

DigitalPersona® Pro

Password Manager

Version 5.2

Application Guide



digitalPersona.

© 1996-2011 DigitalPersona, Inc. All Rights Reserved.

All intellectual property rights in the DigitalPersona software, firmware, hardware and documentation included with or described in this guide are owned by DigitalPersona or its suppliers and are protected by United States copyright laws, other applicable copyright laws, and international treaty provisions. DigitalPersona and its suppliers retain all rights not expressly granted.

U.are.U® and DigitalPersona® are trademarks of DigitalPersona, Inc. registered in the United States and other countries. Windows, Windows Server 2003/2008, Windows Vista, Windows 7 and Windows XP are registered trademarks of Microsoft Corporation. All other trademarks are the property of their respective owners.

This DigitalPersona Pro Enterprise Administrator Guide and the software it describes are furnished under license as set forth in the “License Agreement” screen that is shown during the installation process.

Except as permitted by such license, no part of this document may be reproduced, stored, transmitted and translated, in any form and by any means, without the prior written consent of DigitalPersona. The contents of this manual are furnished for informational use only and are subject to change without notice.

Any mention of third-party companies and products is for demonstration purposes only and constitutes neither an endorsement nor a recommendation. DigitalPersona assumes no responsibility with regard to the performance or use of these third-party products.

DigitalPersona makes every effort to ensure the accuracy of its documentation and assumes no responsibility or liability for any errors or inaccuracies that may appear in it.

Feedback

Although the information in this guide has been thoroughly reviewed and tested, we welcome your feedback on any errors, omissions, or suggestions for future improvements. Please contact us at

TechPubs@digitalpersona.com.

or DigitalPersona, Inc.
720 Bay Road
Suite 100
Redwood City, CA 94063
USA

Table of Contents

1	Product Overview	5
	Introduction	5
	Personal logons vs Managed logons	5
	Central Management	6
	Installation	6
	Configuration	6
	Licensing	8
	User interfaces	8
2	Centralized management	9
	Policies and settings	9
	Pro Enterprise (Active Directory) settings	9
	Web Console settings	11
	Reporting	12
	Password Manager events	12
3	End user experience	13
	Managed logons and personal logons	14
	Adding logons	14
	Editing logons	15
	Organizing logons into categories	16
	Managing your logons	16
	Assessing your password strength	17
	Using the logons menu	17
	Settings	18
	Using managed logons	18
	Logging On	18
	Changing passwords	18
4	Additional features	19
	Password Manager Pro	19
	Overview	19
	About folders and groups	20
	Setting up Password Manager Pro	21
	Managed logons	23
	Creating managed logons	23
	Logon Fields attributes	27
	Values	28
	Logon properties	29
	Creating logons manually	33
	Deploying managed logons	35
	Logon Fields actions	36

Table of Contents

Setting Up a Change Password screen	38
Password policies	40
Setting up a Change Password Screen manually	42
Regular Expression syntax	45
Managing logons	47
Editing logons	47
Deleting logons	48
Deploying logons	48
The Field Catalog	49
Adding fields to the Field catalog	49
Example: Use of Field Catalog for password	49
Finding fields in logons	50
Tools page	51
Finding logons	51
Finding Duplicate Logons	51
5 Glossary	52
6 Index	56

This chapter contains the following topics.

Topics	Page
Introduction	5
Installation	6
Configuration	6
Licensing	8
User interfaces	8

Introduction

DigitalPersona Password Manager and DigitalPersona Password Manager Pro enable users to easily and more securely log on to Windows, websites, applications and network resources through the use of *personal logons* and *managed logons*.

Password Manager logons facilitate the use of stronger passwords, since the passwords don't have to be remembered or written down. Password Manager allows users to log on to resources with any designated authentication credentials or combination of credentials.

Password Manager is included as a core feature in DigitalPersona Pro Enterprise and DigitalPersona Pro Workgroup.

Password Manager *Pro*, used for creating managed logons (described below), is included with the Authentication and Ultimate editions of DigitalPersona Pro Enterprise and DigitalPersona Pro Workgroup.

Personal logons vs Managed logons

Password Manager by default provides a means for end-users to create and manage personal logons for automated logon to Windows, websites and applications. Managed logons, on the other hand, are created, deployed and managed by an administrator using the optional DigitalPersona Password Manager Pro application. Managed logons provide all of the same benefits to the end user, but provide greater flexibility and control to the administrator. See the *Additional features* chapter for details on Password Manager Pro.

Central Management

Centralized management of DigitalPersona Password Manager features is available through Active Directory (via DigitalPersona Pro Enterprise) or through the web consoles of DigitalPersona Pro Workgroup and HP ProtectTools Management Console. IT Administrators may also choose to allow local administrators to manage features if required by their organization, and configure different levels of administration for specified groups.

Major central management features include:

- Enabling and disabling Password Manager
- Specifying whether users may view passwords for managed logons
- Allowing users to add/edit/delete their account data for managed logons
- Designating the location where managed logons are stored.

For additional information on central management features, see *Centralized management on page 9*.

Installation

The DigitalPersona Password Manager security application is a core feature of the DigitalPersona Pro Enterprise, DigitalPersona Pro Workgroup and HP ProtectTools Management Console solutions. There is no separate installation required.

Password Manager *Pro* is an optional and separately licensed administrative tool which requires installation and licensing. For further details on Password Manager Pro, see *Additional features on page 19*.

Configuration

Password Manager is enabled by default in all editions of DigitalPersona Pro Enterprise, DigitalPersona Pro Workgroup and HP ProtectTools Management Console.

There is a computer policy setting that can be used by an administrator to remove the Password Manager features and UI from the client dashboard. This setting is defined below for supported central management solutions. Additional settings available are described in the Centralized Management chapter.

DigitalPersona Pro Enterprise

Initial configuration of the Password Manager application is through an Active Directory Administrative Template. The name of the template is “DigitalPersona Password Manager Administrative Template,” and the filename is DPPasswordManager. The template should be applied to GPOs (Group Policy Objects) where it can be distributed to computers running the Password Manager application.

Prevent Password Manager from running

You can prevent Password Manager from being displayed in the client dashboard using the following setting, located at:

Computer Configuration\Policies\Administrative Templates\DigitalPersona Pro Client\Managed Applications\Disable Applications.

- If enabled, the Password Manager application is not available to the user.
- If disabled or not configured, the Password Manager application is available.

Web Console settings

The following setting is provided through DigitalPersona Pro Workgroup's Web Console.

Password Manager setting

Initial configuration of the Password Manager application is through the "Password Manager" setting on the Computers and Users, Applications tab. (This setting contains additional options as described in the Centralized Management chapter.

- If enabled or not configured, the Password Manager application is available, supporting both personal and managed logons.
- If disabled, Password Manager is not available to the user.

Licensing

Licenses for the Password Manager application are included in, and automatically deployed during, the installation of all editions of DigitalPersona Pro Enterprise, DigitalPersona Pro Workgroup and HP ProtectTools Management Console.

User interfaces

Password Manager functionality is provided at three levels: Centralized Management, End-user, and Additional features. Each level is described in one of the following chapters.

Chapter	Description	Page
Centralized management	Through Active Directory and GPOs	9
End user experience	In compatible client's user dashboard	13
Additional features	In the Administrative Console provided through all compatible clients except DigitalPersona Kiosk	19

This chapter includes the following topics.

Topics	Page
Policies and settings	9
Reporting	12
Password Manager events	12

DigitalPersona Password Manager may be managed through one of the following central management solutions: DigitalPersona Pro Enterprise, DigitalPersona Pro Workgroup or HP ProtectTools Management Console.

DigitalPersona Pro Enterprise is an Active Directory-based solution and provides GPO settings that may be used to manage various aspects of Password Manager.

DigitalPersona Pro Workgroup and HP ProtectTools Management Console provide configuration of management settings through a built-in web-based console.

Central management of DigitalPersona Password Manager is exposed through a single setting described below, identical in each of the supported management solutions.

Password Manager features, as described in the *End-user experience* chapter, are enabled by default in all compatible clients. To disable, or otherwise configure Password Manager, see the policies and settings described in the following topics for each supported management solution.

Policies and settings

Because settings for Password Manager are slightly different in the supported management solutions, they are described below separately for Pro Enterprise and for the web console used in DigitalPersona Pro Workgroup and HP ProtectTools Management Console.

Pro Enterprise (Active Directory) settings

Prevent Password Manager from running

You can prevent Password Manager from being displayed in the client dashboard using the following setting, located at:

Computer Configuration\Policies\Administrative Templates\DigitalPersona Pro Client\
Managed Applications\Disable Applications.

- If enabled, the Password Manager application is not available.
- If disabled or not configured, the Password Manager application is available.

Allow creation of personal logons

You can allow users to create and use personal logons for websites and programs using this setting, located at:

User Configuration\Policies\Administrative Templates\DigitalPersona Pro Client\
Managed Applications>Password Manager.

- If enabled or not configured, personal logons are available.
- If disabled, personal logons are not available.

Managed logons

You can configure additional settings for managed logons which govern the access to account data and deployment to users with this setting, located at:

User Configuration\Policies\Administrative Templates\DigitalPersona Pro Client\Managed
Applications>Password Manager.

If enabled you can select which managed logon policies will be enforced. If not disabled or not configured none of the listed managed logon policies will be enforced.

Available policies are:

- Allow users to view managed logon passwords: If enabled or not configured, users are allowed to view their managed logon passwords after verifying their identity. If disabled, users are not allowed to view managed logon passwords.
- Allow users to edit account data: If enabled or not configured, users can edit their own account data. If disabled, users cannot edit account data.
- Allow users to add account data: If enabled or not configured, users can add to their account data. If disabled, users cannot add new account data.
- Allow users to delete account data: If enabled or not configured, users can delete their account data. If disabled, users cannot delete their account data.
- Path(s) to the managed logons folder(s): If enabled, the logons are copied to the computers that have this setting applied. You can specify multiple folders by separating the paths with a pipe character (|). If disabled or not configured, no copy operation will be performed.

Web Console settings

The following setting is provided through the DigitalPersona Pro Workgroup Web Console.

Password Manager

The Password Manager setting enables and sets policies for the creation and use of personal and managed logons.

This setting is located in the web console at the Computers and Users/Applications tab.

- If enabled or not configured, Password Manager supports both personal and managed logons, and specific policies can be set which govern the behavior of Password Manager.
- If disabled, Password Manager is removed from the client dashboard.

When enabled, the following policies can be set.

- *Allow creation of personal logons*: If enabled or not configured, personal logons are allowed. If disabled, personal logons are not allowed.
- *Allow users to view managed logon passwords*: If enabled or not configured, users are allowed to view their managed logon passwords after verifying their identity. If disabled, users are not allowed to view managed logon passwords.
- *Allow users to edit account data*: If enabled or not configured, users can edit their own account data. If disabled, users cannot edit account data.
- *Allow users to add account data*: If enabled or not configured, users can add to their account data. If disabled, users cannot add new account data.
- *Allow users to delete account data*: If enabled or not configured, users can delete their account data. If disabled, users cannot delete their account data.

Reporting

DigitalPersona Password Manager writes Activity Events to the local Windows Event Viewer Event Log, under the Pro\Password Manager node, whenever a designated activity occurs on the client.

For a listing of Password Manager events, see the table below.

For additional information on the initial setup and configuration of DigitalPersona Reporter, including a list of currently available reports, see the Reporter chapter in the Administrator Guide for the specific management solution being used.

Note that events are only reported on for clients with valid activated licenses.

Password Manager events

Task Category: 1536

These activity events may be generated during Password Manager operations.

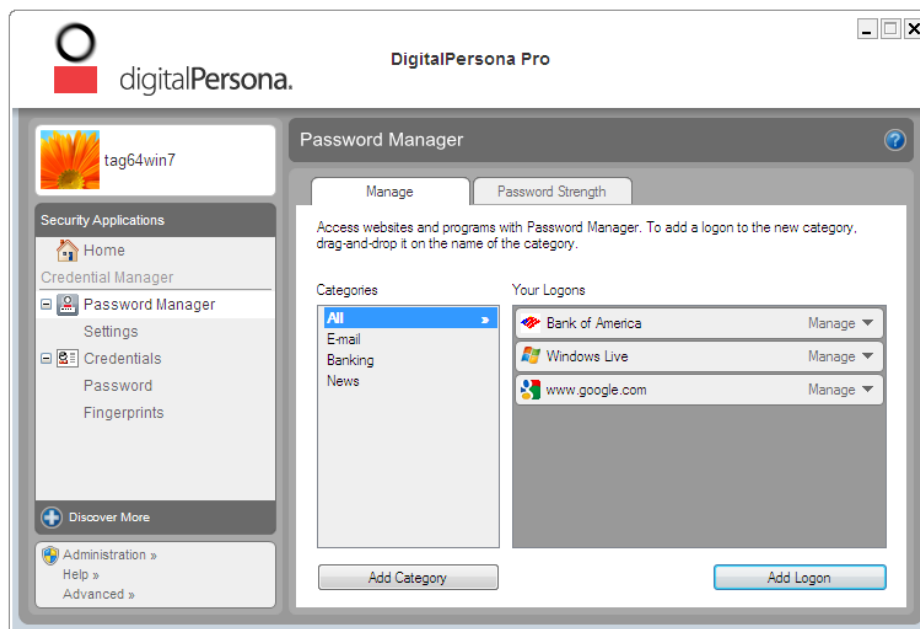
Event	ID	Level	
		Srvr	Wks
Password change was canceled by user.	1541		Dt
Initial Fillin was performed.	1544		Dt
Fillin was performed.	1545		A
Account data could not be modified	1546		E
Account data was successfully modified.	1547		A

Level: E = Error, A - Audit, Dt = Details, Fd = Fine details

This chapter includes the following topics.

Topics	Page
Managed logons and personal logons	14
Adding logons	14
Editing logons	15
Organizing logons into categories	16
Managing your logons	16
Assessing your password strength	17
Using the logons menu	17
Settings	18
Using managed logons	18

Logging on to Windows, websites, and applications is easier and more secure when you use Password Manager. You can use it to create stronger passwords that you don't have to write down or remember, and then log on easily and quickly with a fingerprint, smart card, or your Windows password.



Password Manager provides the following options:

- Personal logons - Add, edit, or delete personal logons and logon account data from the Manage tab.
- Managed logons - Add, edit or delete logon account data for managed logons provided by your administrator through the Password Manager Pro application.
- Use personal or managed logons to launch your default browser and log on to any website or program.
- Drag and drop to organize your logons into categories.
- See at a glance whether any of your passwords are a security risk.

Once a logon has been created for a website or program, the Password Manager icon displays whenever that screen is launched. Click the icon to display a context menu containing commonly used commands.

Managed logons and personal logons

Managed logons are created, managed and deployed by an administrator using the Password Manager Pro application in the Administrative Console of supported clients.

In most cases, the first time a managed logon is used, you will be asked for your personal account logon data for a resource. Whether account data is requested, and what type of data is required is determined when the managed logon is created, and also governed by settings described in the Centralized management chapter beginning on page 9.

If account data is required, it is only entered once. On subsequent use of the logon, account data will be filled in automatically.

Additionally, many options are provided for customizing the use of managed logons for your environment. See the *Additional features* chapter beginning on page 19 for a description of the Password Manager Pro application.

Personal logons are created by an individual for their own use. Account data is entered during the creation of the logon, and filled in automatically during subsequent use of the logon. This chapter primarily addresses the use of personal logons, although much of the information also applies to the use of managed logons.

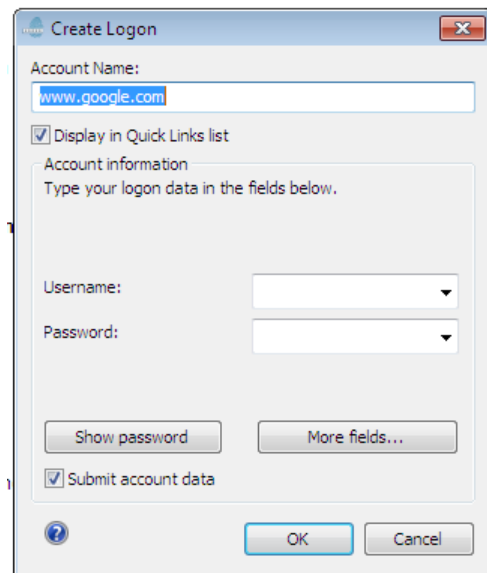
Adding logons

You can easily add a logon for a website or a program by entering the logon information once. From then on, Password Manager automatically enters the information for you. You can use these logons after browsing to the website or program, or click a logon from the Logons menu to have Password Manager open the website or program and log you on.

To add a logon:

- 1 Open the logon screen for a website or program.
- 2 On the Password Manager page, click the **Manage** tab and then click **Add Logon**.

- 3 Enter your logon data. Logon fields on the screen, and their corresponding fields on the dialog box, are identified with a bold orange border.
 - To populate a logon field with one of the preformatted choices, click the arrows to the right of the field.
 - To view the password for this logon, click **Show password**.
 - To have the logon fields filled in, but not submitted, clear the **Submit account data** check box.
- 4 If Password Manager does not display the required logon fields, click **More fields**. Then select the check box for each field that is required for logon, or clear the check box for any fields that are not required for logon.
- 5 If Password Manager cannot detect all of the required logon fields, a message is displayed asking if you want to continue. Click **Yes** to enter manual mode.



Manual mode - A dialog is displayed with your logon fields filled in. Click the icon for each field and drag it to the appropriate logon field, and then click the button to sign into the Web site.

Once you use the manual mode of entering the logon data for a site, you must continue to use this method to log on to the same website in the future.

The manual mode of entering logon data is available only with Internet Explorer 8.

Each time that you access the “trained” website or program, the Password Manager icon is displayed, indicating that you can use any of your enrolled credentials to log on.



Editing logons

To edit a logon, follow these steps:

- 1 Open the logon screen for a website or program.
- 2 To display a dialog box where you can edit your logon information, click the arrow on the Password Manager icon, and then click **Edit logon**. Logon fields on the screen, and their corresponding fields on the dialog box, are identified with a bold orange border.

You can also display this dialog box by clicking **Edit** for the desired logon on the Password Manager **Manage** tab.

- 3 Edit your logon information.

- To populate a logon field with one of the preformatted choices, click the arrows to the right of the field.
 - To add additional fields from the screen to your logon, click **More fields**. To have the logon fields filled in, but not submitted, clear the **Submit account data** check box.
 - To view the password for this logon, click **Show password**.
- 4 Click **OK**.

Organizing logons into categories

Use categories to keep your logons in order by creating one or more categories. Then drag and drop your logons into the desired categories.

To add a category:

- 1 From the dashboard, click **Password Manager**.
- 2 Click the **Manage** tab, and then click **Add Category**.
- 3 Enter a name for the category.
- 4 Click **OK**.

To add a logon to a category:

- 1 Place your mouse pointer over the desired logon.
- 2 Press and hold the left mouse button.
- 3 Drag the logon into the list of categories. Categories are highlighted as you move your mouse over them.
- 4 Release the mouse button when the desired category is highlighted.

Your logons are not moved to the category, but only copied to the selected category. You can add the same logon to more than one category, and you can display all of your logons by clicking **All**.

Managing your logons

Password Manager makes it easy to manage your logon information for user names, passwords, and multiple logon accounts, from one central location.

Your logons are listed on the Manage tab in the client dashboard. Each logon includes an entry for the website, program or other resource, and an indented entry for each set of account data created for the resource.

To manage your logons:



From the dashboard, click **Password Manager**, and then click the **Manage** tab.

- Add a new logon - Click **Add Logon** and follow the on-screen instructions.
- Add an additional account to a logon - Click the logon, click **Manage** and then click **Add**.
- Edit a logon - Click a logon, click **Manage**, then **Edit**, and change the logon data.
- Delete a logon - Click a logon, click **Manage**, and then click **Delete**.

Assessing your password strength

Using strong passwords for logon to your websites and programs is an important aspect of protecting your identity.

Password Manager makes monitoring and improving your security easy with instant and automated analysis of the strength of each of the passwords used to log on to your websites and programs.

To check the strength of the passwords you use for your logons:

From the dashboard, click **Password Manager**, and then click the **Password Strength** tab.

- Double-click a logon to see an assessment of the strength of the password used for the logon.
- Click **Show password** to see the password.

Using the logons menu

Password Manager provides a fast, easy way to launch the websites and programs for which you have created *personal* logons. Double-click a program or website logon from the **Logons** menu to open the logon screen and automatically fill in your logon data.

Managed logons may also be created by your administrator, and may display on the Logons menu.

When you create a logon, it is automatically added to your Password Manager Logons menu.

To display the Logons menu, do one of the following:

- Press the Password Manager hot key combination. `ctrl+win+h` is the factory setting. To change the hot key combination, click Password Manager, and then click Settings.
- Scan your fingerprint (on computers with a built-in or connected fingerprint reader).



Settings

You can specify settings for personalizing Pro Workstation:

- *Open Password Manager with ctrl+win+h* - The default hot key that opens the Password Manager Logons menu is ctrl+win+h. To change the hot key, click this option and enter a new key combination. Combinations may include one or more of the following: ctrl, alt or shift, and any alphabetic or numeric key.

Using managed logons

If you are deploying managed logons to your users, this topic contains information that you will want to make sure is passed on to them. The same information is also included in the end-user help file included with compatible clients.

Logging On

After creating managed logons and deploying them to users, users will be able to launch a logon screen and verify their identity with their specified credentials.

Logon screens that have a logon created for them display the Password Manager icon on the screen.



Depending on the attributes defined by the logon administrator, the logon process may vary.

- A user can be automatically logged on, with all fields populated and submitted, simply by verifying their identity.
- The user may need to supply information for required fields the first time they use the logon, but be automatically logged on subsequently.
- If a user has multiple sets of account data, they will be prompted to select the account they wish to log on to in the **Select Account Data** dialog box.

Changing passwords

After creating logons and deploying them to users, managed password screens display the Password Manager icon on the screen. After verifying their identity, the user is asked to provide an old password, a new password and to confirm the new password.

Depending on the logon attributes, the change password process may vary.

- The user can be allowed to choose a new password with or without constraints on the password content.

A new random password can be automatically generated, in which case the user must log on with alternate credentials.

This chapter covers the following topics:

Topics	Page
Setting up Password Manager Pro	21
Creating managed logons	23
Creating logons manually	33
Setting Up a Change Password screen	38
Regular Expression syntax	45
Setting up Password Manager Pro	21
Managing logons	47
The Field Catalog	49
Tools page	51

Password Manager Pro

Password Manager Pro enables administrators to provide controlled access to websites or programs by adding a variety of authentication mechanisms (such as password, smart card, fingerprint or facial recognition) to their logon and change password screens. Password Manager Pro is an optional, separately purchased and licensed security application which displays its functionality through the Administrator Console once installed.

Overview

Setting up a managed logon screen is as simple as specifying attributes (such as the user name, password, the submit button and other required fields) in a logon for the website or program. Password Manager Pro also provides many configurable options for defining and reusing information for logon and change password screens.

The change password process can also be automated and controlled, by specifying constraints such as the minimum and maximum password length, letters or numbers only, and other format restrictions.

These managed logons can then be automatically deployed to computers where the Password Manager application is installed and which are being managed by a DigitalPersona Pro server.

After managed logons are deployed, they are made available to managed computers after their next restart, or after a specified time interval as configured by the administrator.

- The Password Manager icon displays on screens for which managed logons have been created.
- The user is guided through the process of logging on or changing their password.



Depending on the settings applied by the administrator, the user may be prompted for account data, such as user name, password, and other information during the first logon. During subsequent logons, the account data is provided by Password Manager after the user's identity is confirmed by supplying the credentials required by the Session Authentication Policy in effect.

About folders and groups

DigitalPersona Pro uses the terms folder or group to identify the set of managed logons that are made available to member computers, depending on the specific DigitalPersona solution.

DigitalPersona Pro Enterprise uses shared *folders* for the location of managed logons.

The DigitalPersona Pro Workgroup Web Console uses *groups* to control managed logons.

DigitalPersona Pro Enterprise

In DigitalPersona Pro Enterprise, managed logons are organized in shared folders created and maintained for Password Manager Pro.

The folder should be created on a shared network drive accessible to the DigitalPersona Pro Enterprise server in order to make the logons available for deployment. However, the folder may be created on a local drive for initial testing and later copied to a shared drive. Folders are created and managed from the Logons tab in the Administrative Console.

For instructions on setting up Password Manager Pro for Pro Enterprise, see the topic, *Setting up Password Manager Pro* on the next page.

Web Console

In DigitalPersona Pro Workgroup, managed logons are created and managed in Password Manager Pro through the same group structure used to specify security settings shared by all computers managed by the installed server solution.

However, the groups themselves must first be created and then managed from the Web Console, or from the Administrative Console of a managed workstation.

For instructions on creating groups, see the topic *Managing groups* in the Administrator Guide for your installed server solution.

Setting up Password Manager Pro

This topic applies to DigitalPersona Pro Enterprise only.

Before using Password Manager Pro, you will need to set it up.

Create a shared network folder

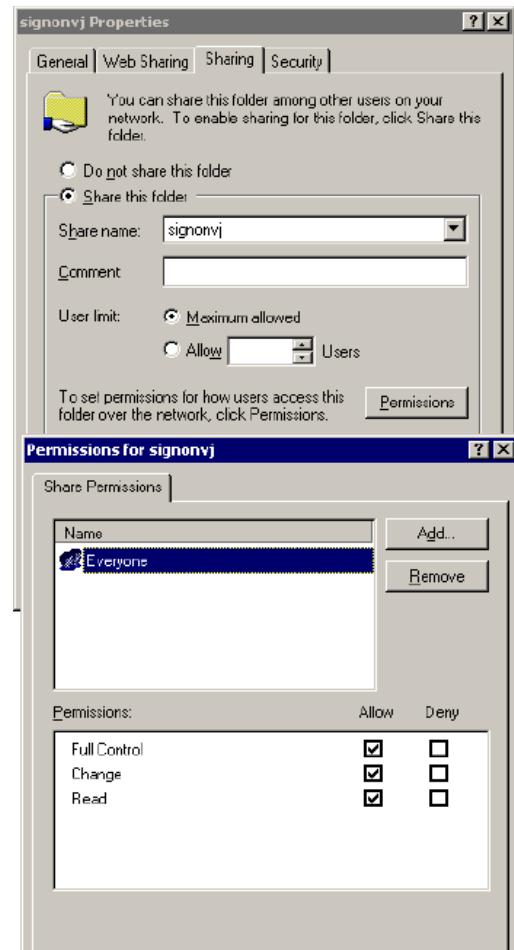
Create a shared folder on the network drive to store Password Manager Pro managed logons and assign appropriate permissions to the users.

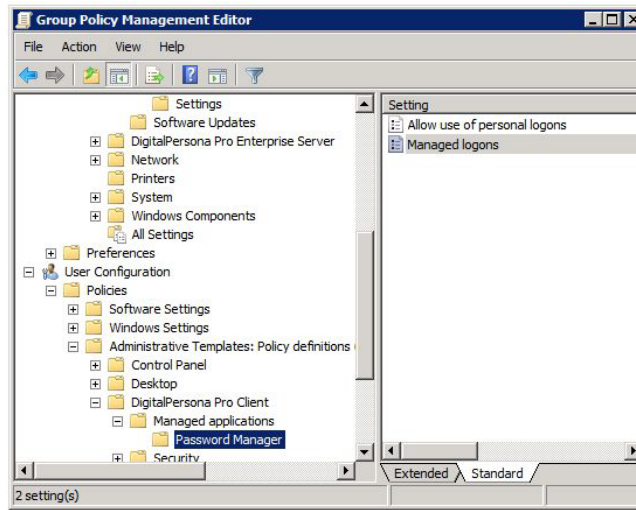
The folder should be created on a shared network drive accessible to the DigitalPersona Pro Enterprise server in order to make the logons available for deployment. However, the folder may be created on a local drive for initial testing and later copied to a shared drive. Folders are created and managed from the Logons tab.

- 1 Create a folder on the server/computer where you will store the managed logons. To create a folder or manage the logons contained in a folder, click **Choose a folder**.
- 2 Share the folder that you just created to allow users to access it.
- 3 Right click on the folder and click on **Properties** in the context menu.
- 4 Click on the **Sharing** tab.
- 5 Verify the permissions by clicking on the **Permissions** button.

Set up the GPO policy

- 1 The Workstation Administrative Template, DPPro5Client(admx/adm) file must be added to the Active Directory Computer Configuration folder in the Administrative Templates folder of the Group Policy Management Editor. For further details on administrative templates, see “Install the Administrative Templates” on page 43.
- 2 Open the GPO where the DigitalPersona template was added.
- 3 Go to User Configuration\Administrative Templates\DigitalPersonaPro Client\Password Manager.

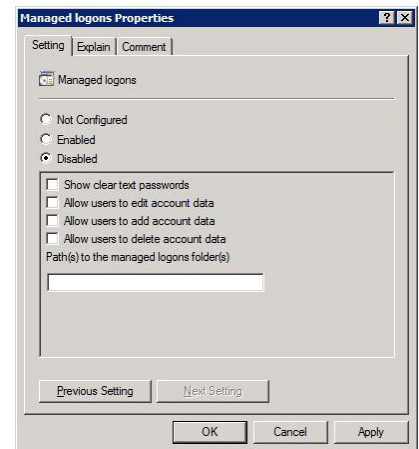




- 4 Double click on **managed logons** (in the right pane).

The default setting is "Not Configured". Click on **Enable** to enable this policy, and then type in the path to the shared folder that you previously created.

- 5 The new setting will be applied to all DigitalPersona Pro clients during the usual refresh interval or the next time they restart Windows.



Managed logons

Password Manager Pro managed logons are used to store attributes such as; the user name, password, the submit button, other required fields and screen information for Logon and Change Password screens.

These managed logons are stored in a shared folder specified in a GPO setting in Active Directory. From there they can be deployed to specific groups of end-users managed by the server. Users of the companion product, Password Manager, on computers managed by DigitalPersona Pro Enterprise, will then automatically have access to the managed logons.

- Managed logons are downloaded to client computers as soon as they are set up to be managed, and at intervals specified by the administrator.
- Note that credentials entered by the end-user for a website or program do not “roam” on the network, and are only available on the computer where they were entered.

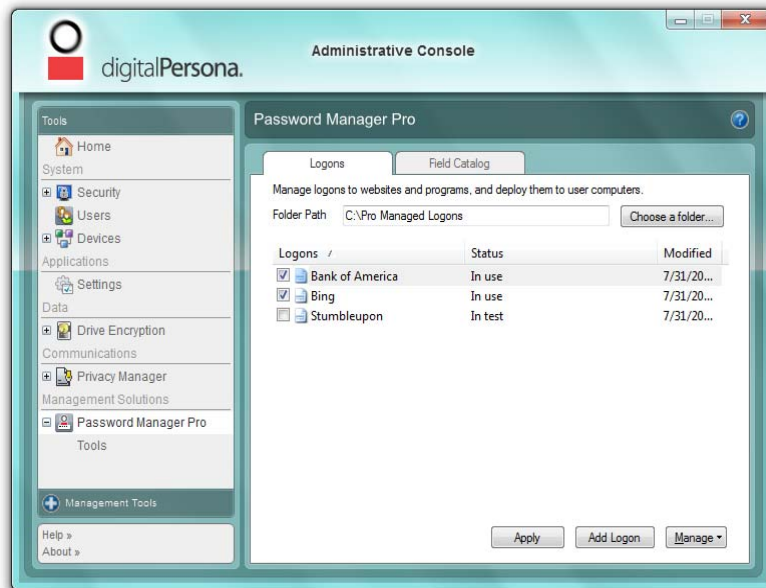
Password Manager Pro includes intuitive wizards that will guide you through the few steps necessary to automatically create a managed logon and an optional change password screen for most websites and programs. For more complex screens, there is also a manual mode that provides more sophisticated options for matching the logon or change password process to non-standard screens.

Creating managed logons

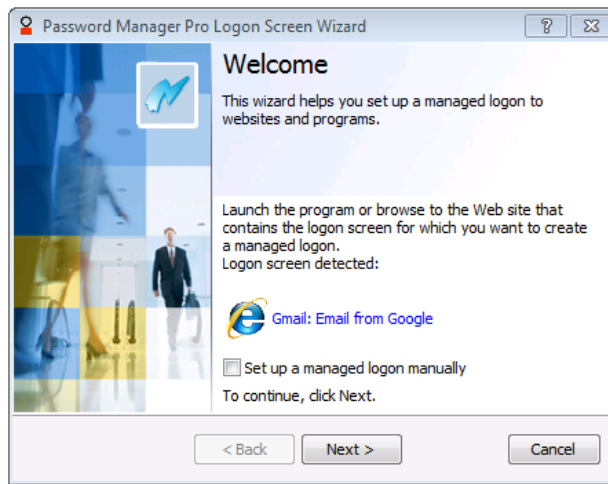
Password Manager Pro managed logons are used to store attributes such as; the user name, password, the submit button, other required fields and screen information for Logon and Change Password screens.

To create a managed logon for a logon screen:

- 1 From within the Administrative Console, launch the Password Manager Pro application.



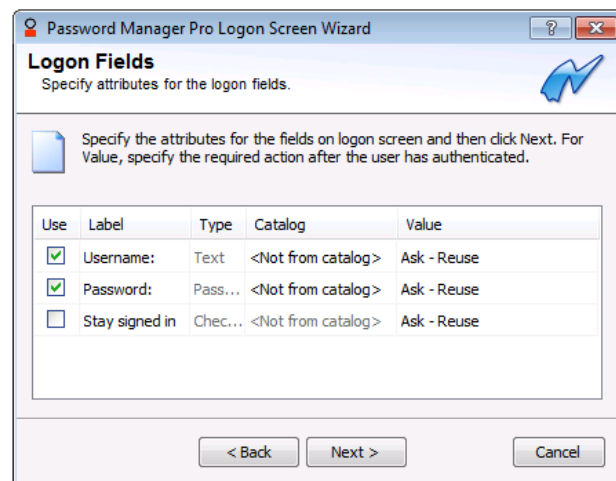
- 2 On the Logons tab, select **Choose a folder**. Click one of the recently used locations, or specify a path and click Browse for folder to add a folder to the list. Then click **Choose**.
- 3 Click **Add Logon**. The Password Manager Pro Logon Screen Wizard launches.
- 4 Launch the logon screen for the password-protected website or program.
- 5 On the first page of the wizard, confirm that the logon screen has been detected and verify the title of the logon screen. Click **Next**.



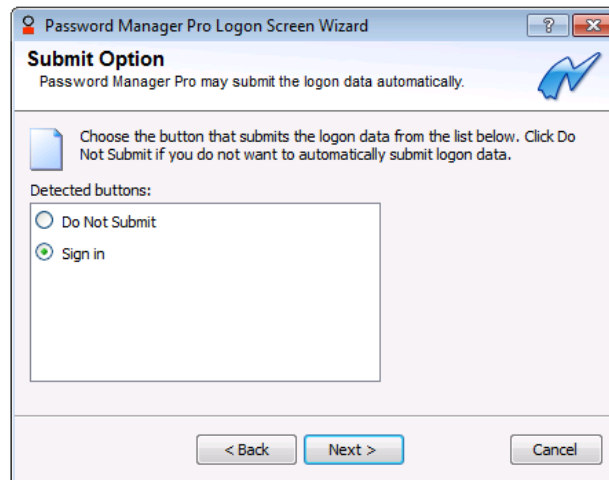
For websites or programs that are difficult for the wizard to detect automatically, such as terminal emulator programs, you can create a logon manually by selecting **Set up a managed logon manually**. This provides additional control for specifying the fields and keystrokes required for logon. Further details on manual creation can be found at “Creating logons manually” on page 33.

- 6 The **Logon Fields** page displays all the fields on the logon screen, using the nearest label to identify each field.

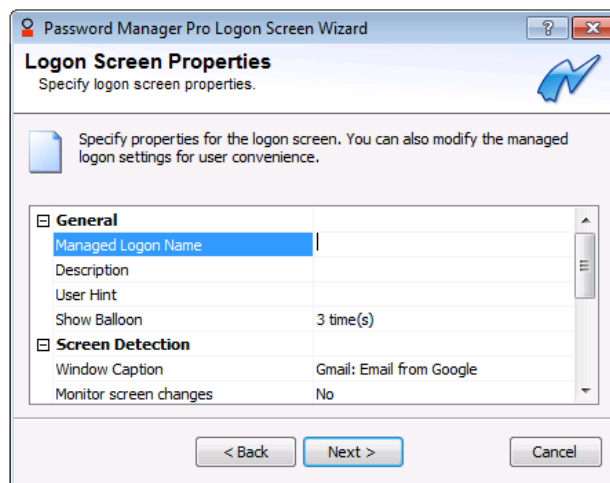
Select which fields are required for logon, set their desired attributes (see page 27) and values (see page 28) and then click **Next**.



- 7 On the **Submit Option** page, choose the button that submits the logon data.



- You can edit the button labels by clicking the label and typing a new name.
 - If you want the user to manually submit the logon data, select Do Not Submit.
- 8 Click **Next** to display the **Logon Screen Properties** page, where you can view and modify the various properties (see page 29) for the Logon Screen.

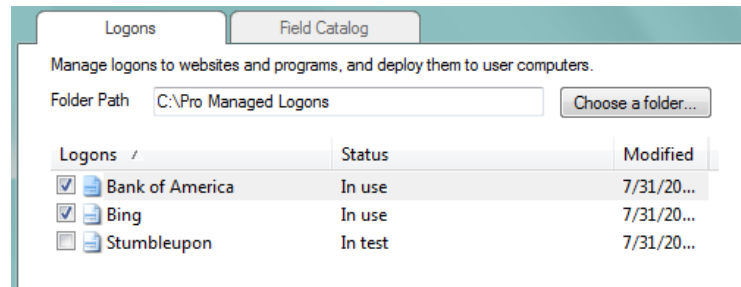


- 9 Click **Next**, and then click **Finish** to create the logon and close the wizard.
- 10 In the Administrative Console's Logon tab, click **Apply** to save your changes to the server.

You do not have to click **Apply** after making *each* change, but be aware that you *do* need to click **Apply** before any new logons or changes to logons will be saved to the server.

To deploy managed logons:

- 1 Check the boxes next to logons to change their status from In Test to In Use. Only logons with an "In Use" status will be visible to your end-users.



- 2 Click **Apply**.
- 3 After a managed logon is deployed to a computer, the Password Manager icon on the end-user's screen signifies that they can fill in the requested account data by verifying their identity with the required credentials.

Notes:

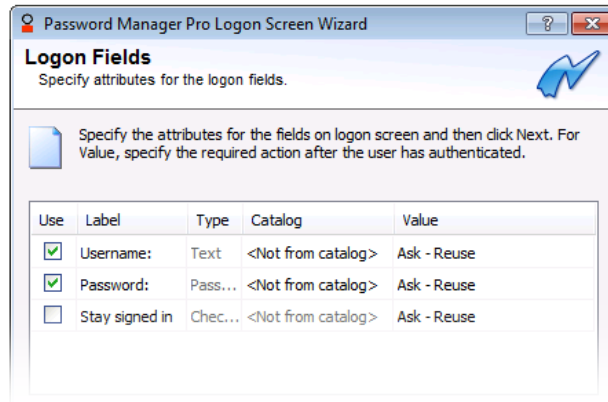
Managed logons, created by Password Manager Pro take precedence over any *personal* logons created for the same screen by end-users of the Password Manager application. The corresponding personal logon will no longer be able to be used to log on, but can be opened by clicking **Edit** in order to retrieve their account information.

If more than one administrator is using Password Manager Pro at the same time, they should make sure not to make changes to logons at the same time; as only the last applied changes will be deployed.

See Also: "Creating logons manually" on page 33.

Logon Fields attributes

Logon Fields attributes are used in the Logon Screen Wizard during the creation of managed logons and Change Password screens.

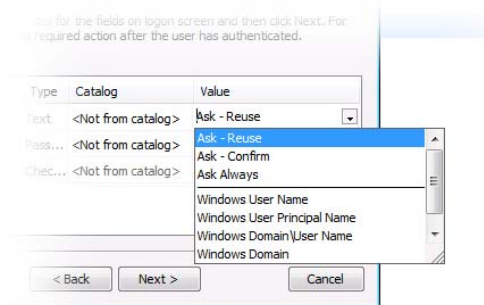


Column headings specify the attributes for each field on a Logon Screen or Change Password screen.

Field	Description
Use	Check the Use checkbox for each field used for log on. Some fields discovered by the wizard may not be relevant to log on, such as a search field on a website logon page. Leave these unchecked.
Label	If the label for a field is not intuitively related to the corresponding field on the logon screen, type a new label. The labels are displayed when users are prompted to type a value for a logon field.
Type	The type of field, either text or password, is displayed in the Type text box. This value is not editable. Password hides the password on the logon screen so it cannot be viewed. Text displays readable text.
Catalog	For added convenience, you can create specifications for frequently used fields using the Field Catalog tab. The Field Catalog is a collection of frequently-used fields and their specifications. If the field is in the Field Catalog, you can click and then choose it from the dropdown list. The specified data will be filled in automatically. To add a field to the Field Catalog, see page 49.
Value	Type a value for the logon field or use the Value dropdown menu (see next section) to indicate a value specified by the user or provided by the program. A typed value is stored in the logon in clear (unencrypted) text and is shared by all of those using the logon.

Values

Logon Field and Password Field values are used on the Logon Fields page of the Logon Screen Wizard during the creation of managed logons and Change Password screens.



A Value dropdown menu provides a list of options for specifying values to be supplied by the user or automatically by Password Manager. The available options vary depending on the type of field selected.

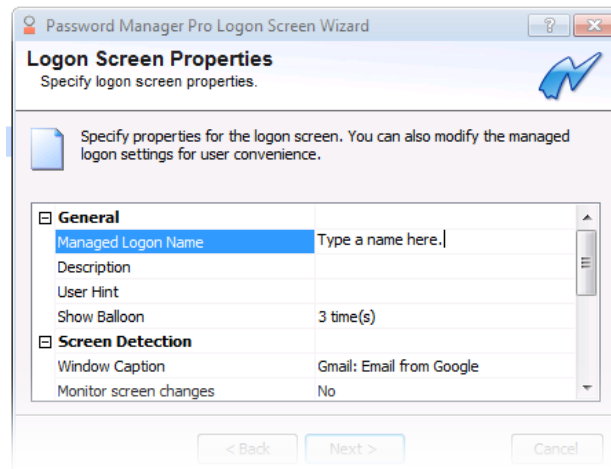
Option	Description
Ask-Reuse	Prompts the user to enter a value for a logon field the first time they use the logon. This value is automatically submitted for them on each subsequent logon without prompting the user again.
Ask-Confirm	Prompts the user to enter a value for a logon field the first time they use it. However, on subsequent logons, the value is automatically entered and they are then prompted to confirm this value or change it.
Ask Always	Prompts the user to enter a value for a logon field each time they use the logon.
Windows User Name	Password Manager provides the Windows user name.
Windows User Principal Name	Password Manager provides the user name and domain values in UPN format. Example: [user name]@[domain] .
Windows Domain\ User Name	Password Manager provides the domain of the user followed by a backslash and the user name. Example: [domain]\[user name].
Windows Domain	Password Manager provides the user domain name only.
Windows E-Mail Address	Password Manager provides the registered E-Mail address for the Windows user account currently logged on.

Option	Description
Windows User Password	Password Manager provides the password used for Windows logon.
Write Only	Always prompts a user for the value.
Defender One-time Password	Password Manager provides a One- time password token for authentication with Defender-compatible VPNs. This option is only shown on the menu when the Defender One-time Password module is installed.
Defender One-time Password + Windows User Password	Password Manager provides a One- time password token for authentication with Defender-compatible VPNs, and also requires the user's Windows password. (Can only be used in a password field.) This option is only shown on the menu when the Defender One-time Password module is installed.

* When using one of the Defender One Time Password values, it is a good idea to label the field with a name that clearly distinguishes it from conventional passwords. For example, instead of labeling it “Password,” you might label it as “Activation Code.”

Logon properties

In the Logon Screen Wizard, both Logon Screens and Change Passwords Screens have associated Properties pages where you can edit the properties for the screen.



Category	Property	Description
General	Managed Logon Name	The name of the logon.
	Description	Can be used to enter optional information about the managed login that is only viewable on the Password Manager Pro Logons tab. By default, this column is hidden. To display the column, right click anywhere in the column headings area and select Description .
	User Hint	Type a message to be displayed when the managed logon is used. For example, a custom prompt to type values for the logon fields. To add more detailed user assistance, type a URL that a user can click to be directed to a web page.
	Show Balloon	Once this managed logon is created and deployed, a balloon tip will automatically display (up to three times) when the user accesses the logon or change password screen. Use this setting to select how many times the balloon is displayed.
Screen Detection	Window Caption	<p>Title of the screen as detected by the wizard; used to match the managed logon to the specified screen.</p> <p>If portions of the window caption will change, you can use wildcards (*) at the beginning, middle or end of the caption. Only one wildcard can be used per caption. The portion of the string that does not change will be used to recognize the screen.</p> <p>For example:</p> <p>*Some Application Login Some Company*Login My Bank Login*</p>

Category	Property	Description
	Monitor screen changes	<p>When enabled, Password Manager continually monitors the titlebar, URL and content of the specified web page for changes that may affect the logon. When disabled, only the titlebar and the URL are monitored.</p> <p>For example, if a page were using frames, and a link in one frame changes another frame in the page in such a way that it changes to a logon page, with this setting on, the change is recognized and appropriate action taken. With the setting disabled, the change would not be recognized.</p> <p>Use of this setting is resource intensive, and it is disabled by default.</p>
	URL	<p>Used by to recognize a website screen. The URL information in the logon is matched to the URL in the screen. If multiple websites have the same title or if portions of the URL change, which can be the case for websites that redirect traffic for load balancing, then specify the portion of the URL to match. The dropdown menu allows you to specify the type of matching to perform on the URL. The options are:</p> <p>Do Not Match - This is the default. URL matching will not be performed.</p> <p>String Match - Matches the exact string displayed.</p> <p>Wildcard Match - Matches a displayed string utilizing an asterisk (*) to represent the portion of the URL that may change.</p> <p>Regular Expression - Matches a displayed string constructed as a regular expression (See “Regular Expression syntax” on page 45).</p> <p>Case Sensitive - Ignore case when matching.</p> <p>Restore Defaults - Return to the default URL settings.</p>

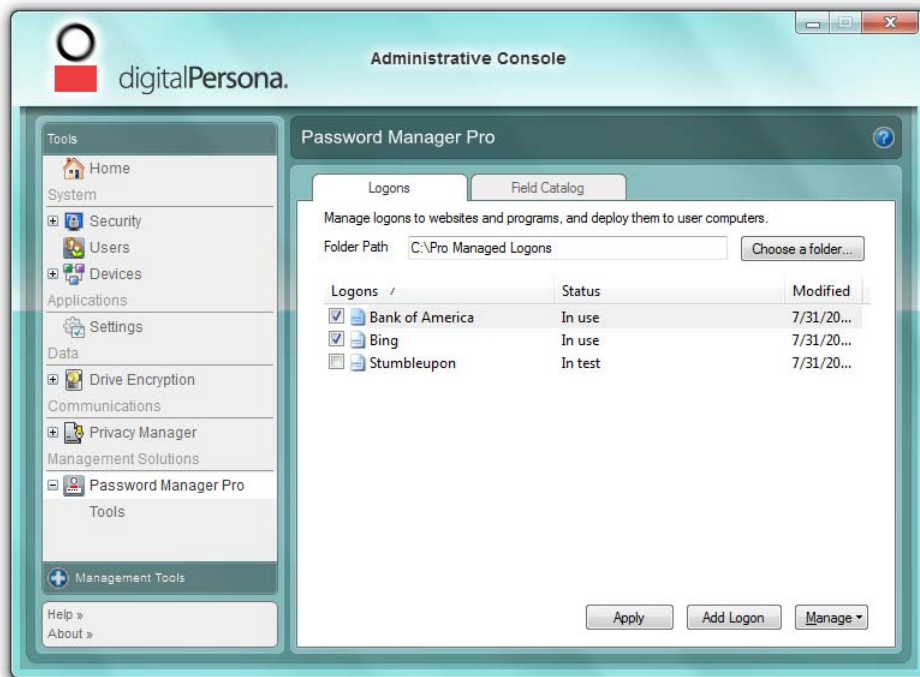
Category	Property	Description
	Extended Match	<p>Displayed only when creating a logon for a program, not a website.</p> <p>Click the button next to the Extended Match field and select any labels that should be used for matching when recognizing the screen. Click the checkbox next to the labels to use.</p> <p>After making selections and clicking OK, you can select the type of matching to perform by selecting it from the dropdown list. The options are the same as those listed above for the URL.</p>
Authentication	Start Authentication Immediately	If set to Yes , the user is prompted for their credential immediately after the logon screen displays. The default setting is No .
	Lock out logon fields	If set to Yes , the user is prevented from typing data in the logon fields. The default setting is No .
Password Manager icon	Location ID	Identifies the location selected in the Location field (below) so that it can be shared with other logon screens.
	Location	From the dropdown menu, select the initial location where the Password Manager icon will appear on the logon screen. The default is the top left corner of the screen.

Creating logons manually

If Password Manager Pro does not detect fields automatically in websites and programs, you can create a managed logon for a logon screen by manually specifying the fields. Creating logons manually can include using additional controls besides specifying fields and field contents, such as adding keystrokes, forcing delays between actions, and specifying the positions of fields.

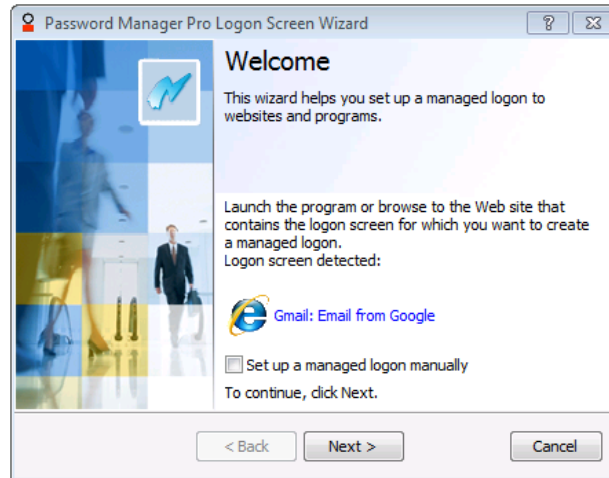
To create a logon manually for a logon screen:

- 1 From within the Administrative Console, launch the Password Manager Pro application.

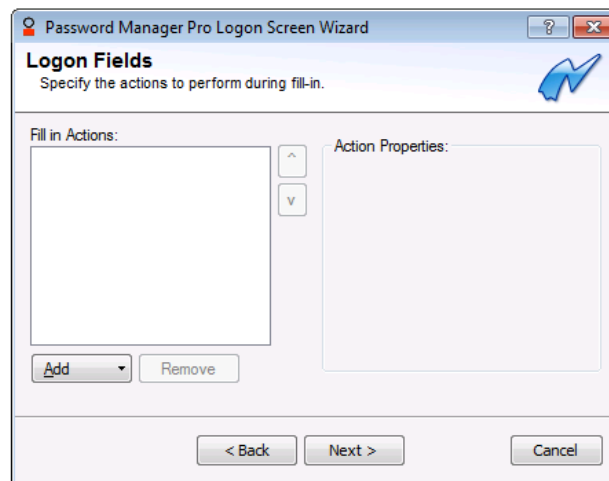


- 2 On the Logons tab, select **Choose a folder**. Click one of the recently used locations, or specify a path and click **Browse for folder** to add a folder to the list. Then click **Choose**.
- 3 Click **Add Logon**. The Password Manager Pro Logon Wizard starts.
- 4 Launch the logon screen for the password-protected website or program.

- 5 On the first page of the wizard, confirm that the logon screen has been detected and verify the title of the logon screen.

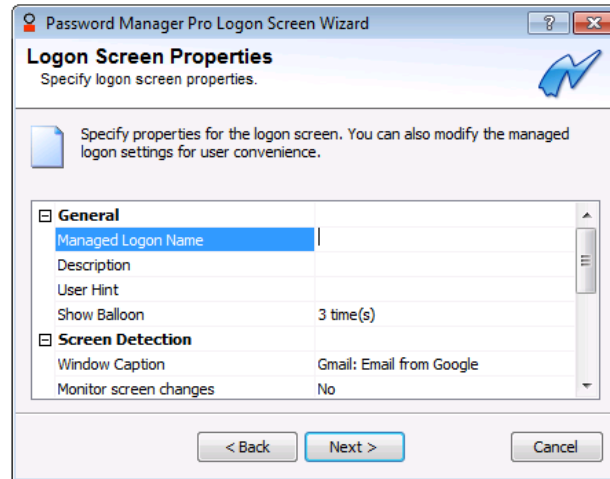


- 6 Select **Set up a managed logon manually** and then click **Next**.
- 7 On the **Logon Fields** page, click **Add** and select an action (see page 36) from the dropdown menu.



- 8 Add additional actions as required. If necessary, use the arrow buttons to modify the order in which the actions are performed.

- 9 Click **Next** to display the **Logon Screen Properties** page, where you can view and modify the various properties (page 29) for the logon screen.



- 10 Click **Next**, and then click **Finish** to create the logon and close the wizard.
- 11 In the Administrative Console's Logon tab, click **Apply** to save your changes to the server.

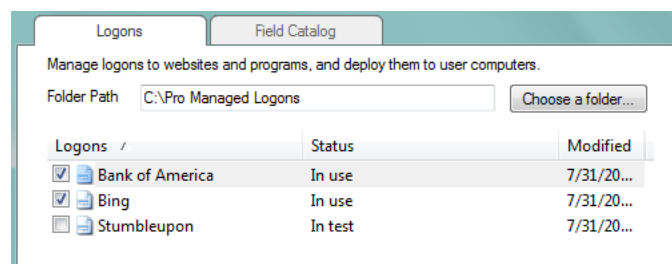
You do not have to click Apply after creating *each* logon or making every change, but you do need to click Apply before any new logons or changes to logons will be saved to the server.

See Also: "Creating managed logons" on page 23.

Deploying managed logons

To deploy managed logons:

- 1 Check the boxes next to logons to change their status from In Test to In Use. Only logons with an "In Use" status will be visible to users.

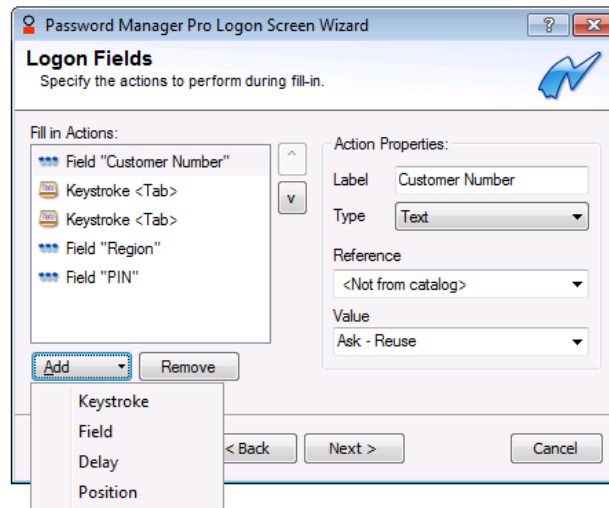


- 2 Click **Apply**.

After a managed logon is deployed to a computer, the Password Manager icon on the screen tells the user that they can fill in the requested account data by verifying their identity with the required credentials.


Logon Fields actions

Logon Fields actions are used when creating logons manually in the Password Manager Pro Logon Screen Wizard and the Password Manager Pro Change Password Screen Wizard.



An Actions dropdown menu provides a list of actions that are used to build a script for those logon and change password screens that cannot be automatically configured by Password Manager Pro.

Action	Description
Keystroke	This sequence of keys will be placed in the keyboard buffer. Keystroke properties are: Key - Select the main key to be entered. Repeat - Specify the number of times the key sequence is entered. Shift, Control, Alt - Optionally, select one of these keys in combination with the main key. You may specify the exact use of a Generic , Left or Right key as well.
Field	Label - Type a label name for the corresponding field on the logon screen. The labels are displayed when users are prompted to type a value for a logon field. Type - Select the type of field, either text or password . Choosing password hides the password on the logon screen; choosing text displays readable text. Reference - Optionally, select a field previously defined on the Field Catalog tab. Value - Type a value for the logon field or use the dropdown menu to indicate a value specified by the user or provided by the program. If you type a value for the logon field, it is stored in the logon in clear (unencrypted) text and is shared by all users using the logon.
Delay	Specify how many seconds to wait before the next action in the list is performed.

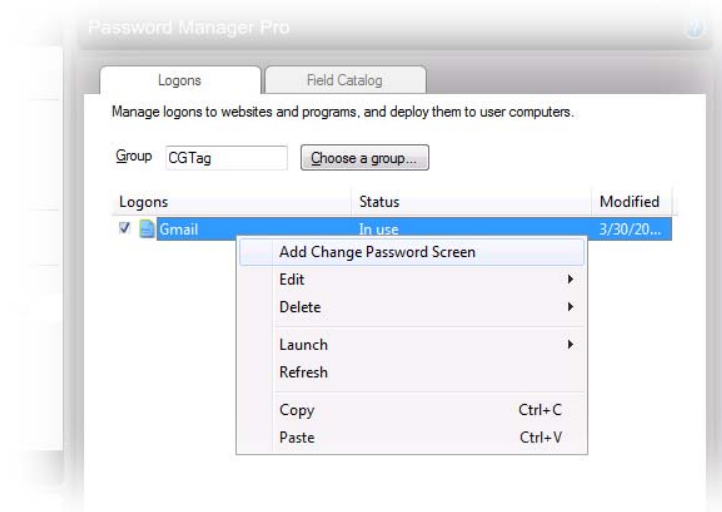
Action	Description
Position	<p>Specify a location where the system will perform a mouse click. Position is measured from the top left corner of the client window area.</p> <p>Client X - Type a number of pixels for the X axis position for the action.</p> <p>Client Y - Type a number of pixels for the Y axis position for the action.</p> <p> Instead of typing X and Y coordinates, you can drag the target icon to the actual logon screen field to specify the position. When you release the target icon at the location you want to specify, the Client X and Y positions will be captured.</p>

Setting Up a Change Password screen

By managing a change password screen, you can specify the fields required by the application for changing passwords, implement password policies and automate the entire process for the end user.

To set up a Change Password Screen automatically:

- 1 Launch the password-protected website or program for which you want to set up a Change Password Screen. Move to that site's or program's Change Password screen.
- 2 In Password Manager Pro, select the logon for that website or program.
- 3 Right-click to display that logon's context menu, then click **Add Change Password Screen**. The Password Manager Pro Change Password Screen wizard starts.



- 4 On the first page of the wizard, confirm that the correct screen has been detected. Click **Next**. The wizard displays the Change Password Screen Fields page.
- 5 Select all fields on the page that are relevant to the change password process, and click **Next**.

Option Heading	Description
Use	Check the Use check box for each field used for password change. If some of the fields displayed by the wizard are not relevant for password change (i.e., a search field on a website change password page), leave those fields unchecked.
Label	If the label for a field is not intuitively related to the corresponding field on the change password screen, enter a new label name in this field. The labels are displayed when users are prompted to type a value for the field.

Option Heading	Description
Catalog	By default, specifies values for fields based on those used in the associated Logon screen. For example, the password used at logon is re-used during the Change Password process. Use the Catalog dropdown menu to change these values as needed.
Value	Specifies the value for this field. For Old Password, the value should be Ask-Reuse. For New Password and Repeat New Password fields, the value should be Write Only.

- 6 On the Password Policy page, optionally, click (...) to specify changes to the password policy. The password policy defined in the wizard should generally be the same as that used on the website or in the program. The default is none.
- 7 Click **Next**, and on the Submit Selection page, select the button used to submit the password data. Or select **Do Not Submit** to fill in the data but not submit it.
- 8 Click **Next** to display the Change Password Screen Properties page. Modify any of the listed properties (see below) to customize behavior of the Change Password screen.
- 9 On the Setup Complete page, click **Finish** to close the wizard.
- 10 Click **Apply** to save your changes to the server.

You do not need to click Apply after creating making every change, but you do need to click Apply to save any changes that you have made.

Managed change password screens are deployed at the same time as the managed logons that they are associated with. After they are deployed, they will display the Password Manager icon, indicating that the user should verify their identity to begin the change password process.

See Also: “Creating logons manually” on page 33.

Password policies

Password policies are used to specify requirements for passwords that are generated by Password Manager Pro or entered by a user.

Option	Description
Password is provided by user	Password Manager Pro does NOT provide password information to the program. (The user has the option to log on by entering their password or another allowed credential.)
Password is generated automatically	Password Manager Pro generates the password automatically. An alternate credential must be used to log on.
Use password policy	<p>When enabled:</p> <p>If the password is provided by the user, it must conform to the listed password requirements.</p> <p>If the password is generated by Password Manager Pro, the password will be generated according to the listed password requirements.</p>
Minimum password length	Select the minimum number of characters allowed in the password.
Maximum password length	Select the maximum number of characters allowed in the password.
Password must contain	<p>Select one of the following requirements:</p> <p>Letters and numbers - allows any combination of letters and/or numbers.</p> <p>Numbers only - allows numbers only.</p> <p>Letters only - allows letters only.</p> <p>Letters and numbers with special characters - passwords must contain at least one number or letter and at least one special character. Special characters include !"#%&'()*+,-./:;<=>?[\\]^_`{ }~@. Spaces are not allowed.</p> <p>Letters and numbers with at least one number - passwords must contain at least one letter and at least one number.</p>

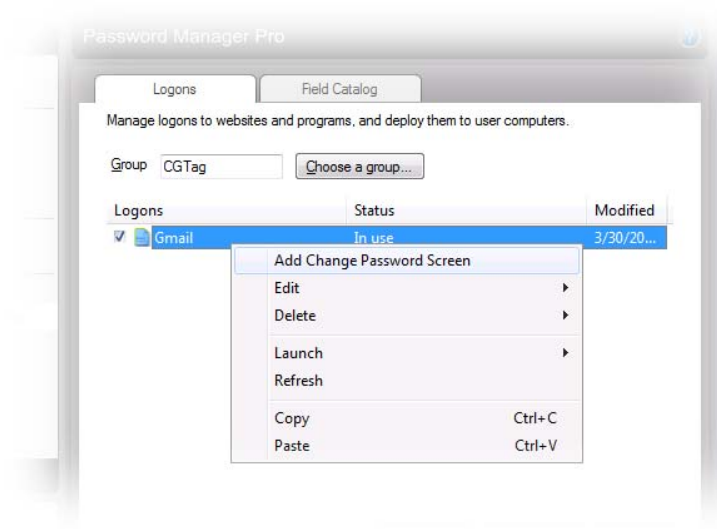
Option	Description
Additional password requirements	<p>None. No other constraints are applied to the password contents.</p> <p>Different than the Windows password. The new password must be different than the current Windows password.</p> <p>Different than any password registered with Password Manager The new password must be different from any password registered with Password Manager.</p> <p>Different than the current password. The new password must be different than the current password for this website or program</p>

Setting up a Change Password Screen manually

If Password Manager Pro does not detect fields automatically in Change Password screens, you can manually specify the fields and actions required. Creating a Change Password screen manually allows you to include additional controls such as adding keystrokes, forcing delays between actions, and specifying positions of fields.

To set up a Change Password screen manually:

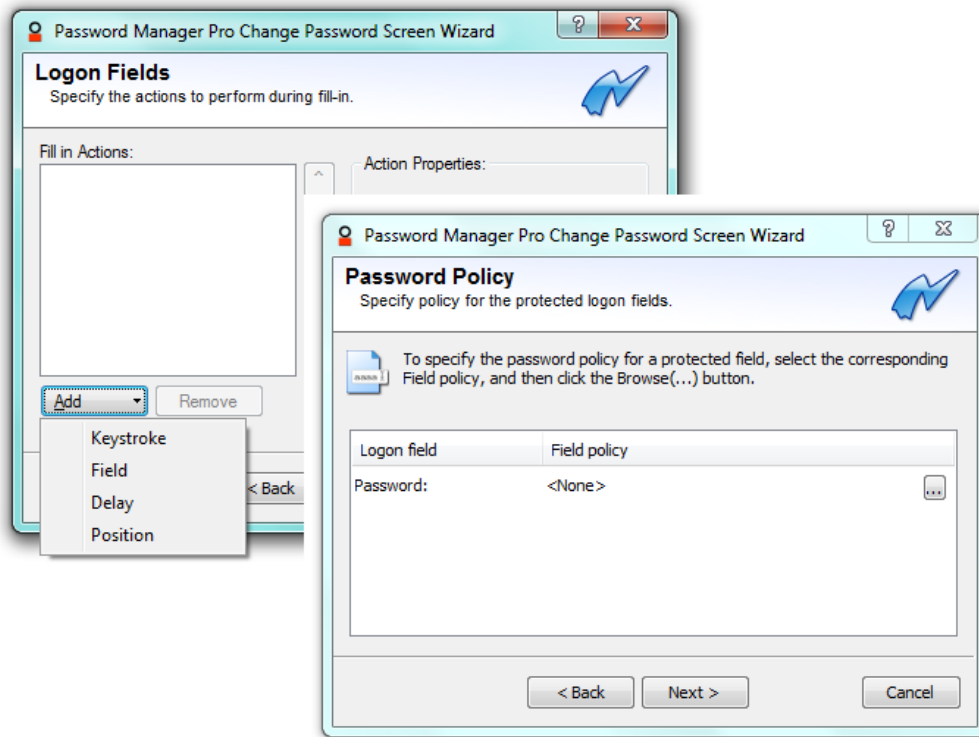
- 1 Launch the password-protected website or program for which you want to set up a Change Password Screen. Move to that site's or program's Change Password screen.
- 2 In Password Manager Pro, select the logon for that website or program.
- 3 Right-click to display that logon's context menu, then click **Add Change Password Screen**.



The Password Manager Pro Change Password Screen wizard starts.

- 4 On the first page of the wizard, confirm that the correct screen has been detected. Select **Set up a managed logon manually**. Click **Next**.

- 5 On the **Logon Fields** page, click **Add** and select an action from the dropdown menu.

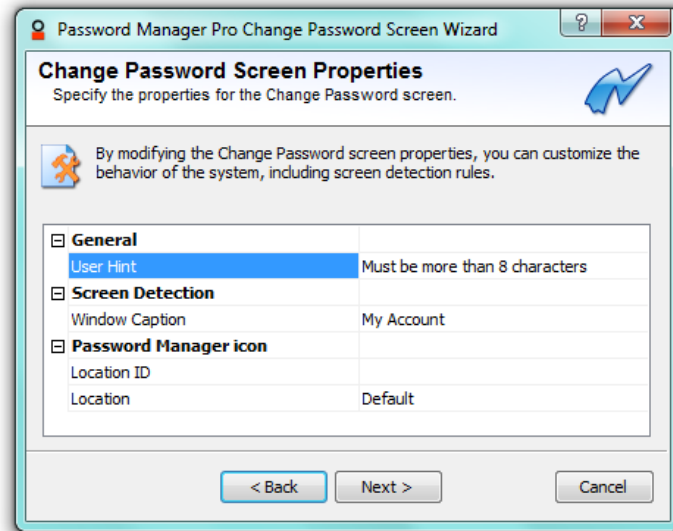


For example, you might study a Change Password screen and discover that it takes nine presses of the tab key to get to the first input field (Change Password).

You could choose Keystroke, select the Tab key, and specify "Repeat 9 times" to get the user where they need to be; or you could choose to use the Position action to place the cursor in the right location to change the password.

- 6 Add additional actions as required. If necessary, use the arrow buttons to modify the order in which the actions are performed.
- 7 On the Password Policy page, optionally, click (...) to specify changes to the password policy. The password policy defined in the wizard should generally be the same as that used on the website or in the program. The default is None.

- 8 Click **Next** to display the Change Password Screen Properties page. Modify any of the listed properties to customize behavior of the Change Password screen.



- 9 On the Setup Complete page, click **Finish** to close the wizard.

- 10 Click **Apply** to save your changes to the server.

You do not need to click Apply after making every change, but you do need to click Apply to save any changes that you have made.

Managed change password screens are deployed at the same time as the managed logons that they are associated with. After they are deployed, they will display the Password Manager icon, indicating that the user should verify their identity to begin the change password process.

Regular Expression syntax

Both Logon Screens and Change Passwords Screens can use regular expressions in the URL field of the Properties page to define the part of a URL that should be matched when determining if the page has changed.

A regular expression is a text string used to create a logon for matching certain characters, or a series of characters, within another text string.

In a regular expression, most characters are treated as literals, i.e. they match only themselves ("a" matches "a", "bc" matches "bc", etc). The exceptions are called metacharacters (MC in the table below).

MC	Description
.	Matches any single character
[]	Matches a single character that is contained within the brackets. For example, [abc] matches "a", "b", or "c". [a-z] matches any lowercase letter. These can be mixed: [abcq-z] matches a, b, c, q, r, s, t, u, v, w, x, y, z, and so does [a-cq-z]. The '-' character should be literal only if it is the last or the first character within the brackets: [abc-] or [-abc]. To match an '[' or ']' character, the easiest way is to make sure the closing bracket is first in the enclosing square brackets: [][ab] matches ']', '[', 'a' or 'b'.
[^]	Matches a single character that is not contained within the brackets. For example, [^abc] matches any character other than "a", "b", or "c". [^a-z] matches any single character that is not a lowercase letter. As above, these can be mixed.
^	Matches the start of the line (or any line, when applied in multiline mode)
\$	Matches the end of the line (or any line, when applied in multiline mode)
()	Defines a "marked subexpression". What the enclosed expression matched can be recalled later. See the next entry, \n. Note that a "marked subexpression" is also a "block."
\n	Where n is a digit from 1 to 9; matches what the nth marked subexpression matched. This construct is theoretically irregular and has not been adopted in the extended regular expression syntax.
*	A single character expression followed by "*" matches zero or more copies of the expression. For example, "[xyz]*" matches "", "x", "y", "zx", "zyx", and so on.

MC	Description
\n*	<p>Where n is a digit from 1 to 9, matches zero or more iterations of what the nth marked subexpression matched. For example, "(a.)c1*" matches "abcab" and "abcabab" but not "abcac".</p> <p>An expression enclosed in "(" and ")" followed by "*" is deemed to be invalid. In some cases (e.g. /usr/bin/xpg4/grep of SunOS 5.8), it matches zero or more iterations of the string that the enclosed expression matches. In other cases (e.g. /usr/bin/grep of SunOS 5.8), it matches what the enclosed expression matches, followed by a literal "*".</p>
{x,y}	Match the last "block" at least x and not more than y times. For example, "a{3,5}" matches "aaa", "aaaa" or "aaaaa".
+	<p>The + operator will match the preceding atom (a single character, a marked sub-expression, or a character class) one or more times, for example the expression a+b will match any of the following:</p> <p>ab aaaaaaab</p> <p>But will not match: b</p>
	<p>The operator will match either of its arguments, so for example: abc def will match either "abc" or "def".</p> <p>Parenthesis can be used to group alternations, for example: ab(d ef) will match either of "abd" or "abef".</p>
?	<p>The ? operator will match the preceding atom (a single character, a marked sub-expression, or a character class) zero or one times, for example the expression ca?b will match any of the following:</p> <p>cb cab</p> <p>But will not match: caab</p>

Managing logons

Password Manager Pro makes managing logons easy. Most management features can be accessed through either of two means available on the Logons tab:

- Right-click on a logon to display the shortcut menu for that logon
- Select a logon and click **Manage** to display available commands for that logon.

After making any changes to your managed logons, remember that they need to be deployed before they can be seen and used by the end-user (see “Deploying managed logons” on page 35).

The following logon management features are described in this section.

Feature	Page
Editing logons	47
Deleting logons	48
Deploying logons	48
The Field Catalog	49
Finding logons	51
Finding duplicate logons	51
Finding fields in logons	50

Editing logons

To edit a logon:

- 1 Select a logon to edit and click **Manage**.
- 2 Click **Edit** and select either **Logon Screen** or **Change Password Screen**.
- 3 In the corresponding wizard, make any desired changes to the logon. For details on specific wizard pages, see one of the following topics:

Reference	Page
Logon Fields attributes	27
Values	28
Logon properties	29
Logon Fields actions	36
Password policies	40

- 4 When editing is complete, click **Finish** to exit the wizard.
- 5 Click **Apply** to save your changes to the server.

You do not need to click Apply after making *each* change, but be aware that you *do* need to click Apply before any changes to logons will be saved.

Deleting logons

To delete a logon:

- 1 Choose a group to edit its managed logons.
- 2 Right-click on the logon that you want to delete and click **Delete**.
- 3 Click **All Screens** to delete the logon and any associated Change Password screens, or click **Change Password Screen** to delete only the Change Password screen.
- 4 Click **Apply** to save your changes to the server.

You do not need to click Apply after making every change, but you do need to click Apply to save any changes that you have made.

Deploying logons

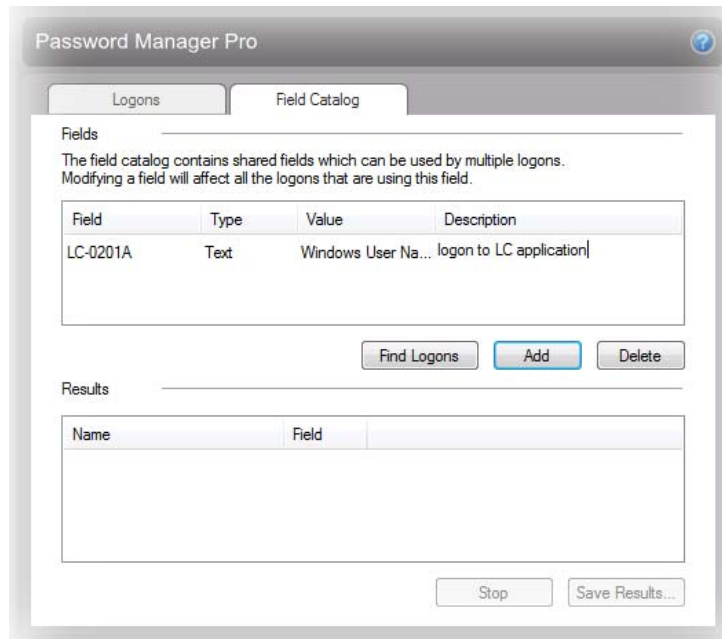
To deploy managed logons:

- 1 Check the boxes next to logons to change their status from **In Test** to **In Use**. Only logons with an "In Use" status will be visible to users.
- 2 Click **Apply**.

After a managed logon is deployed to a computer, the Password Manager icon on the screen tells the user that they can fill in the requested account data by verifying their identity with the required credentials.

The Field Catalog

You can use the Field Catalog to store logon field values and attributes that can be reused in creating managed logons for logon screens that share common fields.



By storing frequently used logon fields in the catalog, you can add commonly used fields to additional logons without setting values or attributes each time. Later changes made to fields in the catalog will then also be propagated to all logons that use the field.

Adding fields to the Field catalog

To add a field to the Field Catalog:

- 1 On the Field Catalog tab, click **Add** to create a new field in the table.
- 2 In the **Field** column, type a name for the field you are adding to the catalog.
- 3 Specify the type of the field by selecting **Password** or **Text** in the **Type** dropdown list.
- 4 Specify the value of the field (see page 28) from the **Value** dropdown menu.
- 5 Add any comments related to this field in the **Description** text box.

Example: Use of Field Catalog for password

To use a field from the Field Catalog for a password:

- 1 Add a field to the catalog, and select **Password** as the type (see previous topic).

- 2 Create a managed logon manually (see page 33).
- 3 On the Logon Fields page of the wizard, from the **Add** dropdown menu, select **Field**.
- 4 In the Action Properties area, enter a label for the field.
- 5 From the Type dropdown menu, select **Password**.
- 6 From the Reference dropdown menu, select the name of the field that you added in step 1 above.
- 7 Continue creation of the logon as described in step 9 of *Creating logons manually* on page 35.

Finding fields in logons

You can search for managed logons that contain fields selected from the Field Catalog.

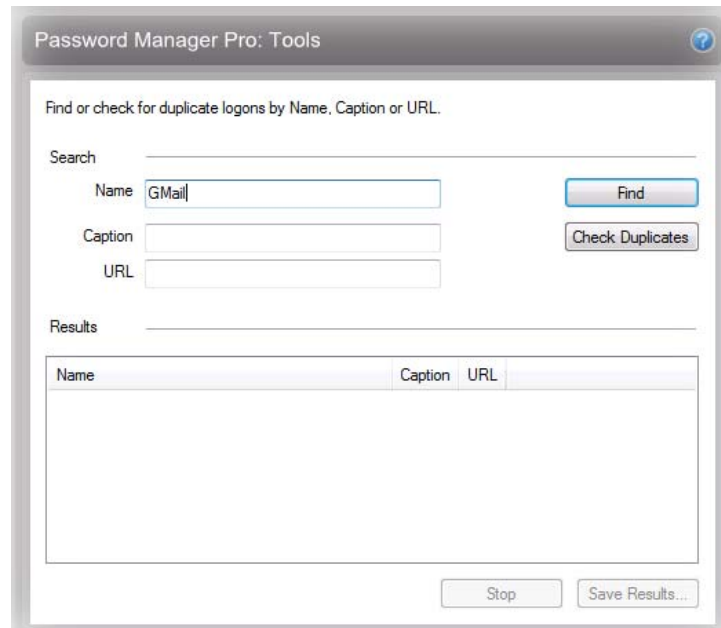
To search for logons that contain selected fields:

- 1 On the **Field Catalog** tab, select the fields to search for and click **Find Logons** to display the search results.
- 2 Optionally, click **Save Results** to save the results to an HTML file.

The results are saved as an HTML table that includes the caption, logon name, created date, modified date and file name.

Tools page

Use the Password Manager Pro Tools page to search for logons, or check for duplicate logons.



Finding logons

To search for logons:

- 1 On the Tools page, enter a logon name, caption or URL to search for. Use ? or * wild cards to indicate individual or multiple characters.
- 2 Click **Find** to display the search results.
- 3 Optionally, click **Save Results** to save the results to an HTML file.

Finding Duplicate Logons

Duplicate logons are multiple copies of logons for a single logon or change password screen.

To search for duplicate logons:

- 1 On the Tools page, click **Check Duplicates**.
- 2 Optionally, click **Save Results** to save the results to an HTML file.
- 3 Right-click on any of the resulting logon names to display a shortcut menu with options to edit or delete the duplicate managed logon.

In order to fully understand and implement the features of DigitalPersona Password Manager, you will need to be familiar with the terms covered in this chapter.

authentication

Process of verifying that you are the person you claim to be, through the use of your specified credentials such as your Windows password, your fingerprint, smart card or face recognition.

back up

Using the backup feature to save a copy of important program information to a location outside the program. It can then be used for restoring the information at a later date to the same computer or another one.

connected device

A hardware device that is connected to a port on the computer.

credentials

Credentials are a set of information used to gain access to your computer, Windows account or to a password protected website or program. Credentials may include a combination of a user name, password, fingerprint, fingerprint PIN, smart card or facial recognition.

dashboard

A central location where you can access and manage the features and settings in DigitalPersona Pro Workstation for Enterprise.

enroll

The process of capturing and storing information about your fingerprints, which are then used to authenticate you in order to access Windows, websites, and programs.

fingerprint

A digital extraction of your fingerprint image. Your actual fingerprint image is never stored by Pro Workstation.

kiosk

A kiosk is a computer, or group of computers, that can be used by designated persons sharing a single Windows user account and its associated programs. Each user of the kiosk can quickly and easily log on to Windows, programs and websites using the minimum credentials (such as fingerprints) specified by the organization.

logon

Account data for a website, program or password change screen that allows a user to logon by using specific credentials as specified by the Pro Workgroup administrator. There are two types of logons, personal logons and managed logons. See separate glossary entries.

managed computer

Any computer running a compatible DigitalPersona Pro client, that has been set up to be managed by a Pro server.

managed logon

A logon (see above) created using Password Manager Pro, which can then be deployed to all managed computers. The term logon is generally used, except when specifically referring to logons created by an administrator with Password Manager Pro (managed logons) as contrasted with those created by an end-user (personal logons). When both managed and personal logons exist for the same program or website, the personal logon is disabled and only the managed logon may be used for access to the specified program or website. See also: personal logon.

Password Manager

A security application included with Pro Workgroup compatible clients, that allows users to create their own personal logons for programs and websites, in addition to using managed logons created through the Password Manager Pro application. These logons may be used to launch the program or website and automatically fill in required account data after verifying their identity with any of a variety of authentication mechanisms (such as password, smart card, fingerprints or Defender-compatible VPN tokens) as specified by the DigitalPersona Pro administrator.

Password Manager Pro

An optional management application that plugs into Administrative Console of compatible workstation clients to enable the creation, administration and management of logons for password-protected software programs and websites. Users simply verify their identity by supplying required credentials to securely provide data for logon fields, such as user name and password, on any website or program logon screen.

Administrators use the Password Manager Pro application to create managed logons specifying information for the logon screens, and can use application policy settings in the GPO to deploy the One Touch SignOn templates to end users.

(Requires Internet Explorer 6 or above.)

personal logon

A logon created by an end-user with the Password Manager application. The term logon is generally used, except when contrasting logons created by an end-user (personal logons) with those created by an administrator with Password Manager Pro (managed logons). See also: managed logons.

Quick Actions

Quick Actions, which combine the Shift or Control Keys with use of the fingerprint to access DigitalPersona Pro features, can be created by end users in the DigitalPersona Workstation Properties dialog.

restore

A process that copies program information from a previously saved backup file into this program.

secret

A DigitalPersona Pro Secret is application specific user data that is stored securely in Active Directory by the DigitalPersona Pro Enterprise Server, or locally by the local authentication server on the workstation. The secret is released to the application upon successful identification of the user, and used to log on to programs and websites for which logon templates have been created.

scene

A photo of an enrolled user to be used for authentication.

smart card

A hardware device that can be used for authentication.

Verification Template

A verification template is created from a fingerprint scan whenever a user places their finger on the fingerprint reader. During authentication, this template is matched to available Enrollment Templates in order to identify the user. At the end of the authentication process the Verification Template is erased.

Windows Logon

Windows Logon provides the ability for you to log on to your Windows account by using any of a variety of authentication mechanisms (such as password, smart card, fingerprints or Defender-compatible VPN tokens).

Windows Logon Security

Protects your Windows accounts by requiring the use of specific credentials for access.

Windows user account

Profile for an individual who is authorized to log on to a network or to an individual computer.

Index

A

- adding a change password screen 38
- adding a change password screen manually 42
- adding fields to the Field catalog 49
- Allow creation of personal logons 10
- attributes 27
- authentication, defined 52

B

- back up 52

C

- change password screen 38
- changing passwords 18
- connected device 52
- Credentials, defined 52

D

- dashboard 52
- delay 36
- deploy managed logons 26, 35, 39, 44, 48

E

- enroll 52

F

- field catalog 49
- finding duplicate logons 51
- finding fields in logons 50
- finding logons 51
- fingerprint 52

L

- logging on 18
- logon 53
- logon field values 28
- logon fields 30
- logon fields attributes 27
- logon fields properties 29

M

- managed computer 53
- Managed logons 10
- managed logons 23, 53

P

- password field values 28
- Password Manager 53
- Password Manager Pro 53
- password policies 40
- personal logon 53, 54
- Prevent Password Manager from running 7, 9
- Pro client 53
- properties 29

R

- regular expression syntax 45
- restore 54

S

- scene 54
- Secret 54
- setting up a change password screen 38
- setting up a change password screen manually 42
- setting up a logon screen 23
- smart card 54

T

- target icon 37
- Tools page 51

U

- using logon screens 18

V

- values 28

W

- Windows E-Mail Address 28