# Table of Contents

## 1 Product Overview

1. Introduction ................................................. 5
2. Personal logons vs Managed logons ............................ 5
3. Central Management ......................................... 6
4. Installation ................................................. 6
5. Configuration ................................................ 6
6. Licensing ................................................... 7
7. User interfaces .............................................. 7

## 2 Centralized management

1. Policies and settings ........................................ 8
2. Reporting ................................................... 10
3. Password Manager events ................................... 10

## 3 End user experience

1. Managed logons and personal logons ........................ 12
2. Adding logons ................................................ 12
3. Creating logons .............................................. 13
4. Remembering logons ........................................ 15
5. Import and export .......................................... 15
6. Importing logons ............................................ 15
7. Editing logons ............................................... 17
8. Organizing logons into categories ........................... 19
9. Managing your logons ....................................... 20
10. Using the Logons Menu ..................................... 20
11. Using managed logons ...................................... 20
12. Logging On .................................................. 21
13. Changing passwords ....................................... 21
14. Differences in supported browsers ......................... 21
15. Backing up your data ..................................... 23
16. Restoring your data ........................................ 23

## 4 Password Manager Admin Tool

1. Overview ................................................... 24
2. System requirements ....................................... 25
3. Installation .................................................. 25
4. Setting up the DigitalPersona Password Manager Admin Tool ....... 26
5. Managed logons ............................................. 29
6. Creating managed logons .................................. 29
7. Logon Fields attributes .................................... 33
8. Values ....................................................... 34
9. Logon properties .......................................... 35
Product Overview

This chapter contains the following topics.

<table>
<thead>
<tr>
<th>Topics</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>Installation</td>
<td>6</td>
</tr>
<tr>
<td>Configuration</td>
<td>6</td>
</tr>
<tr>
<td>Licensing</td>
<td>7</td>
</tr>
<tr>
<td>User interfaces</td>
<td>7</td>
</tr>
</tbody>
</table>

Introduction

DigitalPersona Password Manager and the DigitalPersona Password Manager Admin Tool 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. It is included as a core feature of the DigitalPersona Altus solution.

The Password Manager Admin Tool (see Password Manager Admin Tool on page 24), is a separate Altus component used by administrators for creating managed logons (described below).

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 Admin Tool. Managed logons provide all of the same benefits to the end user, but provide greater flexibility and control to the administrator. See the Password Manager Admin Tool chapter for details on the DigitalPersona Password Manager Admin Tool.
Central Management

Centralized management of DigitalPersona Password Manager features is available through Active Directory. 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 8.

Installation

The DigitalPersona Password Manager application is a core feature of the DigitalPersona Altus solution, and there is no separate installation required. There are no additional system requirements beyond those specified for the Altus Workstation and Kiosk clients specified in the DigitalPersona Altus Administration Guide.

The Password Manager Admin Tool is an optional administrative tool which requires separate installation. For further details on the Password Manager Admin Tool, see Password Manager Admin Tool on page 24.

Configuration

Password Manager features are enabled by default, however 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. Additional settings available are described in the Centralized Management chapter.

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 Altus 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.

**Licensing**

Licenses for the Password Manager application are included in, and automatically deployed, during the activation of licenses for DigitalPersona Altus on the Altus Server.

**User interfaces**

Password Manager functionality is provided at two levels: Centralized Management and End-user.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized management</td>
<td>Through Active Directory and GPOs</td>
<td>8</td>
</tr>
<tr>
<td>End user experience</td>
<td>In a compatible Altus client’s user console</td>
<td>11</td>
</tr>
</tbody>
</table>
This chapter includes the following topics.

<table>
<thead>
<tr>
<th>Topics</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies and settings</td>
<td>8</td>
</tr>
<tr>
<td>Reporting</td>
<td>10</td>
</tr>
<tr>
<td>Password Manager events</td>
<td>10</td>
</tr>
</tbody>
</table>

DigitalPersona Password Manager is centrally managed through the DigitalPersona Altus solution. DigitalPersona Altus provides Active Directory GPO settings that may be used to manage various aspects of Password Manager.

Central management of DigitalPersona Password Manager is initially exposed through a single setting described below.

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.

## Policies and settings

### Computer policies

**Prevent Password Manager from running**

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

```
Computer Configuration\Policies\Administrative Templates\DigitalPersona Altus 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.

### User policies

**Allow creation of personal logons**

You can allow users to create and use personal logons for websites and programs using this setting, located at:
Chapter 2 - Centralized management

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

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

Managed logons
Configure settings for managed logons that govern access to account data and the deployment of logons to users.

If enabled, the options listed below can be configured.
If disabled or not configured managed logons will not be available to users.

- Allow users to view managed logon passwords: If this option is selected, users are allowed to view their managed logon passwords after verifying their identity. If unselected, users are not allowed to view managed logon passwords.
- Allow users to edit account data: If this option is selected, users can edit their account data. If unselected, users cannot edit account data.
- Allow users to add account data: If this option is selected, users can add to their account data. If unselected, users cannot add new account data.
- Allow users to delete account data: If this option is selected, users can delete their account data. If unselected, users cannot delete account data.

Path(s) to the managed logons folder(s): When the setting is enabled, managed logons located in the specified folder are copied to all Altus computers that have this setting applied. Multiple folders may be specified by separating the paths with a pipe character (|). If no valid path is specified, managed logons will not be available to users.
Chapter 2 - Centralized management

**Reporting**

DigitalPersona Password Manager writes Activity Events to the local Windows Event Viewer Event Log, under the Altus\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 Altus Reports, see the Altus Reports chapter in the DigitalPersona Altus Administrator Guide.

**Password Manager events**

Task Category: 1536

These events are generated when personal or managed logons are used or logon account data is modified.

<table>
<thead>
<tr>
<th>Event</th>
<th>ID</th>
<th>Level (Workstation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRC check failure in %1.</td>
<td>1548</td>
<td>Dt</td>
</tr>
<tr>
<td>Logon created</td>
<td>1549</td>
<td>Dt</td>
</tr>
<tr>
<td>Logon modified</td>
<td>1550</td>
<td>Dt</td>
</tr>
<tr>
<td>Logon deleted</td>
<td>1551</td>
<td>Dt</td>
</tr>
<tr>
<td>Password change has been canceled by user</td>
<td>1552</td>
<td>Dt</td>
</tr>
<tr>
<td>Fillin was performed</td>
<td>1553</td>
<td>Dt</td>
</tr>
<tr>
<td>Account data could not be modified</td>
<td>1554</td>
<td>E</td>
</tr>
<tr>
<td>Account data was successfully modified.</td>
<td>1555</td>
<td>Dt</td>
</tr>
<tr>
<td>Account data was successfully entered.</td>
<td>1556</td>
<td>Dt</td>
</tr>
<tr>
<td>Account data was successfully deleted.</td>
<td>1557</td>
<td>Dt</td>
</tr>
</tbody>
</table>

Level: E = Error, A = Audit, Dt = Details, Fd = Fine details
This chapter includes the following topics.

<table>
<thead>
<tr>
<th>Topics</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed logons and personal logons</td>
<td>12</td>
</tr>
<tr>
<td>Adding logons</td>
<td>12</td>
</tr>
<tr>
<td>Importing logons</td>
<td>15</td>
</tr>
<tr>
<td>Organizing logons into categories</td>
<td>19</td>
</tr>
<tr>
<td>Managing your logons</td>
<td>20</td>
</tr>
<tr>
<td>Using the Logons Menu</td>
<td>20</td>
</tr>
<tr>
<td>Using managed logons</td>
<td>20</td>
</tr>
</tbody>
</table>

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 Altus enrolled credentials such as a fingerprint, smart/proximity/contactless card, or your Windows password. Additional auxiliary credentials can also be used in multi-factor authentication.

Password Manager allows you to:

- Personal logons - Add, edit, or delete personal logons and logon account data.
Chapter 3 - End user experience

- Managed logons - Add, edit or delete logon account data for managed logons provided by your administrator. This feature may optionally be disabled by the administrator.
- Use personal or managed logons to launch your default browser and log on to any website or program.
- 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 Admin Tool 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 8.

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 Password Manager Admin Tool chapter beginning on page 24 for a description of the Password Manager Admin Tool.

*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**

There are three ways you can easily add a logon for a website or a program to Password Manager.

- With a website or program logon screen displayed in your browser, scan an enrolled fingerprint or present an enrolled card to display the Create Logon dialog.
- Log in to a website or program and Password Manager will offer to remember your account information.
- Import your previously saved login information from Internet Explorer, Chrome or Firefox.

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.
Creating logons

To add a logon from the Create Logon dialog

1. With a website or program logon screen displayed in your browser, scan an enrolled fingerprint or present an enrolled card to display the Create Logon dialog.

2. Enter your logon data.
   - To populate the Username field with a preformatted Windows credential, click the arrow to the right of the field and select one of the displayed options.
     - Windows User Name
     - Windows User Principal Name
     - Windows Domain\User Name
     - Windows Domain
   - To populate the Password field with a preformatted credential, click the arrow to the right of the field and select one of the displayed options. Note that colored line under the Password field. This indicates password strength from red, through yellow to green for optimum strength.
     - Windows User Password

   Use previous password… - Sometimes, you may modify a password in Password Manager, but this password is rejected by the application. In this case, the software allows you to use a previous password (i.e. a password previously entered for this logon page) instead of the most recent one.

   If you select Use previous Password, after authentication you will be prompted to choose an old password from the Password Manager list. The list includes up to seven passwords and can be cleared (deleted) permanently by clicking the Clear list button.

   - 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.
Chapter 3 - End user experience

3 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 you can clear the check box for any fields that are not required for logon.

4 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 now “trained” website, program or network resource, the Password Manager icon shown below is displayed on the screen (Internet Explorer) or to the right of the first recognized entry field (Firefox and Chrome), indicating that you can use any of your enrolled credentials to log on. An administrator can also create managed logons for resources, including Change Password screens (see **Password Manager Admin Tool** on page 24).

Password Manager Icon for Internet Explorer

Password Manager Icon for Internet Explorer as displayed on a recognized Change Password screen

Password Manager Icon for Firefox and Chrome

Password Manager Icon for Firefox and Chrome as displayed on a recognized Change Password screen
Chapter 3 - End user experience

**Remembering logons**

Simply log in to a website or program as usual and Password Manager will offer to remember your account information.

![Password Manager reminder](image)

Click *Remember* and your logon information is saved. Next time you can log in with any enrolled credential.

If you do not want to see the Password Manager reminder each time you visit this site, select *Never for this site*.

**Import and export**

From the Password Manager Import and export page, you can

- Import logon data from your web browser (see next topic)
- Backup your Password Manager data (see page 23)
- Recover backed up Password Manager data (see page 23)

**Importing logons**

Password Manager provides the ability to import saved logon and password information from popular browsers, i.e. Internet Explorer, Firefox and Chrome.

Importing login information is accomplished on the Import and Export page, accessed from the *Import and export* link at the bottom of the main Password Manager page.

Importing passwords is done on a browser-by-browser basis and the browser may have been set up to require a master password in order to retrieve stored password credentials.
Chapter 3 - End user experience

Note that, on the Import page, a button is displayed for a specific browser only when that browser is actually installed on the system.

Upon successful retrieval of passwords from a browser, the user is provided with the list of addresses and their corresponding user names so they may select/deselect the logons to import into Password Manager.

Once imported, the logons will be shown on the main Password Manager page, where they can then be managed and used to launch the associated website or program.
Editing logons
You can edit a logon from the Password Manager page, or from the Edit Logon dialog, whichever is more convenient at the time.

Editing from the Password Manager page
To edit a previously created logon from within the main Password Manager page
1. Click the logon entry to display the editing options and select _Edit_.

2. The logon entry will be expanded to show previously saved logon information and additional options.

3. The account data includes the following editable fields:
   - Account name – The name used on the main Password Manager page to identify this account.
   - Category - The name used for categorizing accounts on the main Password Manager page.
Chapter 3 - End user experience

- Password – (Hidden by default) To show the password, click the Show button.

- [Any optional additional fields and data saved for this account]
- This password is compromised checkbox (see explanation below).

**Marking compromised logons**

Password Manager provides a feature for marking logons that the user believes have been compromised, and easily identifying any additional stored logons that contain the same logon data.

To mark a logon as compromised

- Select the checkbox. These accounts will then be listed under the Compromised Accounts category.

To mark a logon as not compromised

- Deselect the checkbox. Note that when marking a logon as not compromised, logons have to be unmarked individually, i.e. one at a time. Associated logons with the same password are not affected.

Notice the small flags to the left of the Microsoft logon in the image below. This is the visual indicator for a compromised account.

![Password Manager Interface](image)

When any account is marked compromised, all accounts sharing the same user name and password will be marked with a solid red flag.

Accounts sharing only the compromised password will be marked with a yellow flag.
Chapter 3 - End user experience

**Editing from the Password Manager icon**

To edit logon information from the Password Manager icon

1. Open the logon screen for a website or program.
2. Click the arrow on the Password Manager icon, and then click Edit logon to display a dialog for editing your account information.
3. Edit your logon information. See the topic *Editing from the Password Manager page* on page 17 for further details.
4. Click **Save**.

**Organizing logons into categories**

Keep your logons in order by assigning them to custom categories.

Logons can be added to a group by entering a group name when editing the logon. A logon may belong to only one category.

However, when creating additional logons for the same web domain,

If there are two or more accounts belonging to the same web domain, which do not belong to any custom category, then they will be categorized by their domain name (defined as the characters appearing after "http(s):/" and before the domain zone.)

If an account is already assigned to a custom category, there is no nested category for it based on the domain name.

- To rename a category, select the category and then click **Rename**.
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 Password Manager page in the Altus user console. 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 user console, click **Password Manager**

- Edit a logon - Click a logon, then click **Edit** to change the logon data.
- Delete a logon - Click a logon, then click **Delete**.

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. You can change Hot Key combination from the Altus user console, by clicking Password Manager and then clicking **Settings**.
- Scan your fingerprint (on computers with a built-in or connected fingerprint reader).

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.
Chapter 3 - End user experience

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.

Differences in supported browsers

Internet Explorer

All features described in this Application Guide are supported in those versions of Microsoft Internet Explorer that are listed in the System Requirements.
Firefox
When used with supported versions of the FireFox browser, all Password Manager features are available except for Manual Mode (see page 14), and the following Logon properties used in creating managed logons: Lock out logon fields and Monitor screen changes (see page 35).

Chrome
When used with supported versions of the Chrome browser, all Password Manager features are available except for Manual Mode (see page 14), and the Lock out Logon Fields property used in creating managed logons (see page 35).

When logging in to a website with a managed logon that was created with the Start Authentication Immediately property set, after logging out or canceling the authentication dialog and being returned to the login page, the authentication dialog is not redisplayed.
Chapter 3 - End user experience

**Backing up your data**

It is recommended that you back up your workstation data on a regular basis. How often you back it up depends on how often the data changes. For instance, if you add new logons on a daily basis, you should probably back up your data daily.

Backups can also be used to migrate from one computer to another, also called importing and exporting.

NOTE: Only the data is backed up by this feature.

A DigitalPersona Altus compatible client must be installed on any computer that is to receive backed up data before the data can be restored from the backup file.

To back up your data:

1. From the Password Manager page, select **Import and export**, then **Backup**.
2. Select **Next**.
3. Enter a full path name and filename for the backup file. Click **Browse** to specify a different location.
4. Enter and confirm a password that will be used to protect the file.
5. Then click **Save**.

**Restoring your data**

To restore your data:

1. From the Password Manager page, select **Import and export**, then **Backup**.
2. Click **Restore data**.
3. Specify the previously created backup file. You can enter the full path and filename in the field provided, or click **Browse** and navigate to the file.
4. Enter the password used to protect the file. Then select **Next**.
5. Choose the modules whose data you want to restore. In most cases, this would be all of the modules listed.
6. Click **Restore**.
This chapter covers the following topics:

<table>
<thead>
<tr>
<th>Topics</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>24</td>
</tr>
<tr>
<td>System requirements</td>
<td>25</td>
</tr>
<tr>
<td>Setting up the DigitalPersona Password Manager Admin Tool</td>
<td>26</td>
</tr>
<tr>
<td>Managed logons</td>
<td>29</td>
</tr>
<tr>
<td>Setting Up a Change Password screen</td>
<td>44</td>
</tr>
<tr>
<td>Regular Expression syntax</td>
<td>51</td>
</tr>
<tr>
<td>Managing logons</td>
<td>53</td>
</tr>
<tr>
<td>The Field Catalog</td>
<td>55</td>
</tr>
<tr>
<td>Tools page</td>
<td>57</td>
</tr>
</tbody>
</table>

The Password Manager Admin Tool enables administrators to provide controlled access to websites, programs and network resources by adding a variety of authentication mechanisms (such as password, smart/proximity/contactless card or fingerprint) to their logon and change password screens. The DigitalPersona Password Manager Admin Tool is an add-on module to the Administrative Console, which may be part of your product package, or can be separately purchased through DigitalPersona or your authorized reseller.

**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. The DigitalPersona Password Manager Admin Tool 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 Altus 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.

Each time that a user accesses the “trained” website, program or network resource, the Password Manager icon shown below is displayed in the upper left corner of the screen (Internet Explorer and Firefox) or to the right of the first recognized entry field (Firefox and Chrome), indicating that you can use any of your enrolled credentials to log on.

Password Manager Icon for Internet Explorer

Password Manager Icon for Internet Explorer as displayed on Change Password screens

Password Manager Icon for Firefox and Chrome

Password Manager Icon for Firefox and Chrome as displayed on Change Password screens

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.

**System requirements**

Installation of the DigitalPersona Password Manager Admin Tool requires the previous installation of DigitalPersona Altus Workstation. Although Microsoft Internet Explorer is not required prior to installation, it is required in order to create managed logons with the tool.

**Installation**

To install the DigitalPersona Password Manager Admin Tool
1 Locate and launch the setup.exe located in the software package you were provided.
2 Follow the onscreen instructions.
3 Once installation is complete, set up the tool by following the instructions in the next topic.

**Setting up the DigitalPersona Password Manager Admin Tool**

Before using the DigitalPersona Password Manager Admin Tool, you will need to set it up.

In DigitalPersona Altus, managed logons are organized in shared folders created and maintained through the DigitalPersona Password Manager Admin Tool.

The folder should be created on a shared network drive accessible to the DigitalPersona Altus 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 Password Manager Admin Tool.

**Create a shared network folder**

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

The folder should be created on a shared network drive accessible to the DigitalPersona Altus 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.

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, DPAltusClient (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 the chapter *Install the Administrative Templates* in the DigitalPersona Altus Administrator Guide.

2 Open the GPO where the DigitalPersona template was added.

3 Go to User Configuration\Administrative Templates\DigitalPersona Altus Client\Password Manager.

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

The default setting is "Not Configured". Click on **Enabled** 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 Altus clients during the usual refresh interval or the next time they restart Windows.
Managed logons

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 Altus, 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.

The Password Manager Admin Tool 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 Admin Tool 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 Admin Tool.
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**.

Click **Add Logon**. The Password Manager Admin Tool Logon Screen wizard launches.

Launch the logon screen for the password-protected website or program.

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 39.

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 33) and values (see page 34) and then click **Next**.
7 On the **Submit Option** page, choose the button that submits the logon data.

![Submit Option page]

- 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 35) for the Logon Screen.

![Logon Screen Properties]

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 39.
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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use</td>
<td>Check the Use checkbox for each field used for logon. Some fields discovered by the wizard may not be relevant to logon, such as a search field on a website logon page. Leave these unchecked.</td>
</tr>
<tr>
<td>Label</td>
<td>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.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of field, either text or password, is displayed in the Type text box. This value is not editable. <strong>Password</strong> hides the password on the logon screen so it cannot be viewed. <strong>Text</strong> displays readable text.</td>
</tr>
<tr>
<td>Catalog</td>
<td>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 55.</td>
</tr>
<tr>
<td>Value</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ask-Reuse</td>
<td>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.</td>
</tr>
<tr>
<td>Ask-Confirm</td>
<td>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.</td>
</tr>
<tr>
<td>Ask Always</td>
<td>Prompts the user to enter a value for a logon field each time they use the logon.</td>
</tr>
<tr>
<td>Windows User Name</td>
<td>Password Manager provides the Windows user name.</td>
</tr>
<tr>
<td>Windows User Principal Name</td>
<td>Password Manager provides the user name and domain values in UPN format. Example: [user name]@[domain].</td>
</tr>
<tr>
<td>Windows Domain\ User Name</td>
<td>Password Manager provides the domain of the user followed by a backslash and the user name. Example: [domain][user name].</td>
</tr>
<tr>
<td>Windows Domain</td>
<td>Password Manager provides the user domain name only.</td>
</tr>
<tr>
<td>Windows E-Mail Address</td>
<td>Password Manager provides the registered E-Mail address for the Windows user account currently logged on.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows User Password</td>
<td>Password Manager provides the password used for Windows logon.</td>
</tr>
<tr>
<td>Write Only</td>
<td>Always prompts a user for the value.</td>
</tr>
<tr>
<td>Defender One-time Password</td>
<td>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.</td>
</tr>
<tr>
<td>Defender One-time Password + Windows User Password</td>
<td>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.</td>
</tr>
</tbody>
</table>
## Password Manager Admin Tool

### Category Property Description

<table>
<thead>
<tr>
<th>Category</th>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Managed Logon Name</td>
<td>The name of the logon.</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>Can be used to enter optional information about the managed login that is only viewable on the Password Manager Admin Tool Logons tab. By default, this column is hidden. To display the column, right click anywhere in the column headings area and select <strong>Description</strong>.</td>
</tr>
<tr>
<td></td>
<td>User Hint</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Show Balloon</td>
<td>(Logon screens only) Once this managed logon is created and deployed, a balloon tip will automatically display (up to three times) when the user accesses the logon screen. Use this setting to select how many times the balloon is displayed.</td>
</tr>
<tr>
<td>Screen Detection</td>
<td>Window Caption</td>
<td>Title of the screen as detected by the wizard; used to match the managed logon to the specified screen. 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. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*Some Application Login</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Some Company*Login</td>
</tr>
<tr>
<td></td>
<td></td>
<td>My Bank Login*</td>
</tr>
</tbody>
</table>
Monitor screen changes

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.

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.

Use of this setting is resource intensive, and it is disabled by default.

URL

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:

- Do Not Match - This is the default. URL matching will not be performed.
- String Match - Matches the exact string displayed.
- Wildcard Match - Matches a displayed string utilizing an asterisk (*) to represent the portion of the URL that may change.
- Regular Expression - Matches a displayed string constructed as a regular expression (See “Regular Expression syntax” on page 51).
- Case Sensitive - Ignore case when matching.
- Restore Defaults - Return to the default URL settings.

<table>
<thead>
<tr>
<th>Category</th>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor screen changes</td>
<td></td>
<td>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. 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. Use of this setting is resource intensive, and it is disabled by default.</td>
</tr>
<tr>
<td>URL</td>
<td></td>
<td>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: Do Not Match - This is the default. URL matching will not be performed. String Match - Matches the exact string displayed. Wildcard Match - Matches a displayed string utilizing an asterisk (*) to represent the portion of the URL that may change. Regular Expression - Matches a displayed string constructed as a regular expression (See “Regular Expression syntax” on page 51). Case Sensitive - Ignore case when matching. Restore Defaults - Return to the default URL settings.</td>
</tr>
</tbody>
</table>
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 dropdown list. The options are the same as those listed above for the URL.

<table>
<thead>
<tr>
<th>Category</th>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Start Authentication</td>
<td>If set to <strong>Yes</strong>, the user is prompted for their credential immediately after the logon screen displays. The default setting is <strong>No</strong>.</td>
</tr>
<tr>
<td></td>
<td>Lock out logon fields</td>
<td>If set to <strong>Yes</strong>, the user is prevented from typing data in the logon fields. The default setting is <strong>No</strong>.</td>
</tr>
<tr>
<td>Password Manager icon</td>
<td>Location ID</td>
<td>Identifies the location selected in the Location field (below) so that it can be shared with other logon screens.</td>
</tr>
<tr>
<td></td>
<td>Location</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 Admin Tool.

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 Admin Tool 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 42) 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 35) for the logon screen.

![Logon Screen Properties](image)

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 29.

**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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keystroke</td>
<td>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 <strong>Generic</strong>, <strong>Left</strong> or <strong>Right key</strong> as well.</td>
</tr>
<tr>
<td>Field</td>
<td>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 <strong>text</strong> or <strong>password</strong>. 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.</td>
</tr>
</tbody>
</table>
### Chapter 4 - Password Manager Admin Tool

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delay</td>
<td>Specify how many seconds to wait before the next action in the list is performed.</td>
</tr>
</tbody>
</table>
| Position | Specify a location where the system will perform a mouse click. Position is measured from the top left corner of the client window area.  
Client X - Type a number of pixels for the X axis position for the action.  
Client Y - Type a number of pixels for the Y axis position for the action.  
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. |
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.

<table>
<thead>
<tr>
<th>Option Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use</td>
<td>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.</td>
</tr>
<tr>
<td>Label</td>
<td>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.</td>
</tr>
</tbody>
</table>
Chapter 4 - Password Manager Admin Tool

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.

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.

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.

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

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 39.

<table>
<thead>
<tr>
<th>Option Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalog</td>
<td>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.</td>
</tr>
<tr>
<td>Value</td>
<td>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.</td>
</tr>
</tbody>
</table>
**Password policies**

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password is provided by user</td>
<td>The Password Manager Admin Tool does NOT provide password information to the program. (The user has the option to log on by entering their password or another allowed credential.)</td>
</tr>
<tr>
<td>Password is generated automatically</td>
<td>The Password Manager Admin Tool generates the password automatically. An alternate credential must be used to log on.</td>
</tr>
</tbody>
</table>
| 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 the Password Manager Admin Tool, 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. |
Chapter 4 - Password Manager Admin Tool

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional password requirements</td>
<td>None. No other constraints are applied to the password contents.</td>
</tr>
<tr>
<td></td>
<td><strong>Different than the Windows password.</strong> The new password must be different</td>
</tr>
<tr>
<td></td>
<td>than the current Windows password.</td>
</tr>
<tr>
<td></td>
<td><strong>Unique within Password Manager managed logons.</strong> The new password must be</td>
</tr>
<tr>
<td></td>
<td>different from any other password associated with this managed logon for a</td>
</tr>
<tr>
<td></td>
<td>specified user account.</td>
</tr>
<tr>
<td></td>
<td><strong>Different than the current password.</strong> The new password must be different</td>
</tr>
<tr>
<td></td>
<td>than the current password for this website or program.</td>
</tr>
</tbody>
</table>
Chapter 4 - Password Manager Admin Tool

### Setting up a Change Password Screen manually

If the Password Manager Admin Tool 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 the Password Manager Admin Tool, select the logon for that website or program.

3. Right-click to display that logon’s context menu, then click **Add Change Password Screen**.

   ![Password Manager Admin Tool Change Password Screen wizard](image)

   The Password Manager Admin Tool 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.

![Change Password Screen Properties](image)

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).

<table>
<thead>
<tr>
<th>MC</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td>Matches any single character</td>
</tr>
<tr>
<td>[]</td>
<td>Matches a single character that is contained within the brackets. For example, [abc] matches &quot;a&quot;, &quot;b&quot;, or &quot;c&quot;. [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'.</td>
</tr>
<tr>
<td>^</td>
<td>Matches a single character that is not contained within the brackets. For example, [^abc] matches any character other than &quot;a&quot;, &quot;b&quot;, or &quot;c&quot;. [^a-z] matches any single character that is not a lowercase letter. As above, these can be mixed.</td>
</tr>
<tr>
<td>^</td>
<td>Matches the start of the line (or any line, when applied in multiline mode)</td>
</tr>
<tr>
<td>$</td>
<td>Matches the end of the line (or any line, when applied in multiline mode)</td>
</tr>
<tr>
<td>( )</td>
<td>Defines a &quot;marked subexpression&quot;. What the enclosed expression matched can be recalled later. See the next entry, \n. Note that a &quot;marked subexpression&quot; is also a &quot;block.&quot;</td>
</tr>
<tr>
<td>\n</td>
<td>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.</td>
</tr>
<tr>
<td>*</td>
<td>A single character expression followed by &quot;+&quot; matches zero or more copies of the expression. For example, &quot;[xyz]*&quot; matches &quot;&quot;, &quot;x&quot;, &quot;y&quot;, &quot;zx&quot;, &quot;zyx&quot;, and so on.</td>
</tr>
</tbody>
</table>
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 "abcaec".

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 "*".

<table>
<thead>
<tr>
<th>MC</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\n*</td>
<td>Where <code>n</code> is a digit from 1 to 9, matches zero or more iterations of what the nth marked subexpression matched. For example, &quot;(a.:c\1)*&quot; matches &quot;abcab&quot; and &quot;abcabab&quot; but not &quot;abcaec&quot;.</td>
</tr>
<tr>
<td>{x,y}</td>
<td>Match the last &quot;block&quot; at least <code>x</code> and not more than <code>y</code> times. For example, &quot;a{3,5}&quot; matches &quot;aaa&quot;, &quot;aaaa&quot; or &quot;aaaaa&quot;.</td>
</tr>
<tr>
<td>+</td>
<td>The <code>+</code> operator will match the preceding atom (a single character, a marked subexpression, or a character class) one or more times, for example the expression a+b will match any of the following: ab aaaaaaab But will not match: b</td>
</tr>
<tr>
<td></td>
<td>The `</td>
</tr>
<tr>
<td>?</td>
<td>The <code>?</code> operator will match the preceding atom (a single character, a marked subexpression, or a character class) zero or one times, for example the expression ca?a will match any of the following: cb cab But will not match: caab</td>
</tr>
</tbody>
</table>
Managing logons

The Password Manager Admin Tool 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 41).

The following logon management features are described in this section.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Editing logons</td>
<td>53</td>
</tr>
<tr>
<td>Deleting logons</td>
<td>54</td>
</tr>
<tr>
<td>Deploying logons</td>
<td>54</td>
</tr>
<tr>
<td>The Field Catalog</td>
<td>55</td>
</tr>
<tr>
<td>Finding logons</td>
<td>57</td>
</tr>
<tr>
<td>Finding duplicate logons</td>
<td>57</td>
</tr>
<tr>
<td>Finding fields in logons</td>
<td>56</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Reference</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logon Fields attributes</td>
<td>33</td>
</tr>
<tr>
<td>Values</td>
<td>34</td>
</tr>
<tr>
<td>Logon properties</td>
<td>35</td>
</tr>
<tr>
<td>Logon Fields actions</td>
<td>42</td>
</tr>
<tr>
<td>Password policies</td>
<td>46</td>
</tr>
</tbody>
</table>
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 34) 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 39).
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 41.

**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 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.
Chapter 4 - Password Manager Admin Tool

Password Manager Actions

Password Manager Actions are operations that may be performed when an assigned DigitalPersona Altus Hot Key(s) are pressed, or a specified credential or credential combination is presented.

Password Manager Actions may be assigned to the DigitalPersona Hot Key, credential or credential combination through the Quick Actions GPO setting on the DigitalPersona Altus Server.

The Password Manager Action that will be performed depends on the context. One of the following operations will be performed, in the listed order of preference.

1. When the active window is a website, program or other resource associated with a previously created personal or managed logon - trained fields will be filled in with user account data.

2. If the active window does not have a previously created personal or managed logon - The Create Logon dialog is displayed allowing creation of a personal logon for the resource. This action also requires that the “Allow creation of personal logons” GPO setting must be enabled or not configured.
Glossary

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**

The process of verifying your identity, i.e. 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**

Use 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/Proximity/Contactless cards or Bluetooth devices.

**console**

A central location where you can access and manage the features and settings in DigitalPersona Altus Workstation or Kiosk.

**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**

As used in this documentation, a digital extraction of a fingerprint image. Your actual fingerprint image is never stored by DigitalPersona products.
**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 Altus administrator. There are two types of logons, personal logons and managed logons. See separate glossary entries.

**managed computer**

Any computer running a compatible DigitalPersona Altus client, that has been set up to be managed by an Altus Server.

**managed logon**

A logon (see above) created using the Password Manager Admin Tool, 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 Admin Tool (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 DigitalPersona Altus 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 Admin Tool. 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 a user name, password, fingerprint, fingerprint PIN, proximity, contactless or smart cards as specified by the DigitalPersona Altus administrator.

**Password Manager Admin Tool**

An optional management application that enables 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 Admin Tool to create managed logons specifying information for the logon screens, and can use application policy settings in the GPO to deploy the managed logons 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 the Password Manager Admin Tool (managed logons). See also: managed logons.

**restore**

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

**secret**

A DigitalPersona Altus Secret is application specific user data that is stored securely by the DigitalPersona Altus 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.

**smart card**

A hardware device that can be used for authentication.

**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 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 44
adding a change password screen manually 48
adding fields to the Field catalog 55
Allow creation of personal logons 8
Allow users to add account data 9
Allow users to delete account data 9
Allow users to edit account data 9
Allow users to view managed logon passwords 9
Altus client 60
attributes 33
authentication, defined 59

B
back up 59

C
change password screen 44
changing passwords 21
connected device 59
Credentials, defined 59

D
delay 43
deploy managed logons 32, 41, 45, 50, 54

E
enroll 59

F
field catalog 55
finding duplicate logons 57
finding fields in logons 56
finding logons 57
fingerprint 59

L
logging on 21
logon 60
logon field values 34
logon fields 36
logon fields attributes 33
logon fields properties 35

M
managed computer 60
Managed logons 9
managed logons 29, 60
manual mode 14

P
password field values 34
Password Manager 60
Password Manager Admin Tool 60
password policies 46
Path(s) to the managed logons folder(s) 9
personal logon 60, 61
Prevent Password Manager from running 7, 8
properties 35

R
regular expression syntax 51
restore 61

S
Secret 61
setting up a change password screen 44
setting up a change password screen manually 48
setting up a logon screen 29
smart card 61

T
target icon 43
Tools page 57

U
using logon screens 21

V
values 34

W
Windows E-Mail Address 34