

Dell Data Protection Console User Guide

Encryption Status/Authentication Enrollment/Password
Manager v1.12



Legend

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

 **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

 **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

© 2016 Dell Inc. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. Registered trademarks and trademarks used in the Dell Data Protection | Encryption, Dell Data Protection | Endpoint Security Suite, Dell Data Protection | Endpoint Security Suite Enterprise, Dell Data Protection | Security Tools, and Dell Data Protection | Secure Lifecycle suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. McAfee® and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. in the US and other countries. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, and Xeon® are registered trademarks of Intel Corporation in the U.S. and other countries. Adobe®, Acrobat®, and Flash® are registered trademarks of Adobe Systems Incorporated. Authen Tec® and Eikon® are registered trademarks of Authen Tec. AMD® is a registered trademark of Advanced Micro Devices, Inc. Microsoft®, Windows®, and Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server®, and Visual C++® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® is a registered trademark or trademark of VMware, Inc. in the United States or other countries. Box® is a registered trademark of Box. DropboxSM is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube®, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari®, and Siri® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. GO ID®, RSA®, and SecurID® are registered trademarks of Dell EMC. EnCase™ and Guidance Software® are either trademarks or registered trademarks of Guidance Software. Entrust® is a registered trademark of Entrust®, Inc. in the United States and other countries. InstallShield® is a registered trademark of Flexera Software in the United States, China, European Community, Hong Kong, Japan, Taiwan, and United Kingdom. Micron® and RealSSD® are registered trademarks of Micron Technology, Inc. in the United States and other countries. Mozilla® Firefox® is a registered trademark of Mozilla Foundation in the United States and/or other countries. iOS® is a trademark or registered trademark of Cisco Systems, Inc. in the United States and certain other countries and is used under license. Oracle® and Java® are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. SAMSUNG™ is a trademark of SAMSUNG in the United States or other countries. Seagate® is a registered trademark of Seagate Technology LLC in the United States and/or other countries. Travelstar® is a registered trademark of HGST, Inc. in the United States and other countries. UNIX® is a registered trademark of The Open Group. VALIDITY™ is a trademark of Validity Sensors, Inc. in the United States and other countries. VeriSign® and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. KVM on IP® is a registered trademark of Video Products. Yahoo!® is a registered trademark of Yahoo! Inc. This product uses parts of the 7-Zip program. The source code can be found at 7-zip.org. Licensing is under the GNU LGPL license + unRAR restrictions (7-zip.org/license.txt).

Dell Data Protection Console User Guide

2017 - 02

Rev. A01

Contents

1 DDP Console Introduction	5
Contact Dell ProSupport	5
2 DDP Console	6
Navigation	6
3 Encryption Status	9
4 Enrollments	10
Enroll Credentials for the First Time	10
Add, Modify, or View Enrollments	11
Password	12
Recovery Questions	12
Recovery Questions Already Enrolled	12
Fingerprints	13
Mobile Device	14
Enroll the Mobile Device	14
Set up Security Tools Mobile	16
Pair the mobile device and the computer	16
Enroll Another Mobile Device	17
Unpair a Computer and Mobile Device	17
Log On with One-Time Password	17
Security Tools Mobile Management Tasks	18
Reset the Security Tools Mobile App PIN	18
Uninstall Security Tools Mobile App	19
Smart Cards	19
5 Password Manager	20
Get Started with Password Manager	20
Manage Logons	21
Add Category	22
Add Logon	22
Import Credentials	24
Icon Context Menu	25
Log on to Trained Logon Pages	27
Web Domain Support	27
Fill in Windows Credentials	28
Use Old Password	29
Exclude Websites	29
Disable Prompts to Train Logon Forms	30
Back up and Restore Password Manager Credentials	31
Back up Credentials	31
Restore Credentials	31



6 Glossary.....33



DDP Console Introduction

Dell Data Protection | Security Tools provides you with simple-to-use and intuitive tools to increase the security of your computer.

The following features are available through the DDP Console, on a workstation operating system:

- Enroll credentials for use with Security Tools
- Take advantage of multi-factor credentials, including passwords, fingerprints, and smart cards
- Recover access to your computer if you forget your password without help desk calls or administrator assistance
- Back up and restore your program data
- Easily change your Windows password
- Set personal preferences
- View encryption status (on computers with [self-encrypting drives](#))

DDP Console

The DDP Console is the interface through which you can enroll, manage your credentials and configure self-recovery questions.

You can access these applications:

- The Encryption Status tool allows you to view the encryption status of the computer's drives.
- The Enrollments tool allows you to set up and manage credentials, configure self-recovery questions, and view the status of your credential enrollment. Your ability to enroll in each type of credential is set by the administrator.
- Password Manager allows you to automatically fill in and submit data required to log on to websites, Windows applications, and network resources. Password Manager also lets you change your logon passwords through the application, ensuring that passwords maintained by Password Manager are kept in sync with those of the targeted resource.

This guide describes how to use each of these applications.

Be sure to periodically check dell.com/support for updated documentation.

Contact Dell ProSupport

Call 877-459-7304, extension 4310039 for 24x7 phone support for your Dell Data Protection product.

Additionally, online support for Dell Data Protection products is available at dell.com/support. Online support includes drivers, manuals, technical advisories, FAQs, and emerging issues.

Be sure to help us quickly connect you to the right technical expert by having your Service Code available when you call.

For phone numbers outside of the United States, check [Dell ProSupport International Phone Numbers](#).



DDP Console

The DDP Console provides access to applications that ensure security for all users of the computer, to view and manage encryption status of the computer's drives and partitions and, based on policy set by the administrator, manage their logons to websites, programs and network resources; and to easily enroll their authentication credentials.

To open the DDP Console, from the *Desktop*, double-click the **DDP Console** icon.



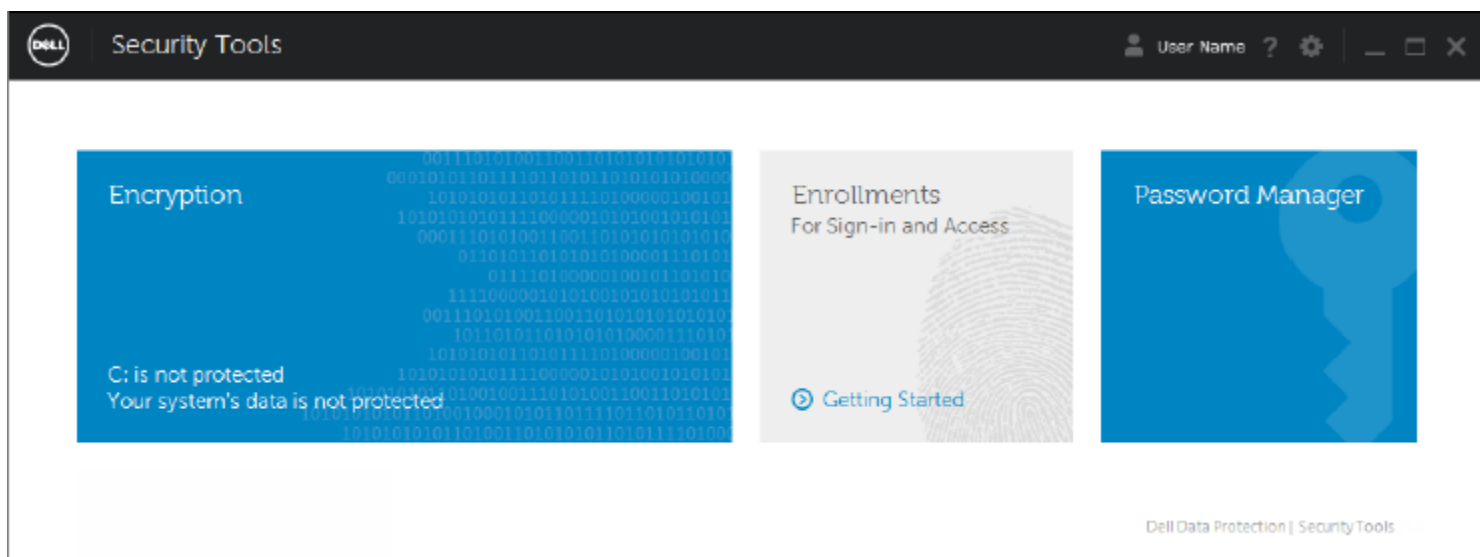
When the DDP Console launches, the home page displays the Security Tools applications:

- [Encryption Status](#)
- [Enrollments](#)
- [Password Manager](#)

To set up credentials for the first time, select the **Getting Started** link on the Enrollments tile. A wizard guides you through the short enrollment process. For more information, see [Enroll Credentials for the First Time](#).

Navigation

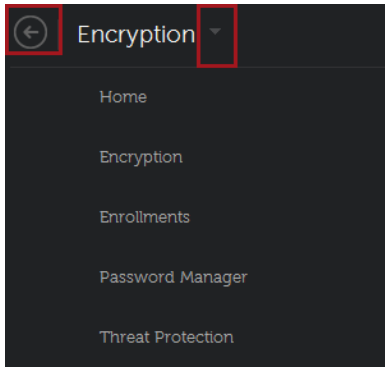
To access an application, click the appropriate tile.



Title bar

To return to the home page from within an application, click the back arrow in the left corner of the title bar, next to the name of the active application.

To navigate directly to another application, click the down arrow next to the active application name, and select an application.



To minimize, maximize, or close the DDP Console, click the appropriate icon in the right corner of the title bar.



To restore the DDP Console after minimizing, double-click its system tray icon.



To open Help, click the ? on the title bar.

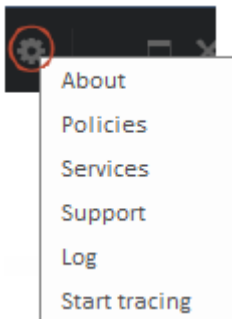


DDP Console Details

To view details about the DDP Console, policies, running services, and logs, click the gear icon on the left side of the title bar. This information might be necessary for an administrator to provide technical support.



Select an item from the menu.



Menu Item	Purpose
About	Contains version and copyright information.
Show Info	Contains the following: <ul style="list-style-type: none">product version and date informationwhether the DDP Console is managed on this computer by the enterprise or by a local administrator



- version numbers of the operating system, BIOS, motherboard, and [Trusted Platform Module \(TPM\)](#).

MS Info	Runs the Microsoft Windows System Information utility to display detailed information about the hardware, components, and software environment.
Copy Info	Copies all of the system information to the clipboard, to paste into an email for your administrator or Dell ProSupport.
Feedback	Displays a form where you can provide feedback to Dell about this product. (On non-domain computers, this option is always available. On domain computers, this option is determined by enterprise policy.)
Policies	Displays a hierarchy of policies that apply to this computer.
Services	Displays details about the services that are running.
Support	Connects to the Dell ProSupport website.
Log	Displays a detailed list of logged events, for troubleshooting.
Start Tracing	Lets you start and stop a recording of sign-in activities, for troubleshooting.



Encryption Status

The Encryption page displays the encryption status of the computer. If a disk, drive, or partition is not encrypted, its status reads *Unprotected*. A drive or partition that is encrypted shows the status *Protected*.

To update encryption status, right-click the appropriate disk, drive, or partition, and select **Refresh**.

The screenshot shows the 'Encryption Status' dashboard. At the top, there is a navigation bar with a back arrow, the title 'Encryption', a user profile icon labeled 'User', and icons for help, settings, and window management. Below the navigation bar, the title 'Encryption Status' is displayed in blue, followed by a subtitle: 'The encryption dashboard allows you to view the protection status of the computer.' The main content area features a table with three columns representing different storage components. Each component is listed with its name, size, and encryption status. All three components shown are 'Unprotected'. At the bottom right of the dashboard, the text 'Dell Data Protection | SecurityTools' is visible.

Component	Size	Status
Drive 0	298.09 GB	Unprotected
Partition 3	296.71 GB	Unprotected
Disk C: *OS*	296.71 GB total, 242.81 GB free (81% available)	Unprotected

Enrollments

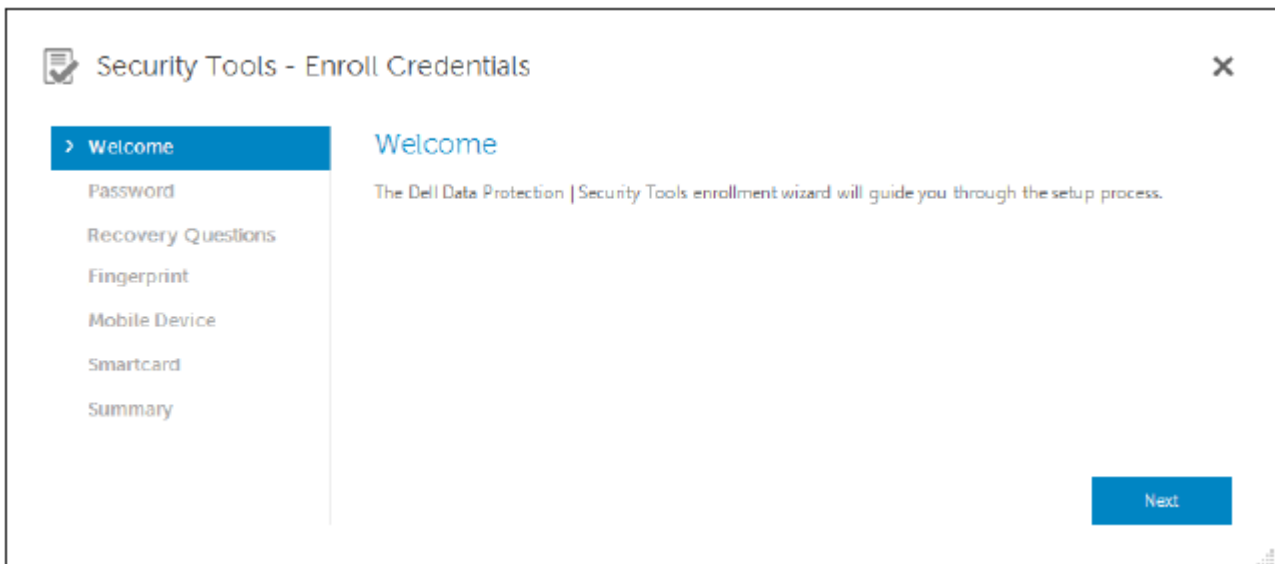
The Enrollments tool lets you enroll, modify, and check enrollment status, based on policy set by the administrator.

The first time you enroll your credentials with the DDP Console, a wizard guides you through enrolling a password change, Recovery Questions, fingerprints, mobile device and smart card. Depending on policy, you can either enroll or skip each credential. After initial enrollment, you can click the Enrollment tile to add or modify credentials.

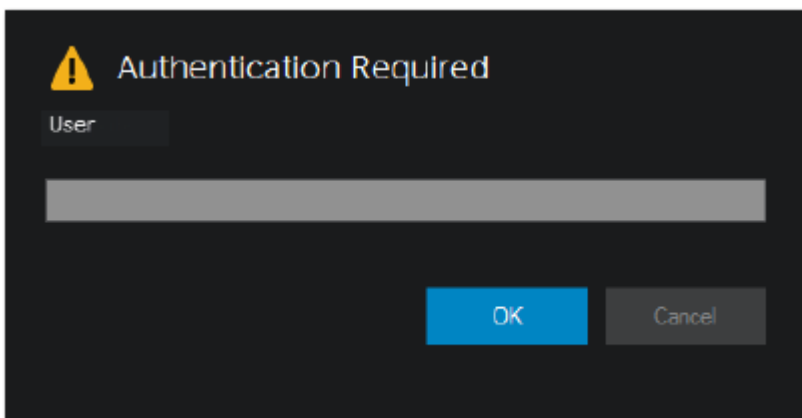
Enroll Credentials for the First Time

To enroll credentials for the first time:

- 1 On the DDP Console home page, click the **Getting Started** link on the Enrollments tile.
- 2 On the Welcome page, click **Next**.



- 3 In the Authentication Required dialog, log in with your Windows password, and click **OK**.



- 4 On the Password page, to change your Windows password, enter and confirm a new password and click **Next**.
To skip changing your password, click **Skip**. The wizard allows you to skip a credential if you don't want to enroll it. To return to a page, click **Back**.
- 5 Follow the instructions on each page, and click the appropriate button: **Next**, **Skip**, or **Back**.
- 6 On the Summary page, confirm the enrolled credentials and, when finished with enrollment, click **Apply**.
To return to a credential enrollment page to make a change, click **Back** until you reach the page you want to change.

For more detailed information about enrolling a credential, or to change a credential, see [Add, Modify, or View Enrollments](#).

Add, Modify, or View Enrollments

To add, modify, or view enrollments, click the **Enrollments** tile.

Tabs in the left pane list available Enrollments. This varies based on your platform or type of hardware.

The Status page displays supported credentials, their policy setting (Required or N/A), and their enrollment status. From this page, users can manage their enrollments, based on policy set by the administrator:

- To enroll a credential for the first time, on the line with the credential, click **Enroll**.
- To delete an existing enrolled credential, click **Delete**.
- If policy does not allow you to either enroll or modify your own credentials, the **Enroll** and **Delete** links on the Status page are inactive.
- To change an existing enrollment, click the appropriate tab in the left pane.

If policy does not allow enrollment or modification of a credential, a message displays on the credential's enrollment page, "Credentials modification is not allowed by policy."

The screenshot shows the 'Enrollments' console interface. On the left, there is a navigation pane with tabs for 'Status', 'Password', 'Fingerprints', 'Recovery Questions', 'Mobile Device', and 'Smartcard'. The 'Status' tab is selected, displaying a table of credentials and their enrollment status.

Credential	Policy	Enrollment Status	
Password	Optional	✓ Enrolled	
Fingerprints	Optional	✓ Not Enrolled	Enroll
Recovery Questions	Optional	✓ Not Enrolled	Enroll
Smartcard	Optional	✓ Not Enrolled	Enroll
Mobile Device	Optional	✓ Not Enrolled	Enroll

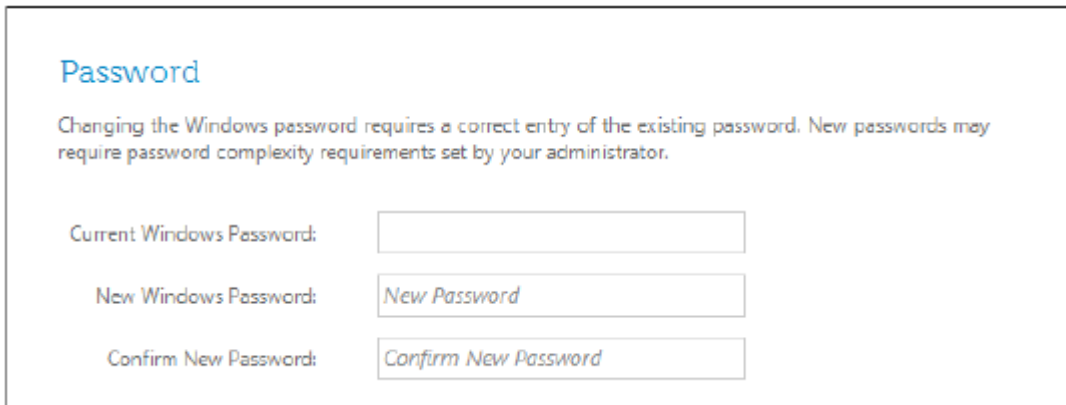
Below the table, the text 'Dell Data Protection | SecurityTools' is visible.



Password

To change your Windows password:

- 1 Click the **Password** tab.
- 2 Enter the current Windows password.
- 3 Enter the new password and enter it again to confirm it, and click **Change**.
Password changes are effective immediately.



The screenshot shows a dialog box titled "Password". Below the title is a message: "Changing the Windows password requires a correct entry of the existing password. New passwords may require password complexity requirements set by your administrator." There are three input fields: "Current Windows Password:" with an empty text box, "New Windows Password:" with a text box containing "New Password", and "Confirm New Password:" with a text box containing "Confirm New Password".

- 4 At the Successful Enrollment dialog, click **OK**.

NOTE:

You should only change your Windows password in the DDP Console rather than in Windows. If the Windows password is changed outside of the DDP Console, a password mismatch will occur, requiring a recovery operation.

Recovery Questions

The Recovery Questions page allows you to create, delete, or change your recovery questions and answers. Recovery Questions provide a question and answer-based method for you to access your Windows accounts if, for example, the password is expired or forgotten.

NOTE:

Recovery questions are used to recover access to a computer only. The questions and answers cannot be used to log on.

If you have no previous Recovery Questions enrolled:

- 1 Click the **Recovery Questions** tab.
- 2 Select from a list of pre-defined questions and then enter and confirm the answers.
- 3 Click **Enroll**.

NOTE:

Click the **Reset** button to clear the selections on this page and start over.

Recovery Questions Already Enrolled

If recovery questions have already been enrolled, you can either delete or re-enroll your recovery questions.

- 1 Click the **Recovery Questions** tab.
- 2 Click the appropriate button:

- To remove the recovery questions completely, click **Delete**.
- To re-define the recovery questions and answers, click **Re-enroll**.

Recovery Questions

Recovery questions allow you to regain access if you are unable to sign in using one of your enrolled credentials. You must set up three questions.

✓

✓

✓

Fingerprints

① NOTE:

To use this feature, your computer must have a fingerprint reader.

To enroll fingerprints, follow these instructions:

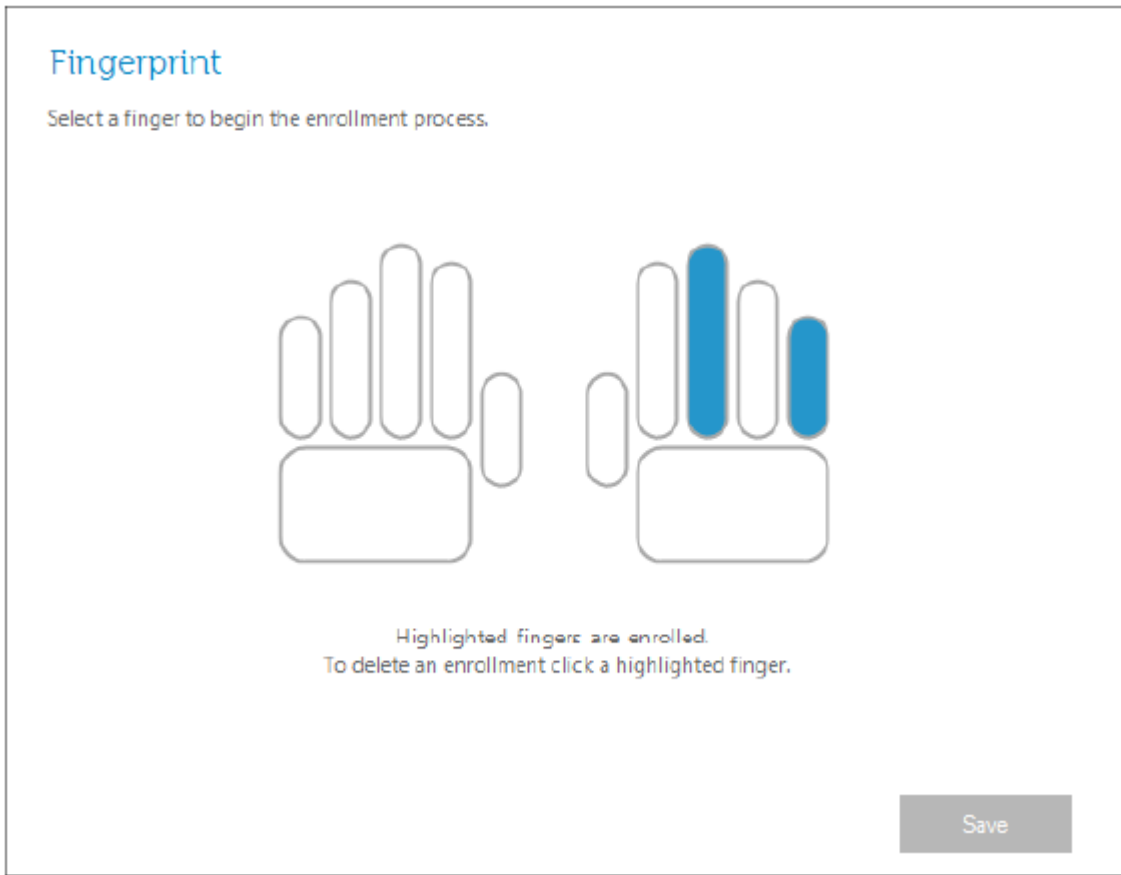
- 1 Click the **Fingerprints** tab.
- 2 On the Fingerprint page, click the finger you want to enroll.
- 3 Follow the on-screen instructions to enroll your fingerprint.

① NOTE:

The finger must be successfully scanned four times to be enrolled. The number of scans needed to complete fingerprint enrollment depends on the quality of each scan. The administrator defined the minimum and maximum number of fingerprints.

- 4 Click each subsequent finger to scan until you have enrolled the minimum number of fingerprints required by policy. A dialog will inform you if you have not enrolled the minimum number of fingerprints. Click **OK** to continue.
- 5 Complete the scanning of the required number of fingerprints, and click **Save**.
To delete a scanned fingerprint, on the Fingerprint enrollment page, click a highlighted fingerprint to unenroll it, click **Yes** to confirm deletion, then click **Save**.





Mobile Device

Mobile Device enrollment provides the [One-time Password \(OTP\)](#) feature. With OTP, the user can log on to Windows using a password generated by the Security Tools Mobile app, on a mobile device that is paired with the computer. Alternatively, if allowed by policy, the OTP feature can be used to recover access to the computer in case a password is expired or forgotten.

NOTE:

If the Mobile Device tab does not display in your DDP Console, your computer's configuration does not support it, or policy set by your administrator does not allow it.

NOTE:

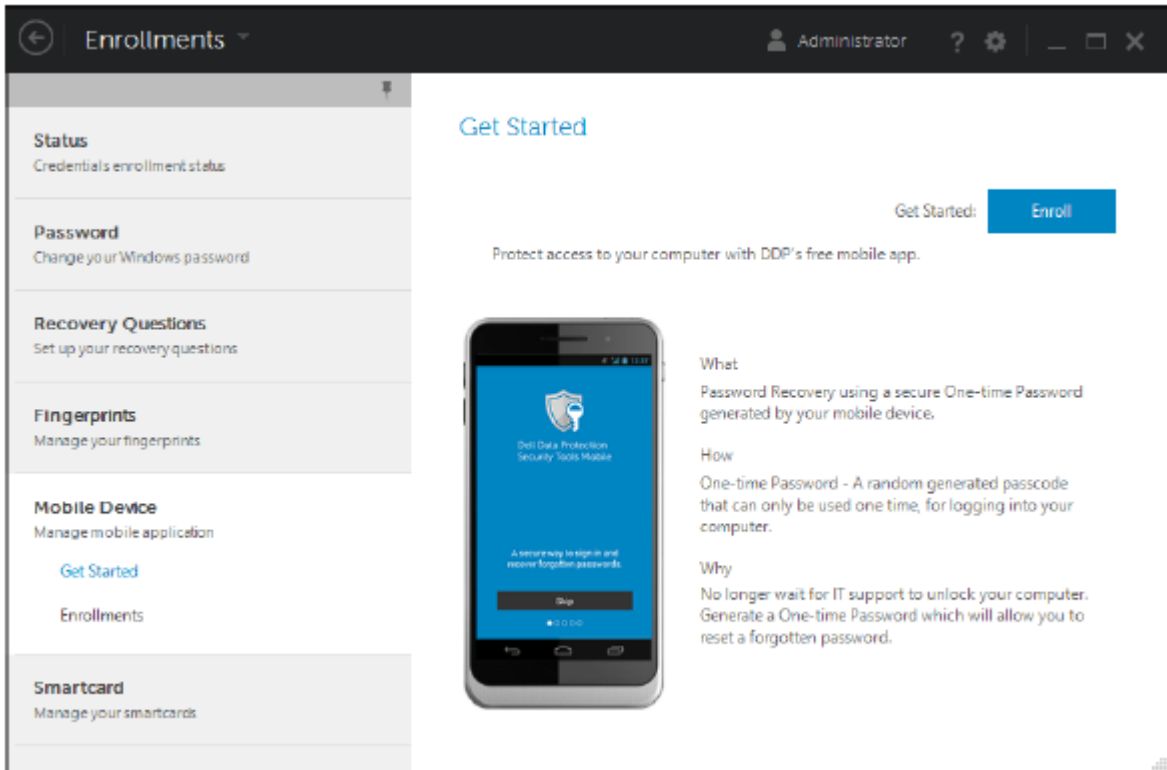
Policy settings determine how the OTP feature can be used - either to log on or to recover access to your computer if your password is expired or forgotten. It cannot be used for both log on and recovery.

To use the OTP feature, you must enroll, or pair, your mobile device with your computer. On a computer with multiple users, each user can enroll one mobile device with the computer. Mobile devices can be enrolled with multiple computers.

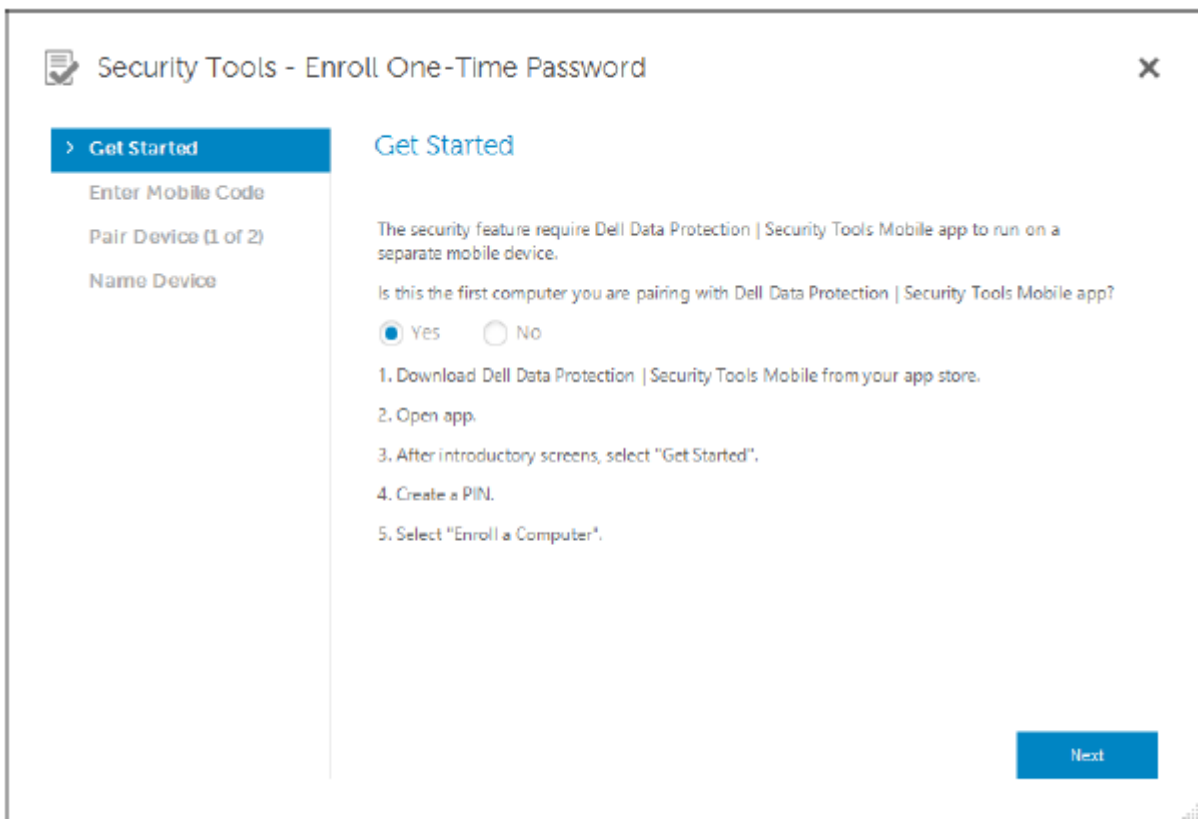
When a device is already enrolled, enrolling a new device automatically unpairs the previous device.

Enroll the Mobile Device

- 1 In the DDP Console Enrollments page, click the **Mobile Device** tab.



- 2 In the upper right, click **Enroll**.
The Enroll One-time Password page opens.
- 3 If this is the first computer to pair, select **Yes**.



- a On the mobile device, download the Dell Data Protection | Security Tools Mobile app from your app store.
- b On the computer, click **Next**.

Set up Security Tools Mobile

- 1 Open the Security Tools Mobile app.
- 2 Create and enter a PIN to access the Security Tools Mobile app.

 **NOTE:**

The PIN may be required by policy when the mobile device is not locked. If you do not use a PIN to unlock the mobile device, you will need one to access the Security Tools Mobile app.

- 3 Select **Enroll a Computer**. (If necessary, tap the upper-left corner of your mobile screen to access the commands.) A code displays on the mobile device. The length of the code and the alphanumeric combination are based on policy set by the administrator.

Pair the mobile device and the computer

- 1 On the computer, in the DDP Console Mobile Code page:
 - a Enter the code from the mobile device into the field.
 - b Click **Next**.
 - c On the Pair Device page, select one:
 - QR Code** - A QR Code displays.or
 - Manual Entry** - A 24-digit pairing code displays.
- 2 On the mobile device:
 - a Tap **Pair Devices**.
 - b Select the same pairing option (**Scan QR Code** or **Manual Entry**) that you selected on the computer.
 - c Select one:
 - For **QR Code**, place the mobile device in front of the computer screen to scan the QR Code. Note the numeric verification code that displays on the mobile device, then tap **Next**.

 **NOTE:**

If the *Trouble Scanning?* bar displays, try again, or select **Manual Entry**.

- For **Manual Entry**, enter the 24-digit pairing code from the computer, then tap **Done**. Note the numeric verification code that displays on the mobile device, then tap **Next**.
- 3 On the computer, in the DDP Console:
 - a Click **Next**.
 - b Enter the verification code displayed on the mobile device and click **Next**.
 - c Optionally, modify the name for the mobile device.
 - d Click **Apply**.
the devices are paired.
- 4 On the mobile device:
 - a Tap **Continue**.
 - b Optionally, modify the name for the computer and tap **Done**.
 - c Tap **Finish**.

Enroll Another Mobile Device

Enrolling a new device automatically unpairs the previous device. No separate steps are required to unpair.

Unpair a Computer and Mobile Device

To unpair a computer and mobile device without enrolling another device, select one:


- In the DDP Console: On the Enrollments Status page, next to the Mobile Device credential, click **Delete**.
 - On the mobile device - see the steps below.
- 1 On the mobile device, complete the following:
 - a Run the Security Tools Mobile app.
 - b In the upper left, tap the menu bars to open the drawer.
 - c Tap **Remove Computers**.
 - d Select the computer to unpair.
 - e Select **Remove** (Android) or tap **Done** (iOS).
A confirmation message appears.
 - f Select **Remove All** to remove all enrolled computers from your device.
The Remove All option appears when you are removing multiple computers and when removing the only computer that was paired.
 - Select **Restore Default Settings** to remove the enrolled computer and remove the PIN. If you restore defaults, it will remove all enrolled computers and the PIN that you use to access the Security Tools Mobile app.
 - Select **Cancel** to leave the computer enrolled.

Log On with One-Time Password

NOTE:

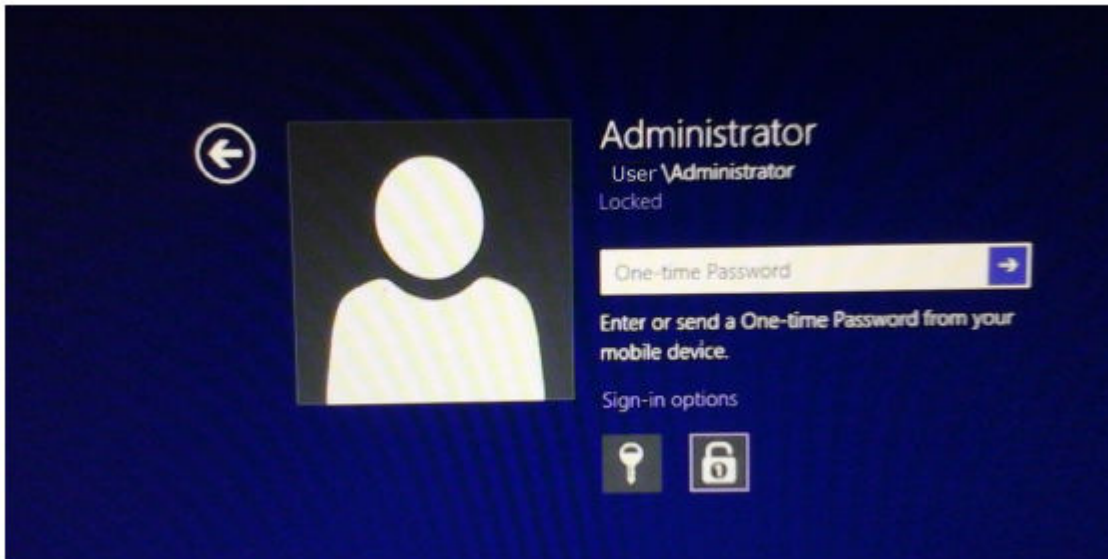
OTP authentication can only be used with Windows logons.

OTP can be used either for recovery, to regain access to a computer from which you have been locked out, or for Windows logon. It cannot be used for both.

If allowed by policy, and the OTP symbol  displays on your logon screen, you can log on to Windows with OTP.

To log on with OTP:

- 1 On the computer, at the Windows logon screen, select the OTP icon .



2 On the mobile device, open the Security Tools Mobile app and enter the PIN.

3 Select the computer you want to access.


If the computer name does not display on the mobile device, one of these conditions may exist:

- The mobile device is not enrolled, or paired, with the computer you are trying to access.
- If you have more than one Windows user account, either Security Tools is not installed on the computer that you are trying to access or you are attempting to log on to a different user account than was used to pair the computer and the mobile device.

4 Tap **One-time Password**.

A password displays on the mobile device screen.

NOTE:

If necessary, click the Refresh symbol  to get a new code. After the first two OTP refreshes, there will be a thirty-second delay before another OTP can be generated.

The computer and mobile device must be in sync so that they both can recognize the same password at the same time. Trying to rapidly generate password after password will cause the computer and mobile device get out of sync and the OTP feature to fail. If this problem should occur, wait for thirty seconds for the two devices to get back in sync, and then try again.

5 On the computer, at the Windows logon screen, type the password displayed on the mobile device and press **Enter**.

If you have used OTP for recovery, after you gain access to the computer, follow the on-screen instructions to reset your password.

Security Tools Mobile Management Tasks

These tasks are performed using the Security Tools Mobile app on the mobile device.

Reset the Security Tools Mobile App PIN

To reset the Security Tools Mobile app PIN:

- 1 In the upper right, tap the menu options.
- 2 Select **Reset Pin**.
- 3 Enter and confirm the new PIN.

Uninstall Security Tools Mobile App

On your mobile device:

- 1 Unpair the device and the computer.
- 2 Delete or uninstall the Security Tools Mobile app as you normally would delete an app from your mobile device.

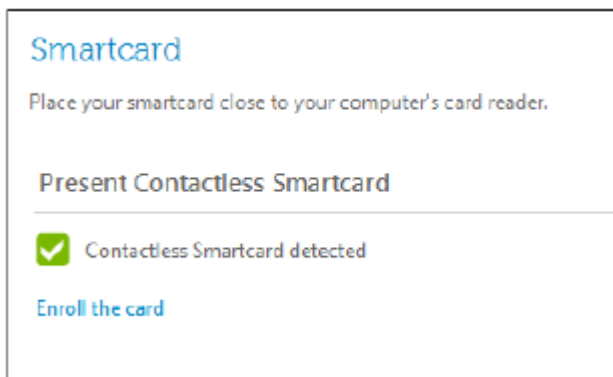
Smart Cards

NOTE:

To use this feature, your computer must have a smart card reader.

To enroll smart cards, follow these instructions:

- 1 Click the **Smartcard** tab.
- 2 Enroll the smart card, based on type of card:
 - Insert the smart card into the card reader.
 - With a contactless card, place and hold the card on or near the reader.
- 3 When the card is detected, a green check box and *Enroll the card* display. Select **Enroll the card**.



- 4 At the Successful Enrollment dialog, click **OK**.

To unenroll all smart cards associated with the user, on the Smartcard enrollment page, select **Remove enrolled cards from your account**.



Password Manager

Password Manager allows you to automatically log on to websites, Windows programs, and network resources and manage logon credentials in a single tool. Password Manager also allows users to change their logon passwords through the application, ensuring that passwords maintained by Password Manager are kept in sync with those of the targeted resource.

Password Manager is supported with Internet Explorer and Mozilla Firefox. Password Manager is not supported with Microsoft accounts (previously Windows Live ID).

NOTE:

If running Password Manager on Firefox, you must install and register the Password Manager extension. For instructions on installing extensions in Mozilla Firefox, see <https://support.mozilla.org/>.

NOTE:

Use of Password Manager icons (both pre-trained and trained icons) in Mozilla Firefox differs from their use in Microsoft Internet Explorer:

- Double-click functionality on Password Manager icons is not available.
- The default action is not shown in bold in the drop-down context menu.
- If a page has multiple logon forms, you may see more than one Password Manager icon.

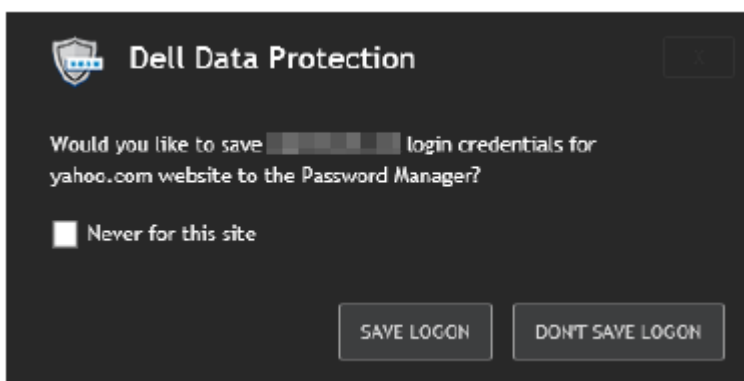
NOTE:

Due to the ever-changing structure of web logon pages, Password Manager may not be able to support all websites at all times.

Get Started with Password Manager

Password Manager collects and stores your logon credentials as you work. You can begin to use Password Manager immediately after Security Tools is installed. When you enter credentials into a logon page, Password Manager detects the

logon form and lets you choose whether you want Password Manager to save your credentials.



You have three options:

- Click **Save Logon** to store your logon credentials in Password Manager.

- If you **do not** want to save your logon, each time you log on to the website or program, you will be prompted to save the logon credentials again. If you prefer not to be prompted, select **Never for this site**. A record will be created in the Website Exclusions list. See [Exclude Websites](#) for details.
- If you do not want to save the credentials, click **Don't Save Logon**.

This dialog also displays when you have previously saved credentials for a website or program, but you enter a different user name or password. With a new user name, if you select **Save Logon**, a new set of credentials is stored. With the previously saved user name and new password, if you select **Save Logon**, your original credentials are updated with the new password.


Manage Logons


Logon Manager simplifies and centralizes management of all of your logons to websites, Windows programs, and network resources.

To open Logon Manager:

- 1 On the DDP Console home page, click the **Password Manager** tile.
- 2 Click the **Logon Manager** tab.

You can add logons and categories and sort and filter them:


 **Add Logon** - Allows you to add a new set of logon credentials. Based on policy, you may be required to enter credentials stored in Security Tools in order to add a logon.

 **Add Category** - Allows you to add a new category (such as Email, Storage, News, Corporate Resources, Social Media), for use in sorting and filtering.


Sort: Sort the logons by Account, Username, or Category. Click a column heading to sort by its column.


Filter: Select a category from the *View* list to hide all logons except for those in the selected category. To remove the filter, select *All*.

You can manage logons:

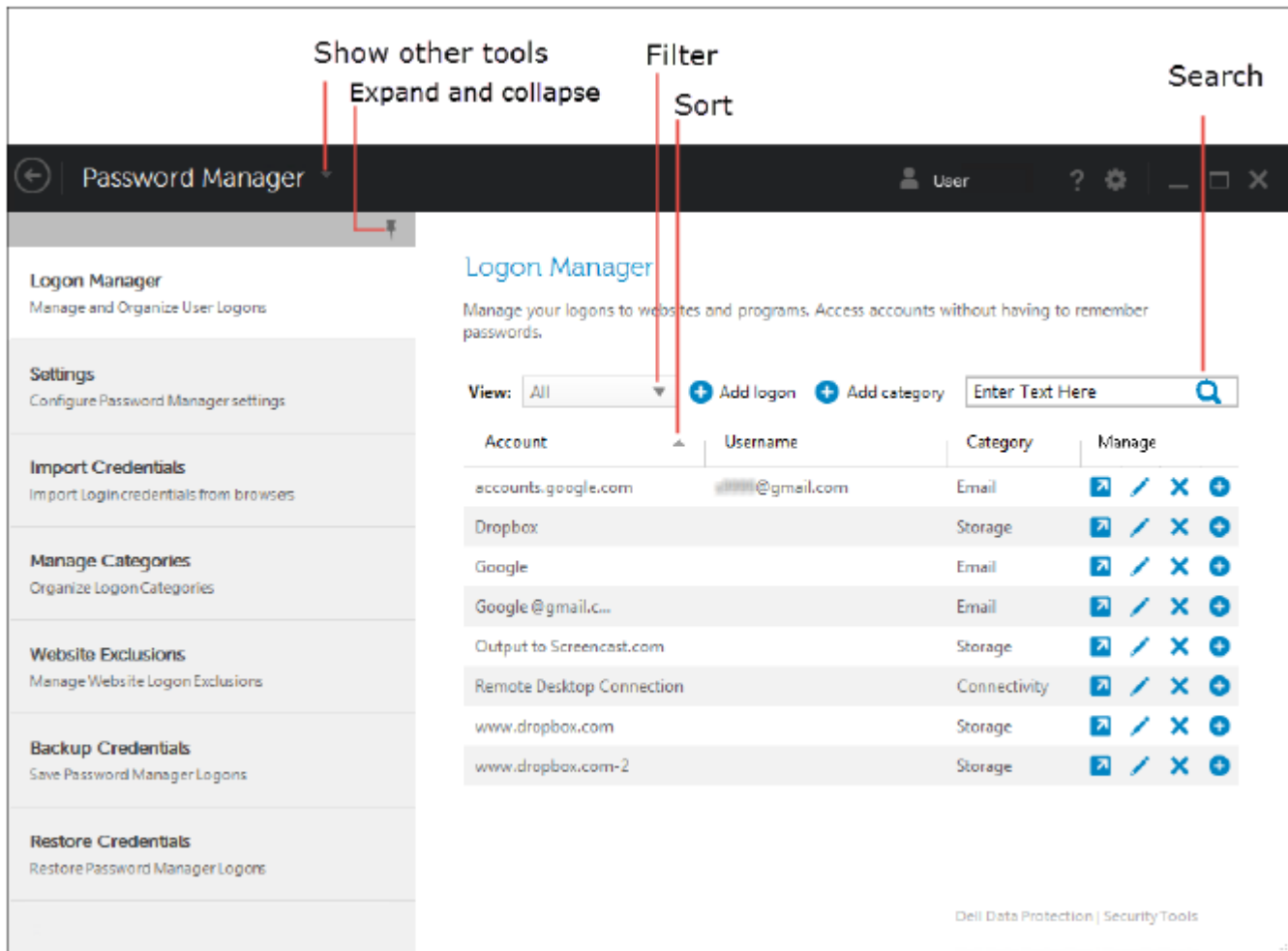
 **Launch** - Opens the website or program and submits logon credentials, based on user settings.

 **Edit** - Allows you to change the stored logon data of a website or program.

 **Delete** - Allows you to remove stored logon data from the Password Manager.

 **Add** - Allows you to add a new logon, category, or new logon data.





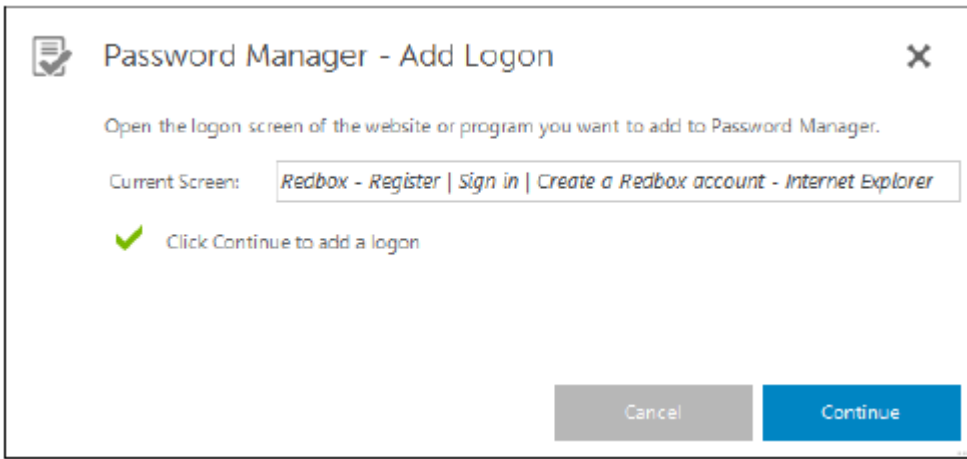
Add Category

Before adding logons, create categories (such as Email, Storage, News, Corporate Resources, and Social Media) so that you can categorize your logons as you create them. Then you can sort and filter your logons by category.

To add a category, on the Logon Manager page, click **Add category**, type a category name, and click **Save**.

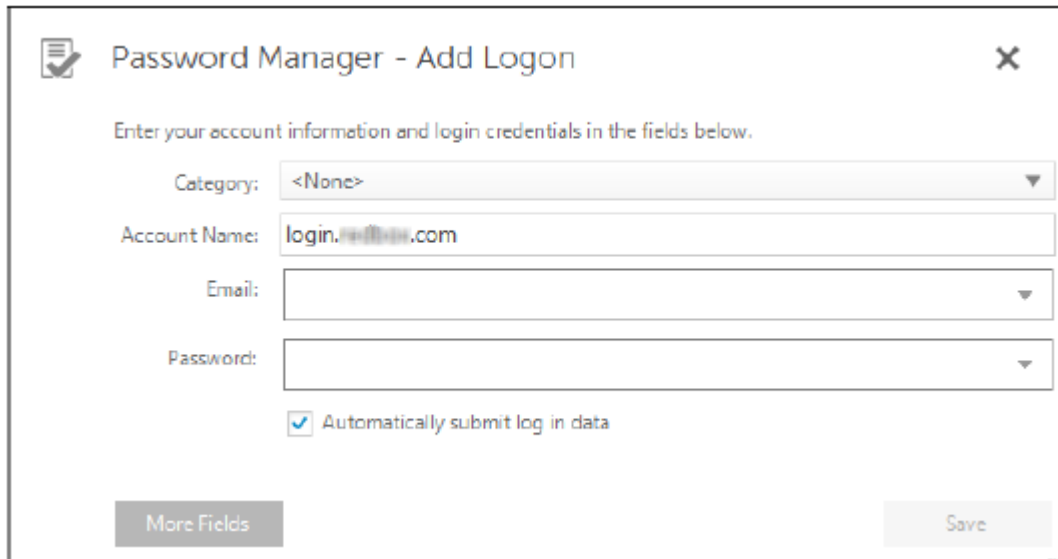
Add Logon

- 1 On the Logon Manager page, click **Add Logon**.
Based on policy, you may be required to authenticate to add a logon.
- 2 Open the website or program to log on to.
- 3 In the Add Logon dialog, click **Continue**.



4 In the next dialog, enter the following:

- **Category** - Choose a category for the website or program logon that you are storing. If you have not added categories, this list will be empty.
- **Account Name** - Leave as-is to accept the pre-filled name, or type the name of the website or program.
- **Undetected Title** - These fields are detected by Password Manager as the fields on the logon page in which you enter your logon information. These fields typically include User Name or Email, and Password.



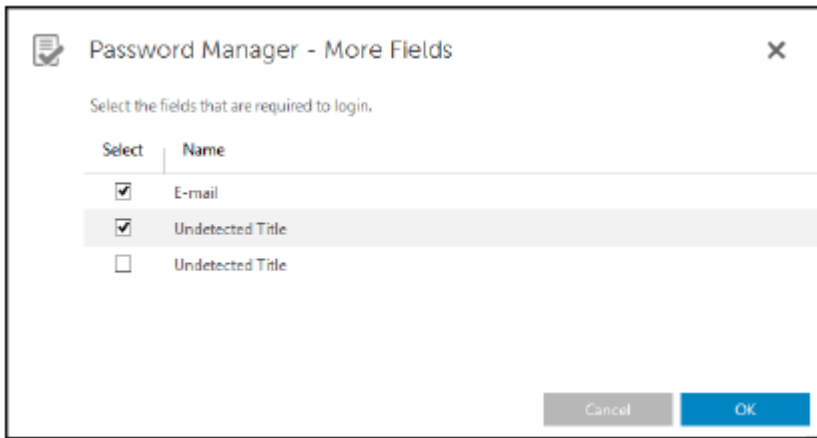
5 If a field name is shown as Undetected Title, or if the wrong fields have been included as logon fields, click the **More Fields** button to edit field names or remove fields.

6 In the More Fields dialog, click **Undetected Title** and enter the correct field name for each field.

When the More Fields dialog displays, the field that was active on the Add Logon dialog is highlighted, to assist you in renaming the fields.

If a field is unnecessary for logon, to exclude it from logon information, clear its check box.

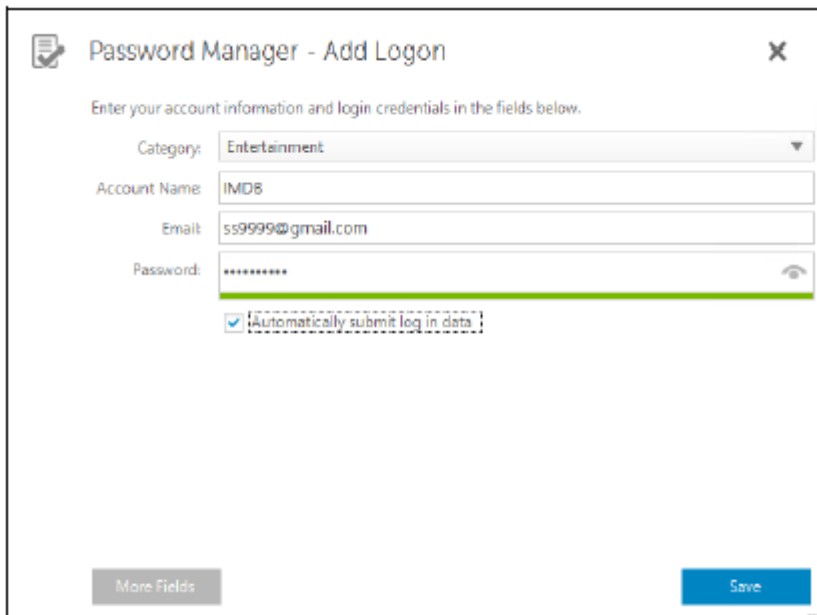




- 7 To save changes, click **OK**.
- 8 In the Add Logon dialog, complete the fields required for logon.

NOTE:

Because you are storing an existing logon, you can only change the password by going to the Change Password function of the website or program.



- 9 If you want Password Manager to automatically fill in and submit the logon information, select **Automatically submit log in data**.
- 10 Click **Save**.

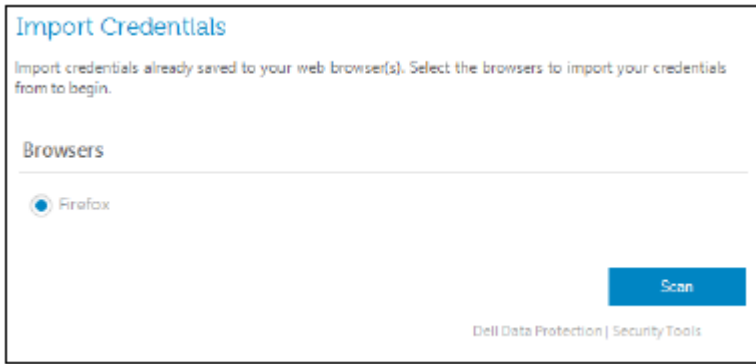
The website or program logon displays on the Logon Manager page.

Import Credentials

You can import credentials stored in web browsers into the Password Manager.

- 1 In the Password Manager tool, select **Import Credentials**.
- 2 Select the browser to import and click **Scan**.

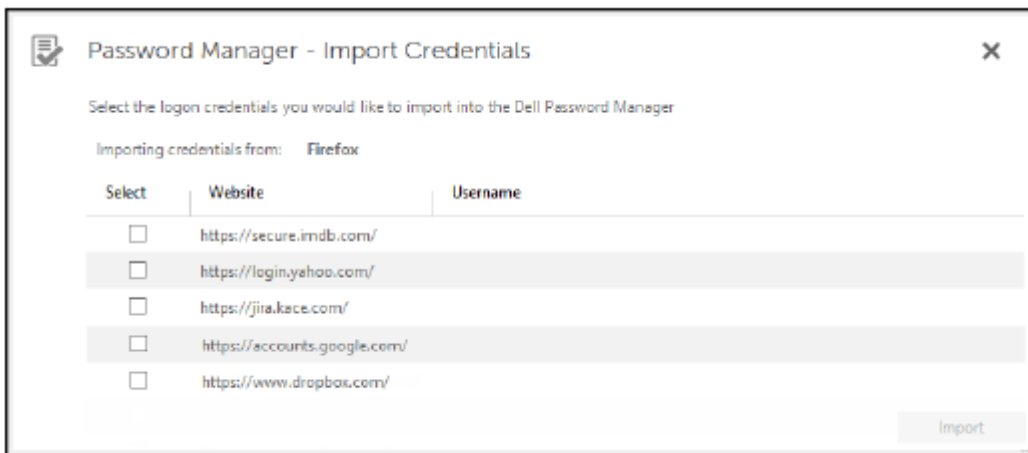




3 When prompted, enter the password for the selected browser.

NOTE:


If the import does not result in imported passwords, check to determine whether the browser has stored data to import. If you are using Firefox, log on to Sync. Try importing your credentials again.



Icon Context Menu

When you visit a website or program, the Password Manager icon displays.

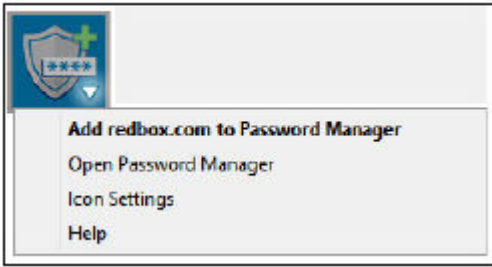
The  indicates that the logon form can be trained.

When the  is not present, the logon form has already been trained. Double-click the icon to log on to the program or website.

When you click the icon a context menu displays different options, based on whether the logon form is trained or untrained.

When the current logon fields are not yet trained, the context menu displays the following options:





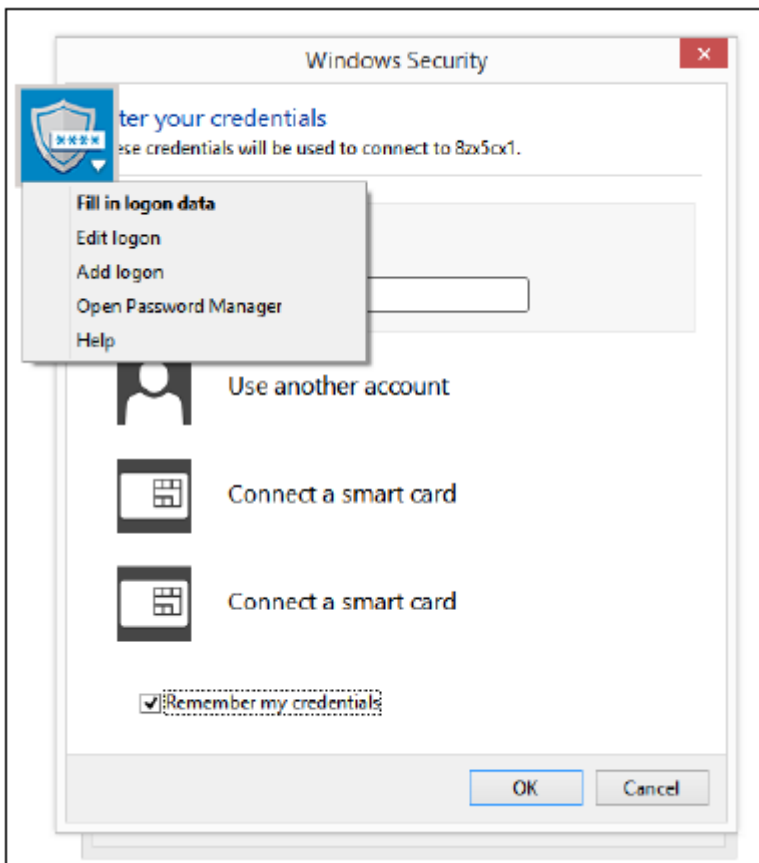
Add to Password Manager - Opens the Add Logon dialog.

Icon Settings - Allows the user to configure the display of the Password Manager icon on trainable logon pages.

Open Password Manager - Launches the *Password Manager Administration* tool and opens the Logon Manager page.

Help - Opens the online help.

When the current logon fields are trained, the context menu displays the following options:



Fill in logon data - Depending on your selections when you trained the logon form, it either automatically logs on or fills the user name and password fields allowing you to submit the logon data.

Edit logon - Opens the Edit logon dialog.

Add logon - Opens the Add logon dialog.

Open Password Manager - Opens the Logon Manager page.

Help - Opens the online help.

If Password Manager icons do not appear with logon forms, turn off your browser's password-saving feature:

- In Mozilla Firefox: Menu icon > Options > Security > clear the **Remember passwords for sites** check box
- In Internet Explorer: Gear icon > Internet Options > Content tab > Autocomplete Settings > clear the **User names and passwords on forms** check box

Log on to Trained Logon Pages

When you open a website or program logon, Password Manager detects whether the page is trained. If trained, the Password Manager icon displays in the logon area. If untrained, the Password Manager icon displays-unless prompts for untrained forms have been disabled.

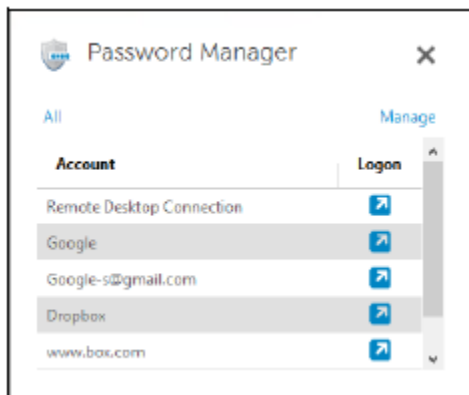
To log on, select one:

- Scan enrolled credentials. If you have enrolled a fingerprint or smart card, you can touch the fingerprint reader with an enrolled fingerprint or present an enrolled card to the card reader.
- Click the Password Manager icon and select **Fill in logon data** from the context menu.
- Press the Password Manager hot key combination: **Ctrl+Win+H**. Password Manager pop-up presents your trained sites in a pop-up, allowing you to launch one quickly.

NOTE:

You can change the hot key combination in the DDP Console > Password Manager > Settings.

If more than one logon for the site or program has been stored, you are prompted to choose the account to use.

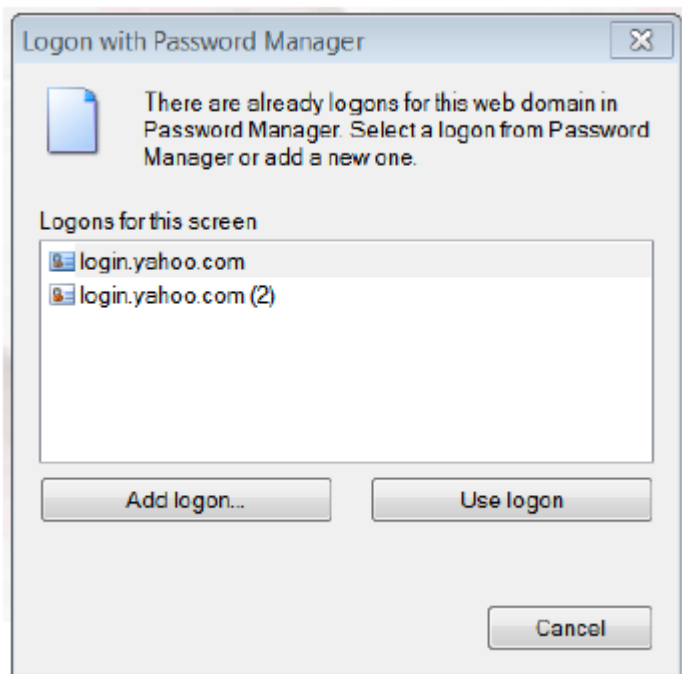


Web Domain Support

If you have trained a logon page for a specific web domain but want to access the account on that web domain from a different logon page, navigate to the new logon page. You are prompted to use an existing logon or to add a new one to Password Manager.

- If you click *Use logon*, you are logged on to the previously created account. The next time you access that account from the new logon page, you are automatically logged on to the previously created account.
- If you click *Add logon*, the Add Logon dialog displays.





Fill in Windows Credentials

Some programs allow the use of Windows credentials for logon.

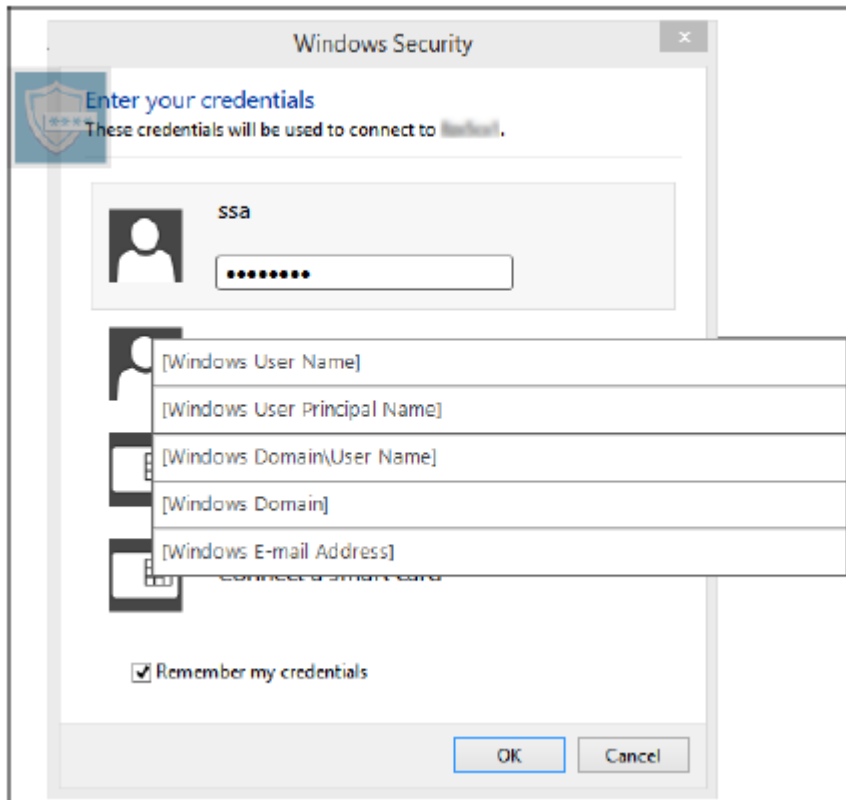
Instead of typing your user name and password, choose the Windows credentials from the drop-down menus available in the *Add Logon* and *Edit Logon* dialogs.

For the username, choose between the following types:

- Windows User Name
- Windows User Principal Name
- Windows Domain\User Name
- Windows Domain

For the password, use your Windows password.

These options cannot be modified.



Use Old Password

It is possible to have changed a password in Password Manager and then the program rejects the new password. In this case, the program allows you to use a previous password (a password previously entered for this logon page) instead of the most recent one.



Select **Password History**. After authentication, you are prompted to choose an old password from the Password History list. The list includes seven passwords.

Exclude Websites

To prevent websites from being managed by the Password Manager, click the **Website Exclusions** tab.

Excluded websites have these characteristics:

- Do not invoke a Password Manager icon.
- Do not automatically log in users.
- Do not display password reminders.

To add a new website to the exclusions list:

- 1 Click the **Website Exclusions** tab.
- 2 Click **Add Website**.

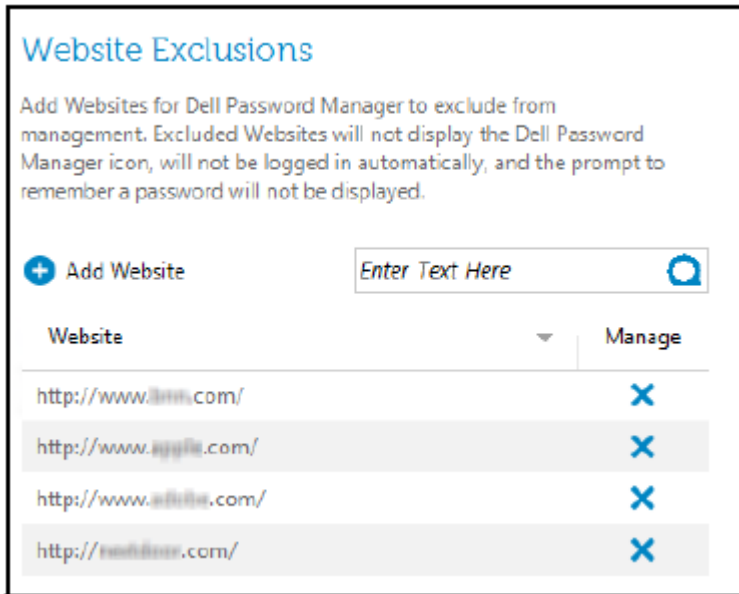


- 3 Enter the URL of the website to exclude.
- 4 Click **Save**.

Once you have excluded a website, the website is not managed by Password Manager. Simply delete the website from the Website Exclusions list to reverse the exclusion. To remove a website from the exclusions list: click X.

After adding several websites, you can:

- To sort the list by website, ascending or descending, click the Website column heading.
- To search within the list, enter part of the URL into the search field. The list is filtered as you type.

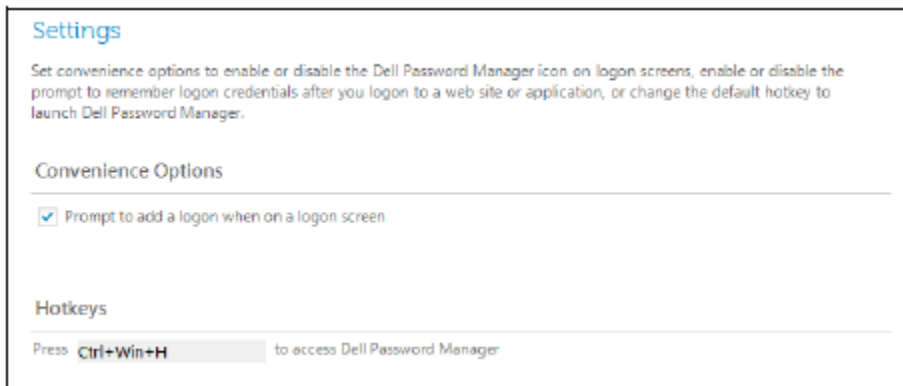


Disable Prompts to Train Logon Forms

You can keep existing trained logons but disable prompts to train new logon forms.

To disable prompts for new logons:

- 1 Open the DDP Console.
- 2 Click the **Password Manager** tile.
- 3 Click the **Settings** tab.
- 4 Clear the **Prompt to add a logon when on a logon screen** check box.



Back up and Restore Password Manager Credentials

The Password Manager lets you securely back up the logon data that is managed by Password Manager. This data can be restored on any computer protected by Password Manager.

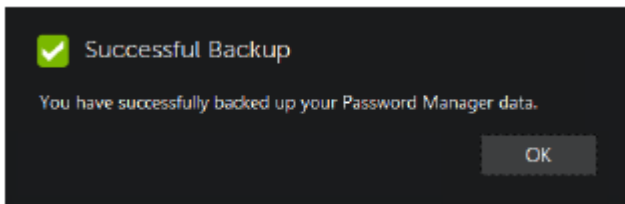
NOTE:

The Password Manager data that is backed up does not include operating system or Preboot Authentication (PBA) logon credentials or credential-specific information, such as fingerprints.

Back up Credentials

To back up credentials:

- 1 Click the **Backup Credentials** tab to set up the backup process.
- 2 Click **Browse** and navigate to the desired backup location.
If you attempt to back up the data to a local drive, a recommendation displays to back up the data to portable storage or a network drive.
- 3 Enter and confirm a password. This password must be used if these backed up credentials must be later restored.
- 4 Click **Backup**.
- 5 Enter your Windows password.
- 6 In the Success dialog, click **OK**.



NOTE:

To view a text log of the backup operation performed, click the  and select **Log**.

Restore Credentials

The backup location must be available, in order to restore credentials.

To restore credentials:

- 1 Click the **Restore Credentials** tab.
- 2 Click **Browse** to navigate to the backup file, and then enter the password for the file.
- 3 Click **Restore**.

WARNING:

Restoring Password Manager data will overwrite any existing data. Logons and other data added after the backup was created will be lost.



Restore Credentials

Type the location and name of the backup file, or click the Browse button.

The backup file is password protected. You must type the same password you used when you backed up the data.

Backup File	<input type="text" value="Select backup file"/>	<input type="button" value="Browse"/>
Password	<input type="text" value="Password"/>	

Warning: If previous Password Manager data exists, it will be overwritten by the data being restored. Data not part of the backup is not merged and will be lost.

4 Click **Next**.

NOTE:

To view a text log of the restore operation, click the  icon in the title bar and select **Log**.

Glossary

Credential - A credential is something that proves a person's identity, such as their fingerprint or their Windows password.

One-Time Password (OTP) - A one-time password is a password that can be used only once and is valid for a limited length of time. OTP requires that the TPM is present, enabled, and owned. To enable OTP, a mobile device is paired with the computer using the Security Console and the Security Tools Mobile app. The Security Tools Mobile app generates the password on the mobile device that is used to log onto the computer at the Windows logon screen. Based on policy, the OTP feature may be used to recover access to the computer if a password is expired or forgotten, if OTP has not been used to log on to the computer. The OTP feature can be used either for authentication or for recovery, but not both. OTP security exceeds that of some other authentication methods since the generated password can be used only once and expires in a short time.

Preboot Authentication (PBA) - Preboot Authentication serves as an extension of the BIOS or boot firmware and guarantees a secure, tamper-proof environment external to the operating system as a trusted authentication layer. The PBA prevents anything being read from the hard disk, such as the operating system, until the user has confirmed they have the correct credentials.

Protected - For a self-encrypting drive (SED), a computer is protected once the SED has been activated and the Pre-boot-authentication (PBA) is deployed.

Self-encrypting Drives (SEDs) - A hard drive that has a built-in encryption mechanism that encrypts all data stored on the media and decrypts all data leaving the media, automatically. This type of encryption is completely transparent to the user.

Single Sign-On (SSO) - SSO simplifies the logon process when multi-factor authentication is enabled at both preboot and Windows logon. If enabled, authentication is required at preboot only, and users are automatically logged on to Windows. If not enabled, authentication may be required multiple times.

Trusted Platform Module (TPM) - TPM is a security chip with three major functions: secure storage, measurement, and attestation. The Encryption client uses TPM for its secure storage function. The TPM can also provide encrypted containers for the software vault. The TPM is also required for use with the One-time Password feature.

