Recovering Encrypted Disks Using Windows Preinstallation Environment

Technical Note

Symantec

Contents

Preface

Documentation version: 11.0.0, Release Date: October, 2014

Legal Notice

Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades

- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Chapter 1

Introduction to Windows Preinstallation Environment

This chapter includes the following topics:

- Overview
- Supported Versions of Windows PE
- How to Obtain Windows PE

Overview

The Microsoft Windows Preinstallation Environment (PE) is widely used by IT professionals in Windows environments for installation tasks, deployment, maintenance, troubleshooting, diagnosis, recovery, and so on.

When an encrypted disk fails to start the Windows operating system, recovery of data becomes the primary goal. Creating a customized Windows PE CD or UFD (USB Flash Drive) provides a bootable recovery tool that can be used for rescue purposes.

To create a bootable Windows PE CD or UFD, you must do the following:

- Pre-install the SEE Drive Encryption driver for decrypting the hard disk.
- Pre-install the SEE Drive Encryption tools for authentication.

This document provides instructions for creating and using both 32-bit and 64-bit Windows Preinstallation Environment.

Supported Versions of Windows PE

Currently, the following versions of Windows PE are supported:

- Windows Server 2008 R2 (Standard and Enterprise SP1 Editions x64 bit): Windows PE version 4.0 and 5.0
- Windows 7 (BIOS) (Pro, Enterprise, and Ultimate Editions): Windows PE version 4.0 and 5.0
- Windows 8 (BIOS and UEFI) (Pro and Enterprise Editions): Windows PE version 4.0 and 5.0
- Windows 8.1 (BIOS and UEFI) (Pro and Enterprise Editions): Windows PE version 5.0
- Windows Server 2012 R2 (Standard and Datacenter Editions x64 bit): Windows PE version 5.0

How to Obtain Windows PE

To use Windows PE, you must obtain and install the Windows Assessment and Development Kit (Windows ADK for Windows PE 4.0, 5.0, and 5.1) from the following location:

http://www.microsoft.com/en-us/download/details.aspx?id=30652

Chapter 2

Creating a Windows PE CD or UFD

This chapter includes the following topics:

- Creating a Windows PE Image
- Customizing Windows PE 4.0 and 5.0 for 32-bit Windows Environment
- Customizing Windows PE 4.0 and 5.0 for 64-bit Windows Environment

Creating a Windows PE Image

Before you create the image, ensure that you do the following:

- Install Windows Assessment and Development Kit (ADK).
- Install Symantec Endpoint Encryption Drive Encryption.
- Create a folder on the C drive to install SEE Drive Encryption driver and tools, such as C:\EEDE.

Note: You must use the deployment tools command prompt as an administrator when creating the Windows PE image.

To create the Windows PE image

1. To open the deployment tools command prompt with the correct path variables, select **Start** > **All Programs** > **Windows Kits** > **Windows ADK**.
2. Do one of the following:
   - To create an image for 32-bit Windows environment, run the following command:

```
copype.cmd x86 C:\winpe_x86
```

This command creates the Windows PE image at C:\winpe_x86.

- To create an image for 64-bit Windows environment, run the following command:

```
copype.cmd amd64 C:\winpe_amd64
```

This command creates the Windows PE image at C:\winpe_amd64

Customizing Windows PE 4.0 and 5.0 for 32-bit Windows Environment

Ensure that you have copied Windows PE in the Windows folder c:\winpe_x86 and is ready for customization.

To copy Windows PE in the Windows folder c:\winpe_x86

- Run the following command:

```
xcopy c:\winpe_x86\media\sources\boot.wim c:\winpe_x86\winpe.wim
```

Note: Follow the instructions that are provided in the *Windows Preinstallation Environment User's Guide* to prepare a drive or folder for customization. The *Windows Preinstallation Environment User's Guide* is included with the Windows Assessment and Development Kit (ADK).

To customize Windows PE, you must:

- Install the SEE Drive Encryption tools.
- Create the bootable ISO file and CD or UFD.

Installing the SEE Drive Encryption tools for 32-bit Windows Environment

---

Note: The eedRecoveryGui.exe file is used to open the Symantec Disk Recovery utility. This utility provides an interface during recovery to help you decrypt and access your encrypted disks.

To install the SEE Drive Encryption tools

1. Copy the following files into the Windows folder c:\eede. These files can be copied from the Drive Encryption installation directory (from a system that has Symantec Endpoint Encryption Drive Encryption installed).

- C:\Program Files\Symantec\Endpoint Encryption Clients\Drive Encryption\eedAdminCli.exe
- C:\Program Files\Symantec\Endpoint Encryption Clients\Drive Encryption\eedDEAL.dll
- C:\Program Files\Symantec\Endpoint Encryption Clients\Drive Encryption\eedEngine.dll
- C:\Program Files\Symantec\Endpoint Encryption Clients\Drive Encryption\eedPE.exe
- C:\Program Files\Symantec\Endpoint Encryption Clients\Drive Encryption\eedRecoveryGui.exe
- C:\Program Files\Symantec\Endpoint Encryption Clients\Drive Encryption\eedStart.exe
- C:\Program Files\Symantec\Endpoint Encryption Clients\Drive Encryption\pgpbootb.bin
- C:\Program Files\Symantec\Endpoint Encryption Clients\Drive Encryption\pgpbootg.bin
- C:\Program Files\Symantec\Endpoint Encryption Clients\Drive Encryption\PGPce.dll
- C:\Program Files\Symantec\Endpoint Encryption Clients\Drive Encryption\PGPce.dll.sig
- C:\Program Files\Symantec\Endpoint Encryption Clients\Drive Encryption\stage1
- %SYSTEMROOT%\system32\SHFOLDER.dll
- %SYSTEMROOT%\system32\drivers\eedDiskEncryptionDriver.sys

2 Open the Windows command prompt (as an administrator) and run the following commands:

```
cd c:\eede
```

```
eedpe /winpe c:\winpe_x86 c:\eede
```

3 Copy the file c:\winpe_x86\winpe.wim to c:\winpe_x86\media\sources\boot.wim and overwrite the old boot.wim file. To copy, run the following command:

```
xcopy /y c:\winpe_x86\winpe.wim
c:\winpe_x86\media\sources\boot.wim
```

4 Close the command prompt.

Creating the bootable ISO file and CD or UFD

The next step is to make the customized Windows PE as a bootable .iso file and CD or UFD.

To create the bootable .iso file or CD

1. To open the deployment tools command prompt, select **Start** > **All Programs** > **Windows Kits** > **Windows ADK**.
2. As an administrator, run the following command:

   ```
   MakeWinPEMedia /ISO C:\WinPE_x86 C:\WinPE_x86\WinPE_x86.iso
   ```

3. Use the CD-record software to burn the CD image file of winpe_x86.iso.

To create a bootable UFD

1. Use the file diskpart.exe in Windows to format the UFD.
2. Open the Windows command prompt as an administrator and run the following commands (the following sample commands assume that disk 1 is the UFD):

   ```
   diskpart

   select disk 1

   clean

   create a partition primary

   select partition 1

   active

   format fs=fat32

   assign

   exit
   ```

3. Open the deployment tools command prompt as an administrator and run the following command (the following sample command assumes that F: is the UFD device):

   ```
   MakeWinPEMedia /UFD C:\WinPE_x86 F:
   ```

Customizing Windows PE 4.0 and 5.0 for 64-bit Windows Environment

Ensure that you have copied Windows PE in the Windows folder c:\winpe_amd64 and is ready for customization.

To copy Windows PE in the Windows folder c:\winpe_amd64

- Run the following command:

```
xcopy c:\winpe_amd64\media\sources\boot.wim
c:\winpe_amd64\winpe.wim
```

Note: Follow the instructions that are provided in the *Windows Preinstallation Environment User's Guide* to prepare a drive or folder for customization. The *Windows Preinstallation Environment User's Guide* is included with the Windows Assessment and Development Kit (ADK).

To customize Windows PE, you must:

- Install the SEE Drive Encryption tools.
- Create the bootable ISO file and CD or UFD.

Installing the SEE Drive Encryption tools for 64-bit Windows Environment

---

Note: The eedRecoveryGui.exe file is used to open the Symantec Disk Recovery utility. This utility provides an interface during recovery to help you decrypt and access your encrypted disks.

To install the SEE Drive Encryption tools

1. Copy the following files into the Windows folder c:\eede. These files can be copied from the Drive Encryption installation directory (from a system that has Symantec Endpoint Encryption Drive Encryption installed).
   - C:\Program Files\Symantec\Endpoint Encryption Clients\Drive Encryption\eedAdminCli.exe
   - C:\Program Files\Symantec\Endpoint Encryption Clients\Drive Encryption\eedDEAL.dll
   - C:\Program Files\Symantec\Endpoint Encryption Clients\Drive Encryption\eedEngine.dll

- C:\Program Files\Symantec\Endpoint Encryption Clients\Drive Encryption\eedPE.exe
- C:\Program Files\Symantec\Endpoint Encryption Clients\Drive Encryption\eedRecoveryGui.exe
- C:\Program Files\Symantec\Endpoint Encryption Clients\Drive Encryption\eedStart.exe
- C:\Program Files\Symantec\Endpoint Encryption Clients\Drive Encryption\pgpbootb.bin
- C:\Program Files\Symantec\Endpoint Encryption Clients\Drive Encryption\pgpbootg.bin
- C:\Program Files\Symantec\Endpoint Encryption Clients\Drive Encryption\PGPce.dll
- C:\Program Files\Symantec\Endpoint Encryption Clients\Drive Encryption\PGPce.dll.sig
- C:\Program Files\Symantec\Endpoint Encryption Clients\Drive Encryption\stage1
- %SYSTEMROOT%\system32\SHFOLDER.dll
- %SYSTEMROOT%\system32\drivers\eedDiskEncryptionDriver.sys

2. Open the Windows command prompt (as an administrator) and run the following commands:

```
cd c:\eede
```

```
eedpe /winpe c:\winpe_amd64 c:\eede
```

3. Copy the file c:\winpe_amd64\winpe.wim to c:\winpe_amd64\media\sources and overwrite the old boot.wim file. To copy, run the following command:

```
xcopy /y c:\winpe_amd64\winpe.wim
c:\winpe_amd64\media\sources\boot.wim
```

4. Close the Windows command prompt.

Creating the bootable ISO file and CD or UFD

The next step is to make the customized Windows PE as a bootable .iso file and CD or UFD.

To create the bootable .iso file or CD

1. To open the deployment tools command prompt, select **Start** > **All Programs** > **Windows Kits** > **Windows ADK**.
2. As an administrator, run the following command:

   ```
   MakeWinPEMedia /ISO C:\WinPE_amd64 C:\WinPE_amd64\WinPE_amd64.iso
   ```

3. Use the CD-record software to burn the CD image file of WinPE_amd64.iso file.

To create a bootable UFD

1. Use the file diskpart.exe in Windows to format the UFD.
2. Open the Windows command prompt as an administrator and run the following commands (the following sample commands assume that disk 1 is the UFD):

   ```
   diskpart

   select disk 1

   clean

   create a partition primary

   select partition 1

   active

   format fs=fat32

   assign

   exit
   ```

3. Open the deployment tools command prompt as an administrator and run the following command (the following sample command assumes that F: is the UFD device):

   ```
   MakeWinPEMedia /UFD C:\WinPE_amd64 F:
   ```

Chapter 3

Using a customized Windows PE CD or UFD for recovery

This chapter includes the following topics:

- Accessing an encrypted disk
- Accessing an encrypted disk using the administrator command line
- Accessing an encrypted disk using the Symantec Disk Recovery Utility

Accessing an encrypted disk

You can use the customized Windows PE CD or UFD to access the encrypted disk in one of the following ways:

- Using the SEE Drive Encryption administrator command line
- Using the Symantec Disk Recovery Utility

Accessing an encrypted disk using the administrator command line

When you start your system in a Window PE environment using the customized Windows PE CD or UFD, the SEE Drive Encryption administrator command prompt appears. You can use the administrator command line to do the following:

- Recover the preboot screen of the client computer when a user fails to authenticate at preboot or the preboot screen is unavailable.

- Restore the previous master boot record (MBR) of the client computer after restoring from a volume backup.
- Decrypt an encrypted disk using the client administrator authentication.
- Decrypt an encrypted disk using Help Desk Recovery (for managed clients) or Advanced Help Desk Recovery (for unmanaged clients).

Recovering the preboot screen

To recover the preboot screen

1. Start the system in Window PE environment using the customized Windows CD or UFD.
2. At the administrator command prompt, run the following command:

   ```
   eedAdminCli --recover
   ```

Restoring the old MBR

To restore the old MBR

1. Start the system in Window PE environment using the customized Windows CD or UFD.
2. At the administrator command prompt, run the following command:

   ```
   eedAdminCli --fixmbr
   ```

   The command replaces the current MBR with the old MBR.

Decrypting an encrypted disk using the client administrator credentials

To decrypt an encrypted disk using the client administrator credentials

1. Start the system in Window PE environment using the customized Windows CD or UFD.
2. To decrypt an encrypted disk, run the following command at the administrator command prompt:

   ```
   eedAdminCli --decrypt --disk <number> --au <AdminUserName> --ap
   <AdminPassword>
   ```

   Where, `<number>` is the disk number on the system, `<AdminUserName>` and `<AdminPassword>` are the user name and password of the client administrator. For example,

   ```
   eedAdminCli --decrypt --disk 0 --au clientadmin1 --ap password1
   ```

3. To check the progress of decryption, run the following command at the administrator command prompt periodically:

   ```
   eedAdminCli --status --disk <number>
   ```

   Where, `<number>` is the disk number on the system. For example,

   ```
   eedAdminCli --status --disk 0
   ```

Decrypting an encrypted disk using the Help Desk Recovery commands

To decrypt an encrypted disk using Help Desk Recovery

1. Call your help desk administrator.
2. Start the system in Window PE environment using the customized Windows CD or UFD.
3. To view the name and sequence number of the computer, run the following command at the administrator command prompt:

   ```
   eedAdminCli --helpdesk-recovery
   ```

4. Read out the displayed computer name and sequence number to the help desk administrator.

5 Note down the response key of the computer that the help desk administrator provides.

6 To use the response key and decrypt, run the following command at the administrator command prompt:

```
eedAdminCli --decrypt --response-key <response-key>
```

Where, `<response-key>` is the response key that the help desk administrator provides.

To decrypt an encrypted disk using Advanced Help Desk Recovery

1 Call your help desk administrator.

2 Start the system in Window PE environment using the customized Windows CD or UFD.

3 To view the name, sequence number, and challenge key of the computer, run the following command at the administrator command prompt:

```
eedAdminCli --helpdesk-recovery --verbose
```

4 Read out the displayed computer name, sequence number, and challenge key to your help desk administrator.

5 Note down the response key of the computer that the help desk administrator provides.

6 To use the response key and decrypt, run the following command at the administrator command prompt:

```
eedAdminCli --decrypt --response-key <response-key>
```

Where, `<response-key>` is the response key that the help desk administrator provides

Accessing an encrypted disk using the Symantec Disk Recovery Utility

Symantec Disk Recovery Utility provides an interface for you to enter your credentials for authentication, select the disk that you want to decrypt, and track the progress of decryption. The utility decrypts the entire disk and does not decrypt a partition.

Note: Ensure that you provide an uninterrupted power supply to your computer when decryption is in progress.

To open the Symantec Disk Recovery Utility

1. Start the system in Window PE environment using the customized Windows CD or UFD.
2. At the administrator command prompt, type `eedRecoveryGUI.exe`, and press Enter.
3. In the **Symantec Disk Recovery Utility** welcome screen, click **Next**.
4. From the **Choose a physical drive to process** list, select the encrypted disk that you want to access, and then click **Next**.

   This list displays only the disks that are encrypted. The list does not show any unencrypted disks, external disks, or removable drives.
5. Select one of the options for authentication. Your options are:
   - **Client Admin**
     You can use the authentication credentials of the client administrator .
   - **Help Desk Recovery**
     You can use the response key that the help desk administrator provides to decrypt the encrypted disk.

Decrypting an encrypted disk using the client administrator authentication

To decrypt an encrypted disk using the client administrator authentication

1. In the **Symantec Disk Recovery Utility** dialog box, select the **Client Admin** option.
2. Do the following:
   - Type the user name of the client administrator in the **Username** box.
   - Type the password of the client administrator in the **Password** box.
3. Click **Next**.
4. Read the message about the uninterrupted power supply, and then click **OK**.

   The utility displays a progress bar to indicate the progress of decryption.
5. After the decryption of the disk is complete, in the confirmation dialog box, click **OK**.

Decrypting an encrypted disk using Help Desk Recovery

To decrypt an encrypted disk using Help Desk Recovery

1. In the **Symantec Disk Recovery Utility** dialog box, select the **Help Desk Recovery** option.
2. Call the help desk administrator for authentication.
3. Provide the following information from the **Symantec Disk Recovery Utility** dialog box to your help desk:
   - **Computer**
     The domain and the name of the computer.
   - **Sequence No.**
     A four-digit number that is used to synchronize a client with the server.
4. If the help desk administrator fails to retrieve your computer information and requests you to use the Advanced Help Desk Recovery, then press F5. The **Symantec Disk Recovery Utility** dialog box displays the **Challenge Key**. Provide the challenge key to your administrator.
5. Note down the response key that the help desk administrator provides.
6. Type the response key in the **Response Key** box, and then click **Next**.
7. Read the message about uninterrupted power supply, and then click **OK**.

   The utility displays a progress bar to indicate the progress of decryption.
8. After the decryption of the disk is complete, in the confirmation dialog box, click **OK**.