Dell Data Protection | Access Home

The **Dell Data Protection | Access** home page is the starting point for accessing the features of this application. From this window, you can access the following:

Set up secure Access options
Customize Access Options
Self-Encrypting Drive
Advanced

NOTE: If you have a pre-Windows password set or fingerprint enrolled, available options (e.g., change password for pre-Windows login) will be displayed on the home page. The available options are shortcuts which, when clicked, take you to the appropriate window for performing a specific task (e.g., changing your pre-Windows password or enrolling another fingerprint).

Set up Secure Access Options

The Set up secure Access options wizard launches automatically the first time the **Dell Data Protection | Access** application is launched. This wizard will walk you through setting up all aspects of the security on your system, including how (e.g., password only or fingerprint and password) and when (at Windows, pre-Windows or both) you want to login to the system. In addition, if your system has a self-encrypting drive you can configure it through this wizard.

The Set up secure Access options wizard can also be accessed by clicking the link at the top right of the Access or the Self-Encrypting Drive tab.

Administrator Functions

Users who have been set up with Windows administrator privileges on the system have the rights to perform the following functions in **Dell Data Access | Protection**, which standard users cannot:

- Set / change System (Pre-Windows) password
- Set / change Hard Drive password
- Set / change Administrator Password
- Set / change TPM Owner password
- Set / change ControlVault Administrator password
- Reset system
- Archive and restore credentials
- Enable / disable Dell Secure Login to Windows
- Set Windows login policy
- Manage self-encrypting drives, including:
    - Enable / disable self-encrypting drive locking
    - Enable / disable Windows Password Synchronization (WPS)
    - Enable / disable Single Sign On (SSO)
    - Perform a cryptographic erase

Remote Management

Your organization can set up an environment in which the security functions of the **Dell Data Protection | Access** application on multiple platforms are centrally managed (i.e. remote management) by Wave Systems' EMBASSY® Remote Administration Server (ERAS).

In this case, the Windows security infrastructure, such as Active Directory, can be used to securely manage specific features of **Dell Data Protection | Access**.

When a computer is remotely managed (e.g. "owned" by the remote administrator), local administration of the **Dell Data Protection | Access** functionality will be disabled; the management windows of the application will not be accessible locally. Management of the following functions can be done remotely:

- Trusted Platform Module (TPM)
- ControlVault
- Pre-Windows login
- Reset System
- BIOS Passwords
- Windows Login policy
- Self-Encrypting Drives
- Fingerprint and Smartcard enrollment

To request more information on using Wave Systems' EMBASSY® Remote Administration Server (ERAS) for remote management, please contact your Dell salesperson or go to dell.com.

Access Options

From the Access Options window, you can set up how you gain access to your system.

General
First, you can specify when to log in (Windows, pre-Windows or both) and how (e.g. fingerprint and password) to log in. You can choose one or two options for how to login; these include combinations of fingerprint, smartcard, and password. The listed options are based on the login policies applied in your environment and what is supported with thesecurity devices installed on your system.

Fingerprint
If your system contains a fingerprint reader, you can enroll or delete fingerprints for use in logging in to your system. Once you have enrolled fingerprints, you can swipe the enrolled finger(s) on your system's fingerprint reader to access your system at Windows, pre-Windows or both (depending on what you have specified in the General Access Options). Refer to Managing User Fingerprints for more information.

Pre-Windows Login
If you have specified that users must log in pre-Windows, you must set up a System Password (sometimes called the pre-Windows password) for pre-Windows access. Once this is set up, the administrator can change the password at any time.

You can also disable pre-Windows login from this screen; to do this you will need to enter your current System Password, verify that the password is correct, then click the **Disable** button.

Smartcard
If you have specified that users must use a smartcard to log in, you must enroll one or more traditional (contacted) or contactless smartcard(s).Click the **Enroll a smartcard or contactless smartcard to use for login** link to launch the smartcard enrollment wizard. Enrolling means setting up your smartcard for use in logging in.

Once you have enrolled a smartcard, you can enroll another card using the **Enroll another smartcard or contactless smartcard to use for login** link.

Pre-Windows Login

When pre-Windows login is enabled, you must provide authentication (password, fingerprint or smartcard) when the system is powered on, before Windows is loaded. The pre-Windows login functionality provides additional security to the system, keeping unauthorized users from compromising Windows and accessing the computer (e.g., when it has been stolen).

From the Pre-Windows Login window, administrators can enable, change (if it has been previously enabled) or disable pre-Windows (system) login.

Enable Pre-Windows Login:
This action will launch a wizard which will do the following:

- System Password: Set up a System Password (also called a pre-Windows password) for pre-Windows access. This password is also used as a backup in cases in which a user has additional authentication factors (e.g., to gain access to the system if there is an issue with the fingerprint sensor).

Change Pre-Windows Login: If pre-Windows login has already been enabled , the user has the ability to change the password. In order to change the password, user must first enter the current password for verification purposes.

Disable Pre-Windows Login
You can also disable pre-Windows login from this window; to do this you will need to enter your current pre-Windows (System) password, verify that the password is correct, then click the **Disable** button. Note that when you disable pre-Windows login, any enrolled fingerprints or smartcards remain enrolled.

Managing User Fingerprints

Users can register fingerprints which can be used to authenticate to the system either pre-Windows or for Windows login. In the Fingerprint tab, images of hands display which fingers have been enrolled, if any. Clicking on a finger in the image launches the Fingerprint Enrollment wizard, which guides you through the enrollment process. "Enrolling" means saving a fingerprint to be used for login. You must have a valid fingerprint reader properly installed and configured in order to enroll fingerprints.

NOTE: Not all fingerprint readers can be used for pre-Windows login. An error message will display if you attempt to enroll for pre-Windows with an incompatible reader. To find out if the device is compatible, contact your system administrator or go to support.dell.com for a list of supported fingerprint readers.

When enrolling fingerprints, you will be prompted to enter your Windows password to verify your identity. If your policy requires it, you will be prompted to enter your Pre-Windows (System) password as well. The Pre-Windows password can be used to gain access to the system if there is an issue with the fingerprint reader.

NOTES:

- It is recommended that you enroll at least two fingerprints during the enrollment process.
- You must ensure that fingerprints are enrolled before you can enable fingerprint authentication capabilities.
- If you change fingerprint readers on a system, you must re-enroll fingerprints with the new reader. Switching back and forth between two different fingerprint readers is not recommended.
- If you see repeated "sensor lost focus" messages when enrolling fingerprints, this may mean that the computer is not recognizing the fingerprint reader. If the fingerprint reader is external, disconnecting and reconnecting the fingerprint reader often resolves this issue.

Deleting Enrolled Fingerprints

The current user can remove an enrolled fingerprint by clicking on (to de-select) the enrolled finger in the Fingerprint Enrollment wizard.

An administrator can only remove stored fingerprints for another user by using the Reset System option, which will remove ALL fingerprints for all users on the system.

NOTE: If you get any errors during the fingerprint enrollment process, you can refer to support.dell.com for additional details.

Enrolling Smartcards

Dell Data Protection | Access gives you the option of using a traditional (contacted) or contactless smartcard for logging into your Windows account or for authentication at pre-Windows. In the Smartcard tab, click the **Enroll a smartcard or contactless smartcard to use for login** link to launch the Smartcard Enrollment wizard, which guides you through the enrollment process. "Enrolling" means setting up your smartcard for use in login. Once you have enrolled a smartcard, you can enroll another card using the **Enroll another smartcard or contactless smartcard to use for login** link.

You must have a valid smartcard authentication device properly installed and configured in order to perform enrollment.

NOTE: To find out if a specific device is compatible, contact your system administrator or go to support.dell.com and search for 'smartcard readers'.

Contactless smartcards supported for Windows and pre-Windows enrollment:

- HID Mifare
- HID Crescendo - C700, C200
- HID I- Class – 2080, 200X, 210X, 201X, 211X, 202X, 212X, 203X, 213X, 204X, 214X, 205X, 206X series cards.

Contacted smartcards supported for pre-Windows enrollment:

- CAC and PIV (US Federal Government Cards)

Enrollment
When enrolling a smartcard you will be prompted to enter your Windows password to verify your identity. If your policy requires it, you will be prompted to enter your pre-Windows (System) password as well. The pre-Windows password can be used to gain access to the system if there is an issue with the smartcard reader.

During enrollment, you will be prompted for the smartcard PIN, if one has been set. If your policy requires a PIN and one has not been set, you will be prompted to create one.

NOTES:

- Once a user is enrolled for smartcard use in pre-Windows, he/she can be removed with Reset System.
- Reset System is the only way to reset a smartcard; the smartcard cannot be used for authentication at Windows login or for pre-Windows until it is re-enrolled.

NOTE: For TPM certificate authentication, administrators can enroll TPM certificates through the Microsoft Windows smartcard enrollment process. Administrators must select "Wave TCG-Enabled CSP" as the Cryptographic Service Provider in place of a Smartcard CSP for compatibility with this application. In addition, Dell Secure login must be enabled with the appropriate Authentication Type Policy for the client.

NOTE: If you get an error that states that the Smartcard Service is not running, you can start / restart this service by doing the following:

- Navigate to the Administrative Tools window from the Control Panel, select Service, then right-click on Smartcard and select Start or Restart.
- Detailed information on the specific error message for Dell Data Protection | Access (DDP|A) can be found by searching for “DDPA Error Codes” at: http://support.dell.com.

Self-Encrypting Drive

Dell Data Protection | Access manages the hardware-based security functions of self-encrypting drives, which have data encryption embedded in the drive hardware. This functionality is used to ensure that only authorized users can access encrypted data (when drive locking is enabled).

The Self-Encrypting Drive window is accessed by clicking the **Self-Encrypting Drive** bottom tab. This tab displays only when one or more self-encrypting drives (SEDs) are present on your system.

Click the **Setup** link to begin the Self-Encrypting Drive setup wizard. In this wizard, you will create a Drive Administrator password, back up this password, and apply your drive encryption settings. Only system administrators can access the Self-Encrypting Drive setup wizard.

Important! Once the drive has been set up, data protection and drive locking are "enabled". When a drive is locked, the following behavior applies:

- The drive enters into *locked* mode whenever power to the drive is turned off.
- The drive will not boot unless the user enters the correct username and password (or fingerprint) at the Pre-Windows login screen. Before drive locking is enabled, the data on the drive is accessible to any user on the computer.
- The drive is secured even if plugged into another computer as a secondary drive; authentication is required to access the drive data.

Once the drive has been set up, the Self-Encrypting Drive window will display the drive(s) and a link for users to change their drive password. If you are a drive administrator, you will also be able to add or remove drive users from this window. If there is an external drive that has been set up, it will display on this window and can be unlocked.

NOTE: To lock a secondary, external drive, the drive must be powered off independently from the computer.

The drive administrator can manage the drive settings in **Advanced>Devices**. For more information, see Device Management - Self-Encrypting Drives.

Drive Setup

The Self-Encrypting Drive setup wizard will guide you through setting up your drive(s). The following concepts are important to keep in mind when going through this process.

Drive Administrator
The first user with system administrator rights who sets up drive access (and sets the Drive Administrator password) becomes the Drive Administrator; this is the only user with rights to make changes to drive access. To ensure that the first user is intentionally being set up as the drive administrator, you must select the "I understand" checkbox to continue with this step.

Drive Administrator Password
The wizard will prompt you to create a Drive Administrator password and to re-enter the password as a confirmation. You must enter your Windows password to establish your identity before you can create your Drive Administrator password. The current Windows user must have administrator rights to create this password.

Backup Drive Credentials
Type in a location, or click the **Browse** button to select a location, to save a backup copy of your drive administrator credentials.

IMPORTANT**!**

- It is highly recommended that you back up these credentials, and that you back them up to a drive other than your primary hard drive (e.g. removable media). Otherwise, if you lose access to your drive you will not be able to access your backup.
- Once you complete drive setup, any users will have to enter the correct username and password (or fingerprint), before Windows loads, to access the system the next time the system is powered up.

Add Drive User

The drive administrator can add other users to the drive who are valid Windows users. When adding users to the drive, the administrator has the option of requiring the user to reset their password on first login. The user will be required to reset their password on the pre-Windows authentication screen before the drive will unlock.

Advanced Settings

- *Single Sign On* - By default, your Self-Encrypting Drive password, which you enter pre-Windows in order to authenticate to the drive, will be used to automatically sign you into Windows as well (this is called "Single Sign On"). To disable this feature, select the "I want to login again when Windows starts" checkbox when configuring your drive settings.
- *Fingerprint Login* - On supported platforms, you can specify that you want to authenticate to your self-encrypting drive using a fingerprint instead of a password.
- *Sleep/Standby (S3) Support* (if supported on platform) - If enabled, your self-encrypting drive can securely be placed in to Sleep/Standby mode (also called S3 mode) and will require pre-Windows authentication when resuming from Sleep/Standby mode.

NOTES:

- When S3 Support is enabled, drive encryption passwords are subject to any BIOS password limitations that may exist. Consult the system hardware manufacturer for more information on any specific BIOS password limitation that may exist for the system.
- Not all self-encrypting drives support S3 mode. During drive setup, you will be notified whether or not the drive supports Standby/Sleep mode. For drives which do not support this mode, Windows S3 requests will automatically be converted to hibernation requests, if hibernation mode is enabled (it is strongly recommended that you enable hibernation mode on your computer).
- The first time you log in after the Single Sign On (SSO) option is set, the process will pause at the Windows login prompt. You will be required to enter your form of Windows authentication, which will be stored securely for future Windows login attempts. The next time the system is booted, SSO will automatically log you into Windows. The same process is also required when a user's Windows authentication (password, fingerprint, Smartcard PIN) changes. If the computer is on a domain, and that domain has a policy that requires ctrl+alt+del be pressed for Windows login, this policy will be respected.
- If the Hard Drive (BIOS) password has been set up, you will not be able to set up the self-encrypting drive.

CAUTION! If you uninstall the **Dell Data Protection | Access** application, you must first disable self-encrypting drive data protection and unlock the drive.

Self-Encrypting Drive User Functions

Self-encrypting drive administrators perform all of the management of the drive security and users. Drive users who are not the drive administrator can perform only the following tasks:

- Change their own drive password
- Unlock a drive

These tasks can be accessed from the **Self-Encrypting Drive** tab in **Dell Data Protection | Access**.

Change Password
This enables enrolled users to create their new drive authentication password. You must enter your current Self-Encrypting Drive password before the drive password is set to the new value.

NOTES:

- The application will enforce the Windows password length and password complexity policies, if they are enabled. If Windows password policies are not enabled, the maximum length for a Self-Encrypting Drive password is 32 characters. Note that this maximum length is 127 characters if S3 (Sleep/Standby) is not enabled.
- A user's Self-Encrypting Drive password is separate from their Windows password. When a user's Windows password is changed or reset it has no effect on the user's drive password, unless Windows Password Synchronization has been enabled. Refer to Devices: Self-Encrypting Drives for details.

Drive Unlock
Drive Unlock enables an enrolled drive user to unlock a locked drive. If drive locking is enabled, the drive enters into the locked state whenever the computer power is turned off. When the system is powered back up, you must authenticate to the drive by entering your password in the pre-Windows authentication screen.

NOTES:

- **The inability to enter into a power saving mode (i.e. Sleep/Standby or Hibernation) may be experienced if multiple self-encrypting drive user accounts are concurrently active on the computer.**

Advanced Options

The Advanced options in **Dell Data Protection | Access** enable a user with administrator privileges to manage the following aspects of the application:

Maintenance
Passwords
Devices

NOTE: Only users with administrator privileges can make modifications in the Advanced options; standard users can view these settings but cannot make any changes.

From the advanced options, you can click the home link in the bottom right of the window to return to the home page.

Maintenance

The Maintenance window can be used by administrators to set up Windows login preferences, reset a system to prepare it to be repurposed, or to archive or restore user credentials stored in the system's security hardware. Refer to the following topics for details:

Access Preferences
Reset System
Credential Archive & Restore

Access Preferences

The Access Preferences window lets administrators specify Windows login preferences for all users of the system.

Enable Dell Secure login
The option to replace the standard Windows ctrl-alt-delete screen enables you to use different factors of authentication instead of (or in addition to) the Windows password for access to Windows. You can choose to add a fingerprint as a second factor of authentication in order to strengthen the security of the Windows login process. Additional factors of authentication can also be added for logging into Windows, including a smartcard or TPM certificate.

NOTES:

- Enabling Dell Secure login affects all users on the system.
- This option is available only AFTER users have enrolled their fingerprints or smartcard.
- The first time you log in after this option is set, you will be prompted to authenticate to Windows according to your standard policy, and then you will need to use your new authentication factor(s) on the next startup.

Disable Dell Secure login
This option disables all **Dell Data Protection | Access** functions for logging into Windows. When this is selected, you will revert to your standard Windows login policy.

NOTES:

- If you get an error concerning Secure Windows login when you are attempting to log in, disable and re-enable the Dell Secure login option.
- Detailed information on the specific error message for Dell Data Protection | Access (DDP|A) can be found by searching for “DDPA Error Codes” at: http://support.dell.com.

Reset System

The Reset System function is used to clear all user data from all security hardware on the platform; this is used, for example, for repurposing a computer. This option will clear all passwords on the system, except for the Windows user passwords, as well as all data in the hardware devices (i.e. ControlVault, TPM and fingerprint readers). Credentials for Smartcards will also be cleared. For self-encrypting drives, this function also disables data protection so the drive data is accessible.

You must confirm that you understand that you are resetting the system, then click **Next**. To reset the system, first you will be required to confirm your identity by entering your Windows password; then you must enter the password for each security device, if they have been set:

- TPM Owner
- ControlVault Administrator
- BIOS Administrator
- BIOS System (pre-Windows)
- Hard Drive (BIOS)
- Self-Encrypting Drive Administrator

NOTE: For self-encrypting drives, only the Drive Administrator password is required; not all of the drive users' passwords.

Important! The only way to recover any of the data cleared when you reset the system is to restore from a previously-saved archive. If you do not have an archive, this data is unrecoverable. For a self-encrypting drive, only the setup data is deleted; no personal data on the drive is deleted.

Credential Archive & Restore

The Credential Archive and Restore functionality is used to back up and restore all user credentials (login and encryption information) stored in the ControlVault and Trusted Platform Module (TPM). A backup of this data is important when re-provisioning a computer or for restoring data in the case of hardware failure. In this case, you can simply restore all of your credentials to your new computer from a saved archive file.

The user credentials consist of data used in pre-Windows or Windows, such as enrolled fingerprints and smartcard data, and keys stored in the TPM. The TPM will create keys as requested by secure applications; for example, generating a digital certificate will create keys in the TPM.

NOTE: To determine if the TPM keys are able to be archived by Dell Data Protection | Access, please consult the documentation for the secure application.

Archiving Credentials
To archive credentials, you must do the following:

- Provide authentication to the security hardware by entering the System (pre-Windows) password, ControlVault Administrator password and TPM Owner password.
- Create a credential backup password.
- Specify an archive location, using the **Browse** button. The archive location should be removable media, such as a USB flash drive or network drive, to protect against a hard drive failure.

Important Notes:

- Make note of the archive location as the user will need this information to restore the credential information.
- Make note of the credential backup password to ensure that data can be restored. This is important as this password cannot be recovered.
- If you do not know the TPM Owner password, contact the system administrator or refer to the computer's TPM setup instructions.

Restoring Credentials
To restore credentials, you must do the following:

- Browse to the archive location, and select the archive file.
- Enter the credential backup password that was created when you set up the archive.
- Provide authentication to the security hardware by entering the System (pre-Windows) password, ControlVault Administrator password and TPM Owner password.

NOTES:

- If you get an error stating that TPM keys could not be restored, create a credential archive, then clear the TPM in the BIOS. To clear the TPM, reboot your computer, press the **F2** key when starting back up to access the BIOS settings, then navigate to Security>TPM Security >Clear TPM. Then re-establish ownership of the TPM and attempt to restore credentials again.
- Detailed information on the specific error message for Dell Data Protection | Access (DDP|A) can be found by searching for “DDPA Error Codes” at: http://support.dell.com.

Password Management

From the Password Management window, an administrator can create or change all of the security passwords on your system:

- System (also known as Pre-Windows)*
- Administrator*
- Hard Drive*
- ControlVault
- Windows
- TPM Owner
- Self-Encrypting Drive

NOTES:

- Only those passwords that are applicable to the current platform configuration will be displayed; so this window will change based on the system configuration and status.
- Those passwords with an * next to them above are BIOS passwords and can also be changed through the system BIOS.
- The BIOS-level passwords cannot be created or changed if the BIOS administrator has denied password changes.
- Clicking the **setup** link for a self-encrypting drive launches the Self-Encrypting Drive setup wizard; clicking **manage** lets a user to change one or more Self-Encrypting Drive passwords.
- Only one drive password – Hard Drive (BIOS) or Self-Encrypting Drive - can be set up at a time. If one of these is set, the other will be unavailable.

Windows Password Complexity Rules

Dell Data Protection | Access ensures that the following password conforms to the Windows password complexity rules for the machine:

- TPM Owner password

To determine the Windows password complexity policy for a machine, follow these steps:

1. Access the Control Panel.
2. Double-click Administrative Tools.
3. Double-click Local Security Policy.
4. Expand Account Policies and select Password Policy.

Devices

The Devices window is used by administrators to manage all of the security devices installed on their system. For each device, you can view the status and additional detailed information, such as the firmware version. Click **show** to view the information for each device, or **hide** to collapse that section. The devices which can be managed are the following, depending on which your platform contains:

Trusted Platform Module (TPM)
ControlVault®
Self-Encrypting Drive(s)
Authentication Device Information

Trusted Platform Module (TPM)

The TPM security chip must be enabled and ownership of the TPM must be established in order to use the advanced security features available with **Dell Data Protection | Access** and the TPM.

The Trusted Platform Module window in **Device Management** displays only when a TPM is detected on your system.

TPM Management

These functions enable the system administrator to manage the TPM.

Status

Displays a status of *active* or *inactive* for the TPM. A status of "Active" means that the TPM has been enabled in the BIOS and is ready to be set up (i.e., ownership can be taken). The TPM cannot be managed and its security features cannot be accessed if the TPM is not active (enabled).

If the TPM is detected on the system but is not active (enabled), you can enable it by clicking the **activate** link on this window, without entering the system BIOS. After enabling the TPM using this feature, the computer must be rebooted. During the reboot, a prompt will appear in some cases, asking you to accept the changes.

NOTE: The ability to enable (activate) the TPM from this application may not be supported on all platforms. If it is not supported, you must enable it in the system BIOS. To do this, reboot your system, press the **F2** key before Windows loads to enter the BIOS setup, then navigate to Security>TPM Security and activate the TPM.

You can also *deactivate* the TPM from here by clicking the **deactivate** link; deactivating the TPM will make it unavailable for the advanced security features. Deactivating does not, however, change any of the TPM settings or delete or change any information or keys stored in the TPM.

Owned

Displays the status of ownership (i.e. "owned") and lets you establish or change the TPM owner. TPM ownership must be established for its security features to be available. Before ownership may be established, the TPM must be enabled (activated).

The process for establishing ownership consists of the user (with administrator privileges) creating a TPM Owner password. Once this password is defined, ownership is established and the TPM is ready for use.

NOTE: The TPM Owner password must conform to the Windows password complexity rules for your system.

Important! It is important that you do not lose or forget the TPM Owner password, as it is required for access to advanced security functions for the TPM in **Dell Data Protection | Access**.

Locked

Displays a status of *locked* or *unlocked* for the TPM. "Locking" is a security feature of the TPM; the TPM will enter a locked state after a specified number of incorrect TPM Owner password entries are made. The TPM owner can unlock the TPM from here; entry of the TPM Owner password is required.

NOTES:

- If you get an error stating that TPM ownership could not be established, clear the TPM in the system BIOS and attempt to establish ownership again. To clear the TPM, reboot your computer, press the **F2** key when starting back up to access the BIOS settings, then navigate to Security>TPM Security>Clear TPM.
- If you get an error stating that the TPM Owner password could not be changed, archive the TPM data (credential archive), clear the TPM in the BIOS, re-establish ownership of the TPM and restore TPM data (restore credentials).
- Detailed information on the specific error message for Dell Data Protection | Access (DDP|A) can be found by searching for “DDPA Error Codes” at: http://support.dell.com.

Dell ControlVault®

The Dell ControlVault® (CV) is a secure hardware store for user credentials used during pre-Windows login (e.g., user passwords or enrolled fingerprint data). The ControlVault window in **Device Management** displays only when a ControlVault is detected on your system.

ControlVault Management

These functions enable the system administrator to manage the system's ControlVault.

Status

Displays a status of *active* or *inactive* for the ControlVault. A status of "Inactive" means that the ControlVault is not available for storage on your system. Consult the Dell system documentation to determine if the system contains a ControlVault.

Password

Indicates whether the ControlVault Administrator password has been set up, and lets you set up a password or change the password (if one has already been set up). Only system administrators can set up or change this password. A ControlVault Administrator password must be set in order to perform a credential archive or restore.

NOTES:

- If an archive or restore is attempted when the ControlVault Administrator password has not been set, he/she is prompted to create one (if they are an administrator).
- If you need to clear user credentials, you must perform a System Reset from the Maintenance section.
- Detailed information on the specific error message for Dell Data Protection | Access (DDP|A) can be found by searching for “DDPA Error Codes” at: http://support.dell.com.

Self-Encrypting Drives: Advanced

Dell Data Protection | Access manages the hardware-based security functions of self-encrypting drives, which have data encryption embedded in the drive hardware. This management is used to ensure that only authorized users can access encrypted data when drive locking is enabled.

The Self-Encrypting Drive window in **Device Management** displays only when one or more self-encrypting drives (SED) are present on your system.

Important! Once the drive has been set up, self-encrypting drive data protection and drive locking are "enabled".

Drive Management
These functions enable the drive administrator to manage drive security settings. Changes to drive security settings take effect after the drive has been powered off.

Data Protection
Displays a status of *enabled* or *disabled* for the self-encrypting drive data protection. A status of "enabled" means that drive security has been set up; however, until drive *locking* has been turned on, users will not have to authenticate to the drive at pre-Windows for access.

You can disable self-encrypting drive data protection from here. When it is disabled, all advanced security functions of the self-encrypting drive are turned off and the drive acts as a standard drive. Disabling data protection also deletes all the security settings, including the credentials of the drive administrator and the drive users. This function does not, however, alter or remove any user data on the drive.

NOTE: If the Hard Drive (BIOS) password has been set up, you will not be able to set up the self-encrypting drive.

Locking
Displays a status of *enabled* or *disabled* for the self-encrypting drive(s). Refer to the Self-Encrypting Drive topic for information on locked drive behavior.

It may be necessary to temporarily disable drive locking, which you can do from here. This is not recommended as no credentials are required to access the drive when drive locking is disabled, so any platform user can access the drive data. Disabling drive locking does not delete any of the security settings, including the credentials of the drive administrator and the drive users, or any user data on the drive.

CAUTION! If you uninstall the Dell Data Protection | Access application, you must first disable self-encrypting drive data protection and unlock the drive.

Drive Administrator

Displays the current drive administrator. The drive administrator can change which user is the drive administrator from here. The new administrator must be a valid Windows user on the system with administrator privileges. There can be only one drive administrator on the system.

Drive Users

Displays the enrolled drive users, and the number of users currently enrolled. The maximum number of users supported is based on the self-encrypting drive (currently 4 users for Seagate drives and 24 for Samsung drives).

Windows Password Sync
The Windows password synchronization (WPS) feature automatically sets users' Self-Encrypting Drive passwords to be the same as their Windows password. This function is not enforced for the drive administrator; it is applicable only to the drive users. The WPS functionality can be used in enterprise environments in which passwords must be changed at specific time intervals (e.g. every 90 days); with this option enabled, all users' self-encrypting drive passwords will be updated automatically when these Windows passwords are changed.

NOTE: When Windows password synchronization (WPS) is enabled, a user's Self-Encrypting Drive password cannot be changed; their Windows password must be changed in order to automatically update the drive password.

Remember Last Username
When this option is enabled, the last username entered will be displayed by default in the **Username** field of the pre-Windows authentication screen.

Username Selection
When this option is enabled, users can view all drive usernames in the **Username** field of the pre-Windows authentication screen.

Cryptographic Erase
This option can be used to "erase" all data on the self-encrypting drive. This does not actually erase the data, but deletes the keys used to encrypt the data, thereby making that data unusable. There is no way to recover drive data after cryptographic erase; also, self-encrypting drive data protection is disabled and the drive is ready to be repurposed.

NOTES:
- If you get any errors related to the self-encrypting drive management functions, completely power down your computer (not a reboot), and restart.
- Detailed information on the specific error message for Dell Data Protection | Access (DDP|A) can be found by searching for "DDPA Error Codes" at: http://support.dell.com.

Authentication Device Information

The Authentication Device Information window in **Device Management** displays information and a status for all connected authentication devices (i.e. fingerprint reader, traditional or contactless smartcard reader) on the system.

Technical Support

Technical support for the **Dell Data Protection | Access** software can be found at http://www.wave.com/http://support.dell.com. Choose Home, Small Business or Enterprise, then enter your Dell service tag number or select your Dell product from the dropdown list.