## Preface

- Introduction ........................................................................................................ 1
- About this Guide .................................................................................................. 2
- Who should read this guide? ............................................................................... 3
- Conventions ......................................................................................................... 3
- Related Documentation ....................................................................................... 3
- Contact Information ........................................................................................... 4
- Documentation Feedback ..................................................................................... 5

## Chapter 1

**Introduction to Full Disk Encryption**

- Overview of PC Security .................................................................................. 7
- Data Security Types .......................................................................................... 8
- Full Disk Encryption Features and Benefits .................................................... 9
- Benefits for Administrators ............................................................................. 10
- Deploying Full Disk Encryption to One or Many PCs ..................................... 11
- Deployment Overview ..................................................................................... 11
- An Administration Overview .......................................................................... 12
- Overview of the Full Disk Encryption Management Console ..................... 12
- Types of User Accounts ................................................................................... 16

## Chapter 2

**Getting Started**

- Full Disk Encryption Terminology .................................................................. 19
- Recommended Roadmap for Implementation .................................................. 20
  - Prepare the Master Installation .................................................................. 20
  - Prepare Your Groups and Users .................................................................. 21
  - Prepare Your Remote Administration Points (Sets) ...................................... 21
  - Prepare to Install FDE on Client Machines ................................................ 21
  - Install Full Disk Encryption on Client Machines ....................................... 22
  - Perform Administration Tasks ..................................................................... 22

## Chapter 3

**System Settings**

- Status Information ........................................................................................... 24
- Encryption Information ..................................................................................... 25
- System Settings ................................................................................................ 25
  - OneCheck Logon .......................................................................................... 26
  - Hardware Device Settings ............................................................................. 28
  - Install Settings ............................................................................................. 35
  - License Settings ........................................................................................... 49
  - Logon Settings .............................................................................................. 51
  - Remote Help Settings .................................................................................... 53
  - System Passwords Policy Settings ................................................................. 54
  - User Account Acquisition Settings ............................................................... 56
## Chapter 4

**Group Settings**

Settings for the “System” or Any Other Group ........................................... 68
- Group Settings ................................................................. 68
- Authentication Settings ......................................................... 70
- Logon Settings ...................................................................... 76
- Password Synchronization Settings ........................................... 77
- Permissions Settings .............................................................. 80
- Privileged Permissions Settings ............................................... 84
- Single Sign-On (SSO) Settings .................................................. 87
- Sanity Checks ...................................................................... 93
- Specified Values, Default Values, and How the Effective Values of Settings are Determined.................................................. 94

## Chapter 5

**Accessing and Configuring Settings for Groups and User Accounts**

Accessing FDE Settings in Full Disk Encryption Management Console ............. 98
- Accessing the Full Disk Encryption Management Console ............................. 98
- Accessing Local Settings for Groups and User Accounts .................................. 99
- Printing Settings .................................................................. 100
- Exporting Settings to a CSV File .................................................................. 100
- Exporting Logs ........................................................................ 101

## Chapter 6

**Protecting Workstations Using Full Disk Encryption**

Introduction .................................................................................. 103
- Full Disk Encryption Deployment Overview ................................................ 104
- Before Deploying ......................................................................... 104
  - About Authentication Methods .............................................................. 105
  - Do Not Modify the Pointsec for PC.msi Package ....................................... 105
  - Read the Release Notes ........................................................................ 105
  - Considerations for Other Programs ......................................................... 106
  - Review precheck.txt ............................................................................ 106
- Managing Groups and User Accounts ......................................................... 107
  - Creating Groups ................................................................................ 107
  - Adding a User Account to a Group ........................................................ 108
- Working with Configuration Sets ............................................................... 113
  - Root Directory Path ........................................................................ 113
  - Directory Paths ............................................................................. 114
  - Creating a New Set .......................................................................... 115
  - Exporting/Importing Set Configurations ............................................... 118
- Working with Installation and Update Profiles .............................................. 119
  - Introduction .................................................................................. 120
  - About Full Disk Encryption Profiles .................................................... 120
  - Before Creating Profiles ................................................................. 123
<table>
<thead>
<tr>
<th>Chapter 7</th>
<th>Upgrading Full Disk Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to Upgrading Full Disk Encryption Software</td>
<td>141</td>
</tr>
<tr>
<td>Upgrading Pointsec for PC 4.x and 5.x Installations to Full Disk Encryption 7.x</td>
<td>142</td>
</tr>
<tr>
<td>Overview</td>
<td>142</td>
</tr>
<tr>
<td>From Which Legacy Versions Can You Upgrade?</td>
<td>144</td>
</tr>
<tr>
<td>Requirements for Upgrading a 4.x/5.x Client</td>
<td>144</td>
</tr>
<tr>
<td>The Process of Upgrading</td>
<td>145</td>
</tr>
<tr>
<td>The Characteristics of an Upgrade Profile</td>
<td>146</td>
</tr>
<tr>
<td>Configuring an Upgrade Profile</td>
<td>149</td>
</tr>
<tr>
<td>Legacy Account Handling</td>
<td>150</td>
</tr>
<tr>
<td>Upgrade Operations</td>
<td>151</td>
</tr>
<tr>
<td>Upgrading from Pointsec for PC 6.x.x to Full Disk Encryption 7.x</td>
<td>155</td>
</tr>
<tr>
<td>Requirements for Upgrading from 6.x.x to FDE 7.x</td>
<td>155</td>
</tr>
<tr>
<td>Upgrading 6.x.x Installations That Have No Encrypted Volumes to FDE 7.x</td>
<td>156</td>
</tr>
<tr>
<td>Before Upgrading</td>
<td>156</td>
</tr>
<tr>
<td>Performing the Upgrade by Running the Msiexec.exe</td>
<td>158</td>
</tr>
<tr>
<td>Performing the Upgrade Using Upgrade Path(s)</td>
<td>159</td>
</tr>
<tr>
<td>Automatic Reboot After Upgrade?</td>
<td>159</td>
</tr>
<tr>
<td>Manual Reboot After Upgrade</td>
<td>159</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 8</th>
<th>Full Disk Encryption Logging Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Local Event Database</td>
<td>162</td>
</tr>
<tr>
<td>The Local Log File</td>
<td>162</td>
</tr>
<tr>
<td>The Central Log Files</td>
<td>163</td>
</tr>
<tr>
<td>Manually Transferring the Local Log File to the Central Log File</td>
<td>164</td>
</tr>
<tr>
<td>Timestamps and the Windows Event Log</td>
<td>165</td>
</tr>
<tr>
<td>Exporting Logs</td>
<td>165</td>
</tr>
<tr>
<td>Viewing a Local Log File</td>
<td>165</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 9</th>
<th>Remote Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementing a Remote Help Procedure</td>
<td>167</td>
</tr>
</tbody>
</table>
Chapter 10  
**Removing Full Disk Encryption**
- Uninstalling FDE Using FDE Management Console ........................................... 174
- Uninstall Profiles ...................................................................................... 174
- Uninstalling FDE Using Windows Add/Remove Programs ............................ 175
- Uninstalling FDE Using Recovery Media...................................................... 176

Chapter 11  
**Backing Up Critical Data**
- Profiles .................................................................................................... 177
- Log Files .................................................................................................. 178
- Recovery Files .......................................................................................... 178

Chapter 12  
**Recovering Information**
- Introduction .............................................................................................. 179
- Permissions ............................................................................................... 180
- The Full Disk Encryption Recovery File ..................................................... 181
- Storage ..................................................................................................... 181
- When the Recovery File is Updated and Written to the Share ...................... 181
- If the Recovery File Path Is Not Found ...................................................... 182
- Recovery and the Full Disk Encryption Version on the Client ................. 183
- Creating a Recovery Disk from the FDE Management Console ........... 183
- Creating a Recovery CD-ROM ................................................................. 187
- Recovering Information ............................................................................ 188
- Recovering from Alternative Media ......................................................... 188
- Using Slave Drive Functionality to Recover Information ....................... 189

Appendix A  
**HTTPS and HTTP Support and Requirements**
- HTTP Servers That FDE Supports .......................................................... 193
- FDE Requirements on the Supported Servers .......................................... 193
- FDE MIME Types ..................................................................................... 194
- Authorization and Permissions ................................................................. 194
- Security .................................................................................................... 194

Appendix B  
**Status Information When Exported to File**
- Installation Status Information ................................................................. 197
- Sample Export Status File ........................................................................ 199

Appendix C  
**Full Disk Encryption Permissions**
- Permissions: With Full Disk Encryption Service Start .............................. 204
- Recommended Users ................................................................................ 204
- Required Permissions .............................................................................. 205
Permissions: Without Full Disk Encryption Service Start .................................... 205
Permissions: Remote Desktop ......................................................................... 206
Windows User Account Registry Permissions .................................................... 206

Appendix D Language Support
Specifying the Language Used in the FDEMCC .............................................. 207
Configuring the Languages Available on the Client(s)................................. 208
Configuring the Language Used on the Clients ............................................. 208
Changing the Language in the Tray ................................................................. 209
Languages Supported .................................................................................. 209
Fallback Languages .................................................................................... 210

Appendix E Keyboard Layouts
The Default Keyboard Layout ........................................................................ 213
Changing the Keyboard Layout ..................................................................... 213
Supported Keyboard Layouts ....................................................................... 214

Appendix F PS Control Command Line Utility
Introduction .................................................................................................. 215
Using the PS Control Utility ........................................................................ 216
Options ...................................................................................................... 216
Commands ................................................................................................. 217
Error Codes ................................................................................................. 218
Examples of Using the PS Control Utility ..................................................... 218
Smart Cards, Smart Card Readers and their Drivers ..................................... 219
Managing Smart Cards, Smart Card Readers and Drivers ............................ 220
Exporting a Machine’s Status Information ..................................................... 221
Export Status File ...................................................................................... 221
Running the PS Control Utility When FDE Is Not Installed ............................ 225

Appendix G The pslogexp.exe Log Export Utility
Introduction .................................................................................................. 227
pslogexp.exe Utility Syntax and Commands .................................................. 228
Syntax ........................................................................................................ 228
Commands ................................................................................................. 228
Examples of Using the pslogexp.exe Utility ................................................... 230
Correct Display of National Characters in Exported Files .............................. 230

Appendix H Using IBM RRU or the Windows Recovery Console
Installing the InstallRRU.msi Package .......................................................... 231
RRU Functionality on a Full Disk Encryption Machine ................................... 232
Accessing ..................................................................................................... 232
Accessing the Windows Recovery Console on a Full Disk Encryption Machine .. 232

Appendix I Dual Boot Support for Windows XP and Red Hat Linux
Operating Systems and Linux Distributions Supported................................. 235
Setting Up a Dual Boot Environment That Runs Both Windows XP and Linux Red Hat with FDE

Appendix J

The Precheck.txt File
Introduction .................................................................................................. 237
Accessing precheck.txt ........................................................................... 238
Precheck Settings ................................................................................... 238
General Settings ................................................................................... 238
GINA Settings ..................................................................................... 244
Central Log Transfer Settings ............................................................... 244
License Server Settings ........................................................................ 245
Single Sign-On Settings ........................................................................ 246

Appendix K

Msiexec.exe Commands
Remove the Start Menu ........................................................................... 249
Disable the FDE Preboot Environment ................................................... 249

Appendix L

Using a Service Start Account
Full Disk Encryption Service Start Service Program - pstartsr.exe ............. 252
Setting up the Full Disk Encryption Service Start Account .......................... 252
General Requirements ........................................................................ 256
What does the Full Disk Encryption Service Start Service Do? ....................... 256
Example of Setup .................................................................................. 257
Upgrade from Pointsec for PC 4.x/5.x Installations ................................... 258

Appendix M

Full Disk Encryption Common Criteria Configuration
Introduction .......................................................................................... 259
Common Criteria EAL4 Configuration Requirements ............................... 260
Cryptographic Algorithms and Key Sizes ............................................... 261
Cryptographic Key Destruction .............................................................. 261
All Partitions Encrypted, Boot Protection Enabled ..................................... 261
No Delete Access to the Full Disk Encryption File Share ............................ 262
Wake on LAN ....................................................................................... 262
Windows Integrated Logon ..................................................................... 262
User Level Permissions ......................................................................... 262
Local Administration Disabled ............................................................... 263
Administration and Configuration via Profiles ......................................... 263
Software Upgrade between Common Criteria Versions Only ...................... 263
Password Requirements ........................................................................ 263
Password Synchronization Requirements ............................................... 264
Maximum Failed Logons before Reboot .................................................. 264

Index ..................................................................................................... 265
Preface

This preface contains background information on PC security and Endpoint Security Full Disk Encryption (FDE) benefits and features, as well as a general discussion of how FDE is structured and how it should be deployed.

In This Section

Introduction
About this Guide
Who should read this guide?
Conventions
Related Documentation
Contact Information
Documentation Feedback

Introduction

Full Disk Encryption combines enforceable, mandatory access control with strong encryption to create an advanced enterprise security solution. Full Disk Encryption ensures that user credentials and confidential information remain private, enabling organizations and agencies to take advantage of today’s mobile technology without compromising security.
About this Guide

This guide explains how to:

- Deploy and manage Full Disk Encryption on computing devices in your organization
- Provide Remote Help for users whose devices have become locked.

This guide contains:

- This preface which introduces the Administrator's Guide, and tells you where to find more information
- An introduction which provides background information on PC security and Endpoint Security Full Disk Encryption benefits and features, as well as a general discussion on how FDE is structured and how it should be deployed. It also contains an overview of the management console.
- Descriptions of the settings available for Full Disk Encryption
- Explanations on how to deploy Full Disk Encryption on workstations in your organization
- Explanations on how to help users re-gain access to locked devices
- Explanations on how to review, repair and recover information protected by Full Disk Encryption
- Discussion on password synchronization and settings which can be configured before installing Full Disk Encryption
- Explanation on how end users use fixed passwords, dynamic tokens and smart cards/USB tokens to authenticate themselves in order to access their Full Disk Encryption-protected computer.

Note - Currently, in this guide:

- While some screen shots may not exactly match the relevant product version, the information in the text is correct.
- If a setting on a property sheet or dialog box is not documented, then you do not need to change the setting
- We use the Check Point X9.9-token in examples where dynamic tokens are required.
Who should read this guide?

Administrators who will be deploying and administrating Full Disk Encryption, and providing Remote Help within their organization should read this guide.

Note - We strongly recommend that anyone planning to install, deploy and/or administer Check Point products attend certification training first. Contact your sales representative or visit: www.checkpoint.com for more information.

Conventions

This guide uses the following formatting and graphics conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>Used for user interface elements, such as panels, tabs, files, buttons, and menu options.</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>Used for emphasis.</td>
</tr>
<tr>
<td><strong>Monospace</strong></td>
<td>Used for file names and paths.</td>
</tr>
<tr>
<td>➔</td>
<td>The ➔ is used to illustrate menu choices. For example, File ➔ Open means that you should choose Open from the File menu.</td>
</tr>
<tr>
<td>🧠</td>
<td>Tip icon. Suggests for example an alternative method for accomplishing tasks or procedures.</td>
</tr>
<tr>
<td>✔</td>
<td>Note icon. Emphasizes related, reinforcing, or important information.</td>
</tr>
<tr>
<td>🚨</td>
<td>Caution icon. Indicates actions or processes that can potentially damage data or programs.</td>
</tr>
</tbody>
</table>

Related Documentation

For the very latest information on Full Disk Encryption, and for system and hardware requirements, please see the Release Notes.
The following Full Disk Encryption documentation is available from the Support Center (https://supportcenter.checkpoint.com):

**TABLE P-2 Full Disk Encryption documentation**

<table>
<thead>
<tr>
<th>Title</th>
<th>This document contains...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Disk Encryption Installation Guide</td>
<td>instructions and information on how to install Full Disk Encryption the first time, the so-called master installation.</td>
</tr>
</tbody>
</table>
| Full Disk Encryption Release Notes         | • system requirements  
• current information about the product, such as:  
  – new features and functions in the current release,  
  – problems that have been fixed since the previous release, and  
  – any known issues in the current release.                                                                                                                                 |
| Full Disk Encryption End-user Guide        | instructions for end users on how to use fixed passwords, dynamic tokens and smart cards/USB tokens to authenticate themselves in order to access their Full Disk Encryption-protected computer.                                           |

**Contact Information**

If you require information on Check Point's other security products or services, or if you should encounter any problems with Full Disk Encryption, visit our web site or call us.

**TABLE P-3 Contact information**

<table>
<thead>
<tr>
<th>Area</th>
<th>Technical Support</th>
<th>Sales</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Americas</td>
<td>972-444-6600</td>
<td>1-800-429-4391</td>
</tr>
<tr>
<td>International</td>
<td>+972-3-6115100</td>
<td></td>
</tr>
<tr>
<td>Web site</td>
<td><a href="http://www.checkpoint.com">www.checkpoint.com</a></td>
<td></td>
</tr>
</tbody>
</table>
Documentation Feedback

Check Point is engaged in a continuous effort to improve its documentation. Please help us by sending your comments to:

techpub_swe@checkpoint.com
Chapter 1

Introduction to Full Disk Encryption

In This Chapter

Overview of PC Security........................................... page 7
Data Security Types....................................................... page 8
Full Disk Encryption Features and Benefits....................... page 9
  Benefits for Administrators.......................................... page 10
Deploying Full Disk Encryption to One or Many PCs................. page 11
  Deployment Overview................................................ page 11
An Administration Overview........................................... page 12
  Overview of the Full Disk Encryption Management Console........ page 12
  Types of User Accounts............................................. page 16

Overview of PC Security

With computer security becoming increasingly important, almost all focus has been on securing large, multi-user machines. This makes sense because mainframes and large servers are not only major repositories of data, they are also crucial to daily operations. However, there is an equally serious and growing risk of compromise to the many smaller, mostly single-user, machines such as desktop and laptop PCs, as well as even Pocket PC, Palm OS and other PDAs. These computers frequently store an enterprise’s most current and valuable information. Increasingly, portable
computers also store passwords, logon scripts, and certificates used to access the enterprise network. The small size and portability of these computers mean that they are also much more vulnerable than large machines are to theft or illicit access.

An additional and often unrecognized problem is that a PC is the most available and vulnerable starting point for access to a network. Studies of computer crime reveal that insiders pose the largest threat. Clearly, providing secure PCs is an essential component of establishing network security.

**Data Security Types**

There are two general types of protection for data at rest: file encryption and full disk encryption.

The following graphic illustrates the difference between unprotected data, standard file encryption, and Full Disk Encryption protection:

**Figure 1-1**
**File Encryption**

File encryption enables users to protect vital data on a file-by-file basis, which is a good solution when, for example, transferring files between users or computers. However, organizations often find file encryption insufficient since they then have to rely on the users’ ability to secure the correct information and their willingness to consistently follow security procedures.

**Full Disk Encryption**

Unlike file encryption, which is not mandatory and therefore dependent on user discretion, Full Disk Encryption provides **boot protection** and sector-by-sector **disk encryption**.

**Boot protection** means authenticating users before a computer is booted.

Full Disk Encryption uses the user’s credentials to derive a user key, which is used to encrypt the disk volume keys. The disk volume keys encrypt the PC disk volumes.

This prevents unauthorized persons from accessing the operating system using authentication bypass tools at the operating system level or alternative boot media to bypass boot protection.

**Disk encryption** includes the system files, temp files, and even deleted files. Encryption is user-transparent and automatic, so there is no need for user intervention or user training. There is no user downtime because encryption occurs in the background without noticeable performance loss. This provides enforceable security that users cannot bypass. Because the data on the disk is encrypted, it is inaccessible to any unauthorized person.

**Full Disk Encryption Features and Benefits**

Full Disk Encryption secures desktop and laptop computers from unauthorized physical access by using both boot protection and full disk encryption.

Full Disk Encryption provides the following security functions:

- Strong user authentication
- Support for user identification using dynamic tokens
- Secure Remote Help for users who have forgotten their passwords
- Central configuration and administration
Benefits for Administrators

- Keyboard lock and screen saver
- Limited number of failed logon attempts with automatic locking
- Audit logging of events such as successful and failed logon attempts

With Full Disk Encryption, all logical partitions/volumes are boot protected and encrypted, even if the disk is removed and loaded into a controlled machine.

The integration of boot protection and automatic encryption provides a high degree of security with minimal impact on users. This allows an organization to determine the security level instead of leaving it up to the user to encrypt information.

Boot protection prevents subversion of the operating system or the introduction of rogue programs, while sector-by-sector encryption makes it impossible to copy individual files for brute force attacks.

Full Disk Encryption guarantees that unauthorized users cannot access or manipulate information on a protected computer, from either available, erased or temporary files. Full Disk Encryption safeguards the operating system and the important system files (which often contain clues to passwords), shared devices, and the network.

The Full Disk Encryption installation on the user’s PC contains all the necessary user account information, keys, and other data to protect the PC. This means there is no central user database or key repository to manage.

Benefits for Administrators

As a Full Disk Encryption administrator, you have centralized control of a decentralized system where you can perform:

- Installation, modification and removal of Full Disk Encryption on users’ PCs in the network.
- Configuration and deployment of a wide range of security and policy settings on users’ PCs.
- Modification of security policy settings to suit the needs of the entire user population, selected groups of users, or individual users.
- The daily administration of the system.
Deploying Full Disk Encryption to One or Many PCs

Using just one installation profile, you can deploy Full Disk Encryption to anywhere from one to thousands of users from a central location.

You do not need to know the details of which users are using which computers when you deploy Full Disk Encryption, that is, you do not need to create individual user accounts manually or migrate user accounts to a central database. User accounts, no matter how many, are established without your intervention on the individual PCs to which Full Disk Encryption is deployed.

This is because users receive the installation profile via a generic temporary user account, which forces the user to create a new user name and password upon logging on for the first time. This deletes the temporary account, and the user is established as a normal user in the system.

Deployment Overview

You can think of Full Disk Encryption deployment in three major steps:

1. The Full Disk Encryption program is first installed and configured on a Full Disk Encryption administrator’s workstation. This is called the master installation.

2. The administrator then configures a Full Disk Encryption installation profile containing all the information and software necessary to install and manage Full Disk Encryption on the PCs in the network.

3. The administrator uses the installation profile to deploy Full Disk Encryption to users.

The following graphic provides an overview of the deployment process via profiles:
Each of the three major steps are broken down into more detail in this guide. The following is a more detailed overview of the steps you take to deploy Full Disk Encryption.

**An Administration Overview**

**Overview of the Full Disk Encryption Management Console**

To start the FDEMC:

1. Click **Start**, navigate to the **Check Point** program group and select **Endpoint Security → Check Point Endpoint Security → Management Console**. The Full Disk Encryption Management Console (FDEMC) program starts:
Overview of the Full Disk Encryption Management Console

Chapter 1  Introduction to Full Disk Encryption 13

Figure 1-3

FDEMC Window

In the FDEMC window, you can select an option either in the folder tree to the left or by clicking the active link in the relevant window box image in the pane to the right, for example, “Go to Local”.

The FDEMC window contains the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local Installation</strong></td>
<td>Select to manage the local installation of the Full Disk Encryption.</td>
</tr>
<tr>
<td><strong>Remote Installation</strong></td>
<td>Select to manage profiles, logs, and recovery files for remote installations.</td>
</tr>
<tr>
<td><strong>Remote Help</strong></td>
<td>Select to help locked-out users change the account password or temporarily logon.</td>
</tr>
</tbody>
</table>

**FDEMC Menu Bar**

The menu bar contains the **File**, **Language** and **Help** menus. The **File** menu contains the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Extend Authority</strong></td>
<td>Enables system administrators and administrators to use FDEMC on any computer where Full Disk Encryption has been installed. See “Extending Authority” on page 15 for more information.</td>
</tr>
<tr>
<td><strong>Import Set Configurations...</strong></td>
<td>See Chapter 6, “Root Directory Path” on page 113.</td>
</tr>
<tr>
<td><strong>Export All Set Configurations...</strong></td>
<td>See Chapter 6, “Root Directory Path” on page 113.</td>
</tr>
<tr>
<td><strong>Exit</strong></td>
<td>Select to save any changes you have made and exit FDEMC.</td>
</tr>
</tbody>
</table>
The Language menu contains the following options:

Table 1-3  File Menu Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>This option sets the language used in the FDEMC to the language of the Windows operating system on the computer. If the operating system language is a nonsupported variant of one of the supported languages (listed below), for example, French (Canada) or Chinese (Singapore), the language variant used in the FDEMC is the fallback language listed under “Language Support” on page 207. If the operating system language is not supported, English is used in the FDEMC.</td>
</tr>
</tbody>
</table>
| [List of supported languages] | The list of the languages supported in the FDEMC:  
– Chinese (Simplified)  
– Chinese (Taiwan)  
– English  
– French  
– German  
– Italian  
– Japanese  
– Spanish  

In addition to the languages listed above, the language of the operating system can be selected, see the description of the Operating System option above.

Extending Authority

The Extend Authority option enables administrators to use FDEMC to access administrator functions on any computer with Full Disk Encryption installed.

To extend authority:
1. From the File menu, select Extend Authority. The Extend Authority dialog box opens.
2. Do one of the following:
– Enter the user account name and authenticate with an authorized administrator password, and, if you use a smart card for authentication, select Use inserted smart card. Click OK.

Note - Throughout the FDEMC the password is obscured with asterisks (*) when entered.

– If you are locked out, click Remote Help to receive assistance logging on.

After authentication, you can manage Full Disk Encryption from this computer.

Types of User Accounts

There are three different types of accounts when adding user accounts to a user group; normal, service user and temporary.

• Normal
  A regular user account is usually created for users of the computer on which you are working. This account can also be used as an administrator account and be included in a profile when you deploy Full Disk Encryption.

• Service User
  A service user account can be used to give a consultant temporary access to a machine, for example, so the consultant can perform maintenance. What distinguishes a service user from other users is that a service user must use Remote Help's Remote Password Change to gain access to the system the first time. After access is granted via Remote Password Change, the service user can reboot the system and log on without requiring this type of Remote Help. But when another user logs on, the service user account is locked, and the service user will need Remote Help's Remote Password Change to log on again.

  Further control can be asserted over service user accounts by limiting the maximum number of logins authorized, so that when this limit is reached, the account is forced to execute another Remote Help operation, thus generating audit information about the use of this account.

  The service user type can also be used to control and limit how local IT operates in larger organizations, without the need for dedicated accounts. This means that the number of management and administration accounts in Full Disk Encryption for pre-boot authentication can be much smaller, which, in turn, means that a smaller amount of data is affected by personnel changes.

• Temporary
A temporary user account is most commonly used when deploying Full Disk Encryption to client computers. The administrator defines one temporary user account and password, and then deploys it to clients. When a user logs on using the temporary user account and password, he/she is immediately prompted for a new user account name and password, which Full Disk Encryption uses to create a new user account that replaces the temporary user account on that computer.

To create a temporary smart card user, the user account must have the user account setting Change Credentials set to Yes. This setting is located under Group/User Account → Permissions → Change Credentials.

If more than one temporary user account is deployed to a machine, when the first temporary user logs on, Full Disk Encryption will display the name of the last user who was logged onto Windows as a suggested user account name for the new user account. But when the second (and third, etc.) temporary user logs on, Full Disk Encryption displays the temporary user account name as the suggested new user account name. The user must then enter another user account name to be able to continue - the temporary user account name cannot be used.

A temporary account can also be created for users on a computer on which you want to limit the time the user can access the computer.

For more information on profiles, see Chapter 6, “Protecting Workstations Using Full Disk Encryption” on page 103.
Types of User Accounts
Getting Started

In This Chapter

Full Disk Encryption Terminology  page 19
Recommended Roadmap for Implementation  page 20

The following information is intended to prepare you to begin working with Full Disk Encryption.

Full Disk Encryption Terminology

You may find it helpful to familiarize yourself with the following Full Disk Encryption terms.

Group

A group is a collection of user accounts. Each user account must belong to a group.

Fact: The System group is created automatically when you install Full Disk Encryption. You must create at least one other group to store other user accounts that will not belong to the System group.

Set

A set is a share point from which you carry out your remote management tasks for groups and users. Such tasks are carried out via profiles, which are collected in the set. Sets help to keep you organized by allowing you to create separate sets for
Recommended Roadmap for Implementation

In This Section

- Prepare the Master Installation
- Prepare Your Groups and Users
- Prepare Your Remote Administration Points (Sets)
- Prepare to Install FDE on Client Machines
- Install Full Disk Encryption on Client Machines
- Perform Administration Tasks

This summary will help you get a bird’s eye view of installing, configuring, deploying, and managing Full Disk Encryption.

Prepare the Master Installation

Install Full Disk Encryption on your workstation

See the *Endpoint Security Full Disk Encryption Installation Guide*, which describes how to do a first-time so-called master installation FDE installation on your PC.

Configure Full Disk Encryption system settings on your workstation

Configure the settings for your FDE installation. See Chapter 1, “Introduction to Full Disk Encryption” on page 7 and Chapter 5, “Accessing and Configuring Settings for Groups and User Accounts” on page 97.
Prepare Your Groups and Users

Configure settings
Configure the settings that control authentication and permission rights for the group and user accounts you will create. See Chapter 5, “Accessing FDE Settings in Full Disk Encryption Management Console” on page 98.

Create group and user accounts
A group is a collection of users. Every user must belong to a group. Therefore, you must create a group or groups before you create users.

Best practice is to create a temporary user account for every group you create. This generic account facilitates large-scale deployment by allowing Full Disk Encryption to deployed to many users without the need to create user accounts for each user prior to deployment. Once Full Disk Encryption is installed on the user’s machine, the user simply logs on to the temporary account, at which time he or she is forced to change the user name and password, thus creating his or her own user account.


Prepare Your Remote Administration Points (Sets)

Create Configuration Sets
A configuration set is a distribution point and storage place from which you carry out your remote management tasks for groups and users in the Full Disk Encryption system. Remote management tasks include installing/uninstalling Full Disk Encryption on remote clients and updating configuration on remote clients. See Chapter 6, “Protecting Workstations Using Full Disk Encryption” on page 103.

Prepare to Install FDE on Client Machines

Create installation profiles
A profile contains all the settings and account information that you configured for groups and users, as well as the software to install Full Disk Encryption on a client machine. You also use profiles to update settings or remove Full Disk Encryption on machines where Full Disk Encryption is already installed. Profiles can exist only in a set. See Chapter 6, “Creating Installation Profiles” on page 124.
Install Full Disk Encryption on Client Machines

Deploy the installation profile to install Full Disk Encryption on client PCs and create user accounts. See Chapter 6, “Creating Installation Profiles” on page 124 and “Installing Full Disk Encryption” on page 105.

Perform Administration Tasks

Once you have installed Full Disk Encryption on client PCs, you can perform administration tasks, such as:

- **Configuring and deploying update profiles.** See Chapter 6, “Creating an Update Profile” on page 134 and “Deploying an Update Profile” on page 138.

- **Providing Remote Help to locked out users.** See Chapter 9, “Remote Help” on page 167.

- **Uninstalling Full Disk Encryption.** See Chapter 10, “Removing Full Disk Encryption” on page 173.

- **Recovering a Full Disk Encryption PC.** See Chapter 12, “Recovering Information” on page 179.
This chapter provides a general description of the system settings with which you configure and manage Full Disk Encryption (FDE). How to configure the settings is described below.

System settings are related to installation, the hardware devices used for authentication, logon, Wake-on-LAN, required path specifications, and a number of other aspects of the product such as OneCheck Logon, screen savers, Remote Help, and hibernation.

Other settings - those for Groups and User Accounts - are relevant for volume access, logging on, authentication, permissions, Remote Help, single sign-on, and password synchronization. These settings are described in Chapter 4, “Group Settings”.

In This Chapter

- Status Information page 24
- Encryption Information page 25
- System Settings page 25
- Export to CSV File Button page 66
- Print Settings Button page 66
## Status Information

The following **Status** information is displayed in the main panel:

<table>
<thead>
<tr>
<th>Status field</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locally installed version</td>
<td>The version of Full Disk Encryption currently installed on this machine.</td>
</tr>
<tr>
<td>Preboot user account</td>
<td>The name of the user account that authenticated at preboot.</td>
</tr>
<tr>
<td>FDEMC user account</td>
<td>The name of the user account currently logged on to FDEMC.</td>
</tr>
<tr>
<td>MI mode</td>
<td>Indicates whether this Full Disk Encryption is running in MI mode or not. The values are: <strong>Yes</strong> or <strong>No</strong>.</td>
</tr>
<tr>
<td>Windows Integrated Logon</td>
<td>The current value specified for the Windows Integrated Logon setting: <strong>Enabled</strong> or <strong>Disabled</strong>.</td>
</tr>
<tr>
<td>Last recovery update</td>
<td>Date and time the most recent recovery file was created.</td>
</tr>
<tr>
<td>Last recovery file delivery</td>
<td>Date and time a recovery file was last copied to its target directory. The target directory is the directory specified under <strong>Recovery Path</strong> in the <strong>Install</strong> settings under <strong>System Settings</strong>.</td>
</tr>
<tr>
<td>Last log file update</td>
<td>Date and time the log file was last updated by Full Disk Encryption.</td>
</tr>
<tr>
<td>Last log file delivery</td>
<td>Date and time the log file was last written by Full Disk Encryption. The file name of the log file is the same as the name of the machine. The log file is written to the same directory or directories as specified in <strong>Set Central Log Path</strong> (<strong>Install</strong> settings under <strong>System Settings</strong>).</td>
</tr>
<tr>
<td>Last local update</td>
<td>Date and time of the most recent change to a Local setting; also contains the user account name that made the change.</td>
</tr>
<tr>
<td>Last update profile</td>
<td>Date and time the most recent update profile was downloaded and the path, including the profile name, from which is was downloaded.</td>
</tr>
</tbody>
</table>
Encryption Information

Besides the volume number, the following Encryption information relevant to each volume is displayed:

Table 3-2 Encryption Information

<table>
<thead>
<tr>
<th>Text</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypting nn%</td>
<td>Displays the progress of encryption and the percentage of encryption completed.</td>
</tr>
<tr>
<td>Fully encrypted</td>
<td>States that the volume is fully encrypted.</td>
</tr>
<tr>
<td>Decrypting nn%</td>
<td>Displays the progress of decryption as the percentage of decryption completed.</td>
</tr>
<tr>
<td>Unencrypted</td>
<td>States that the volume is unencrypted.</td>
</tr>
<tr>
<td>Error</td>
<td>An error has occurred during encryption or decryption.</td>
</tr>
</tbody>
</table>

Note - If a disk is neither encrypted nor boot protected, it is not listed/displayed in the encryption information in the FDEMC.

System Settings

In This Section

- OneCheck Logon page 26
- Hardware Device Settings page 28
- Install Settings page 35
- License Settings page 49
- Logon Settings page 51
- Remote Help Settings page 53
- System Passwords Policy Settings page 54
- User Account Acquisition Settings page 56
- Wake-on-LAN (WOL) Settings page 59
- Windows Integrated Logon (WIL) Settings page 61
OneCheck Logon

OneCheck Logon contains the following settings:

**Figure 3-1**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Minimum Group Authority Level Required</strong></td>
<td>The minimum group authority level required to edit the OneCheck Logon settings. For more information on group authority levels, see Chapter 4, “Group Settings” on page 68.</td>
</tr>
<tr>
<td><strong>Allow Windows Screen Saver</strong></td>
<td>Select Yes to allow the screen saver specified in Windows to be used or No if you want the FDE screen saver to be used.</td>
</tr>
<tr>
<td></td>
<td>If you allow the Windows Screen Saver, the screen saver configured in the user’s Windows profile will take effect only if the following settings are disabled:</td>
</tr>
<tr>
<td></td>
<td>• The group or user setting “Set Screen Saver Timeout” (see page 68)</td>
</tr>
<tr>
<td></td>
<td>• The WIL setting “Set WIL User Screen Saver Timeout” (see page 66)</td>
</tr>
<tr>
<td></td>
<td>If these settings are not disabled, the FDE screen saver will override the Windows user profile screen saver even if enabled here.</td>
</tr>
</tbody>
</table>
### Table 3-3  OneCheck Logon settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable OneCheck Logon</strong></td>
<td>Enable the Check Point OneCheck Logon functionality, which provides single sign-on functionality to Check Point's Endpoint Connect VPN and Media Encryption, and to Windows. Note that: (1) after enabling OneCheck Logon, the single sign-on functionality will not be active until the user account has logged off and then on to Windows, and (2) after disabling OneCheck Logon, the single sign-on functionality will still be active until the user account has logged off from Windows. For more information on how OneCheck Logon and FDE's 'Windows-only' single sign-on function, see “How Single Sign-On and OneCheck Logon Function” on page 87. &lt;br&gt; <strong>Note</strong> - Authentication with smart cards is not supported when OneCheck Logon is enabled. &lt;br&gt; <strong>Note</strong> - Switching users via the Start menu in Windows Vista is not supported when OneCheck Logon is enabled. &lt;br&gt; <strong>Note</strong> - Enabling OneCheck Logon will disable the settings Enable SSO and Enable Entrust SSO under Groups → System → Group Settings → Single Sign-On.</td>
</tr>
<tr>
<td><strong>Set Screen Saver Text</strong></td>
<td>Specifies the text that will be displayed in the Full Disk Encryption screen saver.</td>
</tr>
</tbody>
</table>
Hardware Device Settings

The Hardware Device settings contain, among other things, settings relevant to the use of smart cards in the FDE preboot environment. If you are going to use smart cards, there are a number of other settings that must be configured for smart cards to function.

**Warning** - Do not alter the default values for the following settings unless you are going to use smart cards:

- Enable PCMCIA Devices in Preboot,
- Enable USB Devices in Preboot, and
- Enable Mouse in Preboot.

The other settings are generic preboot settings and are not related to the use of smart cards. The Preboot Drivers setting is related to smart cards, but it does not have default values.

**Hardware Devices** contains the following settings:

**Figure 3-2**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Group Authority Level Required</td>
<td>The minimum group authority level required to edit the Hardware Devices settings. For more information on group authority levels, see Chapter 4, “Group Settings” on page 68.</td>
</tr>
</tbody>
</table>
### Table 3-4 Hardware Device Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable PCMCIA Devices in Preboot</td>
<td>Enables PCMCIA devices in preboot. This setting should be used for PCMCIA smart card reader support. Note that a device’s driver must be installed before the device can be used.</td>
</tr>
<tr>
<td>Enable USB Devices in Preboot</td>
<td>Enables USB devices in preboot. This setting should be used for USB smart card reader support. Note that a device’s driver must be installed before the device can be used.</td>
</tr>
<tr>
<td>Enable Mouse in Preboot</td>
<td>Enables mouse support in the Full Disk Encryption preboot environment.</td>
</tr>
<tr>
<td>Enable Low Graphics Mode</td>
<td>Enables low-graphics mode in the Full Disk Encryption preboot environment.</td>
</tr>
<tr>
<td>Allow Serial over LAN</td>
<td>Allows the use of Serial Over LAN on Intel vPro PCs. This requires an Intel vPro-enabled PC and a telnet session to the client to be reached. The Serial Over LAN functionality will enable administrators to log on to the FDE preboot environment on the remote machine. For more information on Intel vPro technology and its use, contact Intel Support.</td>
</tr>
<tr>
<td>Allow a Slave Hard Drive</td>
<td>Allows the system to use another encrypted drive as a slave drive. SATA drives used as slave drives must be connected directly to the SATA interface on the motherboard. SATA slave drives connected via USB are not supported.</td>
</tr>
<tr>
<td>Allow Hard Drive To Be Slaved</td>
<td>Allows this drive to be a slave drive in other Full Disk Encryption systems. SATA drives used as slave drives must be connected directly to the SATA interface on the motherboard. SATA slave drives connected via USB are not supported.</td>
</tr>
</tbody>
</table>
Hardware Device Settings

Table 3-4  Hardware Device Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preboot Drivers</td>
<td>This setting includes:</td>
</tr>
<tr>
<td></td>
<td>• A display of the drivers (HID, Smart Card, and Smart Card Reader) that are currently supported in the Full Disk Encryption Preboot environment on the local machine. The display includes: Device Name, File Name, Version, and Device Type.</td>
</tr>
<tr>
<td></td>
<td>• A filter for the display of drivers.</td>
</tr>
<tr>
<td></td>
<td>• A button that adds a driver.</td>
</tr>
<tr>
<td></td>
<td>• A display of the drivers (HID, Smart Card, and Smart Card Reader) that are contained in an .inf file in the Path to inf file for Full Disk Encryption drivers text box. This is displayed after clicking Add Driver.</td>
</tr>
<tr>
<td></td>
<td>• A button that enables marking a driver for removal.</td>
</tr>
<tr>
<td></td>
<td>• A checkbox that, if selected, hides device names in the display of devices.</td>
</tr>
<tr>
<td></td>
<td>For details on using these features, see “Adding and Removing Preboot Drivers with the Preboot Drivers Setting” on page 30.</td>
</tr>
</tbody>
</table>

Adding and Removing Preboot Drivers with the Preboot Drivers Setting

You can use the Preboot Drivers setting to install:

– Smart card drivers
– Smart card reader drivers
– HID drivers

on the configuration of the local machine or to push them to clients via an Update profile.

Adding Smart Card, Smart Card Reader, and HID Drivers

To add a driver to the local installation:
1. Click **Preboot Drivers** in the management console. A **Preboot Drivers** window will open.

The window will display any devices currently supported in preboot, the list is empty if none have been installed. The window contains a **Filter** text box. Text entered in this box is matched with the device name, file name, version, and device type, and the display is immediately updated to show the devices that match the filter. Select **Hide device names** to hide the device names and only display the file name, version, and device type columns.

**Figure 3-3** The Preboot Drivers window

<table>
<thead>
<tr>
<th>Device Name</th>
<th>File Name</th>
<th>Version</th>
<th>Device Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abaddon Token PRO 32K</td>
<td>ETOK_P11.BIN</td>
<td>3</td>
<td>Smart Card</td>
</tr>
<tr>
<td>Abaddon Token PRO 64K</td>
<td>ETOK_P11.BIN</td>
<td>3</td>
<td>Smart Card</td>
</tr>
<tr>
<td>Abaddon Token PRO 64K</td>
<td>ETOK_P11.BIN</td>
<td>3</td>
<td>Smart Card</td>
</tr>
<tr>
<td>Abaddon Token PRO 64K</td>
<td>ETOK_P11.BIN</td>
<td>3</td>
<td>Smart Card</td>
</tr>
<tr>
<td>Abaddon Token PRO 64K</td>
<td>ETOK_P11.BIN</td>
<td>3</td>
<td>Smart Card</td>
</tr>
<tr>
<td>Abaddon Token PRO 64K</td>
<td>ETOK_P11.BIN</td>
<td>3</td>
<td>Smart Card</td>
</tr>
<tr>
<td>Abaddon Token PRO 64K</td>
<td>ETOK_P11.BIN</td>
<td>3</td>
<td>Smart Card</td>
</tr>
<tr>
<td>Abaddon Token PRO 64K</td>
<td>ETOK_P11.BIN</td>
<td>3</td>
<td>Smart Card</td>
</tr>
<tr>
<td>Abaddon Token PRO 64K</td>
<td>ETOK_P11.BIN</td>
<td>3</td>
<td>Smart Card</td>
</tr>
<tr>
<td>Abaddon Token PRO 64K</td>
<td>ETOK_P11.BIN</td>
<td>3</td>
<td>Smart Card</td>
</tr>
<tr>
<td>Abaddon Token PRO 64K</td>
<td>ETOK_P11.BIN</td>
<td>3</td>
<td>Smart Card</td>
</tr>
<tr>
<td>Abaddon Token PRO 64K</td>
<td>ETOK_P11.BIN</td>
<td>3</td>
<td>Smart Card</td>
</tr>
<tr>
<td>Abaddon Token PRO 64K</td>
<td>ETOK_P11.BIN</td>
<td>3</td>
<td>Smart Card</td>
</tr>
</tbody>
</table>

2. Click **Add Driver** and the **Add Driver** window is displayed.

The Add Driver window displays the drivers in the .inf file displayed in the **Path to inf files for Full Disk Encryption drivers** in the **Device List**. All drivers provided by Check Point are delivered in .inf files. Adding one driver can add many devices because many drivers support multiple devices. Select **Hide device names** to hide the device names and only display the file name, version, and device type columns. Select **CAC compliant devices** to display only devices that comply with CAC.
3. To add a device, click **Add** in the **Add File** column for the device you want to include in your installation. The file that is added to support the device you have chosen is a driver that might support many devices. A list is displayed of the devices that the driver supports. Click **Yes** if you want to add the driver (and its support for the device you want). Otherwise, click **No**.
If you clicked Yes, the device(s) will now be displayed under **Supported Devices in Preboot**.

**Note** - The device or devices are not added until you save the configuration by:

1. Clicking **OK** in the **Preboot Drivers** window, and then
2. Clicking **Save** in the management console **Local** window.

### Removing Smart Card, Smart Card Reader, and HID Drivers

**To remove drivers:**

1. Navigate to the **Preboot Drivers** window in the management console.
2. Select the device you want to remove and click **Mark Driver for Removal**. A confirmation window, **Remove Driver**, is displayed.
3. Click **OK** to remove the selected driver. **Note**: Removing the selected driver removes the support for all the devices supported by the driver.

**Figure 3-6** The Remove Driver window

![Remove Driver Window](image)

The device is now marked for removal and it is displayed in red.
**Figure 3-7** Device marked for removal

**Note** - Note that the driver or drivers are not removed until you save the configuration by:

1. Clicking **OK** in the **Preboot Drivers** window, and then
2. Clicking **Save** in the management console **Local** window.
Install Settings

Install contains the following settings:

**Figure 3-8**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Group Authority Level Required</td>
<td>The minimum group authority level required to edit the <strong>Install</strong> settings. For more information on group authority levels, see Chapter 4, “Group Settings” on page 68.</td>
</tr>
<tr>
<td>Organization</td>
<td>Name of the organization. Maximum length of this value is 255 bytes. Note that all UNICODE characters are not 1 byte in length, but can be 1, 2 or 4 bytes. Thus the length of the value you input depends on the length of the characters in the character set you use.</td>
</tr>
</tbody>
</table>
Table 3-5 Install Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Owner</td>
<td>Owner of the Full Disk Encryption product. The maximum length of this value is 255 bytes. Note that all UNICODE characters are not 1 byte in length, but can be 1, 2 or 4 bytes. Thus the length of the value you input depends on the length of the characters in the character set you use.</td>
</tr>
<tr>
<td>Set Installation Message</td>
<td>Enter a message to be displayed before starting to install Full Disk Encryption on a workstation.</td>
</tr>
<tr>
<td>Set Post-Installation Message</td>
<td>Enter a message to be displayed after the installation has been completed.</td>
</tr>
<tr>
<td>Select Language</td>
<td>Sets the language that will be used in the:</td>
</tr>
<tr>
<td></td>
<td>• Client preboot interface</td>
</tr>
<tr>
<td></td>
<td>• Client system tray</td>
</tr>
<tr>
<td></td>
<td>• Client single sign-on dialog (if single sign-on is active on that client)</td>
</tr>
<tr>
<td></td>
<td>• Recovery utility.</td>
</tr>
<tr>
<td></td>
<td>If the language specified is not installed on the machine, the language will be set to US English. For more information on FDE language support, see Appendix D, “Language Support” on page 207. Note that you set the language to be used in the FDEMC under Language on the FDEMC menu bar.</td>
</tr>
<tr>
<td>Available Languages</td>
<td>Note - Used to specify the languages that can be selected in the Select Language setting (described above), and in the Check Point Endpoint Security Tray Application. At least one language must be selected here. Only the languages specified here are displayed in the tray menu under Settings... → Advanced → Language → Select Language.</td>
</tr>
</tbody>
</table>
Use to add new language files provided by Check Point after a release. The following types of language files are relevant:

**LANGUAGE.LNZ** -- contains all text used in the FDE Preboot Environment. You can specify the path to the language file in the Preboot language file text box, or you can browse to the file.

**Plang32.Lng** -- contains all text used by FDE in Windows dialogs, for example, single sign-on (SSO), authentication dialogs and message dialogs in Windows. You can specify the path to the language file in the Windows dialogs language text box, or you can browse to the file.

**ZP4PC.zip.dll** -- contains all text used for the FDE information in the Endpoint Security tray. FDE verifies that this files has been digitally signed by Check Point. You can specify the path to the language file in the Windows tray language file text box, or you can browse to the file.

**PointsecForPC.resources.dll** -- contains FDE Management Console (FDEMC) language files. The FDEMC uses one PointsecForPC.resources.dll file per language, and each language is stored in a separate subdirectory. When an FDEMC language is added, FDE detects which language it is and stores it in the proper directory, and FDE verifies that this files has been digitally signed by Check Point. You can specify the path to the language file in the Management Console language files text box, or you can browse to the file.

Note that the language files are not changed or added until you:

1. Click **OK** in the Change Language Files window, and then
2. Click **Save** in the FDEMC Local window.
The administrator uses **Set Update Validation Password** to set the password clients will use to validate update profiles they pull from a shared folder. This password is crucial to the update and the uninstall processes. The profile contains the password set here, and the user does not need to enter a password on the client.

The profile will inherit its password from the workstation on which the profile is created.

If the update validation password is changed on the workstation where profiles are created, any new profiles will contain both the old password and the new. Clients receiving these profiles will first accept the profiles, since they contain the old password, and then change their own update validation password to match the new one in the profile.

**Update Validation Password Compatibility Level**

Because of differences in the formats of the update validation password (UVP) in different versions of the product, not all combinations of UVPs from different product versions will work together. This setting enables you to choose, and thereby limit, which profile versions to import to the current product version.

It is recommended to choose the most restrictive compatibility level possible without excluding any of the profile versions that are currently or recently used at the deployment site.

The following levels are available:

- Pointsec for PC v6.0.0 and later
- Pointsec for PC v6.1.2 and later
- Pointsec PC v6.2.0 and later
- Pointsec PC v6.2.0 HFA1 and later

See also “The Update Validation Password Must Be Reentered After Upgrade” on page 160.

### Table 3-5 Install Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Set Update Validation Password | The administrator uses **Set Update Validation Password** to set the password clients will use to validate update profiles they pull from a shared folder. This password is crucial to the update and the uninstall processes. The profile contains the password set here, and the user does not need to enter a password on the client. The profile will inherit its password from the workstation on which the profile is created. If the update validation password is changed on the workstation where profiles are created, any new profiles will contain both the old password and the new. Clients receiving these profiles will first accept the profiles, since they contain the old password, and then change their own update validation password to match the new one in the profile. **Update Validation Password Compatibility Level** Because of differences in the formats of the update validation password (UVP) in different versions of the product, not all combinations of UVPs from different product versions will work together. This setting enables you to choose, and thereby limit, which profile versions to import to the current product version. It is recommended to choose the most restrictive compatibility level possible without excluding any of the profile versions that are currently or recently used at the deployment site. The following levels are available:  
  - Pointsec for PC v6.0.0 and later
  - Pointsec for PC v6.1.2 and later
  - Pointsec PC v6.2.0 and later
  - Pointsec PC v6.2.0 HFA1 and later

See also “The Update Validation Password Must Be Reentered After Upgrade” on page 160. |
The log password prevents unauthorized access to both local and non-local logs. Note that changing the log password triggers Full Disk Encryption to create a new Central Log file, which has a unique name.

**Note** - The log password cannot be imported into a profile based on local settings; therefore, the log password setting must be specified in a profile that is ‘based on local’.

If enabled, the status information is exported in a file to the directory specified in the **Set Central Log Path** setting. If no path is specified, the file is not written. For a detailed description of the status information in the file, see Appendix B, “Status Information When Exported to File” on page 197.
### Table 3-5 Install Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Upgrade Path(s)</td>
<td>Path(s) to the directory or directories from which the installation will download software upgrades. Enter the path(s) to the directory or directories where the Full Disk Encryption system administrator will place the program upgrade files. The path(s) can be paths to shared folders or to https:// or http:// shares, as illustrated below. Select Specify Authentication if you want to use the username and password authentication available on the web server on which the share resides. See Appendix A “HTTPS and HTTP Support and Requirements” on page 193 for information on configuring HTTPS and HTTP. <strong>Note</strong> - Use HTTPS! Even though it can be selected, do not use HTTP in production environments. HTTP can be subject to malicious attacks, data hijacking, etc. and therefore is not a safe file transfer option from a risk perspective. HTTP should be used only for validating functionality in pilots on a secured network or for internal performance testing etc.</td>
</tr>
</tbody>
</table>
### Table 3-5 Install Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Upgrade Path(s)</td>
<td>If you specify multiple paths, Full Disk Encryption will pull the upgrade profiles from all the paths; but it will not pull duplicates of profiles it has already pulled (profiles that have the same name and date). Full Disk Encryption downloads the software upgrades automatically in the background at predefined intervals or the next restart. See Chapter 6, section “Working with Installation and Update Profiles” on page 119 for more information. When you click Add to add a path, FDE will attempt to verify that the path exists. If the verification is successful, the path is added automatically. If the verification is not successful, you can still add the path by clicking OK in the Path Not Verified window. However, http:// and https:// paths are not verified.</td>
</tr>
</tbody>
</table>
Install Settings

Table 3-5  Install Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Update Profile</td>
<td>Path(s) to the directory or directories from which the installation will download update profiles. Enter the path(s) to the directory or directories where Full Disk Encryption is to look for update profiles to use when updating system, group, and user account information. Note that path(s) can be paths to shared folders or to https:// or http:// shares, as illustrated in Set Upgrade Profile Path(s) above. Select Specify Authentication if you want to use the username and password authentication available on the web server on which the share resides. See Appendix A “HTTPS and HTTP Support and Requirements” on page 193 for information on configuring HTTPS and HTTP. <strong>Note</strong> - Use HTTPS! Even though it can be selected, do not use HTTP in production environments. HTTP can be subject to malicious attacks, data hijacking, etc. and therefore is not a safe file transfer option. HTTP should be used only for validating functionality in pilots on a secured network or for internal performance testing etc. If you specify multiple paths, Full Disk Encryption will pull the upgrade profiles from all the paths; but it will not pull duplicates of profiles it has already pulled (profiles that have the same name and date). Full Disk Encryption downloads these profiles according to the predefined update interval. Default is every third hour or at the next restart, i.e. when the Full Disk Encryption Tray program is loaded next. See Chapter 6, section “Working with Installation and Update Profiles” on page 119 for more information. When you click Add to add a path, FDE will attempt to verify that the path exists. If the verification is successful, the path is added automatically. If the verification is not successful, you can still add the path by clicking OK in the Path Not Verified window. However, http:// and https:// paths are not verified.</td>
</tr>
</tbody>
</table>
### Table 3-5 Install Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Recovery Path(s)</td>
<td>Path(s) to the directory or directories in which the installation will store recovery data. Enter the path(s) to the directory or directories where Full Disk Encryption is to store a recovery file.</td>
</tr>
<tr>
<td></td>
<td>Note that path(s) can be paths to shared folders or to https:// or http:// shares, as illustrated in <strong>Set Upgrade Profile Path(s)</strong> above. Select <strong>Specify Authentication</strong> if you want to use the username and password authentication available on the web server on which the share resides.</td>
</tr>
<tr>
<td></td>
<td>See <strong>Appendix A “HTTPS and HTTP Support and Requirements”</strong> on page 193 for information on configuring HTTPS and HTTP.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> - Use HTTPS! Even though it can be selected, <em>do not</em> use HTTP in production environments. HTTP can be subject to malicious attacks, data hijacking, etc. and therefore is not a safe file transfer option from a risk perspective. HTTP should be used only for validating functionality in pilots on a secured network or for internal performance testing etc.</td>
</tr>
<tr>
<td></td>
<td>Full Disk Encryption writes the recovery file to all the specified paths, see <strong>Chapter 12</strong>, section <strong>“The Full Disk Encryption Recovery File”</strong> on page 181 for more information.</td>
</tr>
<tr>
<td></td>
<td>When you click <strong>Add</strong> to add a path, FDE will attempt to verify that the path exists. If the verification is successful, the path is added automatically. If the verification is not successful, you can still add the path by clicking <strong>OK</strong> in the <strong>Path Not Verified</strong> window. However, http:// and https:// paths are <em>not</em> verified.</td>
</tr>
</tbody>
</table>
### Table 3-5  Install Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Set Central Log Path(s)** | Path(s) to the directory or directories in which the installation will store a copy of the local log file.  
  Full Disk Encryption writes the log file to *all the specified paths*.  
  Note that path(s) can be paths to shared folders or to https:// or http:// shares, as illustrated in **Set Upgrade Profile Path(s)** above. Select **Specify Authentication** if you want to use the username and password authentication available on the web server on which the share resides.  
  See Appendix A “HTTPS and HTTP Support and Requirements” on page 193 for information on configuring HTTPS and HTTP.  
  **Note** - Use HTTPS! Even though it can be selected, *do not* use HTTP in production environments. HTTP can be subject to malicious attacks, data hijacking, etc. and therefore is not a safe file transfer option from a risk perspective. HTTP should be used only for validating functionality in pilots on a secured network or for internal performance testing etc.  
  When you click **Add** to add a path, FDE will attempt to verify that the path exists. If the verification is successful, the path is added automatically. If the verification is not successful, you can still add the path by clicking **OK** in the **Path Not Verified** window. However, http:// and https:// paths are *not verified.* |
Install Settings

Chapter 3  System Settings  45

File Transfer Delay
Use this setting to configure the interval between file transfers to remote computers and the delay before the first retry after a failed transfer. The following values can be specified:

- Average time between file transfers
- Time to wait before the first retry after a failed transfer
- Interval within which the specified number of retries should be performed
- Number of retry attempts within the first 60 minutes.

A graph displays, among other things, the retries against time (in minutes).

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Transfer Delay</td>
<td>Use this setting to configure the interval between file transfers to remote computers and the delay before the first retry after a failed transfer. The following values can be specified: Average time between file transfers, Time to wait before the first retry after a failed transfer, Interval within which the specified number of retries should be performed, Number of retry attempts within the first 60 minutes. A graph displays, among other things, the retries against time (in minutes).</td>
</tr>
</tbody>
</table>
The path(s) to the PKCS#11 dll file.

This setting should be used only if you are going to use the smart card differentiation feature.

If you specify multiple paths, Full Disk Encryption will check the first path to see if the dll can read from the smart card; if the dll cannot, FDE will check the next path and so on until it finds a path which contains a dll that can read from the smart card.

When you click Add to add a path, FDE will attempt to verify that the path exists. If the verification is successful, the path is added automatically. If the verification is not successful, you can still add the path by clicking OK in the Path Not Verified window.

When smart card differentiation is enabled, these serial numbers are stored together with user information in a database. When a user tries to log on with a smart card, the PKCS#11 dll collects the smart card ID and certificate and compares these to the smart card ID and certificate information already stored in the user account.

This makes it possible to have the same certificate on multiple smart cards while the system can still differentiate between different users by using the different smart card IDs.

Windows cannot register the PKCS#11 dll file(s) automatically, the path(s) to the file(s) must be set manually. The dll file is distributed with your smart card so the location depends on the smart card used, refer to your smart card manual to find out where the dll is located.

As an example, the PKCS#11 dll file distributed with Aladdin smart cards is found under: \WINDOWS\system32\eTPkcS11.dll.

### Table 3-5 Install Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set PKCS#11 dll Path(s)</td>
<td>The path(s) to the PKCS#11 dll file.</td>
</tr>
</tbody>
</table>

- This setting should be used only if you are going to use the smart card differentiation feature.
- If you specify multiple paths, Full Disk Encryption will check the first path to see if the dll can read from the smart card; if the dll cannot, FDE will check the next path and so on until it finds a path which contains a dll that can read from the smart card.
- When you click Add to add a path, FDE will attempt to verify that the path exists. If the verification is successful, the path is added automatically. If the verification is not successful, you can still add the path by clicking OK in the Path Not Verified window.
- When smart card differentiation is enabled, these serial numbers are stored together with user information in a database. When a user tries to log on with a smart card, the PKCS#11 dll collects the smart card ID and certificate and compares these to the smart card ID and certificate information already stored in the user account.
- This makes it possible to have the same certificate on multiple smart cards while the system can still differentiate between different users by using the different smart card IDs.
- Windows cannot register the PKCS#11 dll file(s) automatically, the path(s) to the file(s) must be set manually. The dll file is distributed with your smart card so the location depends on the smart card used, refer to your smart card manual to find out where the dll is located.
- As an example, the PKCS#11 dll file distributed with Aladdin smart cards is found under: \WINDOWS\system32\eTPkcS11.dll.
Select Volume Protection

You can use this setting to specify the volume protection policy you want implemented on each volume. In the Select Volume Protection window, you can select preboot authorization (Preboot Auth.) or Encryption or both. Both is recommended. Six tabs (0-5) are displayed, one for each of six possible disks, and 26 (0-25) volumes are listed for each disk. Preboot authentication is mandatory on the boot volume, and that checkbox cannot be cleared.

The algorithm to be used for encryption can be selected in the Algorithm drop-down menu. The following algorithms are supported:

- AES (key size 256 bits)
- Blowfish (key size 256 bits)
- CAST (key size 128 bits)
- 3DES (key size 168 bits)

All volumes will be encrypted and protected by preboot authentication if you select the Encrypt and enable preboot authentication for all disk volumes checkbox. For dynamic encryption of volumes that are added after installation, see the Dynamic Volume Encryption setting, below.

The specifications made for each volume are implemented at installation, and they cannot be later changed later via this setting. For example, if only preboot authentication is selected for a volume, that volume cannot be encrypted after installation by selecting Encryption for that volume in this setting.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Select Volume Protection | You can use this setting to specify the volume protection policy you want implemented on each volume. In the Select Volume Protection window, you can select preboot authorization (Preboot Auth.) or Encryption or both. Both is recommended. Six tabs (0-5) are displayed, one for each of six possible disks, and 26 (0-25) volumes are listed for each disk. Preboot authentication is mandatory on the boot volume, and that checkbox cannot be cleared. The algorithm to be used for encryption can be selected in the Algorithm drop-down menu. The following algorithms are supported:
- AES (key size 256 bits)
- Blowfish (key size 256 bits)
- CAST (key size 128 bits)
- 3DES (key size 168 bits)

All volumes will be encrypted and protected by preboot authentication if you select the Encrypt and enable preboot authentication for all disk volumes checkbox. For dynamic encryption of volumes that are added after installation, see the Dynamic Volume Encryption setting, below.

The specifications made for each volume are implemented at installation, and they cannot be later changed later via this setting. For example, if only preboot authentication is selected for a volume, that volume cannot be encrypted after installation by selecting Encryption for that volume in this setting. |
If selected, this setting enables the encryption of volumes that are added after Full Disk Encryption has been installed. When FDE starts and discovers a newly added volume, it checks the Volume Protection settings for that volume, and if encryption has been correctly specified for that volume, FDE automatically encrypts that volume. Note that initially FDE, after a boot or a manual restart of the Full Disk Encryption service, detects any new volumes and checks the Volume Protection settings to determine whether or not they should be encrypted. At this stage, volumes that are to be encrypted are listed in the tray application under Encryption status as having 0% encryption. The actual encryption starts in the background after the next reboot of the machine.

Dynamic Volume Encryption will not function on Pointsec PC 6.x.x. installations with no encrypted volumes that are upgraded to Full Disk Encryption 7.0 or later. If you attempt to enable Dynamic Volume Encryption when upgrading such installations, FDE will generate an error message (if Dynamic Volume Encryption is selected in the local settings) or an error log event (if Dynamic Volume Encryption is selected in a profile). The error log event ID is 3104; its text is: “An attempt to enable dynamic encryption was made on an unsupported system. Consult the Administrator Guide for more information. The setting was reverted.”

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Volume Encryption</td>
<td>If selected, this setting enables the encryption of volumes that are added after Full Disk Encryption has been installed. When FDE starts and discovers a newly added volume, it checks the Volume Protection settings for that volume, and if encryption has been correctly specified for that volume, FDE automatically encrypts that volume. Note that initially FDE, after a boot or a manual restart of the Full Disk Encryption service, detects any new volumes and checks the Volume Protection settings to determine whether or not they should be encrypted. At this stage, volumes that are to be encrypted are listed in the tray application under Encryption status as having 0% encryption. The actual encryption starts in the background after the next reboot of the machine. Dynamic Volume Encryption will not function on Pointsec PC 6.x.x. installations with no encrypted volumes that are upgraded to Full Disk Encryption 7.0 or later. If you attempt to enable Dynamic Volume Encryption when upgrading such installations, FDE will generate an error message (if Dynamic Volume Encryption is selected in the local settings) or an error log event (if Dynamic Volume Encryption is selected in a profile). The error log event ID is 3104; its text is: “An attempt to enable dynamic encryption was made on an unsupported system. Consult the Administrator Guide for more information. The setting was reverted.”</td>
</tr>
<tr>
<td>Full Disk Encryption Service Start Account</td>
<td>The Windows account to use when starting the Full Disk Encryption service. Specify the account in the form: [Domain][Username]. You will also specify the account password here. See Appendix L, “Using a Service Start Account” on page 251 for more information.</td>
</tr>
</tbody>
</table>
License Settings

License contains the following settings:

Table 3-5  Install Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhance Key Protection in RAM</td>
<td>Activating this setting increases security against so-called Cold Boot attacks by adding an additional layer of protection for keys residing within the computer's RAM.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> - While impractical, in theory, a Cold Boot attack could gain access to, for example, encryption keys on the computer's memory within minutes of its being shutdown even with the setting enabled. However, this setting makes Cold Boot attacks more difficult.</td>
</tr>
</tbody>
</table>

Table 3-6  License settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Group Authority Level Required</td>
<td>The minimum group authority level required to edit the License settings. For more information on group authority levels, see Chapter 4, “Group Settings” on page 68.</td>
</tr>
<tr>
<td>Product Serial Number</td>
<td>The Full Disk Encryption Legacy serial number.</td>
</tr>
<tr>
<td>Set License Server Password</td>
<td>The password utilized to secure the communication with the license server. This password must be identical to the password that is utilized in the license server.</td>
</tr>
<tr>
<td>Set License Server Shared Folder Path(s)</td>
<td>The path(s) to the folder(s) which is utilized for communication with the license server.</td>
</tr>
</tbody>
</table>
Table 3-6  **License settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Offline License Activation Message</td>
<td>The customer-specific message that is displayed during offline license activation.</td>
</tr>
<tr>
<td>Set Offline License Deactivation Message</td>
<td>The customer-specific message that is displayed during offline license deactivation.</td>
</tr>
</tbody>
</table>
Logon Settings

Logon contains the following settings:

Figure 3-9

Table 3-7  Logon settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Group Authority Level Required</td>
<td>The minimum group authority level required to edit the Logon settings. For more information on group authority levels, see Chapter 4, “Group Settings” on page 68.</td>
</tr>
<tr>
<td>Set Logon Verification Time</td>
<td>Sets the number of seconds that the verification text for a successful logon is displayed, or disable the display of the logon verification text.</td>
</tr>
<tr>
<td>Set Max Failed Logons Before Reboot</td>
<td>Sets the maximum number of failed logons allowed before a reboot is invoked or disables this function. Note - This setting does not apply to smart cards: a smart card handles the maximum number of failed logons internally, that is, the smart card itself handles what to do when this maximum is exceeded.</td>
</tr>
<tr>
<td>Skip Management Console Logon</td>
<td>When this setting is selected, Full Disk Encryption reuses the credentials entered for preboot authentication for the logon to the Management Console. Thus, no manual logon to the Management Console is required. This will work only if the user account has permission to access to the Management Console. Note - This setting and the Windows Integrated Logon setting cannot both be enabled at the same time. If they are, the system will deny you access to the Management Console.</td>
</tr>
</tbody>
</table>
Allow Hibernation and Crash Dumps

Allows the client to be put into hibernation and to write memory dumps. This setting is enabled by default.

This setting, when selected, enables Full Disk Encryption protection when the workstation is in hibernation mode. Hibernation must be enabled in Windows for it to work in FDE. It also enables the writing of memory dumps.

On the FDE-protected workstation, all volumes selected for encryption must be fully encrypted before FDE will allow hibernation.

See the current release notes for information on operating system and hardware requirements.

When a machine is hibernating, only the FDE user account that initiated the hibernation may log on to preboot authentication. To allow another user account to use this machine as well, the setting Allow Logon to Hibernated System under Group Settings → Permissions must be enabled for that other account, otherwise a Remote Help session is required. Consider operational security management when enabling hibernation.

As FDE supports one-time logon and remote password change in hibernation mode, you must ensure that the user requesting this help is legitimate. For more information, see chapter 9, “Remote Help” on page 169 for more information.

**Note** - If this setting is changed, the PC must be rebooted before the change takes effect. A dialog box will be displayed, informing you about this.

**Note** - For hibernation to function, the system disk on which Windows is installed must be encrypted. Hibernation will not function with boot-only protection.

---

### Table 3-7 Logon settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Hibernation and Crash Dumps</td>
<td>Allows the client to be put into hibernation and to write memory dumps. This setting is enabled by default. This setting, when selected, enables Full Disk Encryption protection when the workstation is in hibernation mode. Hibernation must be enabled in Windows for it to work in FDE. It also enables the writing of memory dumps. On the FDE-protected workstation, all volumes selected for encryption must be fully encrypted before FDE will allow hibernation. See the current release notes for information on operating system and hardware requirements. When a machine is hibernating, only the FDE user account that initiated the hibernation may log on to preboot authentication. To allow another user account to use this machine as well, the setting Allow Logon to Hibernated System under Group Settings → Permissions must be enabled for that other account, otherwise a Remote Help session is required. Consider operational security management when enabling hibernation. As FDE supports one-time logon and remote password change in hibernation mode, you must ensure that the user requesting this help is legitimate. For more information, see chapter 9, “Remote Help” on page 169 for more information. <strong>Note</strong> - If this setting is changed, the PC must be rebooted before the change takes effect. A dialog box will be displayed, informing you about this. <strong>Note</strong> - For hibernation to function, the system disk on which Windows is installed must be encrypted. Hibernation will not function with boot-only protection.</td>
</tr>
</tbody>
</table>
Remote Help Settings

Remote Help contains the following settings:

**Figure 3-10**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Group Authority Level Required</td>
<td>The minimum group authority level required to edit the Remote Help settings. For more information on group authority levels, see Chapter 4, “Group Settings” on page 68.</td>
</tr>
<tr>
<td>Enable Remote Help</td>
<td>Enable Remote Help functionality? Select Yes or No. By selecting this option, you enable users to use Remote Help on this computer. The corresponding group and/or user account settings must also be selected to enable providing and/or receiving Remote Help: Permissions → Remote Help → Receive One-Time Password or Receive One-Time Logon or Provide One-Time Password or Provide One-Time Logon. <strong>Note</strong> - For Remote Help to function, both the user account of the Remote Help provider and of the Remote Help recipient must exist on the client machine. Note also that the Remote Help provider’s group authority level must be equal to or higher than the group authority level of the Remote Help recipient.</td>
</tr>
<tr>
<td>Use 20-Character Challenge</td>
<td>Select this option to use a 20-character challenge instead of the default 10-character challenge in Remote Help sessions.</td>
</tr>
</tbody>
</table>
System Passwords Policy Settings

The System Password Policy settings define the characteristics of, and requirements for, system passwords, for example, if system passwords must contain both letters and digits, what the minimum password length is, etc.

The System Password Policy settings apply only to the following passwords:

- Update validation password (System Settings → Install → Set Update Validation Password)
- Log password (System Settings → Install → Set Log Password)
- Profile password (in the new profile wizard, this password is specified under Password Protection)

Note - These settings do not affect group and user password settings.

System Passwords Policy contains the following settings:

![Figure 3-11](image)

Table 3-9 System Password Policy settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Group Authority Level Required</td>
<td>The minimum group authority level required to edit the System Passwords Policy settings. For more information on group authority levels, see Chapter 4, “Group Settings” on page 68.</td>
</tr>
</tbody>
</table>
Windows Complexity Requirements

If enabled, Full Disk Encryption will enforce password requirements similar to the Windows Complexity Requirements:

- The password must at least be six characters long.
- The password must contain characters from at least three of the following four categories:
  - English uppercase characters
  - English lowercase characters
  - Base 10 digits
  - Non-alphanumeric (for example: !, $, #, or %)
- The password must not contain the username.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Complexity Requirements</td>
<td>If enabled, Full Disk Encryption will enforce password requirements similar to the Windows Complexity Requirements:</td>
</tr>
<tr>
<td></td>
<td>• The password must at least be six characters long.</td>
</tr>
<tr>
<td></td>
<td>• The password must contain characters from at least three of the following four categories:</td>
</tr>
<tr>
<td></td>
<td>- English uppercase characters</td>
</tr>
<tr>
<td></td>
<td>- English lowercase characters</td>
</tr>
<tr>
<td></td>
<td>- Base 10 digits</td>
</tr>
<tr>
<td></td>
<td>- Non-alphanumeric (for example: !, $, #, or %)</td>
</tr>
<tr>
<td></td>
<td>• The password must not contain the username.</td>
</tr>
<tr>
<td>Require Letters and Digits</td>
<td>Both letters and digits must be used in passwords if this setting is active.</td>
</tr>
<tr>
<td>Case Sensitivity</td>
<td>Accepts upper- and lowercase letters in passwords, if enabled. If the value of this setting is “No”, all letters are interpreted as uppercase regardless of their case when entered.</td>
</tr>
<tr>
<td>Allow Special Characters</td>
<td>If enabled, this setting allows the use of the following other special characters:</td>
</tr>
<tr>
<td></td>
<td>; ! * # $ % &amp;&amp; ' ( ) * + , . / : &lt; = &gt; ? @ { }</td>
</tr>
<tr>
<td>Allow Consecutive, Identical Characters</td>
<td>Allows more than two consecutive, identical characters in passwords, if enabled.</td>
</tr>
<tr>
<td>Require Upper and Lower Case</td>
<td>The password must contain both upper and lower case characters, if enabled.</td>
</tr>
<tr>
<td>Allow Embedded Space Characters</td>
<td>Passwords may contain embedded space characters, if enabled.</td>
</tr>
<tr>
<td>Allow Leading or Trailing Space Characters</td>
<td>Allows leading or trailing space characters or both, if enabled.</td>
</tr>
<tr>
<td>Allow Password of Adjoining Characters</td>
<td>Allows a password to consist of a series of characters from adjoining keys on the keyboard, if enabled.</td>
</tr>
<tr>
<td>Set Minimum Length</td>
<td>Sets the minimum length for passwords.</td>
</tr>
</tbody>
</table>
User Account Acquisition Settings

User Account Acquisition contains the following settings:

Figure 3-12

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Group Authority Level Required</td>
<td>The minimum group authority level required to edit the User Account Acquisition settings. For example, if you set this to 7, user accounts with the group authority levels of 9, 8, and &lt;=7 can edit the User Account Acquisition settings. For more information on group authority levels, see Chapter 4, “Group Settings” on page 68. The default value is 9.</td>
</tr>
<tr>
<td>Enable User Account Acquisition</td>
<td>Enables Full Disk Encryption to automatically acquire Windows user accounts and use them to set up FDE user accounts.</td>
</tr>
</tbody>
</table>

User Account Acquisition - Acquisition Configuration

User Account Acquisition’s Acquisition Configuration folder contains the following settings:
User Account Acquisition Settings

Figure 3-13  Acquisition Configuration settings

Table 3-11  Acquisition Configuration settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Group</td>
<td>Selects the group to which the new user accounts are to be added. The drop down list displays the currently defined groups.</td>
</tr>
<tr>
<td>Period</td>
<td>The period during which this Acquisition Configuration is to be active. Can be specified as either an expiration date or a number of days.</td>
</tr>
<tr>
<td>Do at Period End</td>
<td>The action to be carried out when the User Acquisition period ends. Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Do Nothing - the configuration remains active</td>
</tr>
<tr>
<td></td>
<td>• Disable Windows Integrated Logon</td>
</tr>
<tr>
<td></td>
<td>• Disable User Account Acquisition</td>
</tr>
<tr>
<td></td>
<td>• Disable User Account Acquisition and Disable WIL</td>
</tr>
<tr>
<td>Maximum Number of User Accounts To Acquire</td>
<td>The maximum number of accounts to acquire before the 'Operation executed when maximum accounts reached' is triggered.</td>
</tr>
</tbody>
</table>
Table 3-11  Acquisition Configuration settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do When Max. No. of User Accounts Is Reached</td>
<td>Determines which action is to be taken when the maximum number of user accounts has been acquired. Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Do Nothing - the configuration remains active</td>
</tr>
<tr>
<td></td>
<td>• Execute ‘Do at Period End’</td>
</tr>
<tr>
<td></td>
<td>• Stop User Account Acquisition</td>
</tr>
<tr>
<td></td>
<td>• Overwrite oldest account</td>
</tr>
<tr>
<td></td>
<td>• Overwrite least used user account</td>
</tr>
</tbody>
</table>

**User Acquisition - Acquisition Configuration - Filter**

Acquisition Configuration’s **Filter** folder contains the following settings:

**Figure 3-14  Filter settings**

Table 3-12  Filter settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include or Exclude Matching Accounts</td>
<td>By selecting either <strong>Include</strong> or <strong>Exclude</strong> or, you either include or exclude, respectively, user accounts that match the rules of this filter.</td>
</tr>
</tbody>
</table>
Wake-on-LAN (WOL) Settings

Full Disk Encryption can be used together with Wake-on-LAN (WOL) network cards, which can be configured to start the system in Wake-on-LAN mode. The FDE Wake-on-LAN functionality will automatically log on to the computer after the computer has booted with the help of WOL network cards. This allows the operating system to start and remote updates to be performed.

**Table 3-12 Filter settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Account Name Filter</td>
<td>Here you specify a string that will be compared to the user account name. The wildcard * (asterisk) can be used in the string.</td>
</tr>
<tr>
<td></td>
<td>If the string and the user account name match, the user account name will be either included in, or excluded from, the acquisition according to what has been specified for the Include or Exclude Matching Accounts setting.</td>
</tr>
<tr>
<td>Domain Filter</td>
<td>Here you specify a string that will be compared to the Windows domain that contains the user accounts that are being filtered for user acquisition. The wildcard * (asterisk) can be used in the string.</td>
</tr>
</tbody>
</table>

**Wake-on-LAN (WOL) Settings**

Full Disk Encryption can be used together with Wake-on-LAN (WOL) network cards, which can be configured to start the system in Wake-on-LAN mode. The FDE Wake-on-LAN functionality will automatically log on to the computer after the computer has booted with the help of WOL network cards. This allows the operating system to start and remote updates to be performed.

Note - You cannot extend authority (see “Extending Authority” on page 15) when Wake-on-LAN mode is active.

**Wake-on-LAN Logon Example**

The following is an example of working with Full Disk Encryption WOL. In this example, the WOL boot time delay is set to 30 seconds and the number of permitted WOL logons is five.

1. The Full Disk Encryption profile is deployed to the Full Disk Encryption-protected computer and the WOL settings are implemented.
2. The computer is booted in Pre-Boot Authentication and the Full Disk Encryption logon dialog box is displayed for 30 seconds.
3. WOL logs on and boots the machine. The WOL logon process is now started and WOL will log on as many times as specified in the profile.

4. The computer is rebooted four times and the Full Disk Encryption logon dialog box is displayed for 30 seconds each time. WOL logs on and boots the computer.

5. The computer is rebooted. Now, all the WOL logons specified have been used and WOL is disabled on the computer.

**Note** - If a user logs on to the computer when Wake on LAN is activated, Full Disk Encryption will deactivate Wake on LAN and no Wake-on-LAN logons will be performed.

You must deploy a new profile in order to activate Wake on LAN again.

The Wake-on-LAN settings are located under **System Settings → Wake on LAN**. The following settings are available for **Wake on LAN**:

![Wake-on-LAN settings](image)

### Table 3-13 Wake-on-LAN settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Minimum Group Authority Level Required</strong></td>
<td>The minimum group authority level required to edit the Wake-on-LAN settings. For more information on group authority levels, see Chapter 4, “Group Settings” on page 68.</td>
</tr>
</tbody>
</table>
Windows Integrated Logon (WIL) Settings

Chapter 3  System Settings  61

Windows Integrated Logon (WIL) Settings

The Windows Integrated Logon (WIL) function enables users to automatically log on and preboot authentication is bypassed.
**IMPORTANT – Windows Integrated Logon**

**Warning** - When implementing WIL, weigh the total cost of ownership (TCO) impact of implementing Pre-Boot Authentication against the need for strong security when accessing the encrypted data at rest. WIL simplifies the user’s experience when logging on to encrypted machines at the cost of limiting the strength of the PC’s security configuration. Consider using Single Sign-On (SSO) in conjunction with proper Pre-Boot Authentication as an alternative to WIL.

**Security Features on WIL-enabled Computers**

To increase security when this function is enabled, a number of security feature are available in Full Disk Encryption. These features ensure that:

- The computer has not been moved from the network
- The hard drive has not been tampered with
- The hard drive has not been moved to another computer.

If the system detects any indications of the three issues above, WIL is disabled automatically, the computer reboots, and the user must authenticate in preboot.

The security features which can be enabled together with WIL are:

- **Network Locational Awareness**
  If this feature is enabled, the system pings a defined number of IP addresses during boot to make sure that the client is connected to the correct network. If these IP addresses do not answer, WIL is disabled automatically, the computer reboots and the user must authenticate in preboot.

  **Note** - All of the defined IP addresses must fail to answer for WIL to be disabled. As long as one of the IP addresses answers, WIL will continue to be enabled.

- **Hardware Hash**
  If this feature is enabled, the system generates a hardware hash from, among other things, IDs found in the BIOS and on the CPU at every start-up. If the hash is correct, the hard drive has not been removed and re-inserted into another computer. If the hash is found to be incorrect, WIL is disabled automatically, the computer reboots, and the user must authenticate in preboot.

- **Max Failed Windows Logon Attempts**
When this feature is enabled, WIL is disabled automatically after the specified number of failed logon attempts has been exceeded; the computer will then reboot; and the user must authenticate in preboot.

**Note -** The Max Failed Windows Logon Attempts feature is not supported in Windows Vista.

**User Perspective on WIL**

From the user perspective it is important to remember three things if Network Locational Awareness, Hardware Hash, and Max Failed Windows Logon Attempts are all enabled:

- If the user removes his WIL-enabled computer from the network, WIL will be disabled at the next boot, and the user will have to log on.

- Adding hardware devices to a WIL-enabled computer may be considered as tampering with the computer, and WIL will then be automatically disabled.

- Starting Windows in safe mode is not possible if Network Locational Awareness is enabled.

**Administrator Perspective on WIL**

From the administrator perspective, the following is worth noting when working with WIL-enabled computers:

- If you use the Hardware Hash feature, you should disable WIL before upgrading BIOS firmware and/or replacing hardware. When enabling WIL after the upgrade, the hardware hash will match the new configuration.

- If you enable the security features together with WIL, you should set up a Full Disk Encryption user account with which the users can log on if WIL is automatically disabled for some reason. An alternative is to display an instruction under the “FDEBE Failure WIL message” saying that the user should call the Help Desk if they get the Full Disk Encryption preboot screen due to one of the security features.

**Windows Integrated Logon** (WIL) contains the following settings:
Windows Integrated Logon (WIL) Settings

Figure 3-15

Table 3-14  Windows Integrated Logon (WIL) settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Group Authority Level</td>
<td>The minimum group authority level required to edit the Windows Integrated Logon settings. For more information on group authority levels, see Chapter 4, “Group Settings” on page 68.</td>
</tr>
<tr>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>Windows Integrated Logon</td>
<td>Select this to enable user accounts to log on without preboot authentication, that is, to bypass authentication at startup. Note that this setting affects all your users. See the information on WIL above, in “Windows Integrated Logon (WIL) Settings” on page 61.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> - If both Windows Integrated Logon and Change Credentials in the Full Disk Encryption Tray are enabled, Change Credentials in the Full Disk Encryption Tray will be disabled and grayed out in the tray menu.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> - Note that this setting and the Skip Management Console Logon setting (under “Logon Settings” above) cannot both be enabled at the same time. If they are, the system will deny you access to the Management Console.</td>
</tr>
<tr>
<td>Set PPBE Failure WIL Message</td>
<td>The text specified in this setting is the message that will be displayed to the user in the FDEPBE when WIL has been disabled automatically.</td>
</tr>
</tbody>
</table>
Enable Network Locational Awareness

Enables or disables the Network Locational Awareness function. See the description of Network Locational Awareness on page 62, for more information on how Locational Awareness functions.

Set Network Locations

Specifies the IP addresses that the Network Locational Awareness module will ping during Windows boot. See the description of Network Locational Awareness on page 62, for more information on how Locational Awareness functions.

Set Max Failed Windows Logon Attempts

The maximum number of failed logon attempts in Windows that are allowed before WIL is automatically disabled, the computer reboots, and the user must authenticate in preboot. For example, if this value is set to 1, the first time the user attempts to log on to Windows and fails, the user can still attempt to log on to Windows again (because the user has reached, but has not exceeded, the maximum number of failed Windows logon attempts). If the subsequent attempt to log on to Windows fails, WIL will be disabled etc. But if this second logon attempt is successful, the user will be given access to the machine.

This value is active again after a successful logon has been performed.

Display Enable WIL Switch

Displays the 'Enable WIL' switch in the tray icon menu and in preboot. The user can use this switch to enable WIL after any event that has caused WIL to be disabled.

If Enable Locational Awareness is selected and the user moves to an alternate location from which they cannot reach an IP defined by Set Network Locations, WIL will be disabled. This setting enables the user to disable WIL if he/she, for example, is to remove the computer from the network to work from another location -- it saves the user from a reboot at the next start-up when WIL is automatically disabled.
### Export to CSV File Button

The Export to CSV File button in the Local dialog box allows you to export the settings to a tab-separated CSV file. Note that you can also right-click a group or user account folder and select Export to CSV to export the settings for just that folder.

### Print Settings Button

The Print Settings button in the Local dialog box allows you to print the settings for a group or user account folder that is selected, but you can print only the settings your user account has access to. Note that you can also right-click a group or user account folder and select Print to print the settings for just that folder.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Hardware Hash</strong></td>
<td>Specifies if a hardware hash derived from IDs in the BIOS ROM area together with data from the CPU will be calculated to ensure that the hard drive has not been tampered with.</td>
</tr>
<tr>
<td><strong>Bypass PPBE WIL Message</strong></td>
<td>This setting will be reflected in PPBE when the user selects the 'Don’t show this message again'-checkbox in the PPBE WIL message dialog. This setting is useful for users who regularly disconnect their computers from the network and do not want to see the message explaining that WIL has been automatically disabled each time they disconnect. See the description of Network Locational Awareness on page 62, for more information on how the Locational Awareness functionality relates to the automatic disabling of WIL.</td>
</tr>
<tr>
<td><strong>Set WIL User Screen Saver Timeout</strong></td>
<td>Time in minutes before the Windows screen saver is activated for WIL users.</td>
</tr>
</tbody>
</table>
This chapter provides a general introduction to the settings that can be specified for both groups and user accounts. These settings are related to logging on, authentication, permissions, single sign-on, and password synchronization. How to configure these settings are described in Chapter 5, “Accessing and Configuring Settings for Groups and User Accounts”.

Other settings - that is, the system settings - are related to installation, the hardware devices used for authentication, logon, Wake-on-LAN, required path specifications, and a number of other aspects of the product such as Remote Help, screen savers, and hibernation. These are described in Chapter 3, “System Settings”.

In This Chapter

Settings for the “System” or Any Other Group
  Group Settings  page 68
  Authentication Settings  page 68
  Logon Settings  page 70
  Password Synchronization Settings  page 76
  Permissions Settings  page 80
  Privileged Permissions Settings  page 84
  Single Sign-On (SSO) Settings  page 87
  Sanity Checks  page 93
  Specified Values, Default Values, and How the Effective Values of Settings are Determined  page 94
Settings for the “System” or Any Other Group

Here are the settings associated with the System group; these same settings are available for each group.

If no value has been specified for a setting in either the group or the user account, the default value for that setting, if there is a default value for the setting, takes effect. For specific default values, see the Default column in the tables below.

At the end of this chapter there is a section, “Specified Values, Default Values, and How the Effective Values of Settings are Determined” on page 94, describing how effective values are determined from specified values and default values. It also explains how the values of group and user account settings are inherited.

The following setting is available under Groups → System:

Table 4-1 System settings for groups

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUID</td>
<td>(Globally Unique Identifier) The GUID is a unique reference number that identifies each group and each user account. GUIDs are used internally by Full Disk Encryption to guarantee each group and user account’s uniqueness.</td>
</tr>
</tbody>
</table>

Group Settings

The following settings are available under Groups → System → Group Settings.

Table 4-2 Group Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logon Authorized</td>
<td>User accounts in this group are allowed to log on.</td>
<td>Yes</td>
</tr>
<tr>
<td>Set Screen Saver Timeout</td>
<td>Time in minutes before the Windows screen saver is activated.</td>
<td>10</td>
</tr>
<tr>
<td>Set Expiration Date</td>
<td>The date on which this group will expire.</td>
<td>-</td>
</tr>
</tbody>
</table>
Set Group Authority Level

Sets the group authority level for this group.

A group authority level (GAL) contains a number from zero to nine (0-9) that is set for each group and for each System Settings folder in the FDEMC. Nine is the highest GAL, and zero is the lowest.

A user account with a given GAL level can change settings etc. of groups with a lower GAL: for example, user accounts that have the GAL nine, can access and edit settings for all user accounts with a GAL of eight and lower, user accounts with a GAL of five, can access and edit settings for all user accounts of four and lower, and so on.

Therefore, the GAL numbers are always displayed together with the less than operator: <, for example, <9.

A Remote Help provider's group authority level must be equal to or higher than the group authority level of the Remote Help recipient.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Group Authority Level</td>
<td>Sets the group authority level for this group. A group authority level (GAL) contains a number from zero to nine (0-9) that is set for each group and for each System Settings folder in the FDEMC. Nine is the highest GAL, and zero is the lowest. A user account with a given GAL level can change settings etc. of groups with a lower GAL: for example, user accounts that have the GAL nine, can access and edit settings for all user accounts with a GAL of eight and lower, user accounts with a GAL of five, can access and edit settings for all user accounts of four and lower, and so on. Therefore, the GAL numbers are always displayed together with the less than operator: &lt;, for example, &lt;9. A Remote Help provider's group authority level must be equal to or higher than the group authority level of the Remote Help recipient.</td>
<td>&lt;1</td>
</tr>
</tbody>
</table>

Note - Note that during installation, FDE sets the group authority level of the system group to <=9.
Authentication Settings

**Fixed Password**

Full Disk Encryption supports Unicode characters in passwords. See “Keyboard Layouts” on page 213 and “Language Support” on page 207 for more information.

**Recommendations**

If you specify that a group of accounts must use fixed passwords, you must ensure that the settings for the passwords meet strict security standards:

- Always specify complex passwords that require letters, numbers, special characters and spaces. Do not include repeating characters.
- Use a mix of uppercase and lowercase letters.
- Use non-alphanumeric symbols such as the dollar sign ($) and percentage symbol (%).
- Full Disk Encryption supports Unicode characters in passwords. See “Keyboard Layouts” on page 213 for the keyboards (locale codes) supported and “Language Support” on page 207 for the languages supported.
- Make sure the password does not include any word that can be found in a dictionary – you can use parts of words.
- Make sure the password can be remembered without having to be written down.

When deploying Full Disk Encryption, create a policy to go with the password, including end-user education and enforcement as well as a procedure for action if someone forgets their password or simply cannot get it to work.
The following settings are available under **Groups → System → Group Settings → Fixed Password**.

### Table 4-3 Fixed Password settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows Complexity Requirements</strong></td>
<td>When enabled, each time the password is changed, FDE will enforce password requirements similar to the following Windows Complexity Requirements. The password must:</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• be at least six characters long.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• contain characters from at least three of the following categories:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– English uppercase characters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– English lowercase characters</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– Base 10 digits</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– Non-alphanumeric symbols (for example: !, $, #, or%).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• must not contain the username.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Uppercase and lowercase characters other than English characters can also be used; contact Microsoft for information on exactly what can be used.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the new password does not meet the criteria described above, the password change is rejected, and a message informing the user is displayed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Passwords are checked at the following times:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• when changed in FDE preboot authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• at Windows logon</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• when changing password via the management console.</td>
<td></td>
</tr>
<tr>
<td><strong>Require Letters and Digits</strong></td>
<td>Requires that both letters and digits be used in passwords, if enabled.</td>
<td>No</td>
</tr>
</tbody>
</table>
## Authentication Settings

### Case Sensitivity
Accepts uppercase and lowercase letters in passwords, if enabled. If the checkbox is cleared, all letters are interpreted as uppercase regardless of their case when entered. Furthermore, Full Disk Encryption’s Password History function does not consider case sensitivity when assessing password uniqueness, see the Password History setting below for more details.

This setting must be enabled if the Require Upper and Lower Case setting is to be enabled.

### Allow Special Characters
If enabled, this setting allows the use of the following special characters:

`! "$% & ' () * +, -. /:; < = >? @ {}`

### Allow Consecutive, Identical Characters
Allows more than two consecutive, identical characters in passwords, if enabled.

### Require Upper and Lower Case
Requires that passwords contain both uppercase and lowercase characters, if enabled. For this setting to be enabled, the Case Sensitivity setting must be enabled.

### Allow Embedded Space Characters
Set this setting to Yes to allow the password to include a space between other characters.

### Allow Leading or Trailing Space Characters
Set this setting to Yes to allow the password to begin or end with a space.

### Allow Password of Adjoining Characters
Allows passwords to consist of a series of characters from adjoining keys on the keyboard, if enabled.

### Set Minimum Length
Sets the minimum length for passwords.

### Set Minimum Age
Sets the minimum age of passwords in days, or no limitation for password age. Minimum password age is the number of days the password must exist before being changed.

---

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Case Sensitivity</strong></td>
<td>Accepts uppercase and lowercase letters in passwords, if enabled. If the checkbox is cleared, all letters are interpreted as uppercase regardless of their case when entered. Furthermore, Full Disk Encryption’s Password History function does not consider case sensitivity when assessing password uniqueness, see the Password History setting below for more details. This setting must be enabled if the Require Upper and Lower Case setting is to be enabled.</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Allow Special Characters</strong></td>
<td>If enabled, this setting allows the use of the following special characters: ! &quot;$% &amp; ' () * +, -. /:; &lt; = &gt;? @ {}</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Allow Consecutive, Identical Characters</strong></td>
<td>Allows more than two consecutive, identical characters in passwords, if enabled.</td>
<td>No</td>
</tr>
<tr>
<td><strong>Require Upper and Lower Case</strong></td>
<td>Requires that passwords contain both uppercase and lowercase characters, if enabled. For this setting to be enabled, the Case Sensitivity setting must be enabled.</td>
<td>No</td>
</tr>
<tr>
<td><strong>Allow Embedded Space Characters</strong></td>
<td>Set this setting to Yes to allow the password to include a space between other characters.</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Allow Leading or Trailing Space Characters</strong></td>
<td>Set this setting to Yes to allow the password to begin or end with a space.</td>
<td>No</td>
</tr>
<tr>
<td><strong>Allow Password of Adjoining Characters</strong></td>
<td>Allows passwords to consist of a series of characters from adjoining keys on the keyboard, if enabled.</td>
<td>No</td>
</tr>
<tr>
<td><strong>Set Minimum Length</strong></td>
<td>Sets the minimum length for passwords.</td>
<td>Six characters</td>
</tr>
<tr>
<td><strong>Set Minimum Age</strong></td>
<td>Sets the minimum age of passwords in days, or no limitation for password age. Minimum password age is the number of days the password must exist before being changed.</td>
<td>No minimum age</td>
</tr>
</tbody>
</table>
**Authentication Settings**

Chapter 4  Group Settings  73

Set Maximum Age
Sets the maximum allowed age of a password in days.

*Note* - If you have specified a maximum age at the group level and later decide you want it set at the user account level, do the following:

1. Right-click *Set Maximum Age* in *Group Settings*.
2. Select *Reset value*.
3. Click *OK*.
4. Specify the new maximum age for each user account on the user level.

Password History
Number of passwords that must be used before a previously used password may be used again.

*Note* - Full Disk Encryption’s Password History function does not consider case sensitivity when assessing password uniqueness. Thus, if you change a password that is recorded in Password History by changing only the case of one or more of its letters, it will not be accepted as unique, and therefore that altered password will not be allowed.

Note also that passwords created in the management console are not saved in the password history, for example, if an administrator sets a password via an update profile, that password will not be recorded in the password history.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Maximum Age</td>
<td>Sets the maximum allowed age of a password in days. <em>Note</em> - If you have specified a maximum age at the group level and later decide you want it set at the user account level, do the following: 1. Right-click <em>Set Maximum Age</em> in <em>Group Settings</em>. 2. Select <em>Reset value</em>. 3. Click <em>OK</em>. 4. Specify the new maximum age for each user account on the user level.</td>
<td>No maximum age</td>
</tr>
<tr>
<td>Password History</td>
<td>Number of passwords that must be used before a previously used password may be used again. <em>Note</em> - Full Disk Encryption’s Password History function does not consider case sensitivity when assessing password uniqueness. Thus, if you change a password that is recorded in Password History by changing only the case of one or more of its letters, it will not be accepted as unique, and therefore that altered password will not be allowed. Note also that passwords created in the management console are not saved in the password history, for example, if an administrator sets a password via an update profile, that password will not be recorded in the password history.</td>
<td>1</td>
</tr>
</tbody>
</table>
**Smart Card**

The following settings are available under **Groups → System → Group Settings → Smart Card**.

**Table 4-4 Smart Card settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Expiration Warning</td>
<td>The time in days before the certificate expires and a warning is displayed to the user.</td>
<td>15 days</td>
</tr>
<tr>
<td>Certificate Expiration Action</td>
<td>The action that will be taken when a certificate expires.</td>
<td>Lock the user account and shut down computer</td>
</tr>
<tr>
<td>Certificate Revocation Action</td>
<td>The action that will be taken when a certificate is revoked.</td>
<td>Lock the user account and shut down computer</td>
</tr>
</tbody>
</table>
Windows Smart Card Insertion/Removal Handling

These settings make it possible to control the action taken when a smart-card-authenticated user removes the smart card.

The following settings are available under Groups → System → Group Settings → Smart Card → Windows Smart Card Insertion/Removal Handling.

Table 4-5  Windows Smart Card Insertion/Removal Handling settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Full Disk Encryption Token Insertion/Removal Handling</td>
<td>Enables/disables the Full Disk Encryption functionality to manage smart card removal and reininsertion in Windows. If this feature is disabled, the Windows Token Removal Handling feature is used instead.</td>
</tr>
<tr>
<td>Choose Action If Smart Card Is Removed</td>
<td>Action that will be taken if a smart card is removed. The following actions can be set:</td>
</tr>
<tr>
<td></td>
<td>• Do nothing - the user continues to be logged on.</td>
</tr>
<tr>
<td></td>
<td>• Lock the workstation – the screen lock is activated and the user needs to re-authenticate.</td>
</tr>
<tr>
<td></td>
<td>• Log off the user – the system returns to the initial Windows user logon screen. This log off action will be forced after 30 seconds.</td>
</tr>
<tr>
<td></td>
<td>• Log off and shut down – the system logs off the user, closes all open applications and saves data before shutting down the system. The shutdown will be forced after 30 seconds.</td>
</tr>
<tr>
<td></td>
<td>• Shut down immediately – the system shuts down immediately without any regard to open applications or data being processed.</td>
</tr>
</tbody>
</table>
Logon Settings

The following settings are available under Groups → System → Group Settings → Logon.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Max Failed Logons</td>
<td>Sets the maximum number of failed logons allowed before the account is locked.</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>For smart card users, the <em>smart card</em> is locked when the maximum number of failed logons configured for the individual smart card is exceeded. Note that the Full Disk Encryption Set Max Failed Logons setting is not used for smart cards, so the <em>user account</em> using the smart card will not be locked even though the smart card is locked.</td>
<td></td>
</tr>
<tr>
<td>Set Logon Limit</td>
<td>Sets the maximum number of successful logons allowed before the account is locked.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Set Failed Attempts Before Temporary Lockout</td>
<td>Sets the number of failed logon attempts before a temporary lockout occurs.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Set Temporary Lockout Time</td>
<td>Sets the duration in minutes of a temporary lockout.</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
Password Synchronization Settings

The following settings are available under Groups → System → Group Settings → Password Synchronization.

Table 4-7 Password Synchronization settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronize Windows Password to Preboot</td>
<td>When this setting is enabled, the Windows password is also used for Full Disk Encryption preboot authentication. When a user changes the Windows password, Full Disk Encryption will prompt for the Full Disk Encryption password and then synchronize it with the new Windows password. Once synchronized, changing the Windows password will automatically change the Full Disk Encryption password to the new Windows password. This setting can be enabled together with Synchronize Preboot Password to Windows (below) so that in whichever environment the password is changed it will be synchronized with the password in the other environment.</td>
<td>No</td>
</tr>
<tr>
<td>Synchronize Preboot Password to Windows</td>
<td>When this setting is enabled, the password used for Full Disk Encryption preboot authentication is also used for Windows authentication. When a user changes the Full Disk Encryption password, Full Disk Encryption will prompt for the Windows password and then synchronize it with the new Full Disk Encryption password. Once synchronized, changing the Full Disk Encryption password will automatically change the Windows password to the new Full Disk Encryption password. This setting can be enabled together with Synchronize Windows Password to Preboot so that in whichever environment the password is changed it will be synchronized with the password in the other environment.</td>
<td>No</td>
</tr>
</tbody>
</table>
Password Synchronization Settings

**Synchronizing Using the Windows Password for Authentication in Full Disk Encryption Preboot**

To synchronize and use the Windows password for authentication in Full Disk Encryption preboot, the check box in the Synchronize Windows Password to Preboot dialog box must be selected. This setting can be found under Local → Groups or User Accounts → System → Group Settings → Password Synchronization.

Synchronization takes place the first time the user logs on to Windows (see below), and then the passwords are checked at every subsequent logon until the value of this setting is set to No.

**Example 1 - Different Passwords**

Let us look at an example. In this example User1’s Full Disk Encryption and Windows passwords are different:

- Windows password XyZ123
- Full Disk Encryption password XyZ1234

Synchronize Windows Password to Preboot has been set to Yes for User1.

User1 starts the computer and logs on to Full Disk Encryption with XyZ1234. Windows starts, and User1 logs on to Windows with XyZ123. Because the passwords differ, Full Disk Encryption prompts User1 to enter your current Full Disk Encryption password.

User1 enters the Full Disk Encryption password, XyZ1234, and clicks OK.

Password synchronization is confirmed.

When User1 logs on to Full Disk Encryption again, the password XyZ123 is used. Until the Windows password change is changed, User1’s Windows password, XyZ123, will be used to log on to Full Disk Encryption.

---

*Note* - Password synchronization is associated with only the first user account that is used to log on to Windows after rebooting the workstation. Password synchronization functionality is not supported for third-party solutions.
Example 2 - Identical Passwords

Let us look at another example. In this example User1’s Full Disk Encryption and Windows passwords are the same, but User1 changes the Windows password:

- Windows password XyZ123
- Full Disk Encryption password iXyZ123

Synchronize Windows Password to Preboot has been set to Yes for User1.

User1 starts the computer and logs on to Full Disk Encryption with XyZ123.

Windows starts, and User1 logs on to Windows with XyZ123.

User1 presses Ctrl+Alt+Delete and changes the Windows password to AbC456.

Full Disk Encryption confirms that its password has been successfully changed.

The next time User1 logs on to Full Disk Encryption, the password AbC456 must be used.

Synchronizing Using the Full Disk Encryption Preboot Authentication Password for Authentication in Windows

To synchronize and use the Full Disk Encryption password for preboot authentication for Windows authentication, the check box in the Synchronize Preboot Password to Windows dialog box must be selected. This setting can be found under Local → Groups or User Accounts → System → Group Settings → Password Synchronization.

Synchronization takes place the first time the user logs on to Windows (see below), and then the passwords are checked at every subsequent logon until the value of this setting is set to No. Once the passwords are synchronized, changing the Full Disk Encryption password will automatically change the Windows password to the new Full Disk Encryption password. Note that the Synchronize Preboot Password to Windows setting applies only to password changes made in Full Disk Encryption.
Permissions Settings

The following settings are available under Groups → System → Group Settings → Permissions.

**Table 4-8 Permissions settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Credentials</td>
<td>Sets whether or not the account(s) are allowed to change their own fixed passwords and/or credentials. Note that for account(s) to be able to change other user accounts’ fixed passwords and/or user account names, the Privileged Permissions setting Create and Edit User Accounts must be enabled. See Create and Edit User Accounts under Privileged Permission settings, above. Note - To create a temporary smart card user, this setting must be set to Yes.</td>
<td>No</td>
</tr>
<tr>
<td>Change Single Sign-On</td>
<td>Sets whether or not the account(s) are allowed to change the single sign-on settings. When this option is selected, the account’s SSO setting can be changed when being authenticated by Full Disk Encryption. For more information on SSO, see “Single Sign-On (SSO) Settings” on page 87.</td>
<td>No</td>
</tr>
</tbody>
</table>
Table 4-8  Permissions settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Logs</td>
<td>Sets whether or not the account(s) are allowed to view logs.</td>
<td>No</td>
</tr>
<tr>
<td>Uninstall</td>
<td>Sets whether or not the account(s) are allowed to uninstall Full Disk Encryption and run recovery.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Grants the account the authority to remove Full Disk Encryption from this system. If the account does not have this privilege, an administrator must go to the computer to remove the software.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Full Disk Encryption can only be removed by two user accounts that both have this authority. A Full Disk Encryption user alone cannot remove Full Disk Encryption. See “Removing Full Disk Encryption” on page 173 for more information.</td>
<td></td>
</tr>
<tr>
<td>Management Console Logon</td>
<td>Sets whether or not the account(s) are allowed to log on to the Management Console.</td>
<td>No</td>
</tr>
<tr>
<td>Create Recovery Media</td>
<td>Sets whether or not the account(s) are allowed to create recovery media.</td>
<td>No</td>
</tr>
<tr>
<td>Allow Logon to Hibernated System</td>
<td>Sets whether or not to allow the account(s) to log on to a system hibernated by another account.</td>
<td>No</td>
</tr>
<tr>
<td>Change to Fixed Password</td>
<td>Sets whether or not the account(s) are allowed to be changed to use fixed password authentication.</td>
<td>No</td>
</tr>
<tr>
<td>Change to Dynamic Token</td>
<td>Sets whether or not the account(s) are allowed to be changed to use dynamic token authentication.</td>
<td>No</td>
</tr>
<tr>
<td>Change to Smart Card</td>
<td>Sets whether or not the account(s) are allowed to be changed to use smart-card authentication.</td>
<td>No</td>
</tr>
</tbody>
</table>
Permissions Settings

Table 4-8  Permissions settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Credentials in the Full Disk Encryption tray</td>
<td>Sets whether or not the account(s) are allowed to change their credentials in the Full Disk Encryption tray.</td>
<td>No</td>
</tr>
</tbody>
</table>

Note - When authenticating to change credentials in the Full Disk Encryption tray, the Full Disk Encryption authentication dialog box has a Remote Help button. This button enables only One-time logon; Remote password change is not available via this Remote Help button.

Note - If both Windows Integrated Logon (see Figure 3-15 on page 64) and Change Credentials in the Full Disk Encryption Tray are enabled, Change Credentials in the Full Disk Encryption Tray will be grayed out and disabled in the tray menu.
Remote Help Settings

The following settings are available under Groups → System → Group Settings → Remote Help.

**Note** - For Remote Help to function, *both* the user account of the Remote Help provider and of the Remote Help recipient must exist on the client computer. Note also that the Remote Help provider’s group authority level must be equal to or higher than the group authority level of the Remote Help recipient.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide ‘Remote Password Change’</td>
<td>Sets whether or not the account(s) are allowed to provide Remote Password Change for other user accounts. For a user account to be able to provide Remote Help, this option must be selected and also the Enable Remote Help setting under System Settings → Remote Help.</td>
<td>No</td>
</tr>
<tr>
<td>Provide ‘One-Time Logon’</td>
<td>Sets whether or not the account(s) are allowed to provide One Time Logon for other user accounts. For a user account to be able to provide Remote Help, this option must be selected and also the Enable Remote Help setting under System Settings → Remote Help.</td>
<td>No</td>
</tr>
<tr>
<td>Receive ‘Remote Password Change’</td>
<td>Sets whether or not the account(s) are allowed to receive Remote Password Change. For a user account to be able to provide Remote Help, this option must be selected and also the Enable Remote Help setting under System Settings → Remote Help.</td>
<td>No</td>
</tr>
</tbody>
</table>
The following settings are available under Groups → System → Group Settings → Privileged Permissions.

### Privileged Permissions Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive ‘One-Time Logon’</td>
<td>Sets whether or not the account(s) are allowed to receive <strong>One-Time Logon</strong>.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>For a user account to be able to provide Remote Help, this option must be be selected and also the Enable Remote Help setting under System Settings → Remote Help.</td>
<td></td>
</tr>
<tr>
<td>Response Format</td>
<td>Sets whether to use <strong>Numeric</strong> or <strong>Alphanumeric</strong> format for the response in Remote Help.</td>
<td>Numeric</td>
</tr>
</tbody>
</table>

### Table 4-9 Remote Help settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Permissions</td>
<td>Sets whether or not the account(s) are allowed to change permissions.</td>
<td>No</td>
</tr>
<tr>
<td>Change Privileged Permissions</td>
<td>Sets whether or not the account(s) are allowed to change privileged permissions.</td>
<td>No</td>
</tr>
<tr>
<td>Create and Edit User Accounts</td>
<td>Sets whether or not the account(s) are allowed to:</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>- Create user accounts.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Edit other accounts’ settings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Edit other user accounts’ names.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Edit other user accounts’ fixed passwords.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note that this setting does not allow these accounts to change/edit their own names or fixed passwords; to do that the Permissions setting, <strong>Change Credentials</strong> must be enabled. See Permissions Settings, below.</td>
<td></td>
</tr>
</tbody>
</table>

### Table 4-10 Privileged Permissions settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Permissions</td>
<td>Sets whether or not the account(s) are allowed to change permissions.</td>
<td>No</td>
</tr>
<tr>
<td>Change Privileged Permissions</td>
<td>Sets whether or not the account(s) are allowed to change privileged permissions.</td>
<td>No</td>
</tr>
<tr>
<td>Create and Edit User Accounts</td>
<td>Sets whether or not the account(s) are allowed to:</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>- Create user accounts.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Edit other accounts’ settings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Edit other user accounts’ names.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Edit other user accounts’ fixed passwords.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note that this setting does not allow these accounts to change/edit their own names or fixed passwords; to do that the Permissions setting, <strong>Change Credentials</strong> must be enabled. See Permissions Settings, below.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 4-10 Privileged Permissions settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Create and Edit Groups</strong></td>
<td>Sets whether or not the account(s) are allowed to:</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>– Create groups.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– Edit groups' settings.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– Edit groups' names.</td>
<td></td>
</tr>
<tr>
<td><strong>Advanced Profile Editing</strong></td>
<td>Sets whether or not to allow the following:</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>– Opening and editing of profiles created in versions of Pointsec for PC prior to the current version.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– Changing the GUID on groups and users.</td>
<td></td>
</tr>
<tr>
<td><strong>Create Profiles</strong></td>
<td>Sets whether or not the account(s) are allowed to create profiles.</td>
<td>No</td>
</tr>
<tr>
<td><strong>Remove User Accounts</strong></td>
<td>Sets whether or not the account(s) are allowed to remove user accounts.</td>
<td>No</td>
</tr>
<tr>
<td><strong>Remove Groups</strong></td>
<td>Sets whether or not the account(s) are allowed to remove groups.</td>
<td>No</td>
</tr>
<tr>
<td><strong>Remove Profiles</strong></td>
<td>Sets whether or not the account(s) are allowed to remove profiles.</td>
<td>No</td>
</tr>
</tbody>
</table>
Table 4-10 Privileged Permissions settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit System Settings</td>
<td>Sets whether or not the account(s) are allowed to edit the system configuration under <strong>System Settings</strong>.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Grants the account the authority to change the local system settings on the computer they are logged on to. These changes can be overridden with an update profile.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When this option is not selected, editing system settings will not be available to the user account.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>See Chapter 6, “Working with Installation and Update Profiles” on page 119 for more information.</td>
<td></td>
</tr>
<tr>
<td>Access to Local</td>
<td>Sets whether or not the account(s) are allowed to access <strong>Local</strong> in the Full Disk Encryption folder tree.</td>
<td>No</td>
</tr>
<tr>
<td>Access to Remote</td>
<td>Sets whether or not the account(s) are allowed to access <strong>Remote</strong> in the Full Disk Encryption folder tree.</td>
<td>No</td>
</tr>
</tbody>
</table>
Single Sign-On (SSO) Settings

Single Sign-On Settings

The following settings are available under Groups → System → Group Settings → Single Sign-On.

Table 4-11 Single Sign-On settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SSO</td>
<td>Sets whether or not single-sign-on functionality to Windows (only) is to be enabled for the account(s).</td>
<td>No</td>
</tr>
<tr>
<td>Entrust SSO</td>
<td>Sets whether or not Entrust single-sign-on functionality is to be used by the account(s). For information on Entrust SSO, see Chapter 4, “Entrust SSO” on page 89.</td>
<td>No</td>
</tr>
<tr>
<td>Smart Card Triggers Windows SSO logon</td>
<td>Sets whether or not to allow using a smart card to trigger the Windows SSO logon.</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

How Single Sign-On and OneCheck Logon Function

Full Disk Encryption’s single sign-on functionality enables a user to log on to FDE and to be seamlessly logged into Windows (only). Full Disk Encryption’s OneCheck Logon (see “OneCheck Logon” on page 26) enables a user to log on to FDE and to be seamlessly logged into Windows, Endpoint Connect VPN, and Media Encryption. Enabling OneCheck Logon automatically disables single sign-on.

Single Sign-On

With single sign-on (SSO) enabled for a Full Disk Encryption user account, the user can log on to Full Disk Encryption and automatically authenticate and be logged on to Windows. To enable SSO, select Enable single sign-on functionality? in the Enable SSO dialog in the management console (Group Settings → Single Sign-On → Enable SSO).

Enabling OneCheck Logon automatically disables the Enable SSO setting (see below).
OneCheck Logon

With OneCheck Logon enabled for a Full Disk Encryption user account (see “OneCheck Logon” on page 26), the user will log on to Full Disk Encryption and automatically authenticate and be logged on to Windows, Endpoint Connect VPN, and Media Encryption. Whenever the users unlock their computers, for example after hibernation, stand-by or sleep mode, they will use their Full Disk Encryption user account credentials. The Windows credentials will never be used.

To enable OneCheck Logon, select Enable single sign-on functionality? in the Enable SSO dialog in the management console (System Settings → OneCheck Logon → Enable OneCheck Logon).

Note - Enabling OneCheck Logon automatically disables the Enable SSO setting (see above).

Note - Authentication with smart cards is not supported when OneCheck Logon is enabled.

Getting Account Credentials

After enabling SSO or OneCheck Logon for a Full Disk Encryption user account on a computer, Full Disk Encryption must learn the account’s credentials. This is done at the first logon after Single sign-on or OneCheck Logon is enabled. At this logon, the user logs on to Windows as usual. Full Disk Encryption then stores this information securely and uses it on subsequent logons where SSO or OneCheck Logon has been enabled.

When SSO Is Turned Off

When the SSO option is not selected, no credentials are passed to Windows; this permits a different Windows user account to be used.

Note that when SSO has been turned off, no Windows credentials will be recorded or used, and the ‘chain’ is broken. When SSO is then turned back on, the previous credentials must be specified again for SSO to function again.

Note - When Remote Help is used to authenticate a user account that uses single sign-on (SSO), the recorded SSO credentials for that user account are invalidated. This is to prevent a Remote Help administrator from leveraging SSO to ‘impersonate’ a user.
SSO and OneCheck Logon — Password Changes

Periodically, it will be necessary to change the account’s Windows password. Full Disk Encryption will look for Change Password dialog boxes to record the changes. When a Change Password dialog box is opened, Full Disk Encryption records what is entered into the new password field. At the next reboot, SSO or OneCheck Logon will work as usual, as the new password has already been stored.

Limitation in OneCheck Logon Functionality When Resuming a Hibernated Machine

When a hibernated session is resumed and OneCheck Logon is enabled, the user must enter credentials in both preboot and in the OneCheck Logon logon.

Entrust SSO

After implementing Entrust SSO on a computer, Full Disk Encryption must learn the Entrust profile name. This is used to signify the name of the Entrust account that will be used.

A requirement of the Entrust SSO implementation is that the Full Disk Encryption password and the Entrust password be the same.

Once SSO has been implemented, an Enable Single Sign On option is displayed on the Full Disk Encryption logon screen. Selecting this option will use the stored Entrust profile to log on to Entrust. When the option is not selected, Entrust logon is manual.

It should be noted that when SSO has been turned off, no Entrust credentials will be recorded or used and the previous credentials will continue to be stored. When SSO is then turned back on, those previous credentials will be used again. After SSO has been turned back on, there is a Record New Credentials option on the SSO screen. By selecting this option, the user can enter a new Entrust profile at the logon.

Note - If there is any conflict between the Entrust and Full Disk Encryption user password settings, SSO will not work. The Full Disk Encryption password must be exactly the same as the Entrust password for Full Disk Encryption/Entrust SSO to work.

Entrust Profile Revocation

Entrust SSO will lock a Full Disk Encryption user account if the corresponding Entrust profile has been revoked. In this case, when the computer boots, the profile will be checked before the Windows logon is activated. If the Entrust user has been
revoked the Full Disk Encryption user will be locked, and the computer will be automatically rebooted. At this point, the user will not be able to access the computer without Remote Help.

To ensure that Full Disk Encryption acts on the revocation, you need to configure the Active Directory (AD) server as described below. Use the ADSIEdit extension to the Microsoft Management Console (MMC) (For more information, see http://computerperformance.co.uk/w2k3/utilities/adsi_edit.htm).

Once the active directory server has been configured, Full Disk Encryption will be notified of the revocation of Entrust profiles. When Full Disk Encryption encounters such a notification of revocation, when the user account authenticates to Full Disk Encryption the following occurs:

- The message “Your Full Disk Encryption account has been locked due to a revoked Entrust profile” is displayed
- Authentication to Windows is denied
- The event is logged.

Configuring the Active Directory Server

To configure the active directory server, follow the three steps described below:

- “Setting the dsHeuristic Attribute” on page 90
- “Setting up ANONYMOUS LOGON” on page 91
- “Enabling Issue Updated CRLs on the Entrust Server” on page 92

Setting the dsHeuristic Attribute

First, set the dsHeuristic attribute by following these directions:

1. Connect to Configuration.
2. Browse to CN=Configuration → CN=Services → CN=Windows NT → CN=Directory Service.
4. Set the dsHeuristic attribute to 00000002 (Allow anonymous clients to perform any operation that is permitted by the access control list [ACL]). For more information, see http://support.microsoft.com/default.aspx?scid=kb;en-us;326690.
Setting up **ANONYMOUS LOGON**

Next, do the following to set up anonymous logon:

1. Connect to **Configuration**.
2. Browse to **CN=Configuration → CN=Services → CN=Public Key Services → CN=AIA**.
3. Select **Properties** for **CN=AIA**.
4. Select the **Security** tab.
5. Add **ANONYMOUS LOGON** and go to its **Advanced properties**.
6. Edit **Permission Entries**, making sure that the following are checked: **List Contents**, **Read All Properties**, **Read Permissions**.
7. Apply to **This object and all child objects**.
Enabling Issue Updated CRLs on the Entrust Server

Finally, enable **Issue Updated CRLs** in the Entrust Security Manager Administration, see your Entrust manual for information on how to do this.
Sanity Checks

When a profile is created a number of ‘sanity checks’ are performed to make sure that the profile does not contain any fatal error. The Settings That Might Have Undesirable Effects window displays the results of the sanity checks.

These are the checks performed on the profile:

- **Does at least one account have access to the Management Console?**
  At least one user account with access to the Management Console is required to be able to perform administration on the machine.

- **Are there any accounts in the profile for which no type of authentication has been defined?**
  This warning occurs only when you create a profile ‘based on local settings’. You must manually set the authentication:
  1. Right-click each user in the tree structure.
  2. Select Name and Authentication.
  3. Define the authentication details.

- **Do you really want Windows Integrated Logon enabled on this machine?**
  Windows Integrated Logon bypasses all preboot authentication.

- **Is at least one user account defined in this installation profile?**
  If no user accounts are defined in the profile, no user account will be able to log on to the machine on which Full Disk Encryption is installed with this profile.

- **Do at least two user accounts in the profile have permission to create recovery media?**
  Recovery media cannot be created, and the system cannot be recovered, unless at least two user accounts have permission to create recovery media on the machine on which Full Disk Encryption is installed with this profile.

- **Do at least two user accounts in the profile have permission to uninstall Full Disk Encryption?**
  You will not be able to remove Full Disk Encryption from the machine on which it has been installed with this profile unless the profile contains at least two user accounts that have permission to perform uninstall.

- **Has an expiration date been set for each temp user account in the profile?**
Specified Values, Default Values, and How the Effective Values of Settings are Determined

Usually an expiration date should be defined for each temp user account. If this is not the case, you will be warned about each temp user account that does not have an expiration date defined.

This section describes how effective values are determined from specified values and default values. It also explains how the values of group and user account settings are inherited.

Inheritance

When the value of a group setting is specified and no value is specified for the corresponding user account setting, all user accounts in that group will inherit the group setting value.

Specified, Effective, and Default Values

When the two different values are specified for the same group and user account setting, the value specified for the user account overrides the value set for the group. For example, if the Fixed Password setting Set Minimum Length is set to six for the System group and to eight for the user account ADMIN1, which belongs to the System group, the minimum length for fixed passwords for user account ADMIN1 will be eight. There is, however, one exception to this rule: if Make the group value override the user account value has been selected for the setting, the group value will override the value specified for the user account. Make the group value override the user account value can be selected by right-clicking the setting in the management console and choosing Make the group value override the user account value.

When chosen, the setting Name, Specified Value and Effective Value will be displayed in bold and the hammer handle of the setting icon will be displayed in red, see Figure 4-4 on page 95.
Specified Values, Default Values, and How the Effective Values of Settings are Determined

**Figure 4-4** Make the group value override... The group value when selected

<table>
<thead>
<tr>
<th>Name</th>
<th>Specified Value</th>
<th>Effective Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Complexity Requirements</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

A user account setting that has been overridden by **Make the group value override the user account value** is displayed in italics and the hammer handle of the setting icon is displayed in red, the Specified Value of the setting is also in italics, and the Effective Value is displayed in bold (to signal that the Group Value has overridden the Specified Value), **Figure 4-5 on page 95**.

**Figure 4-5** Make the group value override... The user account value when selected

<table>
<thead>
<tr>
<th>Name</th>
<th>Specified Value</th>
<th>Effective Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Complexity Requirements</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

To remove **Make the group value override the user account value** from a setting, right-click the setting and deselect **Make the group value override the user account value**.

The FDEMC displays the value set for each group setting and each user account setting under **Specified Value**, and it displays the value that is in effect under **Effective Value**, see **Figure 4-6 on page 96** for some examples.

This is how Full Disk Encryption sets the Specified Value and the Effective Value:

- If a value has been specified for a setting, that value is displayed under **Specified Value**.
- If no value has been specified for a setting, a dash ‘-’ is displayed under **Specified Value**.
- If a value has been specified for a setting, but that value has been overridden; the specified value is displayed under **Specified Value**, and the value that overrides the specified value is displayed under **Effective Value**.
- If no value has been specified for a setting at the group and at the user account levels, and Full Disk Encryption assigns a default value for that setting; a dash ‘-’ is displayed under **Specified Value**, and the default value is displayed under **Effective Value**.
- If no value has been specified for a setting, and Full Disk Encryption does not assign a default value to that setting; a dash ‘-’ is displayed under both **Specified Value** and **Effective Value**.
- If no value has been specified for a setting, a dash ‘-’ is displayed under **Specified Value**. If there is no default and no value has been specified for a setting, a dash ‘-’ is displayed under **Effective Value**.
Specified Values, Default Values, and How the Effective Values of Settings are Determined

**Figure 4-6** Specified Value and Effective Value

<table>
<thead>
<tr>
<th>Name</th>
<th>Specified Value</th>
<th>Effective Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logon Authenticated</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Set Screen Saver Timeout</td>
<td>-</td>
<td>10</td>
</tr>
<tr>
<td>Set Expiration Date</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Set Group Authority Level</td>
<td>&lt;=9</td>
<td>&lt;=9</td>
</tr>
</tbody>
</table>
In This Chapter

- Accessing FDE Settings in Full Disk Encryption Management Console page 98
- Printing Settings page 100
- Exporting Settings to a CSV File page 101
- Exporting Logs page 101

This chapter describes how you can access and configure the system settings and settings for group and user accounts.

The system settings are related to installation, the hardware devices used for authentication, logon, Wake-on-LAN, required path specifications, and a number of other aspects of the product such as Remote Help, screen savers, and hibernation. These settings are described in Chapter 3, “System Settings” on page 23.

Other settings - those for Groups and User Accounts - are relevant for volume access, logging on, authentication, permissions, Remote Help, single sign-on, and password synchronization. These settings are described in Chapter 4, “Group Settings” on page 67.
Accessing FDE Settings in Full Disk Encryption Management Console

In This Section

Accessing the Full Disk Encryption Management Console  page 98
Accessing Local Settings for Groups and User Accounts  page 99

Accessing the Full Disk Encryption Management Console

The Full Disk Encryption Management Console (FDEMC) gives you quick and easy access to all Full Disk Encryption functions.

To start the FDEMC:

1. Click Start, navigate to the Check Point program group and select Endpoint Security → Management Console. The Full Disk Encryption Management Console (FDEMC) program starts:

Figure 5-1
Accessing Local Settings for Groups and User Accounts

Local settings are settings for the machine on which you are logged on, usually the machine on which Full Disk Encryption is first installed and from which the installation of Full Disk Encryption will be deployed to all clients.

The Full Disk Encryption Management Console (FDEMC) allows you to work with system, local, and remote settings. It provides wizards for defining, among other things: sets, groups, and users accounts.

To open the Local Settings:

1. Start Full Disk Encryption and select one of the following:
   - Local in the folder tree to the left
   - Go To Local under Local Installation in the main panel

2. The Local dialog box is displayed.

3. Click Edit Settings and the folder tree under Local is displayed in the left panel. This group of settings can be specified for both groups and user accounts.

4. Do one of the following:
   - For group settings
     Under Groups, expand the System folder to see the folders that contain Group Settings.
   - For user settings
     Under User Accounts, expand the tree for a user and then expand the Account Settings folder that is displayed; you will see the folders containing the account settings. You also see that the same settings exist for both groups and user accounts:
Printing Settings

The Print Settings option in the Local dialog box allows you to print the local settings.

Note - Before printing local settings you must have already set up the printer or printers you want to use.

To print local settings:
1. Under Local, click Print Settings. The Print dialog box is displayed.
2. Select a printer and click OK to print the settings.
Exporting Settings to a CSV File

The Export Settings to CSV File option in the Local dialog box allows you to export the settings to a file as tab-separated CSV values.

Exporting Logs

The log export functionality allows log content to be exported in the following formats, which support import into other management and data systems: Comma Separated Values (CSV), Tab Separated Values (TSV) and XML. This includes logs from Local Settings or from a configuration set. Export can be done on the basis of selectable criteria.

To export logs:
1. Select Export Local Log Database in the Local dialog box.
   The Save As window is displayed.
2. Specify the name of the file that will contain the log, as well as the file type in the Save as type drop-down box. Valid file types are XML, CSV (Comma Separated Values) and TSV (Tab Separated Values).
3. Click Save.
Chapter 6

Protecting Workstations Using Full Disk Encryption

In This Chapter

Introduction page 103
Full Disk Encryption Deployment Overview page 104
Before Deploying page 104
Managing Groups and User Accounts page 107
Working with Configuration Sets page 113
Working with Installation and Update Profiles page 119
Before Creating Profiles page 123
Creating Installation Profiles page 124
Deploying Full Disk Encryption page 130
Verifying a Full Disk Encryption Deployment page 132
Running Full Disk Encryption as a Service on a PC page 133
Creating and Deploying Update Profiles page 133

Introduction

This chapter explains how to deploy Full Disk Encryption to protect workstations in your organization. It also gives some useful information about the authentication methods which can be set during the deployment of Full Disk Encryption.
Full Disk Encryption Deployment Overview

Deploying Full Disk Encryption involves completing the following tasks in Full Disk Encryption management console.

- **Creating Group and User Accounts**
  Create the necessary groups and users. Configure authentication methods for any accounts you want to deploy, set security settings and include the accounts in groups, see “Managing Groups and User Accounts” on page 107.

- **Creating Configuration Set**
  Create a set in which to store the installation profile, see “Root Directory Path” on page 113.

- **Creating Installation Profile**
  Configure which volumes are to be encrypted, who can access the drives, privilege levels and update settings etc., see “Working with Installation and Update Profiles” on page 119.

- **Installing Full Disk Encryption**
  Install Full Disk Encryption on end-users' workstations, see “Deploying Full Disk Encryption” on page 130.

- **Verifying Full Disk Encryption Deployment**
  Verify that Full Disk Encryption has been installed and that the clients' volumes have been encrypted, see “Verifying a Full Disk Encryption Deployment” on page 132.

Before Deploying

In This Section

About Authentication Methods  page 105
Do Not Modify the Pointsec for PC.msi Package  page 105
Read the Release Notes  page 105
Considerations for Other Programs  page 106
Review precheck.txt  page 106
About Authentication Methods

Before you start installing Full Disk Encryption, you should know something about the types of passwords you will be asked to specify during the installation.

You can use the following types of passwords when installing Full Disk Encryption: fixed passwords and dynamic tokens.

**Fixed Passwords**

Fixed passwords, as the name implies, do not change. In Full Disk Encryption, a fixed password must contain at least six characters but no more than 31.

**Dynamic Tokens**

Dynamic tokens, also known as one-time passwords, change constantly. Users use a small device, usually called a dynamic token, to generate a new password every time they start their workstations. Dynamic tokens are intended for environments requiring better security than fixed passwords can provide where password standards are not rigorous enough.

**Smart Cards**

Smart cards provide secure storage of user credentials and digital certificates. Full Disk Encryption supports both smart cards with readers, and readerless USB tokens.

Do Not Modify the Pointsec for PC.msi Package

Do not modify the *Pointsec for PC.msi* package in any way. For instance, do not attempt to modify the *Pointsec for PC.msi* package by using transforms. Modification of the *Pointsec for PC.msi* package invalidates the supportability of the product.

The following sections discuss information you need to know and things you need to check before you start to install Full Disk Encryption.

Read the Release Notes

The release notes contain the latest information on Full Disk Encryption. Read them to find out what is new, fixed or changed. You can find the release notes on your Full Disk Encryption CD.
Considerations for Other Programs

Consider the following:

- **Pointsec Media Encryption**
  
  If Pointsec Media Encryption is already installed on the workstation on which you want to install Full Disk Encryption, Single Sign On (SSO) will not work properly.
  
  To fix this, manually insert the string value `CompatibleGinas=pme.dll` in Windows’ registry.
  
  This action does not have to be taken if Pointsec Media Encryption is installed after Full Disk Encryption.

- **Full Disk Encryption and Entrust**
  
  For information on Full Disk Encryption and Entrust installation and integration, please see Chapter 4, “Entrust SSO” on page 89.

**Review precheck.txt**

`precheck.txt` is an installation settings file designed to make installing Full Disk Encryption even simpler. By configuring `precheck.txt`, you can streamline the installation process and configure settings faster. The `precheck.txt` file is in the same folder as the `Pointsec PC.msi` file.

When you start to install Full Disk Encryption, the installation program reads `precheck.txt` and determines if it should terminate in certain circumstances as specified by you. You can also configure `precheck.txt` when installing on a computer running IBM Rapid Restore Ultra (RRU).

In addition, you can use `precheck.txt` to configure settings for third-party Graphical Identification and Authentication (GINA) dlls, Single Sign On (SSO) delay times, and update intervals.

`precheck.txt` settings can be altered after installation by editing them in the `Pointsec` registry key. For more information on the `precheck.txt` settings, please see the appendix “The Precheck.txt File” on page 237.
Managing Groups and User Accounts

In This Section

Creating Groups  page 107
Adding a User Account to a Group  page 108
Password Authentication  page 109
Dynamic Token Authentication  page 110
Smart Card Authentication  page 112

This chapter explains how to create and manage Full Disk Encryption groups and user accounts on the computer on which you have installed Full Disk Encryption.

In Full Disk Encryption, a user account always belongs to one (and only one) group. This means that before you create any user accounts, you must first create one or more groups to contain user accounts.

Note - You cannot move a user account from one group to another, but must instead delete the user account from its current group and then redefine it in the other group.

Creating Groups

Assume that we do a master installation of Full Disk Encryption on an admin PC. Once it is completed and you have opened the Management Console, you can see that a group called System has already been created. (Note that only if the installation was manual is the group called System; if the installation was done by profile, the group could be named anything.)

Under the System group folder, there is a tree of User Accounts where you will find the two users you defined during installation.

You can now create new groups if desired.

To create a new group:

1. Right-click Groups. The New Group menu is displayed.
2. Click New Group and enter a group name in the New Group dialog box.
3. Click OK. The new group is now listed in the tree under Groups.

Note that there are currently no user accounts in the User Accounts folder in the new group.
4. In the Group Settings folder for the new group you have created, configure the relevant group settings, see Chapter 4, “Group Settings” on page 67, for details on these settings.

Expand the Group Settings folder tree for the new group, and you will see the folders as described in Chapter 4, “Group Settings” on page 67.

**Adding a User Account to a Group**

As discussed above, once the installation of Full Disk Encryption is completed and you have opened the Full Disk Encryption Management Console (FDEMC), you can see that a group called System has already been created. Under the System group folder is a tree of User Accounts where you will find the two user accounts you defined during installation.

These two users are assigned what can be called ‘system administrator privileges’, for example, all the Privileged Permissions and all the Permissions except Create Recovery Media are set to Yes. Almost all other user accounts you define will be assigned significantly more restricted privileges than those of a system administrator.

**To add another user account to the group:**

1. Right-click User Accounts and then Add User Account.

2. The User Account wizard opens:

![Figure 6-1](image-url)
3. Select the relevant information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User account name</td>
<td>The name must be 1-31 characters long. Full Disk Encryption supports Unicode characters in user account names. See “Keyboard Layouts” on page 213 for the keyboards (locale codes) supported.</td>
</tr>
<tr>
<td>Type of user account</td>
<td>The type of user account can be: normal, service user, or temporary. These types of accounts are described in Chapter 1, “Types of User Accounts” on page 16.</td>
</tr>
<tr>
<td>Authentication method</td>
<td>Authentication for this user account will be done via:</td>
</tr>
<tr>
<td></td>
<td>• Password</td>
</tr>
<tr>
<td></td>
<td>• Dynamic Token</td>
</tr>
<tr>
<td></td>
<td>Note – Full Disk Encryption does not support dynamic tokens that are formatted to be FIPS compliant.</td>
</tr>
<tr>
<td>Temporary user account settings</td>
<td>Here you can specify the number, from 1-50, of Normal user accounts that can be created from this Temporary user account. Say, for example, that you need to create five Normal accounts on a client. Here you specify ‘5’, and five Normal accounts can be created from this Temporary user account -- this is more efficient than having to send one profile for each Normal user account you want to create.</td>
</tr>
</tbody>
</table>

4. After specifying the logon name, type and password authentication method, click **OK**. Note that defining a temporary user account is done the same way as with a normal user account.

5. The next step in the user account wizard depends on the authentication method you chose in step 3, continue to one of the following sections:
   - “Password Authentication” on page 109,
   - “Dynamic Token Authentication” on page 110,
   - “Smart Card Authentication” on page 112.

**Password Authentication**

1. Set and confirm your password.
Adding a User Account to a Group

2. Click Next, and after viewing the result do one of the following:
   - If you are satisfied, click Finish.
   - If you want to make changes, click Back, make the changes and click Finish.

Use the above process to define any other user accounts that will use password authentication.

**Dynamic Token Authentication**

Note - Full Disk Encryption does not support dynamic tokens that are formatted to be FIPS compliant.

To use dynamic token authentication:

1. Do one of the following:

---

**Table 6-2 Password fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>The password must meet the criteria you have specified for fixed passwords in <strong>Group Settings</strong>, see Chapter 4, “Fixed Password” on page 70. Note that while you enter the password and confirm that password in the <strong>Confirm Password</strong> text box, the text ‘Invalid Password’ is displayed to the right of the <strong>Password</strong> text box. This text is displayed until the password meets all the criteria that have previously been configured for passwords.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Enter the password you entered in the <strong>Password</strong> text box.</td>
</tr>
<tr>
<td>Force change of password at next logon</td>
<td>Selecting this option forces the user to specify a new user account password at the next logon.</td>
</tr>
<tr>
<td>Password Rules</td>
<td>Full Disk Encryption ensures that the fixed password that is entered complies with the fixed password settings specified under <strong>Group Settings</strong> → <strong>Authentication Settings</strong> → <strong>Fixed Password</strong> and under <strong>Account Settings</strong> → <strong>Authentication Settings</strong> → <strong>Fixed Password</strong>. For example, that the password is at least 6 characters long, if the default value for <strong>Set Minimum Length</strong> is being used.</td>
</tr>
</tbody>
</table>
Adding a User Account to a Group

– To enter token values manually, see the procedure “Manually Entering Token Values” on page 111.

– To enter token values by importing a file, see the procedure “Entering Token Values by Importing a File” on page 111.

Manually Entering Token Values

To enter token values manually:

1. Choose Add dynamic token by manually entering values and click Next.
2. Enter the information required.

Table 6-3 Dynamic Token dialog fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Token Serial Number</td>
<td>Serial number, usually found on the back of the dynamic token.</td>
</tr>
<tr>
<td>Algorithm</td>
<td>Choose the algorithm used by the token: DES or 3DES. DES stands for Data Encryption Standard, and 3DES stands for Triple DES.</td>
</tr>
<tr>
<td>Dynamic Token Key</td>
<td>Enter the token key you received from Full Disk Encryption with the token.</td>
</tr>
<tr>
<td>Challenge Length</td>
<td>A number from 1-8.</td>
</tr>
<tr>
<td>Response Length</td>
<td>A number from 1-16.</td>
</tr>
<tr>
<td>Challenge Format</td>
<td>Choose either Hexadecimal or Ascii.</td>
</tr>
<tr>
<td>Response Format</td>
<td>Choose either Friendly or Decimal.</td>
</tr>
</tbody>
</table>

3. Click Next and do one of the following:

   – If you are satisfied, click Finish.
   – If you want to make changes, click Back, make the changes and click Finish.

Entering Token Values by Importing a File

1. Choose Add dynamic token by importing from file and click Next.
2. Navigate to your token import file.
3. Enter the password, which is the Encryption key in the key file you intend to import. The password is usually provided with the material that comes with your dynamic tokens. Click OK.

   The tokens are imported:
4. Select the token you wish to connect to the user. Then click **Next** and do one of the following:
   - If you are satisfied, click **Finish**.
   - If you want to make changes, click **Back**, make the changes and click **Finish**.

**Smart Card Authentication**

A reminder: in order for smart card authentication of a user account to function, note that you must correctly specify the type of smart card readers you will use under **Hardware Devices** in **System Settings**, see “Hardware Device Settings” on page 28 for details. Furthermore, you must ensure that the required drivers are installed for the smart cards and smart card readers you will use, See “Smart Cards, Smart Card Readers and their Drivers” on page 219 for details.

To choose smart card authentication:

1. Select one of the smart card certificates listed under **Issued to**. To display detailed information about a certificate, double-click the certificate in the list.
2. Click \textbf{OK}.

3. Click \textbf{Finish} to complete the creation of a user account that uses a smart card for authentication.

\section*{Working with Configuration Sets}

In This Section

\begin{itemize}
\item Root Directory Path \hspace{1cm} page 113
\item Directory Paths \hspace{1cm} page 114
\item Creating a New Set \hspace{1cm} page 115
\item Exporting/Importing Set Configurations \hspace{1cm} page 118
\end{itemize}

Configuration sets, hereafter referred to simply as sets, are used as share points from which you can carry out your remote management. Typical remote management tasks include installing (and uninstalling) Full Disk Encryption on remote clients, updating the configuration on remote clients, providing one or more centralized points for storage of logs, and so on.

\section*{Root Directory Path}

Best practice is to use the set to provide a central configuration point for a root directory path, as shown in the illustration below.

\begin{itemize}
\item Note - Full Disk Encryption will not allow you to associate the same certificate with two user accounts. When Full Disk Encryption detects that you are attempting to do so it issues an error message and makes an entry in the log, and the wizard closes. Examine the log for more information about the error.

The wizard looks for certificates locally in \textbf{Personal Store} and, if accessible, on smart cards and USB tokens, as well as in Microsoft Active Directory.

If a certificate is stored in more than one place, it will be listed as many times as the wizard finds it. When selecting a certificate listed multiple times, it does not matter which of the listed instances of that certificate you choose. Review the \textbf{Location} column in the list to determine if the a certificate is listed more than once.
\end{itemize}
The root directory path points to a shared folder on a server. When you define a set, one of the things you will do is specify the paths to the directories here. These paths are described below.

**Directory Paths**

The following directory paths should be created. At least one directory path must be specified when you define a set, and the sets can be edited under **System Settings → Install**.

**Tip** - Best practice is to specify the path in UNC format: `\\<server>\<share>\...`

**Profile Storage**

The Profile Storage directory is where profiles are stored while you edit them in the Full Disk Encryption Management Console (FDEM), prior to their being published. There can be more than one Profile Storage directory. As long as the profiles are in one of these directories, they cannot be pulled by clients.

**Update Profile**

The Update Profile directory is where update and uninstall profiles are placed so they can be pulled by the clients. By specifying subdirectories for individual client computers, you can target your updates to individual client computers.

In a profile, this path is referred to as the Update Profile Path.

**Install**

The Install directory is where you store installation packages, install profiles, and other configuration files that are to be used during the installation, for example, the `precheck.txt` file and the files in the `oemvar` folder.
Central Log

This is the directory to which clients copy their log files. In a profile, this path is referred to as the Central Log Path.

Recovery

The Recovery directory should be the target directory or directories for the client’s recovery files. Full Disk Encryption stores recovery files in these directories.

Recovery files contain information required to decrypt the Full Disk Encryption-protected computer. For more information on recovery, see Chapter 12, “Recovering Information” on page 179.

In a profile, this path is referred to as the Recovery Path.

Note - Ensure that the Recovery Path is accessible to the logged on user because encryption will not start if the recovery file cannot be created in the specified directory.

Upgrade

Place the upgrade source package and any supporting configuration files in this directory or these directories. This is the directory from which clients will pull the upgrade source package and other supporting configuration files from these directories.

In a profile, this path is referred to as the Upgrade Path.

Creating a New Set

To create a new set:

1. Start the Full Disk Encryption Management Console (FDEMC) and select Remote.
2. Click **New Set** and the **Create New Set Wizard** opens. Click **Next**.

3. Enter a descriptive name that makes clear what the configurations and profiles belong to.
You can select **Automatically create a directory structure** if you want Full Disk Encryption to create folders. This requires that you have previously configured a root directory on which the directory structure will be created. This root directory must be a shared folder on the network, for example:

```
\<server name>\<shared folder>...
```

You must also have the required permissions to create the directories. If these conditions are met, and you specify the shared folder under **Enter the root directory in which the directories will be created**, the FDEMC automatically enters the following subfolders to the shared folder and displays them in the relevant fields of the wizard:

- `<shared folder>\Profile Storage`
- `<shared folder>\Update Storage`
- `<shared folder>\Install`
- `<shared folder>\Log`
- `<shared folder>\Recovery`
- `<shared folder>\Upgrade`

4. Click **Next**.

![Figure 6-6](image)

5. Specify one or more **Profile Storage Paths** and click **Add** for the path to be included in the set. When no more paths are to be added, click **Next**.

6. Specify one or more **Update Profile Paths** and click **Add** for each path to be included in the set. When no more paths are to be added, click **Next**.
7. Specify one or more Install Paths and click Add for the path to be included in the set. When no more paths are to be added, click Next.

8. Specify one or more Log Paths and click Add for the path to be included in the set. When no more paths are to be added, click Next.

9. Specify one or more Recovery paths and click Add for the path to be included in the set. When no more paths are to be added, click Next.

10. Specify an Upgrade path, and click Add for the path to be included in the set.

11. Click Next.

12. Create the set by clicking Finish.

The set is created. Note that the set configuration is saved when the set is created.

Exporting/Importing Set Configurations

Set configurations can be exported from one FDEMC and imported into another FDEMC. All set configurations, and individual set configurations can be exported or imported.

Exporting All Set Configurations

To export all set configurations:
1. Select File → Export All Set Configurations.... A browser window is displayed.
2. Browse to the directory in which you want so store the set configurations, and click Save.

Exporting One Set Configuration

To export a single configuration set:
1. Right-click on a set in the FDEMC folder tree and select Export Set Configuration.... A browser window is displayed.
2. Browse to the directory in which you want so store the set configuration, and click Save.

Importing a Set Configuration

To import a set configuration:
1. Select File → Import Set Configuration.... A browser window is displayed.
2. Browse to the directory in which you want to store the set configuration, and click **Open**.

**Publishing Profiles Directly from the Profile List**

You can publish a profile directly from the list of profiles in the FDEM.

**Update and Uninstallation Profiles**

To publish an update or uninstallation profile in the profile list:

1. Right-click the profile, and select **Publish profile to**.
2. Select the configured update profile path you want, and the profile is automatically copied to the selected path.

**Installation Profiles**

To publish an installation profile in the profile list:

1. Right-click the profile name, and select **Publish profile to**.
2. Select the configured Install path you want, and the installation profile is automatically copied to the selected path.

![Figure 6-7](image)

**Working with Installation and Update Profiles**

In This Section

- **Introduction**  
  page 120
- **Before Creating Profiles**  
  page 123
- **Creating Installation Profiles**  
  page 124
- **Creating an Update Profile**  
  page 134
- **Deploying Full Disk Encryption**  
  page 130
Introduction

Full Disk Encryption profiles contain user account and group information and the settings which control, for example:

• which volumes are to be encrypted,
• who can access the drives,
• privilege levels and
• update settings.

There are four types of Full Disk Encryption profiles:

• installation profiles

Verifying a Full Disk Encryption Deployment page 132
Running Full Disk Encryption as a Service on a PC page 133
Creating and Deploying Update Profiles page 133
Pushing Update Profiles to Computers page 139

This chapter explains how to create Full Disk Encryption profiles that are used to:

• Install Full Disk Encryption on the computers (client machines) in your networks
• Update/manage the user accounts, groups and other settings on client machines

Upgrading the Full Disk Encryption software is described in Chapter 7, “Upgrading Full Disk Encryption” on page 141 and uninstalling Full Disk Encryption in Chapter 10, “Removing Full Disk Encryption” on page 173.

About Full Disk Encryption Profiles

Full Disk Encryption profiles contain user account and group information, the settings which control, for example:

• which volumes are to be encrypted,
• who can access the drives,
• privilege levels and
• update settings.

There are four types of Full Disk Encryption profiles:

• installation profiles
• update profiles
• uninstall profiles
• upgrade profiles.

**What's in a Profile?**

All profiles contain system settings. Group settings and user account settings are optional, but each user account must belong to a group.

**System Information**

System information includes, for example, paths to the central server where recovery files, update profiles and software updates are stored. It also contains settings related to, for example, installation, hardware devices, Wake-on-LAN, and Remote Help.

In addition to the system information described above, installation profiles also contain information on which disk volumes are to be protected by Full Disk Encryption, the type(s) of security (encryption and/or boot protection) to be used, and the encryption algorithms to be used.

**Group Information**

Group information contains the system settings for local groups and their authorization, including the user's right to receive Remote Help and security settings such as keyboard lock. Group information also contains the privileges for system administrators, administrators, and user accounts at the group level.

**User Account Information**

User account information contains settings for individual user accounts, including the account's authorization for different volumes, Remote Help and security settings such as time-out settings for the screen saver and unlocking the keyboard lock. User account information also contains the privileges for system administrators, administrators and user accounts.

**Types of Profiles**

**Installation Profiles**

There are two types of installation profiles:
• Silent installation
• Interactive installation.

**Silent Installation Profiles** — A silent installation profile contains the group and user account information and system settings. When a silent installation profile is deployed on a computer, Full Disk Encryption is installed on the computer without any interaction with the user. In other words, end users are unaware that Full Disk Encryption is being installed on their computers. The first time an end user will be aware of Full Disk Encryption is the first time the computer is booted after the silent installation.

**Interactive Installation Profiles** — When an interactive installation profile is deployed on a computer, Full Disk Encryption is installed on the computer with some interaction with the user. For example, the administrator can configure the profile so that Full Disk Encryption displays a message informing the logged on user that installation will begin shortly and what, if anything the user should do; similarly the administrator can configure a message to be displayed when the Full Disk Encryption installation is complete and what the user should do at that point.

---

**Note** - If you deploy Full Disk Encryption using interactive installations, you may want to suppress the Reboot needed dialog box, which is normally displayed at the end of the installation dialog. To suppress this dialog box, assign the value ReallySuppress to the MSI REBOOT property in the following way:

```
setup.exe /v"REBOOT=reallySuppress"
```

Note that there is no space between the “v” and the first double quote (““).

---

**Update Profiles**

As changes in security requirements and personnel occur, you will need to update the settings that have been deployed on Full Disk Encryption-protected computers. You can use update profiles to change settings, and to deploy and remove smart card drivers, smart card reader drivers, and HID drivers. This is done by specifying the desired settings in the **Preboot Drivers** setting, see “Adding and Removing Preboot Drivers with the Preboot Drivers Setting” on page 30. You can also use update profiles to deploy language files, see the **Change Language Files** setting under “Install Settings” on page 35.

**Note** - The changes to drivers or language files are not implemented until the update profile has been saved and imported by the client(s).
To do things, create and place a correctly configured update profile in the Update directory on the designated file server.

**Note** - The users on the computers on which you wish to update security settings or make other changes must have read and execute permissions to this directory.

Full Disk Encryption-protected computers regularly check this directory for new update profiles. When they find a new update profile they download it and implement the changes. For more information, see “Creating and Deploying Update Profiles” on page 133.

### Upgrade Profiles

An upgrade profile contains information necessary to upgrade Full Disk Encryption-protected computers to a new version. For more information on upgrade profiles, see “The Characteristics of an Upgrade Profile” on page 146.

### Uninstall Profiles

If, for any reason, you need to remove Full Disk Encryption from computers in your network, you can do so by placing an uninstall profile in the Update directory, see Chapter 10, “Removing Full Disk Encryption” on page 173 for more information.

**Note** - The user accounts on computers from which you wish to remove Full Disk Encryption must have read and execute permissions to this directory.

---

**Before Creating Profiles**

Before you can create a profile you must have set the update validation password and created a set to which the profile can belong to. Sets are meant to help you locate and work with your profiles. For example, you might want to have a set for each department’s profiles if they differ.

How to set the update validation password is described in Chapter 3, “Install Settings” on page 35, and how to create sets in “Root Directory Path” on page 113.
Creating Installation Profiles

In This Section

- Creating an Installation Profile
- Creating a Profile Based on Another Profile or Local Settings
- Converting Pre-6.2 Profiles to 6.3.1 Profiles

The first profile we will create and deploy is a silent installation profile, the most commonly used profile when deploying Full Disk Encryption for the first time.

Creating an Installation Profile

The process of creating and deploying an installation profile involves:

- Creating the profile.
- Adding group and user accounts.
- Configuring the profile settings.
- Deploying the profile to computers in the network; see “Deploying Full Disk Encryption” on page 130.

Note - Before you can create any profiles, the Profile Validation Password (Local → Edit Settings → System Settings → Install) must be set.
To create an installation profile:

1. In FDEM, click **Remote** and then **New Profile**. The **New Profile Wizard** is displayed.
2. Click **Next**. The **New Profile** dialog box opens.
3. Select the set in which you want to include this installation profile. Click **Next**.
Creating an Installation Profile

Figure 6-9

1. Select Installation, silent. Click Next.

2. Enter the name of the new profile.

   Note - Spaces are not allowed in profile names. For example, update_profile.upp is a valid profile name, but update profile.upp is not.

3. Enter and confirm the password, which will be required when you want to edit the profile.

   Note - The password policy applied to the password specified here is the password policy of the user account that is currently logged on and is creating the new profile. See Chapter 4, “Authentication Settings” on page 70 for more information on the settings that can be specified for fixed passwords.

4. Click Next.

5. If you want to base the profile on the local settings of the computer on which you are creating the profile, or on an existing profile, select Existing profile or local settings:

6. If you select to base the profile on Existing profile or local settings, you must then either browse to an existing profile or specify which local settings the new profile is to be based on (System, Group, or User Account), then click Next.

7. View the information and, if satisfied, complete the creation of the profile by clicking Finish.
11. When you click Finish, Full Disk Encryption performs a number of ‘sanity checks’ on the profile that you want to save. The Settings That Might Have Undesirable Effects window displays the results of the sanity checks. For more information on sanity checks, see Chapter 4, “Sanity Checks” on page 93.

12. Choose one of the following to options:
   a. Click Cancel to alter the relevant setting or settings.
      Each time you click OK the sanity checks are performed, and any warnings of problematic settings will be displayed. If none of the sanity checks produce a warning, the profile is created.
   b. Click OK to accept the settings that cause the warnings. The profile will be created with the problematic settings.

13. The installation profile you just created is now displayed among the profiles under Remote → [Your Set] → Profiles. It contains the values for the settings that will be set on the client machines installed with this profile.

   When the profile is created, it is prepopulated with the local System Settings of the machine on which the profile was created. If any of these values have not been set on the local machine, the Full Disk Encryption default values will be used. It is good practice to examine the System Settings in the profile and make any required changes.

**Creating Groups and User Accounts in the Profile**

The next step is to create groups and user accounts in the profile you have created.

**To create groups and user accounts:**

1. Go to Remote → [Your Set] → Profiles and double-click the profile. Create groups, and create user accounts.

2. Define a group that contains at least two administrator user accounts.
3. Best practice: Create another group in which you define a temporary user account. It is preferable to work with group settings rather than with individual user account settings.

   **Note** - There are two reasons a specific group must be created for the temporary user:
   
   – The settings should be completely separate from those of the administrator accounts.
   
   – This group can be used to delete user accounts created with a temporary user account. For instructions on doing this, see “Deleting user accounts created with a temporary user account” on page 128.

4. Examine the default settings in the installation profile and decide if they are to your satisfaction, otherwise change them:

   – **System Settings**
     
     See Chapter 3, “System Settings” on page 23 for a description of these settings.

   – **Group settings for the Administrator group**
     
     Note that administrators usually have stricter rules for passwords than normal user accounts do.

   – **Group settings for the group containing the temp user.**

   The profile is now ready. The next step is to delete the user account created with a temporary user account.

**Deleting user accounts created with a temporary user account**

**To delete user accounts created with a temporary user account:**

1. Create an update profile based on the installation profile containing the temporary user account, based only on **Groups**.

2. Open the update profile for editing and remove all groups except the one that contains the temporary user.

3. Mark the only remaining group for removal.

4. Save the profile by clicking **OK**.
Creating a Profile Based on Another Profile or Local Settings

5. Place this profile in the **Update** folder on the client machine from which you want to remove the user account.

**Note** - Do not place the profile in the **Publish Profile** directory because this will cause the deletion of all user accounts created with the temporary user account.

Deploying Smart Card Drivers Together with Smart Card User Accounts in Installation Profiles

When creating smart card user accounts via installation profiles, it is important that the required smart card drivers exist on the machine prior to logon. This is necessary if smart card user accounts are to be able to log on directly at first-time authentication.

**To install smart card drivers at the same time as Full Disk Encryption is installed:**

1. Add the **Driver** setting to the **precheck.txt** file. Specify each driver file name if more than one driver is involved, separating the file names with semicolons (no spaces are allowed). Below is an example in which the smart card driver files `msc_p11.bin` and `prd_ccid.bin` are specified:

   ```text
   Drivers=msc_p11.bin;prd_ccid.bin
   ```

Creating a Profile Based on Another Profile or Local Settings

To facilitate the specification of the system settings, group settings, and user account settings information in a new profile, you can base the new profile on

- An existing profile, or
- The local settings of the computer on which you create the profile.

When you base a new profile on local settings or an existing profile, you can select which settings you want to use (if however you do not choose to base it on Group Settings, the User Account Settings choice will be grayed out and cannot be selected).

**Note** - A new installation or upgrade profile inherits the Pointsec PC/Check Point license number of the computer on which it is created even if **Existing profile or existing settings** is not selected under **Base new profile on**.
Converting Pre-6.2 Profiles to 6.3.1 Profiles

Pre-6.2 profiles can be used in 6.3.1 only if you convert them to 6.3.1 profiles. To convert a pre-6.2 profile to a 6.3.1 profile:

1. Move the pre-6.2 profile to a 6.3.1 Profile Storage path.
2. Open the pre-6.2 profile in the Pointsec PC 6.3.1 management console.
3. Verify that the 6.3.1 serial number/license is used by checking System Settings → Install → Product Serial Number.
4. Convert and save the pre-6.2 profile by clicking OK.

The converted profile can now be used in Pointsec PC 6.3.1.

Deploying Full Disk Encryption

In This Section

Using an Installation Profile
Using an MSI Package

Using an Installation Profile

This section explains how to deploy Full Disk Encryption using a login script.

You can initiate a Full Disk Encryption silent installation profile from any computer that can map a drive and run an executable file.

To deploy Full Disk Encryption:

1. Copy the contents of the SetupFiles directory on the Full Disk Encryption CD to the Install directory that contains the installation profile.

   **Note** - For installation, recovery, and updates to function correctly, user accounts on Full Disk Encryption-protected computers must have RX permissions to the entire Full Disk Encryption directory structure to handle temporary information and updates.

2. Create and distribute the following login script to the computers on which you want to install Full Disk Encryption:
Using an MSI Package

This section explains how to deploy Full Disk Encryption using an MSI package.

**Note** - When Full Disk Encryption is installed on a client using deployment software such as SMS or Tivoli, the service that runs the msi.exe must be run as LOCAL_SYSTEM, and the service must have “Interact with desktop” activated. If the service is run as a normal user account, the installation will fail.

**Windows XP**

If you are deploying Full Disk Encryption on Windows XP, the Full Disk Encryption MSI package can be started using msiexec.exe /i "Pointsec for PC.msi".

---

If Not Exist %homedrive%\progra~1\Pointsec for PC\pscontrol.exe goto Install
Exit
:Install
start msiexec.exe /i "\[servername]\[installdirectory]\Pointsec for PC.msi" /q
exit

The next time the users log in and the script runs, Full Disk Encryption will be installed with the settings you have configured in the installation profile and the computers will be Full Disk Encryption protected.

**Note** - To log error information from a failed installation, the user executing the script also needs rights to create folders and files in the **Install** directory.

Local administrator permissions are required to install.
The following parameters are supported:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>/i</td>
<td>Installation</td>
</tr>
<tr>
<td>/x</td>
<td>Uninstallation</td>
</tr>
<tr>
<td>/L</td>
<td>Logs installation information</td>
</tr>
<tr>
<td>/q</td>
<td>Silent installation</td>
</tr>
</tbody>
</table>

**Note** - Full Disk Encryption does not support any other parameters, transforms or modifications to the .msi package!

**Windows Vista**

Windows Vista requires higher admin rights than Windows XP when installing. You do not have these higher rights automatically even if you are logged in as administrator on Vista, and therefore you cannot start the msi-file in the same way as on Windows XP. However, these rights have been added to the autorun.exe so if you run the autorun.exe it will generate an msiexec command line with the correct rights.

You can use the same parameters for the autorun file as for the msi-file. The parameters you use for the autorun file will automatically be added to the msiexec command, for example:

```
the command
autorun.exe /install=q
```

generates the command line

```
msiexec /i "Pointsec for PC.msi" /q
```

---

**Verifying a Full Disk Encryption Deployment**

When you have deployed Full Disk Encryption on the clients, it is important to verify that Full Disk Encryption has been installed and that the clients’ volumes have been encrypted.
1. Verify the deployment by checking the text files found in the predefined Log directory/directories on the file share(s).

One text (.txt) file for each client machine is created in the Central Log directory if the System Settings → Install → Enable status export to file checkbox has been selected in the profiles. The text file tells you if Full Disk Encryption has been installed, which volumes have been encrypted (provided that the client machine actually has been encrypted), and if a recovery file has been created for the specific client machine. The text files contain the client machine’s name in the file name, for example:

   london_office_pc_1.txt, london_office_pc_2.txt, london_office_pc_3.txt and so on.

2. Check the recovery (.rec) files found in the predefined Recovery directory/directories on the file share(s). The number of recovery files should correspond to the number of clients deployed; that is, there should be 200 recovery files in the directory/directories if Full Disk Encryption was deployed to 200 clients. Each recovery file is identified with the client machine’s name in the file name, for example:

   london_office_pc_1.rec, london_office_pc_2.rec, london_office_pc_3.rec and so on.

Running Full Disk Encryption as a Service on a PC

For information on running Full Disk Encryption as a service on a PC, see Appendix L, “Using a Service Start Account” on page 251.

Creating and Deploying Update Profiles

In This Section

Creating an Update Profile  page 134
Working with Accounts in an Update Profile  page 138
Creating an Update Profile

You can easily update security settings on Full Disk Encryption-protected computers by creating and deploying an update profile. The best way to create an update profile is to edit the original installation profile and save it as an update profile. For details on available settings, see Chapter 3, “System Settings” on page 23 and Chapter 4, “Group Settings” on page 67.

Creating an Update Profile

An update profile is used to change the settings on a system that has already been installed.

You can either create an update profile from scratch or one based on an already existing installation or update profile.

An update profile contains only the changes you want to make to the target installation(s). For example, if you want to change only one setting, you specify only that setting.

Difference Between Remove and Mark for Removal

Remove

Remove deletes all data regarding the user or group in the profile. If you deploy this profile, it will not affect the users or groups you just removed because there is information left in the profile regarding these users or groups.

Mark for Removal

When marking a group or user account for removal, the group or user remains in the profile and acts as a container for sending the information to remove the group or user on the machine(s) the profile is deployed to.

Summary of Differences

Mark for Removal is used to remove things at remote machines; in other words, all the information about the user or group is in the profile because it has to be sent to the client(s) where it will remove the user or group. The information must be sent to the client, so it is designated as “Mark for Removal” to signify to the admin that this user or group will be removed on the client machine(s).
Remove simply removes data from the profile, and is a way to edit the contents of a profile. You might have five groups, and want to update a setting for only one of the groups. In this case, you could remove the four groups you do not want to affect, leaving only the group you want to change in the profile.

**Unique User Accounts**

**GUIDs**

Full Disk Encryption creates unique user accounts. Even if you define a user account with the same name on two different machines, these are actually two different accounts. While they have the same user account name, because they have unique GUIDs (Globally Unique Identifiers), they are unique user accounts.

**How User Accounts and Groups Are Identified**

When you download an update profile to a local machine, Full Disk Encryption's default processing is to import the profile only if a user account name in the profile matches a user account name on the local machine and their GUIDs are identical. Otherwise, the profile will not be imported by the local machine.

**Matching by User Account Name Only**

You can, however, enable matching by 'user account name only' by selecting User account name in the User account and group identification method window in the New Profile wizard, see Figure 6-10: “The User Account and Groups Identification Method” on page 136. Then, if the user account names match (it does not matter if the GUIDs do not match), the profile will be imported anyway.

When the profile is imported, the GUID of the user account in the profile replaces the GUID of the user account on the local machine, and the settings in the profile will update the settings of the user account on the local machine.

**Note:** if the user account name in the profile is the user account name of the logged on user:

- The profile will be imported
- The logged on user’s GUID will be replaced by the GUID in the profile, and
- The logged on user will be logged off the system.

If the two user accounts whose names matched are members of different groups, the user account on the local machine will be moved to the group of the user account in the profile and will be given the new GUID that resides in the profile. Empty groups will not be removed.
Ensuring that Administrator Accounts Exist on Both the Admin Machine and All Client Machines

Keeping track of which administrator user accounts are defined on which machines can be of critical importance. This is illustrated in the following example of a scenario involving installing Full Disk Encryption and subsequently attempting to uninstall it from a machine using an uninstallation profile.

Manually Installing Full Disk Encryption on the Admin Machine

Manually install Full Disk Encryption on what will be called the admin machine. In the process of installing Full Disk Encryption you will have defined two administrator user accounts, let us call them Admin_A and Admin_B.

To create an installation profile:

1. On the admin machine, create an installation profile that you will use to deploy Full Disk Encryption to 100 client machines.

2. In the installation profile, define two administrator user accounts, Admin_C and Admin_D. These administrators are authorized to authenticate the uninstallation of any of the 100 clients that will have Full Disk Encryption installed on them via this installation profile.

3. Deploy the installation profile to the 100 client machines, and assume that Full Disk Encryption is installed on the 100 client machines.
4. Create an uninstallation profile that you will use to remove Full Disk Encryption from one machine. In the process of creating the profile, the two administrator accounts on the admin machine, Admin_A and Admin_B, must authenticate the uninstall profile.

5. Deploy the uninstallation profile to the machine from which you want to uninstall Full Disk Encryption. You will see, however, that Full Disk Encryption is not uninstalled from the machine.

**Why Full Disk Encryption Is Not Uninstalled**

Full Disk Encryption is not uninstalled from the target machine because the client machines were installed with an installation profile that included Admin_C and Admin_D. When the target machine checked the uninstallation profile, which was created on the admin machine, it finds that it was authenticated by Admin_A and Admin_B, two administrators who are unknown to the target machine (which knows of only Admin_C and Admin_D). For this reason, the profile is not activated on the target machine.

You might think that you can define Admin_A and Admin_B on the target machine via an update profile. But what this will result in is the creation of two user accounts named Admin_A and Admin_B on the target machine, but although these accounts have the same name as the accounts on the admin machine, the accounts on the target machine had GUIDs that are different from those of the Admin_A and Admin_B accounts on the admin machine.

**Ensuring that the Required User Accounts are on the Machines that Require them**

To get the relevant user accounts on the machines that require them:

**Alternative 1**

1. Install Full Disk Encryption on the admin machine.
2. Create the installation profile you will use to install Full Disk Encryption on the client machines.
3. Create an update profile based on the installation profile used to install on the client machines, including Admin_A and Admin_B in this update profile. Thus, Admin_A, Admin_B, Admin_C, and Admin_D will be on the admin machine and Admin_C and Admin_D will be on the client machines.
4. Update the admin machine using the update profile created in the previous step.
**Alternative 2**

1. Install Full Disk Encryption on the admin machine.
2. Create the installation profile that you will use to install Full Disk Encryption on the client machines.
3. Uninstall Full Disk Encryption from the admin machine.
4. Use the installation profile created above to install Full Disk Encryption on the admin machine after adding Admin_A and Admin_B to the profile. Now Admin_A, Admin_B, Admin_C, and Admin_D are in the admin machine and Admin_C and Admin_D are on the client machines.

**Working with Accounts in an Update Profile**

You can add, edit and delete group and user accounts on a Full Disk Encryption-protected computer by configuring accounts in an update profile.

**Deploying an Update Profile**

![Checkmark] **Note** - All computers on which you want to update Full Disk Encryption must have read and execute permissions to the Update directory.

Full Disk Encryption-protected computers check for update profiles at a predefined update interval. The default is 180 minutes. If the computer is not connected to the network, the check is made the next time the user logs on to the network. The update interval can be altered in the precheck.txt file at installation, see the Full Disk Encryption Installation Guide for more information.

**Deploying an Update Profile to a Specific Computer**

The first time a Full Disk Encryption-protected computer retrieves an update profile, it creates a unique folder in the update profile path.

Whenever you need to deploy a specific update profile to the computer, you can do so by placing the profile in this folder.

Full Disk Encryption uses the name of the computer as the folder name.
Pushing Update Profiles to Computers

If you want a Full Disk Encryption-protected computer to search for an update profile outside the set interval, you can achieve this by using Full Disk Encryption’s **Push** feature. This feature enables updates to be imported even if the computer goes off-line once the update has been placed on the system.

**To push an update profile:**

Place the profile in the **Work** folder, for example: C:\Program Files\Pointsec\Pointsec for PC\Work.

If Full Disk Encryption finds an update profile (or software upgrade profile) in the **Work** folder, Full Disk Encryption verifies that the update is new, imports it, and deletes the update from, in this case, C:\Program Files\Pointsec\Pointsec for PC\Work.

The import is completed within 10 seconds. Full Disk Encryption then continues using the normal update interval as specified.

**How Does the Update Profile Affect a Logged-on User?**

If an update profile affects the logged-on user, Full Disk Encryption will execute the new settings in one of two ways. Depending on the settings, they will be implemented either immediately or the next time the user logs on after rebooting the computer.

If the update profile contains a deletion of the logged-on user, the deletion is implemented immediately, and Full Disk Encryption displays a dialog giving the user the choice to reboot the PC.

**Note** - On Windows XP and Vista, Full Disk Encryption will display an additional warning informing the user of what has happened.
How Does the Update Profile Affect a Logged-on User?
Chapter 7

Upgrading Full Disk Encryption

In This Chapter

- Introduction to Upgrading Full Disk Encryption Software ........................................ page 141
- Upgrading Pointsec for PC 4.x and 5.x Installations to Full Disk Encryption 7.x ............ page 142
- Upgrading from Pointsec for PC 6.x.x to Full Disk Encryption 7.x ............................... page 155

Introduction to Upgrading Full Disk Encryption Software

You use upgrade profiles to upgrade 4.x and 5.x versions of Pointsec for PC to Pointsec PC 6.2 or later, see “Upgrading Pointsec for PC 4.x and 5.x Installations to Full Disk Encryption 7.x” on page 142 for details.

**Note** - The users on computers on which you wish to upgrade Full Disk Encryption, must have read and execute permissions to this directory.

For details on upgrading from 6.x to 7.x, which is not done via profiles, see “Upgrading from Pointsec for PC 6.x.x to Full Disk Encryption 7.x” on page 155.
Upgrading Pointsec for PC 4.x and 5.x Installations to Full Disk Encryption 7.x

In This Section

Overview  ................................................................. page 142
From Which Legacy Versions Can You Upgrade?  .................................................. page 144
Requirements for Upgrading a 4.x/5.x Client ......................................................... page 144
The Process of Upgrading ....................................................................................... page 145
The Characteristics of an Upgrade Profile ............................................................ page 146
Configuring an Upgrade Profile ............................................................................. page 149
Legacy Account Handling ...................................................................................... page 150
Upgrade Operations ............................................................................................. page 151

Upgrading is the process of replacing one version of software with a newer version of that software.

This chapter describes how a 4.x or 5.x version of Pointsec for PC can be replaced with Full Disk Encryption 7.x. Note that versions 4.x and 5.x are often called legacy versions below.

For details on upgrading from Pointsec for PC 6.x.x to Full Disk Encryption 7.x, see “Upgrading from Pointsec for PC 6.x.x to Full Disk Encryption 7.x” on page 155.

Overview

The (legacy) Pointsec for PC 4.x or 5.x functionality is used to perform the upgrade to Full Disk Encryption 7.x. This means that the upgrade of legacy clients is performed by distributing/deploying “upgrade packages” to the 4.x/5.x Directory path for software upgrades or to the Full Disk Encryption/Work folder on the client computers.

Note - Upgrading a machine while it is being encrypted is not supported.

It is not possible to perform an upgrade by executing the Full Disk Encryption MSI package.

During the upgrade of a Pointsec for PC 4.x/5.x version to Full Disk Encryption 7.x the following things should be noted:
– Protection of volumes is retained.
– Legacy user/group and system settings are discarded.
– Legacy user accounts can be kept or upgraded.
– Upgraded legacy users keep their names and status. For example, legacy accounts that are locked will be locked after upgrade.
– User credentials are upgraded for legacy password and dynamic token accounts. The credentials for legacy smart card accounts cannot be upgraded, and these accounts are therefore converted during upgrade.
– An Upgrade profile is used to control the upgrade. Via the profile it is possible to:
  » Configure which legacy accounts that shall be preserved during upgrade.
  » Add new user accounts and groups.
  » Specify the System Settings, Group settings, and User Account settings that will be set in the upgraded installation.

**Remote Help**

Upgraded legacy accounts can be used to provide Remote Help, but upgraded legacy accounts that use a fixed password to authenticate must have successfully logged on once before they will be able to provide Remote Help on the upgraded system. Therefore, it is recommended that you always include in the upgrade profile at least one user that is able to provide Remote Help.

**Conversion of Special Legacy Accounts**

During upgrade, legacy TEMPSERVICEUSER users are converted to "service user"-type accounts, see “Full Disk Encryption Service Start Account and the Recovery File” below.

**Smart Card Accounts**

During upgrade, smart card accounts are either removed or converted to temporary smart card accounts/fixed password accounts with a password specified by the upgrade profile. If temporary smart card accounts are used, the users must re-associate the smart card at Windows logon.
**Recovery File**

During the upgrade, a recovery file for the upgraded version is created and stored in the Recovery path. If the creation of this file fails, the upgrade is aborted.

**Full Disk Encryption Service Start Account and the Recovery File**

If a Pointsec PC service start account is configured in the upgrade profile, it will be used to store the recovery file in the Recovery path.

During upgrade, the Pointsec Service Start Service in the 4.x/5.x version of Pointsec PC, and information about the account configured to run the service, will be removed. Consequently the 4.x/5.x version of the Pointsec Service Start Service will not be used for recovery file handling during or after upgrade.

### From Which Legacy Versions Can You Upgrade?

You can upgrade to Full Disk Encryption 7.x from the following legacy versions:

- Pointsec for PC 4.1 sr 2.14 or later
- Pointsec for PC 4.2 sr 1.4 or later
- Pointsec for PC 4.3
- Pointsec for PC 5.x.x

### Requirements for Upgrading a 4.x/5.x Client

The following requirements must be met to upgrade a Pointsec for PC 4.x/5.x client:

- Upgrade from the installed 4.x/5.x version must be supported (see above).
- The 4.x/5.x license serial number is required to start the upgrade.

Select the **Use the serial number of the local installation** checkbox if you are upgrading from 4.x or 5.x and the serial numbers used on the local machine and on the clients are identical. If the serial number used on the local machine is not identical to the serial number used by the clients, ensure that the **Use the serial number of the local installation** checkbox is *not* selected, and then enter the serial number used by the clients in the **Serial number currently used by clients** field. See the description under “Creating the Upgrade Package” on page 151.

- During the upgrade, the user logged on to the client computer must have local administrator privileges.
• Encryption on the client computer to be upgraded must be completed, that is, no encryption may be in progress on that computer.

• The currently logged in user must have access to all protected volumes.

• Upgrade is not supported on computers to which USB hard disk drives or USB flash drives are attached.

• When upgrading a computer that has multiple-disks, all the disks that will be used after the upgrade must be present during the upgrade. A disk that was not present during an upgrade cannot be connected to the computer after the upgrade. In other words, Pointsec PC does not support computers on which different versions of Pointsec PC are installed on different disks.

The Process of Upgrading

The Full Disk Encryption administrator should perform the following operations to upgrade the product on the clients:

1. Install Full Disk Encryption 7.x on a machine; this is referred to as the ‘master installation’.

   The master installation is used to create upgrade profiles and to construct an upgrade package.

2. Create the upgrade profile that will be used for this upgrade.

   Before creating the upgrade profile, the central administrator must do an inventory of the legacy accounts, legacy groups, and the legacy settings that exist on the clients. The information collected in the inventory will enable the central administrator to create an upgrade profile that will upgrade the clients correctly. This inventory must be performed manually.

3. Create the upgrade package via the upgrade wizard, which can be accessed in the FDEMC at Remote → Create 4.x/5.x Upgrade Package.

4. Deploy the upgrade package, if this has not been done via the wizard.

5. Check the progress of the upgrade on the clients by monitoring the central log file directory for the log files from the upgraded clients.

6. Restart the upgrade on the clients on which it has failed.

Most of these steps are explained in detail below.
The Characteristics of an Upgrade Profile

**Settings That Are Specific to Upgrade Profiles**

Upgrade profiles are similar to installation profiles, but they are unique in having the following settings (found under Groups → [Group Name] → Group Settings → Upgrade):

- Choose Upgrade Action.
- Choose How To Convert Upgraded Legacy Smart Card Accounts.
- Set Password for Converted Legacy Smart Card Accounts.
- Limited Volume Access Accounts
- Default Legacy Group

**Note** - Upgrade profiles do not have volume protection settings because the protection is inherited from the legacy installation.
Upgrade Settings

The following Upgrade settings are found under Group Settings:

Table 7-1  Upgrade settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose Upgrade Action</td>
<td>This setting determines how legacy accounts matched by the group/account will be upgraded. The following values can be set for groups and for legacy accounts:</td>
</tr>
<tr>
<td></td>
<td>• Ignore = Legacy account(s) are ignored (handled by default group for authority level)</td>
</tr>
<tr>
<td></td>
<td>• Upgrade = Upgrade legacy account(s) and utilize settings for matching group.</td>
</tr>
<tr>
<td></td>
<td>• Remove = Remove legacy account(s).</td>
</tr>
<tr>
<td>Choose How To Convert Upgraded Legacy Smart Card Accounts</td>
<td>Credentials for legacy smart card accounts cannot be upgraded, so they must be converted during upgrade. This setting determines how to convert these accounts. Note that this parameter has no effect unless the parameter 'Legacy accounts handling' is set to 'Upgrade'.</td>
</tr>
<tr>
<td></td>
<td>• Remove</td>
</tr>
<tr>
<td></td>
<td>• Convert to temporary smart card accounts</td>
</tr>
<tr>
<td></td>
<td>• Convert to fixed password account</td>
</tr>
<tr>
<td>Set Password for Converted Legacy Smart Card Accounts</td>
<td>Set the password for the legacy smart card accounts that, during upgrade, will be converted to temporary smart card accounts or password accounts.</td>
</tr>
<tr>
<td>Limited Volume Access Accounts</td>
<td>Specifies the action that will be taken when accounts without access to all volumes are found.</td>
</tr>
<tr>
<td></td>
<td>• Abort Installation</td>
</tr>
<tr>
<td></td>
<td>• Remove legacy accounts</td>
</tr>
</tbody>
</table>
Default Legacy Groups

In an upgrade profile, a group can be marked as Default Legacy Group for one or several legacy authority levels (Sysadmin, Admin, and User). This is done by right-clicking the group and selecting Default legacy group.

A legacy user is primarily upgraded according to the settings specified for a group (in the upgrade profile) whose name is the same as the legacy group to which the legacy user belongs. If no group name in the profile matches the user’s legacy group name, the user is upgraded according to the settings for a group designated the Default legacy group for the user’s authority level. If no Default legacy group is found, the user is removed.

Legacy Accounts

Legacy accounts are added to profiles for two purposes:
1. To specify a specific upgrade action for an account in a legacy installation.
2. To enable management on user-account level for individual upgraded accounts.
3. You can add legacy accounts to the upgrade profile. But for legacy accounts, you can specify only the legacy user account name, and set the Upgrade Action (and implicitly the group membership).

The Two Types of Upgrade Profile: Silent and Interactive

Upgrade profiles can be either silent or interactive. You choose whether you want to create a silent or an interactive profile in the PCMC’s New Profile wizard. The profile type determines whether the upgrade will be interactive or silent.

Recommendations

The following recommendations apply to upgrade profiles:

- All legacy users can be preserved during upgrade. However, we recommend that legacy users with the authority level User are upgraded and that legacy users with the authority level Admin and Sysadmin are removed and replaced with new user accounts.

With this approach, all information (including credentials) related to the administrative accounts is available in the PCMC. This enables you to create installation/update profiles with the same administrative accounts and thereby unify the configuration of clients with different backgrounds (upgraded from
4.x/5.x or the direct installation of 6.x). Note that an upgrade profile can be based on an installation/update profile and that you thereby can achieve this effect in reverse order.

- The upgrade profile should contain at least one new account with the authority level and permissions required to perform Remote Help for all users.
- The Update Profile Path, Recovery Path, Central Log Path, and Upgrade Path specified in the upgrade profile should be different from those used for the 4.x/5.x versions.
- The parameter **Limited volumes access** should be set to **Abort installation**. If the setting **Remove accounts** is used, the following scenario will result in one or several volumes not being upgraded correctly:
  - A user with access to all volumes is logged on to Full Disk Encryption.
  - Upgrade is performed in the Windows environment, and the computer is restarted.
  - Another user with limited volume access logs into the legacy PPBE.
  - Upgrade is done on all volumes to which that user has access. The other volumes are not accessible and therefore cannot be upgraded.

### Configuring an Upgrade Profile

An upgrade profile can be based on:

- Local settings
- An update profile
- An installation profile

When you create a new upgrade profile that is not based upon local settings or on another profile, the new upgrade profile will contain three groups: Sysadmins, Admins, and Users. Each of these groups has the **Default legacy group** setting for the corresponding legacy authority level. Note that the default groups can be renamed and removed in the same way any other normal group can be.

### Sanity-Check Warnings Related to the Configuration of an Upgrade Profile

In addition to the warnings relevant for installation profiles, the following situations trigger warnings for upgrade profiles:

- No new account has been specified in the upgrade profile.
– No default group exists for one or more of the legacy authority levels.
– The group authority level for the legacy sysadmin default group is lower than the group authority level for legacy admin default group.
– The group authority level for the legacy admin default group is lower than the group authority level for legacy user default group.

**Errors Related to the Configuration of an Upgrade Profile**

In addition to errors relevant for installation profiles, the following situations trigger errors for upgrade profiles:
– The setting, Upgrade Action, has been assigned the value Ignore for a group that is a default group for a legacy authority level.

**Legacy Account Handling**

How legacy accounts are upgraded is determined by the contents of the upgrade profile and by the following four legacy parameters for the account:
– Legacy account name
– Group name
– Authentication method
– Authority level

**Analysis of Legacy Accounts**

During upgrade, the upgrade profile and these parameters are analyzed to determine whether the account will be upgraded or removed.

Remove: The account is removed and will not be present in the upgraded Full Disk Encryption 7.0 installation.

Upgrade: The account is retained during upgrade, and it becomes a member of one of the groups specified in the profile. The account will receive the settings specified for the group in the upgrade profile.

The analysis that attempts to match a legacy account to an user account in the upgraded system is primarily based on the legacy account’s group name and secondarily based upon its authority level.
Upgrade Operations

This section describes how specific upgrade operations can be performed via upgrade profiles.

**Upgrading All Legacy Accounts in a Legacy Group**

To upgrade all the accounts in a legacy group, define the group in the upgrade profile and set the Upgrade Action to Upgrade.

**Removing All Legacy Accounts in a Legacy Group**

To remove all accounts in a legacy group, define the group in the upgrade profile and set the Upgrade Action to Remove.

**Removing All Legacy Accounts**

To remove all legacy accounts, set the Upgrade Action to Remove in all groups. Note that in this case new accounts must be added via the upgrade profile.

**Removing/Upgrading a Specific Legacy Account in a Legacy Group**

Create a legacy account in the upgrade profile with the same name and group as the account and set Upgrade Action to Remove/Upgrade.

**Creating the Upgrade Package**

To create the upgrade package, use the upgrade wizard, which you will find in the FDEMC.

1. Select Remote in the folder tree to the left.
2. Click Create Upgrade Package, and the wizard opens. Then click Next.
The Create Upgrade Package window opens, containing the following information:

Table 7-2  Create Upgrade Package Information

<table>
<thead>
<tr>
<th>Setting</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select directory containing the Pointsec PC installation package</td>
<td>The directory that contains the installation package for version of Pointsec PC to which the clients will be upgraded.</td>
</tr>
<tr>
<td>Use the serial number of the local installation</td>
<td>Select this checkbox when you upgrade from 4.x/5.x and the same serial number is used on the local machine and on the clients. See Serial number currently used by clients, below.</td>
</tr>
<tr>
<td>Serial number currently used by clients</td>
<td>In this text box, enter the 4.x/5.x serial number used by the clients if the serial number used on the local machine is not identical to the serial number used by the clients.</td>
</tr>
<tr>
<td>Algorithm</td>
<td>Select the algorithm, Blowfish/CAST or AES/3DES, that is used by the clients that will be upgraded.</td>
</tr>
<tr>
<td>Upgrade profile</td>
<td>The upgrade profile to be used in the upgrade package.</td>
</tr>
</tbody>
</table>

3. Click the ... button, and browse to the directory that contains the installation package for version of Pointsec PC to which the clients will be upgraded. Select that directory. Some of the files used in the upgrade package are located in the Pointsec PC installation package, that is why it needs to be selected.

4. Select the **Use the serial number of the local installation** checkbox if you are upgrading from 4.x or 5.x and the serial numbers used on the local machine and on the clients are identical. If the serial number used on the local machine is not identical to the serial number used by the clients, ensure that the **Use the serial number of the local installation** checkbox is not selected, and then enter the serial number used by the clients in the **Serial number currently used by clients** field.

5. Select the algorithm, Blowfish/CAST or AES/3DES, that is used by the clients that will be upgraded.

6. Using the ... button, browse to and select the profile to be used in the upgrade package. Then click **Next**.

7. If satisfied with the package information summary, click **Finish**.
The actual package created will be similar in structure to the package shown above.

**Deployment**

The upgrade package is deployed by copying it to the 4.x/5.x Directory path for software upgrades or to the Pointsec/Work folder on the client computers.

**Error Handling and Logging**

All major upgrade actions that are performed and any errors that occur during upgrade are logged in a clear text log file: Upgrade_{computername}.log. During upgrade, this file is stored in the update folder in the Program Files\Pointsec\Pointsec for PC\Update folder. If the upgrade fails, the log file is uploaded to the “Directory for software upgrades” folder (normally a file share). If the upgrade is successful, the log file is stored in Documents and Settings\All Users\Application Data\Pointsec\Pointsec for PC on a Windows XP installation, or in Users\All Users\Pointsec\Pointsec for PC on a Windows Vista installation. This log file contains valuable information for tracing upgrade problems.

**Restarting the Upgrade**

Upgrade can be restarted in two ways. The first solution is the recommended way to restart, while the other way can be considered a fall-back solution when the first solution does not work:

Solution 1:

- Create a new upgrade package via the FDEMC.
- Distribute the upgrade package to the clients’ Software update directory/work folders.
Solution 2:

- Clear the registry values PatchLast and PatchNetLast in key HKEY_LOCAL_MACHINE\SOFTWARE\Pointsec Mobile Tech\Pointsec on the clients.
- Remove the files in C:\Program Files\Pointsec\Update on the clients.
- Distribute the upgrade package to the clients’ Software update directory/work folders.

**Recovery**

Most of the upgrade operations are performed in Windows. However, to finalize the upgrade, the system must be restarted and the user must authenticate once in the legacy PPBE. If the upgrade fails after restart, recovery must be performed on the system. Depending upon the progress of the upgrade process, recovery is performed via a recovery media for the legacy installation or/and the upgraded installation.

If the upgrade fails after restart, and the system becomes inaccessible; perform the following steps:

1. Create recovery media for the legacy version.
2. Create recovery media for the upgraded version (that failed).
3. Attempt recovery using the legacy recovery media on all volumes. Pay close attention to error messages that the recovery program displays. You can, however, ignore the “Simulated boot record differs” error message. This message depends on how the upgrade is carried out, and the problem can be fixed using the recovery media for the upgraded version.
4. Attempt recovery with the recovery media for the upgraded version and perform “Recover all”.
5. Attempt to boot the system.
Upgrading from Pointsec for PC 6.x.x to Full Disk Encryption 7.x

In This Section

- Requirements for Upgrading from 6.x.x to FDE 7.x  page 155
- Upgrading 6.x.x Installations That Have No Encrypted Volumes to FDE 7.x  page 156
- Before Upgrading  page 156
- Performing the Upgrade by Running the Msiexec.exe  page 158
- Performing the Upgrade Using Upgrade Path(s)  page 159
- Automatic Reboot After Upgrade?  page 159
- Manual Reboot After Upgrade  page 159

This chapter describes how to upgrade Pointsec for PC 6.x.x installations to Full Disk Encryption 7.x (FDE 7.x).

You can upgrade from Pointsec for PC 6.x.x to Full Disk Encryption 7.x by:

- Running Msiexec.exe, see “Performing the Upgrade by Running the Msiexec.exe” on page 158. You must use this method if you are upgrading from a Pointsec for PC version that is earlier than 6.2.
- Using upgrade path(s), see “Performing the Upgrade Using Upgrade Path(s)” on page 159. You can use Upgrade for Path(s) only if you are upgrading to Pointsec PC 6.3.1 from Pointsec PC 6.2 or a later version.

Prior to upgrading, you can, if you wish, change the graphic images displayed in preboot, see “Changing the Graphic Images Displayed in Preboot” on page 157.

Requirements for Upgrading from 6.x.x to FDE 7.x

The following requirements must be met to upgrade a Pointsec for PC 6.x.x client to Full Disk Encryption 7.x:

- Encryption on the client computer to be upgraded must be completed, that is, no encryption may be in progress on that computer.
- Upgrade is not supported on computers to which USB hard disk drives or USB flash drives are attached.
When upgrading a computer that has multiple-disks, all the disks that will be used after the upgrade must be present during the upgrade. A disk that was not present during an upgrade cannot be connected to the computer after the upgrade. In other words, FDE 7.x does not support computers on which different versions of Pointsec PC are installed on different disks.

Upgrading 6.x.x Installations That Have No Encrypted Volumes to FDE 7.x

Dynamic Volume Encryption (described under “Install Settings” in Chapter 3, “System Settings” on page 23) will not function on Pointsec PC 6.x.x installations with no encrypted volumes that are upgraded to Full Disk Encryption 7.x. If you attempt to enable Dynamic Volume Encryption when upgrading such installations, FDE will generate an error message (if Dynamic Volume Encryption is selected in the local settings) or an error log event (if Dynamic Volume Encryption is selected in a profile). The error log event ID is 3104; its text is: “An attempt to enable dynamic encryption was made on an unsupported system. Consult the Admin Guide for more information. The setting was reverted.”

Before Upgrading

Permissions Required to Run Upgrade

Upgrading requires the permissions needed to install msi packages on the local machine. By default, the Pointsec for PC.msi program installs the upgrade using the Local System account, which has the required permissions.

When To Deploy Upgrades to Vista Clients

Because the FDE upgrade on Vista is completely silent, we recommend that you deploy the upgrade either during the night or the early morning hours to minimize the risk of an end user rebooting his/her Vista system during the upgrade. This applies to upgrades initiated from the Upgrade path or the Work folder. When an upgrade is initiated via the command line, you specify whether or not the upgrade is silent. If you do a silent update from the command line, you should of course heed the recommendation above.

Rebooting during the upgrade can lead to a severe system failure that can require performing a full recovery of the system.
Changing the Graphic Images Displayed in Preboot

Before you perform the upgrade, you can change the following from the Full Disk Encryption graphic image to, for example, your company’s logo:

- Banner displayed in preboot
- Background image displayed in preboot
- Preboot screen saver image

To change the graphics displayed in preboot authentication:

1. Create a folder named `oemvar` in the folder that contains the `Pointsec for PC.msi` file:

Figure 7-2

2. Add the relevant files (described below) to the `oemvar` folder. During upgrade, the files that have been added to this folder will be registered as the files to be displayed during preboot.

Table 7-3  Files to add to `oemvar` folder

<table>
<thead>
<tr>
<th>Filename</th>
<th>Description</th>
<th>Specifications width * height</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banner.bmp</td>
<td>Banner displayed during installation, except for the InstallShield progress dialog.</td>
<td>499 * 59, 256 colors</td>
</tr>
<tr>
<td>Banner.jpg</td>
<td>Banner displayed in preboot. Jpeg images created with Photoshop 3.0 cannot be used.</td>
<td>447 * 98</td>
</tr>
<tr>
<td>Desktop.jpg</td>
<td>Background image displayed in preboot. Jpeg images created with Photoshop 3.0 cannot be used.</td>
<td>800 * 600</td>
</tr>
</tbody>
</table>
Performing the Upgrade by Running the Msiexec.exe

<table>
<thead>
<tr>
<th>Filename</th>
<th>Description</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scrsvr.jpg</td>
<td>Preboot screen saver image. Jpeg images created with Photoshop 3.0 cannot be used.</td>
<td>260 * 128</td>
</tr>
<tr>
<td>Ssbg.bmp</td>
<td>Windows screen saver background image.</td>
<td>1280 * 1024</td>
</tr>
<tr>
<td>Lic_oem.rtf</td>
<td>License text displayed in installation.</td>
<td>This is a rich text file.</td>
</tr>
</tbody>
</table>

3. Perform the relevant upgrade procedure as described in “Performing the Upgrade by Running the Msiexec.exe” on page 158.

Performing the Upgrade by Running the Msiexec.exe

You can upgrade from Pointsec for PC 6.x.x to FDE 7.x by running the Msiexec.exe, manually as described below.

**Note** - You must use this method (running the Msiexec.exe manually) if your are upgrading from a 6.x.x version that is prior to 6.2.

**Note** - Do not use copy and paste to enter the text shown in the following instructions into the command prompt because this can alter the double quotes, which will cause the command to fail.

Upgrading with a Manual Reboot

1. Execute Msiexec.exe as follows:

   Msiexec.exe /i "PATH_TO_MSI\Pointsec for PC.msi" REINSTALLMODE=vomus REINSTALL=ALL REBOOT=ReallySuppress /q

2. When the upgrade log shows the entry Upgrade Done, reboot the machine.

Upgrading with an Automatic Reboot

Execute Msiexec.exe as follows:

Msiexec.exe /i "PATH_TO_MSI\Pointsec for PC.msi" REINSTALLMODE=vomus REINSTALL=ALL /q
Performing the Upgrade Using Upgrade Path(s)

You can upgrade from Pointsec PC 6.2 (or a later version) to FDE 7.x by placing the Pointsec for PC.msi and the Modules folder the Upgrade path specified in the Set Upgrade Path(s) setting. See the description of the setting under “Install Settings” on page 35.

Note - When a Windows XP installation is upgraded via upgrade path(s), a progress bar indicates how much of the upgrade has been completed. End users should reboot their client machines as soon as possible after the completion of the upgrade.

When a Windows Vista installation is upgraded via upgrade path(s), no progress bar is displayed. Therefore, the administrator must inform end users when to reboot their client machines after the completion of the upgrade.

Automatic Reboot After Upgrade?

It is possible to set up an automatic reboot after the upgrade’s silent installation. Note, however, that this might come as an unpleasant surprise to end users currently working on these machines if they are not aware that their machines will reboot without warning.

If you wish to upgrade without automatic reboot, see the instructions below.

Manual Reboot After Upgrade

During the upgrade, the following upgrade log is maintained:

For a Windows XP installation:
C:\Documents and Settings\All Users\Application Data\Pointsec\Pointsec for PC\Upgrade.log

For a Windows Vista installation:
C:\Users\All Users\Pointsec\Pointsec for PC\Upgrade.log
When a silent installation has completed successfully, an **Upgrade Done** entry is written to the upgrade log. When you see this entry in the log, the machine can be rebooted.

By default, all users have full permissions to the directory that contains the upgrade log. If you experience problems writing or accessing the log, check with your administrator to determine whether the default permissions have been changed.

**Smart Card Drivers Are Updated**

When an upgrade is performed, the smart card and smart card reader *.inf* files in the new installation are registered. The old entries are retained unless they are replaced by new entries in the new *.inf* files. Then, the installed driver files are upgraded, but only if the checksums match those that were updated while the drivers were being registered.

**The Update Validation Password Must Be Reentered After Upgrade**

The security of the update validation password has been enhanced, and because of this it has a new internal format. This requires that you re-enter the update validation password *that was used in the version from which you have just upgraded* after upgrading to Pointsec PC 6.2.0 Hotfix Accumulator 1 (HFA1) or later. When you start the PCMC immediately after upgrading, you will be prompted to set the update validation password. *You must specify the update validation password that was used in the version from which you have just upgraded* because this is the password that the other machines you want to upgrade use to validate profiles. Otherwise, no profiles will be accepted on those machines. After entering this update validation password in the PCMC, you should immediately publish an update profile that contains this password (in its new format).
Chapter 8

Full Disk Encryption Logging Functionality

In This Chapter

The Local Event Database  page 162
The Local Log File  page 162
The Central Log Files  page 163
Manually Transferring the Local Log File to the Central Log File  page 164
Timestamps and the Windows Event Log  page 165
Exporting Logs  page 165
Viewing a Local Log File  page 165

Full Disk Encryption can create and store event logs in a central log file that can be made available to a central management point of access. Full Disk Encryption also maintains local log files on each Full Disk Encryption-protected machine.

Note - Ensure that you use a reliable time source to set clients' internal clocks so that the audit trail from multiple clients, will contain synchronized time stamps.

Full Disk Encryption events are logged in one or more of the following:

- Local event database
- Local log file
The Local Event Database

- Central log file(s)
- Windows Event Log (if enabled)

The Local Event Database

Full Disk Encryption logs information about events such as login attempts, status of encryption, and the time of each update to the configuration. This information is saved as log events in the local event database. These log events comprise an audit trail of Full Disk Encryption activities on the local computer.

Full Disk Encryption stores up to 255 events in the local event database. This information is scrambled and cannot be viewed in a text editor. It can, however, be viewed immediately after preboot authentication by clicking Show Log in the Logon Successful window, and in the management console under Local by clicking View Local Event Database.

The contents of the local event database can also be viewed by clicking View Local Event Database under Local in the FDEMC.

The Local Log File

The contents of the local event database are transferred to the local log file by the PC tray application (CPTray.exe) each time a user logs on to Windows.

The logs are encrypted and integrity protected when stored.

The local log file (Windows XP) is stored locally in the directory C:\Documents and Settings\All Users\Application Data\Pointsec\Pointsec for PC. Note that the Application Data\Pointsec\Pointsec for PC directories are hidden.

The local log file (Windows Vista) is stored locally in the directory C:\Users\All Users\Pointsec\Pointsec for PC.

The local log filename is composed of the computer name and the file extension .log. For example, if the computer name is DEV-PC.024, the local log file on this computer will be DEV-PC.024.log.

The following events are logged directly to the local log file and are therefore never found in the internal log database:
The Central Log Files

The central log files enable the administrator to monitor the clients. The central log files are stored in a specified log path folder to which local log files are copied. The central log file is located in the directory specified in Local → System Settings → Install → Set Central Log Path.

If the central log path has been specified, the Full Disk Encryption tray application (CPTray.exe) transfers the local log file to the directory in that path each time one of the following happens:

- A user logs on to Windows
  The tray application calls the CentralLog.exe program, which copies the local log file to the specified directory.

- The CentralLog.exe program is executed
  Each time the CentralLog.exe program executes, it first transfers all new log events from the local log database (which contains a maximum of 255 events) to the local log file. Then it transfers all new log events in the local log file to the central log file, and simultaneously to the Windows Event Log.

The interval for log transfers can be set in the UpdateInterval registry value. See the table below for default values.

---

- 101
  Account status

- 1010
  Configuration setting changed

- 1100
  Profile setting changed

Thus, these events cannot be viewed immediately after preboot authentication or by clicking View Local Log under Local in the FDEM.
Manually Transferring the Local Log File to the Central Log File

To run the CentralLog.exe program manually:

1. Do one of the following:
   - Run `CentralLog.exe` and transfer the local log file to the central log file.
   - Run `CentralLog.exe /dump`, copy the user account status information to the local log file, and then transfer the local log file (which now contains the user account status) to the central log file.

The manual execution can be customized using the registry values described above. When you run the CentralLog.exe program manually, you might need to run it more than once depending on how much data is to be transferred from the local log file.

---

### Table 8-1 Registry settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UpdateInterval</strong></td>
<td>Time interval in minutes between each transfer. Default = 180.</td>
</tr>
<tr>
<td><strong>ExtendedLogging</strong></td>
<td>1 = Account status events will be included in the data transferred in each execution of the program (Corresponds to CentralLog.exe /dump). Default = 0. 0 = No account status events will be included in the data transferred in each execution of the program. This is the default.</td>
</tr>
<tr>
<td><strong>LogTransfer</strong></td>
<td>1 = Events will also be transferred to the Windows Event Log. This is the default. 0 = Events will not be transferred to the Windows Event Log. Default = 1.</td>
</tr>
</tbody>
</table>
Timestamps and the Windows Event Log

Note that the date and timestamp of an event viewed in the Windows Event Viewer might differ from the date and timestamp of that event in the local log file. This is possible because events are reported to the Full Disk Encryption logs and to the Windows Event Viewer via different independent interfaces. Events logged in preboot are not replicated in the Windows Event Log until the next Windows session, while events logged while operating in Windows are written directly to the Windows Event Log and thus can have an earlier time than that of corresponding events in the local log file.

Exporting Logs

For information on exporting logs, see Appendix G, “The pslogexp.exe Log Export Utility”.

Note - To view the central log file, you must have system administrator privileges.

Viewing a Local Log File

To view local Full Disk Encryption log files:

1. Start the Full Disk Encryption Management Console (FDEMC) and select Local in the folder tree.
2. Click View Local Log Database.
   The local log is displayed.

   In the Filter for Description Text field, you can specify the criteria that will determine which events are displayed.

   You can make various selections and review additional events that Full Disk Encryption has logged. All log information is always available; these selections merely filter what you choose to display or print. Double click an item in the Log Viewer to display the log entry details for that item. The properties listed under Log Entry Details are:
   • Timestamp
Viewing a Local Log File

- Level
- ID
- Parameter 1
- Parameter 2
- Parameter 3
- Parameter 4.
Remote Help

In This Chapter

Implementing a Remote Help Procedure  page 167
Remote Help Settings  page 168
Types of Remote Help  page 168
Verifying Users  page 169
Providing Remote Help for Full Disk Encryption  page 169
Providing Remote Help Using the Full Disk Encryption Management Console  page 169

Users may be denied access to their Full Disk Encryption-protected workstations for a number of reasons. For example, they might have entered an incorrect password too many times or forgotten their password or, in a worst case scenario, a hacker may have tried to break into their workstation.

Full Disk Encryption Remote Help is designed to assist users in these types of situations. All a user has to do is call his/her designated Remote Help administrator and follow the Remote Help procedure.

Implementing a Remote Help Procedure

Companies and organizations implement Remote Help procedures to suit their individual needs and resources. One method of implementing Remote Help is as follows:
Remote Help Settings

- Create designated administrator account(s) for Remote Help. The number of accounts you should create depends on your organization.

Note - Administrators who use smart cards for authentication cannot provide Remote Help as smart cards require physical access to the workstation.

- Once you have created the accounts, assign them to the people who will run the Remote Help procedure.

- Inform users who they should call when they need Remote Help.

- For Remote Help to function, both the user account of the Remote-Help provider and of the Remote-Help recipient must exist on the computer.

- The Remote-Help provider’s group authority level must be equal to or higher than the group authority level of the Remote-Help recipient.

Remote Help Settings

The Remote Help settings are described in “Remote Help Settings” on page 83.

Types of Remote Help

Full Disk Encryption provides two types of Remote Help for users who are denied access to their workstations:

- Remote Password Change
  For users who use fixed passwords and have forgotten them. This type of Remote Help is of no use to users who use either a dynamic token or smart card/USB token for authentication.

- One-Time Logon
  For users who have forgotten or lost their dynamic tokens or smart card/USB tokens.

Note - When Remote Help is used to authenticate a Full Disk Encryption user account that uses single sign-on (SSO), the recorded SSO credentials for that user account are invalidated. This is to prevent Remote Help administrators from leveraging SSO to ‘impersonate’ a user.
Verifying Users

Before you provide Remote Help to a user, you must be sure that the user is actually authorized to access the workstation. You can do this in a number of ways, for example:

- **Use predetermined questions and answers that only legitimate users know**
  Keep a list of sample questions to ask, such as the user’s name and favorite color, wife’s maiden name, brand of car, etc. Some of the questions could have randomized, fixed answers; for example, when asked about his/her favorite pet, the user could answer clouds instead of cat.
  Store the questions and answers in a separate database that is accessible to all Remote Help administrators.

- **Use voice verification software**
  Use security software to extract unique vocal characteristics of the caller and compare them with the Full Disk Encryption user’s reference voiceprint.

Providing Remote Help for Full Disk Encryption

The following sections describe how to access the Remote Help screen and how to help users change fixed passwords and give one-time access to workstations.

Providing Remote Help Using the Full Disk Encryption Management Console

To provide Remote Help:

1. Verify the user who needs Remote Help is legitimate. See “Verifying Users” on page 169 for details.

2. Using an account with Remote Help privileges, start the Full Disk Encryption Management Console and open the Remote Help screen.
3. Enter the following information:

<table>
<thead>
<tr>
<th>Field/option</th>
<th>Information/action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type of end-user assistance to be provided</strong></td>
<td>Select the type of Remote Help the user needs: For a fixed password, select: <strong>Password</strong>; for a dynamic token, select: <strong>Dynamic Token</strong>. Helper authentication using smart cards/USB tokens is not supported.</td>
</tr>
<tr>
<td><strong>End-User Account Name</strong></td>
<td>Enter the name of the end-user account.</td>
</tr>
<tr>
<td><strong>Helper Account Name</strong></td>
<td>Enter the name of the account you are using to provide Remote Help.</td>
</tr>
<tr>
<td><strong>Generate Response One to end user</strong></td>
<td>1. Click <strong>Generate</strong> to generate Response One.</td>
</tr>
<tr>
<td></td>
<td>2. Read Response One to the user who enters it in the Response field.</td>
</tr>
<tr>
<td></td>
<td>3. Tell the user to press the TAB key to generate a challenge.</td>
</tr>
</tbody>
</table>
Note - The checkbox **Case sensitive helper account password** has been added to the Remote Help screen. This checkbox must be checked if the Remote Help provider’s password is case sensitive and cleared if the password is not case sensitive.

The user will now be forced to set a new password or will be given one-time access to the workstation, depending on the type of Remote Help you have provided.

<table>
<thead>
<tr>
<th>Field/option</th>
<th>Information/action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type of helper authentication</strong></td>
<td>Select the type of authentication used by the account you are using to provide Remote Help: For a fixed password, select: <strong>Password</strong>; for a dynamic token, select: <strong>Dynamic Token</strong>. Helper authentication using smart cards/USB tokens is not supported.</td>
</tr>
<tr>
<td><strong>Response One</strong></td>
<td>This is the first response you read to the user.</td>
</tr>
<tr>
<td><strong>Challenge from end user</strong></td>
<td>Enter the challenge the user receives from Full Disk Encryption after entering Response One and pressing the <strong>TAB</strong> key.</td>
</tr>
<tr>
<td><strong>Helper Password</strong></td>
<td>Enter the fixed password or dynamically generated password for the account you are using to provide Remote Help.</td>
</tr>
</tbody>
</table>
| **Generate Response Two to end user** | 1. Click **Generate** to generate Response Two.  
2. Read Response Two to the user who enters it in the Response field.  
3. Tell the user to click **OK**. |
| **Response Two**              | This is the second response you read to the user.                                  |
Chapter 10

Removing Full Disk Encryption

In This Chapter

- Uninstalling FDE Using FDE Management Console  page 174
- Uninstalling FDE Using Windows Add/Remove Programs  page 175
- Uninstalling FDE Using Recovery Media  page 176

You can remove Full Disk Encryption by:

- Creating and deploying an uninstall profile, which allows for easy removal from many computers; see “Uninstall Profiles” on page 174
- Using Add/Remove Programs; see “Uninstalling FDE Using Windows Add/Remove Programs” on page 175
- Allowing a user to remove Full Disk Encryption and decrypt their computer using a recovery medium and Remote Help; see “Uninstalling FDE Using Recovery Media” on page 176.
Uninstalling FDE Using FDE Management Console

Uninstall Profiles

An uninstall profile enables you to remotely remove Full Disk Encryption from multiple machines within your organization without having to visit each machine.

You can use an uninstall profile in a variety of scenarios, for example:

- an employee is no longer with the company
- the operating system on a machine needs to be changed from Windows XP to Windows Vista
- an employee is traveling to a country where strong disk encryption is illegal

An uninstall profile cannot be edited, and requires authentication by two administrator user accounts before it can be created.

The machine on which you create the uninstallation profile must contain at least two system administrator accounts that are also on the clients you want to uninstall. To complete the creation of the uninstall profile, Full Disk Encryption prompts for the authentication of two system administrators before the profile is created (these two system administrator accounts must also exist on the client).

The following sections explain how to create and deploy an uninstall profile.

Creating an Uninstall Profile

To create an uninstall profile:

1. Open FDEMC and click the Remote button.
2. Click New Profile to launch the profile wizard, click Next and select the relevant set, and click Next.
3. Select the Uninstall profile type, click Next and enter the profile name. Click Next and then Finish.
4. Enter the user account name and password of the first user account that is authorized to uninstall Full Disk Encryption and click OK.
5. Enter the user account name and password of the second user account that is authorized to uninstall Full Disk Encryption and click OK.
The uninstallation profile is now available under \texttt{Full Disk Encryption \rightarrow Remote \rightarrow \{Your Set\} \rightarrow Profiles}.

\textit{Deploying an Uninstall Profile}

\begin{itemize}
  \item \textbf{Note} - If you want to deploy an uninstall profile directly after installing Full Disk Encryption, check first that the installation and encryption process is complete. An uninstall profile can only be deployed when Full Disk Encryption is fully installed on the computer.
  \begin{itemize}
    \item The logged-on user account on the computer from which you want to remove Full Disk Encryption must have read and execute permissions to the \texttt{Publish} directory.
    \item The logged-on account must also have access to all volumes on the computer in order to remove Full Disk Encryption.
  \end{itemize}
\end{itemize}

Once you have configured the uninstall profile, you are ready to deploy it.

\textbf{To deploy an uninstall profile:}

1. Simply move the uninstall profile from wherever it is stored to the \texttt{Publish} directory you have specified.

\begin{itemize}
  \item \textbf{Note} - When the PC has finished the decryption process, it will no longer be protected.
\end{itemize}

\section*{Uninstalling FDE Using Windows Add/Remove Programs}

You can use Windows Add/Remove Programs to remove Full Disk Encryption.

When Windows Add/Remove is used, one Full Disk Encryption administrator or system administrator and one Full Disk Encryption user (who could also be an administrator), both with the right to remove Full Disk Encryption, must be authenticated before the removal process can start. This ensures that users cannot remove Full Disk Encryption.

\textbf{To remove Full Disk Encryption using the Windows Add/Remove Program:}

1. On the Windows \texttt{Add/Remove Programs} menu, select \texttt{Full Disk Encryption} and click \texttt{Add/Remove}. 
2. Click **Yes** to confirm that you want to remove Full Disk Encryption. Enter the user account name and password of the first user account that is authorized to uninstall Full Disk Encryption and click **Next**.

3. Enter the user account name and password of the second user account that is authorized to uninstall Full Disk Encryption.

4. Click **Next**. A dialog box opens, displaying the volumes protected by Full Disk Encryption.

5. Select a volume from which you want to remove Full Disk Encryption and click the > button to move it to the **Volumes to Uninstall** dialog box. Repeat this procedure until the required volumes are in the list for uninstallation.

6. Click **Next**.

   **Note** - Select all volumes to decrypt. Leaving one volume encrypted might leave some information inaccessible. Also, if any volumes are to be left encrypted, the volume containing the operating system must also remain encrypted.

7. When the message stating that the computer must be restarted for the process to be completed is displayed, click **OK**.

   When the computer has restarted and logon is successful, background decryption will start in Windows. When this is completed and the computer has been restarted, boot protection and management console will be removed.

---

**Uninstalling FDE Using Recovery Media**

If a client has become corrupt and it is not possible to retrieve the encrypted information it might be necessary to uninstall Full Disk Encryption. This can be done by booting the client from a recovery media, decrypting the client and then removing Full Disk Encryption by using Windows Add/remove programs.

**Follow these steps to uninstall Full Disk Encryption**

1. Boot from a recovery medium as described in chapter “Recovering Information”, section “Recovering Information” on page 188.

2. Perform a remote help procedure as described in chapter “Remote Help” on page 167 to allow the information on the client to be decrypted.

3. Remove Full Disk Encryption as described in section “Uninstalling FDE Using Windows Add/Remove Programs” on page 175 in this chapter.
Back up Critical Data

This chapter describes the shared folders and/or file shares that should be backed up regularly to ensure the integrity of your Full Disk Encryption EW installations. The directories to be backed up contain profiles, log files, and recovery files; and they are described below. The path(s) to these directories can be paths to shared folders or to https:// or http:// shares.

Backups are designed to protect the data in these folders/shares so it is not lost and so it can be recovered in the event of an equipment or software failure, inadvertent or intentional destruction of data, or a disaster. The frequency of the backups will depend on, among other things, the specific requirements of the installation, how dynamic it is, etc.

Note that the loss of the folders/shares will not prevent the FDE clients from operating properly. Backups ensure that profiles, logs, and recovery files are always recoverable, if necessary.

Profiles

Full Disk Encryption profiles contain user account and group information and the settings which control the end-user clients. Update profiles are placed in shared folders or file shares for deployment, specifically, in the directories specified in Local → System Settings → Install → Set Update Profile Path(s). Similarly, upgrade profiles are placed in shared folders or file shares for deployment, specifically, in the directories specified in Local → System Settings → Install → Set Upgrade Path(s).
Log Files

The central log files enable the administrator to monitor the clients. The central log files are stored in the directory specified in Local → System Settings → Install → Set Central Log Path.

Recovery Files

Recovery files contain information required to decrypt the Full Disk Encryption-protected computer. Full Disk Encryption transfers the recovery file from the local directory to the directory specified in the FDEM under Local → Edit Settings → Full Disk Encryption → System Settings → Install → Set Recovery Path.
Recovering Information

In This Chapter:

- Introduction .................................................. page 179
- Permissions ..................................................... page 180
- The Full Disk Encryption Recovery File .................. page 181
- Storage ............................................................ page 181
- When the Recovery File is Updated and Written to the Share .................................................. page 181
- If the Recovery File Path Is Not Found .................. page 182
- Recovery and the Full Disk Encryption Version on the Client .................................................. page 183
- Creating a Recovery CD-ROM ............................. page 187
- Recovering Information ...................................... page 188
- Recovering from Alternative Media ...................... page 188
- Using Slave Drive Functionality to Recover Information .................................................. page 189

Introduction

This chapter explains how to use the management console to review, repair, and recover information protected by Full Disk Encryption.

A common scenario in which recovery is required is when something fails in a computer that is protected by Full Disk Encryption and the user cannot start Windows. To remedy this problem, the administrator creates a bootable media on
another computer, using the recovery file of the failed computer. The administrator, or whoever is performing the recovery, then uses the bootable media to recover the faulty computer.

The bootable media:
- Enables the administrator to recover data on the faulty computer.
- Decrypts the faulty computer’s encrypted volumes.
- Removes the preboot authentication from the faulty computer.
- Gives direct access to Windows on the faulty computer once decrypting has completed successfully.

The administrator can then access the files etc. on the faulty computer and uninstall Full Disk Encryption.

Permissions

Performing Recovery

The user account of the person performing recovery must:
- Exist in the recovery file used for recovery (which means that user account must exist on the machine that needs to be recovered).
- Have uninstall permission; this is set in Groups → System → Group Settings → Permissions → Uninstall.

Creating Recovery Media (Running UseRec.exe)

To be able to create recovery media under Windows Vista you must have administrator permissions.

This can be done by executing UseRec.exe with the Run as Administrator option (assuming User Account Control is active).

To run the UseRec.exe with administrator permission:

1. Run UseRec.exe from the Start menu: All Programs → Check Point → Endpoint Security → Check Point Endpoint Security → Create Recovery Disk.
2. Right-click Create Recovery Disk, select “Run as...”, and there select to run as Administrator.
Storage

Full Disk Encryption stores the recovery file locally in the following directory:

- **Windows XP:**
  
  C:\Documents and Settings\All Users\Application Data\Pointsec for PC

- **Windows Vista:**
  
  C:\Users\All Users\Pointsec\Pointsec for PC

By default, all users have full permissions to this directory. If you experience problems writing or accessing the recovery file, ensure that the default permissions have not been changed.

Full Disk Encryption transfers the recovery file from the local directory to the directory specified in the FDEMC under Local → Edit Settings → Full Disk Encryption → System Settings → Install → Set Recovery Path.

The number of recovery (.rec) files found in the Recovery directory should correspond to the number of seats deployed. If there are 25 seats deployed, there should be 25 recovery files in the Recovery directory. Each file is identified with the client machine name in the file name, for example:

my_computer_1.rec, my_computer_2.rec, my_computer_3.rec and so on.

When the Recovery File is Updated and Written to the Share

**The First Recovery File**

The first recovery file is first written to the share immediately after the first reboot of the computer after installation of Full Disk Encryption.

**When Does Full Disk Encryption Update the Recovery File**

A number of things can trigger the update of the recovery file, for example, the addition of an administrator account that has uninstall permission, or a change to a recovery path.
The recovery file is ‘updated’ by Full Disk Encryption writing and distributing a new recovery file.

**Update Triggered by Update Profile**

If information related to recovery of the computer is changed via an update profile, a new recovery file that contains the new information is written immediately to the local directory and to the directories that were specified in the FDEM under Local → Edit Settings → Full Disk Encryption → System Settings → Install → Set Recovery Path(s).

**Update Triggered Locally by a Change in PPBE**

If information related to recovery of the computer is changed in the Full Disk Encryption Preboot Environment (FDEPBE), a new recovery file that contains the new information is written immediately to the local directory and to the directories that were specified in the FDEM under Local → Edit Settings → Full Disk Encryption → System Settings → Install → Set Recovery Path(s).

**Update Triggered Locally by a Change in the FDEM or Tray**

If information related to recovery of the computer is changed in the FDEM or tray, a new recovery file that contains the new information is written to the local directory and to the directories that were specified in the FDEM under Local → Edit Settings → Full Disk Encryption → System Settings → Install → Set Recovery Path(s). But the writing of the new file is done within the time specified in the UpdateInterval precheck value, whose default is 30 minutes. Thus, if the default value is active, it can take up to 30 minutes before a new recovery file is written after the recovery-related information has been changed via the FDEM or the tray.

**If the Recovery File Path Is Not Found**

If no valid recovery path can be found when Full Disk Encryption is trying to write to the recovery file, the following error message will be displayed:

“The path to the recovery file is not accessible. This is OK if you are working offline and it will reset when connected to your regular network. Otherwise, please contact your administrator or technical support for more information.”

Note that even though the default is to not display this message, if no recovery path is found, an entry to this effect will be written to the local and central logs.
If you receive this message, encryption will not start until Full Disk Encryption has ascertained that it will be possible to carry out a recovery later. Until then, the PC will be left unprotected.

Recovery and the Full Disk Encryption Version on the Client

In most cases, the administrator (or other user account performing recovery) has the same version of Full Disk Encryption as the version installed on the client to be recovered. When this is the case, recovery can be performed as described below.

Otherwise, when creating recovery media, for example when performing ‘stand-alone’ recovery, ensure that you use the Volume Recovery Utility for the version of Full Disk Encryption that is installed on the client you want to recover. The current version of this utility is available in the 1 Pointsec for PC\Tools\Reco_img directory on the installation CD-ROM.

Creating a Recovery Disk from the FDEMC

Using the Recovery Utility, you can create a recovery disk containing recovery, review, and repair options on a floppy disk or removable medium.

**Note** - The removable media option is only available if the Recovery Utility detects that supported removable media is available on the system.

**Note** - If you must perform a forced removal of Full Disk Encryption before encryption has started, create a generic recovery floppy disk by executing reco_img.exe, which is in the Tools directory.
Creating a Recovery Disk from the FDEMCA

To create a recovery disk:

1. On the Full Disk Encryption system administrator’s workstation, in FDEMCA, click Remote.
2. Under Recovery, click Create Recovery Media.

Figure 12-1

Note - In Vista, you will not be able to open the recovery file from which you create recovery media if the Recovery Path specified in the set is specified as a mapped network drive, and you are trying to create the media from the FDEMCA. The Recovery Path should be specified in UNC format: \<server>\<share>\.... Alternatively, execute Create Recovery Media from the Start menu: All Programs → Check Point → Endpoint Security → Check Point Endpoint Security → Create Recovery Disk.

To create a recovery disk:

1. On the Full Disk Encryption system administrator’s workstation, in FDEMCA, click Remote.
2. Under Recovery, click Create Recovery Media.

Figure 12-1

Note - In Vista, you will not be able to open the recovery file from which you create recovery media if the Recovery Path specified in the set is specified as a mapped network drive, and you are trying to create the media from the FDEMCA. The Recovery Path should be specified in UNC format: \<server>\<share>\.... Alternatively, execute Create Recovery Media from the Start menu: All Programs → Check Point → Endpoint Security → Check Point Endpoint Security → Create Recovery Disk.
The Recovery wizard opens. Click Next.

Figure 12-2

3. Choose one of the following:
   a. Find recovery file via a configuration set
      Then follow the instructions in the wizard.
   b. Browse file system for recovery file
      Then browse to your recovery file (see Chapter 6, “Root Directory Path” on page 113).

Click Next.

Figure 12-3

4. Select the set that contains the recovery file from Available Configuration Sets, and click Next:
5. Select the recovery file from Available Recovery Files, and click Next:

Figure 12-5

6. Click Finish to launch the recovery tool for the recovery file displayed in the Finish Recovery Wizard:

Figure 12-6
Creating a Recovery CD-ROM

If a computer can only boot from a CD-ROM, you can write its recovery disk to a CD-ROM using standard CD burning software.

**Note** - Whatever medium you choose for the recovery disk, it must be properly formatted. Any information previously saved on the medium will be destroyed.

It is also possible to use a recovery disk from a floppy or removable medium to create a CD-ROM containing many recovery and repair options. For details, see “Creating a Recovery CD-ROM” on page 187.

**Creating a Recovery CD-ROM**

If a computer can only boot from a CD-ROM, you can write its recovery disk to a CD-ROM using standard CD burning software.

**Note** - When running the recovery program any changes you make to settings, for example language and keyboard settings, will not be saved on the CD-ROM.

**To create a recovery CD-ROM:**

1. For the workstation that needs recovery or repair, create a recovery disk on a floppy disk or removable medium. See “Creating a Recovery Disk from the FDEMC” on page 183 for instructions.

2. Using CD burning software, create a bootable CD-ROM based on the recovery disk. Refer to your CD burning software's documentation for information on creating a bootable CD-ROM.

3. Ensure that the workstation is configured to boot from the CD drive. Insert the CD-ROM and reboot the workstation to access the recovery and repair information on the CD-ROM.

**Note** - CD-ROMs containing recovery information must be handled securely. Create them only when required and ensure that they are securely destroyed when no longer needed.
Recovering Information

Occasionally you might need to recover information that is stored encrypted. This requires authentication similar to that required in normal pre-boot.

**Note** - When using a USB device to store the recovery disk, the USB device may be recognized as the first physical device. If this happens, the recovery program will consider the device to be the first hard disk and display the encrypted volumes (in the PVR file) as non-encrypted.

To work around this, use option 8 in the **Recovery** menu to choose the correct physical device.

**Note** - Floppy disks and other removable media containing recovery information must be handled securely. Only create them when required and ensure that they are securely destroyed when no longer needed.

Recovering from Alternative Media

Using Full Disk Encryption's alternative boot media menu, you can boot from media other than floppy disks. This is useful if, for example, the PC you are working on does not have a floppy disk drive.

**Accessing the Alternative Boot Media Menu**

The options displayed in the alternative boot menu depend on what the BIOS of the machine supports and the hardware that is currently installed. Therefore, the fact that an option is listed does not mean it is supported by Full Disk Encryption.

To access the alternative boot media menu:

1. When the PC reboots and the **User Identification** dialog box is displayed, press **CTRL + F10**.
2. Enter your user account name and password, and press Enter. Full Disk Encryption displays the Alternative Boot Menu. This menu is dynamic, that is, some or all of the following options, or other options, are displayed depending on the BIOS and hardware of your PC:

<table>
<thead>
<tr>
<th>Option</th>
<th>Boot using:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Floppy</td>
<td>Standard floppy.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> - This option is always displayed, even if no floppy disk drive is available.</td>
</tr>
<tr>
<td>Hard drive</td>
<td>Internal hard drive.</td>
</tr>
<tr>
<td>CD/DVD-ROM</td>
<td>CD/DVD-ROM.</td>
</tr>
<tr>
<td>USB</td>
<td>USB.</td>
</tr>
<tr>
<td>[network adaptor]</td>
<td>Network adaptor, which can launch the Preboot Execution Environment (PXE). This enables the computer to boot via a network resource without requiring an installed operating system.</td>
</tr>
<tr>
<td>BIOS IPL devices</td>
<td>Initial Program Load (IPL) device. This can be virtually any device that has the ability to load and execute an operating system. This includes floppy drives, hard drives and CD-ROM drives.</td>
</tr>
<tr>
<td>Windows PE</td>
<td>Microsoft Windows Preinstallation Environment (PE).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> - This option is always displayed last, and it is displayed even if Windows PE is not available.</td>
</tr>
</tbody>
</table>

3. Enter the option number of the media you want to boot from and press Enter. Full Disk Encryption boots using the media you have selected, and displays the authentication dialog box.

**Using Slave Drive Functionality to Recover Information**

There are circumstances under which you need to access information on the hard disk of a Full Disk Encryption-protected machine and do not want to access this information by performing a recovery, for example, if you need to access a disk for forensic reasons or because a failure of the operating system makes it impossible to...
retrieve data on a disk. In such cases you can use Full Disk Encryption’s slave drive functionality. **Note:** we recommend that you use a stationary computer (not a laptop) when slaving a hard disk for forensic purposes.

A slave drive is a hard drive taken from one machine and installed (with the jumpers correctly set) on another machine, the master machine.

The slave drive functionality enables you to take a hard drive from a Full Disk Encryption-protected machine and, on another FDE-protected machine, unlock it in pre-boot and then access the information on that disk in Windows.

Slave drive functionality requires that both the slave drive and the master machine have been encrypted with the same algorithm. Only internal hard drives, and not USB hard drives, are supported.

The machine from which the hard drive is taken must have the **Allow the Hard Drive To Be Slaved** setting set to **Yes**, and the master machine must have the **Allow Slave Hard Drive** setting set to **Yes**. These settings can be found under System Settings Hardware Devices.

![Note - Both drives must use the same type of connector, i.e., IDE drives must use an IDE connector and SATA drives must use a SATA connector.]

**Accessing a Slave Drive**

The following is a typical example of how to access a slave drive:

1. As administrator, attach to your computer (now the master computer) an encrypted drive from a client that allows slaving. Before authenticating, be sure that the BIOS has located the slave drive. If it has not, you will not be able to continue.

2. Start the master computer with the attached slave drive and complete the Full Disk Encryption pre-boot authentication.

   Immediately after the successful pre-boot authentication, a slaving authentication window is displayed. The authentication window and its background are in grayscale to distinguish it from the other authentication windows. The slave drive authentication uses the user account name and fixed password, dynamic token or smart card required by the slave drive. The slave
drive authentication window is displayed for approximately 30 seconds, after which it disappears if no action has been taken. After each action, for example, a keystroke, the timer is reset and starts counting down again.

Note - Press Esc at any time to exit authentication.

3. After successful logon to the slave drive, proceed or cancel. The logon to the slave drive is logged on the master machine.

If you do not cancel, Windows starts and the drive is mounted as a Windows drive. It can now be accessed in Windows.

**Authenticating**

Authentication with fixed passwords and dynamic tokens is supported. Authentication with smart cards is also supported, but the master machine must contain the smart card drivers required to authenticate the slave drive.

**Compatibility of Drives**

Because of differences in the way different BIOSs handle disks, Full Disk Encryption slave-drive functionality currently supports only slave drives of the same drive type as that of the master machine (IDE, SATA or SCSI).

Note - SATA drives used as slave drives must be connected directly to the SATA interface on the motherboard. SATA and IDE slave drives connected via USB are not supported.

**Slave Drive Integrity**

Settings and user accounts, etc., on the slave drive cannot be changed locally. Changes to settings and user accounts on the local machine via profiles will not affect the slave drive.

**Wake-on-LAN**

Wake-on-LAN is supported on the master machine, but you will not be able to access the slave drive via Wake-on-LAN.
Using Slave Drive Functionality to Recover Information

**Windows Integrated Logon**

When a slave drive is connected to a master machine, authentication on the master machine is required even though Windows Integrated Logon is enabled in the Full Disk Encryption settings for this machine. Authentication on the slave drive is always required. If the slave drive is removed from the master machine and Windows Integrated Logon is enabled on that machine, Windows Integrated Logon will again be active.

**Remote Help**

**One-time Logon**

One-time logon is supported on both the master machine and the slave drive, but the user account and password of both the slave drive user and the helper must be on the slave drive for one-time logon to work.

**Remote Password Change**

Remote password change is supported on the master machine but not on the slave drive.

**Recovery**

The slave drive must be removed before performing recovery on the master machine.

**Hibernation**

Hibernation is supported on the master machine, but you must authenticate on the slave drive. The slave drive may not be attached to a hibernated machine. If a slave drive is to be connected to a master machine, the master machine must be shut down instead of hibernated.

**Uninstalling**

Do not uninstall Full Disk Encryption from a master machine; remove the slave drive before uninstalling.
Appendix A

HTTPS and HTTP Support and Requirements

This appendix describes:
- The HTTP servers that Full Disk Encryption supports
- The requirements related to these servers for FDEs https:// and http:// functionality to operate correctly.

HTTP Servers That FDE Supports

Full Disk Encryption supports the following HTTP servers:
- Apache
- IIS

FDE Requirements on the Supported Servers

For FDEs https:// and http:// functionality to work correctly, Full Disk Encryption has the following requirements on the above servers:
- On Apache, WEBDav must be installed and activated.
- On IIS, WebDav must be set to “Allowed” in the IIS Web Services Extensions.
- You must add the MIME types of all extensions that are to be accessible, see “FDE MIME Types” on page 194.
If, on Apache, you want support for NTLM (integrated Windows authentication), you must install a NTLM-authorization module.

**FDE MIME Types**

The following FDE extensions must be added as MIME types:

<table>
<thead>
<tr>
<th>Extension</th>
<th>Mime type</th>
</tr>
</thead>
<tbody>
<tr>
<td>isp</td>
<td>Silent installation profile</td>
</tr>
<tr>
<td>iip</td>
<td>Interactive installation profile</td>
</tr>
<tr>
<td>usp</td>
<td>Upgrade silent profile</td>
</tr>
<tr>
<td>uip</td>
<td>Upgrade interactive profile</td>
</tr>
<tr>
<td>upp</td>
<td>Update profile</td>
</tr>
<tr>
<td>unp</td>
<td>Uninstall profile</td>
</tr>
<tr>
<td>log</td>
<td>Log file</td>
</tr>
<tr>
<td>rec</td>
<td>Recovery file</td>
</tr>
<tr>
<td>bin</td>
<td>Driver file</td>
</tr>
<tr>
<td>inf</td>
<td>Information file for a driver</td>
</tr>
<tr>
<td>msi</td>
<td>Installation package</td>
</tr>
</tbody>
</table>

**Authorization and Permissions**

If the server is listed under trusted sites on the client, FDE will use the current credentials to access the resources on the server.

FDE uses NTLM authorization (Integrated Windows authentication) in this case. We also support basic authentication.

Users must have create, read and write access to the folders where they store their log files, recovery files, and profiles.

**Security**

FDE supports both https and http. If you want to use SSL (Secure Sockets Layer), which https uses, you must set up a certificate on the server.
It is strongly recommended to allow only https connections. Http should be used only in secured networks and only for testing purposes.
Appendix B

Status Information When Exported to File

In This Appendix

Installation Status Information  page 197
Sample Export Status File  page 199

The information reflecting the status of an installation can be exported to a file. The table below contains explanations of the values that certain fields in such a file can have. The values of the other fields are self explanatory. A sample status export file is also listed below, see “Sample Export Status File” on page 199.

Use the utility pslogexp.exe to export the status information to a file, this utility is described in Appendix “The pslogexp.exe Log Export Utility” on page 227.

### Installation Status Information

<table>
<thead>
<tr>
<th>Item</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Autologon</td>
<td>0 = Windows Integrated Logon is not enabled.</td>
</tr>
<tr>
<td></td>
<td>1 = Windows Integrated Logon is enabled.</td>
</tr>
<tr>
<td>Disk Number</td>
<td>A zero-based index of the hard drives on this computer.</td>
</tr>
</tbody>
</table>
## Installation Status Information

<table>
<thead>
<tr>
<th>Item</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Volume Number</strong></td>
<td>A zero-based index of the volumes on this computer.</td>
</tr>
</tbody>
</table>
| **Autologon**      | 0 = Windows Integrated Logon is not enabled.  
                      1 = Windows Integrated Logon is enabled.                                                                                             |
| **Disk Number**    | A zero-based index of the hard drives on this computer.                                                                                     |
| **Volume Number**  | A zero-based index of the volumes on this computer.                                                                                         |
| **Source Algorithm** | The algorithm that is currently in use. It can be one of the following values:  
                      • AES  
                      • 3DES  
                      • Blowfish  
                      • CAST  
                      • None  
                      • Invalid Key                                                                                                                         |
| **Destination Algorithm** | If this algorithm is different from the source algorithm, the driver is currently encrypting/decrypting in the background. It can be one of the following values:  
                      • AES  
                      • 3DES  
                      • Blowfish  
                      • CAST  
                      • None  
                      • Invalid Key                                                                                                                         |
<table>
<thead>
<tr>
<th>Item</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Volume State</strong></td>
<td>Indicates the state of the volume or the encryption action currently being carried out. It can have one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• 0 = Unencrypted</td>
</tr>
<tr>
<td></td>
<td>• 1 = Encrypting</td>
</tr>
<tr>
<td></td>
<td>• 2 = Decrypting</td>
</tr>
<tr>
<td></td>
<td>• 3 = Encrypted</td>
</tr>
<tr>
<td></td>
<td>• 4 = Reencrypting</td>
</tr>
<tr>
<td></td>
<td>• 255 = Missing</td>
</tr>
<tr>
<td><strong>Current State Value</strong></td>
<td>Indicates the current state of the volume encryption; it can have one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• 0-100 = % completed</td>
</tr>
<tr>
<td></td>
<td>• 101 = Internal error</td>
</tr>
<tr>
<td></td>
<td>• 102 = Internal error</td>
</tr>
<tr>
<td></td>
<td>• 255 = Completed</td>
</tr>
</tbody>
</table>

Sample Export Status File

Status
------

Misc
----
System ID:b3b393261b4906bac15c29077ad1793c
Version:6.2.0
Driver:5.0 srl.1
Update Password:0
Wake On LAN:0
Autologon:0
User:ADMIN
Management Console User:

Config
------
Last Local Configuration Change:
Last Profile Configuration Change:
Sample Export Status File

Recovery
--------
Last Recovery File Delivery: 2007-05-30 12:32:13+02:00

Logfile
-------
Last Log File Update: 2007-05-30 12:32:13+02:00
Last Log File Delivery: 2007-05-30 12:32:13+02:00

Encryption
----------
Disk Number: 0
Volume Number: 0
Source Algorithm: AES
Destination Algorithm: AES
Volume State: 3
Current State Value: 255
Disk Number: 1
Volume Number: 1
Source Algorithm: AES
Destination Algorithm: AES
Volume State: 3
Current State Value: 255
Disk Number: 1
Volume Number: 2
Source Algorithm: AES
Destination Algorithm: AES
Volume State: 3
Current State Value: 255
This appendix describes the permissions Full Disk Encryption requires.

**Table C-1 Permissions**

<table>
<thead>
<tr>
<th>Directory/Application</th>
<th>Admin</th>
<th>Install dir</th>
<th>Registry</th>
<th>Recovery dir</th>
<th>Profile dir</th>
<th>\System 32</th>
<th>Update dir</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Remove</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Uninstall profile</td>
<td>No</td>
<td>R,L,X,D,M,C,W</td>
<td>F³</td>
<td>-</td>
<td>(R,L,D,M,C,W)¹</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>FDEMC</td>
<td>No</td>
<td>R,L,X</td>
<td>R</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Create recovery disk(s)</td>
<td>No</td>
<td>R,L,X</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
Table C-1  Permissions

<table>
<thead>
<tr>
<th>Directory/Application</th>
<th>Admin</th>
<th>Install dir</th>
<th>Registry</th>
<th>Recovery dir</th>
<th>Profile dir</th>
<th>\System 32</th>
<th>Update dir</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tray (Px2)</td>
<td>No</td>
<td>R,L,X,(D, M,C,W)²</td>
<td>F³</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Recovery</td>
<td>No</td>
<td>R,L,X,D, M,C,W</td>
<td>R</td>
<td>R,L,X,D, M,C,W</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Central log</td>
<td>No</td>
<td>R,L,X,D, M,C,W</td>
<td>R</td>
<td>R,L,X,D, M,C,W</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>FDEMCUtil</td>
<td>No</td>
<td>-</td>
<td>R</td>
<td>-</td>
<td>R,L,(D, M,C,W)⁴</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>PS Control</td>
<td>No</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>R,L,X,D, M,C,W</td>
<td>-</td>
</tr>
</tbody>
</table>

R=Read, W=Write, L=List, X=Execute, M=Modify, D=Delete, F=Full control, C=Create.

A dash (-) means Not Applicable.

1 Required to publish profiles.

2 Required for Profile.dat.

3 Full access is required because the language setting for the Full Disk Encryption Management Console (FDEMC) is stored in the registry.

4 D,M,C and W are required for the creation of the Px2 directory.

**Install**

Install corresponds to performing an installation of Full Disk Encryption. This requires that the user be logged in with Administrator permissions.

**Remove**

Remove corresponds to removing the Full Disk Encryption application via the Windows Add/Remove Programs tool. This requires that the user be logged in to Windows with Administrator permissions.

**Uninstall Profile**

Uninstall profile corresponds to removing the Full Disk Encryption protection.
**FDEMC**

FDEMC corresponds to the executable file *PointsecForPC*. The application normally does not require any permissions for the Profile directory, however in order to publish profiles it requires the permissions specified in the table above.

**Create Recovery Disk(s)**

Create recovery disk(s) corresponds to the executable file *UseRec*.

**Tray (Px2)**

Tray corresponds to the executable *CPTray.exe*, which uses two other executables for performing some actions. The required permissions for these executables are presented in their own chapters.

**Recovery**

Recovery corresponds to the actions performed by the executable *CreRec*. In a Windows XP installation, the permissions listed above are required by *CreRec* for the 

C:\Documents and Settings\All Users\Application Data\Pointsec\Pointsec for PC directory and for the directory specified in the FDEMC (under Local → Edit Settings → Full Disk Encryption → System Settings → Install → Set Recovery Path) because *CreRec* writes the recovery file to these directories. In a Windows Vista installation, the permissions listed above are required by *CreRec* for the

C:\Users\All Users\Pointsec\Pointsec for PC directory and for the directory specified in the FDEMC (under Local → Edit Settings → Full Disk Encryption → System Settings → Install → Set Recovery Path) because *CreRec* writes the recovery file to these directories.

If these permissions are not granted, recovery file will not be created properly.

Note that, by default, all users have full permissions for C:\Documents and Settings\All Users\Application Data\Pointsec\Pointsec for PC and to C:\Users\All Users\Pointsec\Pointsec for PC. If you experience problems writing or accessing the recovery file, ensure that the default permissions have not been changed.

**Central Log**

Central Log corresponds to the actions performed by the executable *CentralLog*. *CentralLog* requires the permissions shown in the Full Disk Encryption install dir and the Recovery dir since it writes log files to these directories. If these permissions are not granted, the remote logging and Event viewer will not receive new log events.
**FDEMCUtil**

FDEMCUtil corresponds to the actions performed by the tray using the DLL PCMCUtil.dll. The DLL requires the shown permissions in the Profile directory since it writes recovery and log files to the directory.

**PS Control**

PS Control corresponds to the actions performed by the executable pscontrol. The executable requires the shown permissions in the Full Disk Encryption install dir and the System32 directory in order to install Windows language files, smart card/token reader drivers.

---

**Permissions: With Full Disk Encryption Service Start**

**Recommended Users**

The table below describes which users are recommended to run applications and perform specific tasks. X(O) denotes that this is the only possible solution, and X(P) denotes that it is controlled by Full Disk Encryption.

<table>
<thead>
<tr>
<th>User/Application</th>
<th>Administrator</th>
<th>Service Account</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install</td>
<td>X(O)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove</td>
<td>X(O)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Uninstall profile</td>
<td></td>
<td>X(P)</td>
<td></td>
</tr>
<tr>
<td>FDEMC</td>
<td>X</td>
<td></td>
<td>X(P)</td>
</tr>
<tr>
<td>Tray</td>
<td></td>
<td></td>
<td>X(P)</td>
</tr>
<tr>
<td>Recovery</td>
<td></td>
<td>X(P)</td>
<td></td>
</tr>
<tr>
<td>Central log</td>
<td></td>
<td>X(P)</td>
<td></td>
</tr>
<tr>
<td>PS Control</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Required Permissions

The table below describes the required permissions for the recommended setup above. Note that the Service account must be a member of the Administrator group in order to run Service Start.

Table C-3 Required permissions for Service Start

<table>
<thead>
<tr>
<th>Application/Directory</th>
<th>Admin</th>
<th>Normal User</th>
<th>Service Account</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Admin</td>
<td>X</td>
<td>None</td>
<td>X</td>
</tr>
<tr>
<td>Install directory</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pointsec Registry</td>
<td>F(^2)</td>
<td>F(^2)</td>
<td>F(^2)</td>
</tr>
<tr>
<td>Profile directory</td>
<td>None</td>
<td>None</td>
<td>R,L,X</td>
</tr>
<tr>
<td>Update directory</td>
<td>None</td>
<td>None</td>
<td>R,L,X,C</td>
</tr>
</tbody>
</table>

R=Read, W=Write, L=List, X=Execute, M=Modify, D=Delete, F=Full control, C=Create.

\(^1\)These permissions are required in order for Recovery and Log files to be handled correctly (Profile.dat and possibly more files).

\(^2\)Full control is required for updating the Language setting in the registry.

Permissions: Without Full Disk Encryption Service Start

If Full Disk Encryption Service Start is not used, the normal user requires the same access permissions the Service account has (apart from being a member of the Administrator group). In this case, all applications normally run via the service are executed by the normal user.
Permissions: Remote Desktop

The permissions needed by Remote Desktop users on a Full Disk Encryption-installed machine are those required by a locally logged-on user: full permissions for *Program Files* → *Check Point* and Full Disk Encryption registry keys.

Windows User Account Registry Permissions

To install, upgrade, change language, and import profiles on a Windows PC, a user account needs the following registry permissions: Query value, Set value, Create subkey, Enumerate subkey, Notify, Create link, and Read control.

In order to uninstall on a Windows PC, a user account needs the above registry permissions plus Delete.
In This Appendix

Specifying the Language Used in the FDEMC  page 207
Configuring the Languages Available on the Client(s)  page 208
Configuring the Language Used on the Clients  page 208
Changing the Language in the Tray  page 209
Languages Supported  page 209
Fallback Languages  page 210

This appendix describes the language support provided in Full Disk Encryption. FDE is installed with the supported languages listed below under “Languages Supported” on page 209.

Specifying the Language Used in the FDEMC

The administrator selects which language will be used in the Full Disk Encryption Management Console (FDEMC) in the Language menu option on the FDEMC menu bar. The administrator can choose one of the supported languages or he/she can choose Operating System, which sets the language to be used in the FDEMC to the language of the Windows operating system.

If the operating system language is a nonsupported variant of one of the eight supported languages, for example, French (Canada) or Chinese (Singapore), the language variant used in the FDEMC is the fallback language listed under “Fallback
Configuring the Languages Available on the Client(s)

Languages” on page 210. If Operating System is selected and the language of the operating system is not one of the supported languages, US English will be displayed in the FDEMC.

Configuring the Languages Available on the Client(s)

The administrator configures which of the supported languages will be available for use on a client in the client’s preboot interface, system tray, recovery utility, and single sign-on interface (if single sign-on is active). The supported languages are listed below.

To configure which languages are available on the client(s), see the Available Languages setting described “Install Settings” on page 35.

Configuring the Language Used on the Clients

The administrator also configures which of the available supported languages will be used in the client’s preboot interface, system tray, recovery utility, and single sign-on interface (if single sign-on is active). If additional languages are available on the client, the user can change to one of these languages, see “Changing the Language in the Tray” on page 209, below.

If Operating System is selected and the operating system language is a nonsupported variant of one of the eight supported languages, for example, French (Canada) or Chinese (Singapore), the language variant displayed is the fallback language listed under “Fallback Languages” on page 210. If Operating System is selected and the language of the operating system is not one of the supported languages, US English will be displayed.

To configure which language to be used on the client(s), see the Select Language setting under “Install Settings” in Chapter 3, “Install Settings” on page 35.
Changing the Language in the Tray

In the tray, you can change the language used in the client’s preboot interface, system tray, recovery utility, and single sign-on interface (if single sign-on is active). To do this, double-click or right-click the Full Disk Encryption icon. Navigate to where you select the language: Settings... → Advanced → Language → Select Language. The Select Language drop-down menu contains the languages you can choose.

Languages Supported

The following languages are supported in Full Disk Encryption:

- Brazilian Portuguese
- Canada French
- Chinese (Simplified)
- Chinese (Taiwan)
- Czech
- English
- French
- German
- Hungarian
- Italian
- Japanese
- Korean
- Polish
- Portuguese
- Russian
- Spanish
- Thai

These languages are available in:

- Full Disk Encryption Management Console (FDEMC)
• Client preboot interface
• Client system tray
• Client single sign-on dialog (if single sign-on is active on that client)
• Client OneCheck Logon dialog (if it is active on that client)
• Recovery utility.

## Fallback Languages

If the operating system language is a nonsupported variant of one of the supported languages, for example, French (Canada) or Chinese (Singapore), the language variant used in the FDEMC is the fallback language listed in the following table:

<table>
<thead>
<tr>
<th>ID</th>
<th>Selected Language</th>
<th>Fallback Language</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0C04</td>
<td>Chinese (Hong Kong S.A.R.)</td>
<td>Chinese (Traditional)</td>
<td>0x7C04</td>
</tr>
<tr>
<td>0x1404</td>
<td>Chinese (Macau S.A.R.)</td>
<td>Chinese (Traditional)</td>
<td>0x7C04</td>
</tr>
<tr>
<td>0x0804</td>
<td>Chinese (People's Republic of China)</td>
<td>Chinese (Simplified)</td>
<td>0x0004</td>
</tr>
<tr>
<td>0x0004</td>
<td>Chinese (Simplified)</td>
<td>Chinese (Simplified)</td>
<td>0x0004</td>
</tr>
<tr>
<td>0x1004</td>
<td>Chinese (Singapore)</td>
<td>Chinese (Simplified)</td>
<td>0x0004</td>
</tr>
<tr>
<td>0x0404</td>
<td>Chinese (Taiwan)</td>
<td>Chinese (Traditional)</td>
<td>0x7C04</td>
</tr>
<tr>
<td>0x7C04</td>
<td>Chinese (Traditional)</td>
<td>Chinese (Traditional)</td>
<td>0x7C04</td>
</tr>
<tr>
<td>0x0009</td>
<td>English</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x0C09</td>
<td>English (Australia)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x2809</td>
<td>English (Belize)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
</tbody>
</table>
## Table D-1  Fallback Languages

<table>
<thead>
<tr>
<th>ID</th>
<th>Selected Language</th>
<th>Fallback Language</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x1009</td>
<td>English (Canada)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x2409</td>
<td>English (Caribbean)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x1809</td>
<td>English (Ireland)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x2009</td>
<td>English (Jamaica)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x1409</td>
<td>English (New Zealand)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x3409</td>
<td>English (Republic of the Philippines)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x1C09</td>
<td>English (South Africa)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x2C09</td>
<td>English (Trinidad and Tobago)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x0809</td>
<td>English (United Kingdom)</td>
<td>English (United Kingdom)</td>
<td>0x0809</td>
</tr>
<tr>
<td>0x0409</td>
<td>English (United States)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x3009</td>
<td>English (Zimbabwe)</td>
<td>English (United States)</td>
<td>0x0409</td>
</tr>
<tr>
<td>0x000C</td>
<td>French</td>
<td>French (France)</td>
<td>0x040C</td>
</tr>
<tr>
<td>0x080C</td>
<td>French (Belgium)</td>
<td>French (France)</td>
<td>0x040C</td>
</tr>
<tr>
<td>0x0C0C</td>
<td>French (Canada)</td>
<td>French (France)</td>
<td>0x040C</td>
</tr>
<tr>
<td>0x040C</td>
<td>French (French)</td>
<td>French (France)</td>
<td>0x040C</td>
</tr>
<tr>
<td>0x140C</td>
<td>French (Luxembourg)</td>
<td>French (France)</td>
<td>0x040C</td>
</tr>
<tr>
<td>0x180C</td>
<td>French (Principality of Monaco)</td>
<td>French (France)</td>
<td>0x040C</td>
</tr>
<tr>
<td>0x100C</td>
<td>French (Switzerland)</td>
<td>French (France)</td>
<td>0x040C</td>
</tr>
<tr>
<td>0x0007</td>
<td>German</td>
<td>German (Germany)</td>
<td>0x0407</td>
</tr>
<tr>
<td>0x0C07</td>
<td>German (Austria)</td>
<td>German (Germany)</td>
<td>0x0407</td>
</tr>
<tr>
<td>0x0407</td>
<td>German (Germany)</td>
<td>German (Germany)</td>
<td>0x0407</td>
</tr>
<tr>
<td>0x1407</td>
<td>German (Liechtenstein)</td>
<td>German (Germany)</td>
<td>0x0407</td>
</tr>
<tr>
<td>ID</td>
<td>Selected Language</td>
<td>Fallback Language</td>
<td>ID</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------</td>
<td>------------------------------</td>
<td>-----</td>
</tr>
<tr>
<td>0x1007</td>
<td>German (Luxembourg)</td>
<td>German (Germany)</td>
<td>0x0407</td>
</tr>
<tr>
<td>0x0807</td>
<td>German (Switzerland)</td>
<td>German (Germany)</td>
<td>0x0407</td>
</tr>
<tr>
<td>0x0010</td>
<td>Italian</td>
<td>Italian (Italy)</td>
<td>0x0410</td>
</tr>
<tr>
<td>0x0410</td>
<td>Italian (Italy)</td>
<td>Italian (Italy)</td>
<td>0x0410</td>
</tr>
<tr>
<td>0x810</td>
<td>Italian (Switzerland)</td>
<td>Italian (Italy)</td>
<td>0x0410</td>
</tr>
<tr>
<td>0x0011</td>
<td>Japanese</td>
<td>Japanese (Japan)</td>
<td>0x0411</td>
</tr>
<tr>
<td>0x0411</td>
<td>Japanese (Japan)</td>
<td>Japanese (Japan)</td>
<td>0x0411</td>
</tr>
<tr>
<td>0x0019</td>
<td>Russian</td>
<td>Russian (Russia)</td>
<td>0x0419</td>
</tr>
<tr>
<td>0x0419</td>
<td>Russian (Russia)</td>
<td>Russian (Russia)</td>
<td>0x0419</td>
</tr>
<tr>
<td>0x000A</td>
<td>Spanish</td>
<td>Spanish (Spain)</td>
<td>0x0COA</td>
</tr>
<tr>
<td>0x2COA</td>
<td>Spanish (Argentina)</td>
<td>Spanish (Spain)</td>
<td>0x0COA</td>
</tr>
<tr>
<td>0x400A</td>
<td>Spanish (Bolivia)</td>
<td>Spanish (Spain)</td>
<td>0x0COA</td>
</tr>
<tr>
<td>0x340A</td>
<td>Spanish (Chile)</td>
<td>Spanish (Spain)</td>
<td>0x0COA</td>
</tr>
<tr>
<td>0x240A</td>
<td>Spanish (Columbia)</td>
<td>Spanish (Spain)</td>
<td>0x0COA</td>
</tr>
<tr>
<td>0x140A</td>
<td>Spanish (Costa Rica)</td>
<td>Spanish (Spain)</td>
<td>0x0COA</td>
</tr>
<tr>
<td>0x1C0A</td>
<td>Spanish (Dominican Republic)</td>
<td>Spanish (Spain)</td>
<td>0x0COA</td>
</tr>
<tr>
<td>0x300A</td>
<td>Spanish (Ecuador)</td>
<td>Spanish (Spain)</td>
<td>0x0COA</td>
</tr>
<tr>
<td>0x440A</td>
<td>Spanish El Salvador)</td>
<td>Spanish (Spain)</td>
<td>0x0COA</td>
</tr>
<tr>
<td>0x100A</td>
<td>Spanish (Guatemala)</td>
<td>Spanish (Spain)</td>
<td>0x0COA</td>
</tr>
<tr>
<td>0x480A</td>
<td>Spanish (Honduras)</td>
<td>Spanish (Spain)</td>
<td>0x0COA</td>
</tr>
<tr>
<td>0x080A</td>
<td>Spanish (Mexico)</td>
<td>Spanish (Spain)</td>
<td>0x0COA</td>
</tr>
<tr>
<td>0x4COA</td>
<td>Spanish (Nicaragua)</td>
<td>Spanish (Spain)</td>
<td>0x0COA</td>
</tr>
<tr>
<td>0x180A</td>
<td>Spanish (Panama)</td>
<td>Spanish (Spain)</td>
<td>0x0COA</td>
</tr>
<tr>
<td>0x3C0A</td>
<td>Spanish (Paraguay)</td>
<td>Spanish (Spain)</td>
<td>0x0COA</td>
</tr>
<tr>
<td>0x280A</td>
<td>Spanish (Peru)</td>
<td>Spanish (Spain)</td>
<td>0x0COA</td>
</tr>
<tr>
<td>0x500A</td>
<td>Spanish (Puerto Rico)</td>
<td>Spanish (Spain)</td>
<td>0x0COA</td>
</tr>
<tr>
<td>0x0C0A</td>
<td>Spanish (Spain)</td>
<td>Spanish (Spain)</td>
<td>0x0COA</td>
</tr>
<tr>
<td>0x380A</td>
<td>Spanish (Uruguay)</td>
<td>Spanish (Spain)</td>
<td>0x0COA</td>
</tr>
<tr>
<td>0x200A</td>
<td>Spanish (Venezuela)</td>
<td>Spanish (Spain)</td>
<td>0x0COA</td>
</tr>
</tbody>
</table>
Keyboard Layouts

In This Appendix

The Default Keyboard Layout
Changing the Keyboard Layout
Supported Keyboard Layouts

The Default Keyboard Layout

The first time the preboot authentication dialog box is displayed after installation, Full Disk Encryption, by default, uses the keyboard layout that is the default in the Windows operating system. In addition, the US English keyboard layout is always installed as a backup; it cannot be removed.

Changing the Keyboard Layout

If other keyboard layouts are available in your Windows installation (and supported by FDE), you can scroll through the available layouts by repeatedly clicking on the icon in the lower right corner of the dialog box, see the figure below. You can also scroll through the available layouts by repeatedly pressing left shift + left alt. The active keyboard layout is the layout whose name is displayed in the icon (the icon is to the left of the Virtual Keyboard button in the lower right corner of the screen.
image shown in the figure below). After selecting a keyboard layout and successfully logging on to FDE, that is the keyboard that will be active the next time the preboot authentication dialog box is displayed.

Figure E-1

Keyboard layouts in Windows XP and Vista are set up under Regional and Language Options → Languages → Details → Settings.

Supported Keyboard Layouts

FDE supports all Windows keyboard layouts, but with the following limitations:

- Dead keys in the Windows keyboard layouts are not supported.
  
  Dead keys are commonly used, for example, to generate accented letters, because that way one does not need one key for each possible combination of letter and accent, but only one dead key for each accent in addition to the usual letter keys. Take the following example, if a keyboard has a dead key ``, the French character e accent grave (è) can be generated by pressing first ``, then e. Usually pressing a dead key followed by space produces the character denoted by the dead key; e.g. ``, space results in “¨”. Note that dead keys are used in the keyboard layouts for many different languages.

- Right-to-left languages are displayed left to right.

- Input Method Editors (IMEs) are not supported.
Appendix F

PS Control Command Line Utility

In This Chapter

Introduction ........................................ page 215
Using the PS Control Utility ...................... page 216
   Options .......................................... page 216
   Commands ....................................... page 217
   Error Codes .................................... page 218
   Examples of Using the PS Control Utility ... page 218
Smart Cards, Smart Card Readers and their Drivers page 219
   Managing Smart Cards, Smart Card Readers and Drivers page 220
Exporting a Machine’s Status Information ........ page 221
   Export Status File ............................... page 221

Introduction

The PS Control command line utility is meant for administrators. An administrator uses this utility to develop a script (for example, a .bat file) that carries out certain tasks on a machine. The script can also be deployed to carry out tasks on remote machines when users log on.
The PS Control command line utility can be used to manage drivers related to smart cards and to export the status information of a machine.

You can also use the PS Control command line utility when FDE is not installed to determine if a hard disk is encrypted, see “Running the PS Control Utility When FDE Is Not Installed” on page 225 for more information.

The PS Control program file, pscontrol.exe, is found in the Full Disk Encryption folder, which is located in the Check Point folder under Program Files.

### Using the PS Control Utility

The PS Control utility is command based. Each command carries out only one specific task, and only one command can be executed per call. The format of the command is as follows:

```
pscontrol [option] <command>
```

where `option` and `command` can be any of those in the respective tables below.

### Options

PS Control offers the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| -l     | Write a log to `<filename>`.
| -v     | Be verbose. |
The following commands can be executed using PS Control:

**Table F-2**  PS Control utility commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>install-driver</strong></td>
<td>Installs the driver whose filename is specified in the command.</td>
</tr>
<tr>
<td><strong>Note</strong> - Note that the driver must be registered in Full Disk Encryption before it can be installed -- the drivers in the Full Disk Encryption release package and on the Full Disk Encryption installation CD have already been registered. Thus registration is required only for drivers that have not been released together with the Full Disk Encryption package or CD; to register such a driver, see <code>register-prd</code> and <code>register-ptd</code> below. See also “Managing Smart Cards, Smart Card Readers and Drivers” on page 220.</td>
<td></td>
</tr>
<tr>
<td><strong>remove-driver</strong></td>
<td>Removes the driver whose filename is specified in the command. Note that the driver must be unregistered before it can be removed, see <code>unregister-prd</code> and <code>unregister-ptd</code> below.</td>
</tr>
<tr>
<td><strong>list-drivers</strong></td>
<td>Displays a list of currently installed drivers on this machine.</td>
</tr>
<tr>
<td><strong>register-prd</strong></td>
<td>Registers the smart card reader driver whose <code>.inf</code> file is specified as the filename in the command.</td>
</tr>
<tr>
<td><strong>register-ptd</strong></td>
<td>Registers the smart card driver whose <code>.inf</code> file is specified as the filename in the command.</td>
</tr>
<tr>
<td><strong>unregister-prd</strong></td>
<td>Unregisters the smart card reader driver whose <code>.inf</code> file is specified as the filename in the command.</td>
</tr>
<tr>
<td><strong>unregister-ptd</strong></td>
<td>Unregisters the smart card driver whose <code>.inf</code> file is specified as the filename in the command.</td>
</tr>
<tr>
<td><strong>extract-prd</strong></td>
<td>Extracts the contents of the smart card reader driver registry and writes this information to the filename specified in the command.</td>
</tr>
<tr>
<td><strong>extract-ptd</strong></td>
<td>Extracts the contents of the smart card driver registry and writes this information to the filename specified in the command.</td>
</tr>
<tr>
<td><strong>export-status</strong></td>
<td>Exports the status of the machine to <code>&lt;filename&gt;</code>. The file is in XML format.</td>
</tr>
</tbody>
</table>
Error Codes

The error codes in the table below are returned by the PS Control utility so a script can determine whether it has completed successfully.

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Operation successful.</td>
</tr>
<tr>
<td>1</td>
<td>An incorrect argument was specified in the <code>pscontrol</code> command.</td>
</tr>
<tr>
<td>2</td>
<td>Incorrect filename specified. Issued if the file cannot be opened, if the file does not exist in the registry (when installing a driver), or if the file format is incorrect.</td>
</tr>
<tr>
<td>3</td>
<td>A Full Disk Encryption installation cannot be found on this machine.</td>
</tr>
<tr>
<td>4</td>
<td>The operation terminated unexpectedly. This can happen when a read/write to the Full Disk Encryption system area fails, which indicates an error in the local installation of Full Disk Encryption or a corrupt local installation.</td>
</tr>
</tbody>
</table>

Examples of Using the PS Control Utility

**Registering Drivers**

```
C:\Program Files\Pointsec\Pointsec for PC>pscontrol -v register-pto
D:\Modules\ptd.inf
Connected to Pointsec 6.0.0 (2005-12-14 19:21:55 Build 1018).
Replacing section "RSA SecureID 800".
Replacing section "RSA Smart Card 5200".
Replacing section "RSA Smart Card 6100(eGate)".
Replacing section "Schlumberger Cyberflex e-Gate".
Replacing section "Schlumberger Cyberflex e-Gate 32K".
Replacing section "Schlumberger Cyberflex 32K".
Replacing section "Schlumberger Cyberflex 8K".
Replacing section "Aladdin eToken".
```
Installing a Driver

C:\Program Files\Pointsec\Pointsec for PC>pscontrol -v install-driver
D:\Modules\msc_p11.bin

Connected to Pointsec 6.0.0 (2005-12-14 19:21:55 Build 1018).

Writing 285274 bytes...

Exporting Status Information

C:\Program Files\Pointsec\Pointsec for PC>pscontrol.exe export-status mystatus.xml

Executing query – STATUS

Creating output status file as ‘mystatus.xml’

SUCCESS: Export complete

---

Smart Cards, Smart Card Readers and their Drivers

Full Disk Encryption 7.x supports authentication using smart cards. To authenticate a user via a smart card, Full Disk Encryption must be able to communicate with both the smart card and the smart card reader. This requires one driver for communicating with the card and another driver for communicating with the card reader.

Note - Note that smart cards that function as a combined card and card reader unit (for example, the RSA SecureID 800) still require two drivers, one for the card and one for the reader. Note also that some drivers support more than one smart card or smart card reader.

Because smart cards from different manufacturers, and even different models of smart cards from the same manufacturer, communicate differently, Full Disk Encryption provides a variety of drivers. Full Disk Encryption maintains a registry of the supported smart cards and smart card readers (There are smart cards on the market that Full Disk Encryption does not support, and no drivers for these smart cards are provided).

You use the PS Control command line utility to register smart cards and smart card readers in the Full Disk Encryption registry and to unregister smart cards and smart card readers in that registry. The utility also enables you to install drivers on the
Full Disk Encryption system after they have been registered. Note that a driver must be registered before it can be installed, see the `register-prd` and `register-prd` commands above, under “Commands” on page 217. This enables you to use smart cards and smart card readers that are supported after the release of Full Disk Encryption.

Managing Smart Cards, Smart Card Readers and Drivers

Drivers supported by Full Disk Encryption at the time of delivery are provided in the release package (if receiving or downloading a .zip file) or on the Full Disk Encryption CD. The drivers required to communicate with the smart cards and smart card readers your enterprise uses must be installed on the machines that will use this smart card authentication. The installation is usually done by a script that executes PS Control commands.

Similarly, you can also remove a driver or unregister a driver via a script, as well as list all the currently installed drivers, using PS Control.

Registering a Driver

To register a driver you must have an .inf file, which is usually delivered together with the driver. The .inf file contains information about the driver or drivers, for example identifying the driver or drivers and the hardware it or they communicate with.

Note - The drivers in the Full Disk Encryption release package or on the Full Disk Encryption installation CD have already been registered. Registration is required only for drivers that have not been released together with the Full Disk Encryption package.

See “Registering Drivers” on page 218 for an example of using the PS Control utility to register a driver.

Installing a Driver

See “Installing a Driver” on page 219 for an example of using the PS Control utility to install a driver.
Exporting a Machine’s Status Information

The PS Control utility can be used to export status information about a specific machine. The information is exported in an XML file, which can be input to a program that processes the status information.

See the following table for a description of tags in an export status file, and see “Exporting Status Information” on page 219 for an example of using the PS Control utility to export status information.

Export Status File

Description of Tags

The following table contains a description of the most significant tags in the Export Status file. See “Sample Export Status File” on page 223 for an example of the file.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description of Tag Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>VERSION</td>
<td>The version of Full Disk Encryption currently installed on the machine.</td>
</tr>
<tr>
<td>UPDPWD</td>
<td>Specifies if the update validation password has been set. 0 = No, 1 = Yes.</td>
</tr>
<tr>
<td>WAKEONLAN</td>
<td>Specifies whether Wake-on-LAN is enabled. 0 = No, 1 = Yes.</td>
</tr>
<tr>
<td>AUTOLOGON</td>
<td>Specifies whether Windows Integrated Logon is enabled. 0 = No, 1 = Yes.</td>
</tr>
<tr>
<td>USER</td>
<td>User account name of the user account currently logged on to this machine. This information is Base64 encoded.</td>
</tr>
<tr>
<td>LOCAL</td>
<td>Date, time, and user account name of the user account that last updated the configuration of Full Disk Encryption on this machine. The date, time, and user account name are in the following format: yyyy-mm-dd hh:mm:ss - USERACCOUNTNAME. This information is Base64 encoded.</td>
</tr>
<tr>
<td>PROFILE</td>
<td>User account name of the person who created or edited the profile that last updated this machine. This information is Base64 encoded.</td>
</tr>
</tbody>
</table>
Table F-4 Significant tags in the Export Status file

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description of Tag Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>RECOVERY UPDATE</td>
<td>Date and time when recovery information was last updated. This information is Base64 encoded.</td>
</tr>
<tr>
<td>RECOVERY DELIVERY</td>
<td>Date and time when recovery information was last sent to the directory defined in the specified recovery path. This information is Base64 encoded.</td>
</tr>
<tr>
<td>LOGFILE UPDATE</td>
<td>Date and time when log information was last updated. This information is Base64 encoded.</td>
</tr>
<tr>
<td>LOGFILE DELIVERY</td>
<td>Date and time when log information was last sent to the directory defined in the specified log path. This information is Base64 encoded.</td>
</tr>
<tr>
<td>DISKNR</td>
<td>Number of the hard disk drive. Numbering begins with zero.</td>
</tr>
<tr>
<td>VOLNR</td>
<td>Volume number of the hard disk. Numbering begins with zero.</td>
</tr>
<tr>
<td>ALGO1</td>
<td>Current algorithm in use. The tag can have one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• AES</td>
</tr>
<tr>
<td></td>
<td>• 3DES</td>
</tr>
<tr>
<td></td>
<td>• Blowfish</td>
</tr>
<tr>
<td></td>
<td>• CAST</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• Invalid Key</td>
</tr>
<tr>
<td></td>
<td>See also the description of ALGO2, below.</td>
</tr>
<tr>
<td>ALGO2</td>
<td>The target algorithm. During encryption, this is the algorithm being used to encrypt the volume. During decryption, the value will be None. When encryption is completed, the values of ALGO1 and ALGO2 are identical.</td>
</tr>
<tr>
<td></td>
<td>The tag can have one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• AES</td>
</tr>
<tr>
<td></td>
<td>• 3DES</td>
</tr>
<tr>
<td></td>
<td>• Blowfish</td>
</tr>
<tr>
<td></td>
<td>• CAST</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• Invalid Key</td>
</tr>
</tbody>
</table>


The following is an example of an export status file:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<RETURN>
<STATUS>
<MISC>
<VERSION>6.1.3 (2006-11-06 09:17:12 Build 1113)</VERSION>
<DRIVER>5.0 sr1.1</DRIVER>
<UPDPWD>1</UPDPWD>
<WAKEONLAN>0</WAKEONLAN>
<AUTOLOGON>0</AUTOLOGON>
```

---

**Table F-4**  Significant tags in the Export Status file

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description of Tag Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>STATE</td>
<td>State of encryption of this volume (VOLNR) on the disk. Can be one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• 0 = Clear</td>
</tr>
<tr>
<td></td>
<td>• 1 = Encrypting</td>
</tr>
<tr>
<td></td>
<td>• 2 = Decrypting</td>
</tr>
<tr>
<td></td>
<td>• 3 = Encrypted</td>
</tr>
<tr>
<td></td>
<td>• 4 = Re-encrypting</td>
</tr>
<tr>
<td></td>
<td>• 255 = Missing</td>
</tr>
<tr>
<td>VALUE</td>
<td>Value may have one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• 0-100 = % of encryption completed</td>
</tr>
<tr>
<td></td>
<td>• 101 = Internal error</td>
</tr>
<tr>
<td></td>
<td>• 102 = Internal error</td>
</tr>
<tr>
<td></td>
<td>• 255 = Encryption completed</td>
</tr>
<tr>
<td></td>
<td>Note that 255 can also mean “processing completed” when both ALGO1 and ALGO2 are None, as there has been no encryption and this fact has been registered.</td>
</tr>
</tbody>
</table>

---

**Sample Export Status File**

The following is an example of an export status file:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<RETURN>
<STATUS>
<MISC>
<VERSION>6.1.3 (2006-11-06 09:17:12 Build 1113)</VERSION>
<DRIVER>5.0 sr1.1</DRIVER>
<UPDPWD>1</UPDPWD>
<WAKEONLAN>0</WAKEONLAN>
<AUTOLOGON>0</AUTOLOGON>
```
<USER>QURNSU4=/</USER>

<MCUSER/>

</MISC>

<CONFIG>

<LOCAL>MjAwNi0xMS0xNiAxNDo1NDoxMCswMjowMCAtIFN5c3RlbVxBRE1JTg==</LOCAL>

<PROFILE>MjAwNi0xMS0xNiAxNDo...DXFdPUktcdXBkLnVwcA==</PROFILE>

</CONFIG>

<RECOVERY>

<UPDATE>MjAwNi0xMS0xNiAxNDo1NTozNg==</UPDATE>

<DELIVERY>MjAwNi0xMS0xNiAxNDo1NTozNg==</DELIVERY>

</RECOVERY>

<LOGFILE>

<UPDATE>MjAwNi0xMS0xNiAxNDo1NTozNg==</UPDATE>

<DELIVERY>MjAwNi0xMS0xNiAxNDo1NTozNg==</DELIVERY>

</LOGFILE>

<ENCRYPTION>

<VOL>

<DISKNR>0</DISKNR>

<VOLNR>0</VOLNR>

<ALGO1>AES</ALGO1>

<ALGO2>AES</ALGO2>

<STATE>3</STATE>

<VALUE>255</VALUE>

</VOL>

</VOL>

<DISKNR>0</DISKNR>
Running the PS Control Utility When FDE Is Not Installed

There might be times when you want to use the PS Control command line utility when FDE is not installed, for example, if you are doing a zero-touch deployment and need to determine if a hard drive is already encrypted before re-installing FDE.
To run the PS Control command line utility when FDE is not installed, do the following:

1. Ensure that Microsoft Visual C++ 2005 SP1 redistributables are installed.
2. Copy the `Pscontrol.exe`, `ccore32.bin`, and `psutil.dll` from `<Program Files\Poinstec\Pointsec for PC>` to a folder as follows:
   - `C:\temp\pscontrol.exe`
   - `C:\temp\ccore32.bin`
   - `C:\temp\pcmc\psutil.dll`
3. Run the following `pscontrol.exe` command:
   - `C:\temp\pscontrol.exe export-status mystatus.xml`

**Note** - The FDE filter driver must be installed and running before you can use `pscontrol.exe` as described above.
Appendix G

The pslogexp.exe Log Export Utility

In This Appendix

Introduction .............................................................................. page 227
pslogexp.exe Utility Syntax and Commands ......................... page 228
Examples of Using the pslogexp.exe Utility ....................... page 230
Correct Display of National Characters in Exported Files ... page 230

Introduction

The pslogexp.exe utility is meant for administrators; Read and Execute permissions are required to run it. To use the utility, the administrator must have View Logs permission, see Chapter 4, “Permissions Settings” on page 80.

This utility must be executed on a machine running Pointsec for PC 6.1.x or later.

An administrator can use pslogexp.exe to export the local log or a remote log to console or to redirect the data to a file. Available formats are CSV (Comma Separated Values), TSV (Tab Separated Values) or XML.

The utility also enables the administrator to specify the log password.

The utility can be used in a script.
pslogexp.exe Utility Syntax and Commands

The syntax and commands for pslogexp.exe are described in this section.

Syntax

The syntax for using pslogexp.exe is as follows:

pslogexp.exe [/?] [commands] [filename] [log password]

Description:
Export the log file or local log to console in the specified format.
Use ‘>’ to redirect to file.

Commands

The following commands are available:

<table>
<thead>
<tr>
<th>Table G-1</th>
<th>pslogexp.exe commands</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>csv</td>
<td>Export the log data as comma separated values (default).</td>
</tr>
<tr>
<td>tsv</td>
<td>Export the log data as tab separated values.</td>
</tr>
<tr>
<td>xml</td>
<td>Export the log data in XML format.</td>
</tr>
<tr>
<td>local</td>
<td>Export the local machine’s log data.</td>
</tr>
</tbody>
</table>
Table G-1  pslogexp.exe commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>heads</td>
<td>Include headings in the log data that is exported. The following headings are included: Version, Type, Level, Category, Event ID, Source ID, Date and Time, Host, Heading, Body, Caller, Target, Param3, Param4. Headings are available only in CSV and TSV data.</td>
</tr>
<tr>
<td>?</td>
<td>Help for the pslogexp.exe utility.</td>
</tr>
<tr>
<td>[log password]</td>
<td>Full Disk Encryption-protected computers that have the same log password set can export each others logs without authenticating. But a FDE-protected computer that has a different log password than the log it wants to export must authenticate with the password of the log it wants to export. If an administrator, from a computer on which no log password has been set, wants to export a remote password-protected log; authentication using the password of the protected log is required. If a log has no log password, no authentication is required. The log password parameter is used to provide the password required for the authentication required to export a remote log.</td>
</tr>
</tbody>
</table>

The following table contains information on filenames:

Table G-2  Filename information

<table>
<thead>
<tr>
<th>Filename</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filename</td>
<td>On a local machine, the filename will be logfile.log, where logfile is the computer name of the local machine, for example MYCOMPUTER. On a remote machine, the filename will be the full path name of the file to which you will export the log, for example \Share\COMPUTER02.log.</td>
</tr>
</tbody>
</table>
Examples of Using the pslogexp.exe Utility

Exporting the Local Log
Below is an example of exporting the local log database to a file:

   pslogexp.exe /tsv /heads /local >local.tsv
   pslogexp.exe /xml /local >local.xml

Note the use of > to redirect the data to the file local.tsv.

Exporting a Remote Logfile
Below is an example of exporting the log files to a file:

   pslogexp.exe /tsv /heads "MYCOMPUTER.log" >logfile.tsv
   pslogexp.exe /xml "\Share\COMPUTER02.log" logpwd >logfile.xml
   pslogexp.exe /xml "c:\logs\MYLOG.log" >logfile.xml

Note the use of > to redirect the data to the file logfile.tsv.

Correct Display of National Characters in Exported Files
To ensure the correct display of national characters in the exported logs, display the CSV or TSV file in Excel after specifying the following settings (in Excel):

1. In the File drop down menu, select Open.
2. Select the exported CSV or TSV formatted log file and click Open.
3. When the text import guide is displayed, select the Origin:
   65001: Unicode (UTF-8)
4. Click OK.
Appendix H

Using IBM RRU or the Windows Recovery Console

This appendix contains the information you will need for accessing the IBM Rapid Restore Ultra (RRU) and the Windows Recovery Console on a Full Disk Encryption-protected computer.

Note - RRU support is available up to version 3.0 of IBM RRU. Versions later than 3.0 may not work.

Installing the InstallRRU.msi Package

Before you can access RRU functionality on a Full Disk Encryption-protected computer, you need to install the InstallRRU.msi package.

Note - Before you install the InstallRRU.msi add-on package, ensure that you have installed ISScript.msi Version 11 on the computer. Otherwise, InstallRRU.msi will not work correctly.

To install the InstallRRU.msi package:

1. Locate the InstallRRU.msi add-on package in the Resource Kit\Lenovo RRU directory on your Full Disk Encryption CD.
2. Install the package.
Accessing

After installing the InstallRRU.msi add-on package, you can access RRU functionality.

To restore a backup via RRU, do not access RRU through Windows but instead as described in the procedure below.

To access RRU functionality for restoring a backup:
1. Log on to the Full Disk Encryption preboot environment.
2. Immediately after you have logged on to Full Disk Encryption and before Windows starts to load, press F11. This will boot the machine into the RRU partition.
3. Select the backup you want to restore in RRU and continue.

Note - When using RRU on a Full Disk Encryption machine, never attempt to restore to an RRU image taken prior to the installation of Full Disk Encryption.

Accessing the Windows Recovery Console on a Full Disk Encryption Machine

The Windows Recovery Console provides system repair and recovery functionality. For example, you can use it to obtain limited access to the NTFS file system, FAT, and FAT32 volumes without starting the Windows graphical user interface (GUI).

Note - To be able to access the Windows Recovery Console on a Full Disk Encryption-protected machine, the Windows Recovery Console must have been installed on that computer before Full Disk Encryption was installed there.

To access the Windows Recovery Console on a Full Disk Encryption-protected machine, you must first execute the InstallMSRC.msi package.
To install the InstallMSRC.msi package:

1. Locate the InstallMSRC.msi package on your Full Disk Encryption CD; it is found under: 1_Pointsec for PC\Tools\MS Recovery Console.

2. Install the package.

The following log file is created during the execution of the InstallMSRC.msi package: C:\Program Files\Pointsec\Pointsec for PC\InstallMSRC.log.
Appendix I

Dual Boot Support for Windows XP and Red Hat Linux

This appendix describes the dual boot support provided in Full Disk Encryption.

Operating Systems and Linux Distributions Supported

Full Disk Encryption 7.0 dual boot functionality supports the following Windows operating system and Linux distributions:

- Windows XP SP2 or later
- Linux Kernel 2.6.4 or later
- Red Hat Enterprise Linux 4 Workstation
- Red Hat Enterprise Linux 5 Client
Setting Up a Dual Boot Environment That Runs Both Windows XP and Linux Red Hat with FDE

The text below provides a procedure you can use to set up a dual boot environment that runs both Windows XP and Linux Red Hat. It also provides information on troubleshooting.

**The Setup Procedure**

The following procedure can be used to set up the dual boot environment described above:

1. Install Windows XP SP2 on the first partition.
2. Install Linux on any other partition with GRUB as boot loader. Be sure to make a separate /boot partition.
4. Add the value `ChainToMBR=no` to the precheck.txt file.
5. Install Full Disk Encryption for Windows.
6. Boot into Windows again to start the encryption after the first reboot.
8. You should now have a system that can dual boot Windows XP and Red Hat Linux both running Full Disk Encryption. You choose which operating system to use via the GRUB bootloader.

**Troubleshooting**

If Windows will not boot from the GRUB Boot Loader after installing the FDE Linux Edition, check the /boot/GRUB/menu.lst configuration file. Ensure that the Windows entry points to the first partition.
The Precheck.txt File

Introduction

precheck.txt is an installation settings file designed to make installing Full Disk Encryption even simpler. By configuring precheck.txt, you can streamline the installation process and configure settings faster. The precheck.txt file is in the same folder as the Pointsec PC.msi file.

When you start to install Full Disk Encryption, the installation program reads precheck.txt and determines if it should terminate in certain circumstances as specified by you. You can also configure precheck.txt when installing on a computer running IBM Rapid Restore Ultra (RRU).

In addition, you can use precheck.txt to configure settings for third-party Graphical Identification and Authentication (GINA) dlls, Single Sign On (SSO) delay times, and licenses server matters.

precheck.txt settings can be altered after installation by editing them in the Pointsec registry key.
Accessing precheck.txt

To use precheck.txt during the installation:

1. Copy the contents of the Full Disk Encryption directory from the Full Disk Encryption CD to a directory on your computer.

2. In Windows Explorer, browse to the directory and open precheck.txt in any regular text editor.

3. Edit the file to suit your installation preferences and then save it.

4. To start your Full Disk Encryption installation, right-click on Pointsec for PC.msi and select Install.

Precheck Settings

In This Section

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AddFilter=Yes</td>
<td>This is a legacy setting for Windows Full Disk Encryption driver installation. It is no longer used.</td>
</tr>
<tr>
<td>SupportMultiProcessor=Yes</td>
<td>The value can be Yes or No. If the value is set to No, the installation will be terminated if either more than one processor or multithreading is detected. The default value is Yes.</td>
</tr>
</tbody>
</table>
AbortOnWindowsXP=No
The value can be Yes or No. If the value is set to Yes, the installation will be terminated if Windows XP is the operating system on the computer on which Full Disk Encryption is being installed. The default value is No.

AbortOnDualBoot=No
The value can be Yes or No. The default value is No. Yes will cause Full Disk Encryption to terminate an installation on a dual boot system.

IgnoreOldInstallation=No
Set this setting to Yes to enable support for re-installing on selected volumes while keeping old installations on other volumes.

Note - You must use the same user accounts in both installations.

Note - A re-installation of the boot volume requires all volumes to be protected by Full Disk Encryption.

Run=
Here you can enter a program to run before Full Disk Encryption is installed.

RunAfter=
Here you enter the path to scripts or execs that you want run immediately after the user logs on to Windows after the reboot that follows the installation of Full Disk Encryption. For example:

- The path to the script required when installing in an IBM RRU environment.
- The path to the dotnetfx.exe to install the .NET Framework if it is not already installed on this machine. The dotnetfx.exe is found in the Full Disk Encryption directory:
  Pointsec for PC\1_Pointsec_for_PC\Tools\DotNetRunTime\dotnetfx.exe

Note - Best practice is to specify the path in UNC format: \\<server>\<share>\....
Together with `Drivers=` this setting is used to deploy the HID driver, found under `/modules/hid`. For example:

- `Drivers=HID\hptc1100.bin`
- `HidInf=HID\hptc1100.inf`

The HID driver enables the pen on tablet PCs.

See the current Release Notes for available drivers.

**Note** - If you have installed a Wacom driver on a computer that does not have Wacom hardware installed, this can cause hanging during preboot. To avoid this, hold both Shift keys down while the progress bar is visible during the loading of Full Disk Encryption preboot. A new menu selection, **HID drivers**, will be displayed, allowing you to disable the Wacom driver(s).

**Note** - You can also deploy HID drivers after installation using `pscontrol.exe`. For example:

- `C:\>pscontrol register-hid hptc1100.inf`
- `C:\>pscontrol install-driver hptc1100.bin`
### Table J-1  General Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Drivers=    | The value of this setting specifies the preboot smart card drivers that will be installed together with the Full Disk Encryption system. These drivers enable communication between a smart card and Full Disk Encryption prior to the start of Windows.  

The specified value for this setting must be a semicolon-separated list of file names with no paths specified and no blanks. For example:  

\[
\text{Drivers=} \text{msc}_{\text{p}11}.\text{bin;prd}_{\text{ccid}}.\text{bin}
\]

Available drivers are located in the Modules folder.  

With the help of this facility, it is possible to use a smart card to log on at initial authentication.  

See the description of HidInf=, above, for information on using Drivers= to deploy HID drivers. |
| CSPRandom=  | This setting specifies the name of the Cryptographic Service Provider (CSP) to use for random number generation during installation. The CSP name is vendor specific, and it can normally be found in the documentation for the CSP.  

The CSP must be installed on a machine's Windows system prior to Full Disk Encryption installation.  

The Full Disk Encryption installation program will attempt to use the CSP specified in this setting to generate random numbers. The CSP's random number generation is vendor specific, and it might require the presence of external hardware, for example, a smart card.  

If the random number generation fails, the installation is aborted. |
Table J-1  General Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ShowRecoverMessages=</td>
<td>This setting specifies whether or not the message box related to the unavailability of the recovery path will be displayed to the user.</td>
</tr>
<tr>
<td></td>
<td><strong>Yes</strong> = Display the message box related to the unavailability of the recovery path to the user.</td>
</tr>
<tr>
<td></td>
<td><strong>No</strong> = Do not display the message box related to the unavailability of the recovery path to the user.</td>
</tr>
<tr>
<td></td>
<td>No is the default.</td>
</tr>
<tr>
<td>ExtendedLogging=</td>
<td>This setting specifies whether or not log events containing the status of all user accounts and groups will be written to the central log file.</td>
</tr>
<tr>
<td></td>
<td><strong>Yes</strong> = Write log events containing the status of all user accounts and groups to the central log file.</td>
</tr>
<tr>
<td></td>
<td><strong>No</strong> = Do not write log events containing the status of all user accounts and groups to the central log file.</td>
</tr>
<tr>
<td></td>
<td>No is the default.</td>
</tr>
<tr>
<td>KeyImportDirectory=</td>
<td>The path to the key import directory.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> - Specifying a path for this setting activates encryption key import.</td>
</tr>
<tr>
<td></td>
<td>Best practice is to specify the path in UNC format: <code>\\server\\share\\...</code>.</td>
</tr>
</tbody>
</table>
This setting specifies how the imported random data will be processed when using it to make keys.

- **Combine** = Partition keys are generated by combining the imported random data with random data generated by Full Disk Encryption. Data used to protect partition keys is generated by combining partition keys with random data generated by Full Disk Encryption.

  ‘Combine’ is the default: if nothing is specified for this setting, the ‘Combine’ method will be used.

- **Direct** = The imported random data is used ‘as is’ as a partition key. Data used to protect partition keys is generated by combining partition keys with random data generated by Full Disk Encryption.

  You cannot use the key import directory’s `PWD.DAT` file when using the ‘Direct’ method.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KeyImportMethod=</td>
<td>This setting specifies how the imported random data will be processed when</td>
</tr>
<tr>
<td></td>
<td>using it to make keys.</td>
</tr>
<tr>
<td></td>
<td><strong>Combine</strong> = Partition keys are generated by combining the imported random</td>
</tr>
<tr>
<td></td>
<td>data with random data generated by Full Disk Encryption. Data used to</td>
</tr>
<tr>
<td></td>
<td>protect partition keys is generated by combining partition keys with random</td>
</tr>
<tr>
<td></td>
<td>data generated by Full Disk Encryption.</td>
</tr>
<tr>
<td></td>
<td>‘Combine’ is the default: if nothing is specified for this setting, the</td>
</tr>
<tr>
<td></td>
<td>‘Combine’ method will be used.</td>
</tr>
<tr>
<td></td>
<td><strong>Direct</strong> = The imported random data is used ‘as is’ as a partition key.</td>
</tr>
<tr>
<td></td>
<td>Data used to protect partition keys is generated by combining partition keys</td>
</tr>
<tr>
<td></td>
<td>with random data generated by Full Disk Encryption.</td>
</tr>
<tr>
<td></td>
<td>You cannot use the key import directory’s <code>PWD.DAT</code> file when using the</td>
</tr>
<tr>
<td></td>
<td>‘Direct’ method.</td>
</tr>
</tbody>
</table>
GINA Settings

You can set the following Graphical Identification and Authentication (GINA) options:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CompatibleGinas=</td>
<td>Here you can enter the names of compatible Graphical Identification and Authentication (GINA) dlls, separated by semi-colons (;), e.g. CompatibleGinas=xx1.dll; xx2.dll; xx3.dll No value specified is the default. Enter the names of GINAs that you would like Full Disk Encryption to attempt to perform SSO to.</td>
</tr>
</tbody>
</table>

**Note:** The GINAs may not actually be compatible with Full Disk Encryption Single Sign-on (SSO).

Central Log Transfer Settings

Here you can specify how the central log transfer should be managed.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogTransfer=</td>
<td>This setting determines whether or not Windows log transfer process is enabled. The possible values are: 0 = Do not transfer the log file to Windows Event log. 1 = Transfer the log file to Windows Event log.</td>
</tr>
</tbody>
</table>
License Server Settings

Here you can specify settings related to the operation of the license server.

**Table J-4  License Server Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LicenseServerInitialStartDelay=</td>
<td>This setting determines the length of the delay after booting before making the first attempt to access the license server shared folder.</td>
</tr>
<tr>
<td>LicenseServerScanTimeout=</td>
<td>This setting determines the length of the interval between the successful storage of the license request file and the scan for the license response file.</td>
</tr>
</tbody>
</table>
**Single Sign-On Settings**

Here you can specify how the single sign-on (SSO) settings.

**Table J-5  Single Sign-On settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| UpdateSSO=0     | This setting determines how Full Disk Encryption handles third party GINAs. The default value is 0. The following values are permitted:  
0 This is the default value. Whenever the computer is started or shutdown, Full Disk Encryption will check if any GINAs have been added, and if so it will rebuild the GINA order. Pssogina.dll will always be set as the active GINA.  
1 Full Disk Encryption maintains Pssogina.dll as the active GINA. Full Disk Encryption checks every 10 seconds for registry changes to GINA order. If there are any changes, for example, if Pssogina.dll is replaced by nwgina.dll, Full Disk Encryption will rebuild the GINA order so that Pssogina.dll is the first GINA.  
2 The same as 1 but Full Disk Encryption also checks that the files associated with the GINAs are actually physically present. If a file has been removed, Full Disk Encryption deletes the GINA entry in the registry. For example, if a user removes the file associated with nwgina.dll, Full Disk Encryption discovers that the file is missing, removes the entry nwgina.dll from the registry and moves the next GINA up automatically. Pssogina.dll is always the first GINA.  
4 Full Disk Encryption will not make any changes. If a new GINA is added, this will be the active GINA on the system. If Pssogina.dll is replaced, this option will disable Full Disk Encryption SSO, password synchronization, and smart card support. |
| SSODelay_NWGINA= | Here you can specify the delay before performing SSO with a Novell login. The default is 5000 milliseconds (ms). The minimum value is 0 ms, and the maximum is 60000 ms. This setting can be useful when you need to correct problems with SSO caused by slow systems. |
Here you can specify the delay before performing SSO with a Windows XP login. The default is 2000 milliseconds (ms). The minimum value is 0 ms, the maximum value is 60000 ms. This setting can be useful when you need to correct problems with SSO caused by slow systems.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSODelay_MSGINA=</td>
<td>Here you can specify the delay before performing SSO with a Windows XP login. The default is 2000 milliseconds (ms). The minimum value is 0 ms, the maximum value is 60000 ms. This setting can be useful when you need to correct problems with SSO caused by slow systems.</td>
</tr>
</tbody>
</table>
Appendix K

Msiexec.exe Commands

This appendix describes Msiexec.exe commands that Full Disk Encryption supports.

Remove the Start Menu

To remove the Start menu from a client installation, run the following command:

Msiexec.exe /i "Pointsec for PC.msi" DISABLE_START_MENU=1

Disable the FDE Preboot Environment

This feature keeps the FDE preboot components intact while re-imaging the Windows part of the system. It is used only in rare cases, and is done by using an FDE-prepared image on a volume that is still fully encrypted. The administrator can then install/image over the Windows components that are missing or need to be replaced.

To disable the FDE preboot environment on a client installation, run the following command:

Msiexec.exe /i "Pointsec for PC.msi" DISABLE_PBA_INSTALL=1
Disable the FDE Preboot Environment
Using a Service Start Account

In This Appendix

Full Disk Encryption Service Start Service Program - pstartsr.exe

This appendix describes the Full Disk Encryption Service Start service. It also describes the creation of a Windows account you assign to run the service. Together, the service and the account allow you to strictly limit the permissions of the user accounts on client machines while still enabling those machines to access to the file share on which profiles, upgrades, recovery files, and log files are stored.

This chapter provides:

- General information on the Full Disk Encryption Service Start service. See “Full Disk Encryption Service Start Service Program - pstartsr.exe” on page 252 for details.

- Guidance in defining the Windows user account that will run the service and in including this user account in the Power Users group. See “Defining the Windows User Account That Will Run the Service” on page 253.

- Instructions on how to assign Log on as a service rights to this Windows user account. Log on as a service and Manage auditing and security log rights are required for the Windows user account to be able to run the service. See “Specifying the Service Start Account and Password in Full Disk Encryption” on page 254.

- Instructions on how to specify the Windows user account in Full Disk Encryption so it will be used to access the file share on which profiles, upgrades, recovery files, and logs are stored. See “Defining the Windows User Account That Will Run the Service” on page 253.
Full Disk Encryption Service Start Service Program - pstartsr.exe

In This Section

- Setting up the Full Disk Encryption Service Start Account page 252
- General Requirements page 256
- What does the Full Disk Encryption Service Start Service Do? page 256
- Example of Setup page 257
- Upgrade from Pointsec for PC 4.x/5.x Installations page 258

The Full Disk Encryption Service Start service is the pstartsr.exe program. It is added to the Windows services when Full Disk Encryption is installed.

To view the service:
1. In the Start menu, right-click My Computer and click Manage.
2. In the Computer Management window, click Services and Application.
3. To view Full Disk Encryption service start properties, right-click it and select Properties. The Full Disk Encryption service start Properties window is displayed.

Setting up the Full Disk Encryption Service Start Account

The account assigned to the Full Disk Encryption Service Start service must be a domain or Microsoft Active Directory account in order to allow the service to authenticate across the client systems and file share properly.

It is also strongly recommended that this account be treated as a service account, not a normal user account. Additional specific authorization and restrictions (enforced by Group Policy Objects [GPOs] or system policies) should be applied to the service account.

A strong and lengthy password is also recommended to secure this service account.

To use the Full Disk Encryption Service Start service you must perform the following steps, which are elaborated on the following pages:

- Define the Windows user account and password that will run the service.
• Assign **Log on as service** and **Manage auditing and security log** rights to the Windows user account that will run the service.
• Specify the Windows account that will run the service and its password in Full Disk Encryption.

**Defining the Windows User Account That Will Run the Service**

To define the Windows user account that will run the service:
1. On the **Control Panel**, click **User Accounts**.
2. Select the **Advanced** tab.
3. Click **Advanced**.
   The **Local Users and Groups** window is displayed.
4. Right-click **Users** and select **New User...**
5. Enter the **User name** of the user account, enter a password, confirm the password, and click **Create**.
   The Windows user account that will run the service has now been created.
   You must still assign **Log on as a service** rights to this user account, and you must specify this account to Full Disk Encryption. Both these steps are described below.

**Assigning 'Log on as a service' Rights to the User Account**

To assign 'Log on as a service' rights to the user account defined via the Control Panel:
1. On the **Control Panel**, click **Administrative Tools**.
2. In the **Administrative Tools** window, click **Local Security Policy**.
3. In the tree structure on the left side of the window, under **Security Settings/Local Policies/User Rights Assignment**, click **Log on as a service** and **Manage auditing and security log**.
4. Click **Add User or Group**.
5. Do one of the following:
   – Enter the domain and user account name, then click **OK**.
Setting up the Full Disk Encryption Service Start Account

- Click **Advanced**, then on the **Select Users or Groups** window click **Find Now** and select the user account you have defined to run the service.

You still need to specify this account to Full Disk Encryption so it will use this account to access the share and its directories. This is described below.

**Specifying the Service Start Account and Password in Full Disk Encryption**

The Windows user account and password required to run the Full Disk Encryption Service Start service must be specified for Full Disk Encryption in one of the following ways:

- Via the FDEMC
- During a manual (local) installation
- In an installation profile
- On the **Log on** tab of the **Full Disk Encryption service start Properties** window

**Via the FDEMC**

To specify the domain name and user name you want to run the Full Disk Encryption Service Start account in the FDEMC:

1. In FDEMC, go to **Local** and select **Edit Settings**.
2. Under **System Settings → Install**:
   a. Click **Full Disk Encryption Service Start Account**,
   b. Enter the domain and user name (in the form: [Domain]\[Username]) in the **Username** text box,
   c. Enter and confirm the password in the **Password** and **Confirm Password** text boxes respectively,
   d. Optionally, click **Verify** if you want the FDEMC to check whether or not you can log on to Windows with the Windows user account and password you have specified.
   e. Click **OK**.

**During a Manual Installation**

To specify the Windows account and password during a manual installation:

1. In the **Access to network paths** window, select **Use a configured Windows account for access to the network path(s)**.
In an Installation Profile

To specify the domain name and the username when creating or editing a profile:

1. Under System Settings → Install:
   a. Click Full Disk Encryption Service Start Account,
   b. Enter the domain and user name (in the form: [Domain]\[Username]) in the Username textbooks,
   c. Enter and confirm the password in the Password and Confirm Password text boxes respectively,
   d. Optionally, click Verify if you want the FDEMC to check whether or not you can log on to Windows with the Windows user account and password you have specified.
   e. Click OK.

On the Log On Tab of the Full Disk Encryption Service Start Properties Window

The Windows user account and password can be specified on the Log On tab on the Full Disk Encryption service start Properties window. This window (but not the Log on tab) was described above.

To specify the Windows user account and password on the Log On tab on the Full Disk Encryption service start Properties window:

1. Select the Log On tab on the Full Disk Encryption service start Properties window.
2. Select This account: and enter a valid Windows domain and username in the format Domain\Username, for example Domain_A\Run_P4PC_service.
3. Enter a valid Windows password, confirm it and click OK.

Note - If you define the Windows account and password in this way, the account is automatically assigned Logon as service rights, which are required to run the service. See other requirements, below.

The Windows user account can also be defined via User Accounts in the Control Panel.
General Requirements

**On the Local PC**

- The logged-on user account requires **List, Read, Write, Execute, Modify** and **Delete** permissions to the local Pointsec for PC program folder, generally: C:\Program Files\Pointsec.
- The logged-on user account requires full permissions to the Full Disk Encryption registry items on the client PC, generally: HKEY_LOCAL_MACHINE\SOFTWARE\Pointsec Mobile Tech\Pointsec for PC.
- The account configured as the Full Disk Encryption Service Start service requires **List, Read, Write, Execute** and **Modify** permissions to the local Full Disk Encryption program folder, generally: C:\Program Files\Pointsec.
- The account configured as the Full Disk Encryption Service Start service must be a member of the Administrator group on the local PC.
- The account configured as Full Disk Encryption Service Start service requires full permissions to the Full Disk Encryption registry items on the client PC, generally: HKEY_LOCAL_MACHINE\SOFTWARE\Pointsec Mobile Tech\Pointsec.

**On the Network share**

- The user account logging on to the local client PC requires no permissions on the network share once service is configured.
- The account configured as **Full Disk Encryption Service Start** requires full control to the network share.

**What does the Full Disk Encryption Service Start Service Do?**

Once the Full Disk Encryption Service Start service is configured, it handles:

- Creation of the recovery file and the log file
- Download of update profiles placed in the update path
- Download of system upgrade packages (patch files)
**Limitations**

**Computer-specific Update Profile Folder**

A computer-specific update profile folder is not created in the update profile path, since this is not done via the Full Disk Encryption Service Start service but by a process running in the user context (currently).

![Note - If the folder is created manually, it will be used as normal.]

**Software Updates**

Software updates are downloaded and completed on the local PC, but the upload of the log files from the update is not transferred, since this is not done via the Full Disk Encryption Service Start service but by a process running in the user context (currently).

**Workaround Possibility**

In this scenario it is possible that a package can be written for provision through a login script or systems management tool that executes `C:\Program Files\Pointsec\Pointsec for PC\PpupdLog.exe` with a `Run As` operation, where the user account has the necessary rights to the Full Disk Encryption file share.

**Example of Setup**

The following is an example of the setup:

1. Create a domain-wide account (hereafter called **ServiceAccount**) that all client PCs within the organization can use (e.g., added to the Power Users on each machine via GPO). This account also needs to be present on the local machines with the permissions described above.

2. Create a network share and assign full permission on the share, including sub-folders and content to the ServiceAccount. Other permissions can be set as desired.

3. Install Full Disk Encryption.

4. Set the Full Disk Encryption Service Start service to log on with the ServiceAccount.
If configured correctly, the creation of recovery file, download of update profiles and download of software upgrades is now performed via the account assigned to the Full Disk Encryption Service Start service.

**Note** - If you are installing by means of an install profile, the Full Disk Encryption Service Start service can be configured prior to rebooting the system when completing the installation. Doing so should avoid a possible -2 error when logging on (caused by limited permissions for the logged-on user to the recovery folder).

### Upgrade from Pointsec for PC 4.x/5.x Installations

**Note** - During upgrade from Pointsec for PC 4.x/5.x, the 4.x/5.x version of the Full Disk Encryption Service Start Service is removed; and information about the account configured to run the service is lost. The service must therefore be reconfigured in order to function correctly.

The Full Disk Encryption Service Start service allows system administrators to limit user access to the Full Disk Encryption network share and the respective recovery, update profile, and software update directories. Authentication to the share is made with the account assigned to the Full Disk Encryption Service Start service.

**Note** - This documentation does not cover permissions required to install Full Disk Encryption from a network share.
Appendix M

Full Disk Encryption Common Criteria Configuration

In This Appendix

Introduction  page 259
Common Criteria EAL4 Configuration Requirements  page 260

Introduction

Common Criteria (CC) defines a broad, flexible set of requirements for security products, focusing on development best practices and assurances that advertised features have been implemented securely. With a CC EAL4-validated product, you are assured that the product is designed according to strict security engineering standards and quality control.

The CC is a set of functional and assurance IT security requirements that were developed to provide a common baseline against which IT products and systems could be tested and evaluated. The results of these comprehensive security tests are compiled to produce a composite security score or evaluation level for any given security product. The CC evaluation methodology can be used for both hardware and software security products.
Initially supported by the United States, United Kingdom, Germany, France, Canada, and the Netherlands, the CC has since been recognized by many other countries. Evaluations consider not only the product itself, but the intended environment for use and the policies and procedures that will be enforced. The CC has also been codified as ISO standard 15408.

Check Point Software Technologies Ltd. provides world-class security software for the protection of personal computers, smart phones and PDAs. A commitment to achieve CC EAL4 validation is part of the ongoing process of providing the highest quality security products to our most important security partners, our customers.

Common Criteria EAL4 Configuration Requirements

In This Section

Cryptographic Algorithms and Key Sizes.......................... page 261
Cryptographic Key Destruction....................................... page 261
All Partitions Encrypted, Boot Protection Enabled.............. page 261
No Delete Access to the Full Disk Encryption File Share...... page 262
Wake on LAN................................................................ page 262
Windows Integrated Logon.............................................. page 262
User Level Permissions.................................................. page 262
Local Administration Disabled....................................... page 263
Administration and Configuration via Profiles............... page 263
Software Upgrade between Common Criteria Versions Only page 263
Password Requirements............................................... page 263
Password Synchronization Requirements........................ page 263
Maximum Failed Logons before Reboot......................... page 264

The validation of Full Disk Encryption is done in a specific secure configuration. To use Full Disk Encryption as a validated product, this configuration, described in the paragraphs below, must be used on the installed computer. To properly implement a CC EAL4-validated configuration of Full Disk Encryption, specific settings described below must be configured in the profile that will be deployed.
When performing cryptographic operations related to smart card authentication, x.509 certificates should be used; and RSA PKCS#1 version 1.5 should be followed, with key sizes 1024, 2048, or 4096 bits.

**Cryptographic Algorithms and Key Sizes**

The algorithms and key sizes allowed in a CC configuration are:

- 3DES (key size 168-bits)
- AES (key size 256-bits)

**Cryptographic Key Destruction**

Key destruction should be performed in accordance with FIPS 140-2 Level 1, Section 4.7.6 Key Zeroization.

**All Partitions Encrypted, Boot Protection Enabled**

To ensure that the system is secure, all partitions must be encrypted and preboot protection must be enabled.

**Note** - The Profile functionality provides (among others) the capability to restrict the ability to initialize and delete the partition keys to authorized administrators. A FIPS 140-2 approved PRNG is used for generating secure random values.

**In an Installation Profile**

Use the Select Volume Protection setting under System Settings → Install to:

- specify the algorithm to be used
- select **Encryption** for all the volumes, and
- select **Preboot Auth.** (preboot authentication) for all volumes.

**In a Master Installation**

Select **Boot protection** and **Encryption**, then choose the required algorithm in the **Protect volumes** InstallShield Wizard window.
No Delete Access to the Full Disk Encryption File Share

Users of Full Disk Encryption-protected computers may have only RX permissions to the Full Disk Encryption share. This is accomplished by setting up a Full Disk Encryption Service Start Account in the Full Disk Encryption profile deployed on computers. See Appendix L, “Using a Service Start Account” on page 251 for instructions.

Note - Profiles, upgrades, recovery files, and log files are encrypted and integrity protected when transferred to/from the file share.

Wake on LAN

The setting Enable Wake on LAN must be disabled. This setting is found under System Settings → Wake on LAN. Wake-on-LAN is a feature in many computers today whereby the computer can be automatically started when it receives a specific signal from the network. The administrator can then perform maintenance on the computer without having to visit its physical location.

Windows Integrated Logon

The setting Windows Integrated Logon must be disabled. This setting is found under System Settings → Windows Integrated Logon. Windows Integrated Logon enables a user to bypass preboot authentication at startup.

User Level Permissions

The user account must not have any administrative privileges, and must not have more than permissions than View Logs and Uninstall. These settings are located under Groups → System → Group Settings → Permissions for groups and under Account Settings → Permissions for each user account.

The View Logs permission is only necessary if normal users are allowed to view the logs of the system in question. The Uninstall setting will allow a user to uninstall the Full Disk Encryption software from the computer if, and only if, the uninstallation is performed together with an administrator (or another user) who has Uninstall authority.
Local Administration Disabled

The local administration program must be disabled for all clients, that is, machines not used for system administration and administration, e.g. creating profiles, updating profiles and providing remote help. The setting Management Console Logon must be disabled on all clients. These settings are located under Groups → System → Group Settings → Permissions for groups and under Account Settings → Permissions for each user account.

Administration and Configuration via Profiles

All administration and configuration of client installations must be performed via profiles. The only local administration allowed is the first initial administration of an administration installation that, which is then used to create an initial installation profile to be used to install the clients. All updates and new installation profiles for both clients and administration machine are then maintained via profiles, created on an administration installation. In a Common Criteria validated environment, only silent installation profiles should be used to deploy Full Disk Encryption.

Software Upgrade between Common Criteria Versions Only

Only upgrading between CC-certified versions of Full Disk Encryption is allowed.

Password Requirements

If fixed passwords are used for authentication, they should match the strength requirements of the information they are protecting. The required configuration is:

- Minimum length of 8 characters
- Numbers and letters
- Both uppercase and lowercase letters
- No more than two consecutive identical characters

The following configuration is recommended, but not required:

- Disallow 6 previous passwords
- Expiration of 90 days
Password Synchronization Requirements

These recommendations do not apply to users using dynamic tokens or smart cards for authentication.

**Password Synchronization Requirements**

Password synchronization must be inactivated in a CC-validated environment.

**Maximum Failed Logons before Reboot**

The value of *Max Failed Logons Before Reboot* must be set to three or fewer in a CC-validated environment.
Index

Numerics

3DES algorithm 111

A

to access
Local 86
local settings 99
management console 98
Remote 86
settings 97
account(s)
access to Local, allow 86
access to Remote, allow 86
add user to group 108
administrator 136
create group 107
create in profile 127
group account, add user 108
groups, create and edit 85
groups, remove 85
move user accounts between groups 107
name 109
password authentication 109
password change, forced 110
permissions when uninstall 175
service start, see service start account
temporary user, delete 128
temporary user, settings 109
token authentication 110
types of user accounts 16
user accounts, create and edit 84
user accounts, remove 85
Active Directory server, set up 90
admin rights on Windows Vista 132
administrator accounts 136
algorithm(s) 47, 261
algorithm, tokens 111
Allow Windows Screen Saver system setting 26
anonymous logon (Entrust) 91
Apache server 193
assistance, end-user 170
authentication
methods 105, 109
passwords 109
settings 70
smart cards 112
tokens 110
authority, extend 14, 15
authorization
logon 68
preboot 47
automatic reboot 159

B

background image
preboot 157
banner 157
preboot 157
Banner.jpg 157
boot protection 9
bootable CD-ROM 187
bootable media 180
case sensitivity 72
CD-ROM
boottable 187
central log
file 133, 163, 166
path 44
permissions 203
transfer settings 244, 245
certificate(s) 113
challenge(s)
characters, number of 53
format 111

C

data security types 8
database, local 162
compatibility, slavedrives 191
IIS server 193
images in preboot 157
import configuration set 118
install profile(s)
create 124
deploy 124, 130
silent 124
types of 121
installation interactive 122
local 14
on Windows Vista 132
path 114
permissions 202
remote 14
settings 35
silent 122
status information exported to file 197
InstallMSRC.msi package 232
InstallRRU.msi package 231
introduction to Full Disk Encryption 7

K
key(s)
protection 49
sizes 261
tokens 111
keyboard layouts changing 213
default 213

L
language
change language files 37
language files change 37
language(s)
available 36
configuring those available on clients 208
configuring those used on client 208
fallback language 207
files, Windows 204
list of supported 15, 209
specify FDEMC language 207
support 207
LANGUAGE.LNZ files 37
legacy versions 142
license(s)
message, activation 50
message, deactivation 50
number 49
server password 49
derver path 49
settings 49
local
database 162
file, logging 162
log file 162
lockout time 76
logon(s)
central 133, 166
central, transfer settings in precheck.txt 244, 245
export 227
extended logging 164
file, central 163
file, local 162, 165
password 39
transfer 164
transfer local to central 164
view 81
logon(s)
after Wake-on-LAN 61
allow to management console 81
anonymous (Entrust) 91
change to dynamic token 81
change to fixed password 81
change to smart card 81
failed, WIL 65
management console, skip 51
maximum failed 51
maximum failed attempts 76
maximum successful 76
one-time 83, 168
one-time, see also Remote Help
settings 51, 76
temporary lockout time 76
temporary lockout, failed attempts 76
to hibernated system 81
verification time 51

M
management console
access 98
allow logon 81
encryption information 25
local installation 14
menu bar 14
no logon 51
overview 12
permissions 203
remote installation 14
specify language used 207
status information 24
managing groups and user accounts 107
manual reboot 159
memory dumps 52
msi package deploy 131
parameters, supported 132
msiexec.exe commands 193, 249
upgrade with 158

N
national characters, correct display in exported files 230
network location, WIL 65
network locational awareness 62, 65

O
oemvar 157
OneCheck Logon settings 26
OneCheck Logon and single sign-on 87
OneCheck Logon system
setting 27
one-time logon(s) 168
provide 83
receive 84
operating systems
dual boot support 235
menu option 15

password(s)
age, maximum 73
age, minimum 72
authentication, new user account 109
case sensitivity 55, 72
case, upper and lower 55
change 80
change to fixed, allow 81
change with Remote Help 168
change, forced 110
characters, adjoining 55
characters, identical 55
characters, special 55
Common Criteria requirements 263
compatibility level (UVP) 38
consecutive, identical characters 72
embedded space 72
fixed 71
fixed, security standards for 70
history 73
leading or trailing space 72
length, minimum 55, 72
letters and digits 55, 71
license server 49
log 39
policy settings 54
remote password change 83
see also Remote Help
space, embedded 55
space, leading or trailing 55
special characters 72
synchronize preboot password to Windows 77, 79
synchronize Windows password to preboot 77, 78
update validation password 38
upper and lower case 72
Windows complexity requirements 55
path(s) 113
central log 44, 115
configuration sets 114
install 114
license server 49
PKCS#11 dll 46
profile storage 114
recovery 43, 115
update profile 114
update profiles 42
upgrade 40, 115
PC security overview 7
permission(s)
central log 203
change 84
create recovery media 180
FDEMCUtil 204
install 202
management console 203
privileged permissions, change 84
privileged permissions, settings 84
PS Control 204
recovery disk, create 203
recovery file, create 203
recovery, perform 180
remove 202
required by Full Disk Encryption 201
service start account, with 204
service start account, without 205
settings 80
tray 203
uninstall 202
Windows user account registry 206
personal store 113
PKCS#11 dll path 46
Plang32.Lang files 37
Pointsec for PC
upgrade to FDE 142
Pointsec for PC.msi 105
Pointsec Media Encryption 106
Pointsec registry Encryption 106
PointsecForPC.resources.dll 37
preboot
authorization 47
background image 157
banner 157
encryption 47
environment, disable 195, 249
graphic images 157
low graphics mode 29
mouse 29
PCMCIA devices 29
screen saver, image 157
USB devices 29
Windows Integrated Logon, message 66
Windows Integrated Logon, switch 65
preboot drivers setting 30
precheck.txt
accessing 238
central log transfer settings 244, 245
description 106
driver, add 129
general settings 238
GINA 106
GINA settings 244
Single Sign-On settings 106, 246
print settings 66, 100
profile(s)
about 120
allow account to create 85
base on existing profile 126, 129
base on local settings 126, 129
check for update profiles 138
convert pre-6.2 to 6.3.1 130
definition 20
differences between remove and mark for removal 134
difference older versions 85
effect of updates on users 139
force check for update profile 139
group information 121
groups and user accounts, create 127
install, create 124
install, deploy 130, 131
install, description 121
install, interactive 122
install, silent 122
name 126
open older versions 85
publish directly from profile list 119
recommendations 123
remove, allow to 85
revoke (Entrust) 89
storage path 114
system information 121
uninstall 123, 174
uninstall, create 174
uninstall, permissions 202
update 122
update path 42, 114
update profiles to specific computer, deploy 138
update, create 134
update, push 139
upgrade 123
user information 121
what's in a profile 121
PS Control
command format 216
commands 217
call error codes 218
example status file 223
export status information 221
location 216
options 216
permissions 204
smart cards, readers, and drivers 219
status file, export 221
pslogexp.exe 227
national characters, correct display 230
syntax and commands 228
push profile 139

R

RAM, key protection 49
Rapid Restore Ultra

functionality on FDE machine 232
installing msi package 231
reboot
automatic 159
manual 159
recover
by slaving a hard disk 190
recovery
alternative boot menu 188
alternative media, from 188
bootable media 180
CD-ROM, create 187
decryption, and 188
disk, create 183, 203
file path not found 182
file, name 133
file, number of 133, 181
file, storage 181
media, allow create 81
path 43, 115
permissions 180, 203
Remote Help, slave drive 192
slave drive 192
slave drives, from 189
update of file 181
USB device 188
Volume Recovery Utility 183
Wake-on-LAN, slavedrive 191
Windows Integrated Logon, slave drive 192
registry
key, Pointsec 106
permissions 206
values, for logging 164
related documentation 3
Release Notes 105
Remote Desktop permissions 206
Remote Help
enable 53
disable user account name 170
disable user assistance 170
derector account name 170
derector authentication 171
implementing 167
one-time logon 168
providing 169
remote password change 168
response format 84
response, generate 170
settings 83
Single Sign-On 168
slice drives 192
smart cards 168
system settings 53
types of 168
verifying users 169
remote password change provide 83
receive 83
removal
permissions 202
start menu 193, 249
Windows add/remove 175
remove vs mark for removal 134
response(s)
format 84, 111
length 111
Remote Help, generate in 170
root path 113
RRU, see Rapid Restore Ultra

S

SATA
compatibility, slavedrives 191
screen saver 157
activation time 68
image in preboot 157
Windows Integrated Logon, timeout 66
Scrsvr.jpg 158
SCSI
compatibility, slavedrives 191
security standards
serial number 49
serial number, tokens 111
serial over LAN 29
server, active directory 90
service start account
format 48
limitations 257
permissions 204
reconfiguration 258
requirements 256
setting up 252
sets, see configuration sets
setting
File Transfer Delay 45
Preboot Drivers 30
setting(s)
  access 97
  configure 97
  group 67
  print 66, 100
Single Sign-On 87
system 86
Single Sign-On
  change 80
  enable 87
  Entrust 87, 89
  Entrust, profile
    revocation 89
precheck.txt 106
settings 87
settings in precheck.txt 246
smart card trigger
  Windows 87
single sign-on 87
slave drive(s)
  access 190
  authentication 191
  compatibility 191
  connectors 190
  hibernation 192
  recovering information from 189
  Remote Help 192
  uninstall 192
  Wake-on-LAN 191
  Windows Integrated
    Logon 192
smart card
  removal 75
  trigger Windows SSO logon 87
smart card drivers
  adding 30
  removing 33
smart card reader drivers
  adding 30
  removing 33
smart card(s)
  allow change to smart card
    logon 81
    authentication 112
    driver, register 217
    drivers, deploy 129
insertion/removal handling 75
installing with PS Control 220
personal store 113
reader driver, register 217
registering with PS Control 220
same certificates for two users 113
temporary user 17
special characters 72
start menu, remove 193, 249
status information
  example export file 223
  export using PS Control 221
  file, export 39, 197, 199, 221
  installation 197
storage, recovery file 181
synchronization
  passwords 77
  users 139
  synchronize passwords 77
system administrator,
  privileges 108
system setting
  Allow Windows Screen Saver 26
  Enable OneCheck Logon 27
system setting(s)
  access 99
  hardware device 28
  install 35
  license 49
  logon 51
  OneCheck Logon 26
  Remote Help 53
  user account acquisition 56
temporary user, delete 128
time interval for profile checks 138
timestamps 165
token(s)
  add values by import 111
  add values manually 111
  algorithm 111
allow change to dynamic token 81
authentication 110
challenge, format 111
challenge, length 111
FIPS compliant 109
keys 111
removal handling 75
response, format 111
response, length 111
serial number 111
tray
  credentials 82
language, change 209
permissions 203
Windows Integrated
  Logon 65
troubleshooting 259
type of user accounts 109

U
uninstall profile(s) 123, 174
description 174
using 174
uninstall profiles
deploying 175
uninstallation
  account permissions 175
  allow 81
  management console, using 174
  permissions 202
  slave drives 192
  Windows add/remove, using 175
update profile(s)
  check for, predefined time 138
  create 134
  deploy 138
  deploy to specific computer 138
description 122
effect on users 139
path 42
Pointsec for PC 258
push 139
update profiles
deploying drivers with 122
deploying language files with 122
update validation password 38
compatibility level 38
upgrade log 159
path 40, 115
Pointsec for PC 142
profile 123
user account acquisition settings 56
user account(s)
authentication method 109
registry permissions 206
temporary, settings 109
types of 16, 109
user accounts, differentiating without GUIDs 135
user acquisition configuration 56
configuration filter 58
groups 57
period 57
settings 57
user(s)
change GUID 85
normal 16
service 16
temporary 16
temporary, more than one 17
UseRec.exe 180
UVP, see update validation password

W

Wake-on-LAN enable 61
expiration date 61
logons, maximum 61
settings 59
slave drives 191
start delay 61
Windows logon 61
WIL, see Windows Integrated Logon
Windows
Add/Remove programs 175
complexity requirements 55, 71
Event Log 165
language files 204
Recovery Console, accessing 232
Smart Card Insertion/Removal Handling 75
user account, registry permissions 206
Vista, admin rights on 132
Vista, installing on 132
Windows Integrated Logon administrator perspective 63
hardware hash 62, 66
logons, failed 62, 65
message 64
network locational awareness 62, 65
network locations 65
preboot, message 66
screen saver timeout 66
security features 62
settings 61, 63
slave drives 192
tray icon, preboot 65
user perspective 63
WOL, see Wake-on-LAN
Work folder 139

Z

ZP4PC.zip.dll 37