

Dell™ ControlPoint Security Manager

Notes



NOTE: A NOTE indicates important information that helps you make better use of your computer.

Information in this document is subject to change without notice.

© 2009 Dell Inc. All rights reserved.

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: *Dell* and the *DELL* logo are trademarks of Dell Inc. *Microsoft* and *Windows* are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

January 2009

Rev A00

Contents

- About Dell ControlPoint Security Manager 3**
- Quick Links. 3**
- Viewing and Configuring Security Devices. 4**
 - Trusted Platform Module (TPM) 5
 - Fingerprint Reader 5
 - Smart Card Controller 6
 - Contactless Smart Card 6
 - Full Disk Encryption. 6
- Configuring Logins and Passwords 7**
 - Selecting a Windows Login Authentication Type . . 7
 - Configuring a Pre-boot Password 7
 - Managing Password Settings 8
- Modifying Data Protection Settings. 8**
 - Configuring the Hard Drive Password 8
 - Configuring the Document Vault 9
 - Modifying File and Folder Encryption 9
- Embassy Security Center 9**

About Dell™ ControlPoint Security Manager

Security Manager provides local management of system security through the use of features such as Trusted Platform Module (TPM), contact and contactless smart card, fingerprint match processing, system disk encryption, and login passwords.

The Security Manager plug-in includes:

- **Security Center Overview**—Lists the system devices and displays the current status; has a tab to launch the independent application ControlPoint Security Manager.
- **Security Status**—Lists the system security devices and displays the current status.
- **Logins and Passwords**—Allows administrators to select login type and manage password settings.
- **Data Protection**—Allows administrators to set the hard drive password, configure the document vault, and modify file encryption.

To configure the installed security devices, click **Manage Security**. Quick Links provides information on the three links available from the lower portion of Security Manager.

Figure 1-1. Security Center Overview Screen



Quick Links

Three quick links are always available from the lower portion of Security Manager:

- **Run security configuration wizard**—Allows you to configure system security devices.
- **Enroll your fingerprint**—Launches the **Fingerprint Enrollment Wizard** and allows you to configure a fingerprint to be used by the fingerprint processing engine. The scanned fingerprint can be used for Microsoft® Windows® login and pre-boot authentication. This task can be launched multiple times for the same user or it can be launched multiple times for different users.
- **Back up security data**—Creates a backup of security data. Use this in the event the current platform is broken or stolen. From the backup, the security data can be loaded to the new replacement platform.

Viewing and Configuring Security Devices

Security Device Status lists the security devices in your system and displays the current status, as indicated by the colored icon. See Table 1-1 for information on the security device status associated with each colored icon.

If you click **Settings**, a wizard launches that helps you configure each security device. Security devices include:

- Trusted Platform Module (TPM)
- Fingerprint Reader
- Smart Card Controller
- Contactless Smart Card
- Full Disk Encryption

Table 1-1. Security Device Status Icon Legend

Color	Status
Green	Enabled
Yellow	Needs Attention
Gray	Disabled and the device is not available to the user
Red	Not installed

Trusted Platform Module (TPM)

Trusted Platform Module (TPM) is a hardware module that stores critical information such as passwords and encryption keys. Because TPM provides hardware-based authentication, a system with TPM can provide more security from unauthorized access than a system that relies strictly on software-based authentication.

The TPM device must be enabled and ownership must be taken in order for security functions to operate properly. For more information, see the Embassy Security Center documentation.

 **NOTE:** Only a user with administrator rights can configure the TPM device.

To configure the Trusted Platform Module (TPM) device:

- 1 Click **Settings** next to **Trusted Platform Module (TPM)**.
- 2 Use **Embassy Security Center** to enable and set ownership of the TPM device. Embassy Security Center also provides TPM device information, such as version number.

Fingerprint Reader

Fingerprint authentication can be used in place of or in addition to the standard Windows password authentication to increase the security of the Windows login. If fingerprint authentication is used for Windows login or pre-boot authentication, enroll a fingerprint prior to enabling fingerprint authentication.

To enroll or update a fingerprint:

- 1 Click **Settings** next to **Fingerprint Reader**.
- 2 Use the **Fingerprint Enrollment Wizard** to enroll or update a fingerprint. Follow the onscreen prompts.

Smart Card Controller

Contacted smart cards are pocket-sized plastic cards that have an embedded silicon chip containing user information. The information on the card is read when the metal contacts on the smart card are placed directly on the contacts of the smart card reader, also known as a smart card controller.

Smart cards can be used alone or combined with other authentication methods for Windows or TPM authentication. If the smart card is configured for authentication, enroll the smart card prior to enabling smart card authentication.



NOTE: Only a user with administrator rights can configure the smart card.

To enroll a smart card:

- 1 Click **Settings** next to **Smart Card Controller**.
- 2 Use the **Smart Card Enrollment Wizard** to enroll a smart card. Follow the onscreen prompts.

Contactless Smart Card

Contactless smart cards are pocket-sized cards that have an embedded silicon chip containing user information. Unlike contacted smart cards, the information on contactless smart cards is read by the smart card controller with the use of radio frequency when the smart card is in close proximity to the controller.

Contactless smart cards can be used alone or combined with other authentication methods for Windows or TPM authentication. If the smart card is configured for authentication, enroll the smart card prior to enabling smart card authentication.



NOTE: Only a user with administrator rights can configure the smart card.

To enroll a contactless smart card:

- 1 Click **Settings** next to **Contactless Smart Card Controller**.
- 2 Use the **Smart Card Enrollment Wizard** to enroll a smart card. Follow the onscreen prompts.

Full Disk Encryption

The Microsoft Encrypting File System (EFS) is used to encrypt and decrypt files and folder on your system. Use the Secure EFS wizard to configure EFS to use a digital certificate that has its private key protected by the TPM device.

To configure EFS for creating or using a TPM-secured digital certificate:

- 1 Click **Settings** next to **Full Disk Encryption**.
- 2 Use the **Secure EFS Wizard** to create or use a digital certificate for encrypting files and folders on your system. Follow the onscreen prompts.

Configuring Logins and Passwords

Configuring login and password tasks are only enabled for users with administrator rights. Logins and Passwords allow administrators to perform the following tasks:

- Select Windows Login Authentication Type
- Configure Pre-boot Password
- Manage Password Settings

Selecting a Windows Login Authentication Type

The selected Windows login authentication type will apply to all users of the system. To select the Windows login authentication:

- 1 Click **Settings** next to **Require a fingerprint or password for Windows login**.
- 2 Use **Embassy Security Center** to enable Windows login, select the authentication type for Windows login, and enroll users for fingerprints for Windows login. Follow the onscreen prompts.

Configuring a Pre-boot Password

A pre-boot password is used to authenticate the user before the system boots up. This prevents unauthorized users from accessing data on the hard drive in the event the system is lost or stolen. Options for pre-boot login include:

- **None**—No option is chosen for pre-boot login.
- **System password**—The pre-boot login uses the system password for authorization.
- **Hard drive password**—The pre-boot login uses the hard drive password for authorization.
- **Fingerprint**—The pre-boot login uses a fingerprint for authorization.
- **Smart card**—The pre-boot login uses a smart card for authorization.

To configure the pre-boot password:

- 1 Click **Settings** next to **Set a pre-boot system password**.
- 2 Use the Enrollment Wizard to register your fingerprints or smart card for pre-boot authentication.

Managing Password Settings

Windows is set up to manage accounts for all users of a system. Some Microsoft User Accounts tasks available for configuration require that you log on as an administrator or a member of the Administrators group. See the Microsoft documentation for more information.

To manage password settings:

- 1 Click **Settings** next to **Manage your Windows Password Settings**.
- 2 Use **Microsoft User Accounts** to add and remove users, reset passwords, and manage passwords.

Modifying Data Protection Settings

Modifying data protection tasks are only enabled for users with administrator rights. Data Protection is used to perform the following tasks:

- Configure the Hard Drive Password
- Configure Document Vault
- Modify File and Folder Encryption

Figure 1-2. Modify Data Protection Settings Screen



Configuring the Hard Drive Password

The internal hard drive password is separate from the system password and is used by the system's internal hard drive.

To configure the hard drive password:

- 1 Click **Settings** next to **Select or manage your Hard Drive password**.
- 2 Use the wizard to configure the hard drive password. Follow the onscreen prompts.

Configuring the Document Vault

To configure the document vault:

- 1 Click **Settings** next to **Access your Document Vault and adjust settings**.
- 2 Use the wizard to configure document vault. Follow the onscreen prompts.

Modifying File and Folder Encryption

The Microsoft Encrypting File System (EFS) is used to encrypt and decrypt files and folder on your system. Use the Secure EFS wizard to configure EFS to use a digital certificate that has its private key protected by the TPM device.

To modify the settings for file and folder encryption:

- 1 Click **Settings** next to **Modify File and Folder encryption**.
- 2 Use the **Secure EFS Wizard** to create or use a digital certificate for encrypting files and folders on your system. Follow the onscreen prompts.

Embassy Security Center

Wave Systems Embassy® Security Center (ESC) provides the tools for managing the Trusted Platform Module (TPM), which conforms to the standard by the Trusted Computing Group (TCG). ESC also contains advanced password management and authentication functions.

For more information on Embassy Security Center, visit www.wave.com/support.

