

# Trusted Drive Manager



## Getting Started Guide

## Table of Contents

<b>Overview .....</b>	<b>4</b>
What is the Trusted Drive Manager? .....	4
Key Features of Trusted Drive Manager .....	4
<b>Getting Started .....</b>	<b>5</b>
Required Components.....	5
Configure the Trusted Drive Manager Software .....	5
Simple User Experience.....	12
View the Status of the Trusted Drive.....	13
View and Perform Advanced Functions (Administrators Only) .....	15
Un-Initialize the Trusted Drive.....	16
Disable Drive Locking.....	16
Back Up Administrator's Credentials.....	17
Change Administrator's Credentials.....	17
Cryptographic Drive Erase .....	17
Add Trusted Drive Users .....	17
<b>Evaluating the Trusted Drive Manager Software .....</b>	<b>18</b>
What to Look For.....	18
Technical Support.....	18

## Table of Figures

Figure 1: Main Screen of the Security Setup Wizard .....	6
Figure 2: Configure Trusted Drive in the Security Setup Wizard .....	7
Figure 3: Trusted Drive Initialization Wizard .....	8
Figure 4: Back Up Administrator's Credentials .....	9
Figure 5: Add Trusted Drive User .....	10
Figure 6: Wizard Complete.....	11
Figure 7: Preboot Authentication to the Drive.....	12
Figure 8: Desktop.....	13
Figure 9: EMBASSY® Security Center .....	14
Figure 10: Trusted Drive Tab .....	14
Figure 11: Accessing Advanced Features.....	15
Figure 12: Trusted Drive - Advanced Settings .....	16
Figure 13: Trusted Drive - User Management.....	18

## Overview

Seagate Momentus® 5400 FDE.2 fully encrypting hard drives take data protection to a new level by integrating encryption and advanced security features directly in 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 Seagate DriveTrust™ security features available with Wave's EMBASSY Trusted Drive Manager (TDM) software for activating the security features of the Seagate Momentus® 5400 FDE.2 fully encrypting hard drives (called Seagate Trusted Drives or simply Trusted Drives in this guide). The TDM software is included in the EMBASSY® Security Center, a key application of Wave's EMBASSY® Trust Suite (ETS). Beyond the Trusted Drive 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 Trusted 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](http://www.wave.com).

## What is the Trusted Drive Manager?

Wave's Trusted Drive Manager handles all of the Trusted Drive's lifecycle functions from initializing the DriveTrust features for user authentication and security policy setup to drive de-commissioning. A Trusted 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, the Seagate 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, 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 with a Seagate Momentus® 5400 FDE.2 Hard Disk Drive.

**Trusted Drive Manager Software:** The EMBASSY® Security Center contains the Trusted Drive Manager (TDM) plug-in. The software should already be pre-installed on the computer and found at **Start > All Programs > Security by Wave Systems > Embassy Security Center**.

### **Configure the Trusted Drive Manager Software**

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, go to **Start > All Programs > Security by Wave Systems > Security Setup Wizard** (see Figure 1).



**Figure 1: Main Screen of the Security Setup Wizard**

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

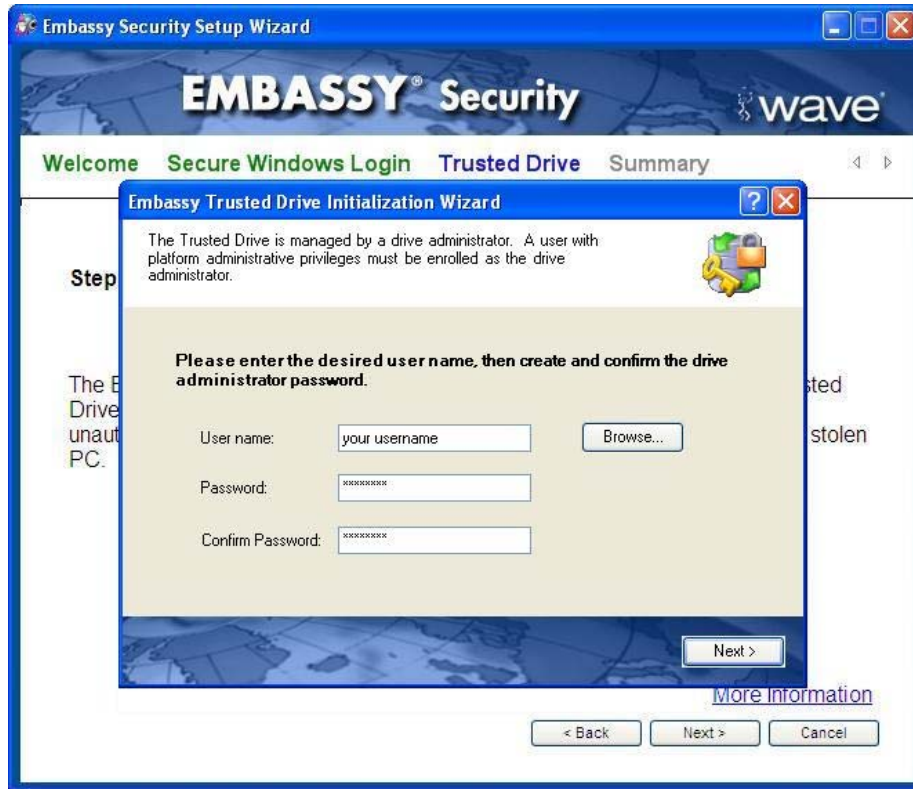
**NOTE:** If the Trusted Platform Module (TPM) security chip is enabled, you will see additional options in this wizard for configuring TPM security. These do not relate to or affect the operation of the Trusted Drive in any way. For simplicity, we show you the screens without the additional options.

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.



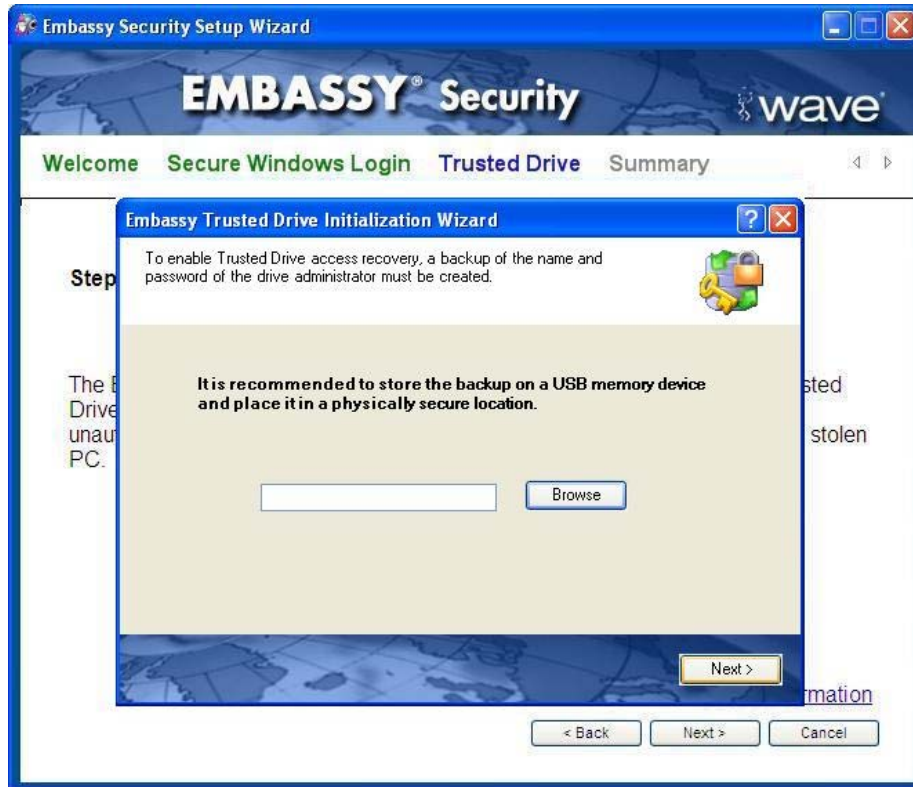
**Figure 2: Configure Trusted Drive in the Security Setup Wizard**

5. The Trusted Drive Initialization Wizard will appear (see Figure 3). Initialization will turn on the Seagate DriveTrust security features for strong access control and 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 Trusted 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: Trusted 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).



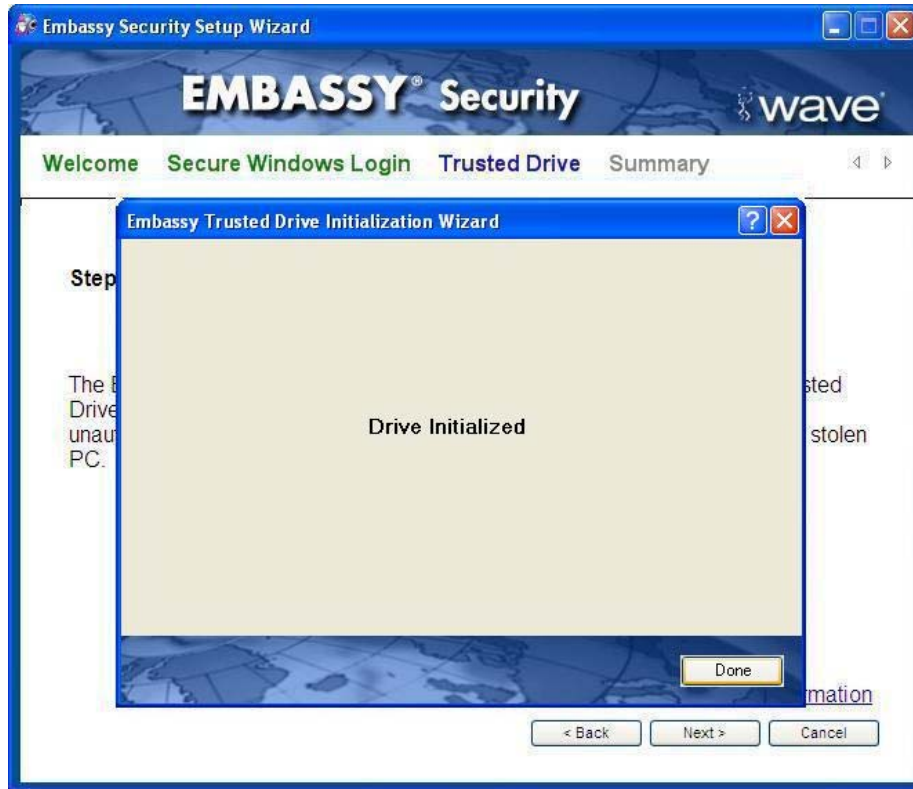
**Figure 4: Back Up Administrator's Credentials**

7. The drive administrator that you created above will be the Trusted Drive administrator. Next, you can add other valid Windows users as Trusted 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 Trusted Drive User**

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

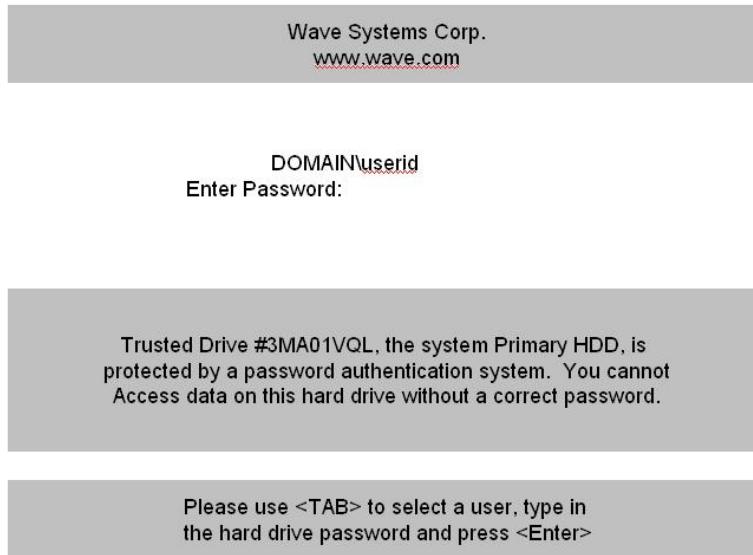


**Figure 6: Wizard Complete**

9. View the status and click **Finish** to exit the Embassy Security Setup Wizard.
10. The wizard has now initialized the Trusted 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 Trusted 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. Select the user ID using the TAB key and then enter your password that you set up in step 5 above to unlock the drive.



**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 Trusted Drive**

1. Double-click on the EMBASSY® Security Center icon on your desktop (see Figure 8). This will open the EMBASSY® Security Center as shown in Figure 9.
2. Click on the Trusted 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 about the drive in the upper right hand corner and about the status of the drive. 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.



**Figure 8: Desktop**



Figure 9: EMBASSY® Security Center



Figure 10: Trusted Drive Tab

## View and Perform Advanced Functions (Administrators Only)

1. Click on the **Advanced** button in the Trusted Drive window (see Figure 10).
2. Only the Drive Administrator with the correct userid and password will be able to access this option.
3. If you enter an invalid userid/password combination to access the **Advanced** window, you will get an invalid drive password prompt (see Figure 11).
4. When you enter a valid Trusted Drive Administrator userid/password combination you will see the Trusted Drive Advanced settings (see Figure 12).

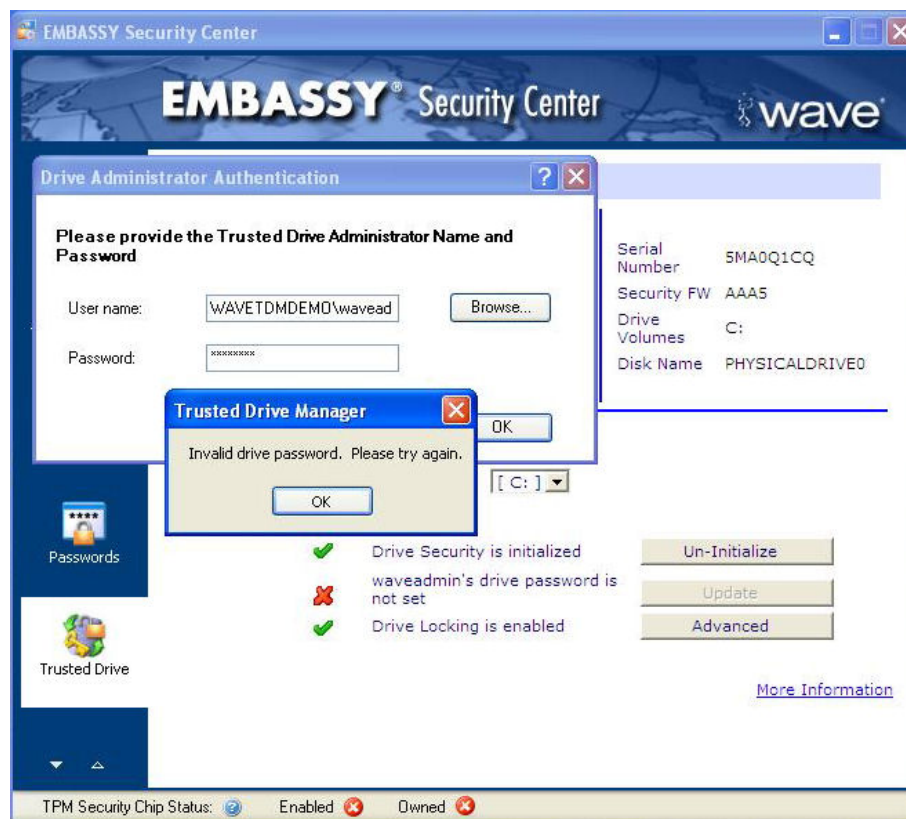
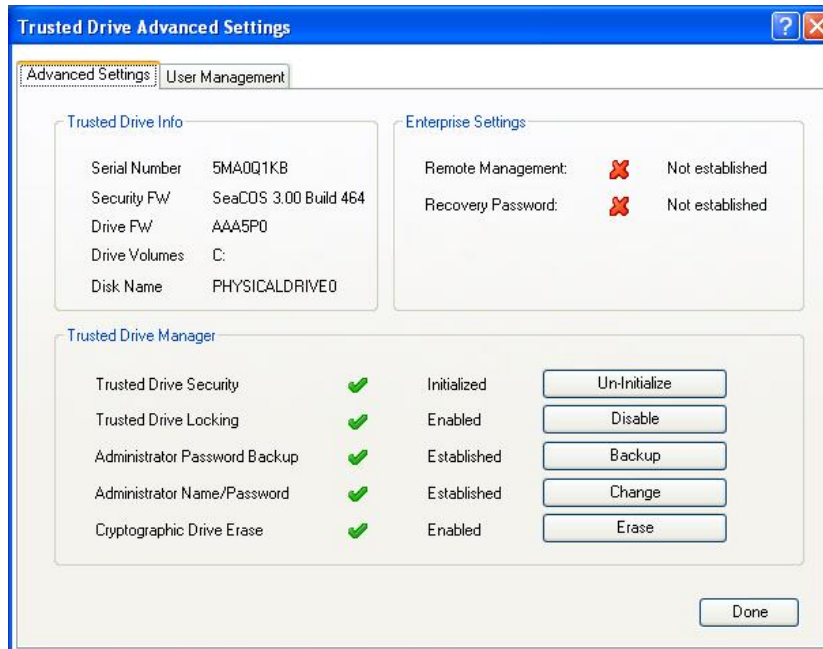


Figure 11: Accessing Advanced Features



**Figure 12: Trusted Drive - Advanced Settings**

5. While viewing the Trusted Drive Advanced Settings (see Figure 12), you will notice in the top right section that the Remote Management and Recovery Password are “Not Configured”. These options are enabled by Wave System’s Embassy Remote Administration Server.

## Un-Initialize the Trusted Drive

1. **Un-Initialize** will remove the pre-boot authentication as well as all users of the Trusted Drive including the administrator. The Trusted 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 Trusted Drive users. 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.

## 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 do this action unless you have consulted the Seagate documentation.

## Add Trusted Drive Users

1. Click on the **User Management** tab. You will see a dialog box as shown in Figure 13. This window displays the currently enrolled users.



**Figure 13: Trusted Drive - User Management**

2. To add a user, click the **Add User** button. You will see the Add Trusted Drive User dialog box appear.
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.

## ***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.