EMBASSY Security Center

ESC 2.9.5 Client Manual

Updated November 28, 2012

http://www.wave.com

Contents

1. Introduction

Welcome and thank you for choosing Wave's EMBASSY® software products. The latest updates to ESC can be found in the readme.txt in the root folder of the installation disk. ESC allows one to:

- Enable and use the security features of self-encrypting hard drives (SEDs)
- Use advanced Trusted Platform Module (TPM) management functions
  - ESC includes the Wave CSP/Toolkit, which enables advanced authentication features of the TPM.
- Make Windows authentication more secure and easier to use

These items denote:
Important Information and/or Additional Requirements

These items denote:
- Warning

For installations of 20 or more, Wave recommends using the EMBASSY Remote Administration Server (ERAS) or the Wave Cloud service - sold separately- which provide centralized user and credential management and robust compliance reporting. For more information please email sales@wave.com.

2. Installation

ESC can be installed interactively or silently following the instructions in this section. Antivirus software can interfere with the installation, so it is recommended this be disabled. It is also recommended that other open programs be shut down to prevent them from interfering with the installation. Running critical Windows updates can interfere with the installation, so it is recommended to Update Windows prior to installing ESC. A reboot is always required after ESC is installed; however the SED can be managed prior to the reboot.

2.1. Prerequisites

2.1.1. Hardware

NOTE: See http://www.wave.com for a list of supported hardware providers.

- PC with a Pentium or newer microprocessor, 800 MHz or greater
- **OPTIONAL:** Trusted Platform Module (TPM) v 1.2
  A firmware update may be required
- **OPTIONAL**: Biometric sensor for Fingerprint support
  A list of supported sensors is found in the Biometrics section
- **OPTIONAL**: Seagate or Opal Compliant Self-Encrypting Drive (SED)

2.1.2. Supported Operating Systems

- Microsoft Windows 7, 32 or 64 bit Professional, Enterprise, or Ultimate
- Microsoft Windows Vista SP2 (or higher), 32 bit or 64 bit, Enterprise or Ultimate
- Microsoft Windows XP Professional SP3 (or higher), 32 bit or SP2 64 bit
  - (.Net Framework 3.5 SP1 needs to be installed separately)

2.1.3. Other Requirements

- Microsoft(R) Internet Explorer version 6.1 or greater.
- For Macrovision-protected versions of ESC: Internet access is required to activate the software.
- Wave software does **NOT** support the IFX TSS on 64-bit platforms. If the endpoint's operating system is a 64-bit edition, then ensure that IFX TSS is not installed (or uninstalled) on the endpoint before installing ESC.

2.1.4. Compatibility with 3rd Party Security Packages

NOTE: TSS, as used below, refers to the Trusted Computing Group's (TCG) Software Stack Specification

Dell Data Protection | Access (DDP|A)

If the Dell Security Driver Pack is installed (this is listed as "Dell Data Protection | Access | Drivers" in add remove programs), ESC will remove this driver pack and replace it with drivers packaged in ESC. These are drivers for managing some of the security hardware, such as fingerprint sensors and the ControlVault.

HP Security ProtectTools Security Manager

If the HP Security ProtectTools Security Manager is installed and has ownership of the TPM then ESC will not properly see nor manage the TPM. This incompatibility is due to a conflict between the Infineon TSS and the Wave TSS.

If the Infineon TSS is installed, do the following to manage the TPM with ESC:
WARNING: The following procedure will result in any Infineon TSS – protected data to be lost.

1) Uninstall the Infineon TSS.
2) Reboot the endpoint.
3) Clear the TPM
4) Run an ESC repair.

Security Innovations NTRU TSS

If the Security Innovations NTRU TSS is installed and has ownership of the TPM then ESC will not properly see nor manage the TPM. This incompatibility is due to a conflict with the Security Innovations NTRU TSS and the Wave TSS.

If the Security Innovations NTRU TSS is installed, do the following to manage the TPM with ESC:
WARNING: The following procedure will result in any Security Innovations NTRU TSS –protected data to be lost.

1) Uninstall the Security Innovation NTRU TSS.
2) Reboot the endpoint.
3) Clear the TPM
4) Run an ESC repair.

2.1.5. Support Statement For SED Management

All platforms and SEDs which meet the following criteria are supported by Wave.

- PC OEM Platforms:
  - From either Dell, HP or Lenovo.
  - Ordered and ship from the factory with an SED.
  - Released within the last three (3) years.
- Self-Encrypting Drives:
  - all TCG OPAL1-compliant SEDs
  - Most TCG OPAL2-compliant SEDs.

2.1.5.1. Supported Platforms for SED Management

Platforms supported for SED management include, but are not limited to:

- **Dell Latitude:** E4300, E4310, E5400, E5410, E5420, E5430, E5510, E5520, E5530, E6220, E6230, E6320, E6330, E6400 ATG, E6410 ATG, E6420 ATG, E6430ATG, E6400, E6410, E6420, E6430, E6430s, XFR E6400, E6420 XFR, E6500, , E6510, E6520, E6530, 5420m, 5520m, XFR, XT3, XT3,
- **Dell Mobile Precision:** M4500, M4600, M4700, M6400, M6500, M6600, M6700,
- **Dell Desktop Precision:** R5500, T1600, T1650, T3500, T3600, T5600, T7600,
- **Dell Optiplex**: 580, 780, 790, 960, 980, 990, 7010, 9010
- **Lenovo:** E30, T420s, T510, X220, W520, T410, T520, X100
- **HP**: 2540p, 2560p, 6450b, 6450b, 6455b, 6550b, 6555b, 6930p, 8200, 8440p, 8440w, 8460p, 8540p, 8540p, 8540w, 8560, 8740w, HP 6000, HP 6005, HP8000, HP 8100,
- **Panasonic:** Panasonic Toughbook CF-H1, Panasonic Toughbook CF-H2Toughbook CF19 Mark4, Toughbook CF19 Mark5,
- **Motion Computing:** J3500

Support Statement for TPM Management

Unless explicitly listed as unsupported, all TPM V 1.2 TPMs are supported with this release. A TPM firmware upgrade may be required for full TPM functionality.

2.2. Upgrades

ESC 2.9.5 supports direct upgrades from ESC 2.8.4 and ESC 2.8.0. The drive the drive can remain initialized while performing this upgrade install. Chained upgrades from 2.7.3 to 2.8.4 to 2.9.5 are also supported.

If using fingerprint readers: Ensure that NTRU TSS is ***NOT*** installed on the endpoint ***PRIOR*** to upgrade or installation of ESC. Failure to do this check may result in fingerprint logon and new fingerprint enrollments to fail.

If ESC is installed with the NTRU TSS is still installed, and the fingerprint authentication is no longer functioning, then perform the following procedure:

1. Uninstall the NTRU TSS.
2. Reboot.
3. Uninstall ESC 2.9.5.
4. Reboot.
5. Install ESC 2.9.5.
6. Reboot.

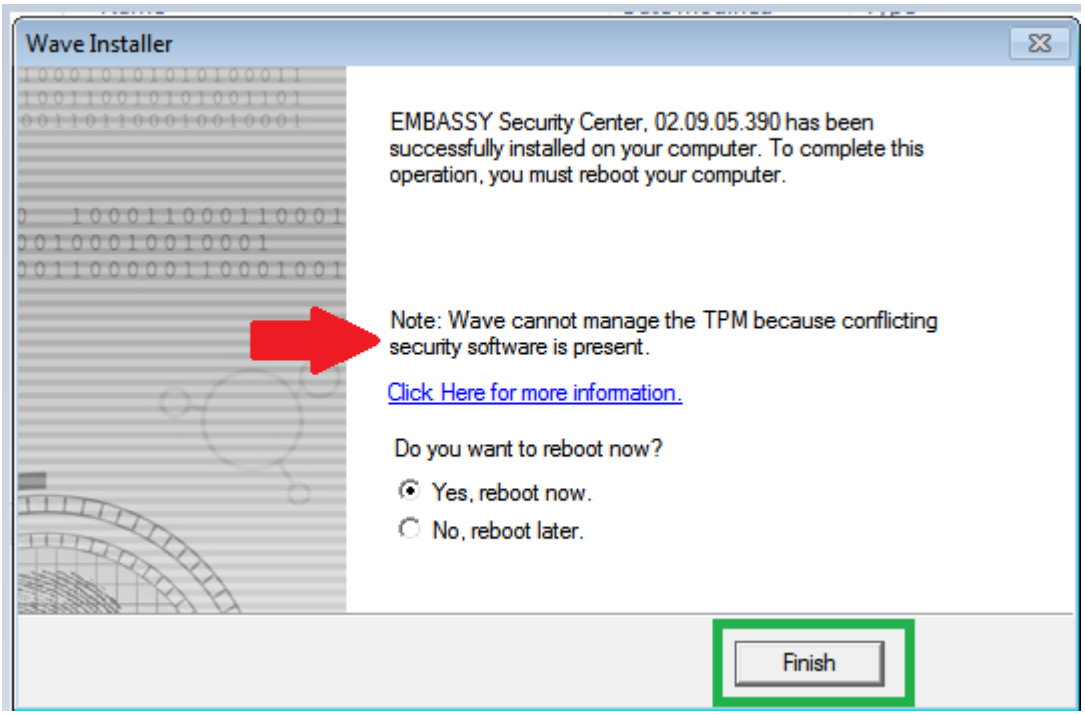
Upgrade procedure:

1. Navigate to the root directory of the ESC installation media.
2. Run **WaveSetup.exe** with administrator privileges.
3. Follow the installation wizard.
4. Restart the endpoint.

If upgrading from 2.7.3 or earlier: The upgrade process will automatically disable Secure Windows Logon. If this is set locally, you will need to re-enable it. If Secure Windows Logon was set by policy and if connected to the domain controller the client will perform a ***gpupdate*** after installation, so Secure Windows Logon will be reset following the installation.

2.3. Interactive Installation

1. Run ***WaveSetup.exe*** in the root folder of the ESC installation media.
2. Follow the instructions in the wizard to complete the installation.
3. **CAUTION**: Carefully read the last window prior to clicking **Finish**. Some third-party security software programs may not be compatible with Wave software and, if so, a note will say so here.



4. ESC will prompt for a restart following the installation. ESC must be restarted to use any functionality other than SED management.

2.4. Silent Installation

User Account Control (UAC) must be disabled, or the installer must be run as administrator. Following ESC installation, ESC must be restarted to use any functionality other than SED management.

Run the following command from the command prompt:
WaveSetup.exe –silent –install

Other commands:
Silent uninstallation
WaveSetup.exe –silent –uninstall

Show(Hide) icons on desktop
WaveSetup.exe –icon(-nicon)

Omit component installers:
WaveSetup.exe –omit="Trusted Drive Manager", "WaveTSS", "S3 Driver"

- Trusted Drive Manager is the component for managing self-encrypting drives. If it is omitted self-encrypting drive management will not be available.

-headless is an option for installation that will not create any desktop or start menu short cuts. This may be used for client endpoint machines that will be managed remotely with EMBASSY Remote Administration Server (ERAS).

The exit code for a successful installation is "0".

You must restart the computer to complete the installation. SED management can be performed without a restart, but all other ESC features require a restart following the installation to function properly.

2.5. Installing ESC to Manage TPM

To fully utilize the TPM for authentication or Wave Endpoint Monitor (WEM), a Trusted Software Stack (TSS) is required. If no software has been installed on the client prior to installing ESC, the ESC installer will automatically install the WaveTSS middleware. If other TPM management software is present, ESC may not install. If WaveTSS does not install, it is either because it is impossible for two TSS to successfully run at the same time, or because there would be potential conflicts between the two TSS. The table below lists the conditions where the WaveTSS will be installed, and also which TSS would be utilized by ESC.

Table 1 - When ESC TPM Management Is Available

	Windows XP	**Windows 7, Vista**
Infineon (TPM Owned)	Wave TSS not installed TPM Management not available unless Infineon is uninstalled	Wave TSS not installed TPM Management not available
Infineon (Not Owned)	Wave TSS not installed TPM Management not available unless Infineon is uninstalled	Wave TSS installed TPM is available through WaveTSS
NTRU (TPM Owned)	Wave TSS not installed TPM management available if NTRU is a supported version	Wave TSS not installed TPM is available through NTRU
NTRU (Not Owned)	Wave TSS not installed TPM management available if NTRU is a supported version	Wave TSS installed TPM is available through WaveTSS
Lenovo TSS (TPM Owned)	Wave TSS not installed TPM Management not available unless Lenovo TSS is uninstalled	Wave TSS installed TPM is available through WaveTSS
Lenovo TSS (Not Owned)	Wave TSS not installed TPM Management not available unless Lenovo TSS is uninstalled	Wave TSS installed TPM is available through WaveTSS

Instructions to install the Virtual Smartcard functionality are found in the TPM as a Virtual Smart Card section.

2.6. Repair an ESC Installation

There may be scenarios where ESC needs to be repaired. The ESC repair procedure can be run interactively or silently.

2.6.1. Perform an ESC Repair Interactively

- Log into the endpoint.
- Navigate to the installed programs applet:
    - Windows XP/Vista = **Start** -> **Control Panel** -> **Add/Remove Programs**.
    - Windows 7 = **Start** -> **Control Panel** -> **Programs and Features**.
- Right-click **EMBASSY Security Center**.
- Select **Uninstall/Change**.
- Click **Next**.
- Check the **Repair** option.
- Click **Next**.
- Follow the Wave installer repair wizard prompts.
- Click **Finish**.
- Restart the endpoint.

2.6.2. Perform an ESC Repair Silently

NOTE: Requires the ESC installation media

1. Log into the endpoint.
2. Open an elevated command prompt.
3. Navigate to the drive\folder containing the ESC installation media.
4. Type the following command:

    Wavesetup.exe –silent –repair

5. When the repair is complete; restart the endpoint.

2.7. Services Installed by ESC

EMBASSY Security Center components are correctly configured at the time of installation. In case they've been changed after the fact, the startup types are listed below. Note – without a complete restart after installing ESC no feature is guaranteed to work completely.

ESC 2.8.4 Services:

ETBIService – This is installed by ERASConnector and must be available for ERAS management. The recommended startup type is *manual*.

SecureStorageService – Installed by ESC. It is a service for the TPM's password vault. The recommended startup type is *manual*.

WaveAuthenticationManagerService – Installed by ESC and is sometimes used for the Wave Gina and Credential Provider (Secure Windows Logon). The recommended startup type is *automatic*.

ESC 2.9.5 Services:

ETBIService – This is installed by ESC and must be available for ERAS management. The recommended startup type is *manual*.

SecureStorageService – Installed by ESC. It is a service for the TPM's password vault. The recommended startup type is *manual*.

WaveAuthenticationManagerService – Installed by ESC and is sometimes used for the Wave Gina and Credential Provider (Secure Windows Logon). The recommended startup type is automatic.

WvPCR – The Wave Toolkit Service is communicates data for the Wave Endpoint Monitor (WEM server. The recommended startup type is *automatic*.

3. Configuration for Remote Management of ESC

When ESC is installed, it checks Windows policy settings to point to the ERAS Server. If the policy is not set when the installation is completed, ERAS will not be able to manage the client. The ESC component that is configured for communication is called ERAS Connector.

3.1. Installation Procedure with No Manual ERAS Connector Configuration:

If you follow the following procedure when installing ESC 2.9, no additional procedure will be necessary for remote communication:

1. Follow the steps to set the ERAS Connector settings as outlined in the ERAS Administrator Manual.
2. Update the policies on the client. This can be done using “gpupdate /force” or by restarting the client computer.
3. Install ESC
4. Following ESC installation, ESC must be restarted. Alternatively, using the SSIP Utility (future) will allow you to install ESC without manually configuring the ERAS Connector.

3.2. Easy Way to Re-Adjust ERAS Connector Settings:

If the ERAS Connector settings are changed or set after ESC is installed, you may use the following procedure to fix them using the ERASConnectorConfigUtil.exe, packaged with ESC:

1. Follow the steps to set the ERAS Connector settings as outlined in the ERAS Administrator Manual.
2. Update the policies on the client. This can be done using “gpupdate /force” or by restarting the client computer.
3. Open a command prompt and navigate to the *Wave Systems Corp* folder under *Program Files\Remote Management*
4. Run ERASConnectorConfigUtil.exe

3.3. Out-Of-Domain Management with ERAS

For out-of-domain management with ERAS, the client needs to adjust ERASConnector to point to the ERAS Server. ERASConnectorConfigUtil must be run as an administrator from the command line, and is found under \Program Files\Wave Systems Corp\Remote Management. The syntax to run ERASConnectorConfigUtil is:
'ERASConnectorConfigUtil.exe ERASaccount=SYSTEM host=IP'
If the Wave SSIP Utility (future release) is configured with this information, the ERASConnectorConfigUtil will not need to be run.

4. TPM Lifecycle Management

A TPM is a hardware chip attached to the motherboard that can make authentication to protected services or data easier and more secure. ESC can manage the TPM chip to securely store keys and certificates. Users must provide credentials to unlock certificates. Thus, the TPM provides both user and device-level authentication.

Additionally, the TPM can be used to detect changes made to the computer's boot process, making it possible to detect many types of malware early. When used with Wave Endpoint Monitor (WEM), the TPM can be used to detect changes and potential tampering to the boot sequence.

Neither ESC nor a TSS is required to use the TPM for BitLocker management with Wave EMBASSY Remote Administration Server (ERAS).

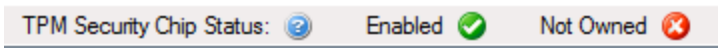
Turn on the TPM

The Trusted Platform Module (TPM) is available on most business class laptops from well-known manufacturers. To determine if your computer has a TPM, the technical specifications on the manufacturer's website are a good place to start.

If you are unsure if your computer has an *enabled* TPM, go to Control Panel > Device Manager and search for a Trusted Platform Module under Security Devices. If the TPM has not been *enabled*, check the system BIOS to see if it has an option to enable a TPM. System BIOS' vary, but you can view the settings for most by pressing the *F2 key* at system boot. Once the TPM is enabled, it will need a TPM driver. If a TPM does not display in Device Manager, a TPM driver may need to be installed. Check your computer manufacturer's website to find and install the appropriate driver.

Take ownership of the TPM

An owner password must be assigned to the TPM before any of its security functions can be utilized. Once the prerequisites have been met, ESC will say "TPM Security Chip Status" at the bottom of the window. There will be a green checkmark by "Enabled". If it does not appear, verify that the prerequisites have been met. If there is a green checkmark by "Owned", than the TPM has already has an owner.

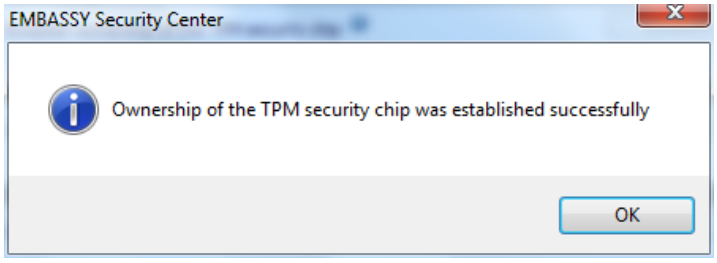


In order to take ownership, the TPM must be Enabled and Not Owned

Lost TPM owner password - If the TPM is owned but the owner password is lost, the TPM can be cleared in BIOS. All data previously protected by the TPM, including passwords and certificates, will be rendered useless if the TPM is cleared.

Select the "Platform Security Modules" tab at the left, followed by the "Manage TPM' tab at the top.

1. Under "Ownership", click the button labeled **"Establish"**.
2. Enter the new owner password twice and select **"OK'**. The password complexity rules match the windows password complexity rules currently applied.
3. A message will inform you that you have successfully taken ownership of the TPM.



Remotely Managed TPM

If the TPM is remotely managed, TPM management functions must be made by an Administrator using EMBASSY Remote Administration Server (ERAS). ERAS will control the TPM owner password, but will delegate users to the TPM. Thus if you forget your TPM password, ERAS will be able to reset it.

Certain commands to the TPM through ERAS management will require physical presence to accept. The next time the computer boots, a message will appear explaining that changes are about to be made to the TPM. One has the option to select **"Modify"** or **"Ignore"**. Select **"Modify"** if you want to accept the changes made to the TPM. On some computers, modify/ignore must be selected through function keys. When a computer is remotely managed (e.g. "owned" by the remote administrator), local administration of the TPM functionality will be disabled; the management windows of the application will not be accessible locally.

4.1. How to Archive and Restore TPM keys

The Archive and Restore functionality is used to back up and restore all user credentials (login and encryption information) stored in the 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. It is recommended to create an archive periodically to prevent credential/data loss.

Examples of when a TPM archive would be useful are:

- The TPM was cleared - If your TPM is cleared, intentionally or accidentally, you can recover keys and data.
- The motherboard/TPM was replaced - In the case of hardware failure; credentials can be migrated to the new TPM.
- You transfer to another computer - If you move to a new computer, you can restore your old credentials to the new computer and protect them with the TPM.
- You re-install your operating system – TPM keys and data will be lost if you re-install your operating system.

To archive keys for each user:

1. Have the user login:
2. Click on the “Archive and Restore” tab at the left.
3. Click the **“Archive”** button; this will open an Archive wizard.
4. Select the checkbox for the data you wish to back up, “TPM Data”.
5. You will be prompted for the TPM Owner Password, and Master Password if applicable.
6. You will be prompted to create a new archive password. This password must be entered later to restore from the archive.
7. A success screen will be displayed, however if no keys have been generated to back up, you will be shown an error message.

To restore keys for a user:

1. Ensure the target machine is running the same version of ESC and has a TPM that is activated, enabled, and owned.
2. Have the user login:
3. Click the **“Restore”** button; this will open a Restoration wizard.
4. Click browse to select the archive you wish to restore.
5. Enter the “archive”/”backup data” password you had entered in step 6 when archiving keys. Click next
6. Select the “TPM Data” and click next
7. Enter the new TPM Owner Password, and Master Password if applicable.

4.2. Wave Cryptographic Service Providers (CSPs)

The following CSPs are made available on the client, and can be selected when making an advanced certificate request to a Microsoft Certificate Authority (CA). For information on how to enforce the use of a Wave CSP (to enforce the use of a TPM to access a resource), refer to the ERAS manual on the section dealing with TPM central management.

Wave TCG-Enabled CSP

This CSP is the 'standard' Wave CSP used for generating TPM keys and related functions unless one of the below apply. The Wave TCG-Enabled CSP also must be used if a use case for VPN authentication requires a user to login to the VPN prior to logging into Windows.

Wave TCG-Enabled Strong Authentication CSP

This CSP is very similar to the "Wave TCG Enabled CSP" with the following exceptions:

1. All Keys created with this CSP are always password protected.
2. This CSP will never store the individual TPM key password in the Wave Password Vault.
3. This CSP must be used for password protected keys with Microsoft VPN. A protected key is one that uses a pin.
4. This CSP must be used for Wave's TPM PKI logon.

Wave TCG Enabled SChannel CSP

This CSP uses the "Microsoft RSA SChannel Cryptographic Provider" as a pass-through CSP so that it can work with SSL based applications (For locating the private key in the SSL connection).

4.3. Wave Key Service Providers (KSPs)

The Wave KSP is another mechanism to provide advanced authentication through the TPM, but it supports access through the Microsoft Cryptography Next Generation (CNG) API. A KSP is necessary for Direct Access authentication, and the Wave KSP can be configured with Direct Access to provide TPM based authentication to Direct Access resources. This guide is limited to explaining how to access the KSP. Please refer to Microsoft documentation for instructions on setting up Direct Access authentication using a KSP. Information on Direct Access can be found at http://technet.microsoft.com/en-us/network/dd420463 and instructions to set up a Direct Access test lab are found at http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=24144.

The KSPs have a couple of pre-requisites before they can be used:

1. The TPM must be activated and owned.
2. ESC must have a supported TSS.
3. A supported Microsoft Windows operating system:
    a. Windows 7 - Supports Microsoft DirectAccess and KSP.
    b. Windows Vista – KSP only.

    NOTE: Windows XP does *not* support either KSP or Direct Access.

Once these prerequisites are met, and ESC 2.9 is installed, both KSPs are available for usage through Windows.

Wave TCG Enabled KSP
This is the standard KSP. The usage of a PIN is optional.

Wave TCG-Enabled Strong Authentication KSP
This KSP supports only protected keys, meaning a pin must always be used with the strong authentication KSP.

1. All Keys created with this KSP are always password protected.
2. This KSP will never store the individual TPM key password in the Wave Password Vault.

4.4. Clearing and Disabling a TPM

TPM hardware state is controlled by the endpoint's BIOS software. In order to clear, enable/disable, or activate/deactivate a TPM you must restart the endpoint and press the appropriate key on the keyboard to enter the endpoint's BIOS environment. Each computer manufacturer implements this procedure differently. Consult your computer owner's manual for the appropriate BIOS environment procedures.

5. TPM as a Virtual Smart Card

If you have a Certificate Authority available, your TPM can give you equivalent functionality to a smart card using the TPM. Your smart card travels with your computer, and becomes a token to authenticate to remote services and the local computer. Compared to password authentication, Virtual Smart Card (VSC) makes it harder for an attacker to use your credentials because your credentials are tied to the TPM chip on your computer. It can also be configured as a credential used for remote desktop. The TPM Virtual Smart card is not supported on Windows XP; and requires additional installation files (minidriver and .vbs script) that ship with the ERAS server.

You cannot enroll TPM Virtual Smart Card certificates created on the ERAS-CCA.

While TPM Virtual Smart Card is a flexible tool that can be configured for a number of purposes, the following are supported:

- Microsoft Remote Desktop (Windows Terminal Services may be running)
- Website login (The website must be configured for smart card login)
- Microsoft VPN
- Cisco VPN
- CheckPoint VPN
- Windows desktop and domain logon using Wave Credential Provider
- Windows desktop and domain logon using the Microsoft Credential Provider

Other applications are not supported yet, but may work.

5.1. Configuration

To configure TPM Virtual Smart card on the client computer to accept certificates:

1. Install ESC 2.9
2. Turn the TPM on and take ownership of it through ESC or ERAS.
3. [Optional but recommended] Open services.msc and stop the "Windows Update" service
4. Copy Install_Virtual_SmartCard_v<x>.<y>.vbs from the ERAS installation media to the ESC client.
5. Open a Windows Command Prompt with Admin rights. This can be done by right clicking the "Command Prompt" in the start menu and selecting "Run as administrator".
6. Navigate to the folder containing the .vbs script and run "cscript.exe Install_Virtual_SmartCard_v<x>.<y>.vbs"
7. Restart the computer

If using TPMVSC for Windows Logon using Wave Secure Logon, be sure to enable authentication using password or certificate.

5.2. Usage

Setting up a smart card authentication requires the IT administrator to have a basic understanding of public key infrastructure (PKI) and the Microsoft "Certificate Authority" server role. Requesting a certificate is simple and works the same as with a physical smart card, certificates can be added using the Certificates MMC snapin, or the Microsoft Internet Information Services (IIS) certificate server (certsrv) page using a web browser.

Certificate Template Requirements

1. TPMVSC supports V1 (server 2000), V2 (server 2003). TPMVSC does not support V3 (server 2008) templates.
2. If a CSP is specified under the "Request Handling" tab within the certificate template, it must be "Microsoft Base Smart Card Crypto Provider". If a CSP is not specified in the template, the user will have to specify it during web-enrollment.
3. The "Extensions" tab must have an "Authentications Policy" extension. When highlighted, it must list "Smart Card Logon", under Description of Application Policies below.
4. The certificate cannot be a certified certificate; it cannot be given a SKAE extension.

Web-Enrollment Requirements:

1. The key size must be either 1024 or 2048
2. The *Smart Card* service must be running on the client machine. This can be checked by running **services.msc**. If it is not running, an error code *SCARD_E_NO_SERVICE* may appear.
3. The TPM will be accessible if **all** of the following requirements are met:
    - Powered on
    - Enabled
    - Activated
    - Owned
    - Unlocked

A reboot is required after taking ownership of the TPM and before enrolling the certificate. Otherwise, the certificate snap-in will prompt for the smart card during enrollment.

4. When using the TPM Virtual Smart Card, you must have the appropriate trusts to your Certificate Authorities. This trust can be created when you download a CA certificate chain from your CA. Without the appropriate trust, you will not be able to enroll certificates.
5. Whenever enrolling a certificate, it must use the "Microsoft Base Smart Card Crypto Provider" CSP.
6. Remote Desktop is supported with TPM Virtual Smart Card, but the target computer must have the .MSI installed.

Example

These steps are provided only as an example of how to configure TPM Virtual Smart card logon, after the *Smartcard Logon* template is made available on the CA, and TPM Virtual Smart Card has been installed.

1. Navigate to **https://<CA server IP address OR DNS entry>\certsrv .**
2. Authenticate via username and password for the user you wish to enroll
3. Click **Download a CA certificate, certificate chain, or CRL**.
4. Click **Download CA certificate chain**
5. Install the resulting certificate in the **Trusted Root Certificate Authority** container.
6. Once the CA certificate chain is installed, click on **Home** in the upper right-hand corner to return to the homepage.
7. Click **Request a certificate**.
8. Click **Advanced certificate request**.
9. Click **Create and Submit a request to this CA**.
10. In the certificate template dropdown box, choose the **Smartcard Logon** template.

    NOTE: If this option does not appear, the Certificate Authority may not yet have been configured to provide this template to this particular user.
11. In the CSP dropdown box, choose **Microsoft Base Smart Card Crypto Provider**.
12. Choose either 1024 or 2048 for the key size.
13. The **User specified key container name** checkbox is optional.
14. All other settings may remain at their default setting.
15. Click **Submit.**
16. At the resulting Pin window, enter any PIN (4 digits). This PIN will be required to use the certificate later.
17. Click the **Install Certificate** link.

NOTE: The page may appear to be "frozen", but it should only take a few minutes for the installation to complete.

It may seem like it's taking a long time for the certificate request to go through. This is normal and will depend on network connection, machine speed, etc.

5.3. Change Pin

The steps to change the TPMVSC pin are slightly different depending if Wave Secure Logon is set.

To change the PIN if Wave Secure Logon is set:

1. While logged onto Windows, press **CTRL + ALT + DEL** once.
2. Select **Change Password**.
3. Select **Other Credentials**.
4. Select the appropriate **TPM Virtual Smart Card**.
5. Enter the previous *PIN.*
6. Enter the new *PIN* twice.

5.4. Remote Desktop

You can remote desktop into a computer that does not contain a TPM using the Wave TPM Virtual Smart Card. A minidriver must be installed on the machine you remote desktop into using TPM Virtual Smart Card. The minidriver does not need to be installed on the client with ESC, the ESC installer includes this.

The Minidriver supports:

- Windows 7
- Windows Vista with SP2 or greater
- Windows Server 2008 Standard Edition
- Windows Server 2008 R2 enterprise with SP1

NOTE: Windows XP and Server 2003 are not supported by the minidriver.

Install the **Minidriver .msi**, and reboot when the installer completes. Afterwards, the *Wave Minidriver for Smart Card* will appear under *Device Manager -> Smart cards*.

a. On a 32 bit system the installation file is *Wave TPM Virtual –SC Minidriver x86.msi*, it is kept in the installer_sc32 folder.

b. On a 64 bit system the installation file is *Wave TPM Virtual –SC Minidriver x64.msi*, it is kept in the installer_sc64 folder.

Remote Desktop – To remote desktop into a computer without TPM virtual smart card, a separate MSI that ships with ERAS must be installed on the target computer.

Uninstalling TPM Virtual Smart Card – To uninstall the TPM Virtual Smart card, you will need to run the following command line from an elevated command prompt:
CScript.exe Uninstall_Virtual_SmartCard.vbs

5.5. Configure for Offline Windows Logon

After a user has enrolled a domain user certificate, the certificate on Virtual Smart Card (VSC) for this domain user **must** be used to logon to the machine at least **once** to create the domain user profile and cache the domain user credential while the network is still on. After the credential is cached, the user is able to logon to the offline endpoint regardless if they are on or off of the network.

If the domain controller is unavailable then the Windows operating system will display one of two messages when a user account attempts to log into the operating system:

- If the logon information is not cached: *The system cannot log you on now because the domain <DOMAIN_NAME> is not available*.
- If the logon information has been cached: *Windows cannot connect to a server to confirm your logon settings. You have been logged on using previously stored account information. If you changed your account information since you last logged on to this computer, those changes will not be reflected in this session.*

5.5.1 Cached Virtual Smartcard Expiration

How long the VSC credential is cashed is based on configurations set on the network domain controller. The endpoint's local security policy also needs to be set for how long the credential will remain cached:

1. Open an elevated command prompt.
2. Type **gpedit.msc**.
3. Navigate to ***Local Security Policy -> Computer Configuration -> Windows Settings -> Security Settings -> Local Policies*** .
4. Open the **Interactive logon: Number of previous logons to cache (in case domain controller is not available)** policy.
5. Configure this number to be above the number of user accounts that access the system.
    a. **EXAMPLE**: If 5 people access the same machine, increase this setting to 6 or above.
    b. **NOTES**:
        i. Default value = 25
        ii. Disable caching = 0
        iii. Cache 50 logon attempts = <50

5.6. Uninstallation/Removal

An uninstallation script is provided to help resolve potential compatibility issues with other smart cards. To remove this functionality from the Client Computer:

2. Copy Uninstall_Virtual_SmartCard_v<x>.<y>.vbs from the ERAS installation media to the client.
3. Open a Windows Command Prompt with Admin rights. This can be done by right clicking the "Command Prompt" in the start menu and selecting "Run as administrator".
4. Navigate to the folder containing the .vbs script and run "cscript.exe Uninstall_Virtual_SmartCard_<x>.<y>..vbs"

5.7. Troubleshooting

Issue: The VBScript fails to run, and the TPM Virtual Smart card driver in device manager is listed as "unknown"
Resolution: Turn of the Windows Update service and run the .VBS script again.

6. Wave Endpoint Monitor

Wave Endpoint Monitor (WEM) is an additional product that can use ESC to help you detect Advanced Persistent Threats (APTs) that would otherwise go unnoticed for long periods of time and cause severe damage and data loss. An APT could be a rootkit, and could even reside in infected firmware. To combat this, Wave utilizes tamper-resistant storage locations on the TPM called Platform Configuration Registers (PCRs). Each is used to securely collect hash information about a computer's pre-OS environment. This information is compared to a known set of trusted values. Malware cannot tamper with the quotes sent to the server, as the quotes are signed by a private key that never leaves the TPM. WEM provides customizable alerts, providing administrators real time warnings so they can take action immediately when threats occur.

6.1. Client Requirements

Broadcom TPMs require firmware version 1.2.7.13 or higher. Other TPMs may require the latest firmware update.

6.2. Additional WEM requirements

Please reference the ERAS/WEM TPM Deployment Guide, ERAS 2.9 Installation Guide and WEM Administrator Manual for more clarification and information specific to installation and use of WEM.

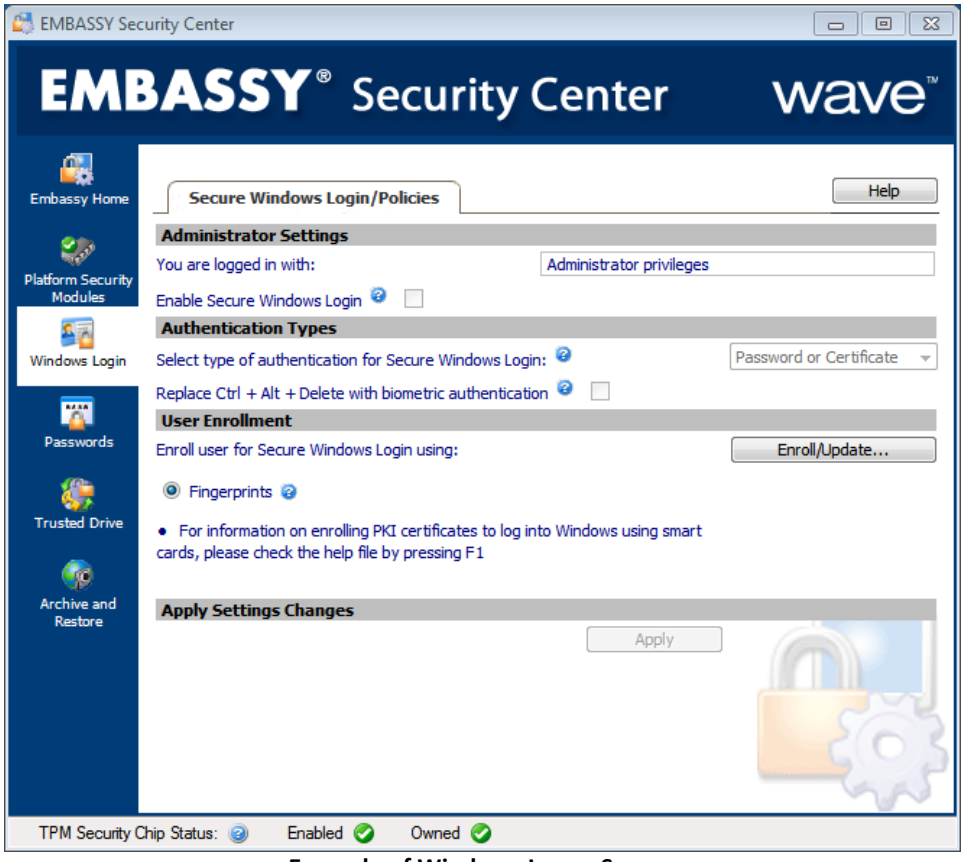
7. Secure Windows Logon

Wave Secure Logon is a way to make authentication to Windows easier and more secure. One would set Secure Windows Logon if they desired Single Sign On (SSO) with the SED or wanted to use Finger Print Authentication to Windows. Fingerprint data is protected by the TPM when the TPM is available. Secure Windows Logon also supports using a certificate on a smart card to log on to Windows.

Secure Windows Logon is implemented through the Wave Credential Provider on Windows 7 or Windows Vista. The Wave Gina is present when using Windows XP. It is required for "Single Sign On" (SSO). Secure Windows Logon can be set locally by the end user, or remotely by the administrator using group policies that ship with ERAS.

To set Windows Login Locally:

1. Open **ESC**.
2. Select the **Windows Login** tab.
3. Place a check in the **Enable Secure Windows Login** check box.



Example of Windows Logon Screen

7.1. Biometrics

The use of biometrics is supported for Secure Windows logon and for authentication to the TPM.

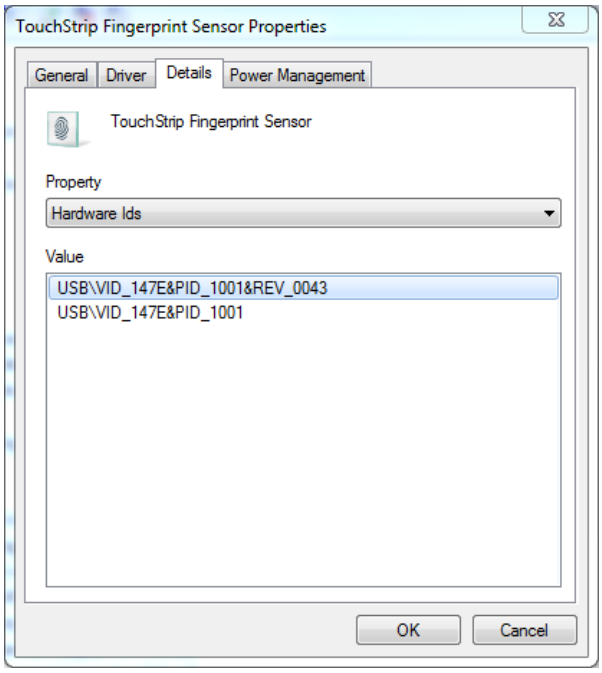
Supported Fingerprint Sensors

The following table lists two columns; the name given by the manufacturer is in the first column. If the label for the sensor is not available, Windows Device Manager can be used to check the VID and PID of the sensor.

Sensor Name	Identifier in Device Manager:
AES 3500 ClipDriveBio	VID_124C&PID_0230
AES 3400 and AES 4000 Targus	VID_08FF&PID_5501
AES 3500 TruePrint	VID_08FF&PID_5731
AES 3400 biometric mouse	VID_08FF&PID_3406
AES 3500 Trueprint	VID_08FF&PID_5700
AT8 (Authentec secure sensors)	
AES 2501 Slide sensor	VID_08FF&PID_2580
Authentec 2810 Swipe Sensor	VID_08FF&PID_2810
AES 1610 SlideSensor	VID_08FF&PID_1600
AES 2550	VID_08FF&PID_2550
AES 2660 Fujitsu T901 Internal Sensor	VID_08FF&PID_2683
AES 2660 External Sensor	VID_08FF&PID_2660
AES 1660 External Sensor	VID_08FF&PID_1660
AES 1660 Internal Sensor	VID_08FF&PID_168A

Sensor Name	Identifier in Device Manager:
Dell Laptop Sensors:	
Broadcom Sensor	VID_0A5C&PID_5801
Broadcom Sensor	VID_0A5C&PID_5802
Broadcom Sensor	VID_0A5C&PID_5803
UPEK Sensors	
	VID_0483&PID_2016
	VID_147E&PID_2016
	VID_147E&PID_1000
UPEK TCS1	
UPEK TCS3	
UPEK TCS4	
Eikon solo sensor	VID_147E&PID_1001
	VID_0483&PID_2015

The process to check the VID and PID in Windows 7 is to go to Device Manager (You can get here if you press Windows key + R, and type devmgmt.msc and hit enter). In most cases, the fingerprint reader will be under the “Biometric Devices” section, but this can vary based on the manufacturer. Expand the heading and right click the device name. Select properties, and navigate to the Details tab. Change the “Property” down arrow to say “Hardware Ids”. Under Value, it will list the VID_# and PID_#.



The Fingerprint Sensor VID and PID are found in Device Manager

7.2. How to Enroll Fingerprints

Fingerprint authentication can be used for Secure Windows. A fingerprint reader is required.

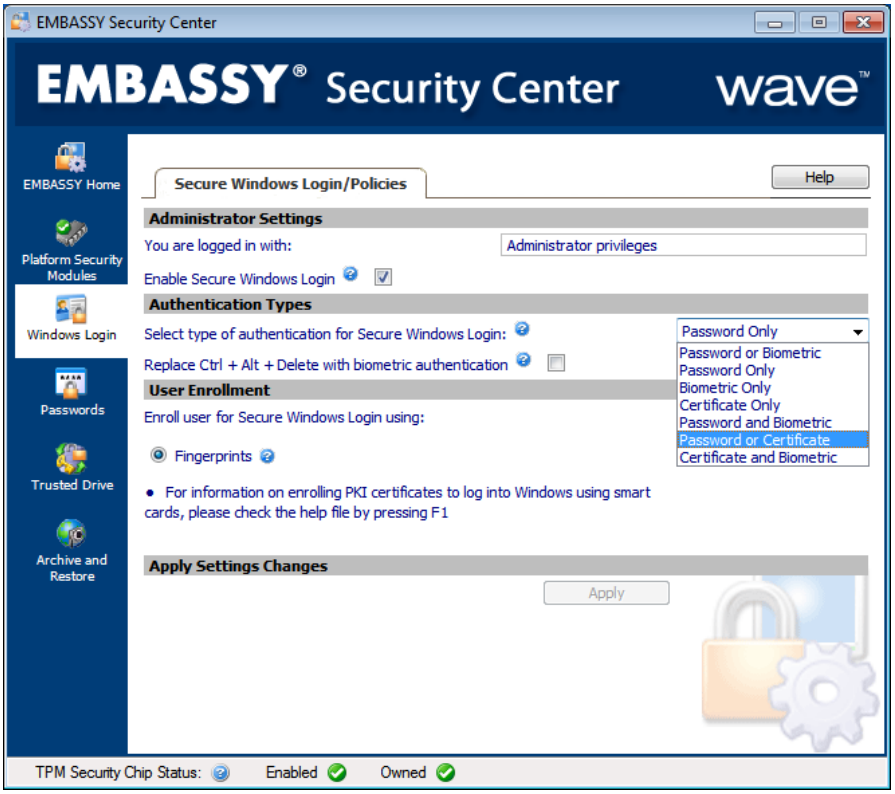
To enroll fingerprints:

1. Click on the "Windows Login" tab at the left
2. Click the **"Enroll/Update"** button
3. Follow the instructions in the wizard. You will be prompted to enter your Windows password before enrolling your fingerprints. You may select which fingerprints you wish to add.

Delete fingerprint - Individual fingerprints may be removed using the same wizard as was used to add them in the first place. On the screen where you select a fingerprint to enroll click on an existing fingerprint, highlighted in green, and select **"yes"** when asked if you want to delete the fingerprint.

7.3. Smart Card at Secure Windows Logon

A smart card can be enrolled for authentication with Secure Windows Logon, provided the smart card middleware is available.



After a valid Windows certificate is placed on the card through the Microsoft Windows Smart Card enrollment process, Secure Windows Logon must be set for certificate authentication. To do this

1. Open **ESC**.
2. Select the **Windows Login** tab.
3. Change the *Select type of authentication for Secure Windows Login* field to one of the following options:
    - Certificate Only
    - Password or Certificate
    - Certificate and Biometric

Create the authentication credentials restricting the credential types to avoid a lock out. Only the authentication credentials selected will be allowed for Windows login.

7.4. Configurable Logon Graphic

The logon graphic for Windows, when Wave secure logon is enabled, can be configured to a different bitmap image than the default Wave logo. Only one logo can be used on one computer at a time, each user will see the same logo.

Requirements:

- Wave Secure Logon must be enabled for the logo to be visible.
- A bitmap image must be used.
- The recommended image size is 128x128 pixels, images of other sizes will be scaled down.

Procedure:

1. Note the location of the logo you wish to use on the endpoint.
2. Create the following registry key as *String Value (Reg_SZ)*.

   HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Wave Systems Corp\Authentication Manager\LogonBitmap
3. Edit the data of the registry key to point to the bitmap.

   EXAMPLE: *C:\Penguins.bmp*

The next time you view the Windows logon screen, it will display the image. To restore the default Wave logo, delete the *LogonBitmap* registry key.

8. Self-Encrypting Drive Management

EMBASSY Security Center 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, however drive locking is selected by default when initializing the drive).

- **TPM Management Not Required** – While both the TPM and SED use related technology to secure authentication and data, the TPM does not need to be configured or present to utilize the SED.
- Docking stations are supported for laptops with SEDs.

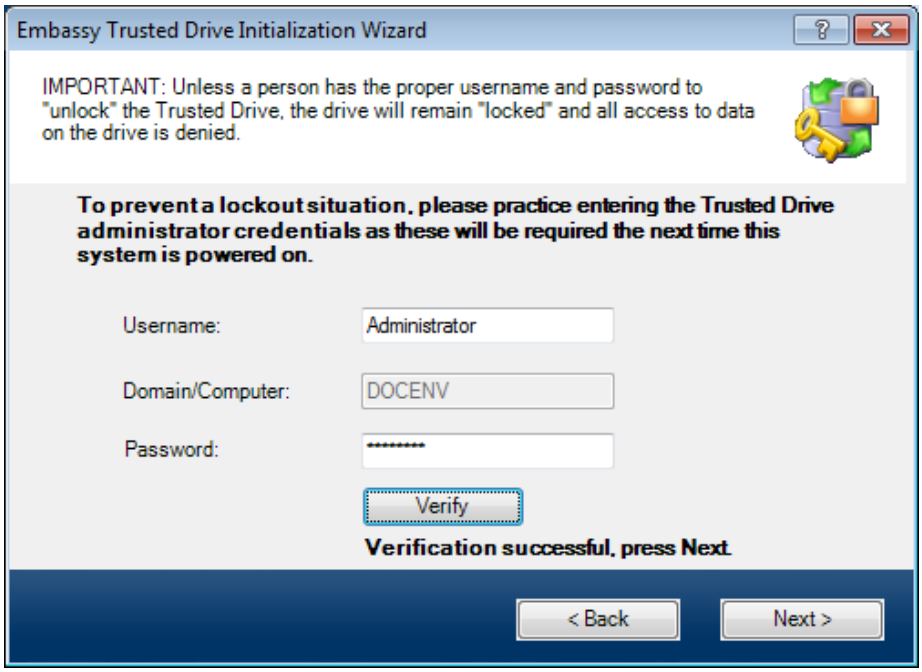
8.1 Initializing Drive Security

Although the self-encrypting drive data is always encrypted, data will not be protected from unauthorized access until the drive is initialized and locked. To initialize the drive through ESC, follow these steps:

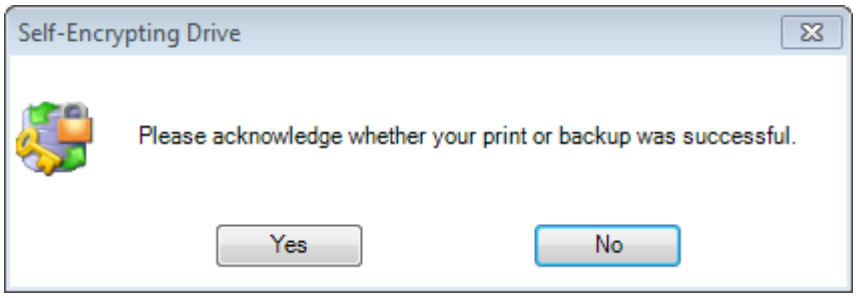
1) Open **ESC**.
2) Select the **Trusted Drive** tab at the left.
3) Select the desired drive from the dropdown menu
4) Click **Initialize**"
5) ESC will notify you that Sleep/Standby is not supported with an initialized drive, and will change your Windows settings from Sleep to Hibernate.
6) On the next screen, enter a valid Windows username.
    - Only a domain user or a user that has previously logged into the computer can be selected and added to the drive, unless the user is added to the drive remotely using the ERAS server (sold separately).
    - All available users who can be added to the drive can be found by clicking **Select**.
    - The drive administrator can add additional users to the drive, disable the security of the drive, or cryptographically erase the drive.
    - The first user added will be the drive administrator.
    - There may only be one drive administrator per drive.
    - A password that meets the Windows password complexity requirements must be entered.
    - Password complexity requirements that are enforced for your system may be viewed from the *Windows Control Panel > Administrative Tools > Local Security Policy > Account Policies > Password Policy*.

7) Enter the username and password again at the practice screen.

8) Click **Verify**. This step is mandatory, in order to prevent lockout in the case of a forgotten username and/or password.



9) A prompt will display as a reminder to back up the username and password.
CAUTION: The username/password can be saved as an electronic file or printed out and kept it in a secure place. Do **NOT** save it to the drive that is being initialized, or the password file will not be accessible if the password is forgotten. You will be prompted to acknowledge if the backup was successful.



IMPORTANT – if you do not back up the password, you will not be able to recover access to the data should the password be forgotten.

10) A *Drive Initialized* screen will display. The security has been enabled on this self-encrypting drive, and password authentication will be required to access the data.

11) Click **Done** to complete the initialization process.

8.2 Un-initialization

Un-initialization will not delete drive data, but will remove the drive security, remove all users, and allow the drive to be initialized by someone else. Once un-initialization is complete, the drive will not require any authentication on any computer before allowing access to the data.

To un-initialize the drive:

1. Logged into Windows with the same account as the drive administrator
2. Launch **ESC**.
3. Navigate to the **Trusted Drive** tab
4. Select the appropriate drive letter.
5. Click **Manage**.
6. Click **Un-Initialize**.
7. The data on the drive can now be accessed without authentication.

8.3 Secondary Drive Support

ESC supports secondary the following for secondary SED drives:

A. StarTech SAT2510U2E enclosures with all SEDs except for DriveTrust (non-Opal) drives

B. CMS CE Secure DiskVault Wave Edition

After the drive is locked, it can be unlocked by another computer running ESC 2.9. When the drive is attached to the computer, the client software will display an authentication prompt.

Policies work differently on secondary drives than primary drives. With a primary drive, policies may be changed after the drive is initialized; however with a secondary drive policies are set at the time of initialization and cannot be changed without re-initializing the drive. The only policies that apply to secondary drives are:

- Remember last user
- Display all users
- Recovery Methods

Drive pairing is available in ESC 2.9. When the credential to unlock the drive is provided at pre-boot, ESC will automatically unlock both the primary and secondary drives. This is only available when locking the drives from ERAS.

8.4 Extended User Support

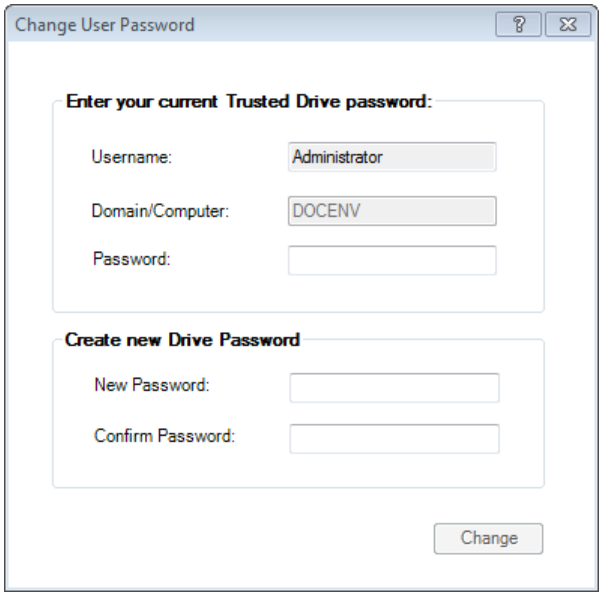
ERAS managed drives can support more users than normal using the "Extended Users Support" (EUS) server setting. The table below lists examples of how many users you can add to a drive. The total number of users will vary, depending on factors such as the length of each user name, and any custom pre-boot messages.

Drive	Model	Firmware	Max Users Without EUS	Max Extended Users With EUS
Seagate OPAL	ST320LT014-9YK142	0001SDM7	16	300
Hitachi (not thin drives)	HTS727575A9E365	JF4OA320	8	300
Micron	C-400MTFDDAA256MAM	040B	16	300
Samsung	PM830 (256GB)	CXM72L15	8	300
Samsung	PM810 (256GB)	AXM77D1Q	4	77
Seagate DT	Holiday ST9250414ASG	DED1	4	27

8.5 Changing your Password

Only the currently logged in user can change their password. This is a separate password than the Windows password, and is used to authenticate to the drive. To change your password:

1) Launch ESC and navigate to the "Trusted Drive" tab and click the "Change Password" button.
2) The "Change User Password" screen will appear. Enter the old password once and new password twice, and then click "Change".
3) When changing the drive administrator password, you will be prompted to back up the new password to a text file or printout. It is recommended you store these in a safe location you can access if you forget your password. Please discard your previous backup after creating the new one.



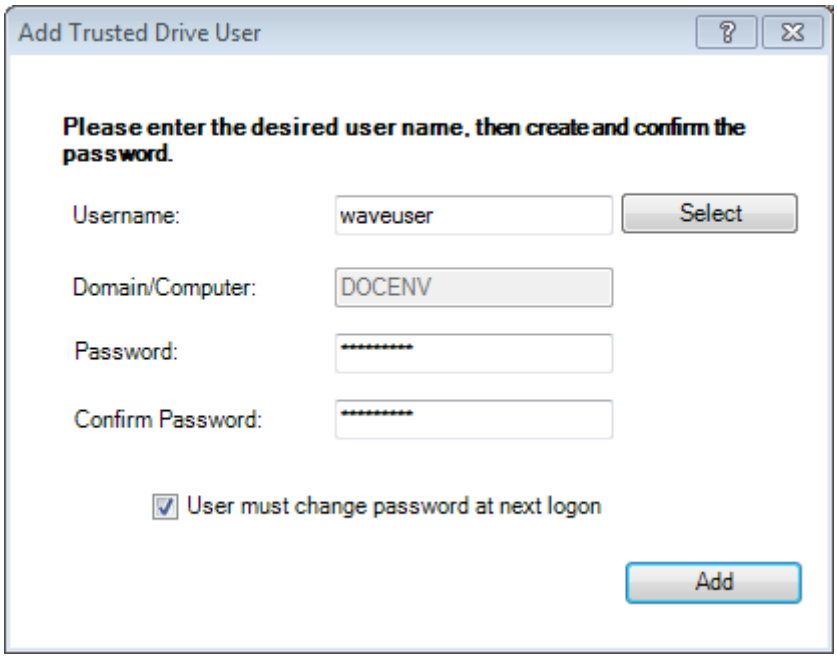
While only the currently logged in user can change their password from the change password screen, the drive administrator can change any user's password from the "Trusted Drive Advanced Settings" management screen which can be accessed by pressing the "Manage" button in the "Trusted Drive" tab.

8.6 Add a User

You can add additional users to unlock each drive. The number of users you can add depends on the space made available by the hard drive manufacturer. Only the drive administrator can add more users, and all users must be existing users on the same domain or workgroup computer.

1. Launch ESC and navigate to the "Trusted Drive" tab and click the "Manage" button. (The drive must first be connected and unlocked by authenticating to it before the "Manage" button will appear)
2. The "Trusted Drive Advanced Settings" screen will appear. At the bottom left is the "Add User" button. Click this button to bring up the "Add Trusted Drive User" screen.
3. Enter a valid Windows user for the PC and click Add.

A drive user is anyone who can authenticate to the drive to access the data. ESC requires that a drive user also be a valid Windows user for the PC where the user is added to the drive.



User must change password at next logon – means the user will need to change their password from the one that was assigned to them the first time they logon. This is referred to as FUMC in ERAS. More details can be found under "First Use Must Change"

Once the additional user has been added, the user will appear in the "Trusted Drive Advanced Settings" screen under "Trusted Drive Users". This user will not have Admin privileges, and cannot add more users unless this user is made the drive administrator (see Change Drive Administrator below).

Trusted Drive Users

Windows Login Name	Domain	Privileges	Trusted Drive Alias
waveuser	DOCENV	USER	
Administrator	DOCENV	ADMIN	

User Self-Enrollment

User Self-Enrollment is a feature where a user can logon to Windows and the ERAS server will lock the drive and add the user who has just logged in, setting that user's password to their Windows password. The enablement of this feature will add the first person who logs on to a computer as a self-encrypting drive user by default. You can add custom scripting to add your own customized logic through a batch file on the server to determine if a user should or should not be added to the drive. Once the server has been configured, as described in the ERAS Manual, the client must be set up for User Self-Enrollment.

If the batch file on the server is customized to not permit a particular user to be added to the drive, the user will not be able to log on to Windows.
After User-Self Enrollment completes and a user has been added to the drive, any user can log onto Windows normally, but only self-encrypting drive users added by ERAS can unlock the drive. User Self Enrollment will only add one user, but additional users can be added through ERAS.

User Self-Enrollment requires:

- ERAS and ESC 2.9.4 or greater
- Windows 7

User Self-Enrollment is set up at the client following these steps:

1. Turn on the Wave Credential Provider, you can do this by turning on the *Enable Wave secure logon* GPO.
2. Navigate to *HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Wave Systems Corp\Authentication* Manager in the registry and create the following three registry keys:

Name: EndpointEnrollmentServiceHost
Type: REG_SZ
Data/Function: String value of Endpoint Enrollment server. This can be Fully Qualified Domain Name (FQDN), NetBIOS, or IP, however if SSL is used, it must match what is used on the SSL certificate (usually FQDN).

Name: EndpointEnrollmentServiceSSLEnabled
Type: REG_DWORD
Data/Function: 32 bit value (1=SSL on; 0=SSL off)

Name: SEDSelfEnrollErrMsg
Type: REG_MULTI_SZ
Data/Function:Customer defined multi-string error string value.

3. Navigate to *HKLM\Software\Wave Systems Corp.\Authentication Manager* and set the following registry key:

Name: EngageSEDSelfEnroll
Type: REG_DWORD
Data/Function:Triggers the SED Self-Enrollment feature upon logon. 1=enables self enrollment on the next logon. 0=self enrollment disabled.

8.7 Remove a User

The drive administrator can remove other drive users, and the removed user will no longer be able to authenticate to and unlock the drive. The data on the hard drive is not lost, but can only be accessed by a user with a valid user account and password. If the maximum of drive users has been reached, then removing a user will free up space to add another user. To remove a user:

1. Launch ESC and navigate to the “Trusted Drive” tab and click the “Manage” button and authenticate with the Drive Administrator. The list of Trusted Drive Users will appear in the “Trusted Drive Advanced Settings” under “Trusted Drive Users”.
2. Use the mouse to highlight the user, and click remove at the bottom right of the screen.

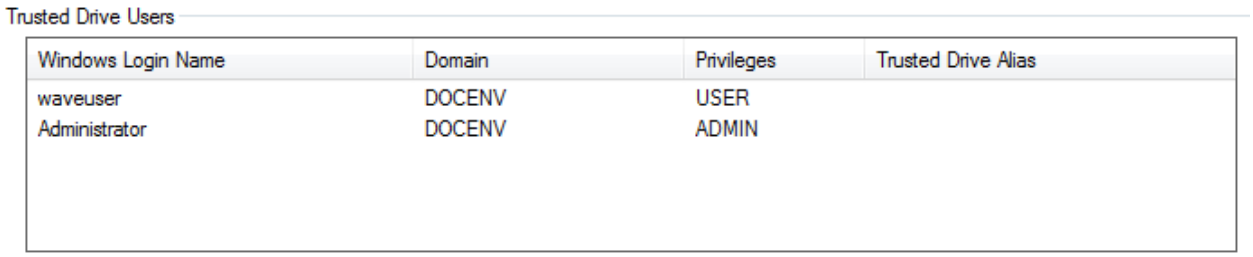
A drive administrator can only be removed by un-initializing the drive.

8.8 Change Drive Administrator

To change the drive administrator, you will use the “Change Name” button. The new administrator must be a valid Windows user, and not already a drive user. The old administrator will no longer be a user for the drive and will not be able to authenticate to the drive, unless they are re-added as a user.

In order to change the drive administrator

1. Launch ESC, navigate to the “Trusted Drive” tab and click the “Manage” button.
2. Highlight the current administrator at the bottom of the “Trusted Drive Advanced Settings” screen.
3. Click the “Change Name” button at the bottom right. (you will be prompted to backup credentials)



On the pop-up screen that appears, select the new drive administrator, and enter a password for the new administrator.

8.9 Disable and Enable Locking

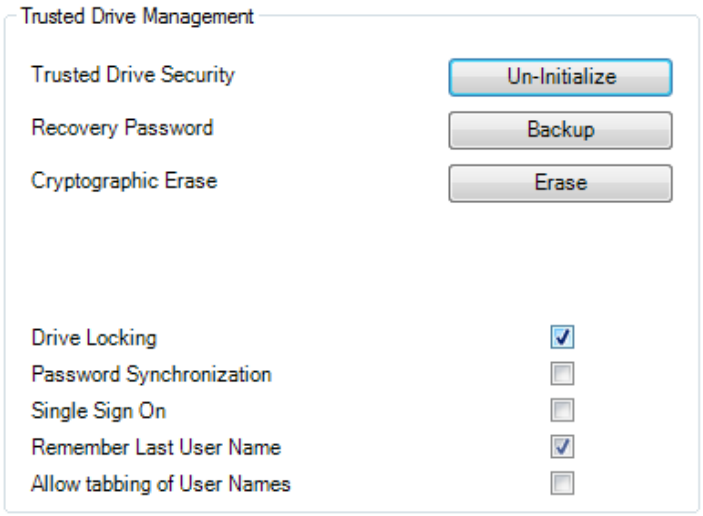
The drive security can be turned off so that the data on the drive can be accessed without authentication. If the security is turned off, users will not need to authenticate to the drive or have any special software installed to access it. The users already present on the drive will not be deleted, nor will data be deleted. When the drive locking is turned off, the drive is still initialized and cannot be initialized by anyone else; meaning no one else is able to manage the authentication and security functionality. When locking is turned back on, authentication will be required once again and the users that remained on the drive will be able to authenticate.

To Disable or Enable Locking:

1) Logged into Windows with the same account as the drive administrator.
2) Launch **ESC.**
3) Navigate to the **Trusted Drive** tab.
4) Click **Manage**.
5) **Uncheck** (clear) *Drive Locking*.

   NOTE: The *Trusted Drive Advanced Settings* screen contains a list of several features with checkboxes.
6) Click **Done**.

   NOTE: The drive can now be accessed without credentials. Afterwards, you can return to this screen to check drive locking and turn the security back on. Drive Locking is turned on by default after the drive has been initialized.



Additional Features On This Screen – Password Synchronization, Single Sign On, Remember Last User Name and Allow tabbing of User Names are all features that do not apply to secondary drives in this software release. While they can be checked, selecting them will not change the behavior of a secondary drive.

Disabling drive security exposes the encrypted data to ANY user who gains access to the drive on ANY computer.

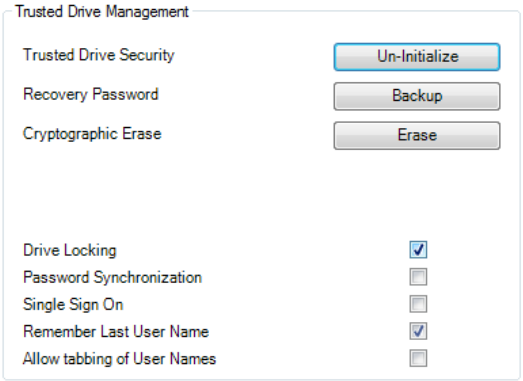
8.10 Crypto-erase

Crypto-erase will delete all data on the drive, and remove any users or security settings on the drive. Crypto-erase is a safe way to dispose of or repurpose drives without compromising the data that was on them. Following the crypto-erase, standard tools can be used to reformat and re-use the drives. Only an initialized drive can be crypto-erased.

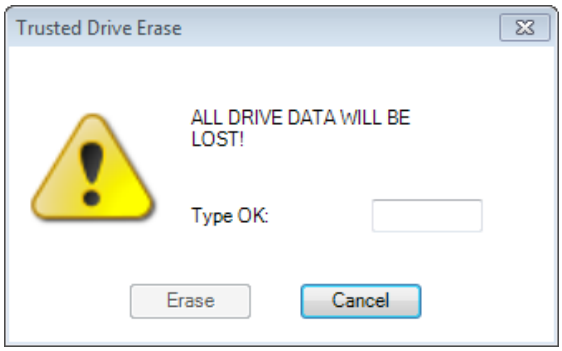
This process is not reversible, once the drive is crypto-erased, the data cannot be recovered from the drive.

To perform a crypto-erase:

1. Log into Windows with the same account as the drive administrator.
2. Open **ESC**.
3. Select the **Trusted Drive** tab.
4. Click **Manage**.
5. Click **Erase**.



6. Type ***OK*** with capital letters
7. Click **Erase**.



8. A warning message will appear.
9. Click **Proceed** to continue erasing the drive.

   NOTE: The "System will immediately crash" message refers to systems where the SED is a primary drive. A crypto-erase of a primary drive will cause a system crash, but it won't cause the system to crash if erasing a secondary SED.

8.11 Keyboard Support in Pre-boot

For the *supported* keyboard layouts below, the user name and password can be entered in the pre-boot authentication screen for TDM using the connected keyboard. The following keyboard layouts are fully supported for ESC 2.9 – both for TDM pre-boot authentication and for managing TDM in ESC while in Windows:

US English, Chinese Simplified PRC - US Keyboard, Chinese Traditional Hong Kong S.A.R - US Keyboard, Chinese Simplified Singapore - US Keyboard, Chinese Trad. Macao S.A.R - US Keyboard, US-International, Canadian French, Czech QWERTY, Turkish Q, Danish, French, Greek, German, Hungarian, Italian, Dutch, Norwegian, Polish Programmer, Polish 214, Portuguese, Romanian, Russian, Swiss French, Swiss German, Slovak, Spanish, Finnish, Swedish, Portuguese Brazil ABNT, Croatian, Slovenian, United Kingdom, Irish, United Kingdom Extended, Belgian French, Canadian French (Legacy), Belgian (Comma), Slovak (QWERTY), Canadian Multilingual Standard, and Korean.

To change the keyboard layout in pre-boot:

1. Click the button at the top left of the pre-boot screen and select the keyboard layout desired. (This can also be adjusted as a policy with the ADMX/ADML that ships with ERAS).

NOTE: Any keyboard that uses an IME (for example Korean or Chinese) can be used, but it does not support the IME itself. Each key press will represent one character, and the IME (input method editor) will not be used. Numbers on the keypad will not represent numbers on the number pad. This is the case for all other keyboards that use an IME as well.

Note: The list of keyboard layouts is not the same as the list of languages ESC is localized in.

On-screen Keyboard Usage

ESC includes an onscreen keyboard that can be used to enter the drive password. To make it appear, click the keyboard icon at the bottom left of the pre-boot screen. If you click the keyboard icon a second time, it will disappear. This keyboard can always be accessed with a mouse.

ESC comes with an on-screen keyboard

It is supported with a touchscreen on the following platforms:

- Panasonic Toughbook CF19 Mark4
- Panasonic Toughbook CF19 Mark5
- Panasonic Toughbook CF-H1
- Panasonic Toughbook CF-H2
- Motion Computing J3500

If touch feedback does not match the actual touch location the user will be allowed to calibrate the input device.

There are two ways to access the calibration screen:

A. Gestures

Using any input device draw two crossing lines anywhere on the screen. If using a mouse, use the left mouse button.

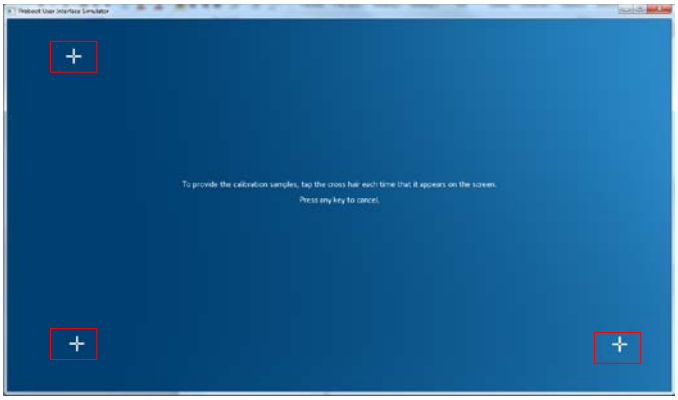
Note – Line direction does not matter, the lines only need to cross.

B. Access Button

1. Pressing the access button on the lower left corner .
2. Choose **Screen Calibration** from the menu.

Access Button

Once the calibration routine is launched the user will be prompted to tap on the cross hairs that are displayed. It is important that they tap using the device that needs calibration.



In order to cancel the calibration routine the user will need to press any keyboard button. Tablets normally provide some button inputs that are treated as keyboard keys, so pressing any of these buttons will cancel the calibration routine.

8.12 Drive Recovery

Drive recovery enables IT staff to deliver an out-of-band password to recover a locked drive. This is done through what is called a challenge-response. The client with the lost password will pull up the recovery screen and be displayed a challenge, a series of thirteen characters, to be read to the IT staff member. The IT staff member will then use the challenge to generate a recovery password, which the client will enter into pre-boot to unlock the drive.

For Challenge-Response Recovery, Wave offers:

- Drive-based Challenge-Response Recovery (128 bit)
- Drive-based Challenge-Response Recovery (256 bit)
- User-based Challenge-Response Recovery (128 bit)
- User-based Challenge-Response Recovery (256 bit)

One offers a shorter recovery password to type (128 bit), and the other offers additional cryptographic strength. Both methods are secure. If AES 256 is required, an AES 256 SED is recommended with a 256 bit recovery mechanism. For each ESC challenge-response recovery mechanism, a thirteen character recovery challenge is provided from the client to the IT staff member. The IT staff member will then provide a thirty-one character recovery password if the drive uses 128 bit recovery mechanism, or a sixty-two character recovery password if the drive uses a 256 bit recovery mechanism..

Most will prefer to use User-based Challenge-Response Recovery because it will automatically sign one into their Windows account, even if the Windows password is forgotten. The automatic sign into Windows after recovery requires the Single-Sign on policy to be configured. To access the User Recovery screen, press the CTRL key and ‘R’ key simultaneously at the pre-boot screen.

The other recovery method is called Drive-based Challenge-Response Recovery. Both Drive-based and User-based will unlock the drive, however Drive-based will not automatically sign one onto Windows. Drive-based Challenge-Response Recovery would typically be used by IT Staff when unlocking a computer for service. To initiate Drive-based Challenge-Response Recovery, press the CTRL key and ‘X’ key simultaneously at the pre-boot screen.

Each set of letters are grouped between hyphens, and contain a checksum. If a set of letters between hyphens are typed incorrectly, you can go back and correct them before moving forward.

The challenge/response uses Base-32 encoding. This means a challenge, or recovery password will never contain numbers one ‘1’, or zero ‘0’. This helps to prevent confusion with the letters “I” and “O”

Primary Drive Recovery with ERAS

Challenge Response Recovery Procedure**:**

1. Click **Forgot you password?**.
2. Select the appropriate recovery method in the drop-down
3. **IF APPLICABLE**: Select or enter the user and domain name to the recovery type.
4. Click the **white arrow** to continue.
5. Share the *Recovery Challenge value* with network helpdesk; they will use it to generate your Recovery Password.
6. Enter the *Recovery Password*
7. Click **Unlock**.

Example of Challenge Response Recovery Screen

Password Recovery Procedure**:**

1. Click **Forgot Your Password**.
2. Select **Drive-based Password Recovery**.
3. Enter the *recovery password* obtained from ERAS.

   NOTE: Your IT administrator or help desk should provide this to you.

Example of Password Recovery Screen

Mobile Unlock - Local Management Access Recovery

IMPORTANT: If you do not back up the password, you will not be able to recover access to the data should you forget the password.

During the initialization of drive security or when changing your administrator password, you will be asked to back up your drive username and password as a text file or as a printout. It is highly recommended that you back up these credentials, and that you back them up to a drive (e.g. removable media, but not the drive that was locked) or print them. Otherwise, if you lose access to the drive with the backup you will not be able to access your credentials. You may also back up the credentials by going to:
ESC -> Trusted Drive -> Manage -> Backup

To recover from a lost password situation:

A. If your backup is on a USB flash drive, insert the flash drive into another computer and read the text file for the administrator username and password that must be used. Plug in the drive and enter the administrator username and password when prompted to unlock the drive.

B. If your backup is on a printout, refer to the printout to find the administrator username and password.

IMPORTANT: Do **NOT** leave the backup in an area that is accessible to others, as the administrator username and password might be compromised.

8.13 Warm Reboot for Multiple Partitions

ESC supports booting from multiple partitions using Microsoft Boot Manager. Other partition manager software such as GRUB is not supported. If a computer has a boot loader with multiple partitions, the BIOS may not be able to recognize the entire drive when the computer is first turned on. You can configure ESC to perform a warm-reboot to give the BIOS a chance to recognize these partitions and boot correctly. This may be configured by a Windows Group Policy (GPO) or locally on the client. If only one option is available, this means it has already been configured remotely by GPO.

This feature only needs to be configured if the computer cannot boot, and is best left alone if changes are not necessary. Enabling it will cause the total boot time to take slightly longer. It can be enabled through the shutdown/restart button at the bottom right of the screen. Any changes made through this menu will only be saved upon login. If you change the setting and shutdown or restart immediately afterwards without logging in, the setting will revert.

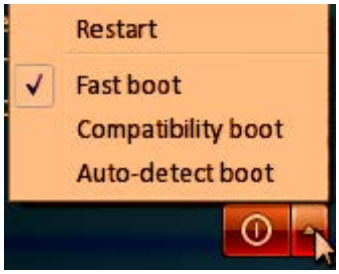


Figure 1 - Options for Warm Reboot

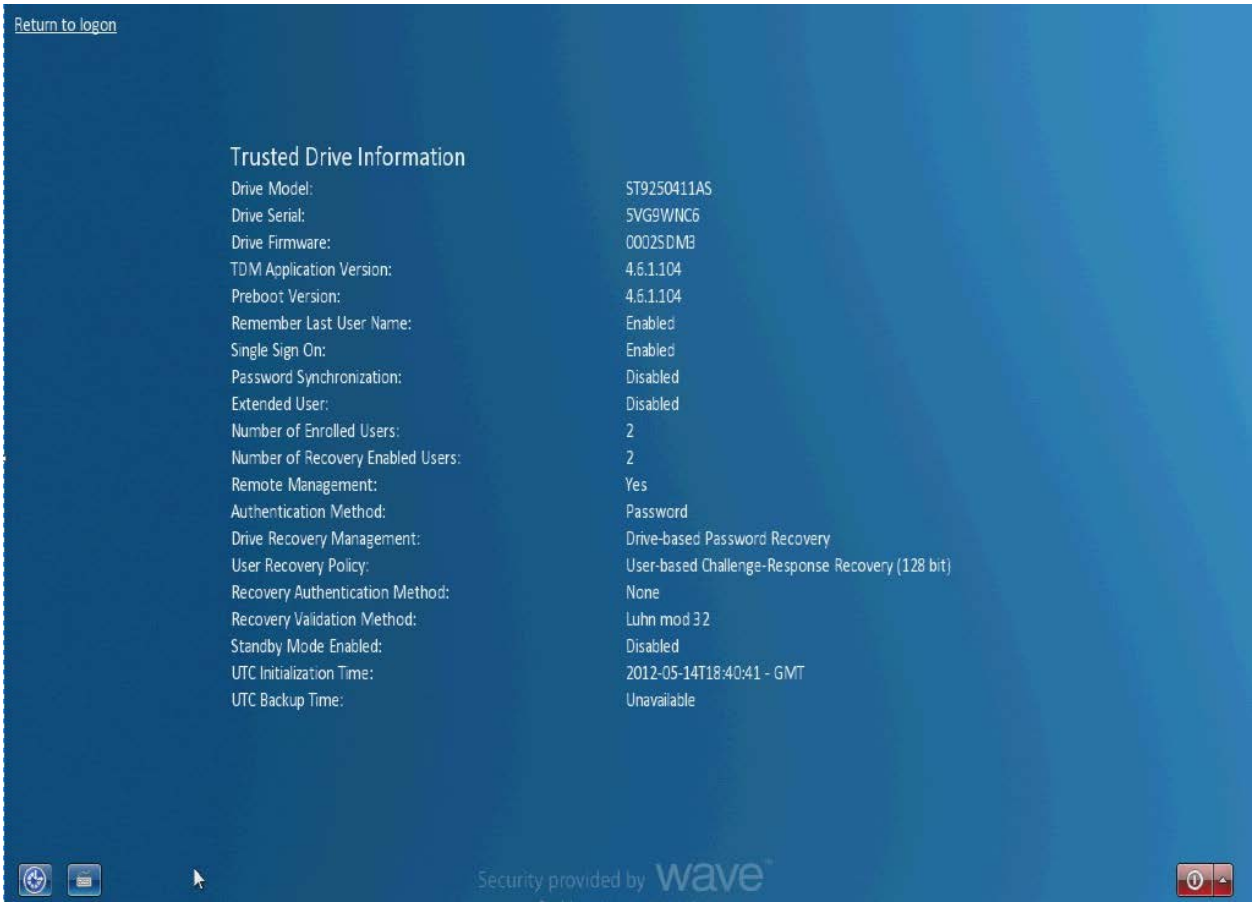
Fast boot – The computer will boot normally. This is the fastest option, and is set by default.

Compatibility boot – The computer will automatically restart once, giving the BIOS a chance to detect all the available partitions on the drive and follow any boot loader instructions. The boot time will take slightly longer when enabled.

Auto-detect boot – If a USB mass storage device is detected, the computer will automatically restart, similar to Compatibility boot. If no USB mass storage device is detected, the computer will boot normally, similar to Fast boot.

8.14 Diagnostics Screen

Information about the recovery, the self-encrypting drive, and the ESC software installed is available through a diagnostics screen. This screen can be accessed by pressing CTRL + D at any time while in pre-boot.



Example of Diagnostics Screen

8.15 Notifications

Embassy Security Center provides notifications that inform the end user of changes made to the self-encrypting drive. They appear as notification balloons in the notification area near the bottom right of the screen, and as logs in Windows Event Viewer.

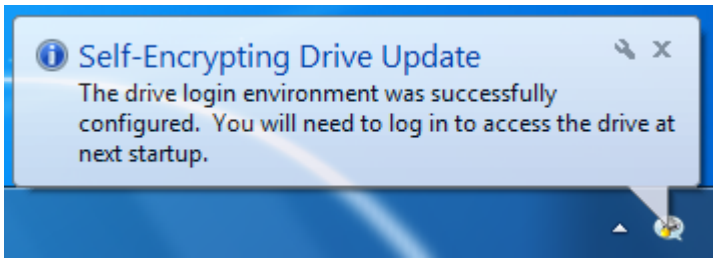


Figure 2 - Notification Balloon Displayed When Drive Configured

8.16 Event Viewer Notifications

The notifications relating to self-encrypting drives are listed under “Windows Logs” -> “Application” in Event Viewer. They can be filtered in event viewer by selecting “Wave Platform Security” as the source, and using the task category “Wave Platform Trusted Drive Security Events”. Most events are “Information” level, however a warning is issued when the drive is uninitialized.

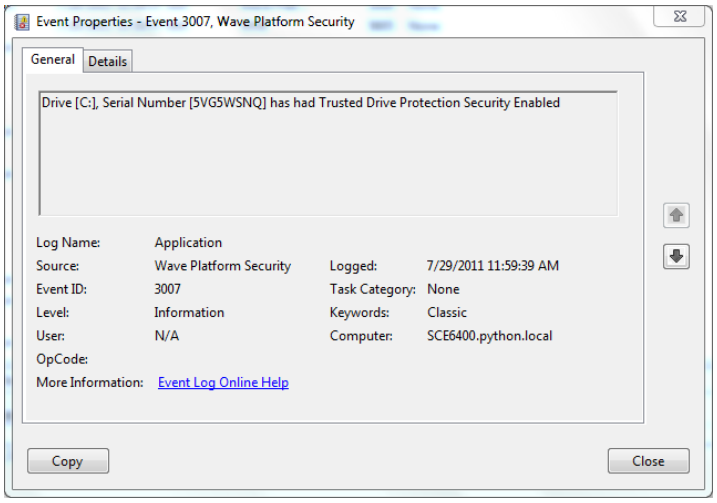


Figure 3 - Log Recording Drive Locking in Event Viewer

Event Viewer Notifications:

Message ID	Event
Event ID 3000	Initialization started.

Drive [Letter], Serial Number [Serial Number] is being initialized.

- Indicates drive initialization has begun. If the computer is shut down before this process completes unexpected behavior could occur.

Event ID 3001 Initialization failed.

- The drive could not be initialized. No changes have been made to the drive.

Event ID 3002 Initialization succeeded.

Drive [Letter], Serial Number [Serial Number] has been initialized, Drive Administrator is User [Domain\Username].

- The drive is initialized. The named user is the only one who can make administrative changes to the drive. The Drive Administrator will be the ERASService account in most enterprise deployments.

Event ID 3003 Un-initialization started.

Drive [Letter], Serial Number [Serial Number] is being uninitialized.

- Indicates drive un-initialization has begun. If the computer is shut down before this process completes unexpected behavior could occur.

Event ID 3004 Un-initialization failed.

- The drive could not be un-initialized. No changes have been made to the drive.

Event ID 3005 Un-initialization succeeded.
Drive [Letter], Serial Number [Serial Number] has been successfully un-initialized

- The drive protection is disabled, all users have been removed, anyone can access the drive

Event ID 3006 Drive admin changed.

- The drive has a new administrator. When remotely managed, the ERAS Service account should be the drive administrator.

Event ID 3007 Drive admin change failed.

- The drive administrator could not be changed.

Event ID 3008 Drive user added.
User [Domain\Username] has been granted permission to Drive [Letter], Serial Number [Serial Number].

- This user now has rights to access the drive. If using smart card, they still may need to provision the smart card to the drive, in which case they can use either a temporary password or recovery method to unlock the drive for the first time.

Event ID 3009 Drive user addition failed.

- A user could not be added to the drive. No changes will be made to the other users assigned to the drive.

Event ID 3010 Drive user removed.
User [Domain\Username] has had access to Drive [Letter], Serial Number [Serial Number] removed.

- This user can no longer authenticate to the self-encrypting drive. If they require access, they can be added to the drive through ERAS, or use a recovery method.

Event ID 3011 Drive user removal failed.

- A user could not be removed from the drive. Their credentials can still be used to unlock the drive.

Event ID 3012 Drive user's password changed successfully.

- The user’s password has changed, the old password will no longer unlock the drive.

Event ID 3013 Drive user's password change failed.

- The drive user’s password could not be changed. They will need to continue to use their old credentials to unlock the drive, unless a new password can be provided.

Event ID 3014 Drive security enabled successfully.
Drive [Letter], Serial Number [Serial Number] has had Trusted Drive Protection Security Enabled.

- The drive is now locked, and now requires authentication.

Event ID 3015 Drive security enabling failed.

- The drive could not be locked, authentication will not be required to unlock the drive.

Event ID 3016 Drive security disabled successfully.

- The drive is no longer locked. It may still be initialized, and retain user information and credentials.

Event ID 3017 Drive security disabling failed.

- The drive security could not be turned off, this means credentials will still be necessary to unlock the drive.

Event ID 3018 Drive recovery method set successfully.
Drive [Letter], Serial Number [Serial Number] has been enrolled with Password Recovery Service.

- ERAS can generate a recovery password to un-lock this drive

Event ID 3019 Drive recovery method failed to set.

- The CRRP II recovery response for service access drive recovery could not be validated. The drive cannot be locked if the drive recovery method fails to set and no users are present on the drive.

Event ID 3020 Preboot update is pending.

- The secure area of the drive needs to be updated. The ERAS administrator can do this by refreshing the drive through the ERAS console. A local drive administrator can do this through the manage screen in the Trusted Drive tab.

Event ID 3021 Preboot update started.

- The secure area of the drive is being updated. If the computer is powered down before this completes, unexpected behavior may occur.

Event ID 3022 Preboot update failed.

- The secure area of the drive could not be updated. A pre-boot update must still be performed either remotely through a refresh in ERAS, or locally through the manage screen in the Trusted Drive tab.

Event ID 3023 Preboot update succeeded.

- The secure area of the drive was updated, a pre-boot update is no longer necessary.

Event ID 3030 Credential sync (SSO/WPS) started.

- The process to update the credentials for Single Sign-On (SSO), or Windows Password Synchronization (WPS) has started. If the computer is powered down before this completes, unexpected behavior may occur.

Event ID 3031 Credential sync failed.

- The credentials for SSO could not be captured by the drive, or the drive password could not be synchronized with the Windows Password.

Event ID 3032 Credential sync succeeded.

- SSO and/or WPS have successfully been updated.

Event ID 3033 Smart card enrollment started.

- The smart card is being enrolled to the drive. Once complete, the user can unlock the drive using the smart card as a credential.

Event ID 3034 Smart card enrollment failed.

- The smart card could not be enrolled, and will not be able to unlock the drive. A temporary password or recovery password may be necessary to unlock the drive, depending on its lock status.

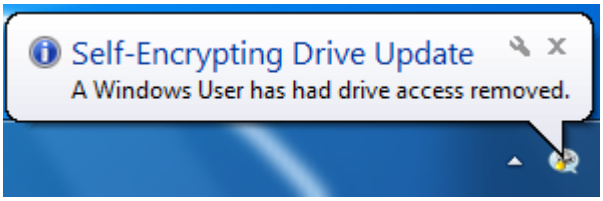
Event ID 3035 Smart card enrollment succeeded.

- The smart card can now be used as a credential to unlock the drive. If a temporary password was assigned, it can no longer be used to unlock the drive.

Event ID 3036 Smart card enrollment is pending.

- There is account on the drive that must enroll their smart card to the drive.

8.17 Notification and Error Messages



Several Error messages appear in the Notification area as balloons. These messages can be used to help troubleshoot issues. The IT staff troubleshooting the issues can check the Application logs in event viewer locally, or from the ERAS console.

These bubble notifications appear when the drive is being initialized, and locked:

- The drive login environment is being configured. Please do not turn off your computer.
    - Take care not to turn off the computer while initializing the drive. If it is turned off during initialization, it may cause unexpected behavior. Typically this process takes less than a minute, however remotely managed users may not understand what it means, as the process is generally initiated remotely.
- The drive login configuration was unsuccessful. Please contact your administrator for assistance.
    - The drive could not be initialized. You will still log into the computer the same as before.
- The drive login environment was successfully configured. You will need to log in to access the drive at next startup.
    - The drive was successfully initialized. Unless it was initialized, and unlocked, you will need to enter valid credentials to unlock the drive the next time it is turned on. These credentials can include a temporary password, a recovery password, or a smart card after it has been enrolled either through auto enrollment or using the TDM enrollment wizard.

These bubble notifications appear when changes are made to the drive credentials:

- Your drive login information is being updated. Please do not turn off your computer.
    - If the drive is turned off while the credentials are being updated, it may cause unexpected behavior
- Your drive login information was not successfully updated for Single Sign-On to Windows. Please contact your administrator for assistance.
    - This error message means single-sign on will not work. After unlocking the drive you will need to sign on again at Windows.
- Your drive login information has been successfully updated for single sign-on to Windows.
    - You will be automatically signed on to Windows the next time the computer is powered on and the drive is unlocked.

- Your drive login information has been successfully updated. You can now use your Windows password to access the drive.
    - You can now use your current Windows password to unlock the drive. The previous password has been over-written and will no longer work.
- Your drive password was not successfully updated with your Windows password. Please contact your administrator for assistance.
    - You will continue to authenticate to both the drive and to Windows. Your drive password has not changed.
- Your smart card is being configured to access the drive. Please do not turn off your computer.
    - If the drive is turned off while the smart card is being configured, it may cause unexpected behavior.
- Your smart card was not successfully configured to access the drive. Please contact your administrator for assistance.
    - Your smart card cannot be used to authenticate to the drive. If the drive is locked, you will have to use another method to sign onto the drive. You can use a temporary password if one is available, or a recovery password.
- Your smart card can now be used to access the drive.
    - Your smart card has been successfully enrolled, and can unlock the drive at pre-boot.
- An update is pending to your drive login environment. If you are the drive administrator, click here to perform this update.
    - This commonly occurs after an upgrade or patch. ESC needs the drive administrator's permission to update the drive. This is required to complete the update.
- The drive login environment is being updated. Please do not turn off your computer.
    - Changes are being made to the drive settings. Do not shut down the computer until this process is complete, or else it may cause unexpected behavior.
- The drive login environment was not successfully updated. Please contact your administrator for assistance.
    - Changes could not be made to your self-encrypting drive. Your sign-on experience will not change.
- The drive login environment was successfully updated.
    - Changes have been made to your self-encrypting drive settings. This may include a change in users assigned to the drive.

- A Windows User has been granted access to the drive.
    - An additional user has been given permission to un-lock the drive at pre-boot.
- The drive recovery method has been set.
    - A recovery password can be generated with ERAS to unlock the drive if the user password is lost or forgotten.
- The drive login environment has been un-initialized.
    - The drive is no longer managed by ERAS, and no longer requires authentication to boot.
- A Windows User has had drive access removed.
    - A user has been removed from the drive remotely through ERAS, and will no longer be able to unlock the drive. Recovery methods will still work.

8.18 Smart Card - Authentication

ESC allows for smart card authentication at pre-boot. A user with a smart card containing a valid security certificate recognized by a Windows Certificate Authority (CA) can be granted rights to unlock the drive. The steps to enroll the certificate, which will make the drive recognize the smart card certificate, can vary depending on configuration settings made remotely. You must obtain steps for enrollment from the system administrator who implemented smart card authentication.

Methods to have the self-encrypting drive pre-boot connect the valid certificate to a valid drive user:

A. You must sign into Windows to access the drive. This can be done:

- through recovery
- through a temporary password
- if the drive was previously unlocked but initialized, no additional steps are necessary

B. You must enroll the card to the drive, so that the drive will recognize the certificate. This can be achieved by:

- Navigating to The Trusted Drive tab and initiating the **TDM Enrollment Wizard**.
- Following the **TDM Enrollment Wizard** set by the system administrator.
- Automatic enrollment. When **automatic enrollment** is set as a policy, TDM will automatically enroll the smart card when the user signs on to Windows.

Smart Card - Supported Cards

ESC 2.9.5 supports the following smart cards for pre-boot authentication:

- .NET V2 and V2+ Smart Cards
- Gemalto TOP IM FIPS CY2, also known as Gemalto Cyberflex Access CY2
- GSCIS V2.1 compliant smart cards, including CAC, PIV, and CAC/PIV transitional smart cards

Smart cards require drivers before they can be used, so check the manufacturer's documentation on where they must be obtained.

- First Use Must Change (FUMC) will not affect Smart Card Authentication
- Only one pin can be used per .Net smart card.

Smart Card to SED - Supported Card Readers

Internal smart card readers are supported on Dell and Lenovo Platforms. External smart card readers are supported on Dell, Lenovo, and HP platforms. The external smart card readers must be CCID-compliant. HP platforms require external readers for pre-boot authentication.

Smart Card to SED – Preparation

The smart card must be prepared in advance. Before Wave can enroll the certificate on the card into pre-boot, you must be able to use the card for Windows logon. This consists of three steps; refer to the smart card vendor documentation for guidance on completing these steps – some of them may already be completed.

1. Provision the card - This involves setting up the setting up the PIN, maximum authentication attempts to the card, allocating size for each certificate, and other settings. (.NET smart cards are already provisioned)

2. Install certificates onto the card.

3. Configure the domain to use the certificate for Authentication (CAC/PIV).

Someone in your organization must also remotely initialize the client for Smart card authentication using ERAS before a smart card can be used to authenticate to the drive; this process is documented in the ERAS Admin Manual.

Smart Card to SED - TDM Enrollment Wizard

Depending on settings made on the server, you may need to initiate the TDM Enrollment Wizard to make the SED recognize the self-encrypting drive. This Wizard is also called the Multifactor Enrollment Wizard.

The TDM Enrollment Wizard will ask you for your smart-card pin. This was created before the card was set-up for Windows Authentication. It may also ask for a drive password. This is a temporary drive password used for the purpose of unlocking the drive in order to enroll the smart card.

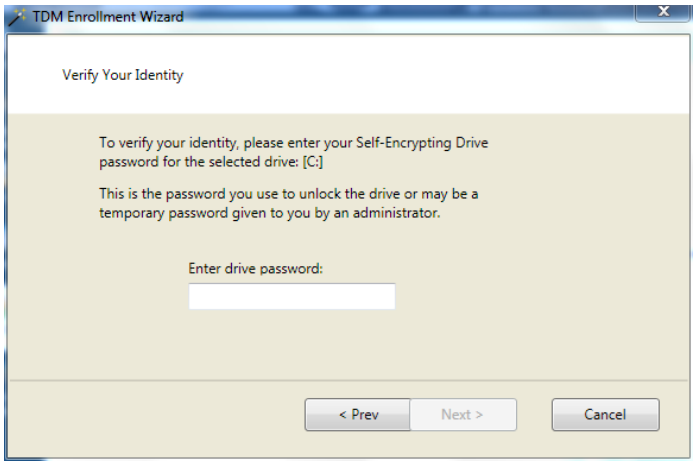


Figure 1 - You may need to enter a password and pin, depending on settings made at the server

Smart Card to SED - Auto-enrollment and Auto-provisioning

A policy may be set remotely by the ERAS Administrator that will automatically enroll the smart card to the drive. The enrollment will occur after the user signs onto Windows with a valid smart card. In addition, the user may or may not need to be provisioned to the drive by ERAS – this is also determined remotely by policy. An example use case could be:

1. The IT staff deliver an unlocked but managed computer and a valid smart card to the end user
2. The end user turns on the computer, but does not need to unlock the drive
3. The end user uses the smart card to sign-on to Windows
4. The policies set remotely by the administrator automatically enroll the smart card, and then lock the drive
5. The end user shuts down the computer, the computer is now locked
6. The user boots the computer, and must use their smart card and pin to unlock the drive

Hibernate and Sleep/Standby

Windows does not natively support sleep/standby (S3) on an SED. When Windows enters Sleep/Standby, the SED is powered down and cannot resume. For the best security, Wave recommends the usage of Hibernate instead. Upon resume from Hibernate, authentication will be required.

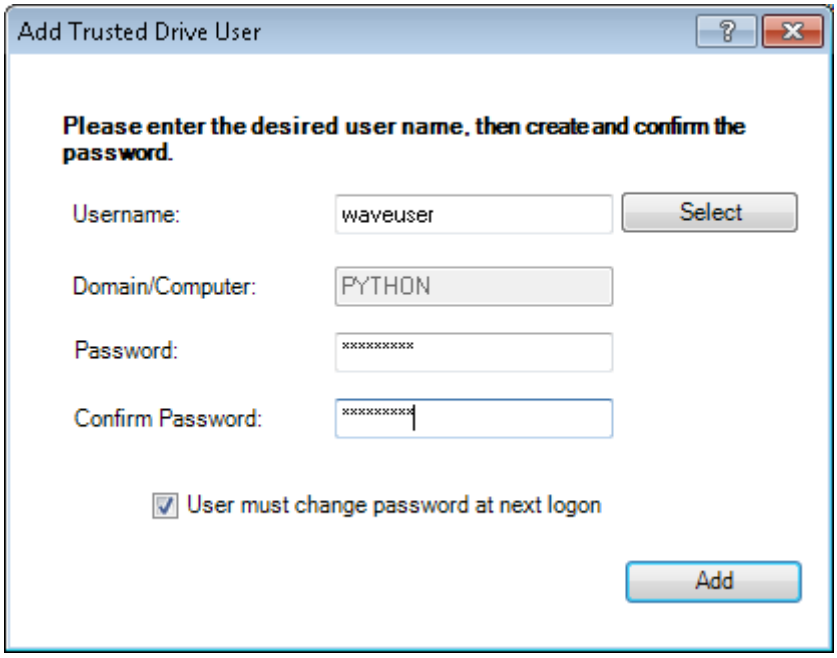
ESC includes a feature to enable Windows to resume from Sleep/Standby even when the SED is locked. This feature is only enabled if the following conditions are met:

- The computer is running Windows 7
- S3 drivers are installed. These are installed by ESC unless omitted.
- The *Enable S3 support for SED* policy, that ships with ERAS, is set.

If using the Sleep/Standby feature on the SED, authentication will not be required on resume from Sleep/Standby. Using Hibernation instead will enhance security and require authentication.

8.19 First Use Must Change

First Use Must Change (FUMC) requires the user to change the password to a different one than what was assigned to them when they first log on. This feature does not apply to a secondary drive, in this case it may remain checked or unchecked. To set FUMC from ESC, select "User must change password at next logon" when adding a new user.



Screen To Add New User

8.20 Windows Password Synchronization

Windows Password Synchronization (WPS) is a setting that will change the drive administrator's password automatically to match the Windows password when it changes.

The drive administrator can set WPS locally:

1. Open **ESC**.
2. Click the **Trusted Drive** tab.
3. Click **Manage**.
4. Select the **Password Synchronization** checkbox.

WPS is not enforced for the drive administrator, and is only applicable to drive users. WPS is applicable to the primary drive, the synchronization event does not occur for the secondary/external drive. Synchronization occurs on user login. With Windows Vista and Windows 7, synchronization will also occur if you lock/unlock the screen. Credentials are synchronized one user at a time, when the user logs in. If using more than one computer with the same logon, the password must synchronize on each computer before ESC can update the drive password on each computer. ERAS ships with a policy to set WPS remotely, documented in the ERAS Manual. When WPS is on, FUMC is disabled because user's drive password is expected to change to his Windows password when he or she logs into Windows.

8.21 Supported Languages

ESC is localized in the following languages, meaning ESC will display text in those languages. For a list of supported keyboards, please view the supported keyboards list.

Arabic, Simplified Chinese, Traditional Chinese for Hong Kong, Traditional Chinese for Taiwan, Croatian, Czech, Danish, Dutch, Finnish, French, German, Greek, Hebrew, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Brazilian Portuguese, Romanian, Russian, Slovak, Slovenian, Spanish, Swedish, Thai, and Turkish.

9. Technical Support

Additional information, technical support and contact information can be found online:

Refer to the Wave Systems website **http://www.wave.com/support/** or

E-mail your questions or issues to: **support@wave.com**

Toll free: (800) WAVE-NET
Tel: (413) 243-1600