Passfaces™ for Windows
Administration Guide

Release 0.9
September 2002
Copyright Notice

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any computer language, in any form or by any means, without the express written permission on Real User Corporation.

This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, is both a civil and criminal offense, punishable by law.

Trademark Information

Passface™ is a registered trademark of Real User Corporation.

All other company and product names are trademarks of their respective owners.

Patent Information

Passface technology is protected under US and other applicable patents.
# Passfaces for Windows Administration Guide

1. Introduction ........................................................................................................................... 3  
   1.1. Passfaces for Windows Overview ................................................................................... 3  
   1.2. Passfaces Technology .................................................................................................... 3  
   1.3. Application Components ............................................................................................... 4  
   1.4. How This Manual is Organized ..................................................................................... 5  
2. System Requirements ............................................................................................................. 6  
   2.1. Operating System Considerations ................................................................................ 6  
   2.2. Active Directory Access Permission Configuration ....................................................... 7  
3. The Passfaces for Windows Client ............................................................................................ 9  
   3.1. Installing the Passfaces for Windows Client ................................................................. 9  
   3.1.1. Removing Passfaces for Windows ........................................................................... 10  
   3.2. Client Software Overview ............................................................................................ 11  
   3.2.1. Enrollment ................................................................................................................ 11  
   3.2.2. Login ........................................................................................................................ 13  
   3.2.3. Changing Password/Passfaces ............................................................................... 14  
4. The Passfaces for Windows Administration Tool ................................................................. 16  
   4.1. Getting Started with the Administration Tool .............................................................. 16  
   4.1.1. Installing the Passfaces for Windows Administration Tool ...................................... 16  
   4.1.2. Removing the Passfaces for Windows Administration Tool .................................... 16  
   4.2. Overview of Passfaces for Windows Administration Tool .......................................... 16  
   4.2.1. Administrator’s Interface ......................................................................................... 17  
   4.2.2. User Logon problems ............................................................................................... 21  
5. User Setup Examples ............................................................................................................. 22  
   5.1. Enabling Passfaces for a User ....................................................................................... 22  
   5.2. To Change User’s Passfaces ......................................................................................... 24  
   5.3. To reset user back to password only ............................................................................ 25  
6. Getting Support .................................................................................................................... 27  
   6.1. README File ................................................................................................................ 27  
   6.2. World Wide Web ......................................................................................................... 27  
   6.3. E-Mail ........................................................................................................................... 27  
   6.4. Additional Resources .................................................................................................... 27
1. Introduction

Welcome to the Passfaces for Windows Administration Guide. This document will provide Systems Administrators with everything they need to know to install and configure the Passfaces for Windows product.

1.1. Passfaces for Windows Overview

Passfaces for Windows is an “out-of-the-box”, strong user authentication solution that can be installed in minutes on any Windows network.

Passfaces for Windows enables you to provide strong authentication for all users accessing your enterprise Windows networks, by providing them with the capability to either replace or enhance their existing passwords. It can be implemented on any Windows clients that authenticate to Windows domain controllers in a networked environment.

Used as a second factor authenticator (in conjunction with a password), Passfaces for Windows provides a clearly definable level of additional security and offers a practical, immediately deployable alternative to smartcards, tokens or biometrics.

The Passface system is completely intuitive to use and ensures 100% reliable access for all authorized users after only 3 to 5 minutes of (automated) training.

With Passfaces for Windows, password policies can be reviewed and revised to reduce administration costs and to improve user productivity and operations efficiency – thereby enabling enterprises to benefit from enhanced security and achieve a cash ROI gain.

1.2. Passfaces Technology

Like passwords and PINs, Real User’s Passface technology is a cognometric method of personal authentication - based on something known by the user and the system (a shared secret); however, instead of characters and numbers, it uses [photographs of] faces as its “alphabet”. Also unlike passwords and PINs, there is no requirement for the user to memorize the secret. Passfaces are self-prompting and the user only need recognize his secret during the authentication process. This underlying principle is supported by extensive academic research and cognitive psychology experiments. Passfaces for Windows implements this patented approach to user authentication based on sound scientific principles. The system works as follows:

- Users start by getting to know a group of (typically 3 to 6) faces – their Passfaces – which are assigned by the system at random from a large library of anonymous faces. This simple and intuitive initial familiarization process takes from 3 to 5 minutes for 5 Passfaces.

- To authenticate a user, the system displays a 3 by 3 grid of faces containing one Passface and 8 decoy faces positioned randomly within the grid.

- The user responds by indicating the position of their Passface in the grid. This challenge/response is repeated with each of the user’s remaining Passfaces – each time presented in a grid with 8 more decoy faces.

- The user is authenticated once all their Passfaces have been recognized successfully.
The Passface system is based on the human brain’s remarkable ability to recognize individual faces. This instinctive ability is completely universal: only one in eight million (sighted) people – suffering from a condition known as prosopagnosia – experience any difficulty in recognizing familiar faces.

**NOTE:** A more complete description of the training and logon processes is contained in Section 3.2 “Client Software Overview”.

### 1.3. Application Components

The *Passfaces for Windows* system is made up of two major components:

**Passfaces for Windows Client** – this module resides on each individual desktop and laptop PC, and, in conjunction with the standard Microsoft Windows Graphical Identification and Authentication (GINA) module provides the user interface for the entry of required information for authentication such as username, password, and Passfaces identification. It combines the password and Passface information into a single *credential* and submits it for validation to the standard Windows GINA module.

**Note:** Throughout this document the term *credential* will be used to refer to the string sent to the Network server for purposes of user authentication.

Like the standard Microsoft GINA module, it responds to, and is activated by the secure attention signal (usually ctrl-alt-delete), and prompts the user for input. It is also the module that performs the ‘get acquainted’ training when users first begin to use Passfaces, or when users change Passfaces.

**Passfaces for Windows Administration Tool** – This tool allows the System Administrator, or designated individuals, to perform many of those functions necessary to administer the authentication tasks of the system. Specifically, it provides for the following common administrative tasks:

- Reviewing all user accounts and their current authentication settings
- Configuring an account to use Passfaces in addition to a password
- Determining how many Passfaces each user will use
- Resetting a user’s password

The Administration Tool allows the administrator to configure users’ Passface authentication settings on the Windows domain controller. Although the Administration tool can be run on any networked computer that the administrator might normally use to manage user accounts, it prompts the administrator to select the domain controller where the user accounts to be viewed/modified are located. In the case where no networked domain controller is in use, the Administration Tool can also be used to configure accounts on the local machine thereby enabling *Passfaces for Windows* to be demonstrated and tested on standalone computers, without a domain controller. We’ll refer to this environment as “standalone mode” throughout the remainder of this document.

The Administration Tool only needs to be installed on networked computers used by the administrator to manage user accounts. It is expected that this tool will be used in conjunction with Windows’ existing tools for managing users and groups.
1.4. How This Manual is Organized

The remainder of this document is devoted to the specific tasks required to install, configure and utilize the Passfaces for Windows system.

Section 2 presents the system requirements for Passfaces for Windows.

Section 3 discusses the Passfaces for Windows Client Application.

Section 4 provides the details of the Passfaces for Windows Administration Tool.

Section 5 walks you through some real world examples of how to use the product.

Section 6 offers some options for obtaining support.
2. System Requirements

2.1. Operating System Considerations

*Passfaces for Windows* is designed for the following Microsoft Windows client (workstation) versions:

- Windows NT 4.0 Workstation
- Windows 2000 Professional
- Windows XP Professional
- Windows 95 and 98 (Contact Real User for details)

It is primarily intended for use in environments where workstations authenticate to a domain controller running one of the following Microsoft Windows server versions:

- Windows NT 4.0 Server
- Windows 2000 Server
- Windows .NET Server

However, *Passfaces for Windows* can also be installed and used on standalone workstations that authenticate locally. This feature can be useful both for demonstration purposes and to enable system administrators to familiarize themselves with the features and concepts of *Passfaces for Windows* before deploying it across their organizational domains.

It is recommended, although, except where noted, it is not essential, that the latest Microsoft Windows service pack for each operating system be applied before installing *Passfaces for Windows*.

For some server versions, and for some workstation/server combinations, additional configuration steps need to be taken to configure the workstation or server for *Passfaces for Windows*. The following table illustrates these requirements.

<table>
<thead>
<tr>
<th>Client OS</th>
<th>Server OS</th>
<th>Windows NT4.0 Server</th>
<th>Windows 2000 Server</th>
<th>Windows .NET Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows NT4.0 Workstation</td>
<td>No additional</td>
<td>See notes 1 and 2</td>
<td>See notes 1 and 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>configuration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows 2000 Professional</td>
<td>No additional</td>
<td>See note 1</td>
<td>See note 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>configuration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows XP Professional</td>
<td>No additional</td>
<td>See note 1</td>
<td>See note 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>configuration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>required</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note 1.** Where Windows 2000 Server (or later) is used as the domain controller, configuration changes need to be applied to the domain controller to adjust access permissions. This is described fully in section 2.2 “Active Directory Access Permission Configuration” (below).
**Note 2.** In *mixed mode domains*, where Windows NT 4.0 workstations authenticate to Windows 2000 (or later) domain controllers, Microsoft Active Directory Client Extensions need to be installed on the Windows NT 4.0 workstations where *Passfaces for Windows* is to be installed. This update is available for free download from Microsoft’s web site and is also included with CD distributions of *Passfaces for Windows*. This update requires Microsoft Windows NT 4.0 with SP6 and Microsoft Internet Explorer 4.01 or higher. Simply run the DSClient.exe (found in the “Utilities” folder of the product distribution) program on each NT 4.0 workstation and follow the instructions. See [http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/adextension.asp](http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/adextension.asp) for more details about this update.

---

**Additional information...**

**How Passfaces for Windows stores its user configuration data**

*Passfaces for Windows* stores configuration information about each user (e.g., whether or not the user is using Passfaces, which Passfaces to present, etc) in a standard Windows attribute associated with each user account. The attribute used is the “user comment” field (LDAP name “comment”). This rarely used field is present as part of NT4.0’s user account information and is an attribute of the Active Directory “User” object on Windows 2000 domain controllers (and later).

By using an existing Windows user attribute, and one that is present across all of the Microsoft “enterprise” operating systems, *Passfaces for Windows* avoids the need for any additional server software or user databases. The major advantage of this approach is that the users’ Passface configuration data will be automatically maintained, managed, replicated across domain controllers and backed up and restored with Windows’ existing user database (or Active Directory).

Similarly, no additional user secret data storage is required. *Passfaces for Windows* combines password data and Passfaces data into a character sequence that is stored using Windows’ existing password storage and authentication mechanisms.

If your organization already makes use of the “user comment” attribute, or if you would prefer to specify another user attribute for storage of *Passfaces for Windows* configuration information, then please contact Real User Corporation to discuss this option.

---

### 2.2. Active Directory Access Permission Configuration

*Passfaces for Windows* uses the “user comment” attribute to store its per-user configuration (see the additional information box above). In order that this attribute can be used by *Passfaces for Windows*, domain controllers using Active Directory (that is Windows 2000 and .NET servers) require two changes to be made to their access rights permissions.

The first change is a standard Windows 2000/.NET option which would normally be used to provide compatibility with clients running pre-Windows 2000 operating systems that require certain types of access to user configuration information. This is required by *Passfaces for Windows* (regardless of the client operating system) in order that users’ Passface configuration information can be retrieved from Active Directory before the user has logged on.

1. To change this permission setting type the following command into a command prompt on the Windows 2000 domain controller when logged on as an administrator:

```bash
net localgroup "Pre-Windows 2000 Compatible Access" everyone /add
```
Then restart the domain controller.

**Note: should you wish to undo this change, you can do so by typing:**

```
net localgroup "Pre-Windows 2000 Compatible Access" everyone /delete
```

For more details on this setting please see:


The second change allows a program that is running as a logged on user to update the “user comment” attribute of that user’s account. This may be achieved by running the PFWRights.exe program provided in the “Utilities” folder of the *Passfaces for Windows* product distribution.

2. Log on as an administrator and run the PFWRights.exe program on the Windows 2000 domain controller.

The following screen will appear:

![Passfaces For Windows Set Server Access Rights](image)

This program adds or removes an access right to all users allowing the logged on user write access to their own account’s “user comment” attribute.

The “user comment” attribute (LDAP name “comment”) is a rarely used attribute of each user within Active Directory. *Passfaces for Windows* uses this attribute to store each user’s passface configuration.

Currently, write access to this attribute is DISABLED. Enable write access to allow *Passfaces for Windows* to be used.

Enable write access to “user comment” attribute by ‘SELF’

This program allows you to add this access right that is required by *Passfaces for Windows*. This same program allows you to remove this access right if *Passface for Windows* is no longer to be used.
3. The Passfaces for Windows Client

The Passfaces for Window client should be installed on all workstations that might be used by any users who you intend to convert to use Passfaces.

3.1. Installing the Passfaces for Windows Client

Before installing Passfaces for Windows on a Windows workstation, please ensure the following:

- If you are using a Windows 2000 (or later) domain controller, the necessary access permission changes have to be configured on the domain controller computer. See section 2.2 “Active Directory Access Permission Configuration” for more details.
- If you wish to install Passfaces for Windows on an NT 4.0 workstation that is part of a Windows 2000 domain (where the domain controller is running Windows 2000), first ensure that Microsoft Active Directory Client Extensions are installed on the workstation. See section 2 for more details.

To install Passfaces for Windows:

1. Log on to the workstation as an administrator.
2. Run the setup.exe program provided in the “Client” folder in the product distribution.
3. You will be asked to choose the location to which the Passfaces for Windows files will be copied.
4. Once installation is complete, you will be asked whether you want to reboot your computer now or later.

When you reboot after installing Passfaces for Windows, you will see the Passfaces for Windows logon screen. Users can log-on as normal by entering a username and password. To upgrade users to use Passfaces, use the Passfaces for Windows Administration Tool, available to the Administrator from any workstation that has access to the network location where the program was installed. (Please refer to section 4 for full details).
**Additional information...**

*What is done during installation?*

This information is provided for administrators who want to automate the deployment of *Passfaces for Windows*. Other readers are advised to ignore this information!

Having installed *Passfaces for Windows* on a single workstation, the installed files can be copied to the other workstations’ file systems and the registry setting changed remotely (for example using Microsoft’s Remote Registry Service). This avoids having to run the setup program on each workstation.

The files copied by the *Passfaces for Windows* setup program are as follows:

| Files copied to the windows system folder (for example c:\winnt\system32) | pfwadsi.dll  
idapfc.dll |
| Files copied to the location chosen during installation | rugina.dll  
images (folder and contents)  
images\faces (folder and contents) |

The installation process also creates or modifies a string value in the following key in the Registry of each workstation:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon
```

The string value is called “GinaDll” and its value should be the location of the rugina.dll file on the local workstation (for example C:\Program Files\Real User Corporation\Passfaces Windows Logon\RUGina.DLL).

Should it be necessary to re-install or upgrade *Passfaces for Windows*, first remove *Passfaces for Windows* following the instructions below. *Passfaces for Windows* can then be re-installed normally.

### 3.1.1. Removing *Passfaces for Windows*  

**Important:** Before removing *Passfaces for Windows* from a workstation, first ensure that at least one administrator account can log on without requiring Passfaces.

Remember that once *Passfaces for Windows* has been removed, any users who are using Passfaces will no longer be able to log on. You can rectify this situation (before or after removing *Passfaces for Windows*) by resetting the passwords of all user accounts that currently use Passfaces to logon. This can be done using either the Passfaces for Windows Administration Tool or standard Windows methods for resetting user passwords.

To remove *Passfaces for Windows*:

1. Open Windows “Control Panel”
2. Choose “Add/Remove Programs”
3. Select “Passfaces for Windows”.
4. Once the removal has completed you should restart the computer.

Note that removing *Passfaces for Windows* does not change existing users’ Passface configuration. If necessary, *Passfaces for Windows* can be removed and re-installed from a
workstation without users having to change their Passfaces. As noted above, however, when Passfaces for Windows is removed, those users who are using Passfaces will not be able to log on until Passfaces for Windows is re-installed, or their passwords reset using available Windows tools.

### Additional information...

#### Emergency removal

If for any reason Passfaces for Windows needs to be removed from a system where the administrator cannot log on normally (for example, if the Passfaces for Windows DLLs are corrupted or inadvertently removed) proceed as follows:

1. Boot into Safe Mode (without network support)
2. Use regedit to delete the string value “GinaDll” in the registry key:
   
   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon
   ```
3. Reboot the computer
4. The files listed above can now be deleted if required or Passfaces for Windows can be reinstalled normally.

---

### 3.2. Client Software Overview

This section will highlight some of the more important features of the client interface. Given the intuitive nature of the software, no separate User’s Guide is required.

#### 3.2.1. Enrollment

It is best if the user can be given advanced notice of the strategy to migrate him/her to the use of Passfaces in conjunction with their password. As with password changes, the user should not be forced to do this at an inopportune time when immediate access to an application or service is more important.

The Passfaces enrollment process trains the user with a new set of Passfaces. The process is optimized to take approximately no more than 5 minutes for most users. The user is first shown his/her Passfaces, as shown below, and given some time to study them.
Then, screens with a 3x3 grid of faces, each screen containing one Passface and 8 other faces (decoys), like the ones the users will experience when they log on, are displayed. For training purposes, the one Passface on each screen is highlighted for the user to easily recognize. The user selects their highlighted Passface from each screen, and then the process repeats. Each successive repeat gives the user more time to select their Passfaces on their own, before a hint is given. The user can go through his training until they feel comfortable with the process.

**Additional information…**

**Extra Precautions**

If the environment is considered susceptible to shoulder surfing, the entire enrollment and login process can be carried out without the use of the mouse. The numeric keypad, with NumLock on, maps to the grid of faces in the standard configuration for face selection. The number one (1) on the keypad maps to the face in the lower left position, the number five (5) maps to the face in the center, etc. The screen transitions, ‘next’ and ‘previous’, can be carried out using the ‘n’ and ‘p’ keys.

A ‘shoulder surfer’ would need to watch the user’s hand AND his screen simultaneously to gain any relevant information.

**NOTE:** It is important that users utilize their Passfaces at least once within a few days of enrollment. In trials conducted at the University of London for users who used their Passfaces to
logon during the week following enrollment, close to 100% were able to recognize them 3 to 6 months later. We encourage you to stress the benefit of this step to your users.

3.2.2. Login

Once a user has been through the Passfaces training process, and has converted to Passfaces, the logon process will begin with the user ID and password component as with the classic Microsoft logon process. The interface will appear only slightly different from the traditional Microsoft screen, and is depicted below.

After entering user ID and password, the user will be presented with the Passfaces identification screens.
The user then needs to recognize and select their Passfaces just as they did during the training. Once the password has been entered, and Passfaces have been recognized and selected, the authentication step is performed on the Windows Domain controller. Both components must be correct for login to occur. In this way, no information is given about which component is potentially incorrect.

Any activity that requires the user to enter his network password (e.g. password change or unlocking the PC) will now also require the recognition of the user’s Passfaces.

### 3.2.3. Changing Password/Passfaces

The user will be able to change his password using `ctl-alt-del` whenever he chooses, just as before. His Passfaces will remain unchanged by this activity, provided you have not scheduled the user to receive new Passfaces at change of password (more details on this will be presented when we discuss the Administration Tool).
When users are scheduled to receive new Passfaces, they will not be prompted to change their password at the same time. If they wish to change it subsequently, they may do so. This is done to keep the process more user friendly.

**NOTE:** Changing *either* component of the credential, Passfaces or password, results in a new authentication credential.
4. The Passfaces for Windows Administration Tool

4.1. Getting Started with the Administration Tool

The two sections that follow describe the steps required to install and remove the Administration Tool Software.

4.1.1. Installing the Passfaces for Windows Administration Tool

The Passfaces for Windows Administration Tool should be installed on the computer (or computers) that the administrator uses to manage user accounts. This could be the domain controller itself or a workstation on the network. It is designed to be used in conjunction with existing Windows administrative programs.

To install the Passfaces for Windows Administration Tool:

1. Log on to the workstation as an administrator.
2. Run the setup.exe program provided in the “Administration” folder in the product distribution.
3. You will be asked to choose a location to which to copy the Passfaces for Windows Administration Tool files.

Once installation is complete you can launch the Passfaces for Windows Administration Tool from the Windows “Start” menu by selecting “Programs” and clicking the “Passfaces Administration” icon.

Additional information...

Note that once the Passfaces for Windows Administration Tool is installed, it can be run from any machine on the network that has access to the network location where the program was installed. The information that you can view or update with this tool will depend on the access rights of the account under which you are running. It is therefore recommended that you run this program as an administrator.

4.1.2. Removing the Passfaces for Windows Administration Tool

To remove the Passfaces for Windows Administration Tool:

1. Open Windows “Control Panel”
2. Choose “Add/Remove Programs”
3. Select “Passfaces for Windows Administration”.

Note that removing the Passfaces for Windows Administration Tool does not change existing users’ Passface configuration or prevent users from logging on using Passfaces.

4.2. Overview of Passfaces for Windows Administration Tool

The Passfaces for Windows Administration Tool is designed to streamline the configuration process that adds Passfaces to the user’s authentication credential. Its straightforward approach allows you to control the introduction of Passfaces to the user, the frequency of change for the Passfaces, and the number of faces that will be used.
In the event that a user of Passfaces forgets his password, the tool makes it easy to reset the password through the same screens.

### 4.2.1. Administrator’s Interface

A series of windows allows the Administrator to perform all the actions required to administer Passfaces for Windows.

**Domain Selection**

When first invoking the Administration Tool, the System Administrator must select the Domain to be acted upon. The drop down box provided in this screen allows the Administrator the ability to easily select the Domain on which they wish to work.

The Passfaces for Windows Administration Tool is used in conjunction with Windows existing password policy and user management tools. The Windows tools provide capabilities to add and delete users. The Passfaces for Windows Administration Tool provides capabilities to select users to adopt Passfaces; select users to obtain new Passfaces, and to reset the users credential to be just a password. All new users must be added with the Windows management tool before any action can be taken with respect to them in the Passfaces for Windows Administration Tool.

**Additional information…**

**Password Changes**

NOTE: It is important to remember to use only the Passfaces for Windows Administration Tool to reset passwords for users once Passfaces have been enabled. Using the Windows Administration capabilities to change the password for an account with Passfaces will result in an inaccessible account. This is because Passfaces are still enabled as part of the credential (by the Passfaces Administration Tool), yet the credential is being reset to use only the password (by the Windows Administration tool). Using the Passfaces for Windows Administration Tool will assure the appropriate changes are made to remove Passfaces from the credential before resetting it.
Main *Passfaces for Windows* Administration Screen

The *Passfaces for Windows* main Administration screen is depicted below, along with an explanation of the attributes. For each user the following information is available or can be configured by you using the *Passfaces for Windows* Administration Tool.

1. **User Name** – List of authorized users of this Domain as listed in the chosen Domain controller.
2. **Group(s)** – Groups to which each user belongs.
3. **Using Passfaces** - This is a status indicator. It reads ‘yes’ when the user is currently using Passfaces as a component of their authentication credential, ‘no’ when they are not.
4. **Train at Change PW** (password) - This setting is used for initial enrollment of the user in the Passfaces system or to force the user to change their Passfaces the next time they change their password.
5. **Number of Passfaces** - There are two entries in this column. The number without brackets is the number of Passfaces currently in use by the user. The number in brackets is the number currently set in the properties for future use. If the “train at change PW” indicates that the user is set to get new Passfaces with the next Password change, then this is the number of Passfaces they will have after that training.
6. **Properties** – When selected will invoke the detailed Properties screen to allow parameter changes for all selected users.
**NOTE:** To effect changes to a user's status, always begin by highlighting that row. To effect changes to multiple users simultaneously, hold down the **shift** key to select a block of names, or hold down the **Ctrl** key to select multiple, non-adjacent names.

**Single User Configuration Screen**

When a single user has been selected (highlighted), and the Properties button chosen, a detailed screen will be displayed allowing changes to be made to the selected user.

- **Current Passface status for selected user**
- **Checkbox that determines if the user will be required to adopt Passfaces when they next change their password. This works for both the initial enrollment, as well as subsequent Passface changes.**
- **Checkbox enabled for those users already selected to receive Passfaces at next password change, indicating whether a new password will be required at that time or not.**
- **Number of Passfaces that will be assigned when the user enrolls or when they next change their Passfaces**
- **Button that invokes a window allowing the Administrator to reset this user to utilize just a password. This capability can be used whether or not the user has been using Passfaces as part of the authentication credential. (See Reset Password Screen below)**
Multi-user Configuration Screen

When multiple users have been chosen in the main Passfaces Administration Screen and the Properties button selected, a Properties box, much like the one above, is presented to allow changes that will affect all users that were selected.

![Multi-user Configuration Screen](image)

- **Require users to adopt Passfaces when they next change their Password.**
- **Checkbox indicating whether users will be allowed to retain their existing password when enrolling with Passfaces.**
- **Number of faces to be presented at enrollment or when the user next changes their Passfaces.**

Reset Password Screen

When the “Reset to Password” button is selected on the single user configuration screen the Administrator is given the ability to reset a user authentication credential to just a password.

![Reset Password Screen](image)

The new password must be entered exactly the same in the “New password” and “Confirm new password” boxes. Failure to do so will cause the reset operation to fail.

The “User must change password at next logon” checkbox is the default setting and forces the user to change their password again when they next logon. This is to allow the entry of a temporary password by the Administrator that requires changing at the next available opportunity.
Additional information…

Requiring a Password Change

It is important to remember that resetting a user's credential to a password effectively removes the Passface authentication step from that account, and resets the password to something that the System Administrator has chosen, or that the user has chosen rather quickly. In either case, there is a higher likelihood of the user having trouble remembering that password. Therefore, we encourage you to leave the “User must change password at next logon” box checked to require the user to reset the password to something they have thought about and chosen, when they next access the account.

NOTE: This option, to force a password change at next logon, is not currently supported in standalone mode under Windows XP.

As noted above, when utilizing the “Reset to Password” functionality, the use of Passfaces is removed from user's account. When this is done, the “Upgrade to Passface at password change” option is automatically selected on the configuration screen. In this way, when next the user changes their password, Passfaces will be re-enabled for the account. The Administrator can keep the account with only a password by unchecking the “Upgrade to Passfaces at password change’ box for this user.

NOTE: To enhance usability, for the initial introduction of a set of Passfaces, the user will be prompted to train on his Passfaces without changing his password. If the user wishes to also change his password, he can do so subsequently using Ctrl-Alt-Del. The introduction of Passfaces or a change of Passfaces alters the authentication credential even when the password remains unchanged.

4.2.2. User Logon problems

If the user is experiencing difficulties with his logon, the administrator can reset the user's credential by following the steps in Reset Password below, after determining the identity of the user in accordance with the enterprise security policies.
5. User Setup Examples
The sections below provide detailed examples of how to perform some of the more common operations with the Passfaces for Windows Administration Tool.

5.1. Enabling Passfaces for a User

It is recommended that users be given warning when Passfaces will be enabled, so that they can be introduced to their new Passfaces when it is reasonably convenient for them to do so. To enhance usability, for the initial introduction to a set of Passfaces, users will be prompted to train on their Passfaces without changing their password. If the user wishes to also change her/his password, (s)he can do so subsequently using Ctrl-Alt-Del. The introduction of the Passfaces effectively changes the (combined) network logon credential without changing the password.

To migrate a user to Passfaces:

- Highlight the user(s) of interest. User ‘pbarrett’ is highlighted in the example below.

- Click on the Properties button to work in the configuration window
- Check the Box “Upgrade to Passfaces at password change”
- Set the Number of Passfaces that the user will be required to use, four (4) in this case.
Click OK. The “Train at Change PW” entry in the Administration window will now be ‘YES’. When the user has enrolled, “Train at change PW” will be reset to “NO” and ‘Using Passfaces” will be set to “YES”. Note that the number of Passfaces is set to four (4), that’s the number to the left, and the number of Passfaces to supply at next change is also set to four (4), keeping the number of faces consistent for this user, unless explicitly changed.
If the user is using Passfaces, and Train at Change PW is toggled to “NO” (the default setting once the user has enrolled with Passfaces), then the user can change his password without changing his Passfaces. Each password change results in a new authentication credential.

5.2. To Change User’s Passfaces
The screen shot below shows the configuration for user ‘pwood’ that will provide new Passfaces for him at the next password change. In this example, ‘pwood’ will be changed to 5 Passfaces for the new set, from the 2 being used at this time.
The Admin screen below shows the status for ‘pwood’ after he has completed the change operation and adopted his new Passfaces. As discussed in a note above, to keep the introduction to a new set of Passfaces user friendly, the user will not be prompted to change his password at this time. Changing either component changes the authentication credential.

5.3. To reset user back to password only

This functionality should be used if it is necessary for you to change the user’s password (e.g. if the user is locked out of the system) for users who are also using Passfaces.

1. After highlighting the row of the user concerned, click Properties to access the Passfaces Configuration screen
2. Click reset password.
3. The ‘reset password’ screen allows you to assign a temporary password and force the user to change his password at his next logon. This setting is checked by default as a security precaution.
4. Click OK to return to the Configuration screen.
5. Also checked by default, as a result of the password reset, is the ‘Change Passfaces at password change’ in the Configuration dialog screen. If this box is unchecked by the administrator before closing the Configuration dialog screen, the user will no longer use Passfaces (as they will not be prompted to acquire a new set of Passfaces when they next log on or change their password).

Because authentication secrets today are not known by anyone other than the user, it is not possible to retain the user’s old Passfaces as part of the new authentication credential when assigning a temporary password. The first logon after the administrator’s reset will be based on the temporary password only. When the user is prompted to select a new password, he will be trained on new Passfaces as well. For this reason, procedures for identifying the individual requesting the reset should follow enterprise policy.
NOTE: Do not use Windows tools to reset the password of individuals using Passfaces. Doing so will not reset the indicator in Passfaces for Windows that says the individual is using Passfaces, and thus the user will be prompted to select Passfaces that are no longer valid. In this case the user will not be able to logon.
6. Getting Support
In the unlikely event you should have difficulty using this product, there are several ways in which you can obtain assistance.

6.1. README File
This file, included with the software, includes any new information not available at the time this manual was printed.

6.2. World Wide Web
Within the products section of our web site, www.realuser.com, you'll find information on new releases, technical updates, or issues regarding the product.

6.3. E-Mail
Send us e-mail at support@realuser.com describing your problem. Please be sure to include the Passfaces for Windows version number, the operating system and release you are using, and as much detail about the error as you can.

6.4. Additional Resources
This document describes how to utilize the Passfaces for Windows product. For more information on the impact of Passfaces for Windows on Security Policies, how and why Passfaces work, as well as other topics, users are encouraged to read.

- **Strategies for using Passfaces for Windows** – This document discusses the impact that Passfaces for Windows can have on your organization’s authentication policies and procedures.
- **The Science Behind Passfaces** – This document presents the scientific case underlying Passface technology.
- **Passfaces FAQ sheet** – An accumulation of answers to questions concerning the products and technology.
- **Real User website (www.realuser.com)** – Here you will find other white papers and information about the company, technology, and products.

Use of the Passfaces for Windows product assumes a certain level of familiarity with Windows administration. For information concerning those tasks at the Windows levels, users should consult the help available from Windows operating system.

And finally, users can learn much more about security and the authentication process itself by consulting a book such as “Authentication – From Passwords to Public Keys” by Richard E. Smith.