ZENworks 2017 Update 2

Full Disk Encryption Emergency Recovery Reference

February 2018

Legal Notice

Contents

About This Guide

This *ZENworks Full Disk Encryption Emergency Recovery Reference* provides information about preparing devices to enable emergency recovery and performing emergency recovering on devices.

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 documentation website.

1 What is Emergency Recovery?

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

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.

Emergency Recovery Disk and Application

ZENworks Full Disk Encryption provides an Emergency Recovery application that is a plug-in to Microsoft Windows Preinstallation Environment (Windows PE).

Windows PE enables 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. 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) or GUID partition tables (GPT), decrypt encrypted disks, deactivate the ZENworks PBA, and perform other recovery operations.

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, and 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.

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 Full Disk Encryption PBA Reference*.

2 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.

About ERI Files

To recover a device, the Emergency Recovery application (see Emergency Recovery Disks) 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:

Contents of ERI Files

An ERI file 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.

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.

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).

Retrieving ERI Files and Passwords

When a new ERI file is created for a device (see Creation of ERI Files), 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 Deleting ERI Files).

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

- Retrieving ERI files and passwords from a device List
- Retrieving ERI files and passwords from the zone List

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.

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.

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.

Deleting ERI Files in ZENworks Control Center

1. In ZENworks Control Center, click **Full Disk Encryption**.
2. Under FDE Agent Management, click **Emergency Recovery Information**.
3. 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.
4. Select the check boxes next to the ERI files to delete, then click **Delete**.

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 time stamp 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 time stamp 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
```

3 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:

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.

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 Assessment and Deployment Kit (ADK). Download the ADK for Windows 8 from the following location: https://www.microsoft.com/en-us/download/details.aspx?id=30652

  NOTE: The ZENworks recovery application is designed to work with an ERD created from the ADK for Windows 8.0 and Windows PE. The ERD can be used to recover devices on any Windows operating system.

- 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** > **Full Disk Encryption**.
  4. Click **ZFDE_WinPE_Plugin.zip** to download the zip file.
  5. Extract the downloaded zip file to `C:\` and rename the folder `winpe`.

     For example: `C:\winpe`

Create a Windows PE ERD

To create a Windows PE ERD:

1. Complete the Prerequisites for Creating a Windows PE Emergency Recovery Disk.
2. In the `C:\winpe` folder, right-click the `makepe.bat` file, and select **Run as administrator**.
3. When the Command Prompt opens, press **Enter** to keep the default setting, or type the other option number and press **Enter** to choose a different platform.
4. Press **Enter** for the next three commands or until the *Media type* option displays.
5. The *Media type* defaults to option **1**, **ISO**. Press **Enter**.
6. When presented with the option to copy the selected *architecture to directory*, type `Y`, and press **Enter**.

The Command Prompt runs through a series of tasks and creates the Emergency Recovery image `winpe.iso` in the directory.

7. Burn the `winpe.iso` image on to a DVD or CD to create your Emergency Recovery Disk (ERD).

The ERD is ready to use.

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 later Windows device. The steps are not supported on Windows XP or Vista. The USB drive size must be at least 256 MB.

To create a Windows PE emergency recovery USB drive:

1. Complete the Prerequisites for Creating a Windows PE Emergency Recovery Disk.
2. In the `C:\winpe` folder, right-click the `makepe.bat` file, and select **Run as administrator**.
3. When the Command Prompt opens, press **Enter** to keep the default setting or type the other option number to choose a different platform, and press **Enter**.
4. Press **Enter** for the next three commands or until the *Media type* option displays.
5. The *Media type* defaults to option **1**, **ISO**. Type `2` for the USB Flash Drive, and press **Enter**.
6. When the default USB drive letter appears, press **Enter** if your USB drive is **F**, or type the letter that matches your USB drive, and press **Enter**.
7. When presented with the option to copy the selected *architecture to directory*, type `Yes`, and press **Enter**.
8. When the MakeWinPEMedia and Format warning display, type `Y` to proceed with the formatting of the USB drive.

   When the ERD formatting is done, the Command Prompt displays the following:

   Success

   USB Flash Drive: f: (or other drive letter)

   Done!

The USB drive is ready to use as an ERD.

4 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.

Launching the Emergency Recovery Application

The following sections explain how to launch the Emergency Recovery application from a bootable Windows PE 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.

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 and Creating a Windows PE Emergency Recovery USB Drive.
- 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 Retrieving ERI Files and Passwords.

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 boot-up 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.

   NOTE: If the application does not start, use the command prompt to change to the `X:\Program Files\FDE` 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 About ERI Files for more information.

The Emergency Recovery application displays that the file is loaded.

4 Perform the necessary recovery operations. See Performing Recovery Operations for instructions.

Performing Recovery Operations

The following sections provide information about the emergency recovery operations you can perform.

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.
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.

Repairing the Master Boot Record

When a Disk Encryption policy is applied to a device, the ZENworks Full Disk Encryption Agent creates a 500 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.
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.

Restoring the Original Master Boot Record

When a Disk Encryption policy is applied to a Windows device, the ZENworks Full Disk Encryption Agent creates a 500 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.
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.

Erasing the Disk

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.
2. Click the **Administration** menu > **Erase Harddrive**, 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.

Setting the Administration Password

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 Micro Focus 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.
2. Click the **Administration** menu > **Set admin-password.**
3. Specify a new password, and then click **OK**.
4. Close the application.

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 the Windows PE ERD, lets you enter console commands directly or include them in scripts to perform recovery tasks.

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 Console Parameters.

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

Console Parameters

Parameter	Details
eripath	The path to the ERI file. Enclose the path in quotation marks if it includes spaces.
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.
/mbr	Reinstalls the ZENworks Full Disk Encryption master boot record (MBR).
/org-mbr	Restores the original master boot record (MBR).
/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.

5 Encrypted Device Imaging

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

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 Preboot Services and Imaging Reference*.

Imaging a Hard Disk

Refer to your imaging application documentation for specific instructions about how to image a drive. As you do so, do not use compression on the hard disk.

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 Micro Focus Technical Services.