

# Dell Data Security Console

User Guide v10.0



## 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.

© 2012-2018 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 Encryption, Endpoint Security Suite Enterprise, and Data Guardian suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. Cylance®, CylancePROTECT, and the Cylance logo are registered trademarks of Cylance, Inc. in the U.S. and other countries. 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®, Windows Vista®, Windows 7®, Windows 10®, Active Directory®, Access®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Outlook®, PowerPoint®, Word®, 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. Dropbox<sup>SM</sup> is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, App Store<sup>SM</sup>, Apple Remote Desktop™, Boot Camp™, FileVault™, iPad®, iPhone®, iPod®, iPod touch®, iPod shuffle®, and iPod nano®, Macintosh®, and Safari® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. 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. 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. 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. Bing® is a registered trademark of Microsoft Inc. Ask® is a registered trademark of IAC Publishing, LLC. Other names may be trademarks of their respective owners.

### User Guide v10.0

2018 - 08

Rev. A01

# Contents

<b>1 Introduction</b> .....	<b>4</b>
Contact Dell ProSupport.....	4
<b>2 Navigation</b> .....	<b>5</b>
<b>3 Encryption Status</b> .....	<b>7</b>
<b>4 Sign-in Access</b> .....	<b>8</b>
Enroll Credentials for the First Time.....	8
Add, Modify, or View Enrollments.....	8
Password.....	9
Recovery Questions.....	10
Recovery Questions Already Enrolled.....	10
<b>5 Glossary</b> .....	<b>12</b>

# Introduction

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 to easily enroll their PBA password and recovery questions.

The following features are available:

- Enroll credentials for use with PBA
- Take advantage of multi-factor credentials, including passwords and smart cards
- Recover access to your computer if you forget your password without help desk calls or administrator assistance
- Easily change your Windows password
- Set personal preferences
- View encryption status

## Data Security Console



To open the Data Security Console, from the Desktop, double-click the Dell Data Security Console icon .

You can access these applications:

- Encryption Status allows you to view the encryption status of the computer's drives and partitions.
- The Sign-In Access tool allows you to set up and manage PBA password, configure PBA self-recovery questions, and view the status of your credential enrollment.

This guide describes how to use each of these applications.

Be sure to periodically check [dell.com/support](https://dell.com/support) for updated documentation.

## Contact Dell ProSupport

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

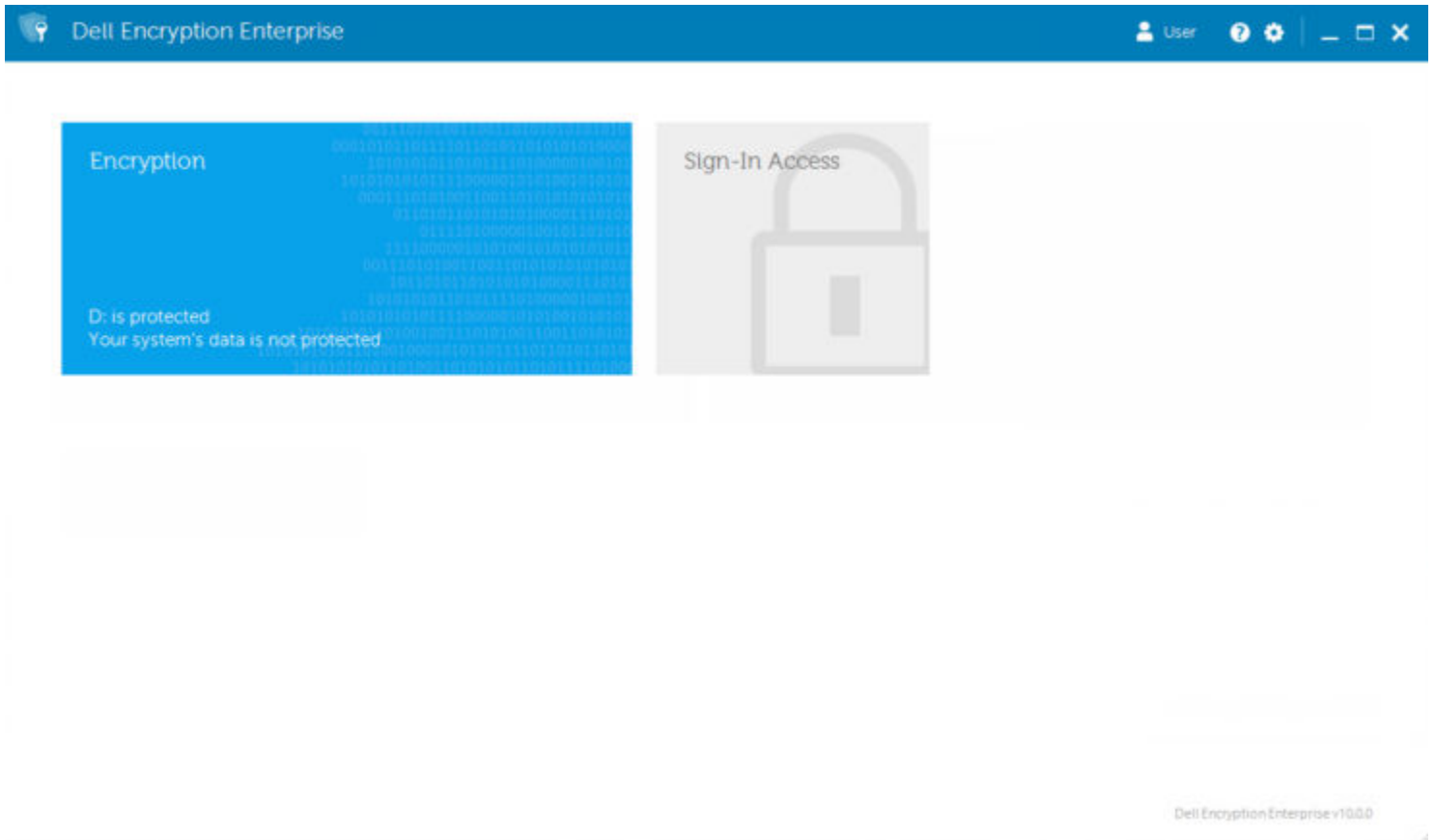
Additionally, online support for Dell products is available at [dell.com/support](https://dell.com/support). Online support includes drivers, manuals, technical advisories, FAQs, and emerging issues.

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

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

## Navigation

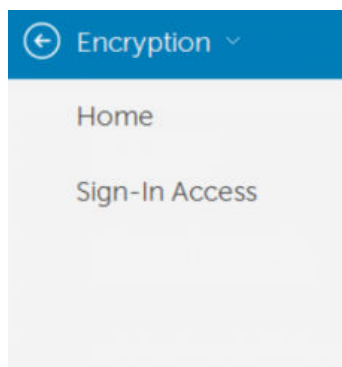
To access an application, click the appropriate tile.



### 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.

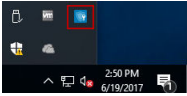
To navigate directly to another application, click the down arrow next to the active application name, and select an application.



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 notification area 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
<b>About</b>	Contains version information.
<b>Show Info</b>	Contains the following: <ul style="list-style-type: none"><li>product version and date information</li><li>whether Dell Encryption and/or PBA advanced authentication is managed by the enterprise or by a local administrator</li><li>version numbers of the operating system, BIOS, motherboard, and <a href="#">Trusted Platform Module (TPM)</a>.</li></ul>
<b>MS Info</b>	Runs the Microsoft Windows System Information utility to display detailed information about the hardware, components, and software environment.
<b>Copy Info</b>	Copies all of the system information to the clipboard, to paste into an email for your administrator or Dell ProSupport.
<b>Feedback</b>	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 policy.)
<b>Policies</b>	Displays a hierarchy of policies that apply to this computer.
<b>Services</b>	Displays details about the services that are running.
<b>Support</b>	Connects to the Dell ProSupport website.
<b>Log</b>	Displays a detailed list of logged events, 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 blue header with a back arrow, the text 'Encryption', a user profile icon labeled 'User', and system icons for help, settings, and window control. Below the header, the title 'Encryption Status' is followed by a brief description: 'The encryption dashboard allows you to view the protection status of the computer.' The main content area displays three rows of drive information, each with a colored background indicating its status: green for 'Protected' and grey for 'Unprotected'.

Drive	Partition	Disk
Drive 0 232.88 GB Protected	Partition 1 232.35 GB Protected	Disk C: 232.35 GB total, 208.26 GB free (89% available) Protected by DDPE
Drive 1 119.24 GB Protected	Partition 0 549 MB Protected	Disk D: "System Reserved" 549 MB total, 516.7 MB free (94% available) Protected by DDPE
Drive 2 7.47 GB Unprotected	Partition 0 7.47 GB Unprotected	Disk F: "ESD-USB" 7.45 GB total, 2.83 GB free (37% available) Unprotected

Dell Encryption Enterprise v10.0.0

# Sign-in Access

Sign-in Access lets you enroll, modify, and check enrollment status, based on policy set by the administrator.

After initial enrollment, you can click the Sign-in Access tile to add or modify credentials.

**NOTE:** The Sign-in Access tile will display only if the PBA is active.

## Enroll Credentials for the First Time

To enroll credentials for the first time:

- 1 On the Data Security Console home page, click the **Sign-In Access** tile.
- 2 On the Password page, to change your Windows password, enter the current password then enter and confirm a new password and click **Change**.
- 3 On the Recovery Question page, select and provide answers to three Recovery Questions then click **Enroll**.

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 **Sign-In Access** tile.

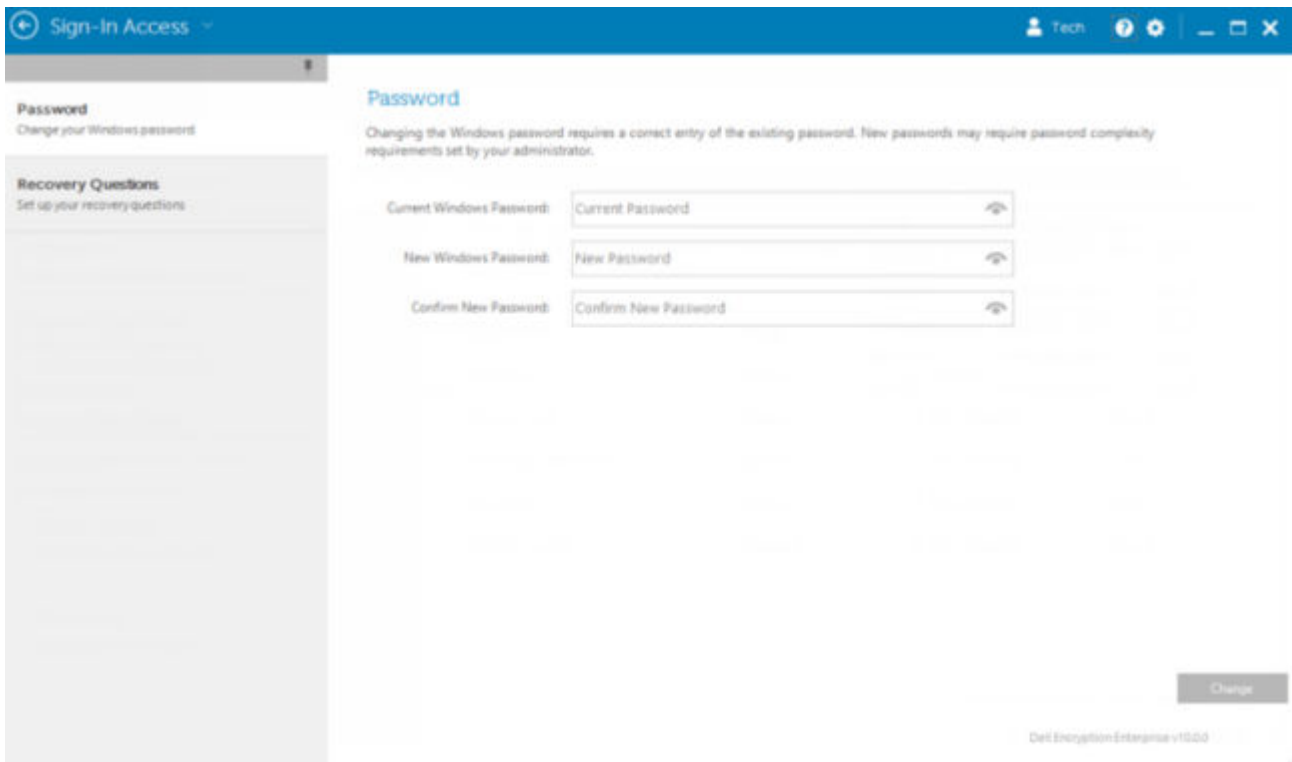
Tabs in the left pane list available Enrollments. This varies based on your platform or type of hardware.

The Sign-in Access 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.

A screenshot of the 'Password' form, enclosed in a black rectangular box. The form title is 'Password'. Below the title is the instruction: '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' (empty), 'New Windows Password' (containing 'New Password'), and 'Confirm New Password' (containing 'Confirm New Password'). Each field has a small eye icon to its right. At the bottom right of the form is a 'Change' button.

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

### **i** 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 PBA 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 **Reset** to clear the selections on this page and start over.

# Recovery Questions Already Enrolled

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

- 1 Click the **Recovery Questions** tab.
- 2 Click the appropriate button:
  - To remove the PBA recovery questions completely, click **Delete**.
  - To re-define PBA 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.

What city were you born in? ✓

.....

What is your mother's maiden name? ✓

.....

What is the name of your first pet? ✓

.....

Reset Enroll



# Glossary

**Credential** - A credential is something that proves a person's identity, such as 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.