Dell Data Security Console User Guide

Threat Protection/Encryption Status/Authentication Enrollment/Password Manager v1.8

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

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

Dell Data Security Console User Guide

2017 - 08

Rev. A01

Contents

1

Dell Data Security Console Introduction

Dell Endpoint Security Suite Pro provides you with simple-to-use and intuitive tools to increase the security of your computer.

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

- Enroll credentials for use with Endpoint Security Suite Pro
- 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)
- View Threat Protection status

Data Security Console

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

You can access these applications:

- The Threat Protection dashboard displays protection status of the computer, based on Threat Protection policies.
- 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 product.

Additionally, online support for Dell 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.

2

Data Security Console

The Data Security 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 Data Security Console, from the *Desktop,* double-click the **Dell Data Security Console** icon.

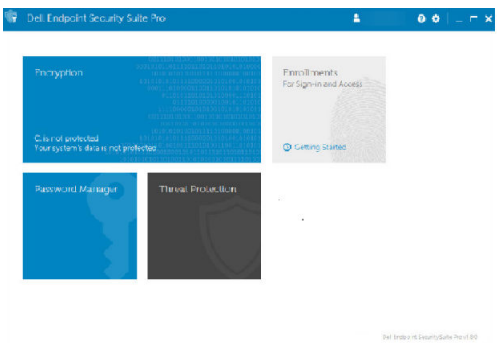
When the Data Security Console launches, the home page displays the Endpoint Security Suite applications:

- Threat Protection
- 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

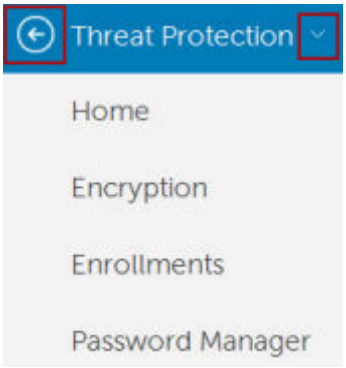
To access an application, click the appropriate tile.



Title bar

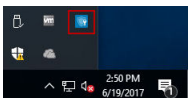
To return to the home page from within an application, click the back arrow in the left corner of the title bar, next to the name of the active application.

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 Data Security Console, click the appropriate icon in the right corner of the title bar.

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

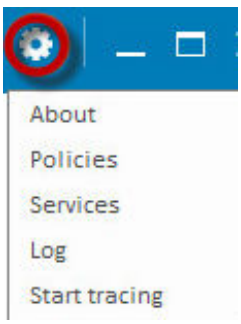


To open Help, click the **?** on the title bar.

Data Security Console Details

To view details about the Data Security 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.



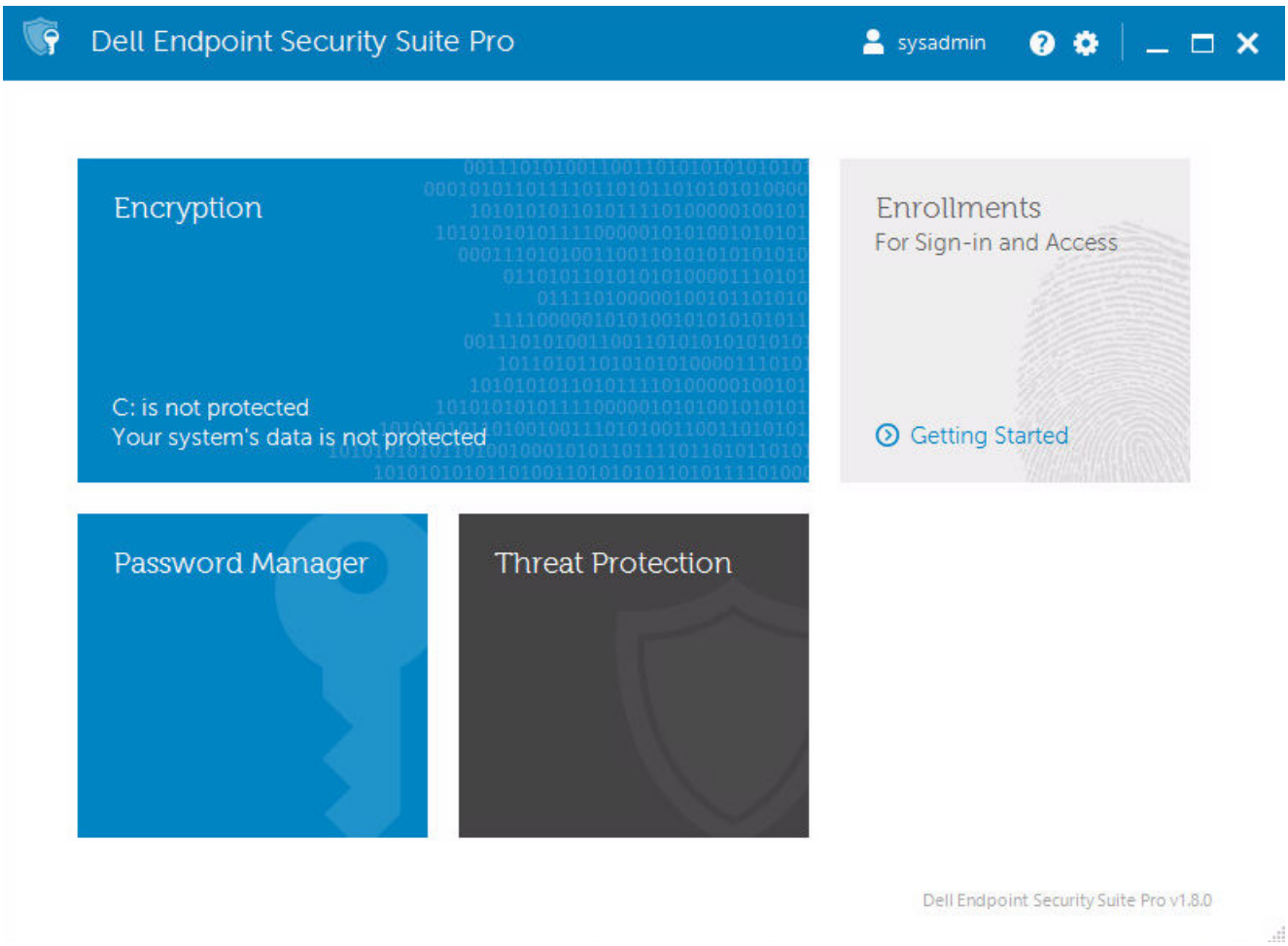
Menu Item	Purpose
About	Contains version and copyright information.
Show Info	Contains the following: • product version and date information • whether the Data Security Console is managed on this computer by the enterprise or by a local administrator • version numbers of the operating system, BIOS, motherboard, and Trusted Platform Module (TPM).

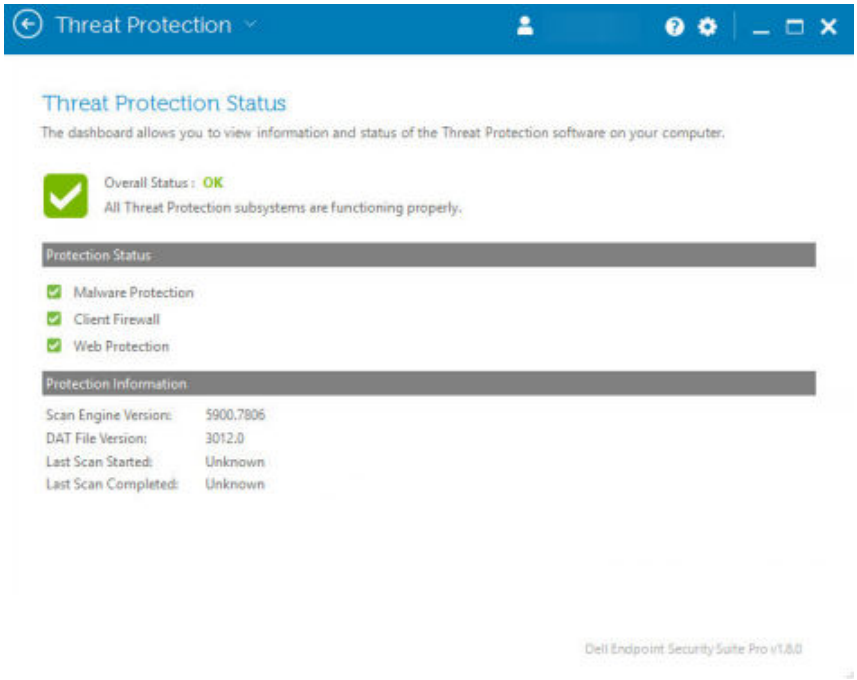
MS Info	Runs the Microsoft Windows System Information utility to display detailed information about the hardware, components, and software environment.
Copy Info	Copies all of the system information to the clipboard, to paste into an email for your administrator or Dell ProSupport.
Feedback	Displays 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.

Threat Protection

Threat Protection Dashboard

Users access the Threat Protection Status dashboard through the Threat Protection tile in the Data Security Console.





- Protected - Overall Status is Protected if *Access Protection*, *Exploit Protection*, and *On-Access Protection* policies are set to True (Enabled).

  or

  Either the *On-Demand Protection - Full Scan* or *On-Demand Protection - Quick Scan* policy is set to True (Enabled) and its corresponding scheduling policies are set.
- Vulnerable - Overall Status is Vulnerable if any of the following policies is set to False (Disabled): *Access Protection*, *Exploit Protection*, and *On-Access Protection*.

  and

  Both *On-Demand Protection - Full Scan* or *On-Demand Protection - Quick Scan* policies are set to False (Disabled) or True (Enabled) without corresponding scheduling policies set.

Protection Status

The Protection Status field displays individual status of Protected (indicated by a green check mark) or Vulnerable (indicated by a red X) based on whether the following master policies are set to True (Enabled):

- Malware Protection
- Client Firewall
- Web Protection

Protection Information

The Protection Information field provides the following information:

- Scan engine version - The version of scan engine used. The scan engine compares the contents of scanned files against known threats.
- DAT File Version - The version of Threat Protection DAT file that the engine uses to detect malware during a scan.
- Last Scan Started - Time stamp of when the last successful scan was started.
- Last Scan Completed - Time stamp of when the last scan was completed.

Gear Menu

The gear menu provides access to the following:

- About - Provides information about the Endpoint Security Suite version and the client computer configuration.
- Policies - Lists many agent policies. Currently, it does not list the Threat Protection policies, due to their large number.
- Services - Displays the state of the AntiMalware Management Plugin and communication with the Dell Management Agent.
- Feedback - Provides a link to the Dell Support website.
- Logs - Displays events related to services, including the AntiMalware Management Plugin.
- Start Tracing - Lets you start and stop a recording of system activities, for troubleshooting.

Popup Notifications

Based on policy, popup notifications may inform the user of threats involving the following:

- Files and folders
- Registry
- Endpoint Security Suite processes
- Unverified or malicious websites
- Phishing pages

The user does **not** need to take any action. All remediation is handled by Endpoint Security Suite Pro.

Suppress Popup Notifications

To suppress messages that alert the user to threats, set the following registry key:

[HKLM\Software\Dell\Dell Data Protection]

"DDPTPHideToasters"=DWORD:1

0=(Default) Disabled, do not hide popup notifications from the user

1=Enabled, hide popup notifications from user

Filter Popup Notifications

To display notifications of a minimum severity level, set this registry key:

[HKLM\Software\Dell\Dell Data Protection]

"DDPTPEventSeverityFilter"=DWORD:3

0=Information (displays all events), 1=Warning, 2=Minor, 3=Major (default, show Major and Critical only), 4=Critical

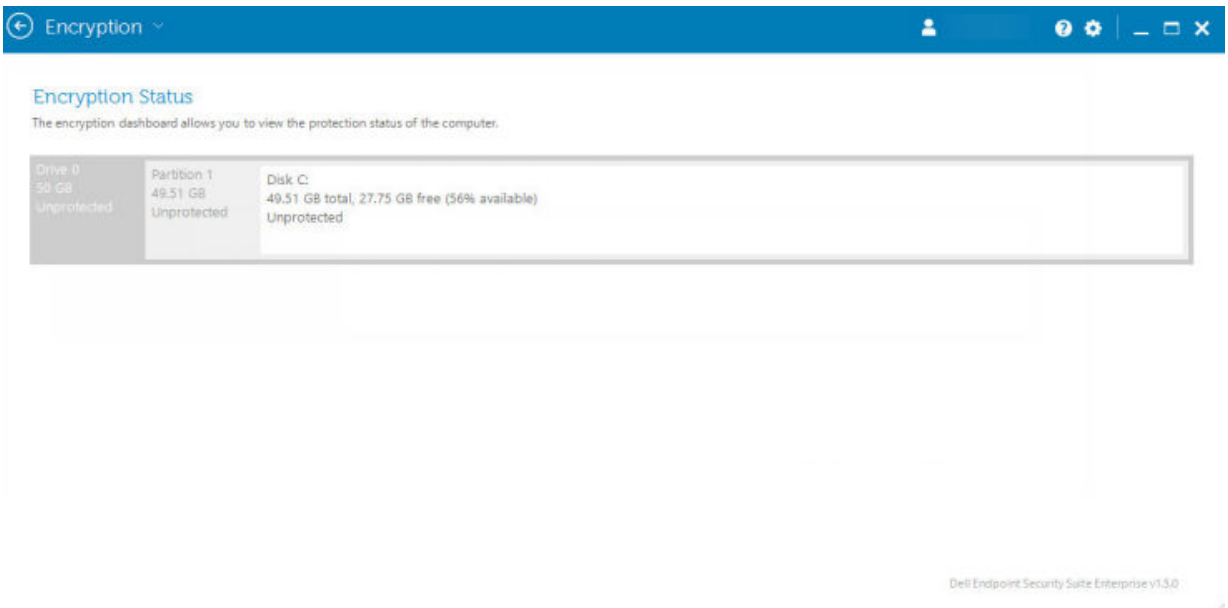
If "DDPTPHideToasters" is set to 1, settings for "DDPTPEventSeverityFilter" are ignored.

4

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**.



5

Enrollments

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

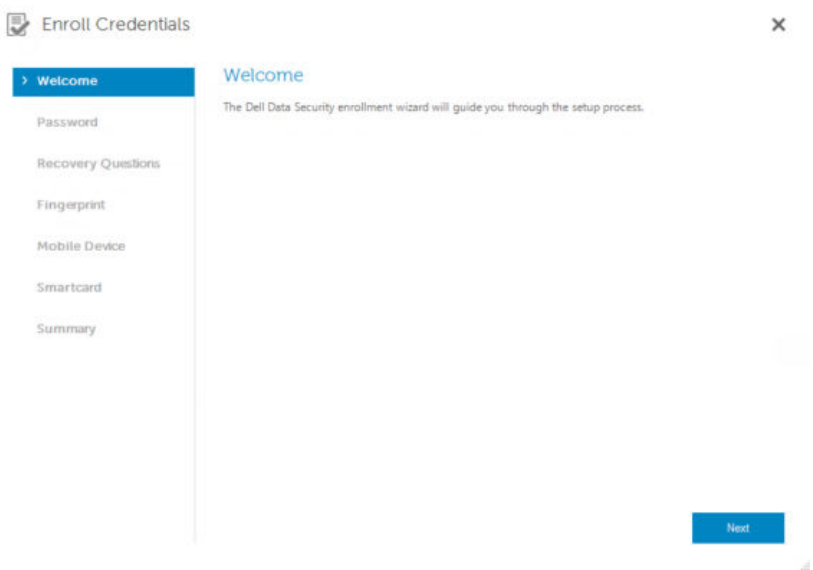
The first time you enroll your credentials with the Data Security Console, a wizard guides you through enrolling a password change, Recovery Questions, fingerprints and smart card. Depending on policy, you can either enroll or skip each credential. After initial enrollment, you can click the Enrollment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

Enroll Credentials for the First Time

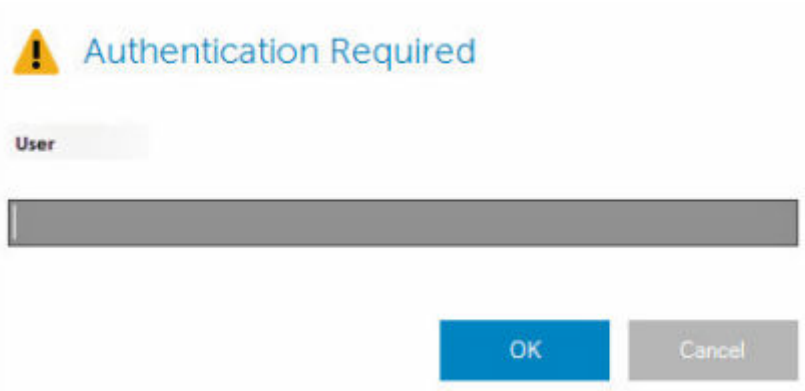
To enroll credentials for the first time:

1 On the Data Security 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

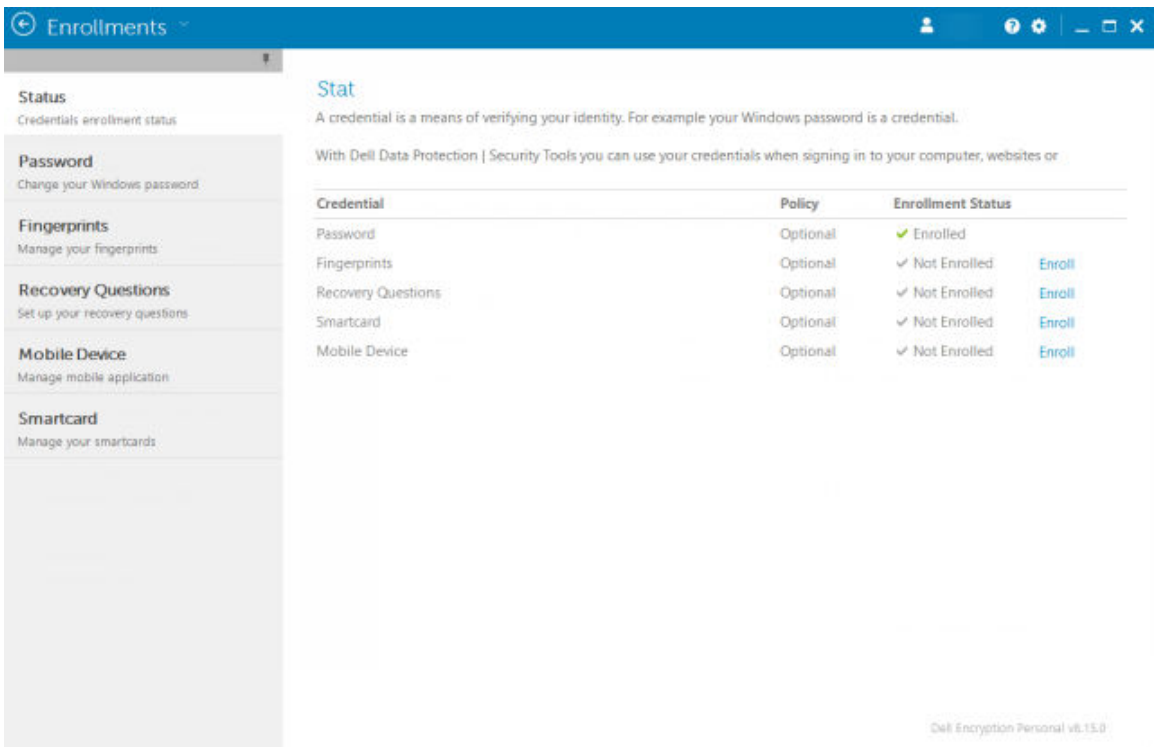
To add, modify, or view enrollments, click the **Enrollments** tile.

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.

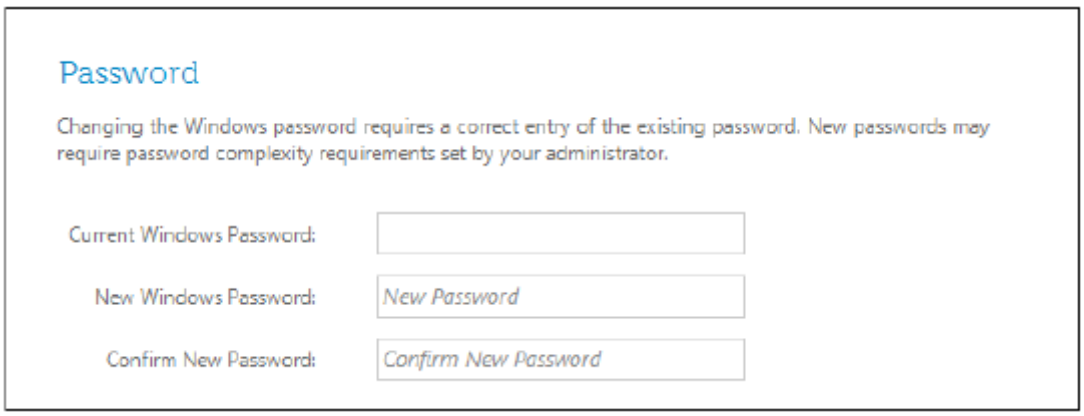
  If policy does not allow enrollment or modification of a credential, a message displays on the credential's enrollment page, "Credentials modification is not allowed by policy."



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.



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

NOTE:
You should only change your Windows password in the Data Security Console rather than in Windows. If the Windows password is changed outside of the Data Security 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**.

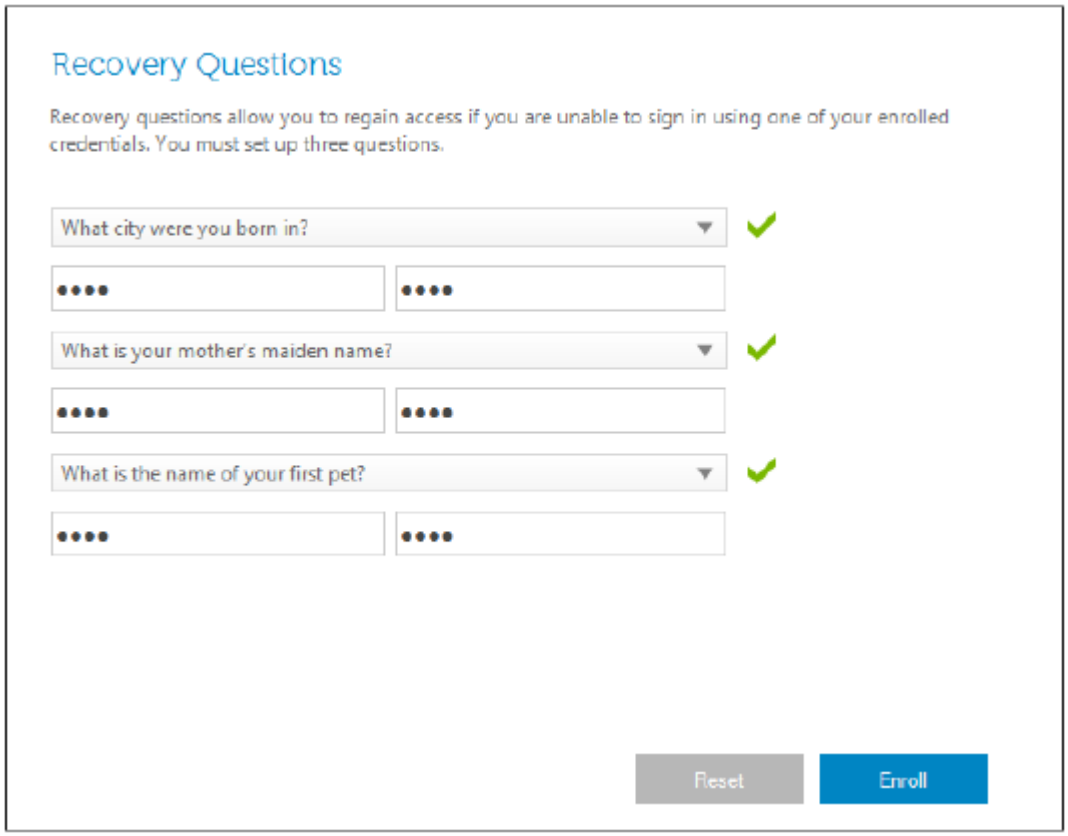
NOTE:
Click the **Reset** button to clear the selections on this page and start over.

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**.



Fingerprints

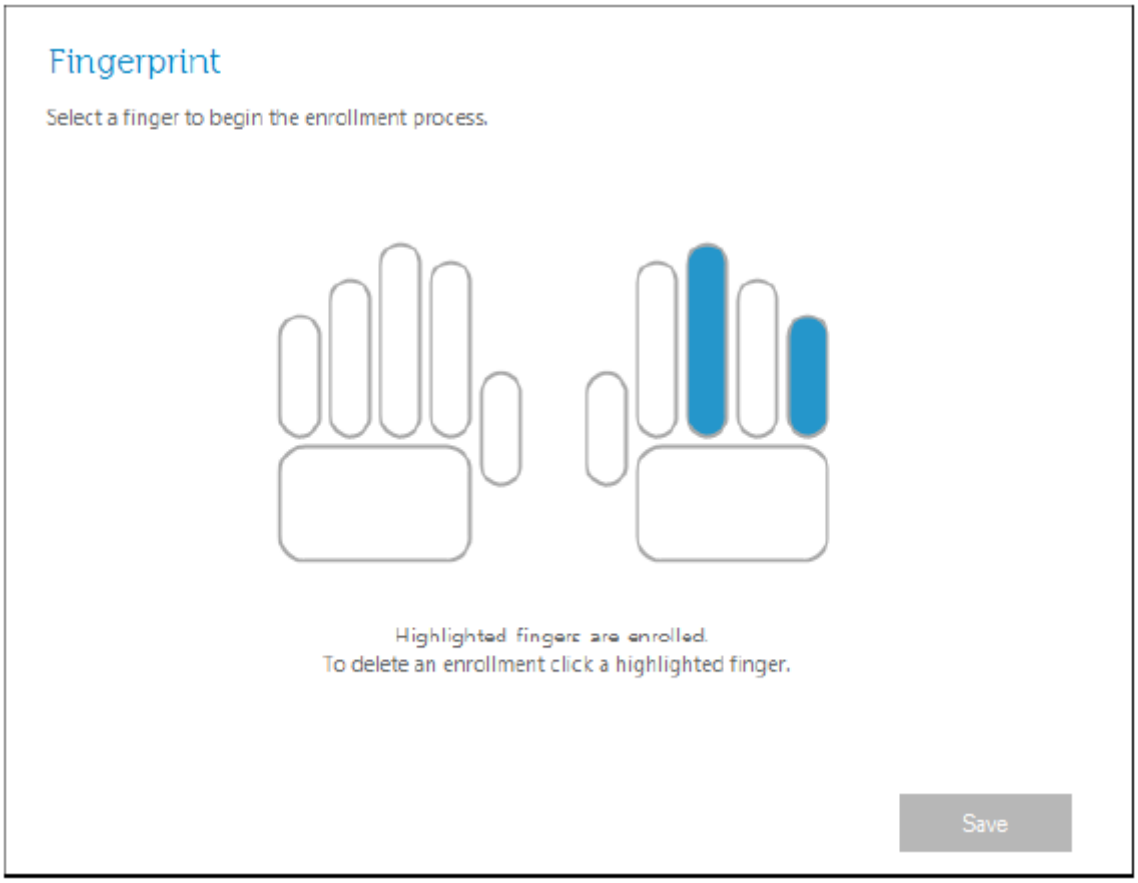
NOTE:
To use this feature, your computer must have a fingerprint reader.

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.

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**.



Smart Cards

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

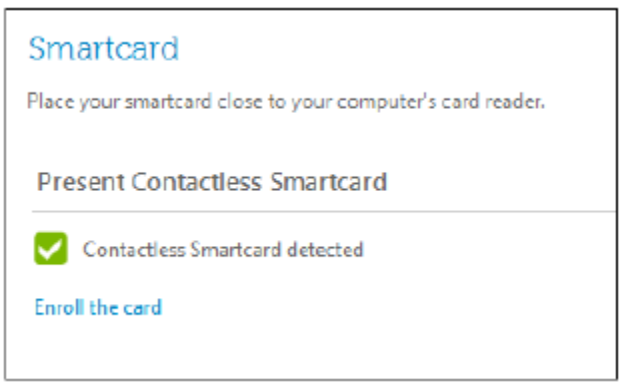
To enroll smart cards, follow these instructions:

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**.

6

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:

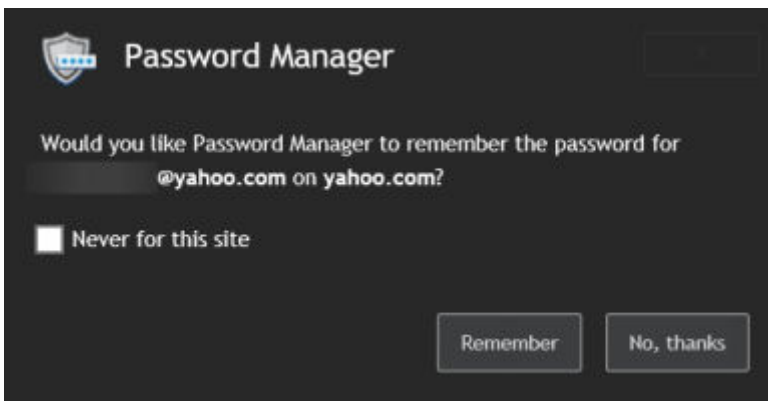
- Double-click functionality on Password Manager icons is not available.
- The default action is not shown in bold in the drop-down context menu.
- If a page has multiple logon forms, you may see more than one Password Manager icon.

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 Endpoint Security Suite 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 Data Security 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 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*.

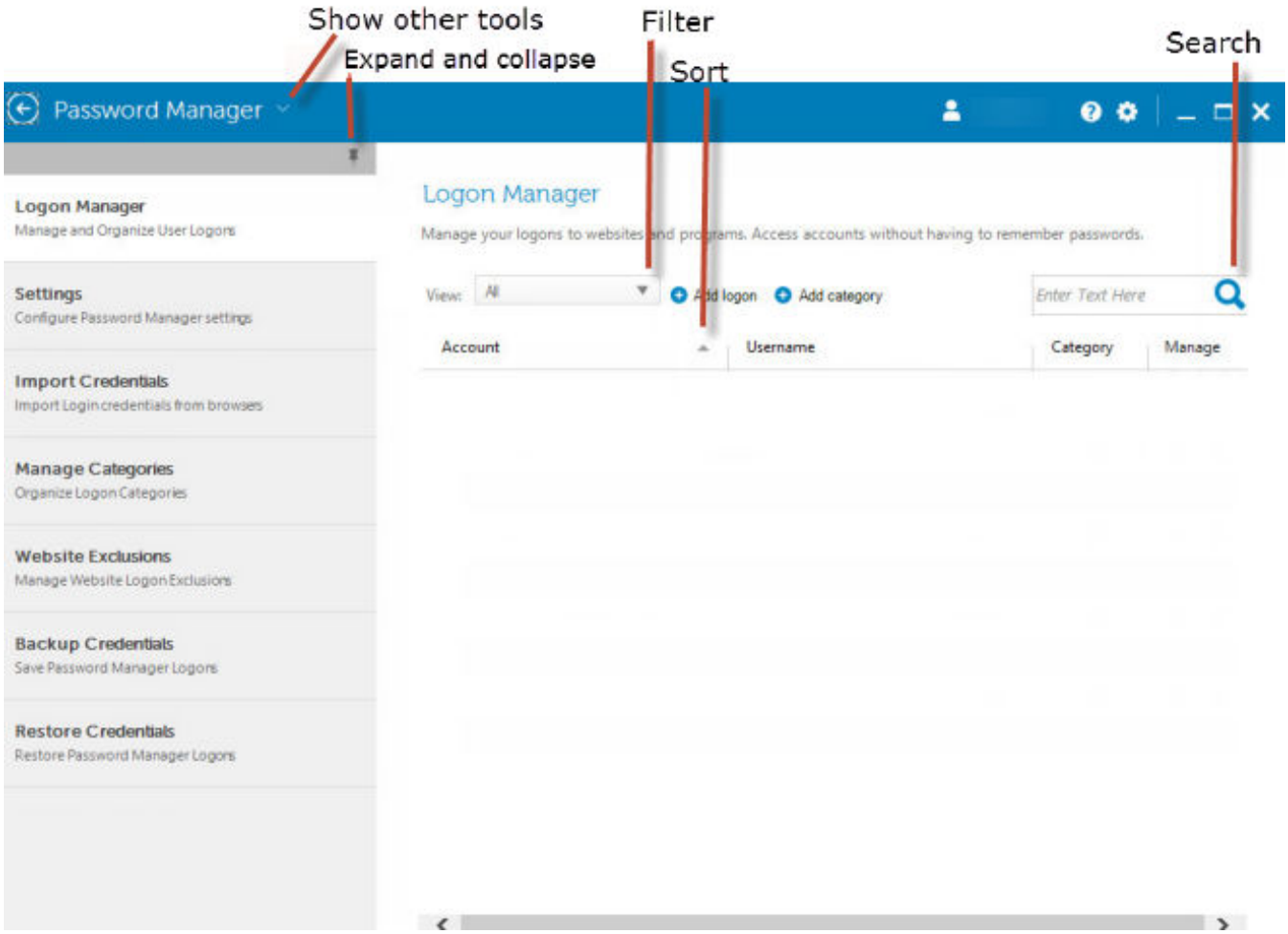
You can manage logons:

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.



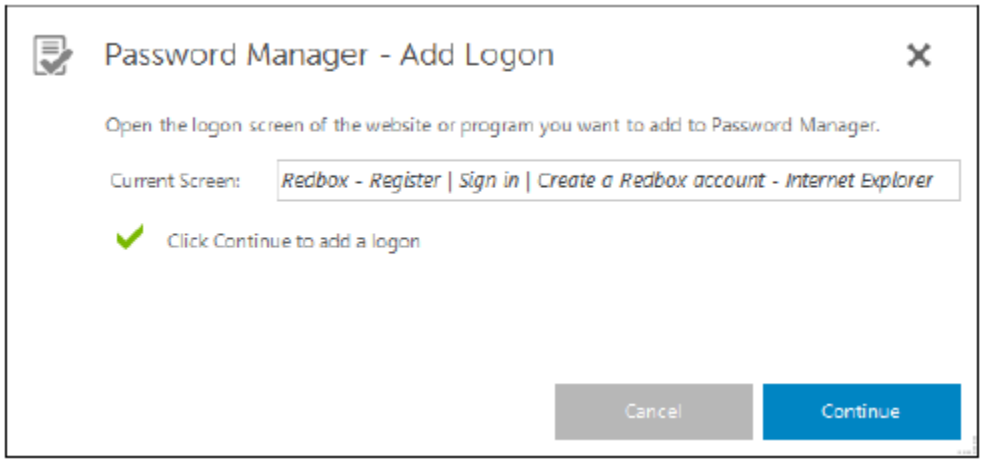
Add Category

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**.

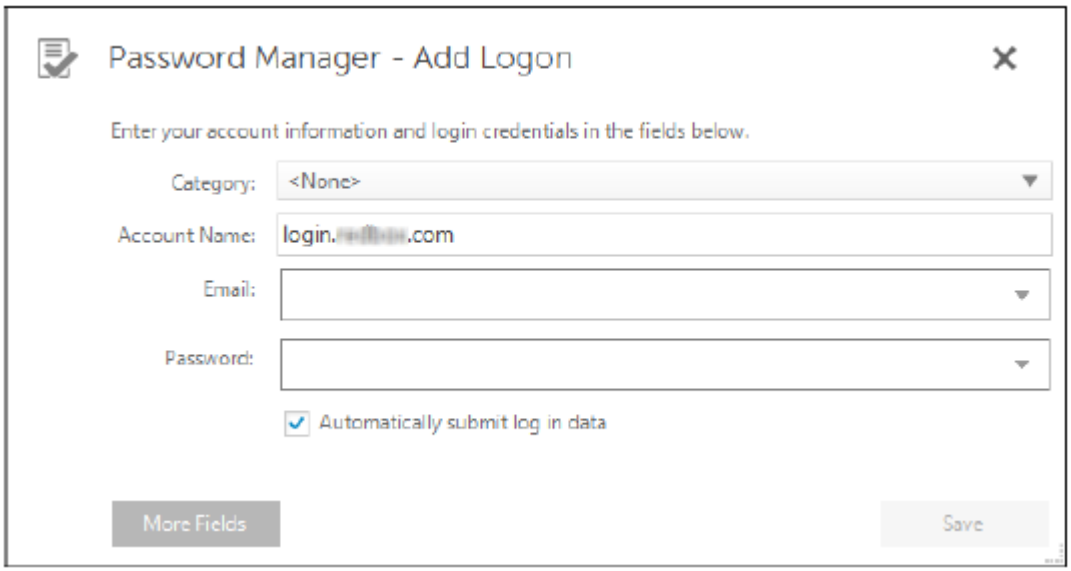
Add Logon

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.

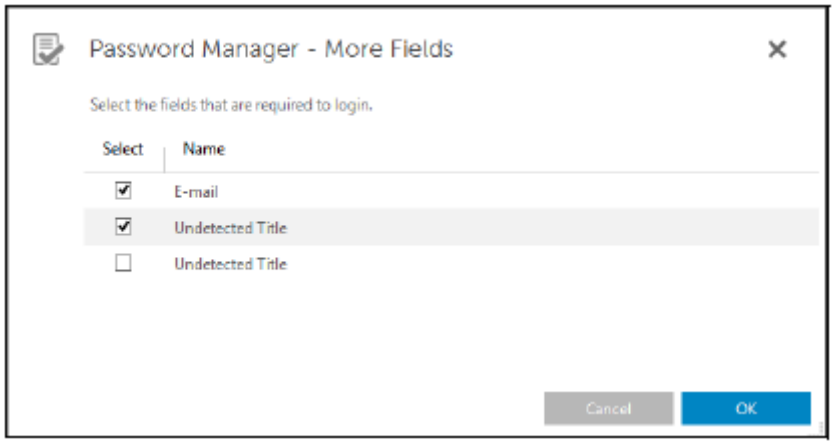


5 If a field name is shown as Undetected Title, or if the wrong fields have been included as logon fields, click the **More Fields** button to edit field names or remove fields.

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.

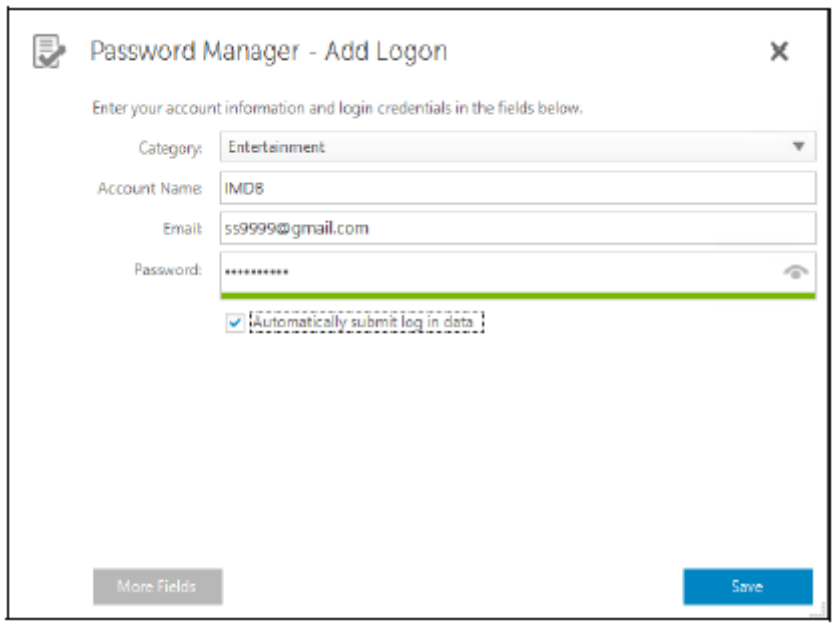
If a field is unnecessary for logon, to exclude it from logon information, clear its check box.



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**.

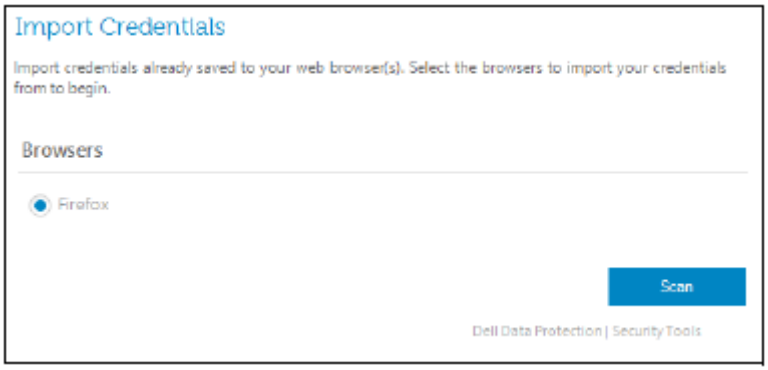
The website or program logon displays on the Logon Manager page.

Import Credentials

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

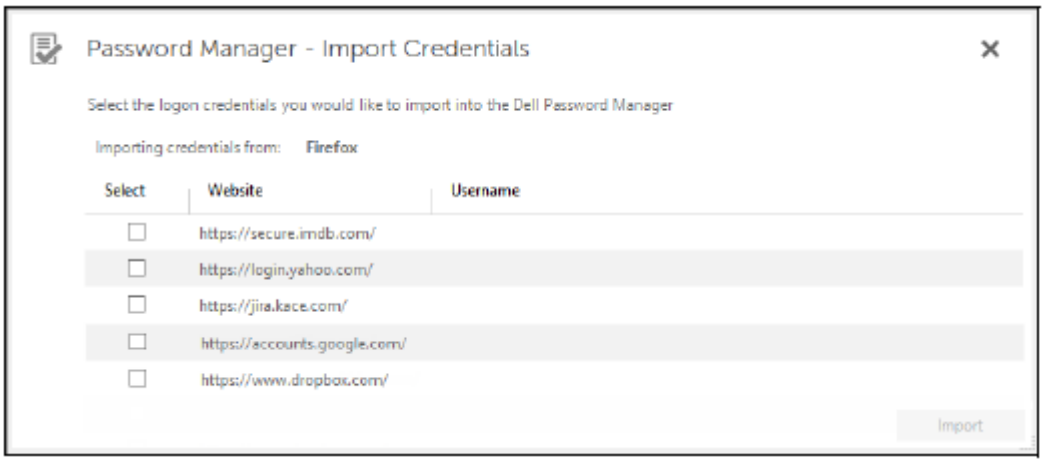
1 In the Password Manager tool, select **Import Credentials**.

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

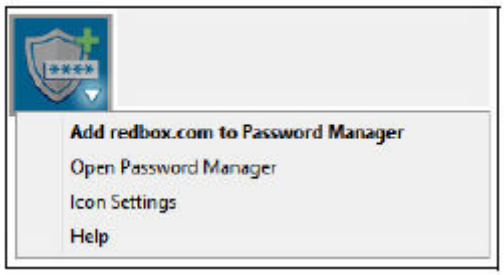
When you visit a website or program, the Password Manager icon displays.

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:



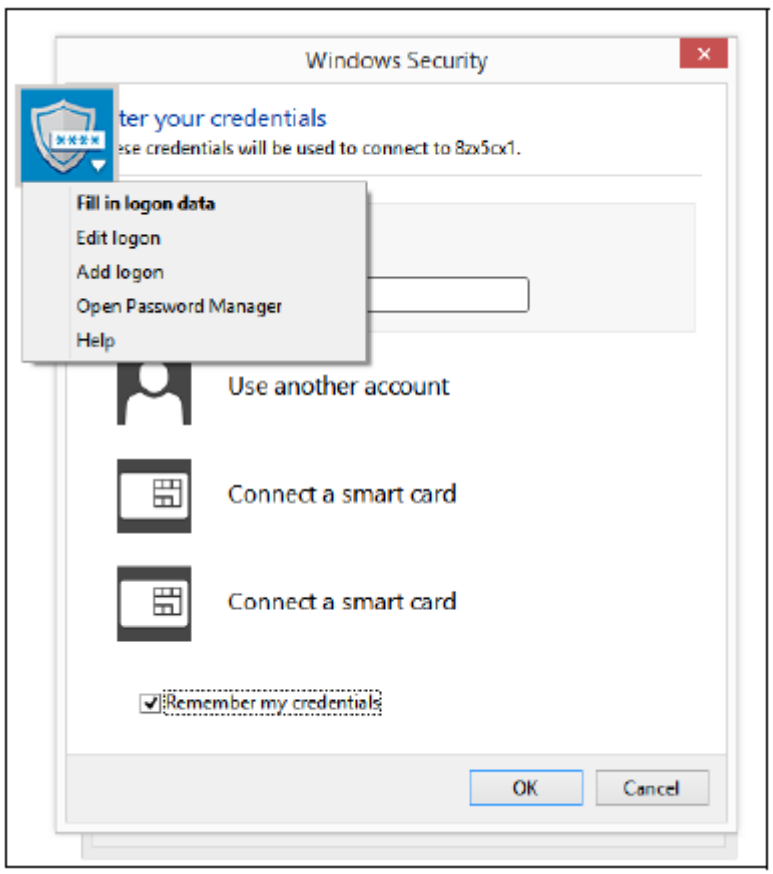
Add to Password Manager - Opens the Add Logon dialog.

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

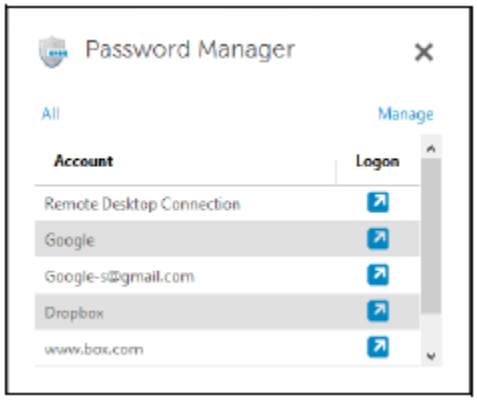
When you open a website or program logon, Password Manager detects whether the page is trained. If trained, the Password Manager icon displays in the logon area. If untrained, the Password Manager icon displays-unless prompts for untrained forms have been disabled.

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 Data Security Console > Password Manager > Settings.

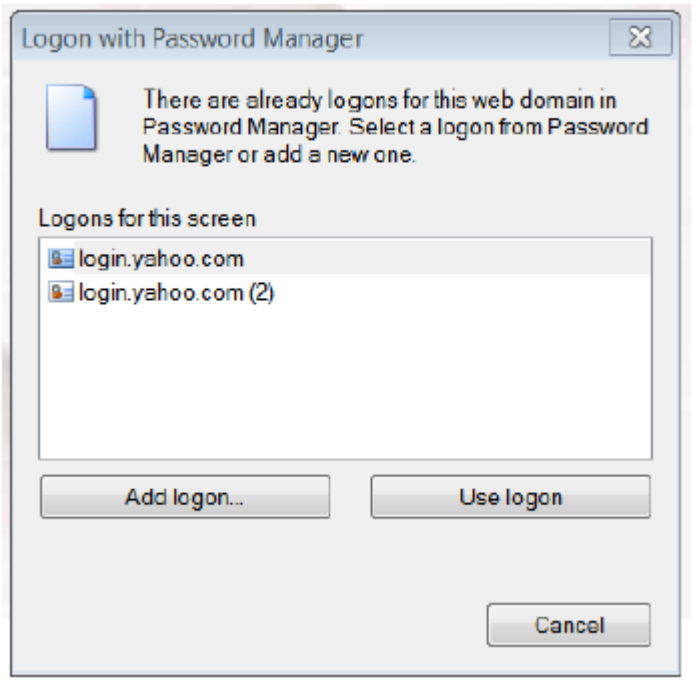
If more than one logon for the site or program has been stored, you are prompted to choose the account to use.



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.

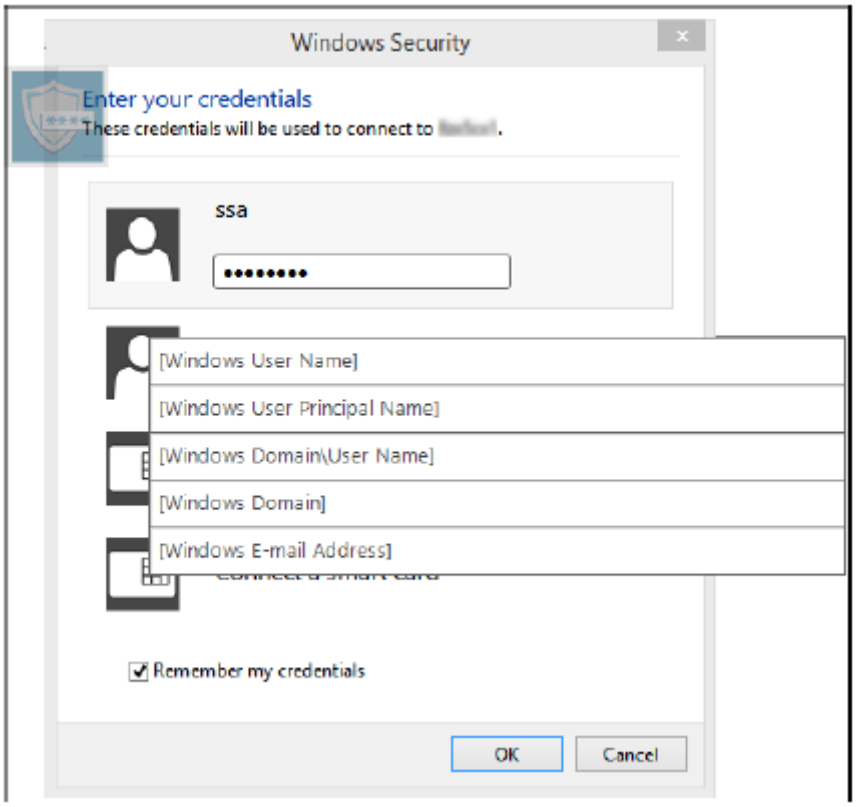
Instead of typing your user name and password, choose the Windows credentials from the drop-down menus available in the *Add Logon* and *Edit Logon* dialogs.

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:

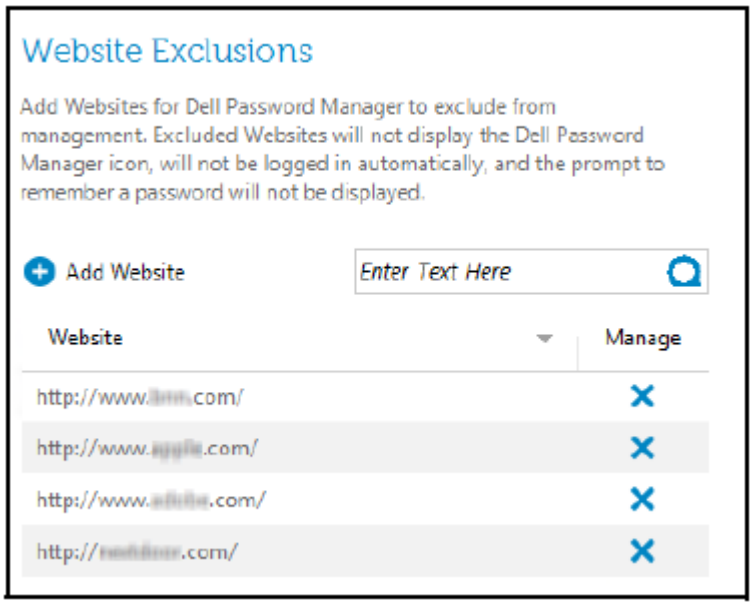
1 Click the **Website Exclusions** tab.
2 Click **Add Website.**

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.

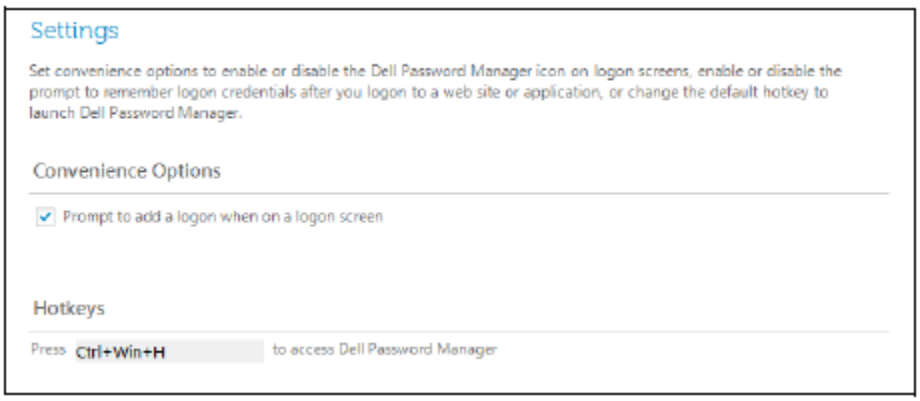


Disable Prompts to Train Logon Forms

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

To disable prompts for new logons:

1 Open the Data Security 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

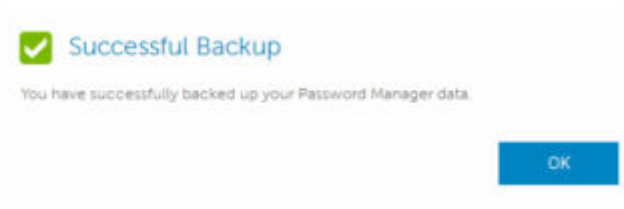
The Password Manager lets you securely back up the logon data that is managed by Password Manager. This data can be restored on any computer protected by Password Manager.

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 restore operation, click the icon in the title bar and select **Log.**

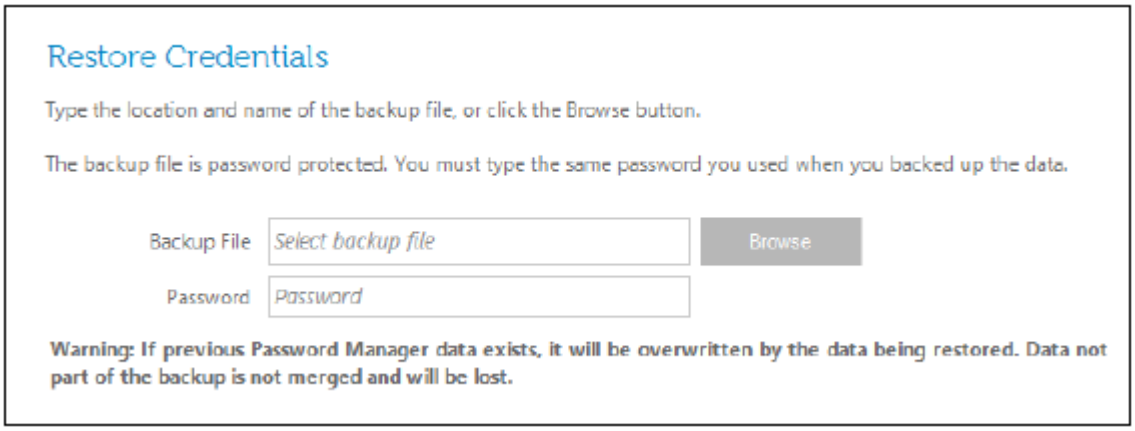
Restore Credentials

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.



4 Click **Next**.

NOTE:

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

7

Glossary

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

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.