecureSuite users.

Exit to the Desktop: Click this tab to close the **Welcome Screen**.

Deselect the **Show this dialog at startup** check box if you do not want the **Welcome Screen** to appear each time you log on.

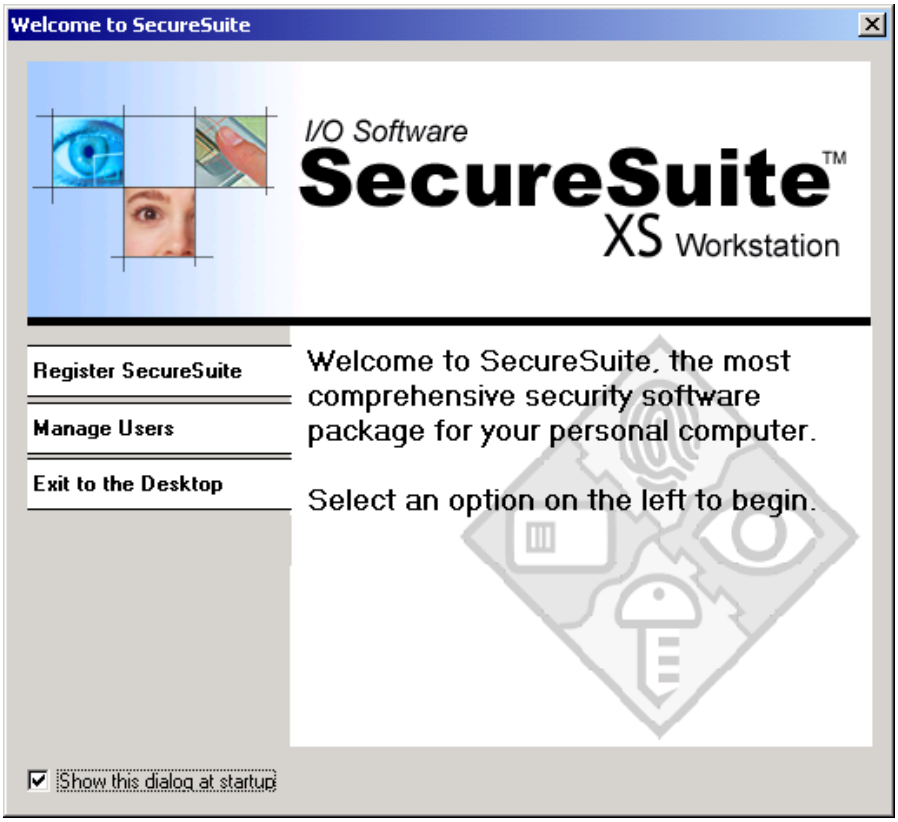

Figure 1: SecureSuite Welcome Screen

Chapter 4: SecureSuite Key Features

System Integrity Verification

On every system restart, SecureSuite makes sure all installed SecureSuite binaries have not been tampered with, replaced, etc. If any corrupt or missing files are detected, SecureSuite will display a message alerting you of the problem. At this point, only an administrator will be able to log on to the computer and either repair or uninstall SecureSuite via the Windows **Add/Remove** application in the **Control Panel**, or by re-running the SecureSuite installation program (**Setup.exe**).

RAS Support

SecureSuite supports Remote Access Service (RAS) connections. Using a RAS connection, a client computer can operate as if it were physically connected to a LAN. RAS makes it possible to connect a remote client workstation to a network server. This can be accomplished over a Wide Area Network (WAN) link or a Virtual Private Network (VPN) using a dial-up connection. The user authentication required in order to establish RAS and/or VPN connections are not controlled by SecureSuite.

The user may notice a delay corresponding to certain activities. The initial logon will take longer. Use of some SecureSuite features may also take longer as the bandwidth available over RAS is limited compared to that available over Ethernet or other network topology.

Policy Management

A computer's configuration is defined in terms of policies. A policy is a permission or attribute for a particular item, action, or object. The ability to consistently manage policies is an essential feature in SecureSuite. All administrator tools are centralized and easy to use. This will lead to lower administration overhead and an enhanced network/server security system. SecureSuite defines four levels of policies: system-level policies, user-level policies, application policies, and user-level application policies. For the two SecureSession applications, there is a another level of policies called "site-level" or "application-level" policies, which are only relevant for and applied to the website or application for which they are set. The settings of some policies affect (and are affected by) the settings of others. See *Appendix 3: A Table of SecureSuite Policies* for an overview of the policies and the dependencies they have on each other.

Credential Caching

Credential caching is a feature that allows the credentials of the last successful logon to a remote domain to be securely cached (stored) on a client computer. This policy can be enabled at the system level, or set per user via the **SecureSuite User Manager**. If the client computer should become disconnected from the network or if no authentication servers are available, the last 10 users who successfully authenticated to the remote domain can perform the same logon procedure and have the standard user desktop available (the user will not be able to access the network). This is a convenient feature for those who plan to travel with their workstation. Credentials uniquely identify a user within the scope of a domain. Credential-cached logon compares submitted credentials against the credentials that have been stored on the computer. You can configure credential-caching policies through the **SecureSuite System Properties** dialog, discussed later in this manual. By default, the credential caching policies are enabled. These policies will be available to remote domain users only. They will not appear on local machines (stand-alone workstations).

Randomize Password

Password randomization is a powerful security feature that provides maximum protection against password-based security attacks. This feature will automatically change a user's Windows password to a secure random password every time the user authenticates. This prevents users from accessing SecureSuite protected network resources from workstations that do not have SecureSuite installed. The randomization process takes place without user knowledge or participation.

You can configure password randomization policies for all users and for **AND** users through the **SecureSuite System Settings** dialog discussed later in this manual. If password randomization is set as **User Defined** at the system level, then you can also enable or disable password randomization for each individual user via the **SecureSuite User Manager**. By default, password randomization is disabled (user defined) for all users, enabled for **AND** users, and disabled for each individual user.

Logon time

Placing your cursor over the SecureSuite icon in the system tray will display how long the current user has been logged on to the system.

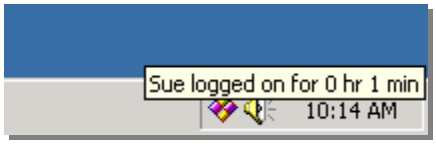

Figure 2: SecureSuite Logon Time

Windows System Tray

SecureSuite adds a SecureSuite shortcut icon to the Windows system tray. The SecureSuite system tray icon allows you to access most SecureSuite functionality quickly and conveniently. If enabled, the SecureSession for Applications icon and any method icons will also appear in the system tray.

SecureSession for Applications Icon

The SecureSession for Applications icon allows users to register and manage SecureSession data. See the *SecureSession for Applications* section in Chapter 9 of this manual.

Authentication Method Icons

If the logged-on user is associated with a biometric authentication method that fully supports the concept of multiple sources (e.g., two or more fingerprints, each one being a source), the method's system tray icon may be displayed in the system tray. From the SecureSuite shortcut icon (represented by the SecureSuite logo), a user can choose to show or hide method icon(s) by checking or unchecking the **`Show SecureSuite Method Icons`** option (which will only be available if the user is enrolled with at least one method that supports this feature).

When a user clicks the method icon, a dialog appears that allows the user to select their current and/or default source during the authentication process. In the case of the fingerprint method, the dialog will typically contain a graphic of two hands with all 10 fingers represented. These method-specific source dialogs indicate all sources that have been enrolled for that authentication method. For example, a red dot on the tip of a finger signifies that the fingerprint is currently selected for authentication. To select a different fingerprint, click the corresponding finger.

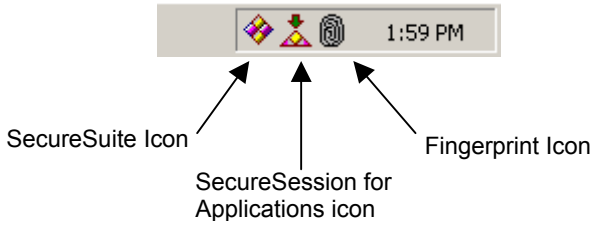

Figure 3: Fingerprint Icon, Windows System Tray

Chapter 5: Using SecureSuite

SecureSuite License Manager

The **SecureSuite License Manager** is an easy-to-use tool for managing your Product License Key and User License Keys.

The License Manager Properties Dialog

From the **SecureSuite License Manager Properties** dialog, administrators can enter a new Product License Key in order to upgrade SecureSuite and utilize features that may be disabled in a demo or evaluation version, or add new User License Keys.

To access the **SecureSuite License Manager Properties** dialog:

1. From the **Start** menu, select **Programs**, **SecureSuite**, and click **SecureSuite License Manager**.
2. Double-click **SecureSuite License Manager** in the right pane. The **SecureSuite License Manager Properties** dialog appears.

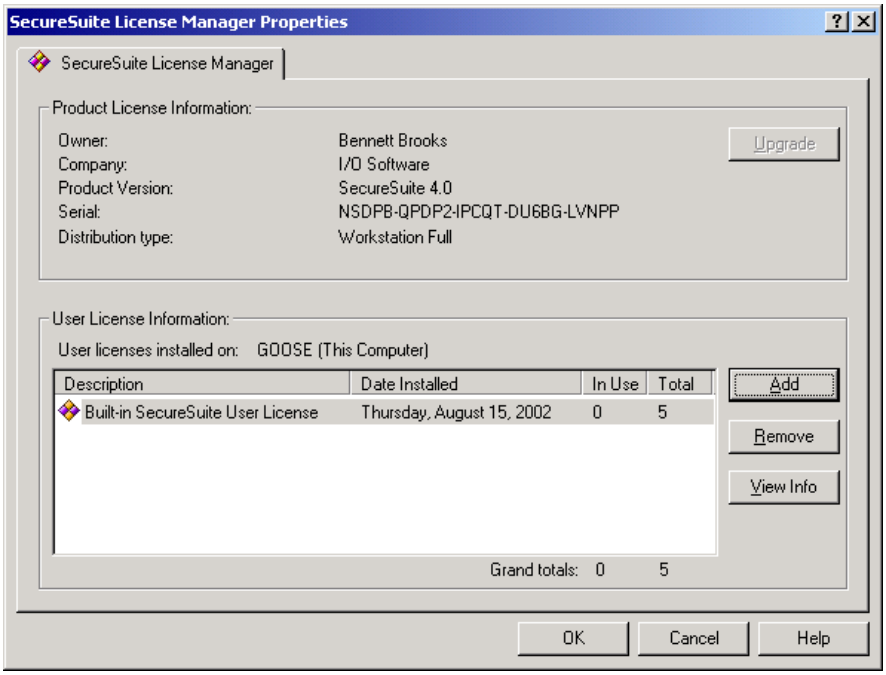

Figure 4: SecureSuite License Manager

Product License Keys

Your SecureSuite Product License Key, which you received with your SecureSuite software for use during the installation process, is synonymous with a serial number. You must have a valid, unique Product License Key in order to install and use SecureSuite. This Product License Key determines the version of your SecureSuite installation.

To enter a new Product License Key in order to upgrade your version of SecureSuite:

1. In the **SecureSuite License Manager Properties** dialog, click the **Upgrade** button. The **Upgrade Product License** dialog appears.

2. Enter your new Product License Key, and click **OK**.

3. Click **Yes** when prompted to reboot your computer. When your system restarts, SecureSuite will be upgraded according to the Product License Key entered.

User License Keys

With SecureSuite installed on your system, all users may use the password method for authentication. However, in order for a user to employ any other authentication method supported by SecureSuite, a user license must be available. Each user license enables a single user to have any SecureSuite-related authentication method (or combination of methods) assigned to their account. Enrolling a single user with multiple methods does not use multiple user licenses. That is, once a SecureSuite user is assigned one user license, they can have any number of authentication methods and devices assigned to their account.

To enter a new User License Key:

1. In the **SecureSuite License Manager Properties** dialog, click the **Add** button. The **Add User License Key** dialog appears.
2. Enter your new User License Key, and click **OK**.
3. Click **Yes** when prompted to reboot your computer. When your system restarts, your new User License Key will be available.

To remove a User License Key from your system:

1. In the **SecureSuite License Manager Properties** dialog, select the User License Key that you want to delete from your system, and click the **Remove** button.
2. The User License Key will no longer appear in the **SecureSuite License Manager Properties** dialog.

Note: If any user licenses from the User License Key that you are trying to remove are still in use, SecureSuite will search for available user licenses from other User License Keys, and assign them to the users. If there are no other available user licenses, a message will appear informing you that there are not enough user licenses to transfer to these user accounts. You will not be able to delete this user license key until another user license is available or until none of the licenses from this User License Key are assigned to users.

To view a description of a User License Key, and the license number itself, select the User License Key and click the **View Info** button.

Duplicate License Keys

If SecureSuite detects that you have entered a Product License Key or User License Key that is already in use, you will receive a message asking if you would like to enter a new License Key. Click **Yes** to enter a new License Key and continue using SecureSuite. If you click **No**, SecureSuite will be disabled the next time you restart your machine. You will have to log on to your system using your Windows password, at which time you will again be prompted to enter a new License Key. SecureSuite will be disabled and you will continue to receive this message until a unique License Key is provided, or until SecureSuite is uninstalled from this machine.

SecureSuite User Authentication

SecureSuite is an advanced authentication infrastructure designed to provide secure and convenient forms of authentication. Before allowing users to access a protected computer, application, web site, file or folder, SecureSuite will prompt them to authenticate (prove who they are) via an authentication dialog. Depending on what authentication method(s) have been installed and enrolled with, users may authenticate using a single method or a combination of password, fingerprint, smart card, iris scan, USB token, and other advanced authentication technologies.

Figure 5: SecureSuite Authentication Dialog

Authentication Methods

An authentication method is a way of proving your identity. Typing a password is a common, but relatively insecure and inconvenient authentication method. Biometric methods, such as scanning your fingerprint, are more secure and convenient (it is hard to forget your finger!). Other methods, such as smart cards and USB tokens, are also more secure than passwords and offer other advantages, such as the ability to store data.

With SecureSuite installed on your system, you may have one or more authentication methods associated with your account. For example, Sue might use fingerprint authentication, while Bob uses only a password, and Carl has the option to use either one. The system administrator is responsible for deciding what authentication methods are assigned you.

Verification vs. Identification

In order to understand SecureSuite's authentication dialog, you must first understand the difference between verification and identification.

- Verification answers the question: "Are you who you say you are?"
- Identification answers the question: "Who are you?"

With Sony Puppy fingerprint identity devices, it is necessary to first identify yourself to the system by typing in your user name. Then SecureSuite performs a one-to-one verification process to check if you are you.

Multiple Authentication Methods

When more than one authentication method is associated with your user account, a relationship between them must be defined. This relationship is categorized into either **AND** or **OR**:

- Method 1 **AND** method 2 (greater security)
- Method 1 **OR** method 2 (greater convenience)

In the case of **OR**, only one method's credential is required in order to successfully authenticate. The user may choose which method to use each time they log on. For **AND** users, all associated authentication method credentials must be supplied for successful authentication. You supply credentials by entering a password (secret), inserting a token (put the smart card into its reader), and/or using a supplied biometric device (allow the device to scan part of you). Credentials are automatically detected. If more credentials are required, SecureSuite will prompt you for the next required authentication step. Credentials can generally be supplied in any order. However, users may specify in what order they would like to be prompted to use their enrolled authentication method.

The Authentication Dialog

To authenticate using a password:

When accessing a secured resource on a SecureSuite-protected system, the **SecureSuite Authentication** dialog will appear. To log on to your system using a password, type your user name in the **User name** text box and your password in the **Password** text box.

(Optional) Click **Options** to change the **Log on to** location to something other than the default local machine (this computer) or network domain server. You can also select the **Authentication Details** check box to view additional authentication instructions. Select the **Log on using dial-up connection** check box to log on to your system or domain by using a RAS connection. (For more information on RAS please consult your Windows Help system. For more information on RAS support in SecureSuite, please consult the SecureSuite Release Notes and SecureSuite Administrator's Guide).

Click **OK** or press **Enter** when you are done. If your password is correct, you will be successfully authenticated and logged on to the system.

To authenticate using a biometric device for verification (we use the fingerprint method as an example):

1. Type your user name in the **User name** text box.

2. (Optional) Select the domain you wish to log on to, via the **Options** button.

3. Place your fingerprint on the fingerprint device's scanning mechanism. SecureSuite will automatically detect the presence of your finger on the device, sample your fingerprint, and submit it for verification against the stored set of fingerprints created during user enrollment.

4. If your fingerprint sufficiently matches your stored fingerprint template, you will automatically be logged on to the target domain.

Figure 6: Multiple Authentication Methods, Password and Fingerprint

Like Windows, SecureSuite retains the last user name of the last user that logged on, and the domain to which that user logged on. On subsequent system boots, this information automatically appears in the **SecureSuite Authentication** dialog.

SecureSuite Icons and the Welcome Screen

SecureSuite Icons

Once you have logged on, SecureSuite will automatically place an icon in the Windows system tray, from which you can quickly access product information, help files, and your user settings. If you are an administrator, you will also be able to access the **`SecureSuite User Manager`** and the **`SecureSuite System Settings`** dialog (on Windows 2000). If enabled when SecureSuite was installed, a SecureSuite shortcut group icon will also appear on your desktop. This icon will allow you to access SecureSuite tools and references including the *SecureSuite XS Workstation Guide* and the **`My SecureSuite Settings`** dialog.

Figure 7: SecureSuite Icons and Welcome Screen

The SecureSuite Welcome Screen

The **SecureSuite Welcome Screen** will also appear. From this screen, you can register your SecureSuite software, view your user settings, or exit to the desktop.

Register SecureSuite: Select this tab to register SecureSuite in order to take advantage of product update notifications and technical support. Your Internet connection must be active in order to register SecureSuite.

My SecureSuite Settings: Select this tab to view your user account properties. You can view and manage your profile, authentication methods, secured applications, web sites and applications you have registered with SecureSession, policies, and secured files and folders.

Exit to the Desktop: Select this tab to close the **Welcome Screen**.

Deselect the **Show this dialog at startup** check box if you do not want the **Welcome Screen** to appear each time you log on.

Using the SecureSuite Help System

Use the SecureSuite Help system to get help on specific topics or dialogs.

From the **Start** menu, select **Programs**, **SecureSuite**, and click **SecureSuite Help** to open SecureSuite's Help system. You can also access Help via the SecureSuite icon in your Windows system tray or on your desktop.

Context-sensitive help topics are available by pressing the F1 key while using a SecureSuite dialog, or clicking the **Help** button in SecureSuite dialogs. When you use the What's This help button (represented by a question mark, located on the title bar of SecureSuite dialogs), context-sensitive popups will appear, giving brief descriptions of specific items (buttons, text boxes, drop-down lists, etc.).

One-Touch Logon

Some authentication methods and devices allow you to log on without pressing any keys – for example by touching a fingerprint sensor or inserting a smart card. To use one-touch logon you must be enrolled with a supported authentication method and the authentication device must be present and in working condition on the system.

Workstation Security

SecureSuite allows you to protect your computer and its contents when you are away from your desk.

Locking Your Workstation

To lock your workstation:

- Click the **SecureSuite** icon in the Windows system tray and select **Lock Workstation**.

- OR -

- Press **Ctrl** + **Alt** + **Delete** to launch the **SecureSuite Logon To Windows** dialog and click the **Lock Computer** button.

Unlocking Your Workstation

To unlock your workstation:

- Press **Ctrl** + **Alt** + **Delete** to launch the **SecureSuite Logon To Windows** dialog.

Your workstation will be unlocked after successful authentication, and your desktop will be in the same state that it was in when you locked your computer. Only the user who locked the workstation or a system administrator can unlock the workstation.

Chapter 6: Account Management

My SecureSuite Settings

My SecureSuite Settings is a SecureSuite tool that you can use to view and modify your SecureSuite account properties. From the **My SecureSuite Settings** dialog, you can:

- Select and enroll authentication methods (if an administrator has granted you permission)
- View and modify your user-level security policies
- Manage your SecureSuite application information and associated user-level policies

To Access My SecureSuite Settings:

1. From the **Start** menu, select **Programs**, **SecureSuite**, and click **My SecureSuite Settings**.
2. Authenticate if required. Your **User Properties** dialog appears.

- OR -

1. Click the SecureSuite system tray icon and select **My SecureSuite Settings**.
2. Authenticate if required. Your **User Properties** dialog appears.

Note: "My SecureSuite Settings" and **"User Properties"** are synonymous.

User Properties – SecureSuite Policies

SecureSuite's behavior is determined by a number of policies, which are typically set by a system administrator. Administrators can configure many of these policies separately for each user. Users can set some of their own policies. Which policies may and may not be modified by each user depends on the configuration options made available to each user by a system administrator. Only users who are members of the administrator group or equivalent user group can at all times modify these policies.

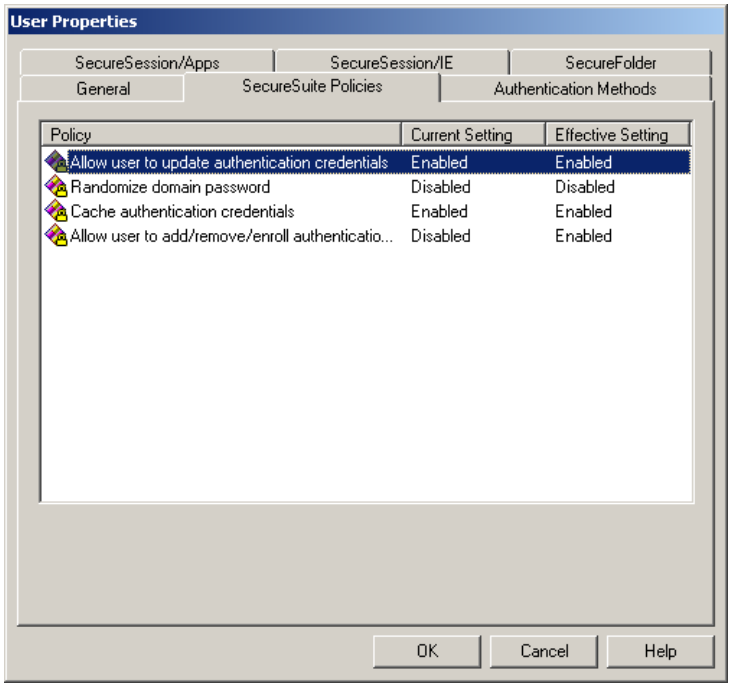

Figure 8: User Properties, SecureSuite Policies

Authentication Methods

SecureSuite allows users to verify their identities using one or more authentication methods. A user's associated (enrolled) authentication methods are listed in the **Authentication Methods** tab of their **User Properties** dialog.

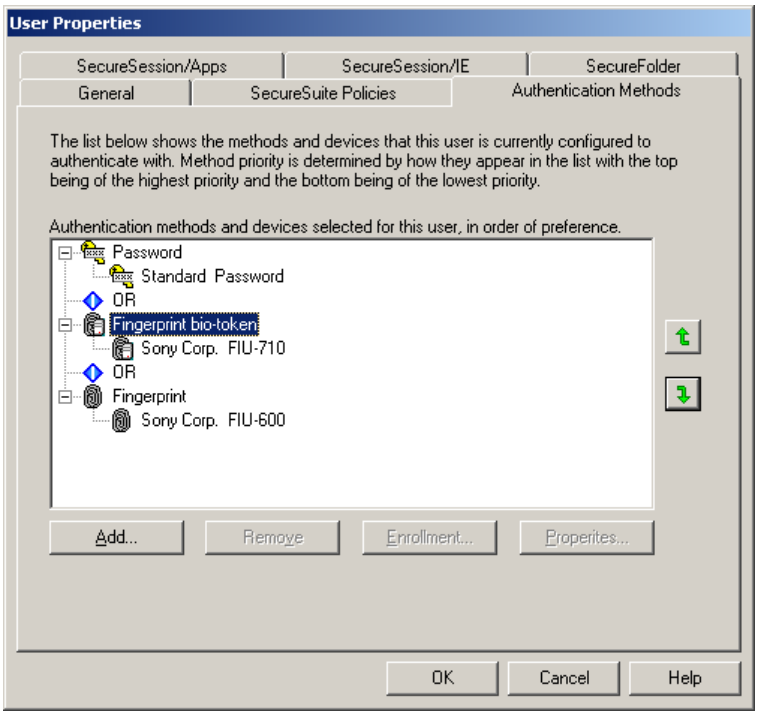

Figure 9: User Properties, Authentication Methods

The **Authentication Methods** tab of your **User Properties** dialog lists methods and associated devices with which you are currently enrolled. The only functionality you have access to is to re-enroll yourself with a selected authentication method. For example, you may change your password, or rescan your fingerprint or iris.

If more than one method is listed, a method relationship icon appears between the methods. Only administrators can change the method relationship. As mentioned above, if **AND** is specified, then all enrolled authentication methods must be satisfied in order to consider a user authenticated. If **OR** is specified as the method relationship, then you can choose which method to use each time you authenticate.

User Properties – SecureSession Policies

SecureSession is divided into two separate applications: SecureSession for Applications, and SecureSession for Internet Explorer. Both applications allow you to store text-based information that you need to enter often, and have SecureSuite enter the text for you. The following discussion refers to SecureSession in general since the information pertains to both applications. The **SecureSession** tab of your **User Properties** dialog allows you to manage your stored SecureSession data. This data typically consists of a user name and password, which are required to access an application or web site. The act of registering an application window or web form with SecureSession is called "account registration". SecureSession provides default descriptions based on application names, web site URLs, or window titles, but you can enter your own description for each account. The registration date and time are shown following the description.

- Use the **Cut**, **Copy**, and **Paste** buttons to relocate or duplicate stored information.

- To change the description of a registered SecureSession account, select the account and click the **Rename** button.

- To remove a registered account, select it and click the **Delete** button. SecureSession will no longer provide this set of information for that application window or web site.

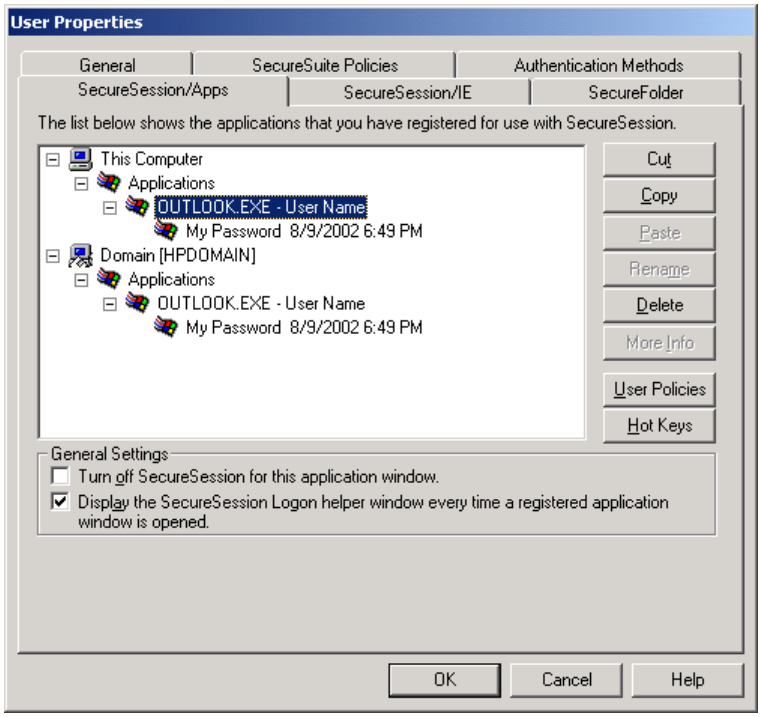

Figure 10: User Properties, SecureSession/Apps

Changing User-Level Policy Settings

Click the **User Policies** button in the **SecureSession** tab of your **User Properties** dialog to bring up the **SecureSession User Policies** dialog. From this dialog, you can set general user-level application policies, which can override account-specific (web site-specific or application-specific) policies.

To set user-level SecureSession policies:

1. From the **Start** menu, select **Programs**, **SecureSuite**, and click **My SecureSuite Settings**.
2. Select the **SecureSession/IE** or **SecureSession/Apps** tab.
3. Click the **User Policies** button. A **SecureSession User Policies** dialog appears.
4. Double-click a policy to modify its setting.
5. After setting the policy, click **OK**.
6. When you are finished setting policies, click the **Close** button in the **SecureSession User Policies** dialog.

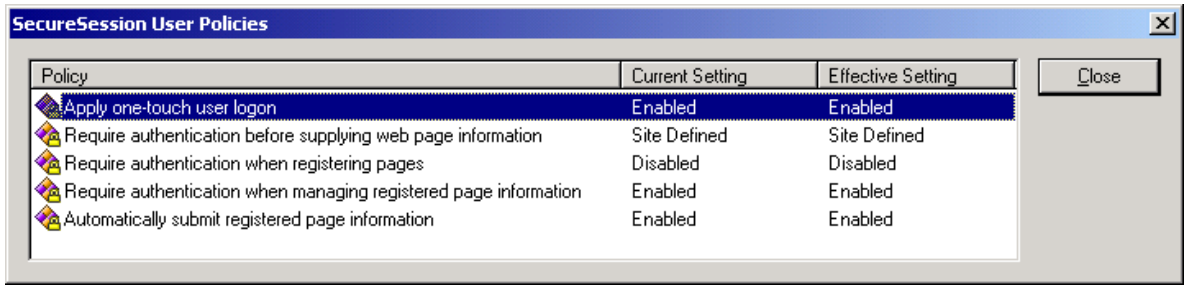

Figure 11: SecureSession User-Level Policies

Modifying Individual SecureSession Account Information

To access information for a particular registered web form or application window:

1. From the **Start** menu, select **Programs**, **SecureSuite**, and click **My SecureSuite Settings**. Your **Properties** dialog appears.

2. Select the **SecureSession/Apps** or **SecureSession/IE** tab.

3. Select the SecureSession account, and click the **More Info** button. All of the relevant registered information will be displayed in a **SecureSession Information** dialog.

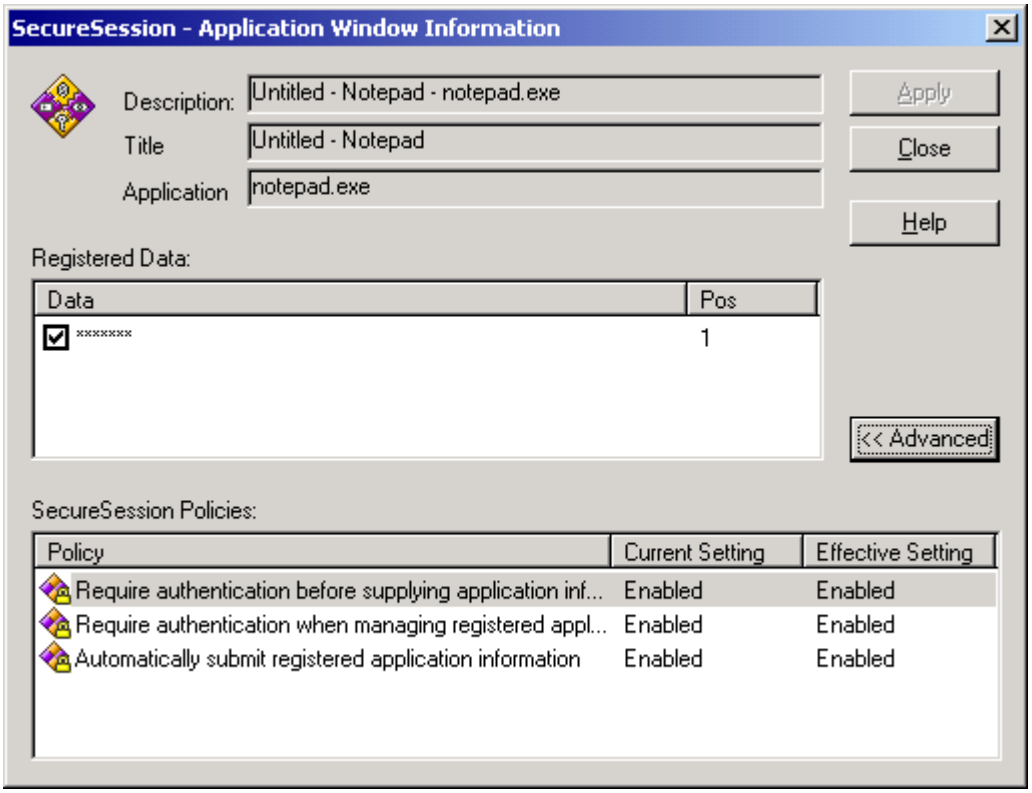

Figure 12: SecureSession/Apps, Application Window Information

If you change any information for a web site or application that you have registered with SecureSession, you will also need to update the information with SecureSession so that the correct information is provided.

To modify your stored information for an individual SecureSession account:

1. Open the appropriate **SecureSession Information** dialog (see previous instruction).
2. Make sure that the check box next to the data you are modifying is not selected, so that the data is not hidden.
3. Select the data by clicking it once. Then click the data again (i.e., click the data itself twice *slowly*). A cursor appears in the text field.
4. Type your new information, and then press **Enter** on your keyboard.
5. Select the check box next to the data if you want the information to be hidden.
6. Click the **Apply** button to save that data.

From the **SecureSession Information** dialog, you can also configure the account-specific policies for this SecureSession account. This procedure is discussed below.

Changing policies for an individual application window or web site

The account-level policies for SecureSession are similar to the user-level SecureSession policies (with the exclusion of **Require authentication when registering applications**) and can be configured in the same way.

To set account-level policies for SecureSession:

1. From the **Start** menu, select **Programs**, **SecureSuite**, and click **My SecureSuite Settings**. Your **User Properties** dialog appears. A **SecureSession Information** dialog appears.

2. Select the **SecureSession/IE** or **SecureSession/Apps** tab.

3. Select the SecureSession account (either a specific web form or a specific application window) for which you want to modify policy settings, and click the **More Info** button.

4. Click the **Advanced** button to view the account-specific policies.

5. Double-click the policy you wish to change for this application window or web site.

6. After setting the policy, click **OK**.

7. When you are finished setting policies, click the **Close** button in the **SecureSession Information** dialog.

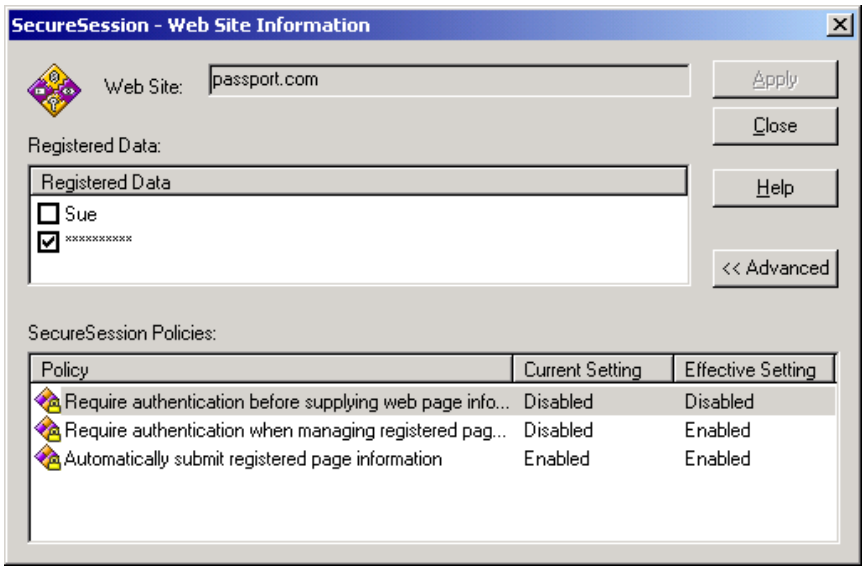

Figure 13: Account-Specific SecureSession Policies

User Properties – SecureFolder Policies

To set user-level SecureFolder policies:

1. From the **Start** menu, select **Programs**, **SecureSuite**, and click **My SecureSuite Settings**. Your **User Properties** dialog appears.
2. Select the **SecureFolder** tab.
3. Double-click a policy to modify its setting.
4. After setting the policy, click **OK**.

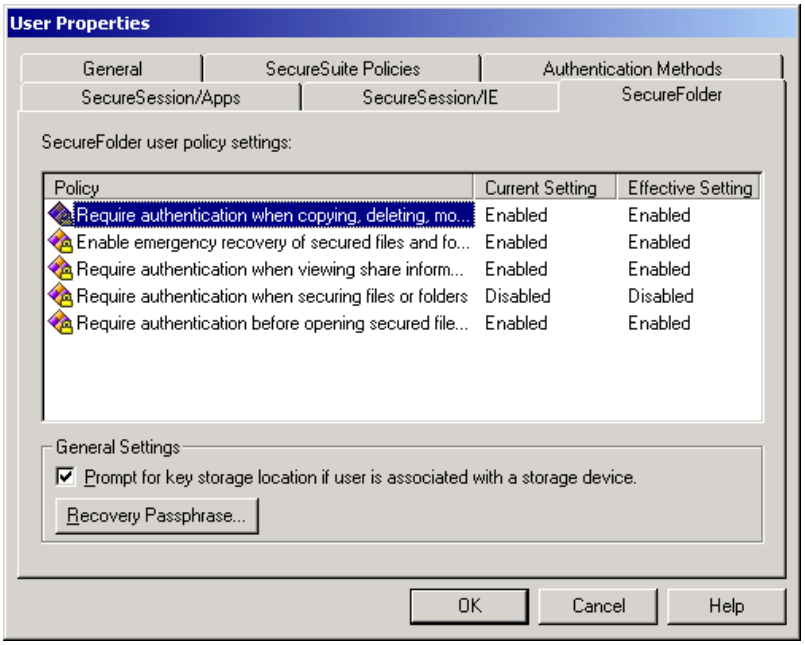

Figure 14: User Properties, SecureFolder

Chapter 7: System Administration

Administering SecureSuite on Windows 2000 and XP Professional

The **SecureSuite User Manager** on Microsoft Windows 2000 and Windows XP Professional is a Microsoft Management Console (MMC) snap-in, which enables management of authentication processes for all workstations and users from the same application that was used for user management prior to installing SecureSuite.

SecureSuite User Manager

To access the **SecureSuite User Manager** on Windows 2000 and XP Professional:

- From the **Start** menu, select **Programs**, **SecureSuite**, and click **SecureSuite User Manager**.

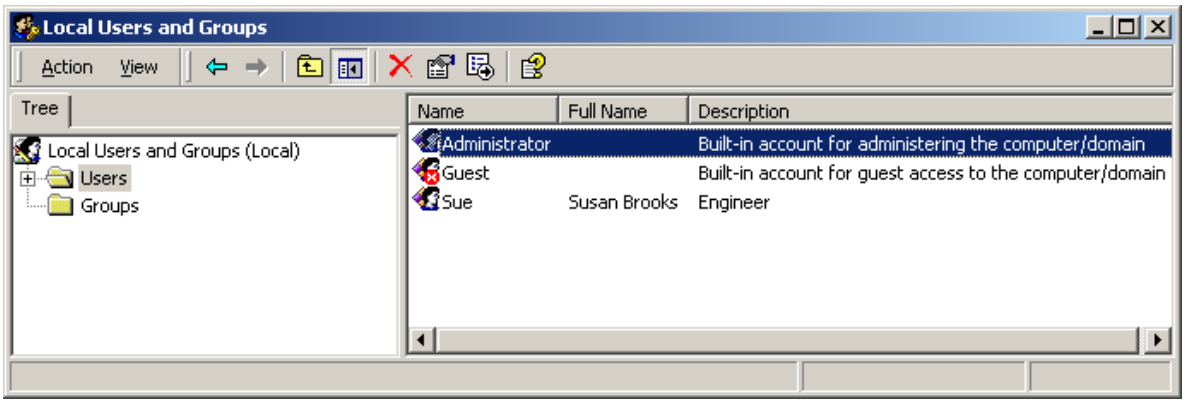

Figure 15: SecureSuite User Manager for Windows 2000

Note: A SecureSuite user can access their **User Properties** dialog without authenticating. However, they will see only Windows-related properties, which were accessible before SecureSuite was installed. In order to view SecureSuite-related user properties, an administrator must be logged.

Creating a New User Account

Note: During this process, you must enter a password for each user even if a password is not one of the selected methods of verification. This is a requirement for Windows.

To create a new SecureSuite user account on Windows 2000 and XP Pro:

1. From the **Start** menu, select **Programs**, **SecureSuite**, and click **SecureSuite User Manager**. The **Local Users and Groups** dialog appears.

2. From the **Action** menu, select **New User**. The **New User** dialog appears.

3. Enter the **User Name** (required), **Full Name** (optional) and a **Description** (optional) for this user. Enter and confirm the new user's password. Select whether or not the user must change or cannot change the password, as well as if the password expires after initial logon or if the account will initially be disabled. Click **Next.**

Important: Please note that when you are setting up a new user, you must enter a password for the user, even if the user will not use the password method. However, you may leave the password blank, which assigns a blank password to the user. In this case, though, fingerprint authentication will not provide security to this user account. If you are working with an existing user, you will probably already have a password, and will not need to enter a new one.

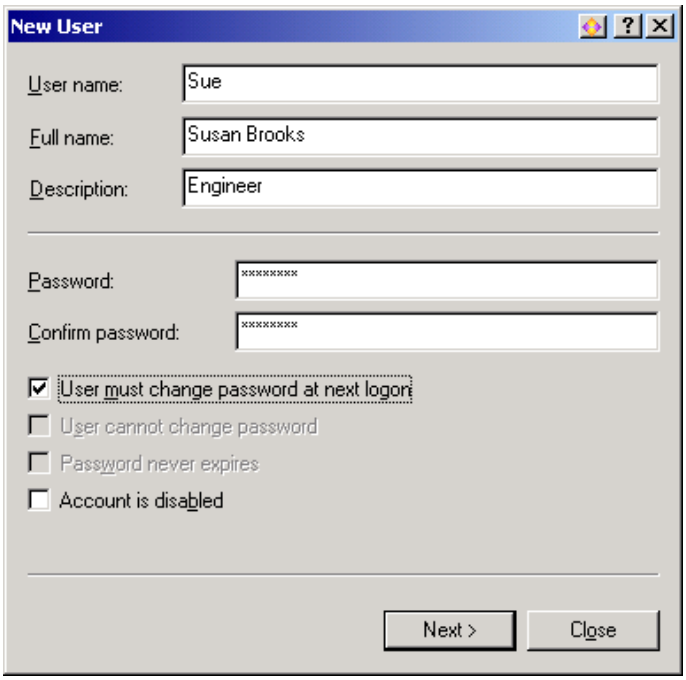

Figure 16: New User Account, Microsoft Windows 2000

4. The **User Authentication Methods** dialog appears. If another method of authentication is selected, a device-specific enrollment wizard will guide you through the enrollment process. For more information, see the *Adding Additional Methods of Authentication to a User Account* section below.

5. Click **OK.**

Administering SecureSuite on Windows XP Home

After SecureSuite installation, all users are converted to SecureSuite users. This conversion process does not affect a user's Windows account profile in any way—it simply involves setting up and initializing a user's profile in the SecureSuite database. All authentication methods (except the password method, which is installed by default and cannot be removed) must be installed either during installation, later by re-running the SecureSuite installer (**Setup.exe**) or via the Add/Remove application in the Windows control panel (select the **Modify** option). After an authentication method is installed, any associated devices that will be used on your system must also be installed. Only administrators can install and remove authentication methods and associated devices.

SecureSuite User Manager

The **SecureSuite User Manager** allows administrators to manage many aspects of user accounts including SecureSuite functionality, applications, and authentication methods and devices. From the **User Manager**, an administrator can add new user accounts to the system, change a current user's properties, add authentication methods and devices, and change a user's access privileges.

Note: User management functionality is available in both the SecureSuite User Manager and the native Windows User Manager, but for ease of use, only SecureSuite related functionality is available in the **SecureSuite User Manager**. Refer to your Windows documentation for more information on the native Windows User Manager.

To access the **SecureSuite User Manager** on Windows XP Home:

1. Click the **Start** button, select **Programs**, **SecureSuite** and click **SecureSuite User Manager**.

2. Type the user name and password of a SecureSuite administrator when the **SecureSuite Authentication** dialog appears.

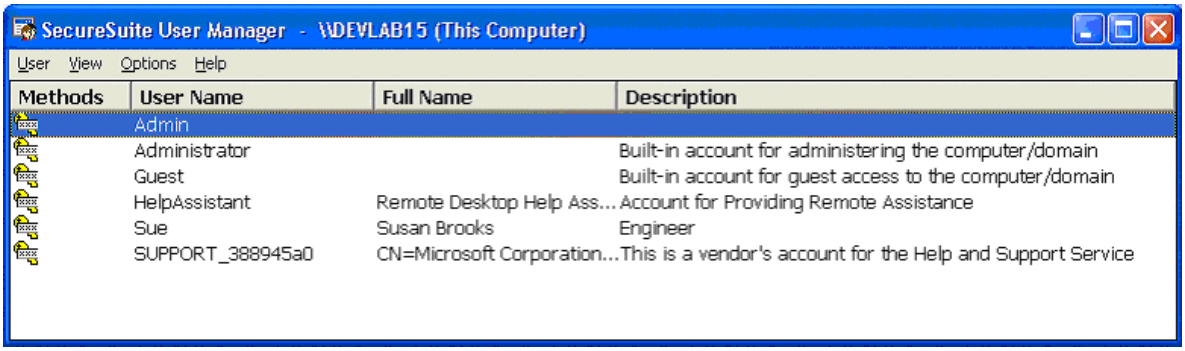

Figure 17: SecureSuite User Manager for Windows XP Home

Creating a New User Account

To create a new SecureSuite user account on Windows XP Home:

1. From the **Start** menu, select **Programs**, **SecureSuite**, and click **SecureSuite User Manager**.

2. Type the user name and password of a SecureSuite administrator when the **SecureSuite Authentication** dialog appears.

3. From the **User** menu, select **New User**. The **New User Enrollment Wizard** appears. Click **Next** to begin the enrollment process.

Figure 18: New Enrollment Wizard, Welcome Screen

4. Enter the **User Name** (required), **Full Name** (optional) and a **Description** (optional) for this user and click **Next**.

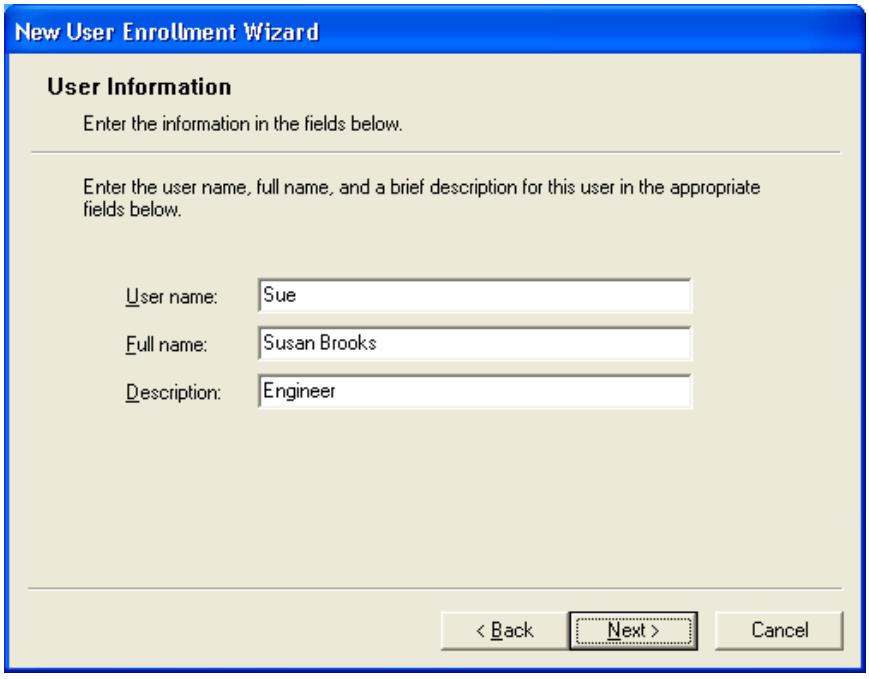

Figure 19: New User Enrollment Screen, User Information Screen

Table 2: User Information Description

Option	Description
User name	Identifies the user account (required).
Full name	The user's complete name. It is a good idea to establish a standard for entering full names so that they always begin with either the first name (Louise G. Morgan) or the last name (Morgan, Louise G.). This field may be left blank.
Description	The description can be any text describing the user account or the user. This field may be left blank.

5. Use the **Add** and **Remove** buttons to select group memberships for the new user. Click **Next** when finished.

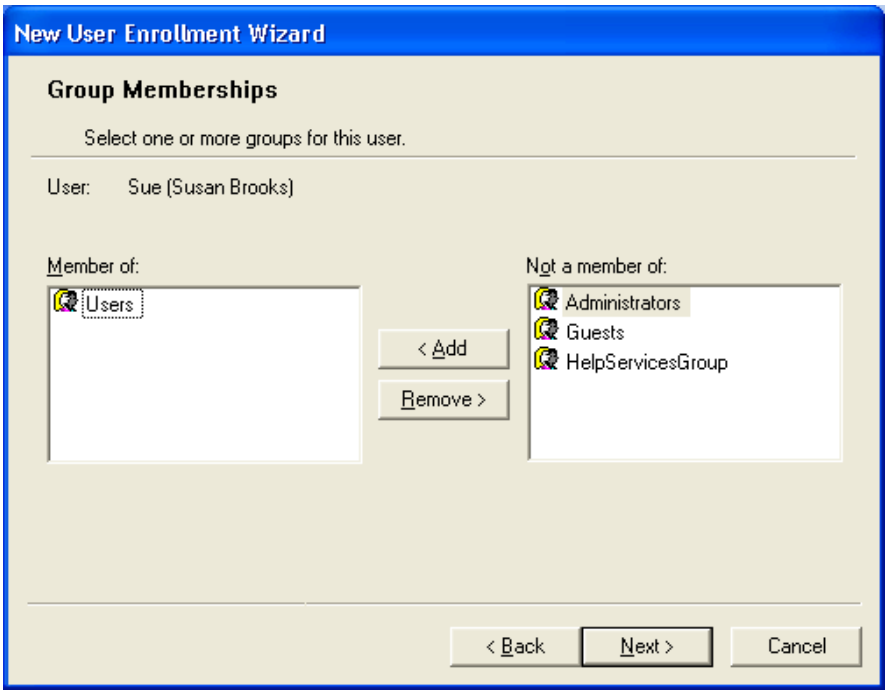

Figure 20: New Enrollment Screen, Group Memberships

SecureSuite allows administrators to assign a user to one or multiple standard Windows user groups. The different levels of group memberships are:

Table 3: Levels of User and Group Memberships

Option	Description
Account Operators	Members can administer domain users and group user accounts.
Administrators	Members can fully administer the computer / domain.
Backup Operators	Members can bypass file security to back up files.
Guests	Users granted guest access to the computer / domain.
Replicator	Supports file replication in a domain.
Users	Ordinary users.

6. The **Completing New User Enrollment Wizard** dialog appears. Click **Finish** to proceed to the **User Authentication Methods** dialog.

Figure 21: New User Enrollment, Completing Screen

7. In the **User Authentication Methods** dialog, click the **Add** button to add one or more authentication method to the user account. The **Add Authentication Device** dialog appears.

8. Select the appropriate device, listed under the corresponding authentication method, and click **OK**.

9. If the password method is assigned to the new user, enter and confirm the new user's password. Click **OK**.

Important: Please note that when you are setting up a new user, you must enter a password for the user, even if the user will not use the password method. However, you may leave the password blank, which assigns a blank password to the user. In this case, though, fingerprint authentication will not provide security to this user account. If you are working with an existing user, you will probably already have a password, and will not need to enter a new one.

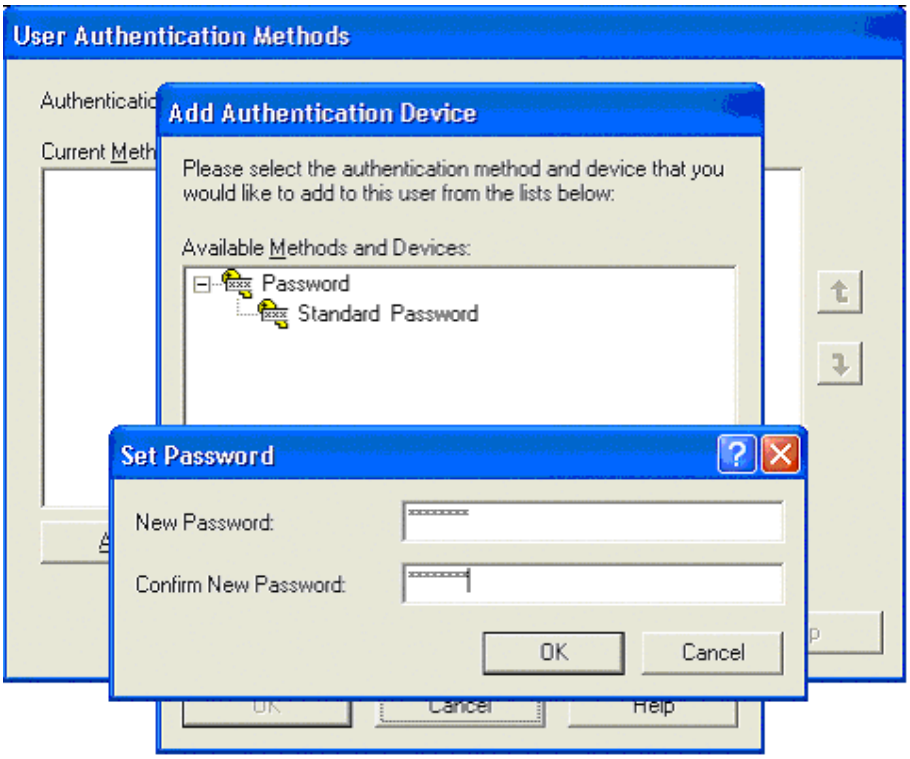

Figure 22: Add Authentication Method

10. If a different method of authentication is selected, such as the fingerprint method, a device-specific enrollment wizard will guide you through the enrollment process. For more information, see the *Adding Additional Methods of Authentication to a User Account* section below.

11. Click **OK**.

Adding Authentication Methods to a User Account

Note: During this and the following examples, the fingerprint authentication method is used for illustration purposes only. Also, this sample procedure assumes that a system administrator has previously installed the fingerprint device with SecureSuite.

User License Keys

SecureSuite uses licenses to delegate how many users may employ authentication methods other than the standard password method (which has no user limit). SecureSuite includes one User License Key, which enables 5 users to utilize non-password authentication methods. If there will be more than 5 advanced authentication method users on the system, you will need to add one or more User License Keys via the **SecureSuite License Manager**. For more information on adding user licenses, refer to the *SecureSuite License Manager* section in this manual.

Important: Please refer to the Sony® Puppy® installation guide ("Training Your Puppy Unit") included in your package or on the CD-ROM for specific instructions on the installation and use of your fingerprint identity device.

To enroll a user with a fingerprint authentication device:

1. From the **Start** menu, select **Programs**, **SecureSuite**, and click **SecureSuite User Manager**.

2. Select the user account to which you wish to assign the fingerprint authentication method. If you are working on Windows 2000 or XP Professional, select **Properties** from the **Action** menu. For Windows XP Home, select **Properties** from the **User** menu.

3. Type the user name and password of a SecureSuite administrator when the **SecureSuite Authentication** dialog appears. The **User Properties** dialog appears.

4. Select the **Authentication Methods** tab and click the **Add** button. The **Add Authentication Device** dialog appears.

5. Select the fingerprint method and associated fingerprint device from the **Available Methods and Devices** list. Click **OK**.

6. When the **Fingerprint Enrollment Wizard** appears, click **Next**. Select a fingerprint to enroll by clicking its image with your mouse, and click **Next**.

7. Scan your fingerprint four times (the default number). The first three times enroll your fingerprint, and the fourth verifies that the fingerprints sufficiently match for later use in the verification process. Click **Next**.

8. Click **Finish**. The **User Properties** dialog appears.

   - Use the **Add** button to add an additional method of authentication.

   - Use the **Remove** button to delete an enrolled method of authentication.

9. If more than one method has been added, a method priority icon will appear between each pair of devices in the **Current Methods and Devices** list view in the **Authentication Methods** tab of this user's **Properties** dialog. This icon specifies the relationship between this user's authentication devices. Right-click this icon to choose one of the two following relationships:

   - Select **AND** to require the user to authenticate with all enrolled methods of verification.

   - Select **OR** to allow the user to choose any one method of verification each time they authenticate.

10. To specify a method that the user will be prompted to use first when authenticating, select the method and use the green method priority arrows on the right side of the **Authentication Methods** tab of the **User Properties** dialog to move the desired method to the top of the list. This does not force the user to use this authentication method or prevent them from using other methods.

11. Click **OK** when finished.

Chapter 8: SecureSuite System Settings

System Settings refer to SecureSuite tools that allow administrators to manage SecureSuite options and policies from one easy-to-use centralized access point. An administrator can use these tools to view and modify system properties for a target computer or for a domain. Using the **SecureSuite System Settings** or **System Properties** dialog, administrators can:

- Set system-level policies
- Manage authentication devices
- Manage the local SecureSuite database
- Configure system-level SecureFolder and SecureSession policies
- Set SecureLaunch restrictions for applications for users and groups, and assign access policies (local machine only)
- Configure the communication settings

Note: Only members of the Administrators group can access the **SecureSuite System Settings** or **System Properties** dialog in order to configure system properties.

SecureSuite applications are installed on the local machine only. Therefore, policy settings and other options configured for SecureSuite applications pertain only to the local machine. The same is the case for event logging functionality as well as user- and workstation-specific options such as hot-keys. However, SecureSuite event logging is integrated with the native event logging available in all versions of Windows, and the logged event information can be retrieved remotely. See your Windows documentation for more information on native event logging.

To use the **SecureSuite System Settings** dialog on Windows 2000 and XP Professional:

- From the **Start** menu, select **Programs**, **SecureSuite**, and click **SecureSuite System Settings**.

- From this dialog, select the SecureSuite feature that you want to access from the left pane, and then double-click an option in the right pane. The SecureSuite functionality that can be accessed from this dialog is described in the following sections.

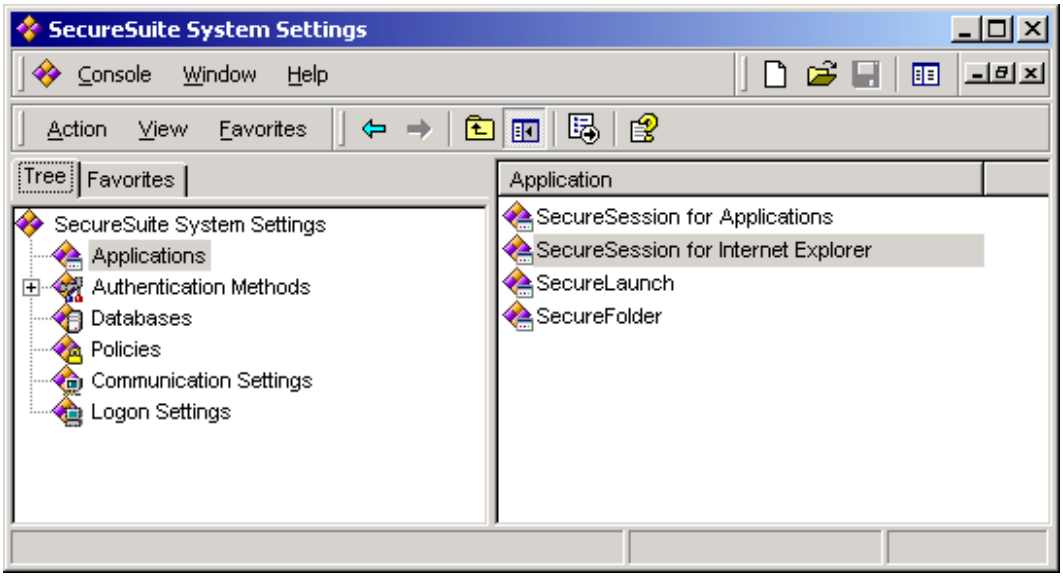

Figure 23: SecureSuite System Settings - Windows 2000

To use the **SecureSuite System Properties** dialog on Windows XP Home:

1. From the **Start** menu, select **Programs**, **SecureSuite**, and click **SecureSuite User Manager**.

2. From the **Options** menu, select **System Properties**.

3. From this dialog, select the appropriate tab to access the desired functionality. The SecureSuite functionality that can be accessed from this dialog is described in the following sections.

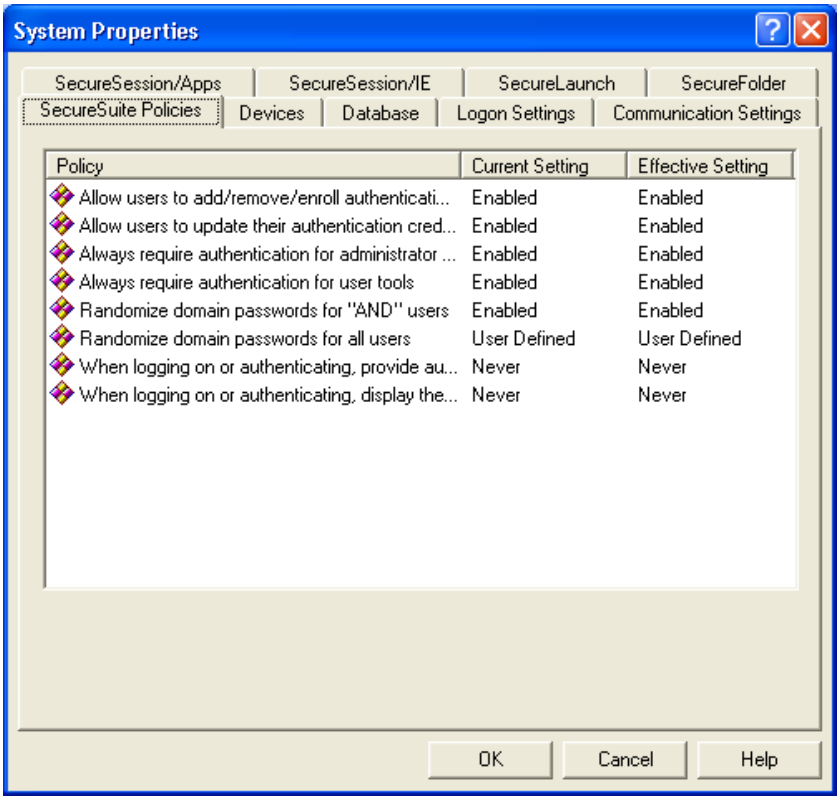

Figure 24: System Properties - Windows XP Home

System Settings – Policies

The **SecureSuite System Settings – Policies** dialog allows an administrator to configure the policy settings for a specific workstation or an entire domain.

These policies are effective for all users on the target workstation or domain. Some system-level policies also allow administrators to configure the policy for individual users at the user level. Note that system-level policies override user-level policy settings. See *Appendix 3: A Table of SecureSuite Policies* for more information.

To set system-level SecureSuite policies:

1. Double-click the policy that you want to set. A **SecureSuite System Policy Setting** dialog appears.

2. Select the desired setting, and click **OK**.

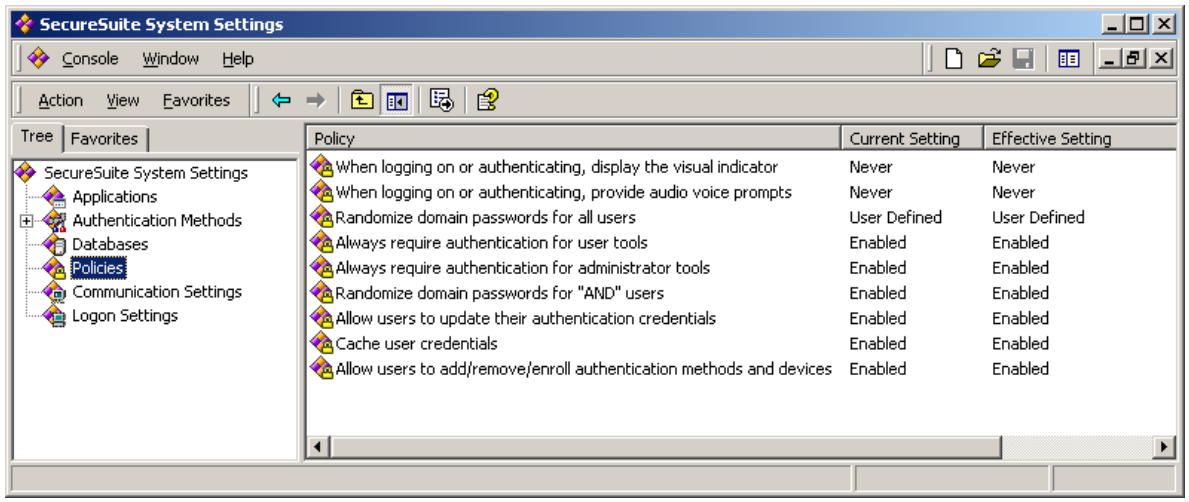

Figure 25: System Settings – Policies

System Settings – Authentication Methods

The **System Settings – Authentication Methods** dialog allows a SecureSuite administrator to install, configure, and uninstall any authentication device supported by SecureSuite. Devices must be "added" to SecureSuite after they and their associated methods are installed on a system or domain. This security feature prevents users from replacing, or altering the configuration of available devices and their associated authentication methods (e.g., it prevents hackers from acquiring their own tokens and then configuring them for SecureSuite authentication). There are two ways to add a device to your system. The first is called "in-lining" and refers to the fact that during user enrollment, the device setup is combined with user enrollment using a single wizard (for more information, refer to the *Adding Authentication Methods to a User Account* section in this manual); the second is outlined below.

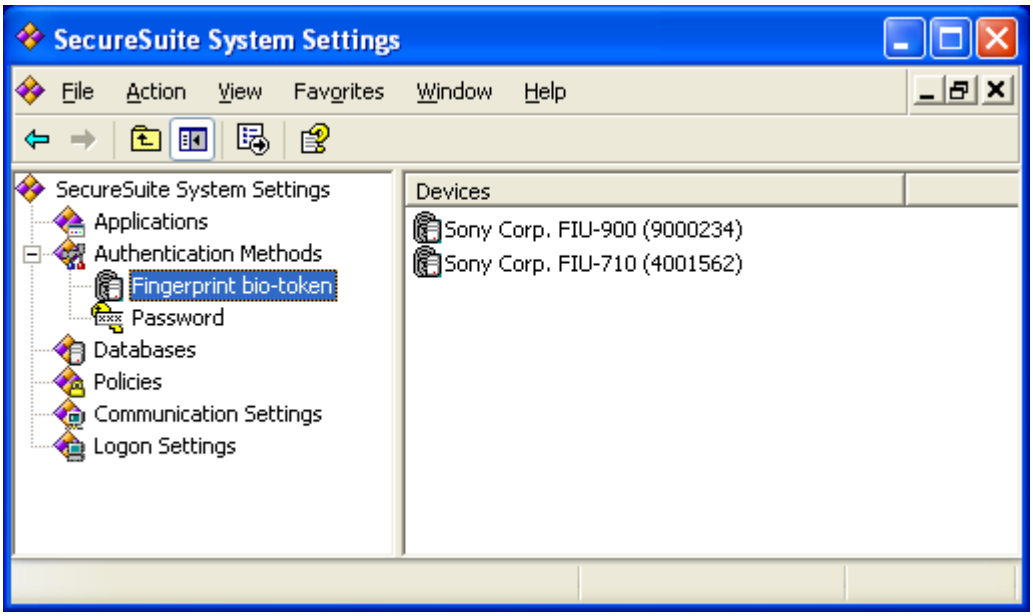

Figure 26: System Settings – Authentication Methods

Managing Authentication Devices on Windows 2000 and XP Professional

Note: The following instructions assume that the OEM's device module was previously installed with SecureSuite. For information on installing an OEM device module, refer to the *Installing OEM Device Modules* section in Chapter 12 of this manual.

To add an authentication device to your system:

1. Since you have already installed the OEM device module, the method will be listed in the left pane of the **System Settings – Authentication Methods** dialog. Right-click the method under which the device that you want to add is categorized, and select **Add Device** from the menu that appears. The **Add Authentication Device** dialog appears, listing the installed authentication methods and associated devices that SecureSuite has detected, but which are currently not in use.

2. Select the authentication device you wish to add, and click **OK**. The authentication device you selected will now be available in the right pane of the **System Settings – Authentication Methods** dialog.

To view or change the settings for an installed device:

- Right-click the device, and select **Properties**. (This is not available for all devices.)

To remove a device from your system:

- Right-click the device you wish to remove, and select **Remove Device**.

Important: Please refer to the Sony® Puppy® installation guide ("Training Your Puppy Unit") included in your package or on the CD-ROM for specific instructions on the installation and use of your fingerprint identity device.

System Settings – Database

The SecureSuite database stores SecureSuite user data, settings for SecureSuite policies, and other program information for the local machine only.

The **SecureSuite System Settings - Database** dialog allows administrators to view and edit local SecureSuite database options, including the database backup schedule. Normally, there will be no need to change the default settings.

Note: We strongly suggest that you are familiar with Microsoft Windows domain models and basic networking principles before configuring your system's database.

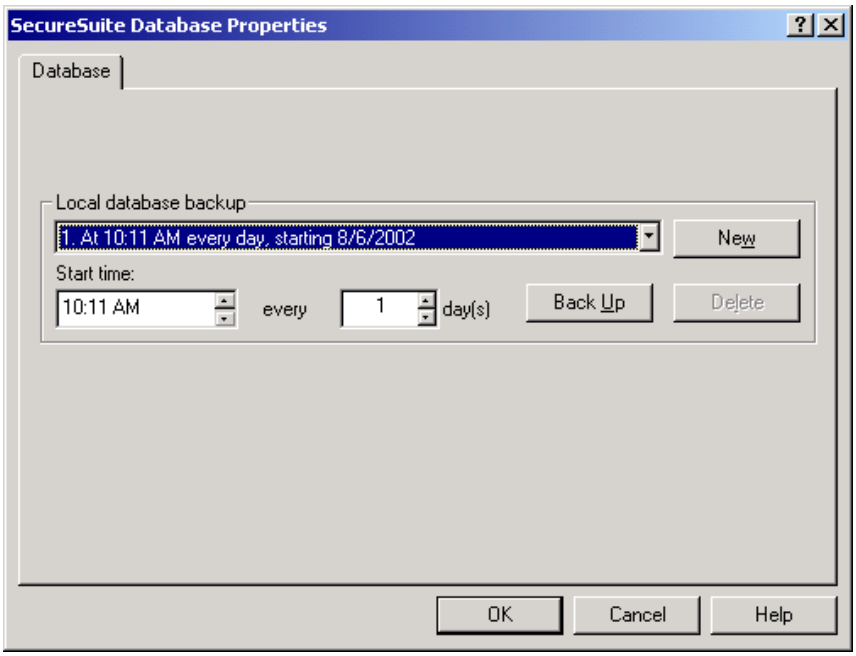

Figure 27: System Settings - Database

Local Database Backup - Setup and Operation

To create a schedule for automatic backup of your local database:

1. In the **Start Time** box, click the up and down arrows to select the local database backup start time.
2. In the **Every**…**Day(s)** box, click the up and down arrows to select the frequency of the local database backup.
3. Click **New** to set the start time and duration of the new local database backup schedule.

Note: Clicking **New** before specifying a start time or frequency will automatically set the current time as the start time with everyday set as the frequency.

To perform a manual back up of your local database:

- Click **Back Up Now** to manually initiate local database backup.

System Settings – SecureFolder

Policies for SecureFolder can be configured from the **SecureSuite System Settings – SecureFolder** dialog.

To set system-level SecureFolder policies:

1. Double-click the policy that you want to set. A **SecureFolder Application Policy Setting** dialog appears.
2. Select the desired setting, and click **OK**.

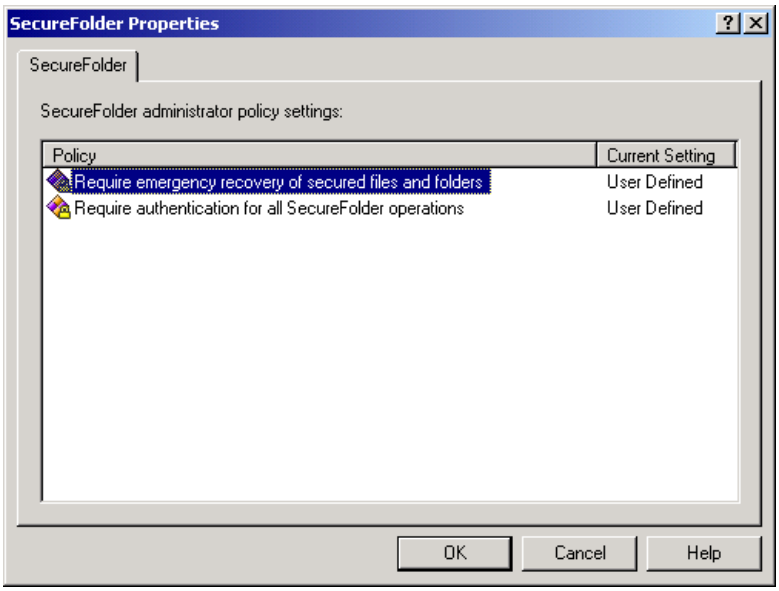

Figure 28: System Settings – SecureFolder

System Settings – SecureLaunch

SecureLaunch allows SecureSuite administrators to restrict access to most Windows applications. Access may be granted or denied to each individual user or group. For more information on securing Windows applications, refer to *Chapter 11: SecureLaunch*.

System Settings – SecureSession for Applications

Policies for SecureSession for Applications can be configured from the **SecureSuite System Settings – SecureSession/Apps** dialog.

To set the system-level SecureSession for Applications policy:

1. Double-click the policy that you want to set. The **SecureSession for Apps Application Policy Setting** dialog appears.

2. Select the desired setting, and click **OK**.

System Settings – SecureSession for Internet Explorer

Policies for SecureSession for Internet Explorer can be configured from the **SecureSuite System Settings – SecureSession/IE** dialog.

To set the system-level SecureSession for Internet Explorer policy:

1. Double-click the policy that you want to set. The **SecureSession/IE Application Policy Setting** dialog appears.

2. Select the desired setting, and click **OK**.

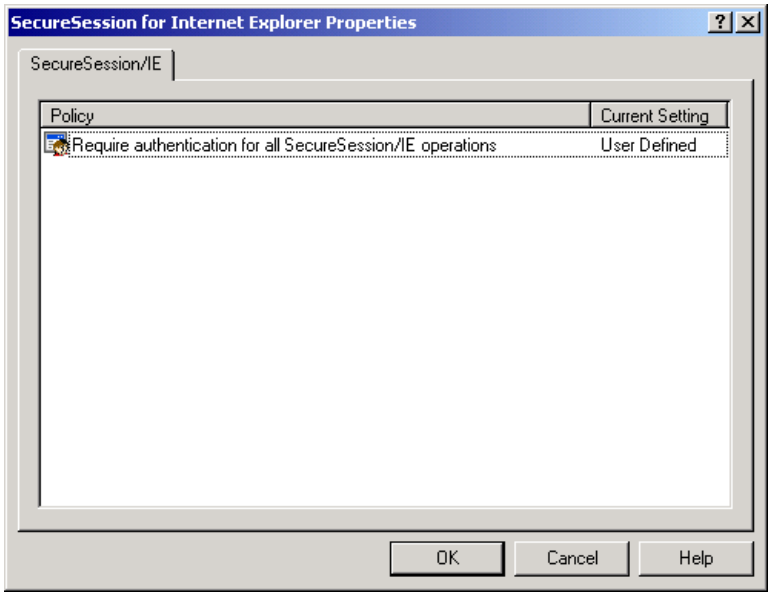

Figure 29: System Settings - SecureSession/IE

System Settings – Communication Settings

An administrator can configure the communication settings in order to ensure proper communication between a server and its clients. This is necessary when the server is protected by a firewall that uses Network Address Translation (NAT) or a similar mechanism *and* one or more client machines are outside of the firewall. From the **SecureSuite System Settings - Communication Settings** dialog, a SecureSuite administrator can specify which ports and IP addresses will be used for client/server communication, as well as set the SecureSuite timeouts.

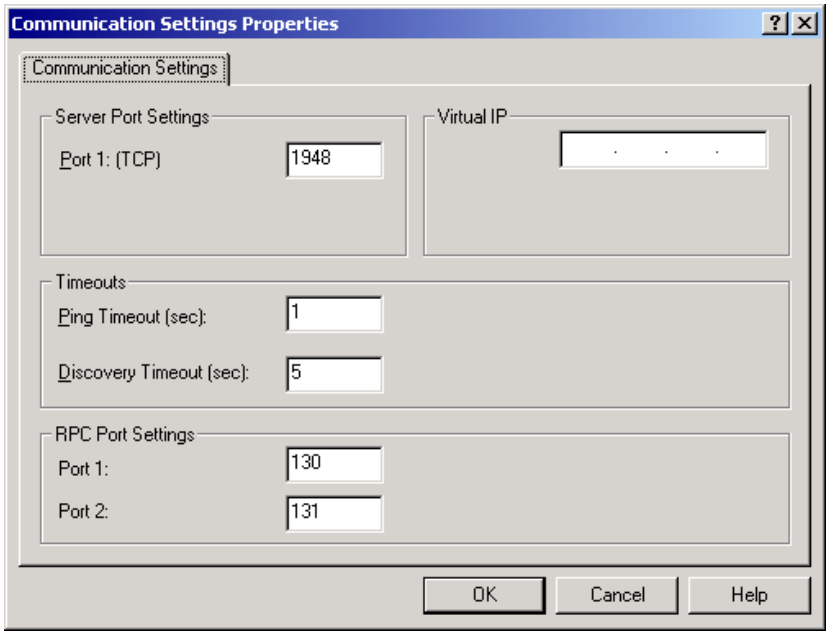

Figure 30: System Settings - Communication Settings

Port Settings

Changing a port from **0** (which allows the use of any available port) to another port allows SecureSuite to function over a firewall or similar security component.

The **Server TCP Port Setting** allows an administrator to specify which TCP port the server will use to receive messages from client machines during the ping process.

The **RPC Port Settings** allow an administrator to specify which ports will be used in order to ensure proper RPC communication. **Port 1** specifies which port the client machine will use to call CSS functions from the server. **Port 2** specifies which port the client machine will use to call LAS functions from the server.

Timeouts

The **Ping Timeout** value specifies the amount of time (in seconds) that a client machine will wait for a response from the server during the ping process. For example, if this is set at **10** seconds, then when the client is attempting to ping the server, the client machine will wait for 10 seconds before returning a message stating that the server could not be found. Increasing this setting will allow the client machine more time to wait for a response from the server.

The **Discovery Timeout** value specifies how long a client will search for the server during the discovery process. If a domain is a LAN (as opposed to a WAN), this value can be as little as **5** to **10** seconds. For more geographically abundant networks, the default value should be left as is, or increased if you are having problems with clients detecting available SecureSuite servers.

Virtual IP

When the server is protected by a firewall and one or more client machines are outside of the firewall, it may be necessary to specify the server's IP address in order to ensure successful communication. The **Virtual IP** setting allows an administrator to specify the IP address.

Chapter 9: SecureSession

SecureSession consists of two different applications (related in their basic functionality):

- **SecureSession for Applications** (SecureSession/Apps) stores passwords and other text-based information for Windows applications.

- **SecureSession for Internet Explorer** (SecureSession/IE) stores passwords and user information for web sites.

SecureSession will remember user names and passwords for application windows or web sites. The process of having SecureSession remember information is known as "registration". Once an application or web site is registered with SecureSession, whenever the application is executed again or the web site is revisited, SecureSession will automatically recognize the application or web site. Clicking a button will cause SecureSession to fill in your stored information (upon authentication, if required). Each application window or web site you register with SecureSession can contain unique information. The text you submit in a **SecureSession Registration** dialog is directly related to that application or web site, and is exclusive to each.

For both SecureSession for Applications and SecureSession for Internet Explorer, there are three account-specific (application window-specific or web site-specific) policies, which can be set exclusively for each application window and web site. These are available in the **Registration** and **More Info** dialogs. There are four user-specific policies, which are available in your **User Properties** dialog. User-level policies override account-specific policies when set as enabled. If the user-level policies are disabled, then the account-specific policies will determine the effective settings. SecureSession for Applications and SecureSession for Internet Explorer policies defined at the system level always supersede user-level and account-level policy settings. If the system-level policies are enabled, they take precedence. If they are set as **User Defined**, then the user-specific and the account-specific policies will determine the effective settings.

Note: SecureSession data is available only for the user who is currently logged on.

SecureSession for Applications

SecureSession for Applications remembers passwords and other text-based information that you would normally type into Windows dialog boxes, and submits them for you. Each of your application accounts is unique. Therefore, you must follow the registration procedure individually for each application window that you wish to access with SecureSession.

The **SecureSession for Applications** system tray icon is located in the Windows system tray. This icon allows you to access most SecureSession for Applications functionality, including:

- Register an application window with SecureSession for Applications
- Update or remove registered information
- Access the **Logon Helper** window in the event that it has been disabled
- Access and modify your SecureSession for Applications information
- Generate a password for your SecureSession accounts

Registering an Application

To register an application window with SecureSession for Applications:

1. Click the **SecureSession for Applications** button and select **Register** from the menu that appears. The **SecureSession – Window Registration** dialog appears. Click **More** to view detailed information about the application window you are registering. The data you entered in the target window is automatically listed in the **Control Data** field of the **SecureSession Window Registration** dialog.

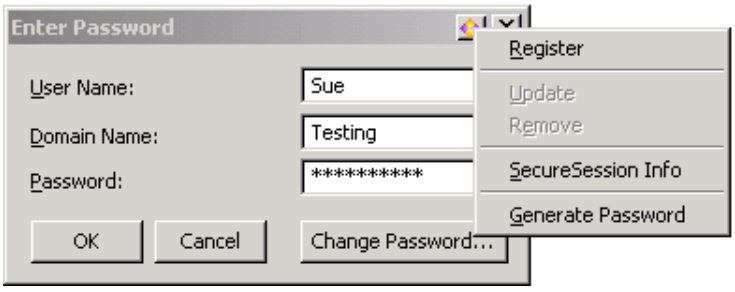

Figure 31: Registering your Application Window with SecureSession

Note: SecureSession will only register those application windows that do not belong to SecureSuite and contain at least one text box.

2. Confirm that you want to register your information by clicking **Yes**.

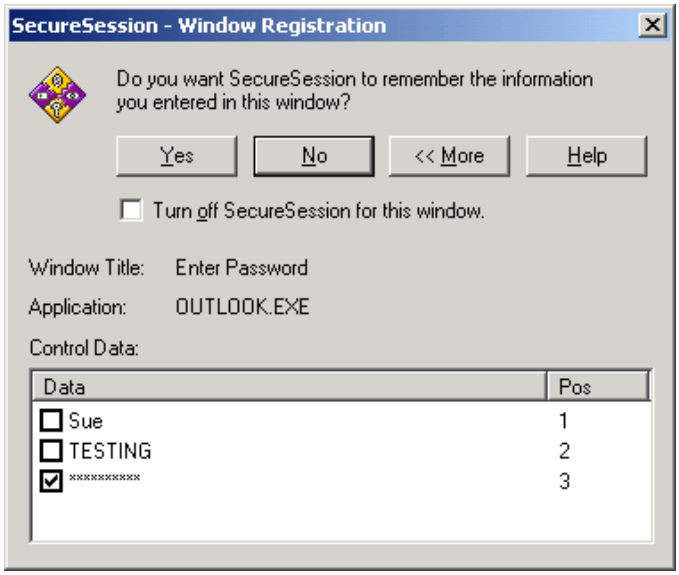

Figure 32: SecureSession - Window Registration

Note: You have the ability to turn off SecureSession for this application window. If you select the **Turn off SecureSession for this window** check box, SecureSession will not automatically display the **Logon Helper** window (which allows you to have your information entered by SecureSession) when you open this application window in the future. SecureSession will still store your information, but you will have click the **SecureSession for Applications** button and select the **Logon Helper** option in order to have your information submitted.

3. After registering the application, you are prompted to enter a description and select a storage location for the registered information. Depending on your system configuration, you may have one or more options for the storage of your registered information. Your local machine is always an option. If your machine is a member of a domain, you will have the option of storing your information on the domain. Additionally, if you have enrolled any authentication device that is capable of storing data, then that device will be listed as a possible location for information storage. For more information, please refer to the *SecureSuite XS Administrator's Guide*, or contact your system administrator. The choice of where to store the registered application information should be carefully considered.

   - Choose **This Computer** to store the information on your local machine. The information will only be available when working on that workstation.

   - Choose **Domain** to store the information on your server. The data will be available to you from any SecureSuite-enabled workstation on the domain.

   - If you choose to store the information on a portable authentication device, you can take the information with you wherever you go. As long as SecureSuite and the device's corresponding authentication method are installed on a machine, you will be able retrieve the information from the device on that machine for use by SecureSession.

4. Click the **Advanced** button to view and modify the policies for the window being registered. Double-click a policy to modify its setting. The **SecureSession for Applications Window Policy Setting** dialog appears.

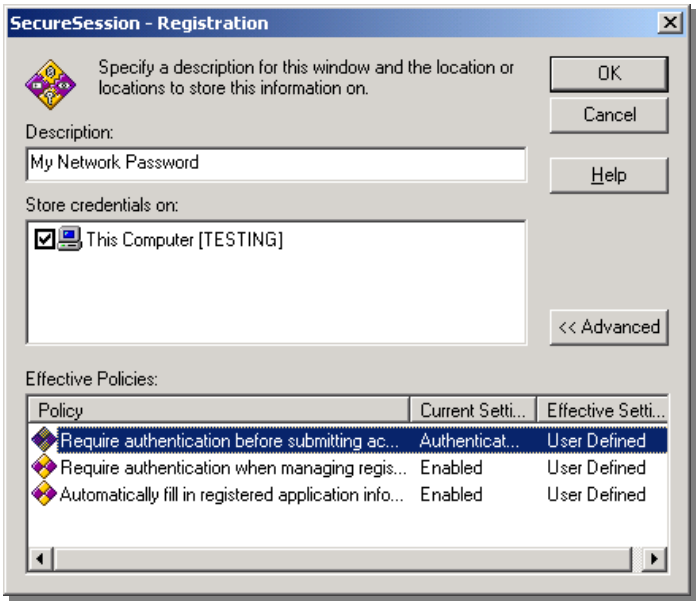

Figure 33: SecureSession/Apps Window Registration

5. Make the desired changes and click **OK**. For more information on individual policy settings refer to the *Managing SecureSession/Apps* section in Chapter 3 of this manual.

6. The **SecureSession – Registration Successful** dialog appears. Click **OK** to complete the SecureSession application window registration process.

Activating SecureSession for Applications

Every time you return to a registered application window, the **Logon Helper** window will appear to automatically enter your registered information.

To have SecureSession provide your registered information:

1. Open the registered application. The **Logon Helper** window appears.

2. Select the description for the information that you want SecureSession to submit for you. (You also have the option of turning SecureSession off for this application window or deactivating the **Login Helper** window. You may also delete a stored data set for this application by selecting that data set, and then selecting **Remove** from the same drop-down list.)

3. Click **OK** and SecureSession will fill in your registered information. If you have the **Automatically submit registered application information** policy set as enabled, then when you click **OK** you will not have to do anything else in order to submit your information to the application. If this policy is disabled, then you will have to manually submit the information (by clicking a button in the application window, pressing **Enter** on your keyboard, etc.) once SecureSession fills it in.

Figure 34: SecureSession Logon Helper Window

Editing SecureSession Information

If you need to change your password, user name, or other information for a registered application, you must also update that information with SecureSession.

To modify registered SecureSession information:

1. Open the application window you wish to update.
2. Type your new information in the appropriate fields, as if you were logging on to the application.
3. Click the **SecureSession for Applications** icon in the Windows system tray, and select **Update**. The **SecureSession – Window Registration** dialog appears.
4. Click **Yes** to confirm that you want to register the new data.
5. In the **SecureSession** dialog that appears, you may change the storage location for this data, or click the **Advanced** button to modify the account-specific policies. Click **OK** when finished.

- OR -

1. From the **Start** menu, select **Programs**, **SecureSuite**, and click **My SecureSuite Settings**.
2. Select the **SecureSession/Apps** tab.
3. Select the SecureSession account that you wish to update, and click the **More Info** button. A **SecureSession – Application Window Information** dialog appears.
4. Make sure that the check box next to the data you are changing is deselected so that the data is not hidden.
5. Click the data once to select it, and then click it again (i.e., click the data itself twice *slowly*). A cursor appears allowing you to change the stored text.
6. Click **Apply** when finished, and then click **Close**.

Removing Registered Application Information

If you no longer want SecureSession to remember and provide a certain set of information, you can remove the stored information for that registered application window.

To remove SecureSession registration from an application window:

1. Open the application window for which you wish to remove registered data.
2. In the drop-down list of the **Logon Helper** window, select the description of the data that you want to remove.
3. Click the **SecureSession for Applications** icon in the Windows system tray, and select **Remove**, or simply select **Remove** from the same drop-down list in the SecureSession **Logon Helper** window.
4. At the prompt, confirm that you want to remove the registration by clicking **OK**.

- OR -

1. From the **Start** menu, select **Programs**, **SecureSuite**, and click **My SecureSuite Settings**. Your **Properties** dialog appears.
2. Select the **SecureSession/Apps** tab.
3. Select the SecureSession account from which you want to remove registration and click **Delete**.
4. At the prompt, click **OK**.

SecureSession for Internet Explorer

SecureSession for Internet Explorer allows you to log on to a web site without having to type your user name and password. The **SecureSession Web Site Registration** dialog is only accessible when SecureSession recognizes that you are at a web site that requires a password. You will then have the option of allowing SecureSession to remember the password you entered for the web site. This gives you the convenience of registering frequently used web sites that require logon information.

The **SecureSession for Internet Explorer** button (represented by the SecureSuite icon) will appear in the Internet Explorer toolbar. This button provides some additional functionality such as manually launching the **Logon Helper** window if it is not automatically launched, as well as editing or removing registered a user name and/or password.

Registering a Web Site

To register a web form with SecureSession for Internet Explorer:

1. When you access a web site that requires a user name and password combination, log on to the site as normal. The **SecureSession Web Site Registration** dialog appears.

2. Click **Yes** to allow SecureSession to remember the username and password you entered for the web site. The **SecureSession – Registration** dialog appears.

Note: You may disable SecureSession and prevent this dialog from reappearing by selecting the **Turn off SecureSession for this site** check box. For maximum security, select the **Always require SecureSuite authentication for this web site** check box. The next time you return to this site, SecureSuite will prompt you to authenticate before allowing the SecureSession Web Site **Logon Helper** window to enter your registered information.

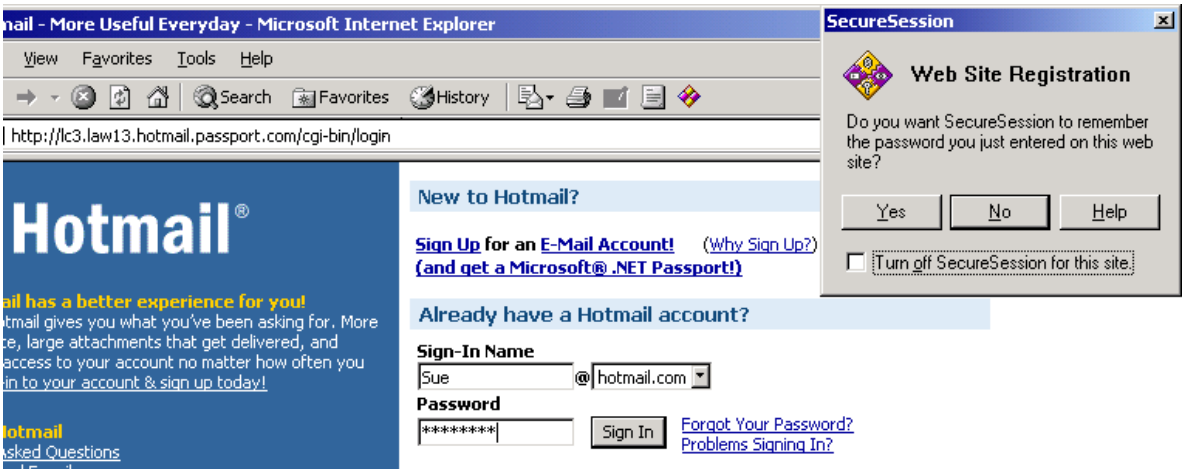

Figure 35: SecureSession Web Site Registration

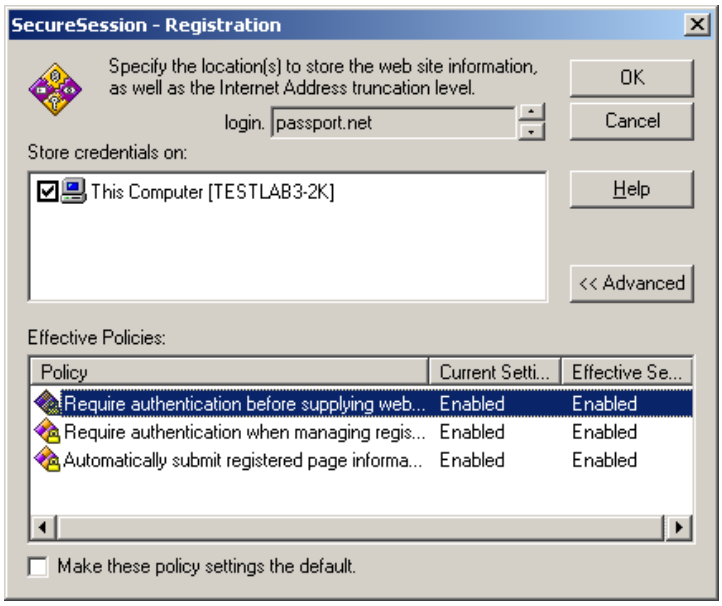

Figure 36: SecureSession for Internet Explorer Registration

3. Use the up and down arrows next to the text box near the top of the dialog to specify the level of truncation for the web site's URL. This allows you to log on to multiple web pages that use the same logon credentials. For example, you may have the same user name and password for logging on to your Hotmail account and your MSN Messenger account. In this case you would want to truncate the URL so that only "passport.net" appears in the text box. This signifies that you use the same user name and password for all "passport.net" logon pages. As another example, suppose that you have separate accounts on the same domain, such as "accounting.company.com" and "mail.company.com", for which you use different user names and/or passwords. You can increase the truncation level to include "accounting" or "mail" when registering each of these accounts so that SecureSession will differentiate between them and provide the correct logon credentials.

4. In the **Store credentials on** field, select a check box to specify where you would like the information from your registered web form to be stored. In addition to your local computer, you may have the option to store credentials on your domain as well as some authentication devices.

5. Click the **Advanced** button to set policies that apply to this web site only.

6. Click **OK** to complete the registration process.

Activating SecureSession for Internet Explorer

Every time you return to a registered web site, the **Logon Helper** window will appear.

To have SecureSession provide your registered information:

1. Verify that the correct logon information is selected in the **User Name** drop-down list of the **Web Site Logon** window.

2. Click **Log On** to have SecureSession fill in your information. As long as the **Automatically submit web site information** policy is enabled, you will automatically be logged in to the web site. If this policy is disabled, you will need to perform the usual action in order to submit your information, such as clicking an **OK** or **Submit** button.

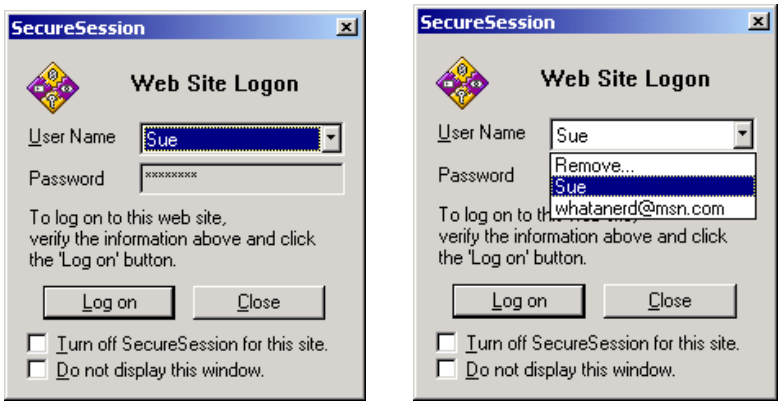

Figure 37: SecureSession Logon Helper Window

Note: If you wish to turn off this feature, select the **Turn off SecureSession for this site** check box. To display the **SecureSession Web Site Logon** window again, click the **SecureSession** button located on the standard toolbar of Internet Explorer.

Editing SecureSession Information

If you need to change your password or user name for a registered web site, you must also update that information with SecureSession.

To modify registered SecureSession information:

1. From the **Start** menu, select **Programs**, **SecureSuite**, and click **My SecureSuite Settings**. Your **Properties** dialog appears.

2. Select the **SecureSession/IE** tab.

3. Select the SecureSession account that you wish to update, and click the **More Info** button. A **SecureSession – Web Site Information** dialog appears.

4. Make sure that the check box next to the data you are changing is deselected so that the data is not hidden.

5. Click the data once to select it, and then click it again (i.e., click the data itself twice *slowly*). A cursor appears allowing you to change the stored text.

6. Click **Apply** when finished, and then click **Close**.

Removing Registered Web Site Information

If you no longer want SecureSession to remember and provide a certain set of information, you can remove that stored information.

To remove SecureSession registration from an application window:

1. Using Internet Explorer, open the registered web site for which you wish to remove registered data.
2. From the **User Name** drop-down list in the **Logon Helper** window, click **Remove**.
3. Click **OK** to confirm removal of your user name and password.
4. When the **SecureSession Web Site Registration** dialog appears, click **Close**.

- OR -

1. From the **Start** menu, select **Programs**, **SecureSuite**, and click **My SecureSuite Settings**. Your **Properties** dialog appears.
2. Select the **SecureSession/IE** tab.
3. Select the SecureSession account from which you want to remove registration, and click **Delete**.
4. At the prompt, click **OK**.

If there are no registered web sites remaining for a web site, SecureSession will display a **SecureSession Web Site Registration** dialog, notifying you that SecureSession for Internet Explorer is still active and will attempt to register your logon information in the future. At this point, you have the option to disable SecureSession for Internet Explorer for the current web site, which will stop SecureSession from asking if you would like to register the information when you revisit this site.

Chapter 10: SecureFolder

SecureFolder provides a powerful, yet fast and convenient way to protect sensitive data in secured files, or groups of files in secured folders. Once files or folders are encrypted, only the owner (the user who initially secured the file or folder) and users to which the owner has granted permission can view its contents.

Note: You cannot secure files or folders in the **Windows** or **Program Files** directories since modifying their contents can cause your programs to stop working correctly. More specifically, you cannot secure the following folders:

- The Windows folder and its subfolders
- The Desktop folder
- The Start Menu folder
- Any root drive
- The Recycle Bin
- The SecureSuite folder and its subfolders
- Any shared folders
- A network share
- Other special folders: (Application Data, Cookies, Favorites, Fonts, History, Temporary Internet Files, NetHood, PrintHood)

Furthermore, to avoid causing system or configuration problems, SecureFolder will not secure the following types of files:

- .dll
- .bat
- .com
- .hlp
- .ocx
- .bpw
- .sys
- .inf
- .nls
- .bdm
- .ini
- .vxd
- .swp
- .cpl

Note: Administrators can delete other users' secured folders, but cannot view or modify their contents.

Securing a File or Folder

To secure a file or folder with SecureFolder:

1. Right-click the file or folder, and select **Secure**.

2. If you are securing a folder, the SecureFolder – Secure dialog appears, asking if you are sure that you want to secure the folder. Click **Yes** to confirm that you want to encrypt the data. (Select the **Do not show this dialog again** check box if you do not want to be prompted for confirmation when securing files and folders in the future.) This dialog does not appear when securing files.

3. If this is the first time that you are securing a file or folder, and you have not yet specified an emergency recovery passphrase, the **SecureFolder Emergency Recovery Passphrase** dialog appears. See the *SecureFolder Emergency Recovery Utility* section below for more information.

4. SecureFolder begins an encryption process. A dialog indicates the progress as the files are encrypted. The SecureSuite icon will be added to the file or folder icon once the file or folder has been secured.

Note: You cannot secure a folder that contains secured files. You must first unsecure the secured files and then secure the folder and all of its content.

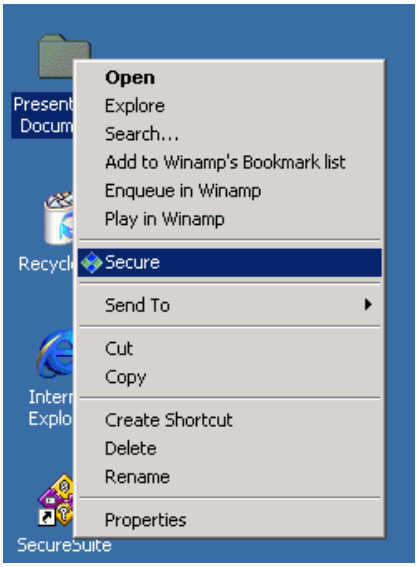

Figure 38: Securing a Folder

SecureFolder Emergency Recovery Utility

Since SecureFolder manages encryption keys for your files and folders, if SecureFolder is uninstalled from your system while files or folders are secured, the encryption keys for those files and folders will be lost. Furthermore, if a user account is removed from the system while that user has files or folders secured, the encryption keys for those files and folders will be lost. Therefore, SecureFolder includes an emergency data recovery utility that uses a passphrase, which is chosen by the owner. If SecureFolder is uninstalled, or if a user account with secured files or folders is deleted, the passphrase can be used to decrypt the data.

Choosing your Emergency Recovery Passphrase

To choose an emergency recovery passphrase:

1. The first time you secure a file or folder, the **SecureFolder Emergency Recovery Passphrase** dialog appears.
2. Enter and confirm your passphrase.
3. Click **OK**.

- OR -

1. From the **Start** menu, select **Programs**, **SecureSuite**, and click **My SecureSuite Settings**. Your **Properties** dialog appears.
2. Select the **SecureFolder** tab.
3. Click the **Recovery Passphrase** button. The **SecureFolder Emergency Recovery Passphrase** dialog appears.
4. Enter and confirm your passphrase.
5. Click **OK**.

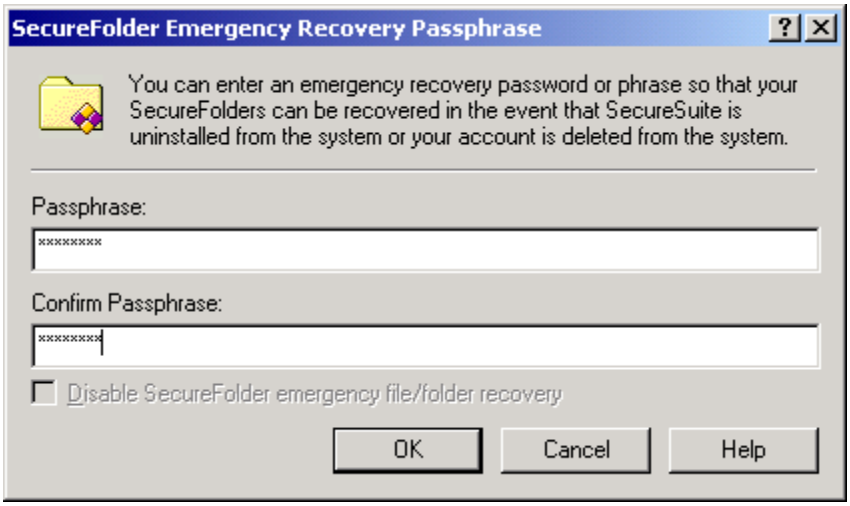

Figure 39: SecureFolder Emergency Recovery

Changing your Emergency Recovery Passphrase

To change your emergency recovery passphrase:

1. From the **Start** menu, select **Programs**, **SecureSuite**, and click **My SecureSuite Settings**. Your **Properties** dialog appears.
2. Select the **SecureFolder** tab.
3. Click the **Recovery Passphrase** button. The **SecureFolder Emergency Recovery Passphrase** dialog appears.
4. Enter and confirm your new passphrase.
5. Click **OK**.

Important: Changing your emergency recovery passphrase does not change the passphrase for files and folders that were secured before you changed it. Whatever emergency recovery passphrase is in effect when a file or folder is secured will be the passphrase for that file or folder until it is unsecured or deleted. This means that, if you change your passphrase, you will need to remember your old passphrase. There is no limit to how many different passphrases you can have. Since this can be confusing and may lead to the loss of data, it is suggested that you keep one passphrase at all times. If you need to change your passphrase for any reason, you should unsecure and re-secure any files and folders. This will assign the new passphrase to these files and folders.

Disabling the Emergency Recovery Utility

There are two ways to disable SecureFolder's Emergency Recovery Utility. One way is to disable it the first time you secure a file or folder by selecting the **Disable SecureFolder emergency recovery** check box in the **SecureFolder Emergency Recovery Passphrase** dialog. The second is to disable it in your **Properties** dialog via your user-level SecureFolder policy settings, which can be done at any time.

To disable SecureFolder emergency recovery utility at any time:

1. From the **Start** menu, select **Programs**, **SecureSuite**, and click **My SecureSuite Settings**. Your **Properties** dialog appears.
2. Select the **SecureFolder** tab.
3. Double-click the **Enable emergency recovery of secured files and folders** policy. A **SecureFolder User Policy Setting** dialog appears.
4. Select **Disabled**.
5. Click **OK**.

Important: Disabling SecureFolder emergency recovery does not remove your emergency recovery passphrase from files and folders that were secured before you disabled this feature. Whatever emergency recovery passphrase is in effect when a file or folder is secured will be the passphrase for that file or folder until it is unsecured or deleted. Therefore, if you want to disable the emergency recovery utility for files and folders that have already been secured, you will need to unsecure and re-secure those files and folders *after* you have disabled the SecureFolder emergency recovery utility. Furthermore, any files or folders that you secure while emergency recovery is disabled will never have an emergency recovery passphrase assigned to them, even if you enable emergency recovery in the future and choose a new passphrase. If you enable emergency recovery and want previously secured files and folders to have the new passphrase associated with them, you will need to unsecure and re-secure those files and folders *after* you activate emergency recovery.

SecureFolder Sharing

Once a file or folder has been secured, the owner can choose to share it with other users.

To share a secured file or folder:

1. Right-click the file or folder that you wish to share, and select **Share** from the menu that appears.

2. Verify your identity when the **SecureFolder Owner Authentication** dialog appears. The **Properties** dialog for the file or folder appears with the **Share** tab selected.

3. Click the **Add** button. A **Select Users** dialog appears.

4. Use the **Look in** drop-down list to select the domain on which the user account(s) with which you want to share the file or folder is located. The available user names may vary depending on which domain you choose. If you know the name of a particular user, you can type the user name in the **lower pane** and click the **Check Names** button.

5. When all users that with which you wish to share the file or folder are listed in the lower pane, click **OK**. The user name(s) appear in the **Authorized User(s)** list of the **Properties** dialog for the file or folder. Click **OK** to exit.

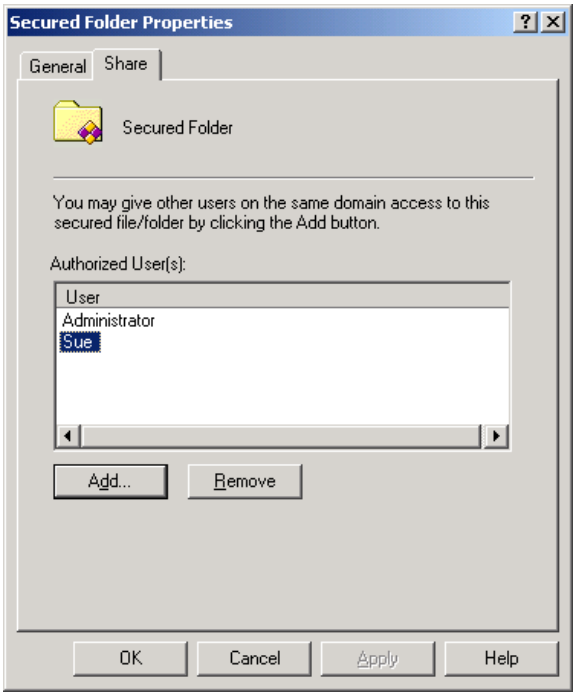

Figure 40: SecureFolder Properties – Sharing

To remove a user's share privileges:

1. Right-click the file or folder that you wish to share, and select **Share** from the menu that appears.

2. Verify your identity when the **SecureFolder Owner Authentication** dialog appears. The **Properties** dialog for the file or folder appears with the **Share** tab selected.

3. From the **Authorized User(s)** list, select the user whose access privileges you want to remove, and click the **Remove** button. The user name no longer appears, and that user may no longer access the file or folder. Click **OK**.

Note: The owner of a secured file or folder (the user who originally secured the file or folder) cannot be removed from the **Authorized User(s)** list.

Working with Secured Files and Folders

After the file or folder is secured, only the owner and users to which the owner has granted permission can unsecure it or view its contents.

To access a secured file:

1. Double-click the file as usual.
2. Verify your identity when the **SecureFolder Owner Authentication** dialog appears. The file becomes unsecure.
3. View and modify the file as usual.
4. When you are finished with the file, re-secure it if desired.

To access a secured folder:

1. Double-click the folder as usual.
2. Verify your identity when the **SecureFolder Owner Authentication** dialog appears.
3. You must drag secured files out of the secured folder into a new location (such as your desktop) before you can open or work with them. After working with a file, place it back in the secured folder to re-secure it.

Note: If you want to work with many files in a secured folder, it is suggested that you unsecure the folder and then re-secure it when you are finished.

Important: SecureFolder encrypts your files with a key that is associated with your user account and authentication methods enrolled on this computer (or domain server, if you are using SecureSuite domain account). *If you copy or move a secured file to another computer (or domain), you will not be able to unsecure or open the file on that computer.*

Removing Security From a File or Folder

To unsecure a file or folder:

1. Right-click the file or folder.
2. Click **Unsecure**.
3. At the prompt, click **Yes** to confirm that you wish to unsecure the file or folder.
4. Verify your identity when the **SecureFolder Owner Authentication** dialog appears.
5. The security icon will no longer be displayed on the file or folder. Any user will be able to access the file or folder without authenticating.

Note: In a client/server scenario, if you try to unsecure a folder that was secured on the domain while you are logged on to the local machine, the name of the domain on which you initially secured the folder will be locked into the **SecureFolder Owner Authentication** dialog. Therefore, you must enter your user name and password information for this domain in order to access the folder. In all other cases, your user name and domain will be locked and you will have to enter only your password to unsecure a folder.

Chapter 11: SecureLaunch

SecureLaunch prevents unauthorized users from running Windows applications. SecureLaunch is ideal for accounting software and databases that contain sensitive and confidential information. It can also limit access to applications such as web browsers and games. In general, only files with an extension of EXE are supported, although other (unsupported) file types will be listed in the **Select Program File** dialog.

Important: Some files with an extension of EXE merely launch another application. Securing theses files *will not* restrict access to the application launched by them. For example, a file named **dvd.exe** may only launch a media player. If **dvd.exe** is secured via SecureLaunch, any user will still be able to open it and launch the media player. In this case, it is necessary to secure the media player itself. In general, it is a good idea to test the restrictions that you implement to ensure that you have secured the correct file. One way to see if an EXE file merely launches another application is to run the EXE and check your task manager to see what is actually running.

Setting User Restrictions

To set user restrictions on Windows 2000 and XP Professional:

1. From the **Start menu**, select **Programs**, **SecureSuite**, and click **SecureSuite System Settings.**
2. In the left pane, double-click **Applications.**
3. Type the user name and password of a SecureSuite administrator when the **SecureSuite Authentication** dialog appears.
4. In the right pane, double-click **SecureLaunch**.

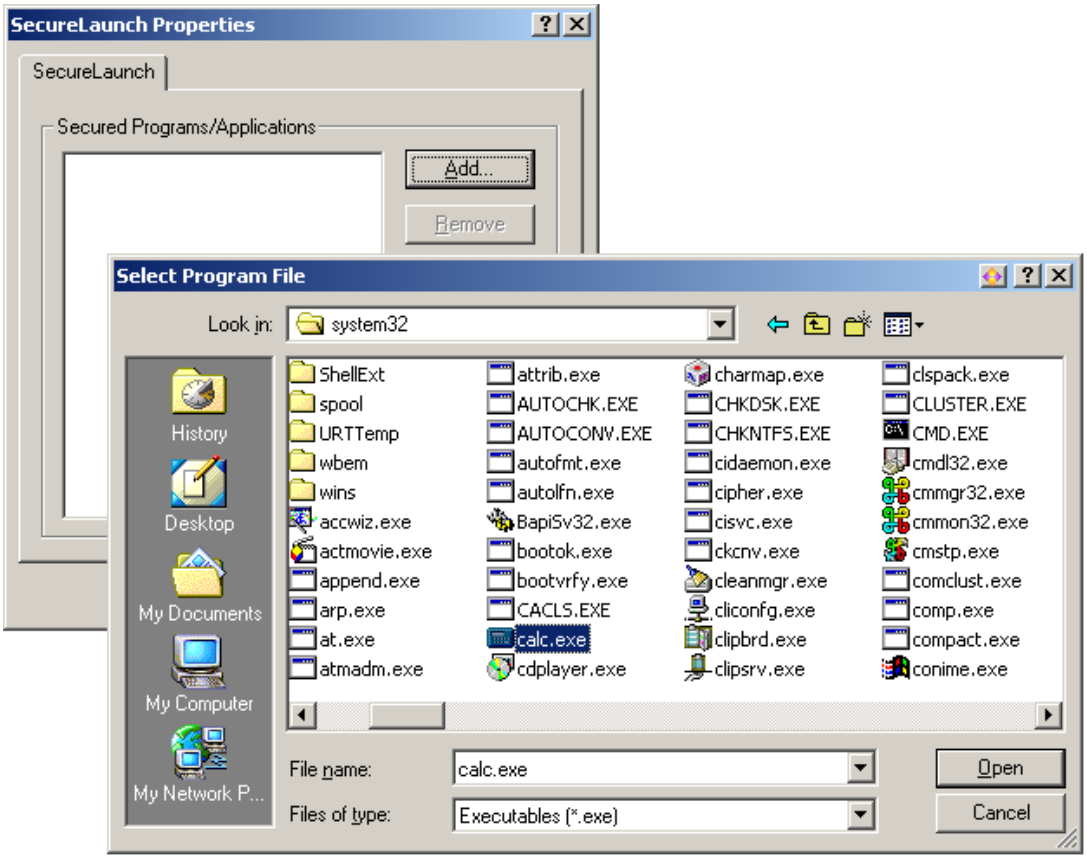

Figure 41: SecureLaunch, Browsing for a Program

5. Click **Add**. The **Select Program Files** dialog appears.

6. Browse for the application you want to secure and click **Open**.

7. The **SecureLaunch Access Policies** dialog for the selected application appears.

8. From the **Access Policies** dialog, you can select the **Administrators** and/or **Users** (the default groups), and grant permissions. To add another user or group, click the **Add** button.

9. From the **Look in** drop-down list, select the domain on which the user/group you wish to add is located. The names of available users/groups will change according to your selection. If you know the name of a particular user/group, you can type the user/group name in the **Search Name** text box and click **Add**. To complete the selection click **OK**.

Note: An administrator must log on in order to display the list of users/groups on that domain. SecureLaunch will prompt an administrator to authenticate whenever it detects that remote domain information is needed for display purposes.

10. In the **Access Policies** dialog, select users or groups and set permissions. The default permission is "**Access with Authentication**". Other available permissions are "**Access Allowed**", and "**Access Denied**".

Note: Any user who is not assigned an access policy (or associated with a group that is assigned an access policy) in the **SecureLaunch Access Policies** dialog will automatically be denied access to the secured application. If no users or groups are specified, then *all* users and groups will be assigned the **Access Denied** policy and will not be allowed to run the secured application.

11. Click **OK** when finished.

To set user restrictions on Windows XP Home:

1. From the **Start menu**, select **Programs**, **SecureSuite**, and click **SecureSuite User Manager**.

2. Type the user name and password of a SecureSuite Administrator when the authentication dialog appears.

3. From the **Options** menu, select **System Properties**.

4. Select the **SecureLaunch** tab.

5. Click **Add**.

6. Browse for the application you want to secure and click **Open**.

7. The **Access Policies** dialog for the selected application appears.

8. From the **Access Policies** dialog, you can select the **Administrators** and/or **Users** (the default groups), and grant permissions. To add another group or a single user, click the **Add** button.

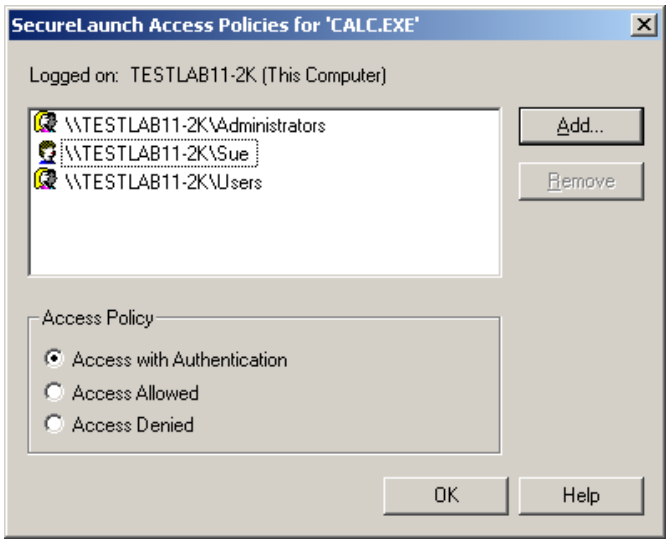

Figure 42: SecureLaunch, Setting the Access Polices

9. From the **Look in** drop-down list, select the domain on which the user/group you wish to add is located. The names of available users/groups will change according to your selection. If you know the name of a particular user/group you can type the user/group name in the **Search Name** text box and click **Add**. To complete the selection click **OK**.

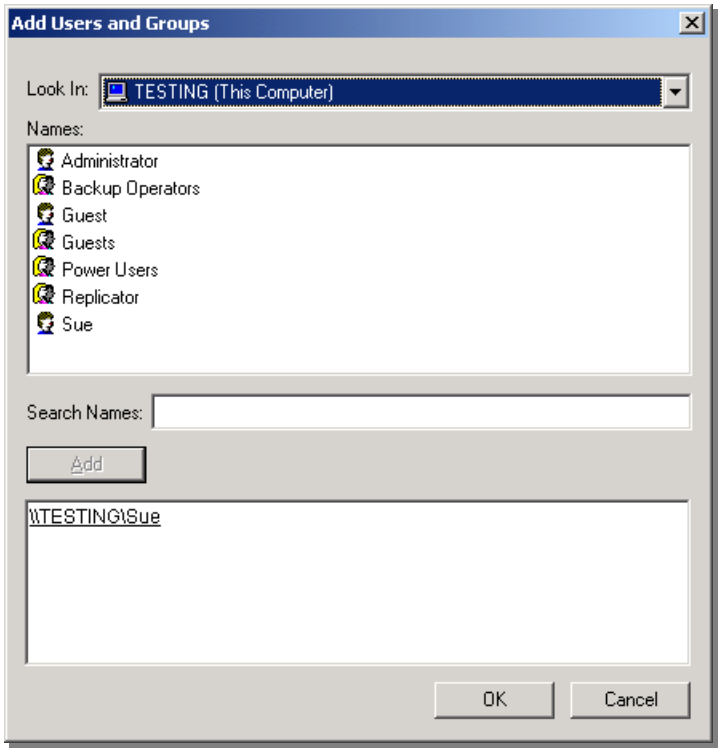

Figure 43: SecureLaunch, Selecting Additional Users/Groups

Note: An administrator must log on in order to display the list of users/groups on that domain. SecureLaunch will prompt an administrator to authenticate whenever it detects that remote domain information is needed for display purposes.

10. In the **Access Policies** dialog, select users or groups and set permissions. The default permission is "**Access with Authentication**". Other available permissions are "**Access Allowed**", and "**Access Denied**".

Note: Any user who is not assigned an access policy (or associated with a group that is assigned an access policy) in the **SecureLaunch Access Policies** dialog will automatically be denied access the secured application. If no users or groups are specified, then *all* users and groups will be assigned the **Access Denied** policy and will not be allowed to run the secured application.

11. Click **OK** when finished.

Changing User Restrictions

Administrators can change the access policies for any user or group at any time.

To change the access policies for an application:

1. In the **System Settings – SecureLaunch** dialog, click the **Security** button. The **SecureLaunch Access Policies** dialog for the selected application appears.

2. Select the user(s) and/or group(s) whose policies you wish to change and select their new access level.

3. Click **OK** when satisfied with all user/group access policies.

Removing User Restrictions

To remove user restrictions from an application on Windows 2000 and XP Professional:

1. From the **Start** menu, select **Programs**, **SecureSuite**, and click **SecureSuite System Settings**.
2. In the left pane, double-click **Applications.**
3. Type the user name and password of a SecureSuite Administrator when the **SecureSuite Authentication** dialog appears.
4. Double-click **SecureLaunch**.
5. In the **Secured Programs/Applications** list, select the application from which you wish to remove access restrictions.
6. Click **Remove**.
7. Click **Yes** to confirm restriction removal.
8. Use of the application is now unrestricted. You must remove restrictions individually for each application.

Note: If you re-secure an application that was previously controlled with SecureLaunch, SecureSuite will ask you if you would like to restore the previous security settings. By clicking **OK** you will restore the previous access policy settings. Click **Cancel** to redefine the security restrictions.

To remove user restrictions from an application on Windows XP Home:

1. From the **Start** menu, select **Programs**, **SecureSuite**, and click **SecureSuite User Manager**.

2. Type the user name and password of a SecureSuite Administrator when the **SecureSuite Authentication** dialog appears.

3. From the **Options** menu, select **System Properties**.

4. Select **SecureLaunch**.

5. Select the application from which you wish to remove access restrictions.

6. Click **Remove**.

7. Click **Yes** to confirm restriction removal.

8. Use of the application is now unrestricted. You must remove restrictions individually for each application.

Note: If you re-secure an application that was previously controlled with SecureLaunch, SecureSuite will ask you if you would like to restore the previous security settings. By clicking **OK** you will restore the previous access policy settings. Click **Cancel** to redefine the security restrictions.

SecureLaunch Access Policy Rules

There are several scenarios you may encounter while configuring access policies for individual users and groups. The following list demonstrates, by way of examples, the rules associated with the different policies and the level of importance given to each of them when deciding which policy to associate with each user and group.

Individual user access policies have the highest priority. For example, suppose that Sue is a member of the Users group and the Users group policy is set as **Access Denied**. Sue also has a user-specific policy set as **Access with Authentication**. In this case, Sue will be able to access the application for which the policy is set upon successful authentication since user-specific access policies take priority over group policies.

If a user is a member of more than one group and these groups have policies set in SecureLaunch, then the least restrictive access policy is associated with that user. For example, suppose that Sue is a member of the Administrators group as well as the Users group. If the access policy for the Administrators group is set as **Access Allowed** and the Users group as **Access with Authentication**, then Sue will be able to access the application for which the policy is set without having to authenticate since the setting **Access Allowed** is less restrictive than **Access with Authentication**.

If a user is only a member of a group for which access policies have not been set, then the user will automatically be denied access to the application. For example, suppose that Sue is a member of only the Backup Operators group and there is no access policy associated with this group. Sue will then be denied access to the application for which the policy has been set.

Chapter 12: SecureSuite Program Maintenance

The **SecureSuite Installation Wizard** allows you to make changes to your SecureSuite configuration, repair SecureSuite in the event of damaged or missing components, or completely remove SecureSuite from your system.

Changing your Configuration

To modify or repair SecureSuite:

1. From the **Start** menu, select **Settings**, **Control Panel** and double-click **Add/Remove Programs**.

2. From the list of installed programs, select **SecureSuite** and click the **Change** button. The **SecureSuite Installation Wizard** will appear. Click **Next** to continue.

3. Select **Modify** or **Repair**. The **SecureSuite Installation Wizard** guides you through the process.

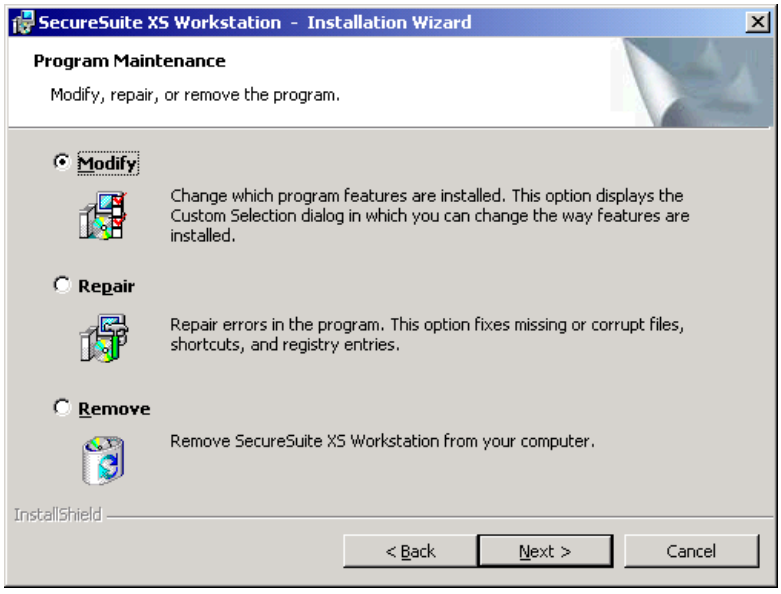

Figure 44: SecureSuite Installation Wizard

Installing OEM Device Modules

In order to utilize any of the advanced authentication devices supported by SecureSuite, the corresponding OEM device module, which contains the files necessary for your new device to work with SecureSuite, must first be installed on your system. If you followed the installation process in Chapter 3, you will not need to go through the following steps.

To install an OEM device module:

1. From the **Start** menu, select **Settings**, **Control Panel** and double-click **Add/Remove Programs**.

2. From the list of installed programs, select **SecureSuite** and click the **Change** button. The **SecureSuite Installation Wizard** will appear. Click **Next** to continue to the **Program Maintenance** screen.

3. Select the **Modify** option, and click **Next** to continue to the **Authentication Device(s)** screen.

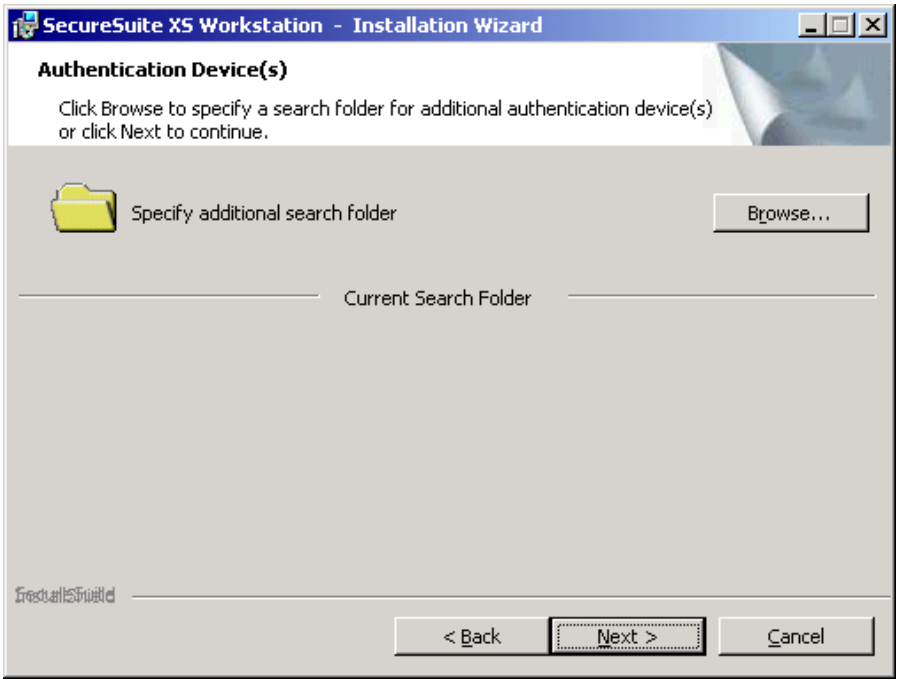

Figure 45: Specifying the Location of OEM files

4. Click the **Browse** button to specify (or verify) the location of the OEM files, which are necessary in order for your new authentication device to work with SecureSuite.

   - If you received the device with SecureSuite, these files were included with your installation software, and the current search folder may be the correct location.

   - If you received the device after SecureSuite was installed, be sure to specify the directory under which the OEM files are located.

5. Click **Next** to continue to the **Custom Setup** screen. In the **SecureSuite Components** list, under **Authentication Methods**, click the name of the device that you want to install, and select **This feature will be installed on local hard drive**. Click **Next** to continue.

6. Click **Install** to begin the installation process. Once the installation is finished, you will be informed that the installation was successfully completed. Click **Next** to continue.

7. Restart your machine. When your system reboots, the device will be available. You can add the device to user accounts via the **SecureSuite User Manager**, or configure the device's properties via the **SecureSuite System Settings** dialog.

Note: If users will be using advanced authentication devices in order to log on to a domain from their workstation and access domain resources, the respective OEM device module must be installed on both the client workstation and the domain server(s). Refer to the SecureSuite XS Server Guide for more information.

Removing OEM Device Modules

If you no longer want an authentication device to be available on your system, you must either deactivate the device, or completely uninstall the OEM device module from your system.

If you plan to use the same device *model* in the future, you should simply disable the device. The files necessary for operation of this device will be left on your system.

To disable an advanced authentication device:

1. From the **Start menu**, select **Programs**, **SecureSuite**, and click **SecureSuite System Settings.**
2. In the left pane, select the method under which the device you want to disable is categorized.
3. In the right pane, right-click the device, and select **Remove Device**.
4. Click **OK** to confirm device removal. The device will no longer appear in the right pane of the **SecureSuite System Settings** dialog and will not be available for users on your system.

If you need to reactivate this device in the future, follow the previous instruction in the *Installing OEM Device Modules* section.

If you do not plan on using this specific device *model* in the future, you should completely uninstall the OEM device module from your system.

To uninstall an OEM device module:

1. From the **Start** menu, select **Settings**, **Control Panel** and double-click **Add/Remove Programs**.

2. From the list of installed programs, select **SecureSuite** and click the **Change** button. The **SecureSuite Installation Wizard** will appear. Click **Next** to continue to the **Program Maintenance** screen.

3. Select the **Modify** option, and click **Next** to continue to the **Authentication Device(s)** screen.

4. Click **Next** to continue to the **Custom Setup** screen. In the **SecureSuite Components** list, under **Authentication Methods**, click the name of the device that you want to uninstall, and select **This feature will not be available**. Click **Next** to continue.

5. Click **Install** to begin the uninstallation process. Once the installation is finished, you will be informed that the "installation" was successfully completed. Click **Next** to continue.

6. Restart your machine. When your system reboots, the device will no longer be available.

If you decide to use this device in the future, you will need to completely reinstall the OEM device module by following the instruction in the *Installing OEM Device Modules* section.

Uninstalling SecureSuite XS Workstation

Important: You should unsecure any secured files and folders before you uninstall SecureSuite. Although SecureFolder includes an emergency data recovery utility, any files or folders that were secured while this feature was deactivated (or for which the passphrase has been lost or forgotten) will not be recoverable if you uninstall SecureSuite—you will not be able to access the data in the files or folders again, even if you re-install SecureSuite!

Important: Please turn off your screensaver before uninstalling SecureSuite. If the screensaver activates during uninstallation, you may not be able to recover your computer.

To uninstall SecureSuite XS Workstation:

1. From the **Start** menu, select **Settings**, **Control Panel** and double-click **Add/Remove Programs**.
2. From the list of installed programs, select **SecureSuite** and click the **Remove** button.
3. Select the **Remove** option from the installation options provided.
4. Restart your computer once the uninstallation wizard is complete.

Appendix 1: Troubleshooting

Following is a list of questions that frequently arise while using SecureSuite. For more comprehensive help with SecureSuite, refer to our online KnowledgeBase.

Common User Problems

Important: Please refer to the Sony® Puppy® installation guide ("Training Your Puppy Unit") included in your package or on the CD-ROM for specific instructions on the installation and use of your fingerprint identity device.

Q: How many fingers should I enroll?

A: Multiple fingerprint readings ensure access to authorized users. Also, if you enroll only one finger, and that finger becomes damaged, you may not be able to access your computer. Therefore, we recommend enrolling at least two fingers.

Q: What should I do if I have trouble enrolling or verifying my fingerprint?

A: If you have trouble enrolling or verifying a fingerprint, try touching the conductive material surrounding the sensor surface on both ends of the sensor, while centering the finger on the sensor. Hold your finger as parallel as possible to the fingerprint sensor surface when making contact to give the device a good, readable fingerprint to enroll or verify.

Q: If I have dry fingers how can I reduce false rejections and ease the enrollment of my fingerprints?

A: In case of dry fingers try these suggestions:

Clean the scanner surface.

Use a hand moisturizer.

Moisten your fingertips by breathing on the surface of your finger.

Rub your finger on your forehead before placing it on the fingerprint sensor.

Q: What do I do if my fingers are too moist and I cannot enroll my fingerprints or authenticate?

A: If your hands are too moist, wipe your finger before placing it on the fingerprint sensor.

Q: What happens if I remove my authentication device while my computer is on?

A: Removing your authentication device while your computer is running will cause your device to be unavailable for authentication purposes with SecureSuite. To use your device, reconnect it. For more information, please refer to the Sony Puppy installation guide.

Q: What do I do if my computer doesn't recognize my authentication device?

A: Try the following

- Try restarting your computer, and look to see if the device is being recognized.
- Make sure the device is firmly connected to the computer.
- Unplug the device, plug it back in, and restart your computer.
- Move the device to another USB port or PC card slot, depending upon your device, and restart your computer.

Appendix 2: Glossary

A

Account
See User account, Group, SecureSession account.

Account lockout
A SecureSuite security feature that locks a user account if a number of failed logon attempts occur within a specified amount of time, based on account policy lockout settings.

Administrator
A person responsible for setting up and managing domain controllers or local computers and their user and group accounts, assigning passwords and permissions, and helping users with networking issues. To use administrative tools such as SecureSuite User Manager, an administrator must be logged on as a member of the Administrators local group of the computer or domain respectively.

Application
A computer program used for a particular kind of work, such as word processing.

Application window
The main window for an application, which contains the application's menu bar and work area.

Authentication
Validation of a user's logon information.

Authentication credential
Information submitted for comparison during the verification and identification processes, such as a password, fingerprint characteristics, etc.

Authentication Device
Hardware, such as a fingerprint scanner, iris scanner, security token or smart card, used for proving a user's identity. Contrast with Authentication method.

Authentication Method
A means of proving user identity. SecureSuite supports many authentication methods, including the password, fingerprint, iris, token and smart card methods. For each authentication method (except the password method), there are multiple manufacturers, each of which produces multiple models of associated authentication device.

B

Biometrics
The automated technique of measuring a physical characteristic or personal trait of an individual and comparing that characteristic to a comprehensive database for purposes of identification.

C

Client
A computer that accesses shared network resources provided by another computer, called a server. See also Server, Workstation.

D

Decryption
The inverse of encryption.

Domain
In SecureSuite, a collection of computers defined by the administrator of a SecureSuite Server network that share a common directory database. A domain provided access to the centralized user accounts and group accounts maintained by the domain administrator. Each domain has a unique name. See also Workgroup.

Domain controller
In a SecureSuite XS Server domain, refers to the computer running Windows 2000 Server that manages all aspects of user-domain interactions, and uses information in the directory database to authenticate users logging on to domain accounts. One shared directory database is used to store security and user account information for the entire domain.

Domain name
Part of the Domain Name System (DNS) naming structure, a domain name is the name by which a domain is known to the network. Domain names consist of a sequence of labels separated by periods. See also Domain Name System (DNS).

Domain Name System (DNS)
DNS offers a static, hierarchical name service for TCP/IP hosts. The network administrator configures the DNS with a list of hostnames and IP addresses, allowing users of workstations configured to query the DNS to specify remote systems by hostnames rather than IP addresses.

E

Encryption
The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission or when it is stored on a transportable magnetic medium.

Enrollment
The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity.

Event
Any significant occurrence in the system or an application that requires users to be notified, or an entry to be added to a log.

Event logging
The SecureSuite process of recording an audit entry in the audit trail whenever certain events occur, such as services starting and stopping and users logging on and off and accessing resources.

G

Group
In SecureSuite User Manager, an account containing other accounts that are called members. The permissions and rights granted to a group are also provided to its members, making groups a convenient way to grant common capabilities to collections of user accounts. See also User account.

Group memberships
The groups to which a user belongs. Permissions and rights granted to a group are also provided to its members. In most cases, the actions a user can perform in SecureSuite are determined by the group memberships of the user account the user is logged on to.

I

Identification
A one-to-many comparison of an individual's submitted biometric sample against the entire database of biometric reference templates to determine whether it matches any of the templates and, if so, the identity of the enrollee whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity within a database, rather than verify a claimed identity. (Contrast with Verification.)

L

Log off
To stop using the network and remove your user name from active use until you log on again.

Log on
To provide a user name and password that identifies you to the network.

Logon time
For SecureSuite, a definition of the hours and minutes during which a user account has been in use.

O

OEM Device Module
The OEM-provided set of files necessary for an authentication device to work with SecureSuite. See also Original Equipment Manufacturer (OEM).

Original Equipment Manufacturer (OEM)
A biometric organization (manufacturer) that assembles a complete biometric system from parts, or a biometric module for integration into a complete biometric system.

P

Password bank
A database used for storing username, password and other personal information, to be released upon validation of an individual's identity.

R

Remote Access Service (RAS)
A service that provides remote networking for telecommuters, mobile workers, and system administrators who monitor and manage servers at multiple branch offices. Users with RAS on a SecureSuite computer can dial in to remotely access their networks for services such as file and printer sharing, electronic mail, scheduling, and SQL database access.

S

SecureSession account
A set of logon credentials that has been registered (stored for later submittal) with SecureSession. In SecureSession for Applications, a registered set of credentials needed to access an application window (and data set). In SecureSession for Internet Explorer, a user name and password required for access to a web site. You may have multiple SecureSession accounts for a single application or web site. For example, you might have more than one account with Microsoft Outlook or Hotmail, each of which requires a different set of logon credentials.

Server
In general, refers to a computer that provides shared resources to network users.

Single Sign-On
A service that coordinates multiple domain sign-on procedures into one authentication process. Single sign-on services reduce the time taken by users in sign-on operations to multiple domains, including a reduction in the possibility of such sign-on operations failing; improve security through the reduced need for a user to handle and remember multiple sets of authentication information; reduction in the time taken, and improved response, by system administrators in adding and removing users to the system or modifying their access rights; improved security through the enhanced ability of system administrators to maintain the integrity of user account configuration including the ability to inhibit or remove an individual user's access to all system resources in a coordinated and consistent manner.

U

User account
Consists of all the information that defines a user to SecureSuite. This includes such things as the user name and password required for the user to log on, the groups in which the user account has membership, and the rights and permissions the user has for using the system and accessing its resources. The accounts are managed with SecureSuite User Manager. See also Group.

User Manager
A SecureSuite tool used to manage the security for a computer. Administers user accounts, groups, and security policies.

User name
A unique name identifying a user account to SecureSuite. An account's user name cannot be identical to any other group name or user name of it's own domain or workgroup. See also User account.

User password
The password stored in each user's account. Each user generally has a unique user password and must type that password when logging on or accessing a server.

V

Verification
A comparison of two sets of biometrics to determine if they are from the same individual; or, in fraud prevention applications, a one-to-one comparison of a live finger and a previously enrolled record to ensure that the applicant is who he/she claims to be.

W

Workstation
Any networked computer using domain resources.

Appendix 3: A Table of SecureSuite Policies

Domain/System-Level SecureSuite Policies (Start, Programs, SecureSuite, SecureSuite System Settings, Policies)			
Policy	**Available Settings** (Default settings are **bold**)	**Limits settings of…**	**Depends on setting of…**
Allow users to add/remove/enroll authentication methods and devices	**Enabled** / User Defined	Allow management of authentication methods and devices (user-level)	None
Cache user credentials (only available if logged on to domain)	**Enabled** / User Defined	Cache authentication credentials (user-level)	None
Allow users to update authentication credentials	**Enabled** / User Defined	Allow user to update authentication credentials	None
Always require authentication for administrator tools	**Enabled** / Disabled	None	None
Always require authentication for user tools	**Enabled** / Disabled	None	None
Randomize domain passwords for “AND” users	**Enabled** / Disabled	Randomize domain password (user-level, if “AND” user)	Randomize domain passwords for all users
Randomize domain passwords for all users	Enabled / **User Defined**	Randomize domain passwords for “AND” users; Randomize domain password	None
When logging on or authenticating, provide audio voice prompts	Always / System logon only / **Never**	None	None
When logging on or authenticating, display the visual indicator	Always / System logon only / **Never**	None	None

User-Level SecureSuite Policies (Start, Programs, SecureSuite, SecureSuite User Manager, SecureSuite Policies)			
Policy	**Available Settings** (Default settings are **bold**)	**Limits settings of…**	**Depends on setting of…**
Allow user to add/remove/enroll authentication methods and devices	**Enabled** / Disabled	None	Allow users to manage their authentication methods and devices (system-level)
Cache authentication credentials (only available if logged on to domain)	**Enabled** / Disabled	None	Cache user credentials (system-level)
Randomize domain password	Enabled / **Disabled**	None	Randomize domain passwords for all users; Randomize domain passwords for "AND" users (if "AND" user)
Allow user to update authentication credentials	**Enabled** / Disabled	None	Allow users to update authentication credentials (system-level)
User-Level SecureFolder Policies (Start, Programs, SecureSuite, SecureSuite User Manager, Select User, User Properties, SecureFolder tab)			
Policy	**Available Settings** (Default settings are **bold**)	**Limits settings of…**	**Depends on setting of…**
Require authentication when copying, deleting, moving or renaming a secured folder	**Enabled** / Disabled	None	Require authentication for all SecureFolder operations
Require authentication when securing files or folders	Enabled / **Disabled**	None	Require authentication for all SecureFolder operations
Require authentication before opening secured files or folders	**Enabled** / Disabled / Authenticate after	None	Require authentication for all SecureFolder operations
Enable emergency recovery of secured files and folders	**Enabled** / Disabled	None	Support emergency recovery of secured files and folders (system-level)
Require authentication when viewing share information	**Enabled** / Disabled	None	Require authentication for all SecureFolder operations

Domain/System-Level SecureFolder Policies (Start, Programs, SecureSuite, SecureSuite System Settings, Applications, SecureFolder)			
Policy	**Available Settings** (Default settings are **bold**)	**Limits settings of…**	**Depends on setting of…**
Require emergency recovery of secured files and folders	Enabled / **User Defined**	Support emergency recovery of secured files and folders (user-level)	None
Require authentication for all SecureFolder operations	Enabled / **User Defined**	Require authentication when copying, deleting, moving or renaming a secured folder; Require authentication when securing files or folders; Require authentication before opening secured files or folders; Require authentication when viewing share information	None
User-Level SecureSession for Internet Explorer Policies (Start, Programs, SecureSuite, SecureSuite User Manager, select user, User Properties, SecureSession/IE tab, User Policies)			
Policy	**Available Settings** (Default settings are **bold**)	**Limits settings of…**	**Depends on setting of…**
Apply one-touch user logon	**Enabled** / Disabled	None	None
Require authentication before supplying web page information	Enabled / **Site Defined**	Require authentication before supplying web page information (site-level)	Require authentication for all SecureSession/IE operations
Require authentication when registering pages	Enabled / **Disabled**	None	Require authentication for all SecureSession/IE operations
Require authentication when managing registered page information	**Enabled** / Site Defined	Require authentication when managing registered page information (site-level)	Require authentication for all SecureSession/IE operations
Automatically submit registered page information	**Enabled** / Site Defined	Automatically submit registered page information (site-level)	None

Site-Level SecureSession for Internet Explorer Policies (Start, Programs, SecureSuite, SecureSuite User Manager, select user, User Properties, SecureSession/IE tab, select web form, More Info)			
Policy	**Available Settings** (Default settings are **bold**)	**Limits settings of…**	**Depends on setting of…**
Require authentication before supplying web page information	**Enabled** / Disabled	None	Require authentication for all SecureSession/IE operations; Require authentication before supplying web page information (user-level)
Require authentication when managing registered page information	**Enabled** / Disabled	None	Require authentication for all SecureSession/IE operations; Require authentication when managing registered page information (user-level)
Automatically submit registered page information	**Enabled** / Disabled	None	Automatically submit registered page information (user-level)
Domain/System-Level SecureSession for Internet Explorer Policy (Start, Programs, SecureSuite, SecureSuite System Settings, Applications, SecureSession/IE)			
Policy	**Available Settings** (Default settings are **bold**)	**Limits settings of…**	**Depends on setting of…**
Require authentication for all SecureSession/IE operations	Enabled / **User Defined**	Require authentication before supplying web page information; Require authentication when registering pages; Require authentication when managing registered page information	None
User-Level SecureSession for Applications Policies (Start, Programs, SecureSuite, SecureSuite User Manager, select user, User Properties, SecureSession/IE tab, User Policies)			
Policy	**Available Settings** (Default settings are **bold**)	**Limits settings of…**	**Depends on setting of…**
Apply one-touch user logon	**Enabled** / Disabled	None	None
Automatically submit registered application information	**Enabled** / App Defined	Automatically submit registered application information (application-level)	None
Require authentication when managing registered application information	**Enabled** / App Defined	None	Require authentication for all SecureSession/Apps operations
Require authentication before supplying application information	Enabled / **App Defined**	Require authentication before supplying application information (application-level)	Require authentication for all SecureSession/Apps operations
Require authentication when registering applications	Enabled / **Disabled**	Require authentication when registering applications (application-level)	Require authentication for all SecureSession/Apps operations

Application-Level SecureSession for Applications Policies (Start, Programs, SecureSuite, SecureSuite User Manager, select user, User Properties, SecureSession/IE tab, select web page, More Info)			
Policy	**Available Settings** (Default settings are **bold**)	**Limits settings of…**	**Depends on setting of…**
Automatically submit registered application information	**Enabled** / Disabled	None	Automatically submit registered application information (user-level)
Require authentication when managing registered application information	**Enabled** / Disabled	None	Require authentication for all SecureSession/Apps operations; Require authentication when managing registered application information (user-level)
Require authentication before supplying application information	**Enabled** / Disabled	None	Require authentication for all SecureSession/Apps operations; Require authentication before supplying application information (user-level)
Domain/System-Level SecureSession for Applications Policy (Start, Programs, SecureSuite, SecureSuite System Settings, Applications, SecureSession/Apps)			
Policy	**Available Settings** (Default settings are **bold**)	**Limits settings of…**	**Depends on setting of…**
Require authentication for all SecureSession/Apps operations	Enabled / **User Defined**	Require authentication when managing registered application information; Require authentication before supplying application information; Require authentication when registering applications	None
SecureLaunch Access Policy (Start, Programs, SecureSuite System Settings, Applications, SecureLaunch, during application registration process)			
Policy	**Available Settings** (Default settings are **bold**)	**Limits settings of…**	**Depends on setting of…**
SecureLaunch Access Policy	**Access with Authentication** / Access Allowed / Access Denied	None	None