



Simplifying Encryption and Authentication

Trusted Drive Manager

User Guide



Version 1.4

A Component of **EMBASSY®** Trust Suite

This document guides the user through the setup and basic feature set of Wave Systems' Trusted Drive Manager, providing full lifecycle management of self-encrypting hard disk drives

Wave Systems Corp.
480 Pleasant Street, Lee, MA 01238
www.wave.com

Table of Contents

Overview.....	3
What is the Trusted Drive Manager?.....	3
Key Features of Trusted Drive Manager	3
Getting Started	4
Required Components	4
Configure the Trusted Drive Manager Software	4
Simple User Experience	11
Use the Trusted Drive Manager Software to View and Manage Security Settings	12
View the Status of the FDE drive	12
View and Perform Advanced Functions (Administrators Only).....	14
Un-Initialize the FDE drive	15
Disable Drive Locking.....	15
Back Up Administrator’s Credentials.....	15
Change Administrator’s Credentials	16
Cryptographic Drive Erase	16
Single Sign-On (SSO) for the FDE drive	16
Windows Password Synchronization (WPS) for the FDE drive.....	16
<i>Change FDE drive Password while Windows Password Synchronization (WPS) is Disabled (default)</i>	17
Add FDE drive Users.....	17
In Case of a Forgotten FDE drive Password at Preboot (remotely managed client)	17
Evaluating the Trusted Drive Manager Software	18
What to Look For	18
Technical Support	18

Table of Figures

Figure 1: Main Screen of the Security Setup Wizard.....	5
Figure 2: Configure FDE drive in the Security Setup Wizard	6
Figure 3: FDE drive Initialization Wizard.....	7
Figure 4: Back Up Administrator’s Credentials.....	8
Figure 5: Add FDE drive User	9
Figure 6: Wizard Completion	9
Figure 7: Preboot Authentication to the Drive.....	11
Figure 8: Desktop.....	12
Figure 9: EMBASSY® Security Center	13
Figure 10: FDE drive Tab.....	14
Figure 11: FDE drive - Advanced Settings	15

Overview

Self-encrypting hard drives take data protection to a new level by integrating encryption and advanced security features directly into the hard drive. If the computer or drive gets lost or stolen, the organization can have the utmost confidence that the data within the drive will remain secure.

The purpose of this guide is to demonstrate the advanced security features available with Wave's EMBASSY Trusted Drive Manager (TDM) software for any [TCG Opal standards-compliant](#) FDE fully encrypting hard drive (simply called self-encrypting drives or FDE drives in this guide). The TDM software is included in the EMBASSY® Security Center, a key component of Wave's EMBASSY® Trust Suite (ETS). Beyond the FDE Drive management functions, ETS provides the premier tools for using the advanced security of Trusted Platform Module (TPM) security chips, which are embedded in most new business-class PCs and laptops. Even though the FDE Drives and TPMs are managed in the same unified security console, each device can be used and managed independently.

To learn more about the Wave Systems EMBASSY® Trust Suite and its tools for Trusted Computing, please visit www.wave.com.

What is the Trusted Drive Manager?

Wave's Trusted Drive Manager handles all of the self-encrypting hard drive's lifecycle functions from initializing the advanced security features for user authentication and security policy setup to drive de-commissioning. A FDE drive with the Wave pre-boot authentication feature enforces access control policies whenever the drive powers up. Only authorized users will be able to unlock the drive and access the data. Out of the box, FDE drives operate as standard drives and even though the hardware encryption is always on, there is no security enforced or user authentication needed for accessing the data. Wave's TDM is used to turn on the security features and manage all the advanced security functions provided in the drives hardware and firmware. Once the drive has been set up or "initialized", the user experience is designed to be extremely simple and non-obtrusive. The drive will lock whenever the system is shut down and upon power up the user must enter their credentials to unlock the drive. After that, the drive security will be completely invisible to the user, including no performance impact.

Key Features of Trusted Drive Manager

- Drive initialization
- Pre-boot authentication setup
- Drive user management
- Drive de-commissioning
- Back-up and recovery of drive access credentials

Getting Started

Required Components

To start, you will need the following components:

- **Client Computer:** Laptop with Microsoft Windows XP SP2 or Windows Vista with any [TCG Opal-compliant](#) FDE Hard Disk Drive.
- **Trusted Drive Manager Software:** The EMBASSY® Security Center contains the Trusted Drive Manager (TDM) plug-in.

Configure the Trusted Drive Manager Software

Trusted Drive Manager can be configured in several places.

- From the EMBASSY Security Setup Wizard
- From the Trusted Drive Manager tab in EMBASSY Security Center
- From the [EMBASSY Remote Administration Server](#) Console
- On Dell Precision and E-Series laptops that come pre-loaded with EMBASSY Trust Suite and Trusted Drive Manager, from the Dell ControlPoint Security Manager module

This guide will describe the steps to configure the FDE drive from the EMBASSY Security Setup Wizard.

To Launch the EMBASSY Security Setup Wizard:

1. Log on to the computer and ensure that you have administrative privileges for the PC.
2. Click **I Accept** when the End User License Agreement appears.
3. If the Embassy Security Setup Wizard does not appear automatically, launch **C:\Program Files\Wave Systems Corp\EMBASSY Security Setup\EmbassySetupWizard.exe** (see Figure 1).



Figure 1: Main Screen of the Security Setup Wizard

4. Press **Next** twice to get to the Configure FDE drive screen. Ensure that the box next to **Initialize FDE drive** is checked and press **Next** (see Figure 2)

NOTE: If the Trusted Platform Module (TPM) security chip is enabled, you will see additional options in this wizard for configuring TPM security. These do not relate to or affect the operation of the FDE drive in any way. For simplicity, we show you the screens without the additional options.

The TPM security chip is enabled through the BIOS. Consult your PC manufacturer's documentation for information on the TPM security chip and accessing the settings in the BIOS.

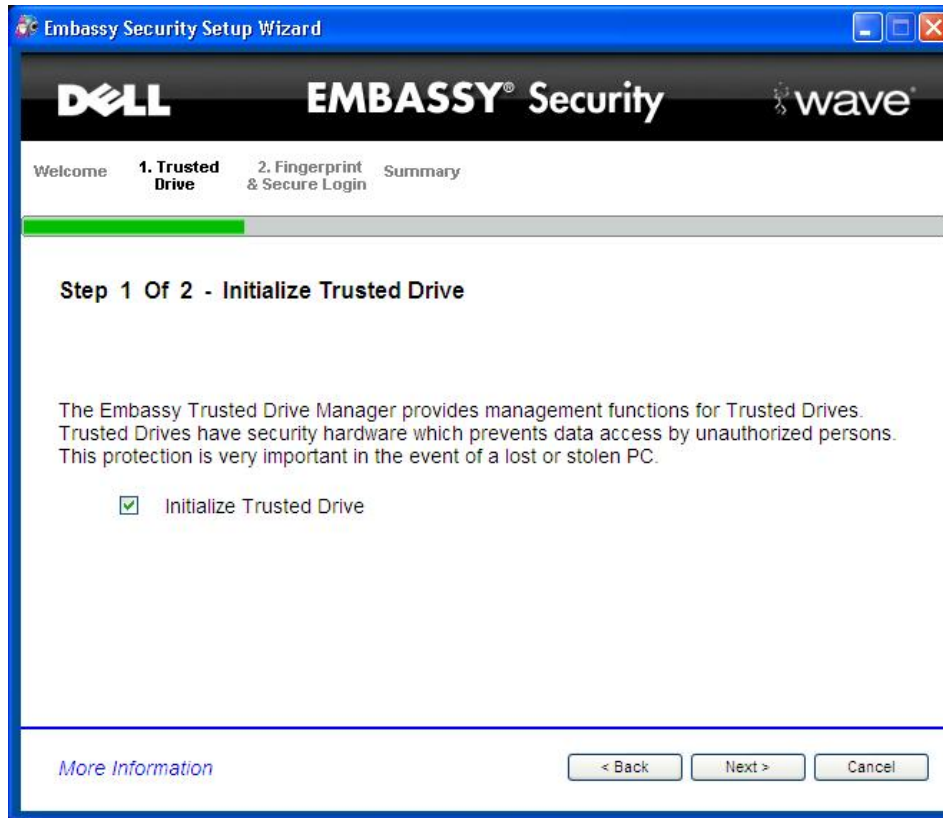


Figure 2: Configure FDE drive in the Security Setup Wizard

5. A confirmation prompt will appear, explaining that by initializing the FDE drive, this adds an additional level of preboot authentication. Click **Yes** to proceed. Next, the FDE drive Initialization Wizard will appear (see Figure 3). Initialization will turn on the advanced security features of the self-encrypting drive for strong access control and will install a pre-boot environment in a protected area of the drive which will be used to authenticate the users before the FDE drive is unlocked at power up time. To establish yourself as the drive administrator, enter your username that you used to log into the computer (if not already filled in) and create a password. This will be the pre-boot password that you will need when powering up the FDE drive. This does not have to be the same password as your Windows logon password, but it *does* need to meet the same password complexity requirements. Press **Next**.



Figure 3: FDE drive Initialization Wizard

6. Select a location off of the local hard drive to store the administrator's username and password for recovery purposes (see Figure 4).



Figure 4: Back Up Administrator's Credentials

7. The drive administrator that you created above will be the FDE drive administrator. Next, you can add other valid Windows users as FDE drive users if other people will be using the PC (see Figure 5). Up to four users can be added, each with their own unique pre-boot password.

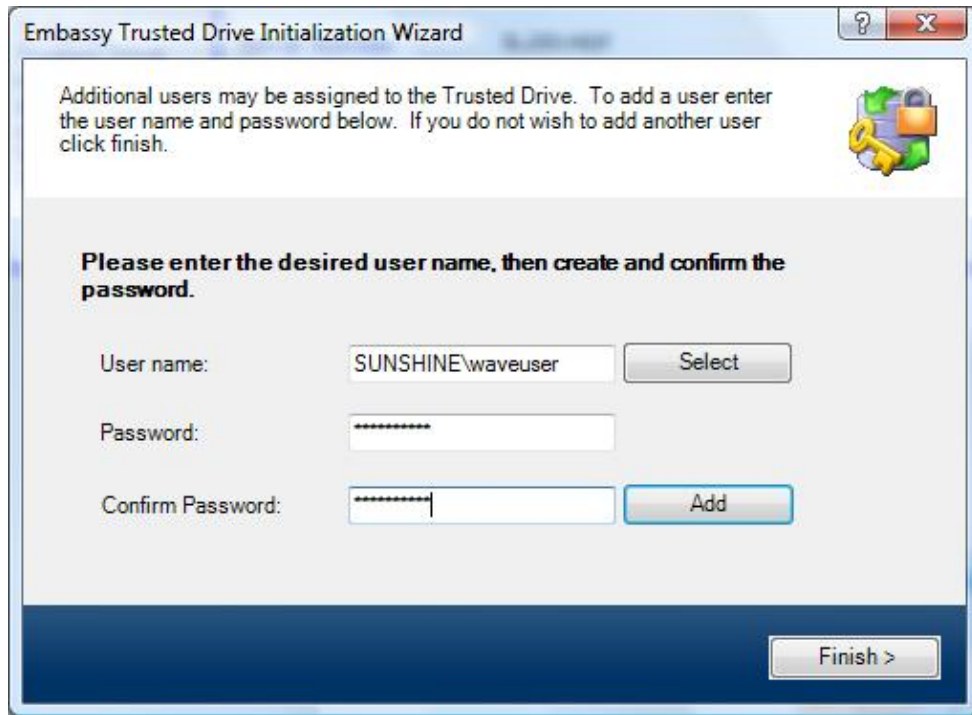


Figure 5: Add FDE drive User

8. Click **Finish** and **Done** to exit the FDE drive Initialization Wizard (see Figure 6).

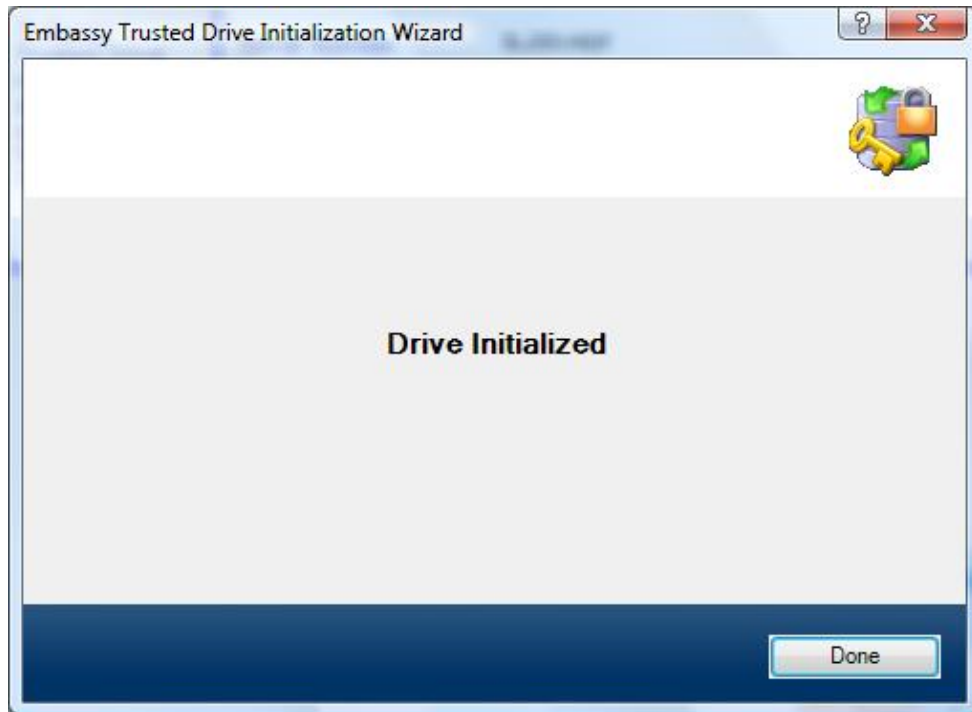


Figure 6: Wizard Completion

9. View the status and click **Finish** to exit the Embassy Security Setup Wizard.
10. The wizard has now initialized the FDE drive's pre-boot authentication and set up the administrator and users of the drive. Shut down the system and then power-up to the system to start using the FDE drive. Note: This requires a full shutdown of the system, not just a restart or reboot of the Windows OS.

Simple User Experience

You should see the pre-boot authentication screen appear as in Figure 7. To access the machine, enter the Windows User Name and FDE drive password into the appropriate fields. If Windows Password Synchronization (see [below](#)) is enabled, the FDE drive password will be identical to the Windows password for the account. If Single Sign-On (see [below](#)) is enabled, the user will be brought directly to their Windows desktop without any additional authentication.

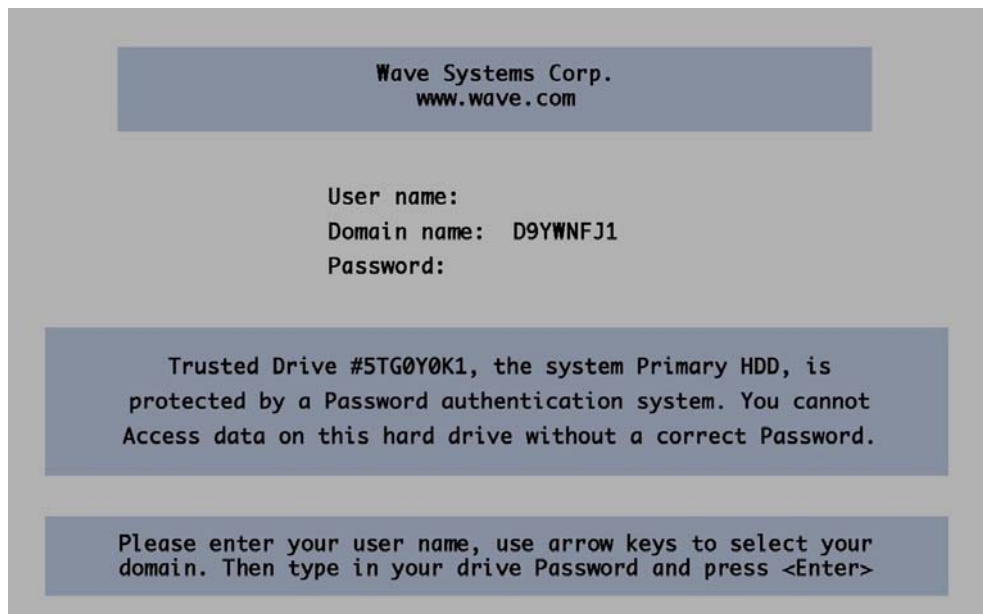


Figure 7: Preboot Authentication to the Drive

After the drive has been unlocked, Windows will boot normally and the user experience will be identical to a normal drive, including full performance of the drive.

Use the Trusted Drive Manager Software to View and Manage Security Settings

Once the drive has been initialized and the users added, the only time a user or administrator will need to access the Trusted Drive Manager software will be to change passwords or to update drive security settings.

Since the access control, pre-boot authentication, and encryption keys are all integrated securely inside the FDE drive, the security around the data will stay in place even if the drive is moved to another platform, or if Wave's TDM software is uninstalled.

View the Status of the FDE drive

1. Double-click on the EMBASSY® Security Center icon on your desktop (see Figure 8). Alternatively, launch 'C:\Program Files\Wave Systems Corp\EMBASSY Security Center\EmbassySecurityCenter.exe'. This will open the EMBASSY® Security Center as shown in Figure 9.
2. Click on the FDE drive Tab shown on the left, which will take you to the Trusted Drive Manager (see Figure 10).
3. The Trusted Drive Manager window shows information regarding the status of the drive in the upper right-hand corner. Initialization enables the pre-boot authentication when the computer is powered on. Un-initializing the drive through the Trusted Drive Manager disables the pre-boot authentication prompt and removes all users from the drive. Disabling "drive locking" disables the pre-boot authentication prompt, but does not remove users from the drive.
4. While viewing the FDE drive status (see Figure 10), you will notice in the top right section that the Remote Management and Remote Recovery are "OFF". These options are enabled by Wave System's Embassy Remote Administration Server.



Figure 8: Desktop



Figure 9: EMBASSY® Security Center

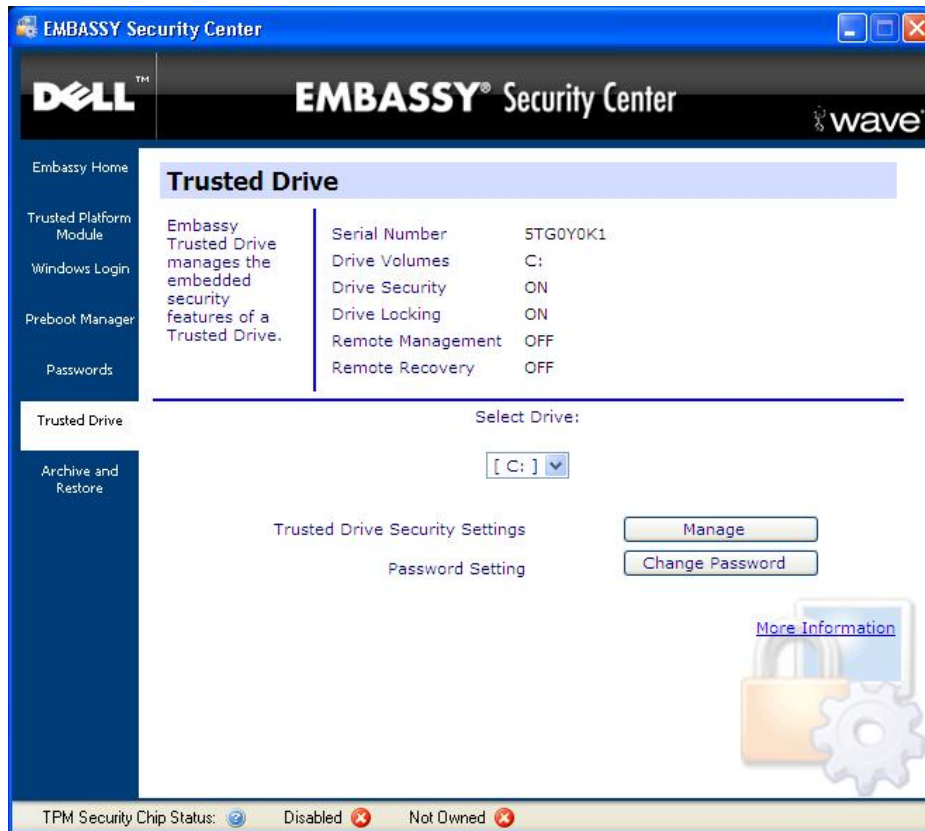


Figure 10: FDE drive Tab

View and Perform Advanced Functions (Administrators Only)

1. Click on the **Manage** button in the FDE drive window (see Figure 10).
2. Only the FDE drive Administrator with the correct user id and password will be able to access this option.
3. If you enter an invalid user id/password combination to access the **Advanced Settings** window, you will receive an error restricting you from access to the menu.
4. When you enter a valid FDE drive Administrator user id/password combination you will see the FDE drive Advanced settings (see Figure 11).

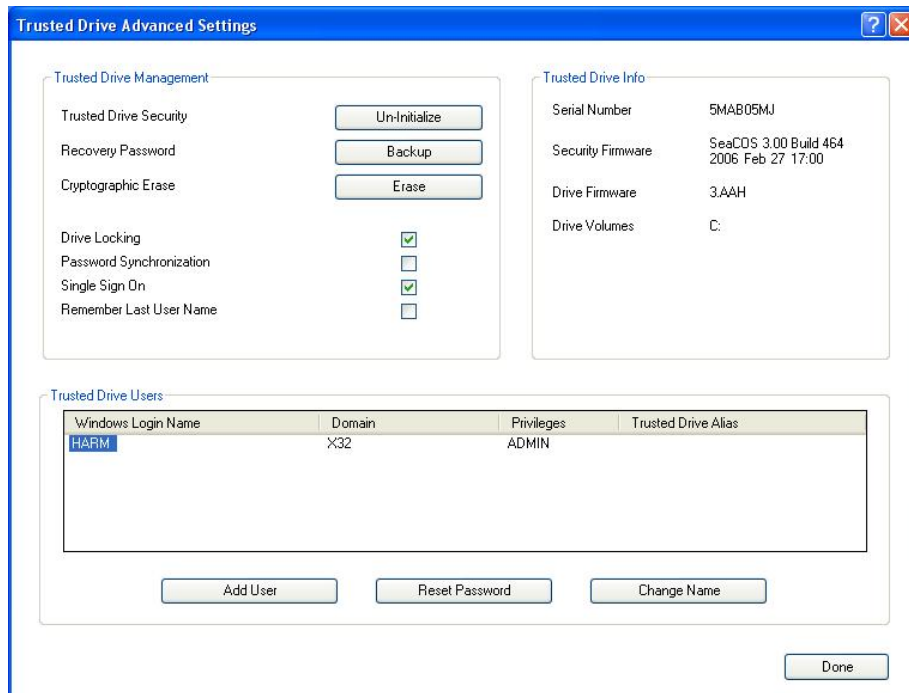


Figure 11: FDE drive - Advanced Settings

Un-Initialize the FDE drive

1. **Un-Initialize** will remove the pre-boot authentication as well as all users of the FDE drive including the administrator. The FDE drive will then function as a standard hard drive. The administrator will need to initialize the drive again, add users, and back up the password to restore it to the secured state.

Disable Drive Locking

1. Disabling drive locking will make the drive function as a normal drive. The drive will not lock when powered down and will not enforce any access control to the drive, which means the data is unprotected and accessible to anyone with access to the system. However, disabling drive locking will not remove all FDE drive users. This feature is intended to be a temporary setting when pre-boot authentication needs to be bypassed. Click **Disable** to disable the drive locking.
2. Power down the computer.
3. Power on the computer.
4. Verify that there is no pre-boot authentication required.
5. Return to the Trusted Drive Manager Advanced Screen and click **Enable** to re-enable drive locking. It is not recommended to leave drive locking disabled.

Back Up Administrator's Credentials

1. **Backup** will bring up a Browse dialog where you can back up the administrator's credentials. This will facilitate recovery if the administrator's password is forgotten; however, the password in this file is in the clear. Therefore, it is recommended to store the backup on a USB drive

placed in a secure location. With [EMBASSY Remote Administration Server](#), administrators can perform password management, control and recovery conveniently and securely.

Change Administrator's Credentials

1. **Change** will bring up a dialog where you change the drive administrator credentials. You can change just the password or the password and username.

Cryptographic Drive Erase

1. **Erase** will delete the encryption key in the drive controller and render all the drive data unusable. Once the key has been erased there is no recovery for the data. The drive controller will immediately generate a new encryption key to encrypt all new data written to the drive. While two warnings will be given before deletion occurs, it is not recommended to proceed cautiously—as this action is irreversible.

Single Sign-On (SSO) for the FDE drive

When this feature is enabled, users can enter their drive password at preboot and Trusted Drive Manager will automatically log them into Windows.

Please note that when the Administrator first enables Single Sign-on, the Single Sign-on process will pause at the Windows Login prompt. The user will be required to enter their form of Windows Authentication (password, fingerprint, Smart Card PIN), which will be stored securely for future Windows Login attempts. Upon the next reboot, Single Sign-on will successfully log the user into Windows. The same process is also required when a user's Windows Authentication Method (password, fingerprint, Smart Card PIN) changes.

If the PC is on a domain, and that domain has a policy that requires ctrl+alt+del to be pressed for Windows login, Trusted Drive Manager will respect the policy. In this instance, the user will be required to press ctrl+alt+del, and TDM will then continue the Single Sign-on process.

For most Dell E-Series and Precision laptops, SSO using Biometrics, Smart Card or Contactless Smart Card while FDE drive is present and locked is available. Please contact sales@wavesys.com and request the companion document for setup instructions.

Windows Password Synchronization (WPS) for the FDE drive

Once this feature is enabled, users will be prompted with a dialog explaining that they need to enter their Windows password and FDE drive passwords. As a result, a success message will appear explaining that the password synchronization is done.

Please note that Windows Password Synchronization is not enforced for the drive administrator; WPS is only applicable to drive users.

Change FDE drive Password while WPS is Enabled

To change the FDE drive Password while WPS is enabled on the platform, simply change the Windows password through the Windows interface. Depending on the setup of the

machine, this can be done in the Control Panel > User Accounts or by pressing ctrl+alt+del and selecting “change password”.

Please note this will change both the Windows password *and* the FDE drive password, keeping them both in sync. If SSO is also enabled, after the first power cycle (power off, then power on) subsequent to the password change, the user will be stopped at the Windows logon prompt and required to enter the new Windows password once before the SSO experience will resume.

If return from Standby (S3) is enabled, the FDE drive password is subject to any BIOS password limitations that may exist. Please consult the ERAS administrator or the system hardware manufacturer for more information on any specific BIOS password limitation that may exist for the system.

Change FDE drive Password while Windows Password Synchronization (WPS) is Disabled (default)

To change the FDE drive password while WPS is disabled, click "Change Password" on the TDM screen in Embassy Security Center. Enter the existing and new FDE drive passwords for the account. A dialog will be displayed messaging the credentials have been successfully changed.

If return from Standby (S3) is enabled, the FDE drive password is subject to any BIOS password limitations that may exist. Please consult the ERAS administrator or the system hardware manufacturer for more information on any specific BIOS password limitation that may exist for the system.

Add FDE drive Users

1. To add a user, click the **Add User** button. You will see the Add FDE drive User dialog box appear.
2. Once complete, the new user will appear in the list at the bottom of the **Advanced Settings** screen.
3. Enter the username and password. Click **Add**. Enter or browse to the appropriate user, create and confirm the password and click **Add**. The user must be a valid Windows local or domain user. If you enter the username directly, it must be preceded by either “[domain name]\” or “[local computer name]\” where [domain name] or [local computer name] are replaced by the actual values.

In Case of a Forgotten FDE drive Password at Preboot (remotely managed client)

1. In the Trusted Drive Manager preboot interface, enter *Recovery_Agent* as the username.
2. Enter the recovery password provided by your company’s ERAS administrator.
3. Regardless of whether Single Sign-on is enabled or not, the user will be stopped at the Windows logon prompt and required to enter the Windows password.

4. Once the system is connected to the network where the ERAS server resides, an ERAS administrator can reset the FDE drive password and provide the new password to the user. After this, the user is strongly encouraged to change the password to one of their choosing as described in the sections above.

Evaluating the Trusted Drive Manager Software

What to Look For

- Ease of use in enabling Full Disk Encryption with strong access control on the system compared to software-based methods
- Simple user interface for drive authentication with transparency during operation
- Speed of encrypted data access – not slowed down by encryption processes
- For network administrators, the availability of remote administration as well as easy and secure drive repurposing

Technical Support

Thank you for using the Trusted Drive Manager! For technical support questions, please send an e-mail to: support@wavesys.com.