Full Disk Encryption Emergency Recovery Reference

ZENworks® 11 Support Pack 4

Beta
April 2015

Novell®

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

This *Novell ZENworks 11SP4 Full Disk Encryption Emergency Recovery Reference* provides information about preparing devices to enable emergency recovery and performing emergency recovering on devices. The information in this guide is organized as follows:

Audience

This guide is written for the ZENworks Full Disk Encryption administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Additional Documentation

ZENworks Full Disk Encryption is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the ZENworks 11 SP4 documentation Web site (http://www.novell.com/documentation/zenworks114).

Overview

ZENworks Full Disk Encryption provides an emergency recovery application to help you regain access to encrypted drives on devices that have become inaccessible.

The following sections address the concepts you need to understand in order to effectively prepare for and perform emergency recovery of devices.

1 What is Emergency Recovery?

Emergency recovery is the process of accessing encrypted data from a device that is not functioning correctly. For example, the device might not be starting correctly or the ZENworks Full Disk Encryption Agent was removed before encrypted drives were fully decrypted.

1.1 Emergency Recovery Disk and Application

ZENworks 11 Full Disk Encryption provides an Emergency Recovery application that is a plug-in to Microsoft Windows Preinstallation Environment (Windows PE) or Bart’s Preinstalled Environment (BartPE).

Both Windows PE and BartPE enable you to build a boot CD, referred to as an emergency recovery disk (ERD), based on Windows components. The Emergency Recovery application plugs in to the Windows PE or BartPE ERD. After the device is booted with the ERD, you can use the Emergency Recovery application to attempt to repair or restore the master boot record (MBR), decrypt encrypted disks, deactivate the ZENworks PBA, and perform other recovery operations.

1.2 Emergency Recovery Information File

To recover a device, you must have an emergency recovery information (ERI) file for the device. If you don’t have an ERI file specific to the device you are recovering, the data is lost.

An ERI file is a password-protected file that contains the encryption keys to the encrypted volumes of the hard disk. Each volume has its own encryption key.

The ZENworks Full Disk Encryption Agent generates an ERI file the first time disk encryption is applied to a device. After that, it generates a new ERI file any time the encryption settings (volumes, algorithm, key length, an so forth) are changed.

The ERI files are uploaded to the ZENworks Primary Server. If a new ERI file is generated but the agent does not have network access to the ZENworks Primary Server, the ERI file is stored and then uploaded when network access is restored.

1.3 Emergency Recovery Versus PBA Override

ZENworks Full Disk Encryption provides both emergency recovery of devices and override of ZENworks Pre-Boot Authentication.

You need to perform an emergency recovery in the following situations:

- The device does not start correctly or does not present the user with the ZENworks PBA login or the Windows login.

- Windows login is being used as the authentication method (no ZENworks PBA) and the Windows credentials have been forgotten or the user's smart card has been lost or damaged.
- ZENworks Full Disk Encryption has been removed from the device but the hard disk is still encrypted.

You can perform a PBA override in the following situations:

- The smart card reader is defective.
- The smart card is lost or broken.
- The smart card PIN is forgotten or blocked.
- The PBA credential (user ID/password) is forgotten.
- The PBA lockout has been invoked because of too many failed logins.

This *ZENworks Full Disk Encryption Emergency Recover Reference* does not provide information about PBA override. For information about overriding the PBA, see the *ZENworks 11 SP4 Full Disk Encryption PBA Reference*.

II Emergency Recovery Information Files

To recover a device, you must have the device's emergency recovery information (ERI) file. The following sections provide information about creating, using, and maintaining ERI files.

2 About ERI Files

To recover a device, the Emergency Recovery application (see Part III, “Emergency Recovery Disks,” on page 19) requires an emergency recovery information (ERI) file that is specific to the device. The following sections explain what ERI files contain, how they are created, and where they are stored:

2.1 Contents of ERI Files

An ERI file for a device with standard hard disks contains the encryption keys for the device’s encrypted volumes. The encryption keys provide information about which volumes are encrypted and the encryption algorithm and key length used on the volumes.

An ERI file for a device with self-encrypting hard disks contains the information to unlock the devices’ disks.

2.2 Creation of ERI Files

The Full Disk Encryption Agent generates an ERI file any time it applies new encryption settings to the device. The following are triggers for creating a new ERI file:

- A volume is encrypted or decrypted
- The encryption algorithm is changed
- The encryption key length is changed

The Disk Encryption policy also includes an option to enable users to manually generate ERI files through the Full Disk Encryption Agent.

An ERI file is protected by a password that the Full Disk Encryption Agent generates randomly if it initiates the ERI file. If a user initiates the ERI file, the user is prompted to supply a password.

2.3 Location of ERI Files

When the Full Disk Encryption Agent creates an ERI file, it stores the file in the following locations:

- A cache on the ZENworks partition.
- The ZENworks Primary Server. If the agent cannot immediately contact the ZENworks Primary Server, it retries the upload at 5 minute intervals until successful.
- A location specified by the user, if the user initiated the creation of the file. To be useful in an emergency recovery situation, the user should save the file to a removable storage device such as a USB device.

You should use a device's newest ERI file when recovering the device. This ensures that all encryption information required to access or decrypt the device's drives is correct for the current state of the drives. If necessary, you can use an older ERI, but depending on the changes since the ERI was generated, you might not be able to access or decrypt drives.

The cache always contains a device's newest ERI file. If the file has also been uploaded to the ZENworks Primary Server, you can use ZENworks Control Center to view the file's password. When you use the Emergency Recovery application, you can load the file from the device's cache and then enter the password.

ZENworks Control Center contains all of a device's ERI files, including the newest ERI file unless the Full Disk Encryption Agent has not been able to connect and upload the file. You can download the newest ERI file and include it on the emergency recovery disk (ERD) along with the Emergency Recovery application, or you can download it and include it on a removable storage device (such as a USB device).

3 Retrieving ERI Files and Passwords

When a new ERI file is created for a device (see Section 2.2, “Creation of ERI Files,” on page 13), the file and its password are uploaded to the ZENworks Primary Server the next time the device contacts the server.

There is no automatic deletion of ERI files and passwords from the ZENworks Primary Server, even if a device is unregistered, deleted, or retired from the zone. The ZENworks Primary Server retains all of a device’s ERI files and passwords unless you manually delete the files (see Chapter 4, “Deleting ERI Files,” on page 17).

ZENworks Control Center provides two areas from which you can retrieve a device’s ERI file and its password:

- Section 3.1, “Retrieving ERI Files and Passwords from a Device List,” on page 15
- Section 3.2, “Retrieving ERI Files and Passwords from the Zone List,” on page 15

3.1 Retrieving ERI Files and Passwords from a Device List

A device list contains the ERI files and passwords for a single device.

1. In ZENworks Control Center, click *Devices*, then locate and click the device whose ERI file and password you want to retrieve.
2. On the device’s property page, click *Emergency Recovery*.
3. In the list, locate the ERI file you want to retrieve or whose password you want to view.
4. Click the ERI filename, then follow the prompts to download it.
5. Click *view* in the *ERI Password* column to display the file’s password.

   You must provide the ERI password when using the Emergency Recovery application on the device. You should record the password so that it is available when you use the ERI file.

3.2 Retrieving ERI Files and Passwords from the Zone List

The zone list contains the ERI files and passwords for all devices in the zone.

1. In ZENworks Control Center, click *Full Disk Encryption*, then click *Emergency Recovery*.
2. In the list, locate the ERI file you want to retrieve or whose password you want to view.

   Files are listed by device name and date. You can use the *Search* box to find all ERI files associated with a specific device or all ERI files within a certain time period.
3. Click the ERI filename, then follow the prompts to download it.
4. Click *View* in the *ERI Password* column to display the file’s password.

   You must provide the ERI password when using the Emergency Recovery application on the device. You should record the password so that it is available when you use the ERI file.

4 Deleting ERI Files

Any time new encryption settings are applied to a device, the Full Disk Encryption Agent generates an emergency recovery information (ERI) file and uploads it to the ZENworks Primary Server. Previous ERI files for the device are retained on the ZENworks Primary Server, even after the device is unregistered, deleted, or retired from the zone.

If you decide that you no longer need all or some of a device's ERI files, you can delete them.

4.1 Deleting ERI Files in ZENworks Control Center

1. In ZENworks Control Center, click *Full Disk Encryption*, then click *Emergency Recovery*.
2. In the list, locate the device whose ERI files you want to delete.

   Files are listed by device name and date. You can use the *Search* box to find all ERI files associated with a specific device.
3. Select the check boxes next to the ERI files to delete, then click *Delete*.

4.2 Deleting ERI Files Using the zman Utility

1. At a ZENworks Primary Server command prompt, enter the following command:

   ```
   zman fdepolicy-purge-eri (fpe) [(device path)(device path)...(device path)] [-b|--begin-date=yyyy-MM-dd HH:mm:ss] [-e|end-date=yyyy=MM-dd HH:mm:ss] [-u|--unregisteredDevices]
   ```

   The options are:

   [(device path) (device path) ... (device path)]: To purge the ERI files for specific devices, specify the full path for each device. Ignore this option to purge files for all devices.

   [-b|--begin-date=yyyy-MM-dd HH:mm:ss]: To purge ERI files starting with a specific date, specify the begin date. All files with a timestamp on or after the begin date are purged. Use this option with the end-date option to designate a specific time period.

   [-e|--end-date=yyyy=MM-dd HH:mm:ss]: To purge ERI files up to a specific date, specify the end date. All files with a timestamp on or before the end date are purged. Use this option with the begin-date option to designate a specific time period.

   [-u|--unregisteredDevices]: Purge ERI files for devices that are no longer registered in the zone but that still have ERI files in the ZENworks database.

   The following example purges all ERI files for device1:

   ```
   zman fpe /Devices/Workstations/device1
   ```

   The following example purges all ERI files for device1 that were created between the two specified dates:

   ```
   zman fpe /Devices/Workstations/device1 -b "2011-10-10 10:10:10" -e "2011-12-31 24:00:00"
   ```

The following example purges all ERI files not associated with a registered device:

```
zman fpe -u
```

The following example purges all ERI files for all devices:

```
zman fpe
```

III Emergency Recovery Disks

The following sections help you build emergency recovery disks (ERDs) that can be used to recover encrypted drives that are no longer accessible:

5 Creating a Windows PE Emergency Recovery Disk

This section explains how to create a bootable Emergency Recovery Disk (ERD) using Microsoft Windows Preinstallation Environment (Windows PE). When it is booted, the ERD provides access to the Emergency Recovery application you can use to perform recovery operations on a device.

IMPORTANT: ZENworks Cool Solutions provides a Windows Powershell script that automates the creation of Windows PE ERDs. For details, see the *Windows Powershell script to create a Windows PE emergency recovery disk for ZENworks Full Disk Encryption (https://www.novell.com/communities/coolsolutions/?s=Windows+PE+emergency+recovery)* article.

5.1 Prerequisites

Before you can create a Windows PE ERD, you must complete the following on the device where you plan to create the ERD:

- Install the Windows Automated Installation Kit (AIK) on a Windows XP, Windows Vista, or Windows 7 device. Windows PE is included in the AIK. Download the AIK from the following locations:
  - Windows 7 (http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=5753)
  - Windows XP and Vista (http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=10333)
- If the device you are using has Windows XP with Service Pack 2, install Microsoft Management Console 3.0 (MMC 3.0). Download MMC 3.0 from the following location:
  - MMC 3.0 (http://www.microsoft.com/download/en/details.aspx?id=20525)

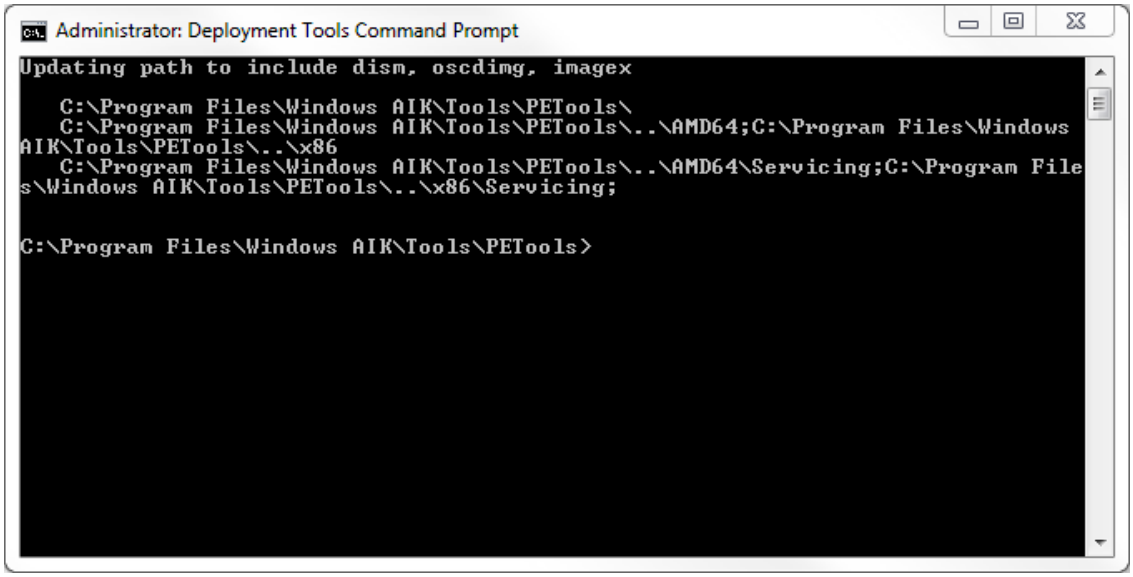
  Windows XP Service Pack 3 already includes MMC 3.0.
- Download the Emergency Recovery application for Windows PE:
  1. In ZENworks Control Center, click *Home*.
  2. Under *Common Tasks* (in the left navigation panel), click *Download ZENworks Tools*.
  3. Click *Administrative Tools*, then click *Full Disk Encryption*.
  4. Click *ZFDE_WinPE_Plugin.zip* to download the zip file.
  5. Extract the zip file to a directory on the device (for example, `c:\winpe_plugin`)

5.2 Creating a Windows PE ERD

1 Open the Windows PE Deployment Tools command prompt:

- Windows XP: Click *Start* > *All Programs* > *Microsoft Windows AIK* > *Deployment Tools Command Prompt*.
- Windows Vista/7: Click *Start* > *All Programs* > *Microsoft Windows AIK*. Right-click *Deployment Tools Command Prompt* and select *Run as administrator*.

The command prompt is displayed.



2 In the Deployment Tools command prompt:

2a Enter the following command to create the build directory for the Windows PE CD:

```
copype <architecture> <destination>
```

Use the following options:

Option	Details
<*architecture*>	Always use `x86` for this setting. The `x86` setting works for both 32-bit and 64-bit operating systems.
<*destination*>	The build directory to which the Windows PE files will be copied

For example:

```
copype x86 c:\winpe
```

This example creates the following build directory structure:

- `c:\winpe`: Contains the Windows PE bootstrap loader (`ETFSBoot.com`) and a Windows PE image file (`winpe.wim`) that has all of the files for a basic Windows PE CD.
- `c:\winpe\ISO`: Contains the files needed to create the base Windows PE ISO image.
- `c:\winpe\mount`: An empty folder that will be used to mount the Windows PE image file (`winpe.wim`) so that changes can be made to it.

2b Enter the following command to mount the `winpe.wim` image in the `c:\winpe\mount` directory:

```
imagex /mountrw c:\winpe\winpe.wim 1 c:\winpe\mount
```

This command (and all commands in the next steps) assumes that you specified `c:\winpe` as your build directory when running the `copype` command. If you used another directory, substitute that directory in the commands.

2c Create the following directory structure:

```
c:\winpe\mount\program files\FinallySecure\eri
```

You can create the directories at the Deployment Tools command prompt or in another tool such as Windows Explorer.

The Emergency Recovery application, as well as the encryption drivers, are provided by SECUDE AG. The application, files, and directories have not been renamed. As you prepare and use the application, you will see directory names such as `FinallySecure` and registry keys such as `fsesys`.

2d Copy the Emergency Recovery application files to the `FinallySecure` directory created in the previous step:

```
xcopy c:\winpe_plugin\EN\files\*.* "c:\winpe\mount\program
files\FinallySecure" /s /e
```

These paths assume that you extracted the application files to the `c:\winpe_plugin` directory (see “Prerequisites” on page 21). If you used a different directory, copy the files from that directory.

2e Copy the encryption drivers to the Windows PE system drivers directory:

```
xcopy c:\winpe_plugin\EN\files\*.sys
c:\winpe\mount\windows\system32\drivers /s /e /y
```

2f Copy the Microsoft OLE User Interface Support file from the device’s system directory to the Windows PE system directory:

```
xcopy c:\windows\system32\oledlg.dll c:\winpe\mount\windows\system32 /I /e
/Y
```

3 Open a standard command prompt and do the following:

3a Enter the following command to load the FinallySecure registry hive:

```
REG LOAD "HKLM\fsesys" c:\winpe\mount\windows\system32\config\system
```

3b Add the following registry entries for the plug-in by typing each line at the command prompt and then pressing Enter.

```
REG ADD HKLM\fsesys\ControlSet001\Services\NBFDENC /v DisplayName /t REG_SZ
/d NBFDENC

REG ADD HKLM\fsesys\ControlSet001\Services\NBFDENC /v ErrorControl /t
REG_DWORD /d 0x1

REG ADD HKLM\fsesys\ControlSet001\Services\NBFDENC /v Type /t REG_DWORD /d
0x1

REG ADD HKLM\fsesys\ControlSet001\Services\NBFDENC /v Start /t REG_DWORD /d
0x0

REG ADD HKLM\fsesys\ControlSet001\Services\NBFDENC /v Group /t REG_SZ /d
"System Bus Extender"

REG ADD HKLM\fsesys\ControlSet001\Services\NBFDENC /v Tag /t REG_DWORD /d
```

```
0x2

REG ADD HKLM\fsesys\ControlSet001\Services\AES /v DisplayName /t REG_SZ /d
AES

REG ADD HKLM\fsesys\ControlSet001\Services\AES /v ErrorControl /t REG_DWORD
/d 0x1

REG ADD HKLM\fsesys\ControlSet001\Services\AES /v Type /t REG_DWORD /d 0x1

REG ADD HKLM\fsesys\ControlSet001\Services\AES /v Start /t REG_DWORD /d 0x0

REG ADD HKLM\fsesys\ControlSet001\Services\AES /v Group /t REG_SZ /d
"Primary Disk"

REG ADD HKLM\fsesys\ControlSet001\Services\DES /v DisplayName /t REG_SZ /d
DES

REG ADD HKLM\fsesys\ControlSet001\Services\DES /v ErrorControl /t REG_DWORD
/d 0x1

REG ADD HKLM\fsesys\ControlSet001\Services\DES /v Type /t REG_DWORD /d 0x1

REG ADD HKLM\fsesys\ControlSet001\Services\DES /v Start /t REG_DWORD /d 0x0

REG ADD HKLM\fsesys\ControlSet001\Services\DES /v Group /t REG_SZ /d
"Primary Disk"

REG ADD HKLM\fsesys\ControlSet001\Services\DESX /v DisplayName /t REG_SZ /d
DESX

REG ADD HKLM\fsesys\ControlSet001\Services\DESX /v ErrorControl /t
REG_DWORD /d 0x1

REG ADD HKLM\fsesys\ControlSet001\Services\DESX /v Type /t REG_DWORD /d 0x1

REG ADD HKLM\fsesys\ControlSet001\Services\DESX /v Start /t REG_DWORD /d
0x0

REG ADD HKLM\fsesys\ControlSet001\Services\DESX /v Group /t REG_SZ /d
"Primary Disk"

REG ADD HKLM\fsesys\ControlSet001\Services\BLOWFISH /v DisplayName /t
REG_SZ /d BLOWFISH

REG ADD HKLM\fsesys\ControlSet001\Services\BLOWFISH /v ErrorControl /t
REG_DWORD /d 0x1

REG ADD HKLM\fsesys\ControlSet001\Services\BLOWFISH /v Type /t REG_DWORD /d
0x1

REG ADD HKLM\fsesys\ControlSet001\Services\BLOWFISH /v Start /t REG_DWORD /
d 0x0

REG ADD HKLM\fsesys\ControlSet001\Services\BLOWFISH /v Group /t REG_SZ /d
"Primary Disk"

REG ADD "HKLM\fsesys\ControlSet001\Control\Class\{71A27CDD-812A-11D0-BEC7-
08002BE2092F}" /v LowerFilters /t REG_MULTI_SZ /d nbfdenc\0fvevol /f

REG ADD "HKLM\fsesys\ControlSet001\Control\Class\{4D36E967-E325-11CE-BFC1-
08002BE10318}" /v UpperFilters /t REG_MULTI_SZ /d PartMgr\0nbfdenc /f
```

3c Enter the following command to unload the FinallySecure registry hive:

```
REG Unload "HKLM\fsesys"
```

4 (Optional) Copy ERI files to the following directory:

```
c:\winpe\mount\program files\FinallySecure\ERI
```

In order to recover a device, the Emergency Recovery application must have access to the device's ERI file.

If you are creating the ERD to recover a specific device, you might want to add the ERI file to the ERD so that everything required to recover the device is on the ERD. If you are creating a generic ERD for use with any device, you might want to wait until a recovery situation arises with a device and then add the device's ERI file to a USB device that can be distributed with the ERD.

For information about accessing ERI files, see Chapter 3, "Retrieving ERI Files and Passwords," on page 15.

5 Configure the Emergency Recovery application to autostart in the desired language:

5a In a text editor (run as Administrator), open the `c:\winpe\mount\windows\system32\startnet.cmd` file.

5b Under `wpeinit` add the following line:

```
"X:\Program Files\FinallySecure\pe_erd_w32.exe"
```

5c (Optional) Add the following lines to change the input language and keyboard layout from the default (EN-US):

```
wpeutil SetKeyboardLayout <keyboard layout ID>
wpeutil SetUserLocale <language name>-<language name>
```

For a list of *<keyboard layout ID>* values, see the Microsoft Go Global Development Center (http://msdn.microsoft.com/en-us/goglobal/bb895996). The *<language-name>* values are in standard international language code format (en-US, de-DE, es-ES, and so forth). For example, a German keyboard layout and locale would be:

```
wpeutil SetKeyboardLayout 0407:0000407
wpeutil SetUserLocale de-DE
```

5d Verify that the final changes are similar to the following:

```
wpeinit
"X:\Program Files\FinallySecure\pe_erd_w32.exe"
wpeutil SetKeyboardLayout 0407:0000407
wpeutil SetUserLocale de-DE
```

5e Save the changes.

6 At the Deployment Tools command prompt:

6a Enter the following command to unmount the image and commit the changes to the original image file (`winpe.wim`):

```
imagex /unmount /commit c:\winpe\mount
```

6b Enter the following command to replace the image in the ISO directory with the newly updated image file (`winpe.wim`):

```
copy c:\winpe\winpe.wim c:\winpe\iso\sources\boot.wim
```

6c Enter the following command to create the ISO image file:

```
oscdimg -n -h -bc:\winpe\etfsboot.com c:\winpe\iso c:\winpe\winpe.iso
```

7 Burn the `winpe.iso` image to a DVD.

or

Use the `winpe.iso` image to create a bootable USB device. See Chapter 6, "Creating a Windows PE Emergency Recovery USB Drive," on page 27.

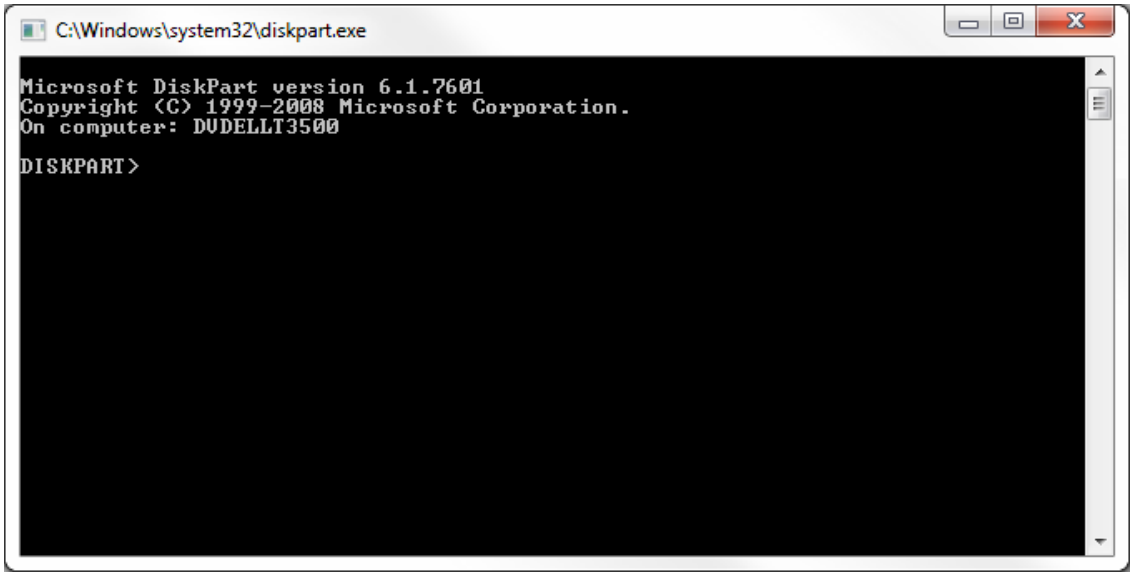
The ERD is ready to use.

6 Creating a Windows PE Emergency Recovery USB Drive

This section explains how to create a bootable Emergency Recovery USB device (ERD) using Microsoft Windows Preinstallation Environment (Windows PE). When it is booted, the ERD provides access to the Emergency Recovery application you can use to perform recovery operations on a device.

You must perform the following steps on a Windows 7 or Windows Vista device. The steps are not supported on Windows XP. The USB drive size must be at least 256 MB.

1. Complete Step 1 through Step 6 in Section 5.2, “Creating a Windows PE ERD,” on page 22 to create the ERD ISO image. Make sure you also complete the prerequisites listed for the steps.
2. At a command prompt on a Windows 7 or Windows Vista, enter `diskpart` to start the DiskPart utility used to prepare the USB device.



3. At the DISKPART prompt, enter each of the following commands, one at a time. Press Enter after each command.

Command	Explanation
`list disk`	Displays the list of disks and USB drives for the device. Note the disk number of your USB drive. It is typically Disk 1.
`select disk 1`	Selects the disk on which to perform actions. If your USB is not Disk 1, substitute the correct number in the command (for example, `select disk 2`).
`clean`	Removes all partition and volume formatting from the USB drive.
`create partition primary`	Creates a primary partition on the USB drive.
`select partition 1`	Selects the primary partition.
`active`	Sets the primary partition to active so that it is recognized as a valid system partition.
`format fs=fat32`	Formats the partition as a FAT32 file system.
`assign`	Assigns the next available drive letter to the USB drive.
`exit`	Exits the DiskPart utility.

4 At a command prompt on the device where you created the Windows PE ISO image, enter the following command to copy the ISO image to the USB drive:

```
xcopy <path>\iso\*.* <USB drive letter>:\ /e/h/f
```

For example:

```
xcopy c:\winpe\iso\*.* f:\ /e/h/f
```

The USB drive is ready to use as an ERD.

7 Creating a BartPE Emergency Recovery Disk

This section explains how to create a bootable Emergency Recovery Disk (ERD) using Bart's Preinstalled Environment (BartPE). When it is booted, the ERD provides access to the Emergency Recovery application you can use to perform recovery operations on a device.

7.1 Prerequisites

Before you can create a BartPE ERD, you must complete the following on the device where you plan to create the ERD:

- Install BartPE on a Windows XP device. Download BartPE from the following location:
  - Bart's Preinstalled Environment (http://www.nu2.nu/pebuilder/download)
- Make sure you understand and agree to all Microsoft Windows licensing issues associated with using BartPE. See BartPE Licensing Issues (http://www.nu2.nu/pebuilder/#licensing)
- Download the Emergency Recovery application to the Windows XP device:
  1. In ZENworks Control Center, click *Home*.
  2. Under *Common Tasks* (in the left navigation panel), click *Download ZENworks Tools*.
  3. Click *Administrative Tools*, then click *Full Disk Encryption*.
  4. Click *ZFDE_BartPE_Plugin.zip* to download the zip file.
  5. Extract the zip file to a directory on the device (for example, `c:\zen_er_app`)

7.2 Creating a BartPE ERD

1 Add the ZENworks Full Disk Encryption BartPE plug-in to the PE Builder plug-in directory:

1a Locate the PE Builder plug-in directory.

The default directory is `c:\pebuilder<version>\plugin`. For example, `c:\pebuilder3110a\plugin`.

1b In the `plugin` directory, create a `pe_erd` directory.

The result should be a directory structure like:

`c:\pebuilder3110a\plugin\pe_erd`.

1c Copy all contents (folders and files) from the `EN` directory of the Emergency Recovery application directory created in Prerequisites to the `pe_erd` directory created for PE Builder.

For example, copy all contents from `c:\zen_er_app\EN` to `c:\pebuilder3110a\plugin\pe_erd`.

2 (Optional) Add ERI files to the PE Builder directory structure.

In order to recover a device, the Emergency Recovery application must have access to the device's ERI file.

If you are creating the ERD to recover a specific device, you might want to add the ERI file to the ERD so that everything required to recover the device is on the ERD. If you are creating a generic ERD for use with any device, you might want to wait until a recovery situation arises with a device and then add the device's ERI file to a USB device that can be distributed with the ERD.

For information about accessing ERI files, see Chapter 3, "Retrieving ERI Files and Passwords," on page 15.

2a In the PE Builder `pe_erd\files` directory, create an `eri` directory.

The result should be a directory structure like:

```
c:\pebuilder3110a\plugin\pe_erd\files\eri
```

2b Copy any ERI files to the directory.

3 If you are using a Windows XP CD as the source for the Windows installation files, make sure the CD is loaded in the Windows XP device.

4 Start PE Builder.

5 (Conditional) If this is the first time PE Builder has run on the device:

5a Read the PE Builder license, then click *I agree*.

5b When you receive the *Search files* prompt, click *No* to skip the search and to display the PE Builder dialog box.

6 In the *Source* field, click the browse button and select the source location of the Windows installation files.

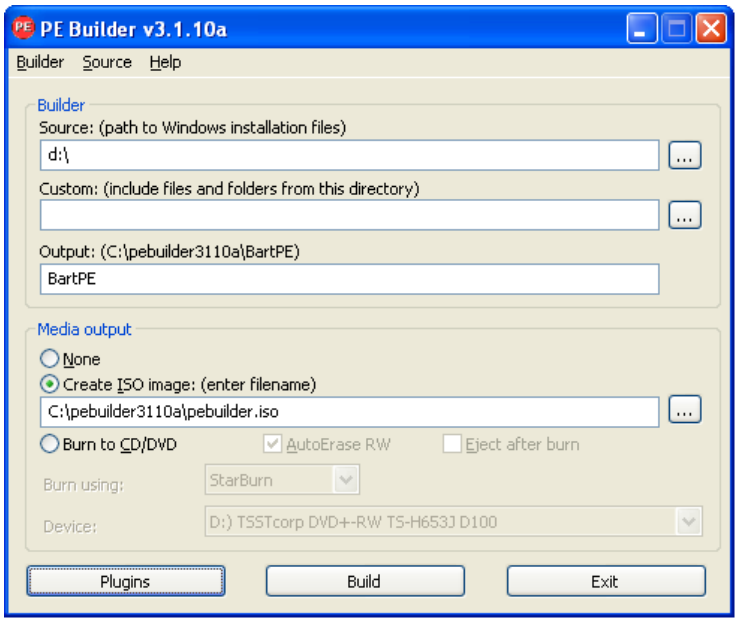
or

If you don't know the location of the Windows installation files, click the *Source* menu, click *Search*, then follow the prompts to search for and select the Windows installation files.

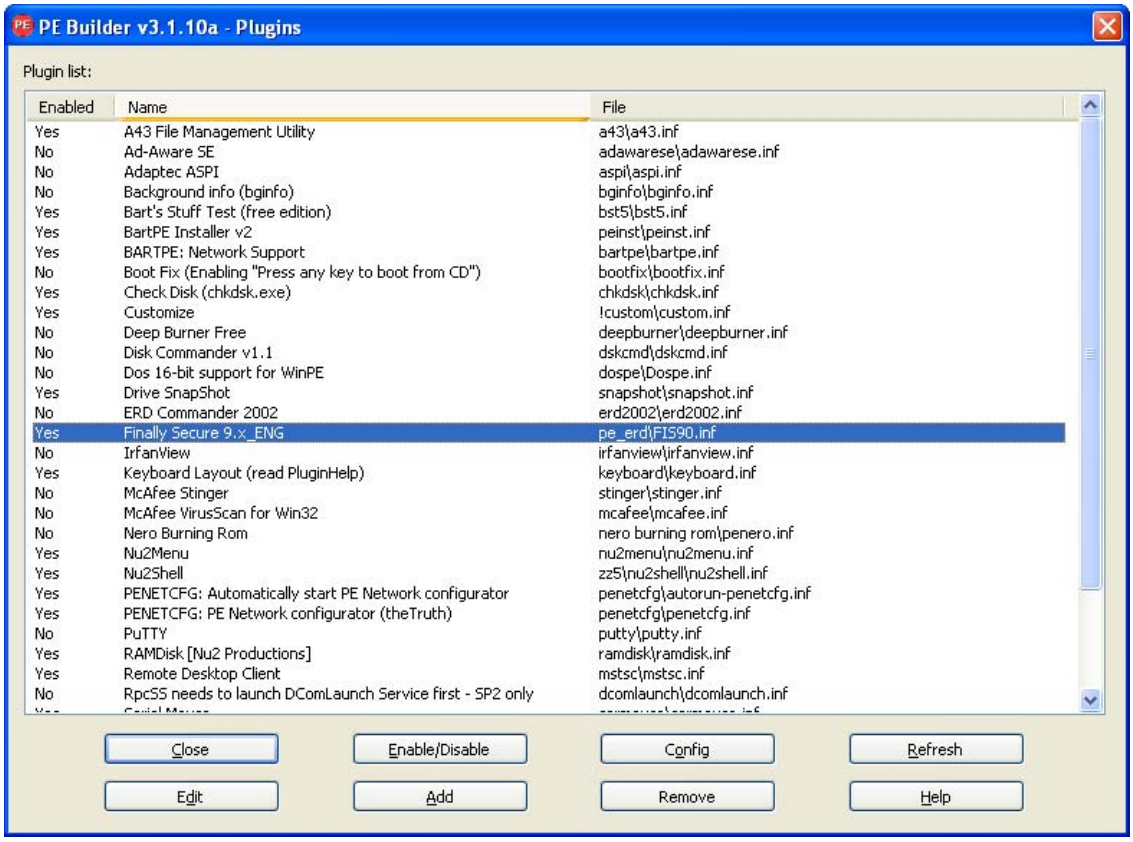
7 Under *Media output*, select one of the following options:

- **Create ISO image:** Select this option to create an ISO image that you can burn to a CD/DVD. After you select the option, you can specify the name and target location for the ISO image.
- **Burn to CD/DVD:** Select this option to burn directly to a CD/DVD. After you select this option, enable *AutoErase RW* if you are using an erasable CD/DVD, leave *Burn using* set to *StarBurn*, and select your CD/DVD burner in the *Device* list.

At this point, the PE Builder dialog box should contain information similar to the following example:



8 Click the *Plugins* button to display the Plugin list.



9 In the Plugin list, do the following:

9a Make sure the Emergency Recovery application plug-in (Finally Secure 9.x_ENG) is displayed in the list and is enabled.

If the plug-in is not in the list, exit PE Builder and repeat the steps to this point, paying careful attention to Step 1.

If the plug-in is in the list but is not enabled, select the plug-in, then click the *Enable/Disable* button.

9b Click *Close* to close the Plugin list.

10 Click the *Build* button to start the build and open the Build dialog box.

11 When the build is complete, click *Close* to close the Build dialog box.

12 Click *Exit* to close PE Builder.

13 If you created an ISO image, burn the image to a DVD.

The ERD is ready to use.

IV Encrypted Device Recovery

The following sections provide instructions for using the Emergency Recovery application on an Emergency Recovery Disk (ERD) to regain access to a device's encrypted disks:

8 Launching the Emergency Recovery Application

The following sections explain how to launch the Emergency Recovery application from a bootable Windows PE or BartPE emergency recovery disk (ERD) and then load the device's emergency recovery information (ERI) file. After you have completed these two tasks, you can perform any of the recovery tasks (decrypting drives, repairing the boot chain, and so forth) needed to recover the device.

8.1 Launching the Recovery Application from a Windows PE ERD

You can launch the Emergency Recovery application from a Windows PE emergency recovery CD, DVD, or USB device. The instructions assume that you have completed the following prerequisites:

- Created a Windows PE ERD. If not, see "Creating a Windows PE Emergency Recovery Disk" on page 21 and "Creating a Windows PE Emergency Recovery USB Drive" on page 27.
- Included the device's emergency recovery information (ERI) file on the ERD or copied it to a removable media device (such as a USB drive) that can be read by the Windows device. If not, see Chapter 3, "Retrieving ERI Files and Passwords," on page 15.

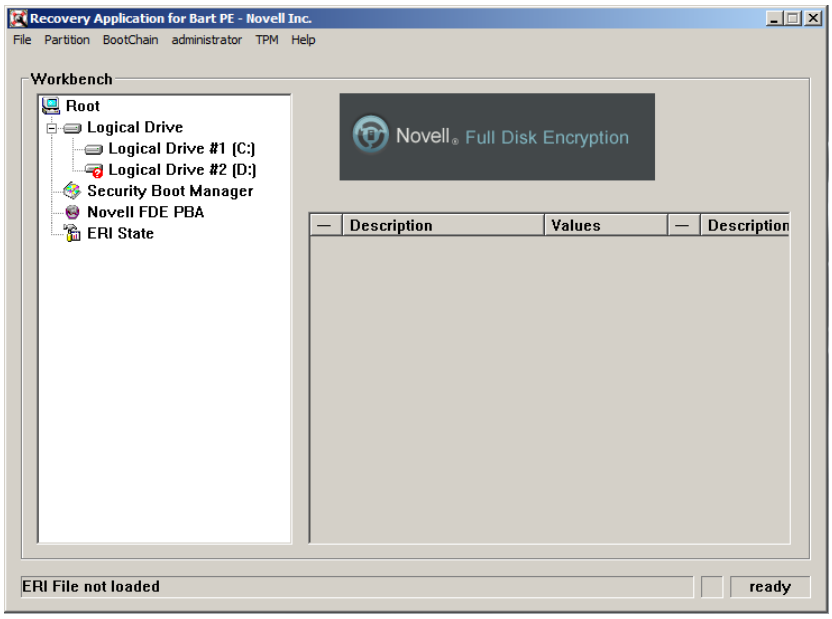
To launch the Emergency Recovery application:

1. If the device's ERI file is on a removable storage device (such as a USB drive), insert it into the Windows device.

   This is required so that the removable storage device can be recognized during the bootup of the Windows device.

2 Reboot the Windows device by using the ERD.

The Emergency Recovery application launches automatically, scans the device, then displays the main window. The application provides different menu options for standard hard disks versus self-encrypting hard disks. The screen shot below is for standard hard disks.



The Emergency Recovery application title states that it is for Bart PE. However, the application is for Windows PE. This issue will be addressed in a future release. In addition, the Emergency Recovery application is provided by SECUDE AG and has not been rebranded.

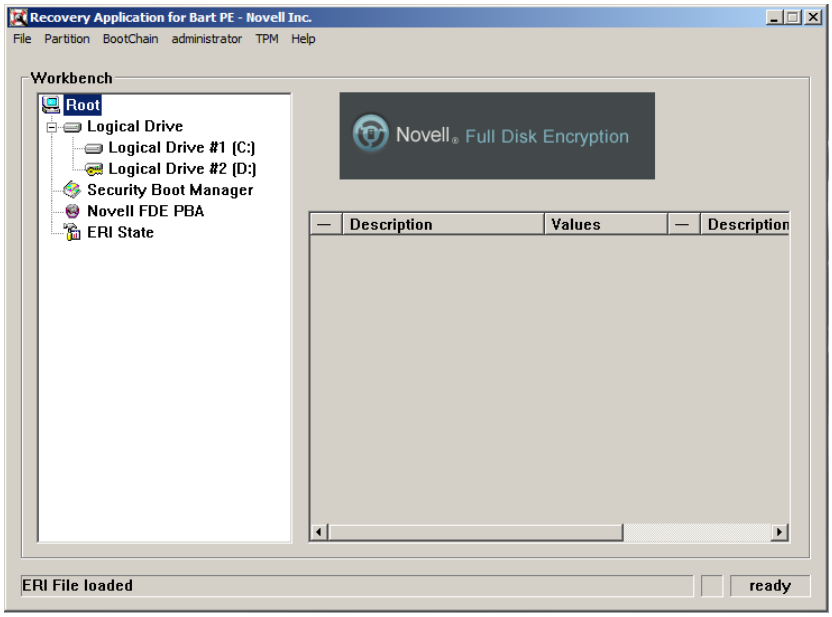
NOTE: If the application does not start, use the command prompt to change to the `X:\Program Files\FinallySecure` directory, then enter `pe_erd_w32.exe` to start the application.

---

3 Click *File*, then click one of the following options to load the device's ERI file:

- **Open ERI file:** Opens Windows Explorer so that you can browse to and select the correct ERI file. After you select the ERI file, you are prompted for the ERI password.
- **Load ERI from Cache:** Prompts you for the password for the device's cached ERI file, then loads the file. If you do not know the password, you can view it in ZENworks Control Center under *Full Disk Encryption* > *Emergency Recovery*. If the device has multiple ERI files, the cached file is the most recent file listed. If the cached file was not uploaded, you won't have access to the correct password and you need to use an older ERI file. See Chapter 2, "About ERI Files," on page 13 for more information.

The Emergency Recovery application displays that the file is loaded.



4 Perform the necessary recovery operations. See the following sections for instructions:

- Chapter 9, “Performing Recovery Operations on a Standard Hard Disk,” on page 41
- Chapter 10, “Performing Recovery Operations on a Self-Encrypting Hard Disk,” on page 49

8.2 Launching the Recovery Application from a BartPE ERD

The instructions in this section assume that you have completed the following prerequisites:

- Created a BartPE ERD. If not, see Chapter 7, “Creating a BartPE Emergency Recovery Disk,” on page 29.
- Included the device’s emergency recovery information (ERI) file on the ERD or copied it to a removable media device (such as a USB drive) that can be read by the Windows device. If not, see Chapter 3, “Retrieving ERI Files and Passwords,” on page 15.

To launch the Emergency Recovery application:

1 If the device’s ERI file is on a removable storage device (such as a USB drive), insert it into the Windows device.

This is required so that the removable storage device can be recognized during the bootup of the Windows device.

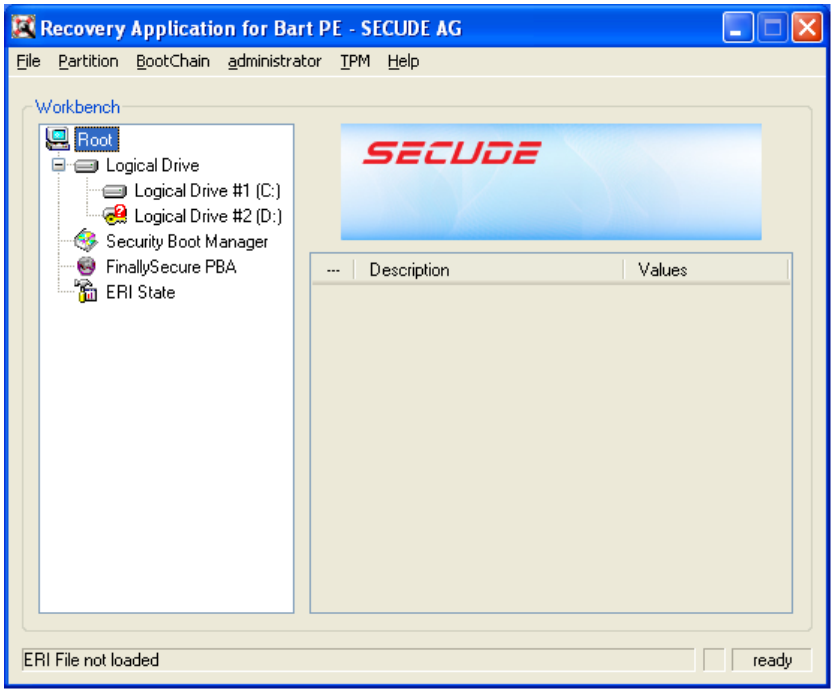
2 Reboot the Windows device by using the ERD.

The BartPE desktop is loaded.

3 (Conditional) To change the keyboard layout from the default English-US to another language, click the *Go* menu > *System* > *Keyboard Layout*, then follow the prompts to change the language.

4 Click the *Go* menu > *Programs* > *FinallySecure ERD* to launch the Emergency Recovery application.

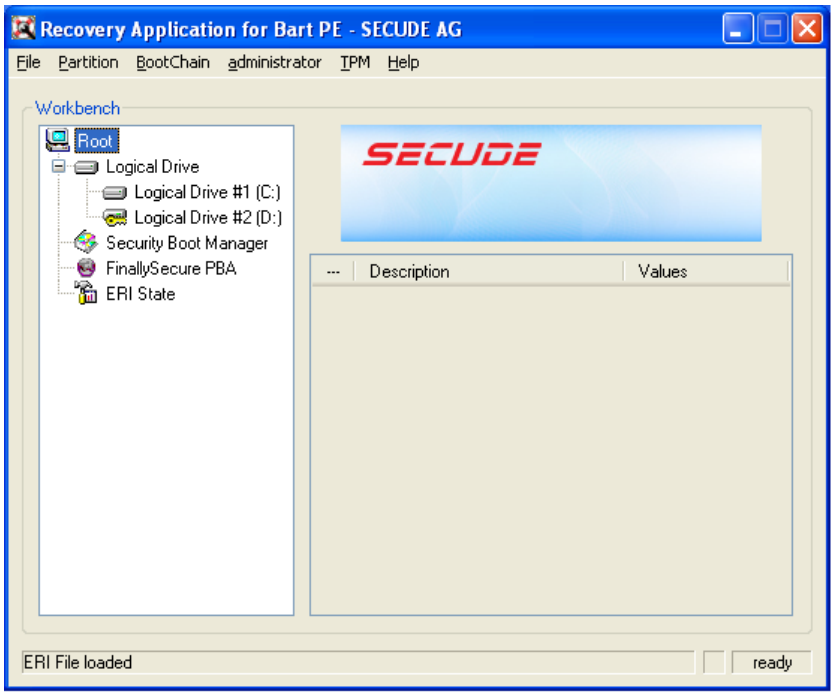
The application launches, scans the device, then displays the main window. The application provides different menu options for standard hard disks versus self-encrypting hard disks. The screen shot below is for standard hard disks.



5 Click *File*, then click one of the following options to load the device's ERI file:

- **Open ERI file:** Opens Windows Explorer so that you can browse to and select the correct ERI file. After you select the ERI file, you are prompted for the ERI password.
- **Load ERI from Cache:** Prompts you for the password for the device's cached ERI file, then loads the file. If you do not know the password, you can view it in ZENworks Control Center under *Full Disk Encryption* > *Emergency Recovery*. If the device has multiple ERI files, the cached file is the most recent file listed. If the cached file was not uploaded, you won't have access to the correct password and you need to use an older ERI file. See Chapter 2, "About ERI Files," on page 13 for more information.

The Emergency Recovery application displays that the file is loaded.



6 Perform the necessary recovery operations. See the following sections for instructions:

- Chapter 9, “Performing Recovery Operations on a Standard Hard Disk,” on page 41
- Chapter 10, “Performing Recovery Operations on a Self-Encrypting Hard Disk,” on page 49

9 Performing Recovery Operations on a Standard Hard Disk

The following sections provide information about the emergency recovery operations you can perform on standard hard disks. For information about emergency recovery operations for self-encrypting hard disks, see Chapter 10, “Performing Recovery Operations on a Self-Encrypting Hard Disk,” on page 49.

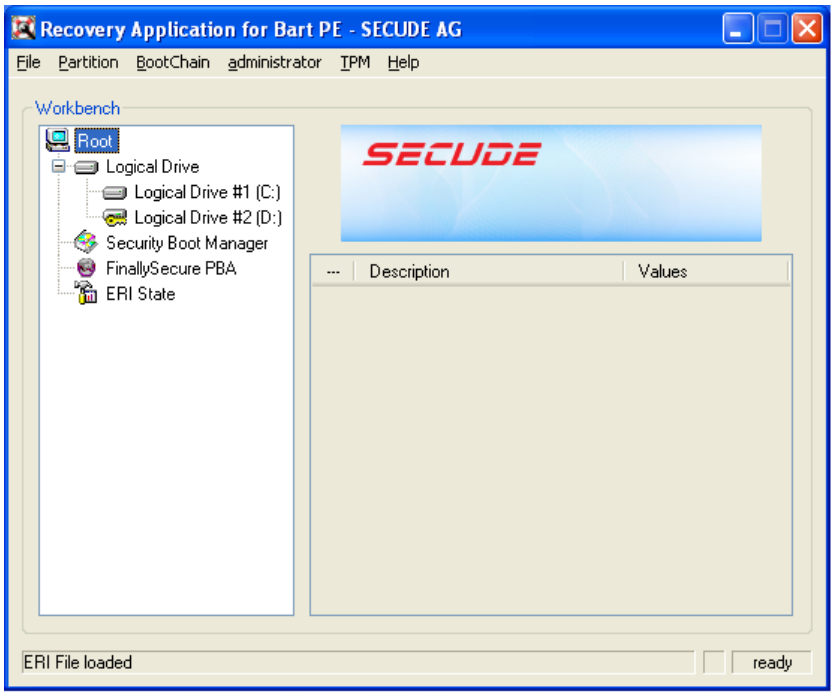
9.1 Decrypting a Drive

Typical scenarios where you might need to decrypt a drive include:

- ZENworks Full Disk Encryption was removed from the device before the drive was decrypted.
- Decryption was interrupted abnormally (for example, because of a power failure).

To decrypt a drive:

1. Make sure you have launched the Emergency Recovery application and loaded the device’s ERI file. See “Launching the Emergency Recovery Application” on page 35.



2 In the Workbench tree, select the drive you want to decrypt, then click the *Partition* menu > *Decrypt* to display the Decrypt Drive dialog box.

3 Deselect the *Decrypt only used sectors* option if you want to decrypt all of the drive's sectors (both used and unused).

   Decrypting all sectors (used and unused) can take significantly longer than decrypting only used sectors.

4 Click *OK* to start the decryption process.

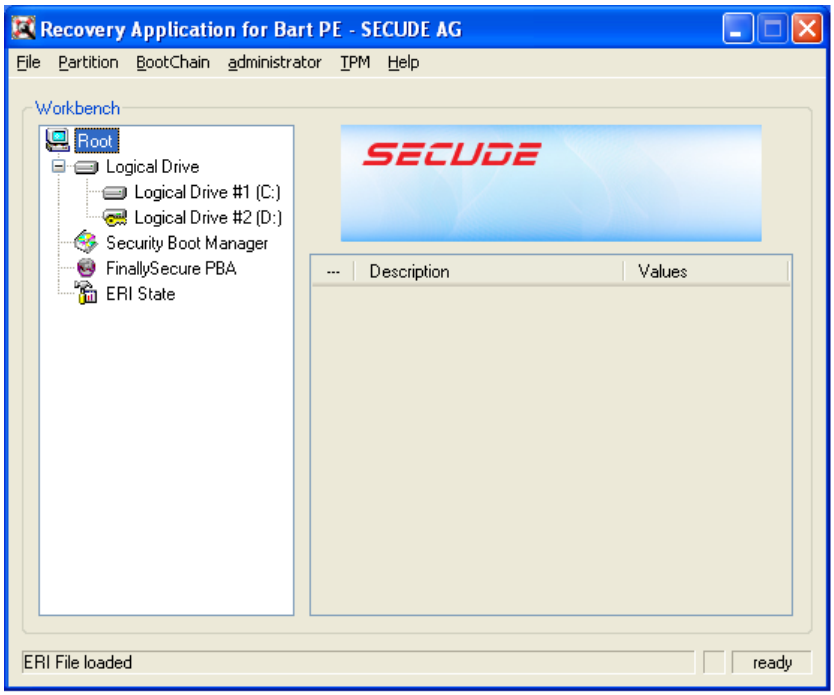
9.2 Repairing the Boot Chain

This section applies to standard hard drives encrypted by ZENworks Full Disk Encryption. It does not apply to self-encrypting drives.

If a device cannot locate the ZENworks partition at boot time, the boot chain might be damaged. You can repair the damaged boot chain. During the repair process, the Emergency Recovery application rewrites all of the files necessary to start the device and resets the ZENworks PBA settings to the defaults. This means that all PBA user accounts are removed.

To repair the boot chain:

1 Make sure you have launched the Emergency Recovery application and loaded the device's ERI file. See "Launching the Emergency Recovery Application" on page 35.



2 Click the *BootChain* menu > *Repair BootChain* to display the Repair Boot Information dialog box.

3 Choose one of the following options:

- **Repair FDE / Deactivate PBA (BartPE):** Repairs the boot chain and deactivates the ZENworks PBA.
- **SBS-bootsector overwriting (Windows PE):** Repairs the boot chain and deactivates the ZENworks PBA.
- **Self-init options:** These options are available only if the *Repair FDE / Deactivate PBA* or *SBS-bootsector overwriting* option is not selected. After the boot chain is repaired, the ZENworks PBA remains active and you can use one of the following options to initiate user capturing on the first reboot of the device:
  - **All Users SelfInit:** Enables user capturing for either user ID/password or smart card authentication.
  - **SmartCard SelfInit:** Enables user capturing for smart card authentication only.
  - **Password SelfInit:** Enables user capturing for user ID/password authentication only.

4 Click *OK* to start the repair process.

5 When the repair process is complete, close the application.

6 Shut down the device, then restart it.

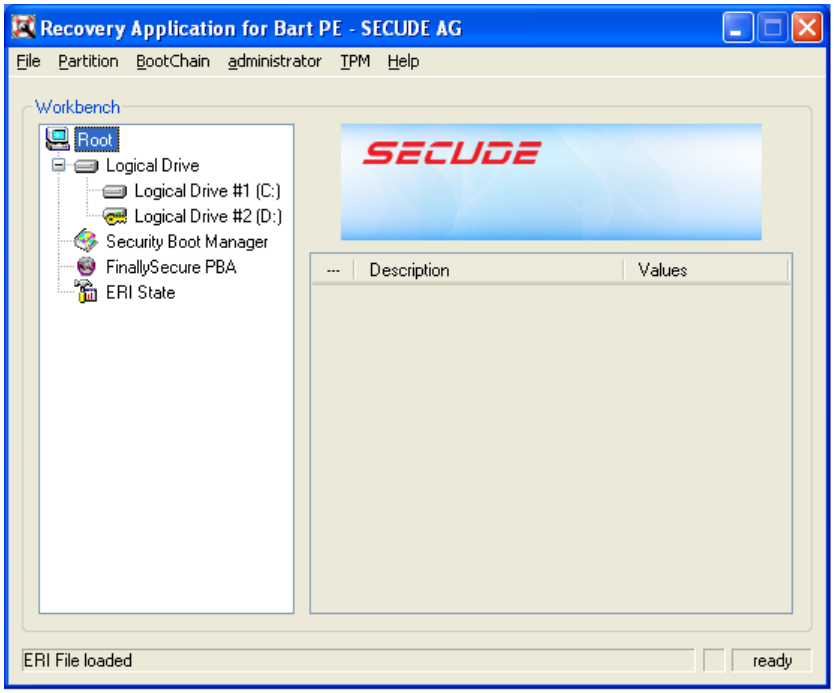
9.3 Repairing the Master Boot Record

This section applies to standard hard drives encrypted by ZENworks Full Disk Encryption. It does not apply to self-encrypting drives.

When a Disk Encryption policy is applied to a device, the ZENworks Full Disk Encryption Agent creates a 100 MB partition, referred to as the ZENworks partition, and modifies the master boot record (MBR) to set the ZENworks partition as the boot partition.

It is possible for other applications to modify the MBR and cause the device to no longer boot to the ZENworks partition. If this occurs, you can repair the MBR. Repairing the MBR fixes any problems that prevent the device from booting to the ZENworks partition.

1 Make sure you have launched the Emergency Recovery application and loaded the device's ERI file. See "Launching the Emergency Recovery Application" on page 35.



2 Click the *BootChain* menu > *Repair MBR* to display the Repair MBR dialog box.

3 Click *OK* to start the repair process.

The dialog box closes when the repair is complete.

4 Close the application.

5 Shut down the device, then restart it.

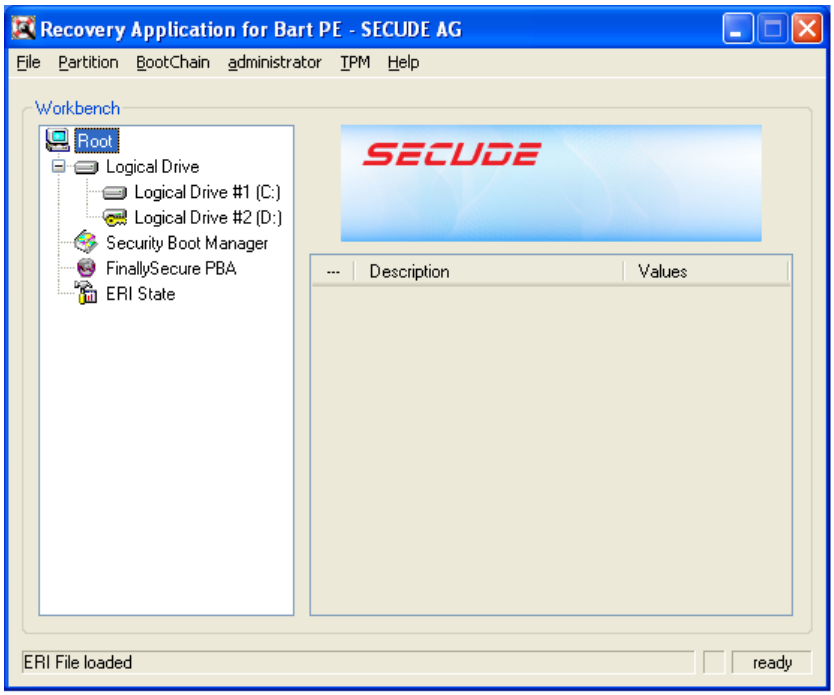
9.4 Restoring the Original Master Boot Record

This section applies to standard hard drives encrypted by ZENworks Full Disk Encryption. It does not apply to self-encrypting drives.

When a Disk Encryption policy is applied to a Windows device, the ZENworks Full Disk Encryption Agent creates a 100 MB partition, referred to as the ZENworks partition, and modifies the master boot record (MBR) to set the ZENworks partition as the boot partition.

You can restore the original MBR if necessary.

1 Make sure you have launched the Emergency Recovery application and loaded the device's ERI file. See "Launching the Emergency Recovery Application" on page 35.



2 Click the *BootChain* menu > *Restore Original MBR* to display the Restore Original MBR dialog box.

3 Click *OK* to start the restore process.

The dialog box closes when the original MBR is restored.

4 Close the application.

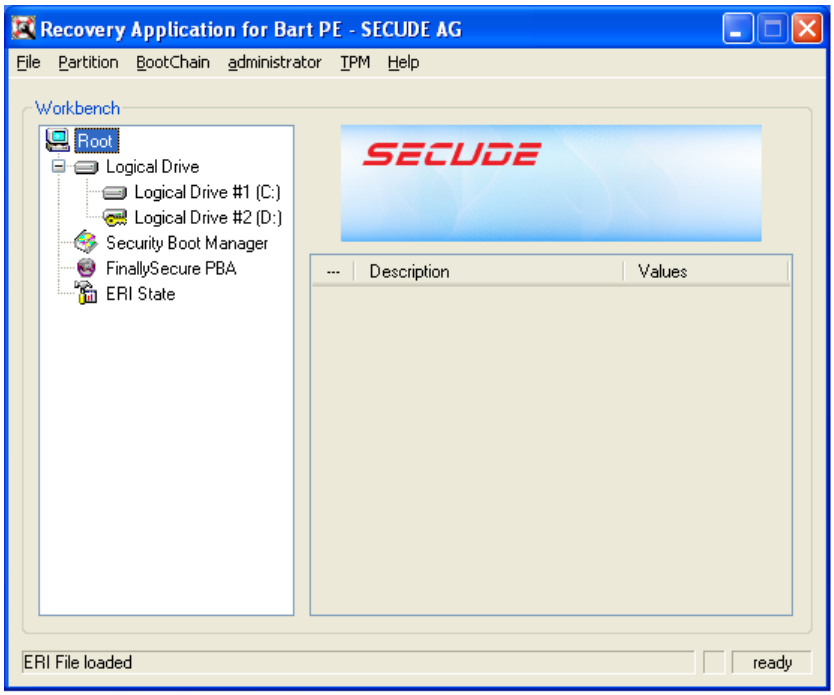
5 Shut down the device, then restart it.

9.5 Erasing the Disk

This section applies to standard hard drives. It does not apply to self-encrypting hard drives. For information about erasing a self-encrypting hard drive, see Section 10.5, “Erasing the Disk,” on page 53.

The Emergency Recovery application can perform a secure erase of a standard hard disk. The process removes all data from the disk. This includes both encrypted and unencrypted volumes.

1 Make sure you have launched the Emergency Recovery application and loaded the device’s ERI file. See “Launching the Emergency Recovery Application” on page 35.



2 Click the *Administration* menu > *Wipe Data* (for BartPE) or *Erase Harddrive* (for Windows PE), then follow the prompts.

   It takes approximately 30 to 40 minutes to erase 10 GB of data, so the entire process can take a long time.

3 When the erasure process is complete, close the application.

4 Shut down the device.

9.6 Setting the Administration Password

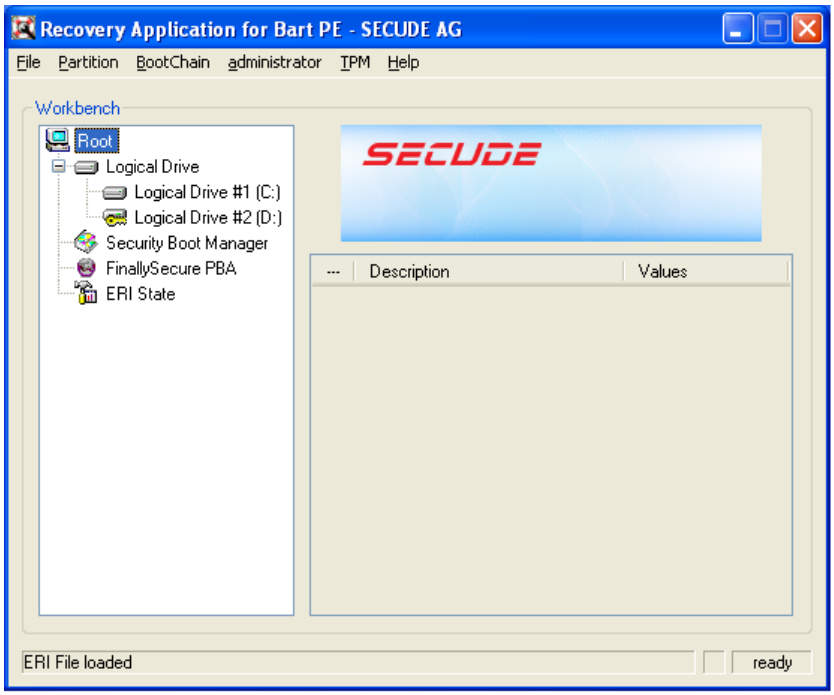
This section applies to standard hard drives. It does not apply to self-encrypting hard drives. For information about setting the Administration password for a device with a self-encrypting hard disk, see Section 10.5, “Erasing the Disk,” on page 53

The ZENworks Full Disk Encryption components (Full Disk Encryption Agent and ZENworks PBA) have an Administration password that is for internal administrative functions as well as several administrator functions available during ZENworks PBA login. The only time you should need to use this password is in conjunction with Novell Support.

The password is device specific and is randomly generated when a Disk Encryption policy is applied to the device. The password is recorded in ZENworks Control Center in the same location as the device’s ERI file (*Full Disk Encryption* > *Emergency Recovery*).

You can use the Emergency Recovery application to assign a new Administrator password to a device.

1 Make sure you have launched the Emergency Recovery application and loaded the device’s ERI file. See “Launching the Emergency Recovery Application” on page 35.



2 Click the *Administration* menu > *Set Admin Password.*

3 Specify a new password, then click *OK*.

4 Close the application.

10 Performing Recovery Operations on a Self-Encrypting Hard Disk

The following sections provide information about the emergency recovery operations you can perform on self-encrypting hard disks. For information about emergency recovery operations for standard hard disks, see Chapter 9, “Performing Recovery Operations on a Standard Hard Disk,” on page 41.

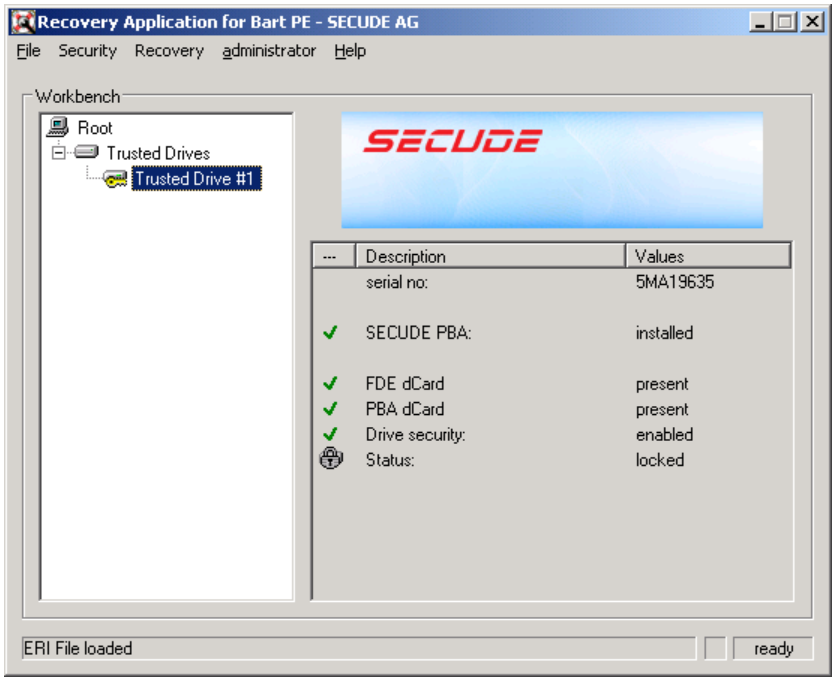
10.1 Unlocking a Drive

This section applies to self-encrypting hard drives. It does not apply to standard hard drives.

When a device powers down, the ZENworks PBA locks the self-encrypting hard disk. You can use the Emergency Recovery application to unlock the disk. After you unlock the disk, the ZENworks PBA is bypassed and the device boots directly to the Windows operating system

The disk remains unlocked unless the ZENworks PBA is still enabled. In that case, the next time the device powers down, the ZENworks PBA locks the disk.

1 Make sure you have launched the Emergency Recovery application and loaded the device's ERI file. See "Launching the Emergency Recovery Application" on page 35.



2 Click the *Security* menu > *Unlock Drive,* then click *Yes* when prompted to continue.

   The Emergency Recovery application unlocks the self-encrypting hard disk.

3 When the hard disk is unlocked, click *File* > *Exit* to close the application.

4 Restart the device.

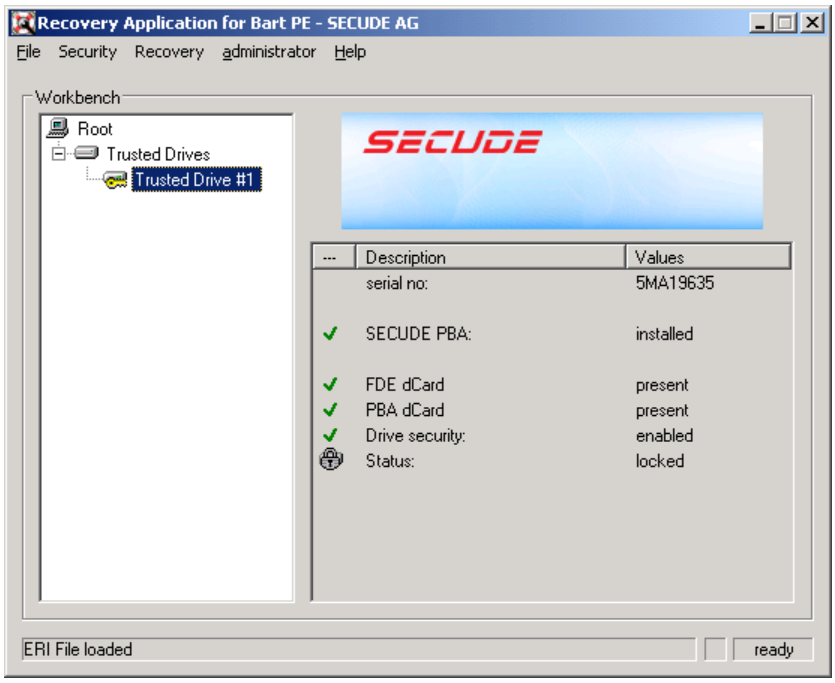
   The ZENworks PBA is bypassed and the device boots to Windows.

10.2 Deactivating the PBA

This section applies to self-encrypting hard drives. It does not apply to standard hard drives.

When you deactivate the ZENworks PBA, the PBA login is bypassed and the device boots directly to the Windows operating system. The PBA remains deactivated until you use the Emergency Recovery application to reactivate it. It can also be reactivated by removing the current Disk Encryption policy from the device (so that the ZENworks PBA is removed) and then reapplying a Disk Encryption policy (so that the ZENworks PBA is installed).

1 Make sure you have launched the Emergency Recovery application and loaded the device's ERI file. In necessary, see "Launching the Emergency Recovery Application" on page 35.



2 Click the *Recovery* menu > *Deactivate PBA*, then click *Yes* when prompted to continue.

The Emergency Recovery application deactivates the ZENworks PBA and unlocks the self-encrypting hard disk.

3 When the deactivation process is complete, click *File* > *Exit* to close the application.

4 Restart the device.

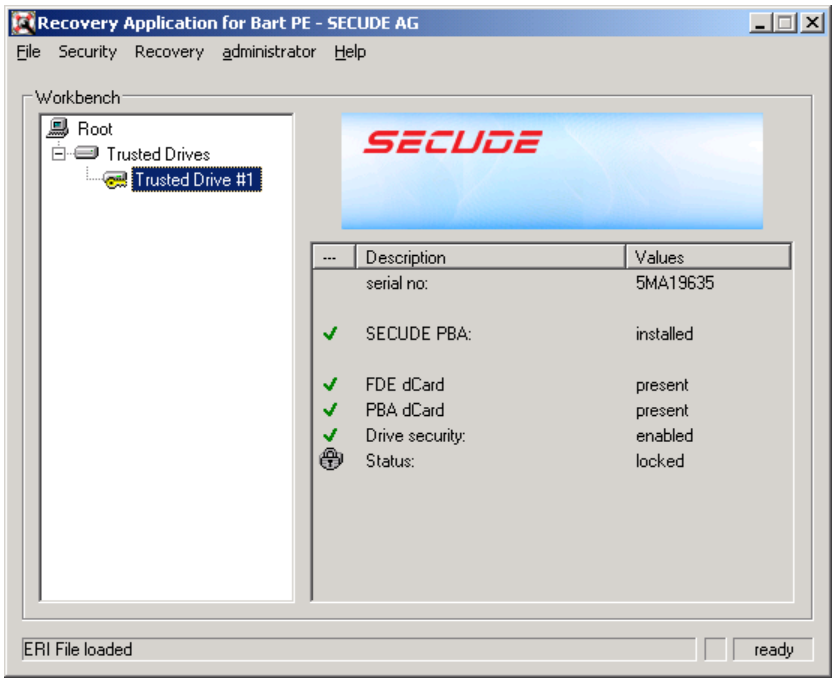
The device boots to Windows.

10.3 Activating the PBA

This section applies to self-encrypting hard drives. It does not apply to standard hard drives.

If you have deactivated the ZENworks PBA on a device (see Section 10.2, "Deactivating the PBA," on page 51), you can use the Emergency Recovery application to reactivate the PBA.

1 Make sure you have launched the Emergency Recovery application and loaded the device's ERI file. See "Launching the Emergency Recovery Application" on page 35.



2 Click the *Recovery* menu > *Activate PBA*, then follow the prompts.

3 When the deactivation process is complete, click *File* > *Exit* to close the application.

4 Shut down the device, then start it.

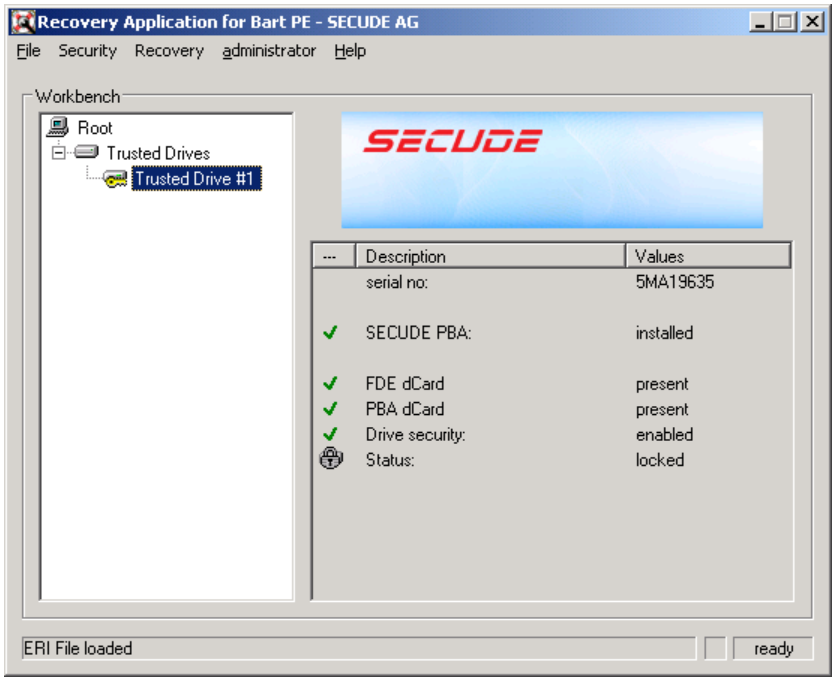
The device must be powered down. When it is started, the device boots to the ZENworks PBA.

10.4 Removing the PBA

This section applies to self-encrypting hard drives. It does not apply to standard hard drives.

When you remove the ZENworks PBA, the Linux system and PBA components are removed from the disks MBR shadow. The device then boots directly to the Windows operating system.

1 Make sure you have launched the Emergency Recovery application and loaded the device's ERI file. See "Launching the Emergency Recovery Application" on page 35.



2 Click the *Recovery* menu > *Remove PBA*, then follow the prompts.

The Emergency Recovery application removes the ZENworks PBA and unlocks the self-encrypting hard disk.

3 When the removal process is complete, click *File* > *Exit* to close the application.

4 Restart the device.

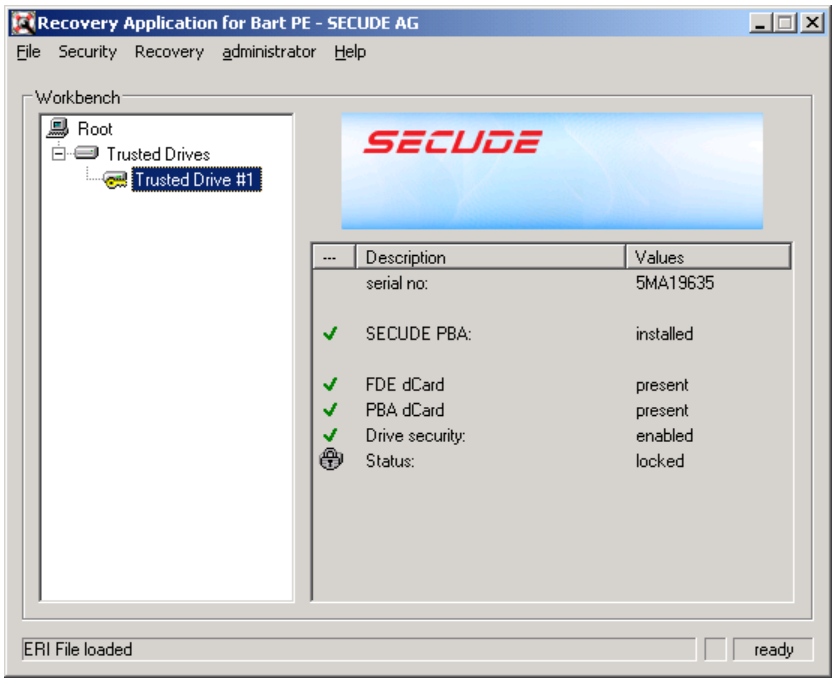
The device boots to Windows.

10.5 Erasing the Disk

This section applies to self-encrypting hard drives. It does not apply to standard hard drives.

The Emergency Recovery application can perform a secure erase of a self-encrypting hard disk. The process removes the ZENworks PBA, erases the encryption key from the disk's dCard, removes the ZENworks PBA, and resets the hard disk to factory settings. The data on the hard disk becomes unreadable and the disk is ready for reuse.

1 Make sure you have launched the Emergency Recovery application and loaded the device's ERI file. See "Launching the Emergency Recovery Application" on page 35.



2 Click the *Security* menu > *Crypto Erase*, then follow the prompts.

3 When the erasure process is complete, close the application.

4 Shut down the device.

10.6 Setting the Administration Password

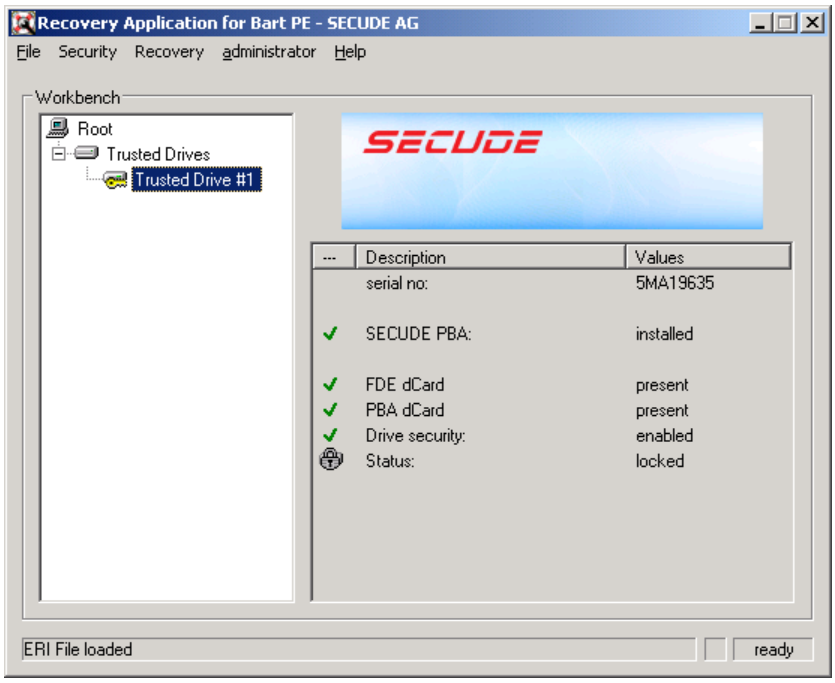
This section applies to self-encrypting hard drives. It does not apply to standard hard drives.

The ZENworks Full Disk Encryption components (Full Disk Encryption Agent and ZENworks PBA) have an Administration password that is for internal administrative functions as well as several administrator functions available during ZENworks PBA login. The only time you should need to use this password is in conjunction with Novell Support.

The password is device specific and is randomly generated when a Disk Encryption policy is applied to the device. The password is recorded in ZENworks Control Center in the same location as the device's ERI file (*Full Disk Encryption* > *Emergency Recovery Information*).

You can use the Emergency Recovery application to assign a new Administrator password to a device.

1 Make sure you have launched the Emergency Recovery application and loaded the device's ERI file. See "Launching the Emergency Recovery Application" on page 35.



2 Click the *Administration* menu > *Set Admin Password.*

3 Specify a new password, then click *OK*.

4 Click *File* > *Exit* to close the application.

11 Using the Emergency Recovery Console (Command Line)

You can use the Emergency Recovery console, a command line utility, to perform some of the same recovery operations as the Emergency Recovery application. The utility, which is included on both the Windows PE ERD and the Bart PE ERD, lets you enter console commands directly or include them in scripts to perform recovery tasks.

11.1 Running the Console on a Windows PE ERD

1. If the Emergency Recovery application is open, exit the application.

   When you exit the application, a command prompt window remains open.
2. At the command prompt, change to the following directory:

   `X:\Program Files\FinallySecure`
3. Run `pe_erd_console.exe` with the desired parameters. For information about parameters, see Section 11.3, “Console Parameters,” on page 57.

   You can also run the console without any parameters to display usage and option information.

11.2 Running the Console on a Bart PE ERD

1. Click the *Go* menu, then click *Command Prompt (CMD)*.

   When you exit the application, a command prompt window remains open.
2. Run `pe_erd_console.exe` with the desired parameters. For information about parameters, see Section 11.3, “Console Parameters,” on page 57.

   You can also run the console without any parameters to display usage and option information.

   If the console does not launch, change to the following directory and run pe_erd_console.exe again:

   `X:\Programs\FIS`

11.3 Console Parameters

Parameter	Details
eripath	The path to the ERI file. Enclose the path in quotation marks if it includes spaces.

Parameter	Details
eripwd	The password for the ERI file. Enclose the password in quotation marks if it includes spaces.
partition	The partition to decrypt.
/H	Displays information about the parameters.
/L	Loads the encryption keys to memory for all encrypted partitions.
/disable	Disables the ZENworks PBA. Applies only to self-encrypting hard disks.
/enable	Enables the ZENworks PBA. Applies only to self-encrypting hard disks.
/remove	Removes the ZENworks PBA from the device. Applies only to self-encrypting hard disks.
/mbr	Reinstalls the ZENworks Full Disk Encryption master boot record (MBR). Applies only to standard hard disks.
/org-mbr	Restores the original master boot record (MBR). Applies only to standard hard disks.
/tpmoff	Trusted Platform Module (TPM) is not supported. Do not use this parameter.
/tpmon	Trusted Platform Module (TPM) is not supported. Do not use this parameter.
/tpmrebind	Trusted Platform Module (TPM) is not supported. Do not use this parameter.

Example:

```
pe_erd_console.exe eripath=f:\dev1_20120315_1629.eri
eripwd=83DEBF516EAD0A4CB27F6328C5AB8342 partition=d
```

This example decrypts the D partition. The command prompt returns if the partition is decrypted successfully. If decryption is not successful, an error message is returned.

Example:

```
pe_erd_console.exe eripath=f:\dev1_20120315_1629.eri
eripwd=83DEBF516EAD0A4CB27F6328C5AB8342 /disable
```

This example deactivates the ZENworks PBA.

V Encrypted Device Imaging

The following sections provide instructions for imaging an encrypted device and restoring the image to the device:

12 Supported Imaging Applications

If you already have an imaging application that you use, you can continue to use that application to take images and restore images for devices that use ZENworks Full Disk Encryption.

You can also use the Imaging solution included with ZENworks Configuration Management. For information, see the *ZENworks 11 SP4 Preboot Services and Imaging Reference*.

13 Imaging a Hard Disk

Refer to your imaging application documentation for specific instructions about how to image a drive. As you do so, follow the requirements listed below.

Standard Hard Disk

- Do not use compression.

Self-Encrypting Hard Disk

- The device must be in a *warm start* state or the PBA must be temporarily deactivated. The device is in a warm start state only after a restart. Hibernate, shutdown, and standby all result in the device being in a cold start state.

14 Restoring an Image

Refer to your imaging application documentation for specific instructions about how to restore an image to a device. As you do so, follow the requirements listed below:

- Restore the image to the device from which it was taken. Restoring an image to a different device is not supported because differences in device hardware can cause failure or problems with the restored image. In some cases where the new device is identical to the old device, restoring an image might work; however, it is not supported by Novell Technical Services.