

DigitalPersona®

Password Manager Pro

Version 5.0

Administrator Guide



digitalPersona.

© 2010 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.

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

This document 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

We welcome your feedback on any errors, omissions, or suggestions for future improvements.

Contact us at:

- TechPubs@digitalpersona.com
- DigitalPersona, Inc.
720 Bay Road, Suite 100
Redwood City, California 94063 USA
- Tel: (650) 474-4000
- Fax: (650) 298-8313

Document Revised: 8/6/2010 (Software version 5.0.1)

Table of Contents

1 Introduction	1
Chapter Overview	1
Glossary	2
Support Resources	3
Installation	4
2 Creating managed logons	5
Creating logons	5
Logon Fields attributes	10
Values	11
Logon properties	12
Creating logons manually	16
Deploying managed logons	19
Logon Fields actions	20
Setting Up a Change Password screen	22
Password policies	24
Regular Expression syntax	27
3 Managing logons	29
Editing logons	29
Deleting logons	30
Importing logons	30
Deploying logons	31
The Field Catalog	31
Adding fields to the Field catalog	31
Example: Use of Field Catalog for password	32
Finding fields in logons	32
Tools page	33
Finding logons	33
Finding Duplicate Logons	33
4 Using logons	35
Logging On	35
Changing passwords	35
5 Index	36

Password Manager Pro enables administrators to provide controlled access to Web sites 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.

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. Password Manager Pro also provides many configurable options for defining and reusing information for logon and change password screens.

- Setting up a 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.
- The change password process can also be automated by specifying details such as whether the password can be changed by the user at will, or must be changed at prescribed intervals, and any additional password format restriction.

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

The DigitalPersona Password Manager Pro Administrator Guide provides information that an administrator will need to know in order to understand, plan for, install and deploy this solution in your enterprise.

Chapter Overview

Chapter 1, *Introduction*, provides a general orientation to the product, its installation, terminology, and the contents of this Administrator Guide.

Chapter 2, *Creating managed logons*, gives detailed instructions on how to create managed logons for programs and websites, through a simple automated process, or through a more robust manual mode.

Chapter 3, *Managing logons*, explains the ins and outs of managing your logons, including editing, deleting, importing to another group and final deployment.

Chapter 4, *Using logons*, includes additional information that you will want to pass on to your end-users.

Glossary

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.

group

A collection of managed computers sharing identical Pro Workgroup settings.

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 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.

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

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 whatever credentials may be specified by the Pro Workgroup administrator.

Password Manager Pro

A plug-in application module that plugs into the 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 and deploy the managed logons. End-users access the logons through the Password Manager application and replication of the logons is handled through the Pro Workgroup server.

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.

web console

A web application used to administer Pro Workgroup server and manage its groups, computers and users.

Support Resources

In addition to this guide, the following resources are provided for additional support to users of this product:

- Readme files are provided in the root directory of the product package for each product. These files often contain late-breaking information about the product.
- AskPersona.com (<http://askpersona.com>) is a DigitalPersona Knowledge Portal providing answers to many frequently asked questions about our products.
- DigitalPersona Maintenance and Support customers will find additional information about technical support resources in their Maintenance and Support confirmation email.
- Online help is included with each component of the product. Context-sensitive help is accessible from various pages, menus and dialog boxes that appear during the use of the software.
- Full description of the functionality of the companion end-user application, Password Manager, is provided through the online help and context-sensitive help within the application.

Installation

Password Manager Pro installs as a plug-in application within the Administrative Console of compatible HP ProtectTools and DigitalPersona Pro clients. See the readme.txt file included with the product for specific versions supported.

To install the Password Manager Pro application -

- Run the Setup.exe file located in the Password Manager Pro folder of the product package.

Creating managed logons

2

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 on a DigitalPersona Pro Workgroup server. From there they can be deployed to specific groups of end-users managed by the server. These managed computers, running the companion product, Password Manager, will then automatically have access to the managed logons for their group.

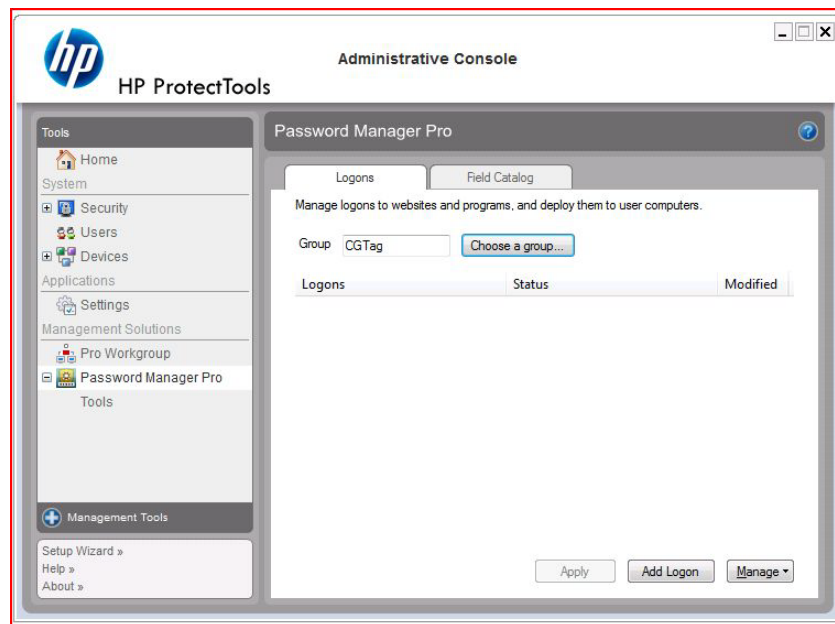
- Managed logons are downloaded to client computers as soon as they are set up to be managed, and at intervals specified by the administrator on the DigitalPersona Pro Workgroup server.
- Note that credentials entered by the end-user for a Web site or program do not “roam” on the network, and are only 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 Web sites 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.

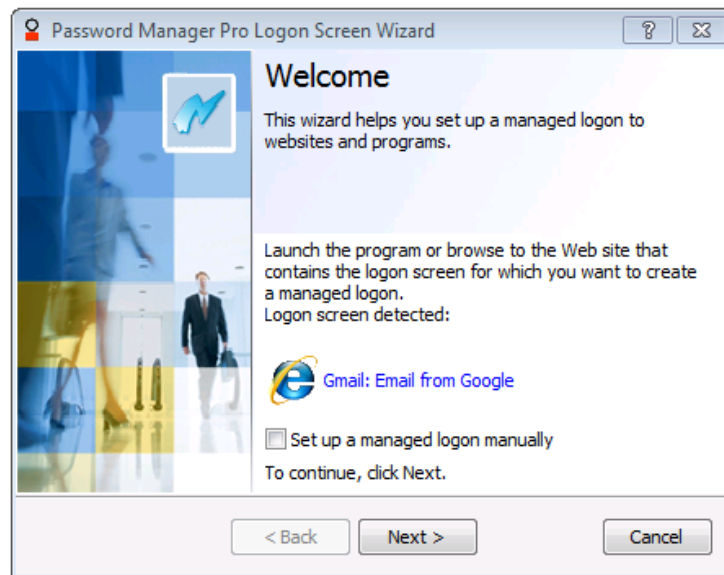
Creating logons

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 the group that you want to create managed logons for.
3. Click **Add Logon**. The Logon Screen 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. 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 16.

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 10) and values (see page 11) and then click **Next**.

Use	Label	Type	Catalog	Value
<input checked="" type="checkbox"/>	Username:	Text	<Not from catalog>	Ask - Reuse
<input checked="" type="checkbox"/>	Password:	Pass...	<Not from catalog>	Ask - Reuse
<input type="checkbox"/>	Stay signed in	Chec...	<Not from catalog>	Ask - Reuse

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

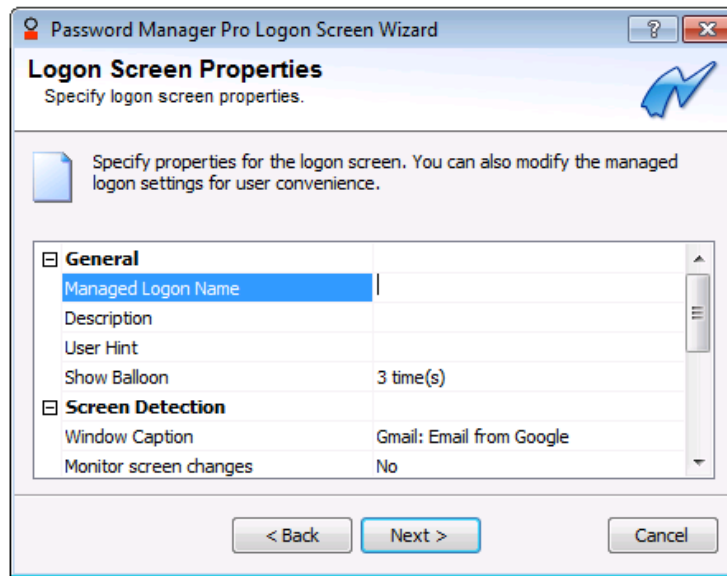
Detected buttons:

Do Not Submit

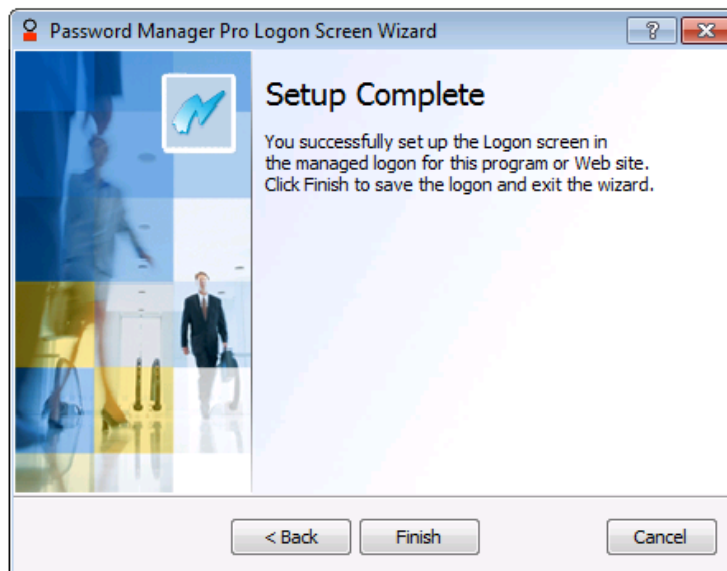
Sign in

- 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 12) 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:

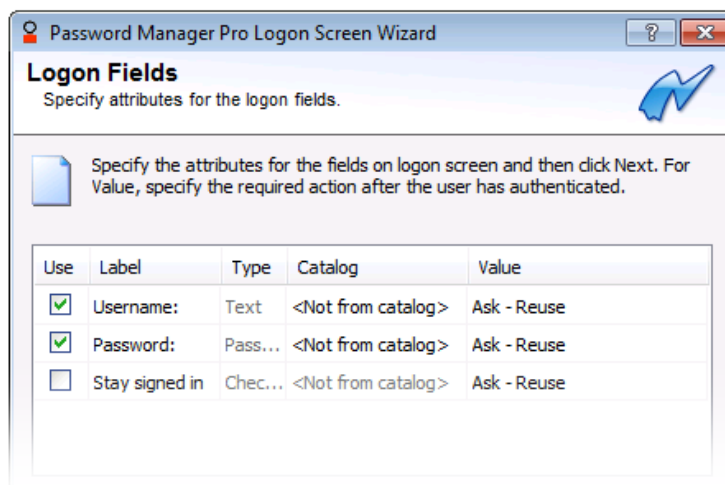
Logons created by Password Manager Pro (also called managed logons) take precedence over any personal logons created for the same screen by end-users of the Password Manager application. The corresponding personal logon will no longer be able to be used to log on, but can be opened by clicking Edit in 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 for the same group; as only the last applied changes will be deployed.

See Also: *Creating logons manually* on page 16.

Logon Fields attributes

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



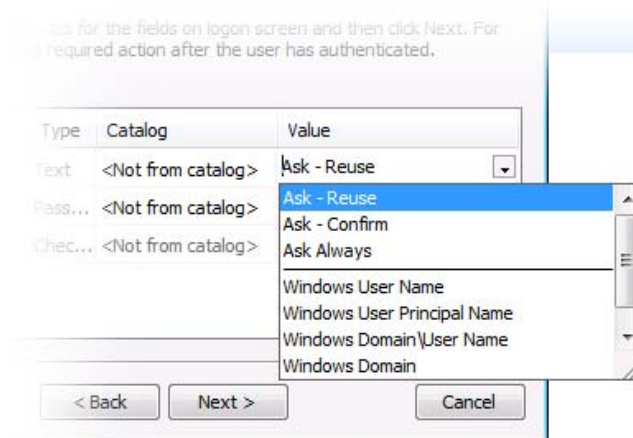
Column headings specify the attributes for each field on a Logon Screen or Change Password screen.

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 drop-down list. The specified data will be filled in automatically. To add a field to the Field Catalog, see page 31.

Field	Description
Value	Type a value for the logon field or use the Value drop-down 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.



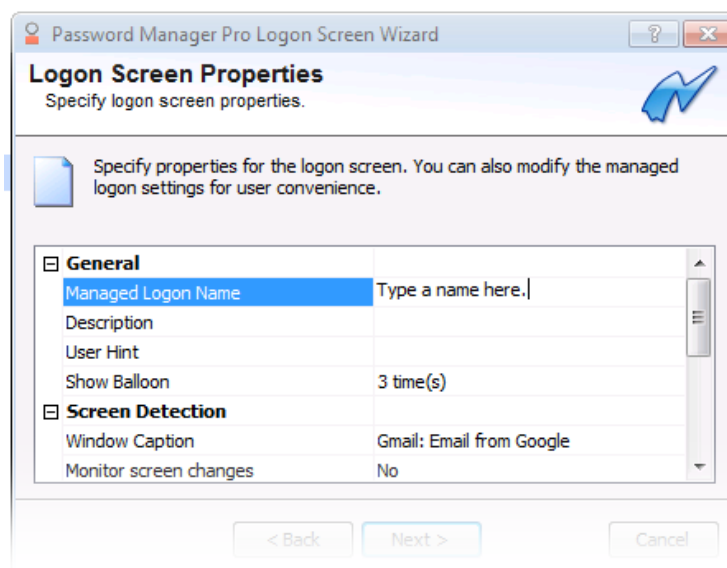
A Value drop-down menu provides a list of options for specifying values to be supplied by the user or automatically by Password Manager. The available options vary depending on the type of field selected.

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.

Option	Description
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 User Password	Password Manager provides the password used for Windows logon
Write Only	Always prompts a user for the value.

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 logon 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, you could type a URL in the field 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 end-user accesses the specified logon or change password screen. Use this setting to select how many times the balloon is displayed.
Screen Detection	Window Caption	<p>This is the title of the screen as detected by the wizard. This caption is used to match the managed logon to the specified screen.</p> <p>If portions of the window caption will change, represent that portion with an wildcard (*) at the beginning, inside of, or at the end of the caption. Only one wildcard can be used per caption.</p> <p>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 Password Manager 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 drop-down 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 <i>Regular Expression syntax</i> on page 27).</p> <p>Case Sensitive - Ignore case when matching.</p> <p>Restore Defaults - Return to the default URL settings.</p>

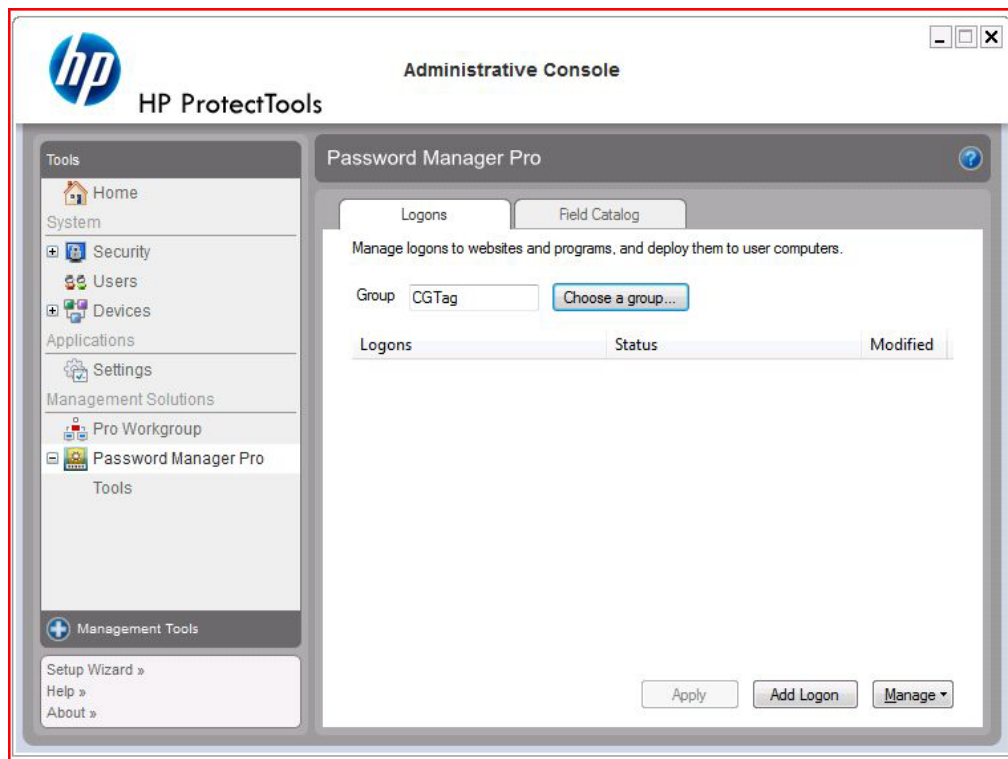
Category	Property	Description
	Extended Match	Displayed only when creating a logon for a program, not a website. Click the button next to the Extended Match field and select any labels that should be used for matching when recognizing the screen. Click the checkbox next to the labels to use. After making selections and clicking OK, you can select the type of matching to perform by selecting it from the drop-down list. The options are the same as those listed above for the URL.
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 drop-down 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.

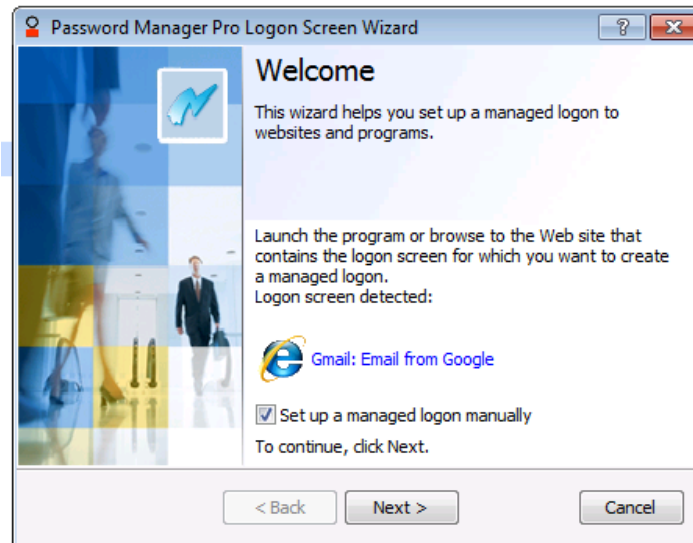
To create a logon manually for a logon screen:

1. From within the Administrative Console, launch the Password Manager Pro application.
2. On the Logons tab, select the group that you want to create managed logons for.

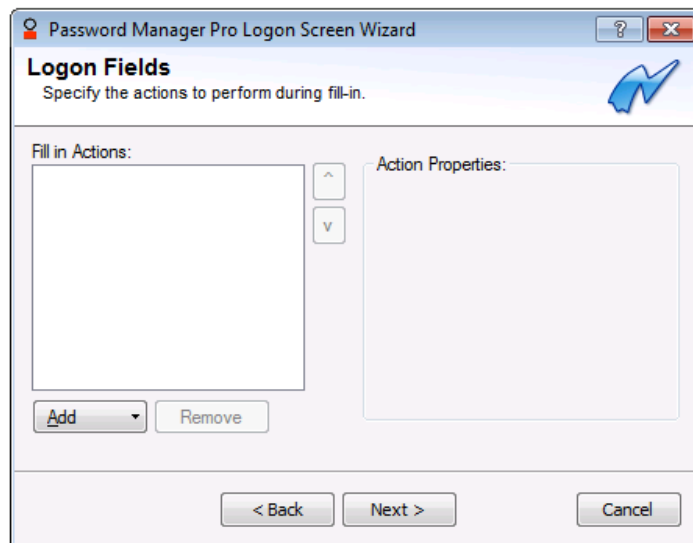


3. Click **Add Logon**. The Logon Screen wizard starts.
4. Launch the logon screen for the password-protected website or program.

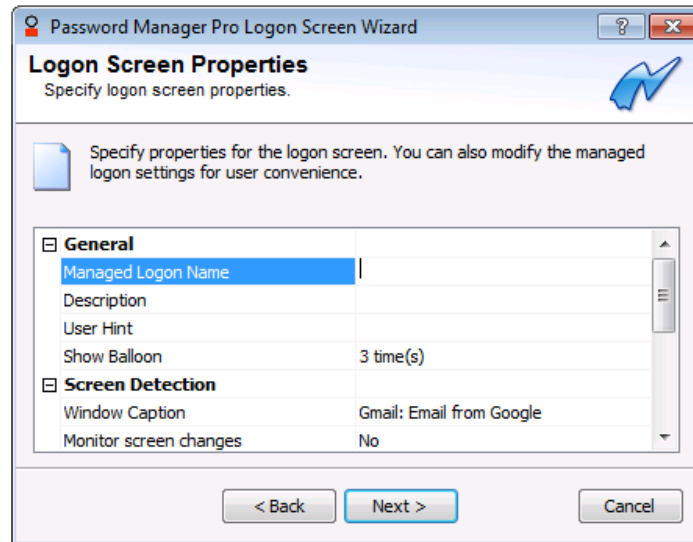
5. On the first page of the wizard, confirm that the logon screen has been detected and verify the title of the logon screen.



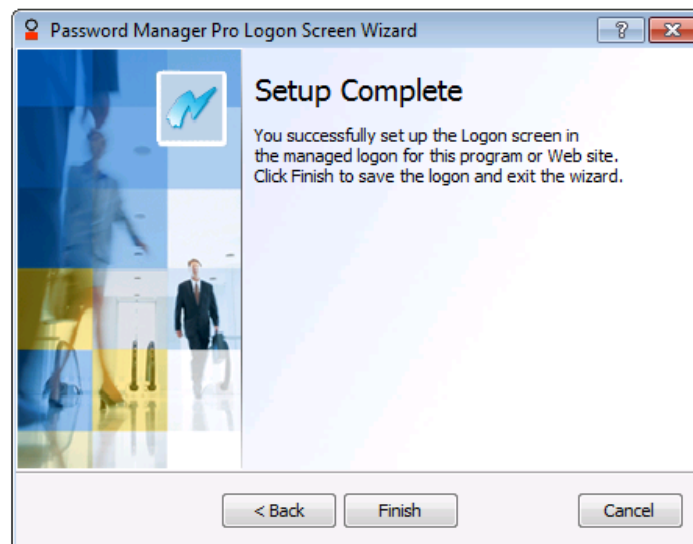
6. Select **Set up a managed logon manually** and then click **Next**.
7. On the **Logon Fields** page, click **Add** and select an action from the drop-down menu.



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 12) 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.

12. 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 logons* on page 5.

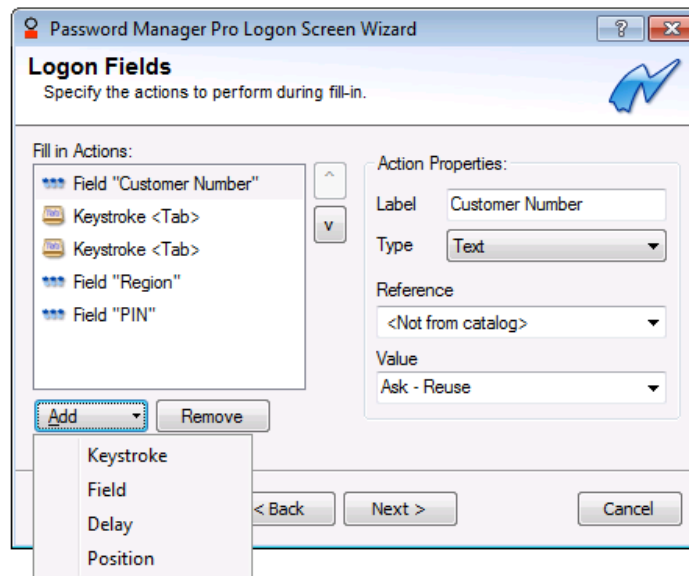
Deploying managed logons

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**.
3. 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 drop-down menu provides a list of actions that are used to build a script for logon and change password screens that cannot be automatically configured by Password Manager Pro.

Action	Description
Keystroke	<p>This key sequence of one or more keys will be placed in the keyboard buffer. Keystroke properties are:</p> <p>Key - Select the main key to be entered.</p> <p>Repeat - Specify the number of times the key sequence is entered.</p> <p>Shift, Control, Alt - Optionally, select one of these keys in combination with the main key. Check Generic, Left or Right to simulate pressing one or more of these keys in addition to the key you selected.</p>

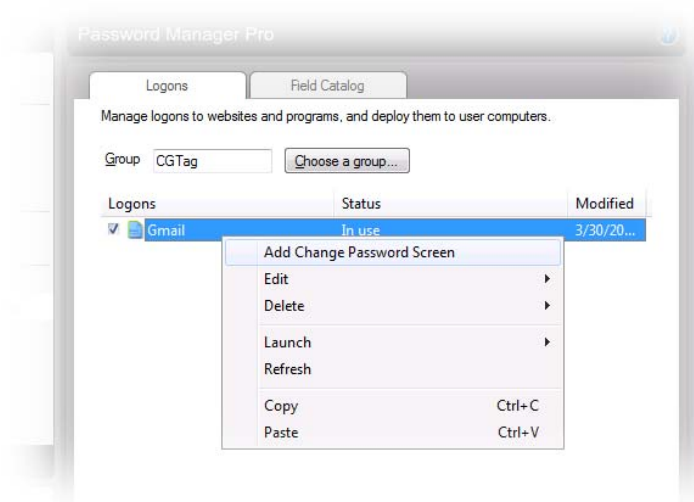
Action	Description
Field	<p>Define a Logon field by specifying these properties:</p> <p>Label - Type a label name for the corresponding field on the logon screen. The labels are displayed when users are prompted to type a value for a logon field.</p> <p>Type - Select the type of field, either text or password. Choosing password hides the password on the logon screen; choosing text displays readable text.</p> <p>Reference - Optionally, select a field previously defined on the Field Catalog tab.</p> <p>Value - Type a value for the logon field or use the Value drop-down menu to indicate a value specified by the user or provided by the program.</p> <p>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.</p>
Delay	Specify how many seconds to wait before the next action in the list is performed.
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.

Option Heading	Description
Label	If the label for a field is not intuitively related to the corresponding field on the logon screen, enter a new label name in this field. The labels are displayed when users are prompted to type a value for a logon field.
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 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 16.

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	When enabled: If the password is provided by the user, it must conform to the listed password requirements. If the password is generated by Password Manager Pro, the password will be generated according to the listed password requirements.
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	Select one of the following requirements: Letters and numbers - allows any combination of letters and/or numbers. Numbers only - allows numbers only. Letters only - allows letters only. 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. Letters and numbers with at least one number - passwords must contain at least one letter and at least one number.

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 drop-down menu.

For example, you might study a Change Password screen and discover that it takes presses of the tabs 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.)c\1*" 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}	<p>Match the last "block" at least x and not more than y times. For example, "a{3,5}" matches "aaa", "aaaa" or "aaaaa".</p>
+	<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:</p> <p>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:</p> <p>caab</p>

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 logons* on page 31).

The following logon management features are described in this section.

Feature	Page
Editing logons	29
Deleting logons	30
Importing logons	30
Deploying logons	31
The Field Catalog	31
Finding logons	33
Finding duplicate logons	33
Finding fields in logons	32

Editing logons

To edit a logon:

1. Choose a group to edit its managed logons.
2. Select a logon to edit and click **Manage**.
3. Click **Edit** and select either **Logon Screen** or **Change Password Screen**.
4. 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	10
Values	11

Reference	Page
Logon properties	12
Logon Fields actions	20
Password policies	24

- When editing is complete, click **Finish** to exit the wizard.
- 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:

- Choose a group to edit its managed logons.
- Right-click on the logon that you want to delete and click **Delete**.
- 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.
- 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.

Importing logons

To import (copy) logons from one group to another

- Choose a group.
- Click **Manage**, and then select **Import Logons**.

In most cases, this feature will be used to copy logons from an existing group into an empty group. However, note that imported logons *will overwrite all* previously existing logons in the selected target group.

Deploying logons

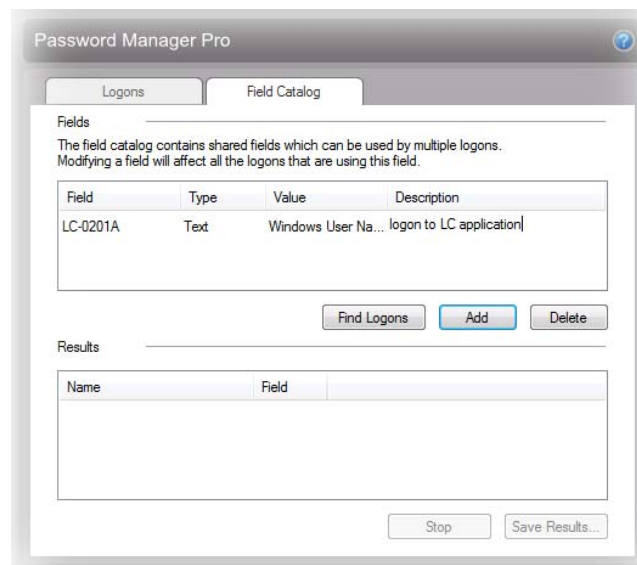
To deploy managed logons:

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** drop-down list.
4. Specify the value of the field (see page 11) from the **Value** drop-down 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, and set any desired values (see previous topic).
2. Create a managed logon manually (see page 16).
3. On the Logon Fields page of the wizard, **Add** a password field.
4. In the Action Properties area, under Reference, select the desired field from the catalog.
5. Add any further fields or actions need to complete the logon.

Finding fields in logons

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

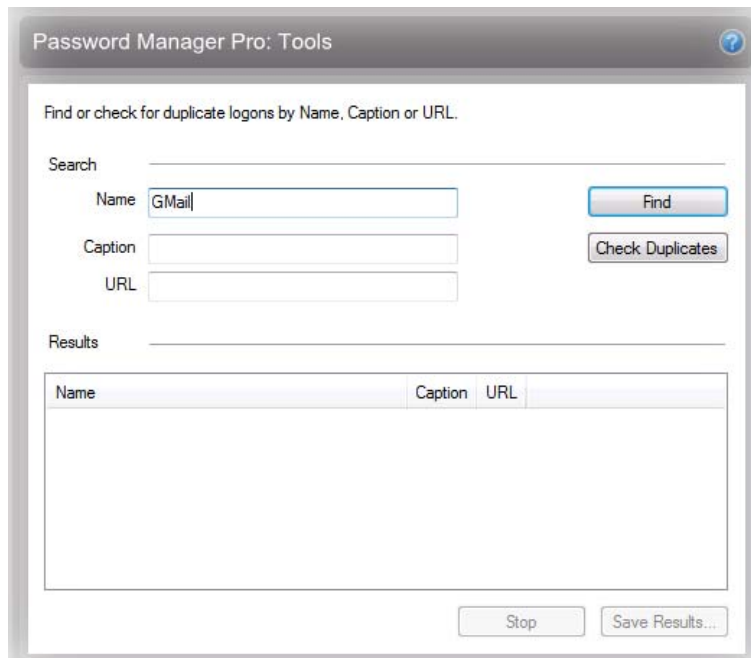
To search for logons that contain selected fields:

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.

This chapter contains information that you will want to make sure is passed on to your end-users. The same information is also included in the end-user help file included with the client Password Manager application.

Logging On

After creating managed logons and deploying them to users, they will then 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 the user has set up 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.

Index

A

adding a change password screen **23**
adding a change password screen manually **23**
adding fields to the Field catalog **31**
attributes **10**

C

change password screen **23**
changing passwords **35**
chapter overview **1**
credentials, defined **2**

D

delay **21**
deploy managed logons **9, 19, 23, 26, 31**

E

editing logons **29**

F

field catalog **31**
finding duplicate logons **33**
finding fields in logons **32**
finding logons **33**

G

group, defined **2**

I

installation **4**

K

Knowledge Portal **3**

L

logging on **35**
logon field values **11**
logon fields **10, 13**
logon fields actions **20**
logon fields attributes **10**
logon fields properties **12**
logon, defined **2**

M

Maintenance and Support **3**
managed computer **2**
managed logons **2, 5**

O

online help **4**

P

password field values **11**
Password Manager **2**
Password Manager Pro **3**
password policies **24**
personal logon **2, 3**
Pro Workgroup client **2**
Pro Workgroup server **3**
properties **12**

R

regular expression syntax **27**

S

secret **3**
setting up a change password screen **22**
setting up a change password screen manually **25**
setting up a logon screen **5**
support
 online help **4**
 readme file **3**

T

target icon **21**
Tools page **33**

U

using logon screens **35**

V

values **11**

W

web console **3**