Dell Data Security Console

User Guide v2.0

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.**

User Guide v2.0

2018 - 08

Rev. A01

Contents

1

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
- View Advanced Threat Prevention status

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

- View encryption status (on computers with self-encrypting drives)
- View Advanced Threat Prevention

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:

- The Advanced Threat Prevention dashboard displays protection status of the computer, based on Advanced Threat Prevention policies.
- 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 for updated documentation.

Contact Dell ProSupport

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

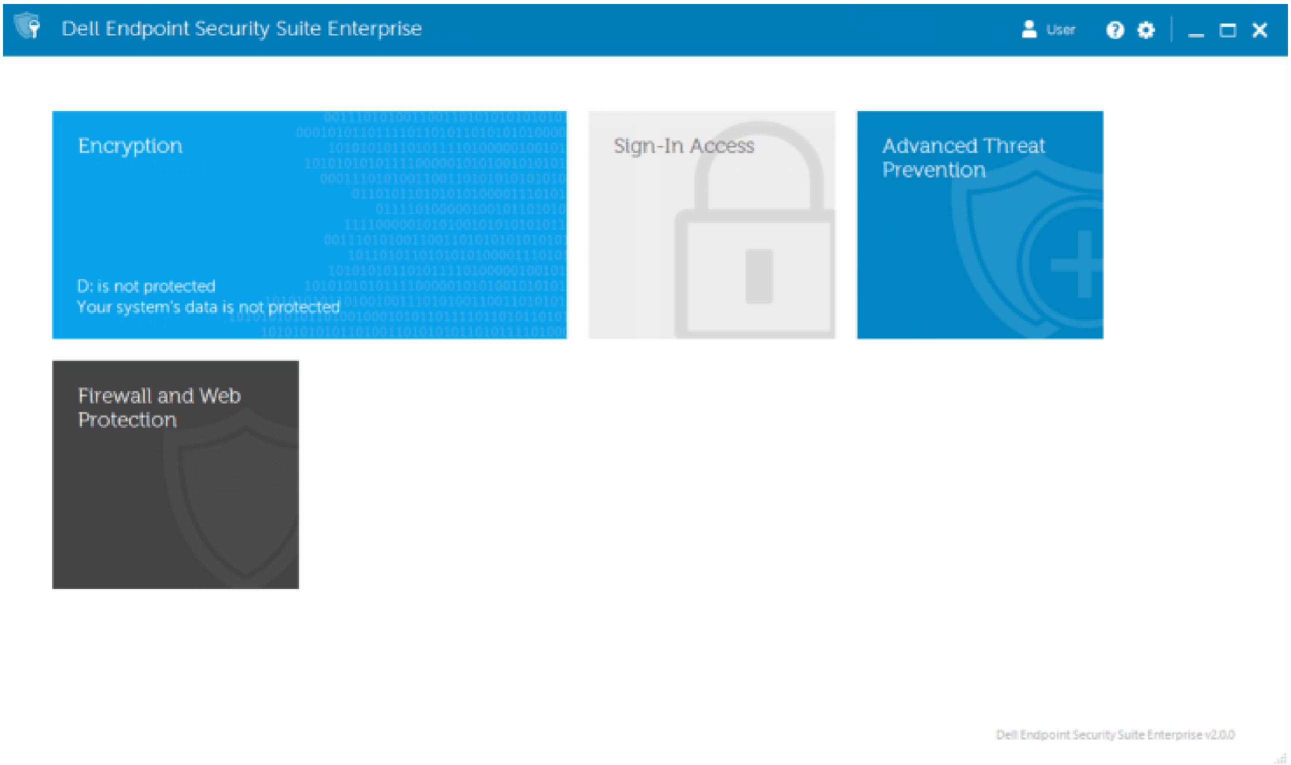
Additionally, online support for Dell products is available at dell.com/support. Online support includes drivers, manuals, technical advisories, FAQs, and emerging issues.

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

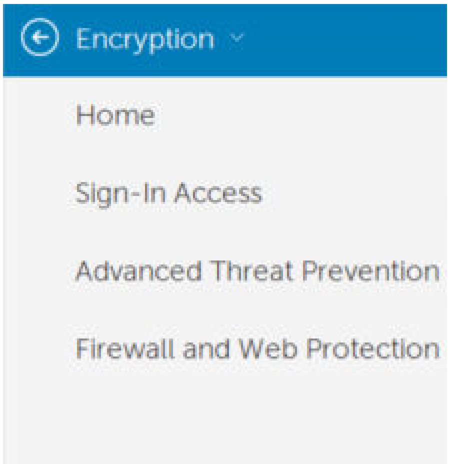

Dell Endpoint Security Suite Enterprise
User
Encryption
Sign-In Access
Advanced Threat Prevention
Firewall and Web Protection
Dell Endpoint Security Suite Enterprise v2.0.0

D: is not protected
Your system's data is not protected

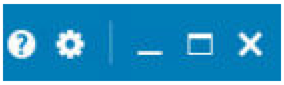
Title bar

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.

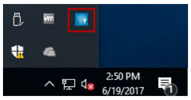
To navigate directly to another application, click the down arrow next to the active application name, and select an application.



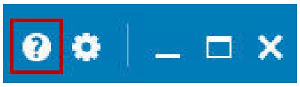
To minimize, maximize, or close the Data Security Console, click the appropriate icon in the right corner of the title bar.



To restore the Data Security Console after minimizing, double-click its notification area icon.

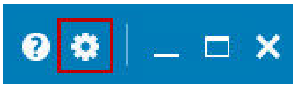


To open Help, click the **?** on the title bar.



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**
About	Contains version information.
Show Info	Contains the following: • product version and date information • whether Dell Encryption and/or PBA advanced authentication is managed 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 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.
Advanced Threat Prevention	Enables Standard UI for the Advanced Threat Prevention pane.
Log	Displays a detailed list of logged events, for troubleshooting.

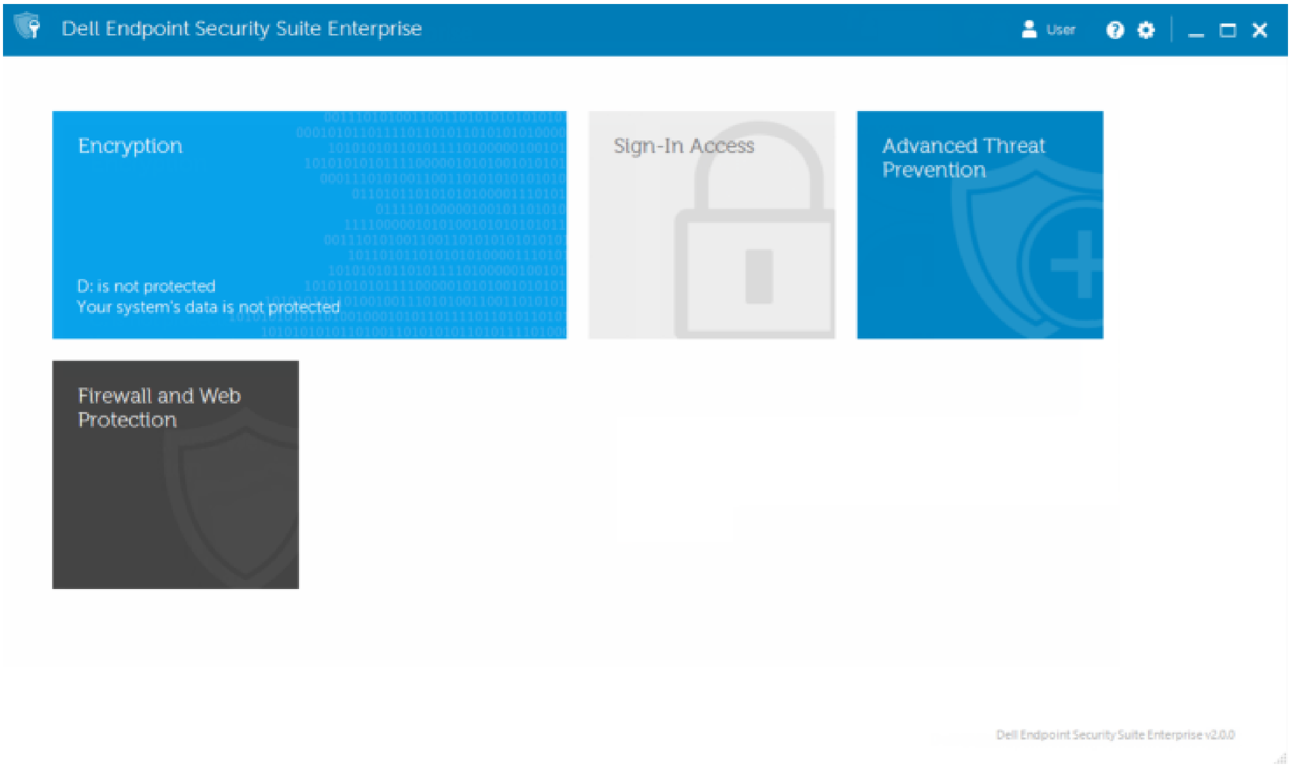
3

Advanced Threat Prevention

Advanced Threat Prevention protects your computer against malware by monitoring all processes attempting to execute on your computer or within memory space, and flagging any that are deemed abnormal or unsafe.

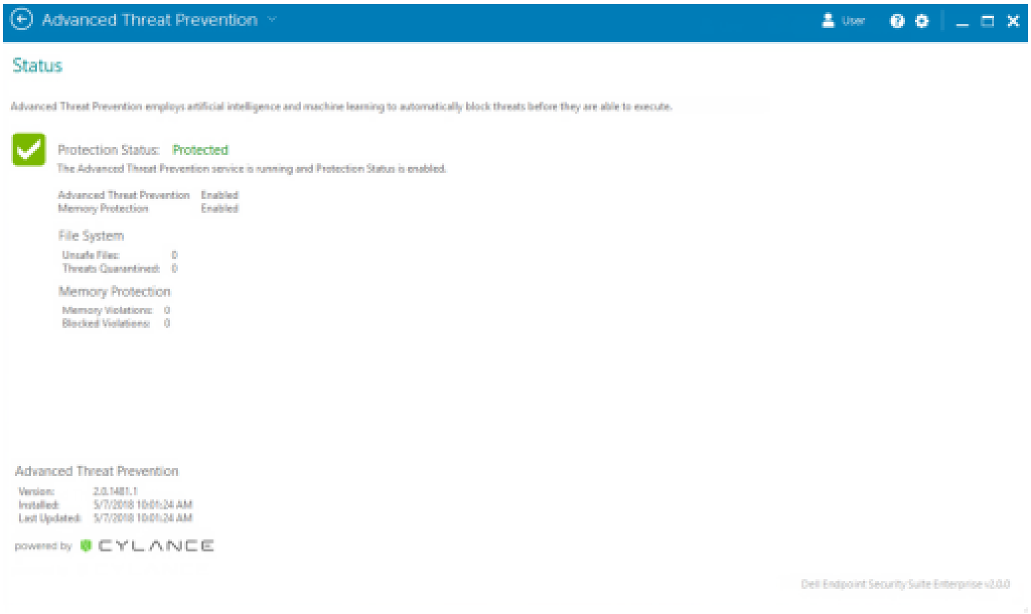
Advanced Threat Prevention is installed by default with Endpoint Security Suite Enterprise. Firewall and Web Protection are optionally installed as part of Endpoint Security Suite Enterprise.

Select the Advanced Threat Prevention tile to view your computer's statistics resulting from advanced monitoring and analysis.


Dell Endpoint Security Suite Enterprise
User
Encryption
D: is not protected
Your system's data is not protected
Sign-In Access
Advanced Threat Prevention
Firewall and Web Protection
Dell Endpoint Security Suite Enterprise v2.0.0

Advanced Threat Prevention Status

Access the Advanced Threat Prevention Status page through the **Advanced Threat Prevention** tile in the Data Security Console.



Status

Advanced Threat Prevention employs artificial intelligence and machine learning to automatically block threats before they are able to execute.

Protection Status: Protected

The Advanced Threat Prevention service is running and Protection Status is enabled.

Advanced Threat Prevention	Enabled
Memory Protection	Enabled

File System

Unsafe Files:	0
Threats Quarantined:	0

Memory Protection

Memory Violations:	0
Blocked Violations:	0

Advanced Threat Prevention

Version:	2.0.1481.1
Installed:	5/7/2018 10:01:24 AM
Last Updated:	5/7/2018 10:01:24 AM

powered by CYLANCE

Dell Endpoint Security Suite Enterprise v2.0.0

Protection Status

The Protection Status indicates whether the computer is Protected (indicated by a green check mark) or Not Protected (indicated by a red X), based on whether the Advanced Threat Prevention service is running and Advanced Threat Prevention is On (Enabled) in the Dell Server.

- Advanced Threat Prevention - Indicates whether Advanced Threat Prevention is On (Enabled) in the Dell Server.
- Memory Protection - Indicates whether Memory Protection is On (Enabled) in the Dell Server.

File System

- Unsafe Files - Number of files on the computer that are likely to be malware.
- Threats Quarantined - Number of files moved from their original locations on the computer and prevented from executing.

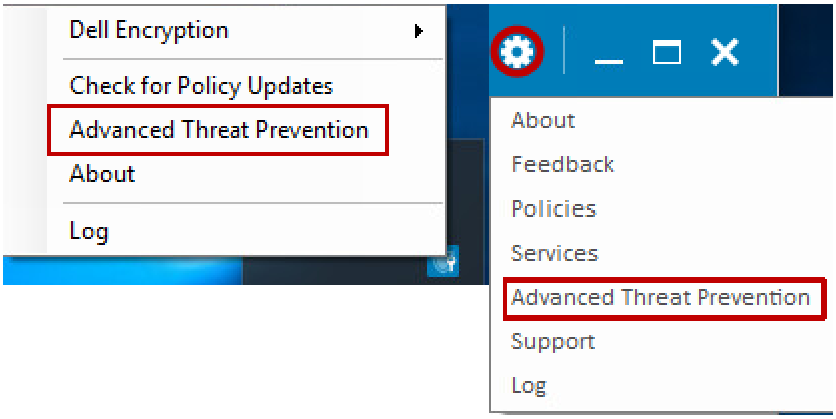
Memory Protection

- Memory Violations - Number of attempts by applications to attach to computer memory.
- Blocked Violations - Number of blocked attempts by applications to attach to computer memory.

Standard UI

Standard UI enables a new feature within the gear menu or systray menu in the Data Security Console that displays detailed information on what events have been captured on a specific endpoint. Standard UI can be enabled **only** if the Standard UI policy is enabled in the Remote Management Console. For additional information, see *AdminHelp* by selecting the **?** in the top right corner of the Remote Management Console.

Standard UI can be enabled in the Data Security Console via the systray icon or gear icon on the left side of the title bar.



Select one of the following options to display verbose Advanced Threat Prevention details:

- **Show Threats**

  The **Show Threats** option displays threats that were mitigated by Advanced Threat Prevention and the following details:

  File Hash ID - Displays the SHA256 hash information for the threat.

  File MD5 - The MD5 hash.

  Currently Running? - Is the threat currently running on the device? Running or Not Running.

  File Path - The path where the threat was found. Includes the file name.

  Score - Ranking of the threat.
- **Show Exploits**

  The **Show Exploits** option displays exploits that were mitigated by Advanced Threat Prevention and the following details:

  Event ID - Unique number assigned to each threat event.

  Process ID - Displays the process ID of the application identified by Memory Protection.

  Process Tag - A unique identifier categorizing processes per boot cycle.

  Image Hash - Displays the SHA256 hash information for the exploit.

  Image Path - The path where the exploit originates. Includes the file name.

  File Version - Displays the version number of the exploit file.
- **Show Scripts**

  The **Show Scripts** option displays scripts that were mitigated by Advanced Threat Prevention and the following details:

  Script Path - The path where the script originates. Includes the file name.

  Event ID - A unique number assigned to each script event.

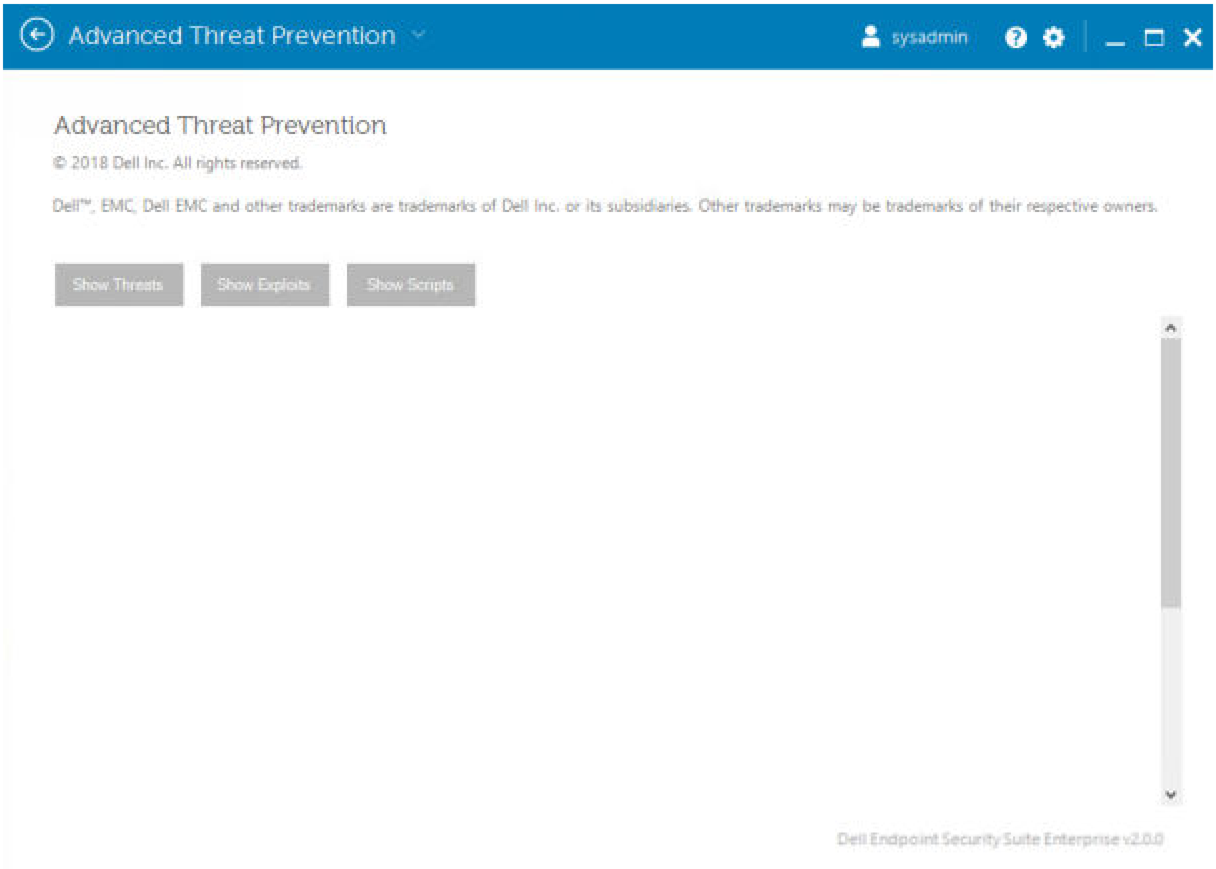
  File Hash ID - Displays the SHA256 hash information for the script.

  File MD5 - The MD5 hash.

  Drive Type - Details if the drive is internal or external.

Interpreter Name - The name of the script control feature that identified the malicious script.

Interpreter Version - The version number of the script control feature.



Advanced Threat Prevention

© 2018 Dell Inc. All rights reserved.

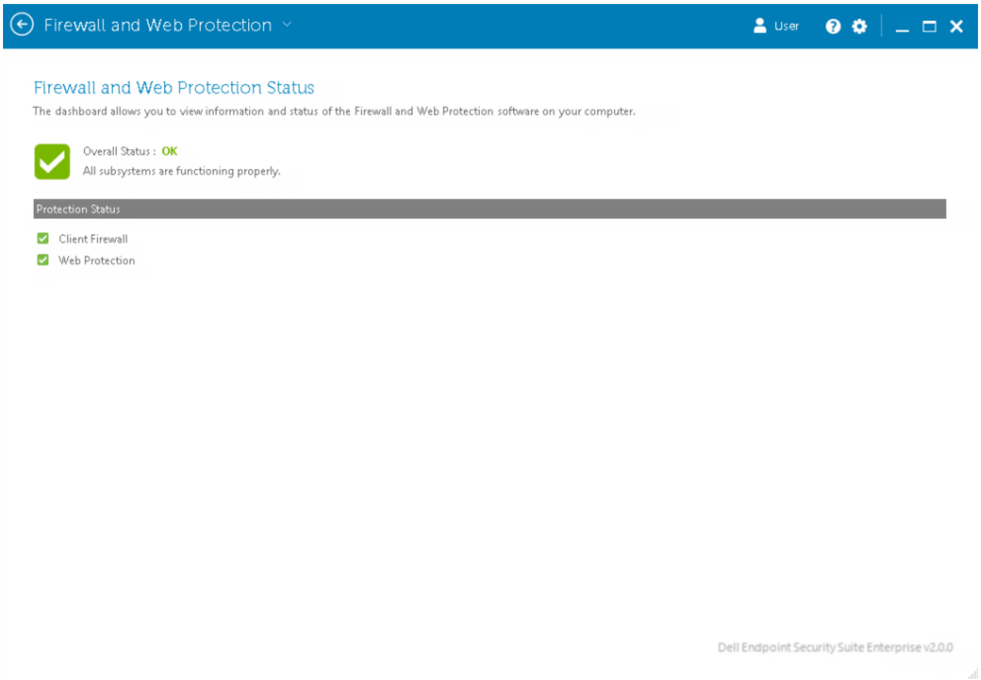
Dell™, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Dell Endpoint Security Suite Enterprise v2.0.0

The displayed list of events is collected when that Data Security Console session is launched. To retrieve new events, close the Data Security Console then re-launch.

Firewall and Web Protection Status

Access the Firewall and Web Protection Status page through the **Firewall and Web Protection** tile in the Data Security Console.



Firewall and Web Protection Status

The dashboard allows you to view information and status of the Firewall and Web Protection software on your computer.

Overall Status : OK

All subsystems are functioning properly.

Protection Status

☑ Client Firewall

☑ Web Protection

Dell Endpoint Security Suite Enterprise v2.0.0

Overall Status

The Overall Status indicates whether the computer is Protected or Vulnerable, based on Firewall and Web Protection policy settings in the Dell Server.

- Protected - Overall Status is Protected if *Web Protection* or *Client Firewall* policies are On (Enabled).
- Vulnerable - Overall Status is Vulnerable if *Web Protection* and *Client Firewall* policies are Off (Disabled).

Protection Status

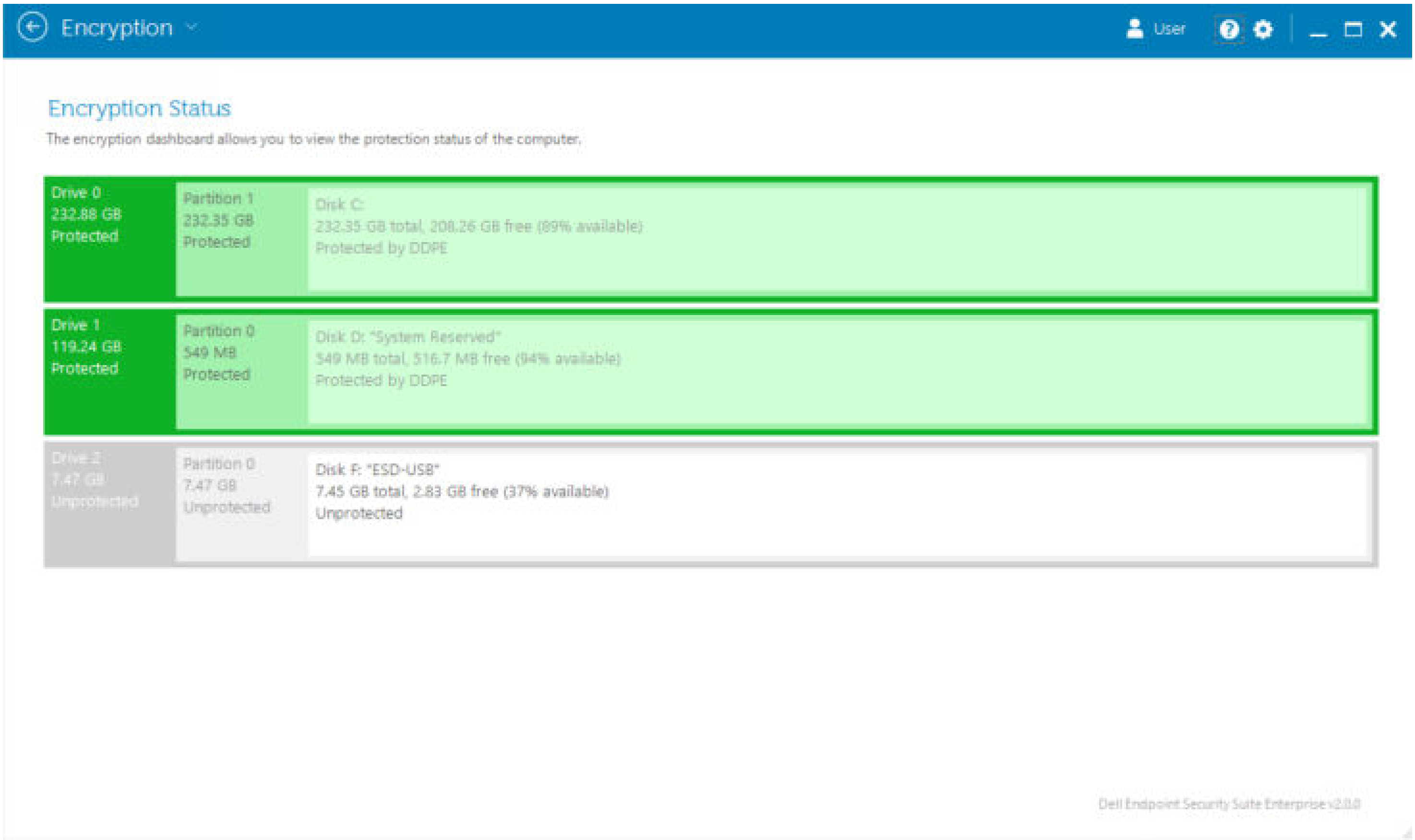
The Protection Status field displays individual status of Protected (indicated by a green check mark) or Vulnerable (indicated by a red X) based on whether the following policies are On (Enabled) in the Dell Server:

- Client Firewall - Overall Status is Protected if the *Client Firewall* policy is On (Enabled).
- Web Protection - Overall Status is Protected if the *Web Protection* policy is On (Enabled).

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**.



Encryption Status

The encryption dashboard allows you to view the protection status of the computer.

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 Endpoint Security Suite Enterprise v2.0.0

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:

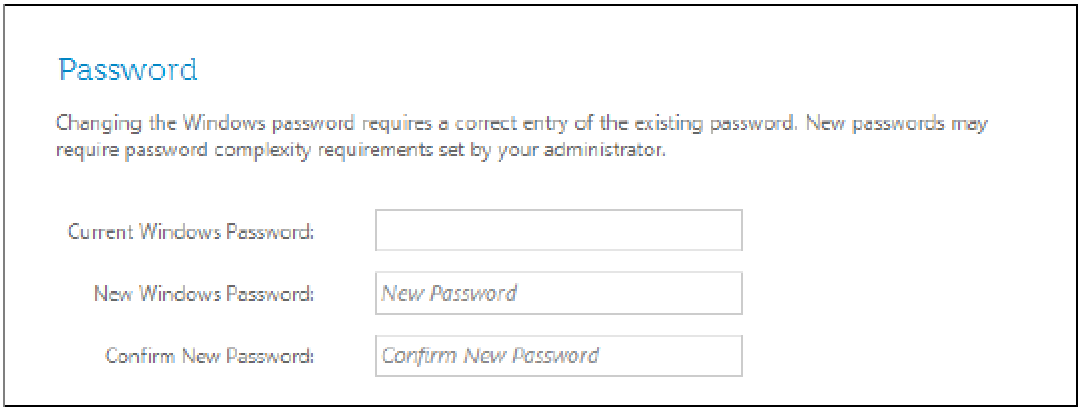
- To enroll a credential for the first time, on the line with the credential, click **Enroll**.
- To delete an existing enrolled credential, click **Delete**.
- If policy does not allow you to either enroll or modify your own credentials, the **Enroll** and **Delete** links on the Status page are inactive.

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.



Password

Changing the Windows password requires a correct entry of the existing password. New passwords may require password complexity requirements set by your administrator.

Current Windows Password:

New Windows Password: New Password

Confirm New Password: Confirm New Password

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 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.

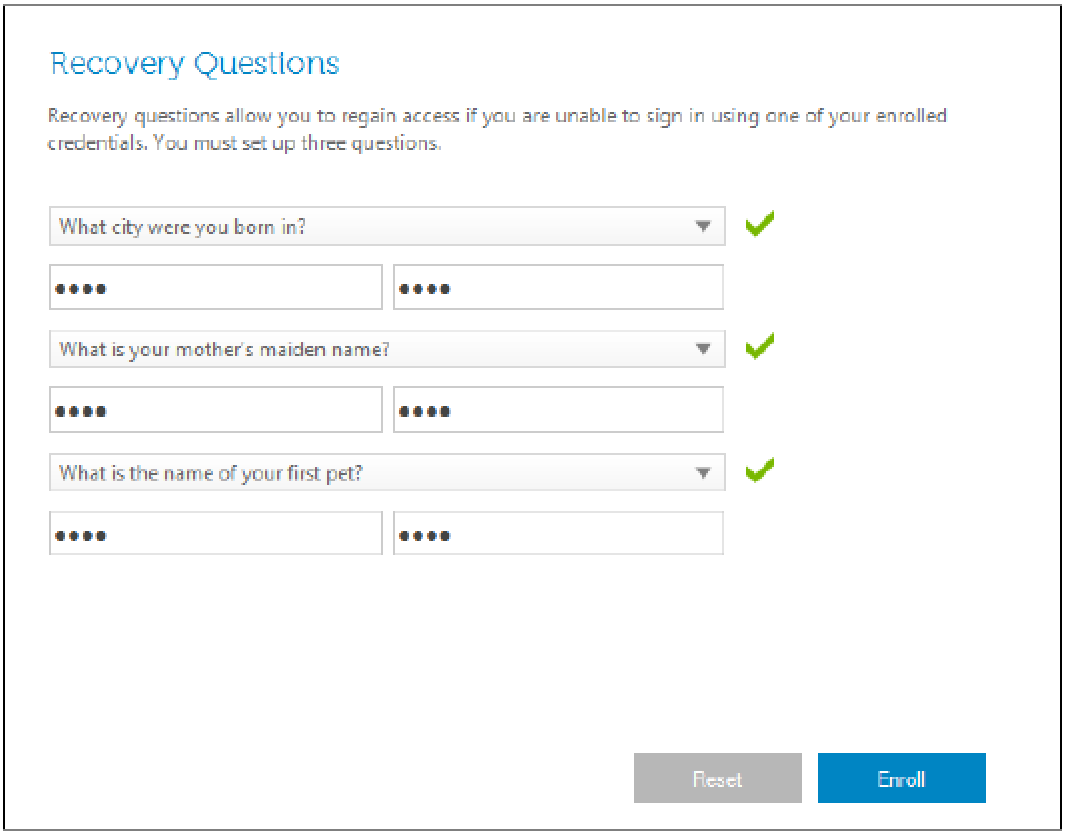
Recovery Questions Already Enrolled

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? ✓

●●●● ●●●●

6

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.