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.

Copyright © 2012-13 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

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/tmplist.html).

Third-Party Materials

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

About This Guide 5

Part I Installation and Removal 7

1 System Requirements 9

2 Installing the Full Disk Encryption Agent 13

3 Uninstalling the Full Disk Encryption Agent 15
   3.1 Using ZENworks Control Center to Uninstall the Full Disk Encryption Agent 15
   3.2 Uninstalling the Full Disk Encryption Agent Locally 16
   3.3 Uninstalling the ZENworks Adaptive Agent 17

4 Decommissioning a Device 19
   4.1 Temporarily Decommissioning a Device 19
   4.2 Permanently Decommissioning a Device 20

5 Moving a Managed Device From One Zone to Another Zone 23
   5.1 Moving a Device to a Zone Where Full Disk Encryption Is Not Active 23
   5.2 Moving a Device to a Zone Where Full Disk Encryption Is Active 24

Part II Disk Encryption 25

6 Viewing the Disk Encryption Settings 27

7 Decrypting Drives 29

Part III Pre-Boot Authentication 31

8 Viewing the Pre-Boot Authentication Settings 33

9 Enabling User Capturing 35

10 Managing PBA User Accounts 37

11 Synchronizing the PBA and Windows Credentials 39
   11.1 Using the Windows Login 39
   11.2 Using the Full Disk Encryption Agent 39
About This Guide

The ZENworks 11 SP2 Full Disk Encryption Agent Guide provides information to help you manage the Full Disk Encryption Agent. The information in this guide is organized as follows:

- Part I, “Installation and Removal,” on page 7
- Part II, “Disk Encryption,” on page 25
- Part III, “Pre-Boot Authentication,” on page 31
- Part IV, “Troubleshooting,” on page 43
- Part V, “Appendixes,” on page 59

Audience

This guide is intended for ZENworks administrators who need to configure, manage, and troubleshoot the Full Disk Encryption Agent.

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 Management 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 SP2 documentation Web site (http://www.novell.com/documentation/zenworks11).
Installation and Removal

- Chapter 1, “System Requirements,” on page 9
- Chapter 2, “Installing the Full Disk Encryption Agent,” on page 13
- Chapter 3, “Uninstalling the Full Disk Encryption Agent,” on page 15
- Chapter 4, “Decommissioning a Device,” on page 19
- Chapter 5, “Moving a Managed Device From One Zone to Another Zone,” on page 23
The ZENworks 11 SP2 Installation Guide provides a list of software and hardware requirements that must be met to install the ZENworks Adaptive Agent on a device (see “Managed Device Requirements”). Devices that you want to use for ZENworks Full Disk Encryption must meet those requirements. Any additions or exceptions to those requirements are provided in the following list:

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>• Windows XP Professional (x86) with SP2 or SP3</td>
</tr>
<tr>
<td></td>
<td>• Windows Vista (x86 and x86-64) with SP1 or SP2 — Business, Ultimate, and Enterprise versions only</td>
</tr>
<tr>
<td></td>
<td>• Windows 7 (x86 and x86-64) with or without SP1 — Professional, Ultimate, and Enterprise versions only</td>
</tr>
<tr>
<td></td>
<td>• Windows 8 (x86 and x86-64) — Professional and Enterprise versions only</td>
</tr>
<tr>
<td>Firmware</td>
<td>BIOS firmware is required. UEFI firmware is not supported.</td>
</tr>
</tbody>
</table>
### Hard Disks: Standard (no self-encrypting mechanism)

**Disks:**
- IDE, SATA, and PATA hard disks are supported. SCSI and RAID hard disks are not supported.
- Multiple standard disks (one primary and multiple secondary) are supported in one device. When using multiple disks, all disks must be the same (for example, all IDE or all SATA).
- Encryption of both standard and self-encrypting hard disks in the same device are not supported. A device can have standard disks or it can have self-encrypting disks, but it cannot have both.

**Disk communication modes:**
- ATAPI and AHCI are supported.
- When using ZENworks Pre-Boot Authentication, we strongly recommend that you use the standard Microsoft drivers. Other drivers can cause issues such as CD and DVD drives disappearing.

**Supported disk types:**
- Basic disks are supported. Dynamic disks and other disk types are not supported.

**Supported file system:**
- NTFS is supported. FAT32 and all other file system formats are not supported.

**Partition tables and partitions:**
- All disks must use a master boot record (MBR) partition table. GUID partition tables (GPT) are not supported.
- ZENworks Full Disk Encryption creates a primary partition (referred to as the ZENworks primary partition) on the system disk to store files required for encryption and pre-boot authentication. Windows supports a maximum of four primary partitions; one primary partition must be available for ZENworks Full Disk Encryption. If all four primary partitions already exist, ZENworks Full Disk Encryption cannot create the required ZENworks primary partition and encryption fails.
- A maximum of 10 partitions can be encrypted. The partitions can be on one disk or spread across multiple disks.

**Disk space:**
- 100 MB of free disk space on the primary (system) hard disk for the ZENworks primary partition that is created when the Disk Encryption policy is applied. To create the 100 MB partition, 300 MB of disk space must be available or the creation process will fail.
- 140 MB of free disk space on the system volume for ZENworks Full Disk Encryption software files.
### System Requirements

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| Hard Disks: Self-Encrypting   | • Seagate Momentus (FDE.x) hard disks that are based on DriveTrust technology and support Enterprise-mode (as compared to BIOS-only mode).  
• 140 MB of free disk space on the system volume for ZENworks Full Disk Encryption software files.  
• Encryption of both standard and self-encrypting hard disks in the same device are not supported. A device can have multiple standard disks or it can have multiple self-encrypting disks, but it cannot have both. When using multiple standard disks, all disks must be the same (for example, all IDE or all SATA). |
| Drivers                       | When using ZENworks Pre-Boot Authentication, we strongly recommend that you use the Microsoft IDE/SATA drivers. Other drivers can cause issues such as CD and DVD drives disappearing.                           |
| Virtual Machines              | Virtual machines must meet the requirements listed above and in “Managed Device Requirements” in the ZENworks 11 SP2 Installation Guide, with the following exception:  
• VMs can have only one hard disk. Virtual machines with multiple hard disks are not supported. |
| Smart Cards                   | ZENworks Pre-Boot Authentication (PBA) supports smart card authentication. For a list of supported smart card solutions, see Appendix A, “Supported Smart Card Terminals and Tokens,” on page 61.                                      |
| Single Sign-On                | ZENworks Pre-Boot Authentication (PBA) supports single sign-on with Windows via both the Windows Client and the Novell Client. When using the Novell Client, the following requirements apply:  
• Novell Client 2 SP2 IR1 is required on Windows 7 and Windows Vista.  
• When using user ID/password authentication with the Novell Client and DLU, the user needs to log in to the Novell Client once before single sign-on will work. During single sign-on, the ZENworks PBA passes the user ID and password to the Novell Client. However, the client requires other details (tree, server, context, and so forth) that are available only if the user has populated the details during a previous log in.  
• When using smart card authentication with the Novell Client, NESCM (Novell Enhanced Smart Card Method), and DLU, the user needs to be the last user to have logged in to the Novell Client. During single sign-on, the ZENworks PBA passes the pin to the Novell Client. However, the client requires other details (tree, server, context, and so forth) that are available only if the user was the last smart card user to log in to the client.  
• Smart card authentication with the Novell Client, NESCM, and Disconnected Workstation Only mode is not supported. |
Installing the Full Disk Encryption Agent

The Full Disk Encryption Agent is the ZENworks Adaptive Agent module that is responsible for enforcing Disk Encryption policy settings on managed devices. Because it is a module, it can be installed, enabled, disabled, and uninstalled without affecting the other capabilities provided by the Adaptive Agent. The following operational states are possible for the Full Disk Encryption Agent:

- **Installed and enabled:** The Full Disk Encryption Agent is installed and can enforce a Disk Encryption policy assigned to the device.
- **Installed and disabled:** The Full Disk Encryption Agent is installed but its drivers are not loaded. Therefore it cannot enforce a Disk Encryption policy assigned to the device.
- **Uninstalled:** The Full Disk Encryption Agent is not installed on the device.

By default, the Full Disk Encryption Agent is installed and enabled on managed devices if ZENworks Full Disk Encryption is activated in either license mode or evaluation mode. If you want to change the operational state of the agent, see the instructions in “Customizing the Agent Features” in the *ZENworks 11 Discovery, Deployment, and Retirement Reference*.

**IMPORTANT:** ZENworks Full Disk Encryption is not supported on devices that use UEFI firmware; BIOS firmware is required. The Full Disk Encryption Agent will not be installed to any UEFI devices in your ZENworks Management Zone.
There are several methods you can use to uninstall the Full Disk Encryption Agent from a device:

- Section 3.1, “Using ZENworks Control Center to Uninstall the Full Disk Encryption Agent,” on page 15
- Section 3.2, “Uninstalling the Full Disk Encryption Agent Locally,” on page 16
- Section 3.3, “Uninstalling the ZENworks Adaptive Agent,” on page 17

### 3.1 Using ZENworks Control Center to Uninstall the Full Disk Encryption Agent

The recommended way to uninstall the Full Disk Encryption Agent is through the ZENworks Control Center:

1. If the device has a Disk Encryption policy assigned to it, remove the policy assignment in ZENworks Control Center. See “Removing Policy Assignments From Devices” in the ZENworks 11 SP2 Full Disk Encryption Policy Reference.

   Removing the policy assignment causes the Full Disk Encryption Agent to decrypt the drives and remove the ZENworks PBA. You are not required to remove the policy prior to uninstalling the Full Disk Encryption Agent (the agent uninstall removes the policy if it is still applied), but doing so is a recommended best practice.

2. Uninstall the Full Disk Encryption Agent:
   - **2a** Log in to ZENworks Control Center.
   - **2b** To uninstall the module from a single device, click Devices, click the device to display it’s details, click the Settings tab, click Device Management, then click ZENworks Agent.
     
     or

     To uninstall the module from all device’s in a device folder, click Devices, select the check box next to the device folder and click Details to display the folder details, click the Settings tab, click Device Management, then click ZENworks Agent.

     or

     To uninstall the module from all device’s in the zone, click Configuration, click Device Management (under Management Zone Settings), then click ZENworks Agent.

   - **2c** (Conditional) If you are uninstalling from a single device or a device folder, click Override to enable the settings to be modified.

   - **2d** Under Agent Features, deselect the Installed check box for Full Disk Encryption.

   - **2e** Click OK to save the change.
2f Perform an agent refresh on the target device (or devices).

The refresh takes longer than normal as the Full Disk Encryption Agent is removed. When the refresh completes, you can view the ZENworks Adaptive Agent's property pages (double-click the icon in the notification area) to verify that Full Disk Encryption is no longer listed. In addition, the Full Disk Encryption Agent is no longer available in the Start menu.

3.2 Uninstalling the Full Disk Encryption Agent Locally

The recommended way to uninstall the Full Disk Encryption Agent is through the Agent Features setting in ZENworks Control Center (see Section 3.1, “Using ZENworks Control Center to Uninstall the Full Disk Encryption Agent,” on page 15). This method requires the device to have network access to a ZENworks Server.

If a device does not have network access, you can use the following steps to uninstall the Full Disk Encryption Agent locally:

1 Make sure you know the uninstall password for the ZENworks Adaptive Agent (if one is defined).

If an uninstall password is defined, it is required when locally uninstalling the Full Disk Encryption Agent. The password is defined in ZENworks Control Center under Configuration > Management Zone Settings > Device Management > ZENworks Agent.

2 Uninstall the Full Disk Encryption Agent:

2a Remove the agent API by running the following Windows Installer command at a command prompt:

For a Windows 32-bit device:

```
msiexec.exe /x {6BA0056E-7559-45FF-AC4C-A3D9588E2B25} /L*v C:\WINDOWS\novell\zenworks\bin\zfde_api_uninstall_log.txt FDESHOWNUNINSTALLWARNING=1
```

For a Windows 64-bit device:

```
msiexec /x {780D6F24-F9A9-4688-AFEF-6801237A53C0} /L*v C:\WINDOWS\novell\zenworks\bin\zfde_api_uninstall_log.txt FDESHOWNUNINSTALLWARNING=1
```

2b (Conditional) If you are prompted for the uninstall password, provide the password.

2c (Conditional) If a Disk Encryption policy is still applied to a device, you are prompted that the disk must be decrypted before the uninstall can be performed. Click OK to start decryption of the disk and removal of the ZENworks PBA.

The process decrypts the disk, removes the ZENworks PBA, and reboots the device (according to the reboot option set for the policy). You can use the Full Disk Encryption Agent’s About box to verify that the policy is no longer being enforced. When the process is complete, run the command in Step 2a again.

You can view the zfde_api_uninstall_log.txt file to verify that the uninstall is successful. The status is recorded in the last few lines of the log file.

2d Remove the agent drivers by running the following Windows Installer command at a command prompt (for both Windows 32-bit and 64-bit devices):

```
msiexec /x {CD19D7B6-F08E-489D-8808-3C0FAD1265EB} /L*v C:\WINDOWS\novell\zenworks\bin\zfde_sec_uninstall_log.txt
```
You can view the `zfde_sec_uninstall_log.txt` file to verify that the uninstall is successful. The status is recorded in the last few lines of the log file.

2e Remove the agent policy handler by running the following Windows Installer command at a command prompt (for both Windows 32-bit and 64-bit devices):

```
msiexec /x {14588647-0376-45A8-8F81-59D2A7B758B} /L*v C:\WINDOWS\novell\zenworks\bin\zfde_pol_uninstall_log.txt
```

You can view the `zfde_pol_uninstall_log.txt` file to verify that the uninstall is successful. The status is recorded in the last few lines of the log file.

3 Restart the device.

You can view the ZENworks Adaptive Agent’s property pages (double-click the icon in the notification area) to verify that Full Disk Encryption is no longer listed. In addition, the Full Disk Encryption Agent is no longer available in the Start menu.

4 (Conditional) If the device will connect to a ZENworks Server in the future, disable the device’s Full Disk Encryption setting in ZENworks Control Center. If the setting is enabled, the next time the device connects, the Full Disk Encryption Agent is reinstalled.

4a In ZENworks Control Center, click Devices, click the device to display its details, click the Settings tab, click Device Management, then click ZENworks Agent.

4b Click Override to enable the settings to be modified.

4c Under Agent Features, deselect the Installed check box for Full Disk Encryption.

4d Click OK to save the change.

### 3.3 Uninstalling the ZENworks Adaptive Agent

You can uninstall the ZENworks Adaptive Agent to remove the Full Disk Encryption Agent. This, of course, removes all other ZENworks functionality from the device.

1 (Optional) Remove the policy assignments in ZENworks Control Center and then refresh the device. See “Removing Policy Assignments From Devices” in the ZENworks 11 SP2 Full Disk Encryption Policy Reference.

Removing the policy assignments is not required but is a recommended best practice.

2 Make sure you know the uninstall password for the ZENworks Adaptive Agent (if one is defined).

If an uninstall password is defined, it is required when locally uninstalling the ZENworks Adaptive Agent or any modules such as the Full Disk Encryption Agent. The password is defined in ZENworks Control Center under Configuration > Management Zone Settings > Device Management > ZENworks Agent.

3 Uninstall the ZENworks Adaptive Agent:

3a Start the uninstall through the Windows Control Panel (for example, Add or Remove Programs in Windows XP or Uninstall a program in Windows Vista/7).

3b At the Welcome screen, click Next.

3c To uninstall the agent and unregister the device from the ZENworks Management Zone, provide the user name and password of a ZENworks administrator, click Next, select Uninstall the ZENworks Agent and unregister the device from the zone, then click Next.

or

To uninstall the agent only, select Local uninstallation only (Retain the device in the zone), then click Next.
3d (Conditional) If you are prompted for the uninstall password, provide the password.

3e (Conditional) If a Disk Encryption policy is still applied to a device, you are prompted that the disk must be decrypted before the uninstall can be performed. Click OK to start decryption of the disk and removal of the ZENworks PBA. When the process is finished, start the uninstall again (Step 3a).

4 Restart the device.
Decommissioning a Device

You can prevent access to encrypted data by either temporarily or permanently decommissioning a device. Temporarily decommissioning a device removes all Pre-Boot Authentication (PBA) user accounts from the device; the device can be recovered through a PBA override or through the use of an emergency recovery disk. Permanently decommissioning a device erases all data on the encrypted devices; the erased data is unrecoverable.

- Section 4.1, “Temporarily Decommissioning a Device,” on page 19
- Section 4.2, “Permanently Decommissioning a Device,” on page 20

4.1 Temporarily Decommissioning a Device

You can prevent access to encrypted data by temporarily decommissioning the device. When a device is temporarily decommissioned, all of the Pre-Boot Authentication (PBA) user accounts are removed. The only way to access the device after the users are removed is to perform a PBA override or an emergency recovery. Before decommissioning the device, you should ensure that an Emergency Recovery Information (ERI) file exists for the device (see Creating an Emergency Recovery Information File).

1 Make sure you know the FDE Admin password for the policy that is assigned to the device.
   To temporarily decommission a device by removing all PBA users, you must know the FDE Admin password for the policy assigned to the device, or you must know the ZENworks Adaptive Agent override password or key. For more information about passwords, see Appendix B, “Administrator Passwords,” on page 63.

2 On the device, double-click the icon in the notification area, then click Full Disk Encryption.

3 In the Full Disk Encryption Agent Actions section, click About to display the About dialog box.
4 Click the Commands button.
5 Supply the password, then click OK to display the Commands dialog box.

6 Click the Temporary Decommission button.
7 In the confirmation dialog box that is displayed, click Yes to proceed.
   The device immediately shuts down.

4.2 Permanently Decommissioning a Device

You can prevent access to encrypted data by permanently decommissioning the device. You do this by erasing all of the encrypted data. The erased data is unrecoverable.

1 Make sure you know the FDE Admin password for the policy that is assigned to the device.
   To permanently decommission a device, you must know the FDE Admin password for the policy assigned to the device, or you must know the ZENworks Adaptive Agent override password or key. For more information about passwords, see Appendix B, “Administrator Passwords,” on page 63.
On the device, double-click the icon in the notification area, then click Full Disk Encryption.

In the Full Disk Encryption Agent Actions section, click About to display the About dialog box.

Click the Commands button.

Supply the password, then click OK to display the Commands dialog box.

Click the Permanent Decommission button.

In the confirmation dialog box that is displayed, click Yes to proceed. The device immediately shuts down.
The following sections provide instructions to help you move a managed device that has the Full Disk Encryption Agent installed from one zone to another zone:

- Section 5.1, “Moving a Device to a Zone Where Full Disk Encryption Is Not Active,” on page 23
- Section 5.2, “Moving a Device to a Zone Where Full Disk Encryption Is Active,” on page 24

## 5.1 Moving a Device to a Zone Where Full Disk Encryption Is Not Active

When you unregister a device from its zone, the Full Disk Encryption Agent continues to enforce the Disk Encryption policy. Encrypted volumes remain encrypted and the ZENworks PBA (if it is enabled in the policy) continues to provide pre-boot authentication.

If you register the device in a zone where Full Disk Encryption is not active (or the Full Disk Encryption Agent is disabled or not installed), the Disk Encryption policy and the Full Disk Encryption Agent are removed from the device. Encrypted volumes are decrypted and the ZENworks PBA is removed.

To move a device:

1. Unregister the device. See “Unregistering a Device” in the ZENworks 11 Discovery, Deployment, and Retirement Reference.

   After the device is unregistered, the Full Disk Encryption agent continues to enforce the Disk Encryption policy. Encrypted volumes remain encrypted and the ZENworks PBA (if it is enabled in the policy) continues to provide pre-boot authentication.

2. Register the device in the new zone. See “Manually Registering a Device” in the ZENworks 11 Discovery, Deployment, and Retirement Reference.

   After the device registers in the zone, the Disk Encryption policy is removed and the Full Disk Encryption Agent decrypts any encrypted volume. The ZENworks Adaptive Agent then uninstalls or disables the Full Disk Encryption Agent.
5.2 Moving a Device to a Zone Where Full Disk Encryption Is Active

When you unregister a device from its zone, the Full Disk Encryption Agent continues to enforce the Disk Encryption policy. Encrypted volumes remain encrypted and the ZENworks PBA (if it is enabled in the policy) continues to provide pre-boot authentication.

If you then register the device in another zone (or reregister it in the same zone) and assign a Disk Encryption policy to the device, the Full Disk Encryption Agent enforces the new policy. If the new policy uses the same encryption settings (algorithm, key length, and so forth) as the device’s current policy, no encryption changes take place. If the new policy has different encryption settings, any encrypted volumes are decrypted and then re-encrypted using the new encryption settings.

To move a device:

1 Unregister the device. See “Unregistering a Device” in the ZENworks 11 Discovery, Deployment, and Retirement Reference.

   After the device is unregistered, the Full Disk Encryption Agent continues to enforce the Disk Encryption policy. Encrypted volumes remain encrypted and the ZENworks PBA (if it is enabled in the policy) continues to provide pre-boot authentication.

2 Register the device in the new zone. See “Manually Registering a Device” in the ZENworks 11 Discovery, Deployment, and Retirement Reference.

   After the device registers in the zone, the Full Disk Encryption Agent continues to enforce the Disk Encryption policy. However, because the policy is not assigned to the device through the zone, you cannot modify the policy in ZENworks Control Center.

3 (Optional) Assign a new Disk Encryption policy to the device.

   If you want to manage the Disk Encryption policy for the device, you need to assign a new policy that exists in the zone. To ensure that the device’s volumes are not decrypted and then encrypted again, make sure the new policy uses the same encryption settings (algorithm, key length, and so forth) as the device’s current policy.
Disk Encryption

- Chapter 6, “Viewing the Disk Encryption Settings,” on page 27
- Chapter 7, “Decrypting Drives,” on page 29
The Full Disk Encryption Agent lets you view the disk encryption settings for the policy being applied to the device.

1. Make sure you know the FDE Admin password for the policy that is assigned to the device.

   To view the disk encryption settings, you must know the FDE Admin password for the policy assigned to the device, or you must know the ZENworks Adaptive Agent override password or key. For more information about passwords, see Appendix B, “Administrator Passwords,” on page 63.

2. On the device, double-click the icon in the notification area, then click Full Disk Encryption.

3. In the Full Disk Encryption Agent Actions section, click About to display the About dialog box.
4 Click View Policy, type the FDE Admin password for the policy, then click OK. The View Policy dialog box includes a tab for the policy’s Full Disk Encryption settings and Pre-Boot Authentication settings.

5 After you finish viewing the policy settings, click Close to exit the dialog box.
7 Decrpyting Drives

You can use the Full Disk Encryption Agent to decrypt any of the device’s encrypted drives. The drive remains decrypted unless a new Disk Encryption policy is applied that causes the drive to be encrypted again.

1. Make sure you know the FDE Admin password for the policy that is assigned to the device.

To decrypt a drive, you must know the FDE Admin password for the policy assigned to the device, or you must know the ZENworks Adaptive Agent override password or key. For more information about passwords, see Appendix B, “Administrator Passwords,” on page 63.

2. On the device, double-click the icon in the notification area, then click Full Disk Encryption.

3. In the Full Disk Encryption Agent Actions section, click About to display the About dialog box.

4. Click the Commands button.

5. Supply the password, then click OK to display the Commands dialog box.
6 Click the *Decrypt Drive* button.
7 Select the drive to decrypt, then click *OK*.
8 In the confirmation dialog box that is displayed, click *Yes* to proceed.
III Pre-Boot Authentication

- Chapter 8, “Viewing the Pre-Boot Authentication Settings,” on page 33
- Chapter 9, “Enabling User Capturing,” on page 35
- Chapter 10, “Managing PBA User Accounts,” on page 37
- Chapter 11, “Synchronizing the PBA and Windows Credentials,” on page 39
Viewing the Pre-Boot Authentication Settings

The Full Disk Encryption Agent lets you view the pre-boot authentication settings for the policy being applied to the device.

1. Make sure you know the FDE Admin password for the policy that is assigned to the device. To view the pre-boot authentication settings, you must know the FDE Admin password for the policy assigned to the device, or you must know the ZENworks Adaptive Agent override password or key. For more information about passwords, see Appendix B, “Administrator Passwords,” on page 63.

2. On the device, double-click the icon in the notification area, then click Full Disk Encryption.

3. In the Full Disk Encryption Agent Actions section, click About to display the About dialog box.
4 Click *View Policy*, type the FDE Admin password for the policy, then click *OK*.
The View Policy dialog box includes a tab for the policy’s pre-boot authentication settings.

![View Policy dialog box](image)

5 After you finish viewing the policy settings, click *Close* to exit the dialog box.
Enabling User Capturing

You can use the Full Disk Encryption Agent to enable user capturing for pre-boot authentication. Enabling user capturing causes ZENworks Pre-Boot Authentication to capture the credentials (user ID/password or smart card) of the first user to log in after the device is rebooted.

You can also use ZENworks Control Center to enable user capturing on a device. For information, see “Enabling User Capturing” in the ZENworks 11 SP2 Full Disk Encryption PBA Reference.

1. Make sure you know the FDE Admin password for the policy that is assigned to the device.
   To enable user capturing, you must know the FDE Admin password for the policy assigned to the device, or you must know the ZENworks Adaptive Agent override password or key. For more information about passwords, see Appendix B, “Administrator Passwords,” on page 63.

2. On the device, double-click the icon in the notification area, then click Full Disk Encryption.

3. In the Full Disk Encryption Agent Actions section, click About to display the About dialog box.

4. Click the Commands button.

5. Supply the password to display the Commands dialog box.
6 Click the Enable User Capture button.

You can verify the setting by viewing the agent status and looking at the PBA Self Initialization Mode value (see Viewing the Agent Status). If user capturing is enabled, the value will be WINDOWS_CRED_SELFINIT.
Managing PBA User Accounts

You can use the Full Disk Encryption Agent to add or delete user accounts for ZENworks Pre-Boot Authentication (PBA). PBA user accounts you add exist only on the device; they are not added to the Disk Encryption policy. In addition, if the Remove existing users from PBA if not in this list option is enabled in the Disk Encryption policy, the added user is removed after the next login.

You can also use ZENworks Control Center to add PBA users on a device. For information, see “Manually Adding Users” in the ZENworks 11 SP2 Full Disk Encryption PBA Reference.

1 Make sure you know the FDE Admin password for the policy that is assigned to the device.
   To add or remove a PBA user account, you must know the FDE Admin password for the policy assigned to the device, or you must know the ZENworks Adaptive Agent override password or key. For more information about passwords, see Appendix B, “Administrator Passwords,” on page 63.

2 On the device, double-click the icon in the notification area, then click Full Disk Encryption.

3 In the Full Disk Encryption Agent Actions section, click About to display the About dialog box.

4 Click the Commands button.

5 Supply the password, then click OK to display the Commands dialog box.
6 Click the Add/Delete PBA User button.

7 Provide the username, password, and domain of the user you want to add or delete. If the user is not part of a Windows domain, specify the computer name instead.

8 (Conditional) If you want to delete the user, select the Check to Delete User box.

9 Click OK to add or delete the user.

You can verify the change by viewing the agent status and looking at the PBA User List (see “Viewing the Agent Status” on page 45).
Synchronizing the PBA and Windows Credentials

This information applies only if ZENworks Pre-Boot Authentication (PBA) is installed on the device.

If a device’s Disk Encryption policy has single sign-on enabled so that the ZENworks PBA login credentials are the same as the Windows login credentials, the passwords remain synchronized if the Windows password is changed through one of the following methods:

- Via Windows domain login
- Via Windows local login
- Using Ctrl+Alt+Del to access the change password feature

The passwords are not synchronized if one of the following methods is used:

- Control Panel
- Device Manager

If the passwords become out-of-sync, the following methods can be used to synchronize them while at the device:

- Section 11.1, “Using the Windows Login,” on page 39
- Section 11.2, “Using the Full Disk Encryption Agent,” on page 39

In addition, you can use a ZENworks Control Center Quick Task to synchronize the passwords. For information, see “Synchronizing PBA and Windows Credentials” in the ZENworks 11 SP2 Full Disk Encryption PBA Reference.

11.1 Using the Windows Login

This is the recommended way to synchronize a user’s PBA and Windows passwords because the user can complete these steps without administrator assistance:

1. Restart the device.
2. Log in to the ZENworks PBA using the old Windows/PBA password.
3. When the Windows login screen is displayed, enter the password required to log in to Windows.
   The ZENworks PBA detects the difference in the current PBA and Windows passwords and changes the PBA password to the Windows password.
4. Restart the device and log in to the ZENworks PBA using the new Window/PBA password.

11.2 Using the Full Disk Encryption Agent

1. Make sure you know the FDE Admin password for the policy that is assigned to the device.
To change the user’s PBA password, you must know the FDE Admin password for the policy assigned to the device, or you must know the ZENworks Adaptive Agent override password or key. For more information about passwords, see Appendix B, “Administrator Passwords,” on page 63.

2 On the device, double-click the icon in the notification area, then click Full Disk Encryption.

3 In the Full Disk Encryption Agent Actions section, click About to display the About dialog box.

![ZENworks Full Disk Encryption About Box]

4 Click the Commands button.

5 Supply the password, then click OK to display the Commands dialog box.

![ZENworks Full Disk Encryption Commands]

6 Click the Add/Delete PBA User button.

7 Provide the following:

   **User Name:** Specify the user name for the user whose password you want to change.

   **User Password:** Specify the user’s Windows password. This becomes the PBA password.

   **User Domain:** Specify the user’s Windows domain name. If the user is not a member of a domain, you can specify the computer name or leave the field blank.
If you don't know the domain or computer name, you can cancel to exit the dialog box, close the ZFDE Commands dialog box, click the Agent Status button, click the PBA tab, then scroll down to the User List at the bottom of the page. The user name and domain/computer name are listed in the PBA User Name column, with the domain/computer name listed second (after the colon).

8 Click OK to change the PBA password.
Troubleshooting

- Chapter 12, “Viewing the Agent Status,” on page 45
- Chapter 13, “Creating an Emergency Recovery Information File,” on page 47
- Chapter 14, “Logging Agent Events,” on page 49
- Chapter 15, “Creating a Diagnostics Package,” on page 55
- Chapter 16, “Viewing the List of Agent Modules,” on page 57
Viewing the Agent Status

The Full Disk Encryption Agent provides a variety of status information related to the enforcement of the Full Disk Encryption policy on the device. For example, the agent displays the current enforcement settings for both encryption and pre-boot authentication. It also lists the Emergency Recovery Information (ERI) files created for the device and shows the enforcement history for previous Full Disk Encryption policies or versions applied to the device.

To view the Full Disk Encryption Agent status information:

1. Make sure you know the FDE Admin password for the policy that is assigned to the device.
   To view the agent status, you must know the FDE Admin password for the policy assigned to the device, or you must know the ZENworks Adaptive Agent override password or key. For more information about passwords, see Appendix B, “Administrator Passwords,” on page 63.

2. On the device, double-click the icon in the notification area, then click Full Disk Encryption.

3. In the Full Disk Encryption Agent Actions section, click About to display the About dialog box.
4 Click *Agent Status*, type the FDE Admin password for the policy, then click *OK*. The Agent Status dialog box includes tabs for Full Disk Encryption status, Pre-Boot Authentication (PBA) status, and general agent settings status.

![Zenworks FDE Agent Status](image)

5 After you finish viewing the status pages, click *Close* to exit the dialog box.
Creating an Emergency Recovery Information File

If a situation occurs where a user cannot access the encrypted volumes on a device, you might need to perform an emergency recovery of the device. This requires an Emergency Recovery Information (ERI) file for the device.

An ERI file is a password-protected file that contains the encryption keys for the encrypted volumes of the device’s hard disk. The file is the only way to get in to the device in an emergency.

By default, whenever the ZENworks Full Disk Encryption Agent changes the encryption settings (volumes, algorithm, and so forth) for the hard disk, an ERI file is created and sent to the ZENworks server to be stored on your network.

If a user infrequently connects to the network, or if you simply want to ensure that the user has a personal backup copy of the ERI file, you or the user can manually create an ERI file and store it in a secure location other than the device’s local hard disk. For example, a removable storage device such as a USB drive could be used.

To create an ERI file:

1 Double-click the icon in the notification area, then click Full Disk Encryption.
2 In the Full Disk Encryption Agent Actions section, click About to display the About dialog box.

3 Click the Create ERI File button if it is available.
If the Create ERI File button is not available, click Commands, specify the password to display the Commands dialog box, then click the Create ERI button.

The Create ERI File button is only available in the About dialog box if the feature has been enabled in the Disk Encryption policy applied to the device. However, the Create ERI button is always available in the Commands dialog box. To access the Commands dialog box, you must know the FDE Admin password for the policy assigned to the device, or you must know the ZENworks Adaptive Agent override password or key. For more information about passwords, see Appendix B, “Administrator Passwords,” on page 63.

4 When you are prompted to assign a password to the ERI file that will be generated, specify a password, then click OK.

If a strong password is required, it must include at least one uppercase letter, one lowercase letter, one number, and one special character. Special characters are:

```
~ ! @ # $ % ^ & * ( ) _ + { } [ ] : ; < > ? , . / \ - = | 
```

Make sure the password is one that you can remember. The password is required to use the ERI file for an emergency recovery.

The Full Disk Encryption Agent creates a computer-name_yyyy_mmdd_hhmm.eri file on your desktop (for example, computer1_2011_1208_1435). If you are connected to the ZENworks server on your network, it is also sent to the server.

5 Copy the ERI file to a secure location that is still accessible when the device is not.
14 Logging Agent Events

The Full Disk Encryption Agent logs information to the device’s local disk. The log files can be used in conjunction with Novell Support to troubleshoot issues with Full Disk Encryption.

- Section 14.1, “Log Files,” on page 49
- Section 14.2, “Accessing the Logging Settings,” on page 50
- Section 14.3, “Changing the Logging Level,” on page 51
- Section 14.4, “Viewing Log Files,” on page 51
- Section 14.5, “Inserting a Comment in the Log Files,” on page 52
- Section 14.6, “Deleting All Log Files,” on page 53

14.1 Log Files

The ZENworks Full Disk Encryption Agent consists of multiple processes and drivers, each of which performs specific functions related policy handling and disk encryption. Four of these processes log activities to their own files:

- Log_YYYYMMDD_HHMMSS_NNNN.txt: This log contains any Full Disk Encryption messages generated by the ZESService.exe process. This agent process performs the majority of activities for Full Disk Encryption.
- Cmd_YYYYMMDD_HHMMSS_NNNN.txt: This log contains any Full Disk Encryption messages generated by the ZESCommand.exe process. This agent process executes agent commands (such as creating diagnostic packages) from a command line.
- User_YYYYMMDD_HHMMSS_NNNN.txt: This log contains any Full Disk Encryption messages generated by the ZESUser.exe process. This agent process executes agent commands (such as creating diagnostic packages) through the user interface.
- ZID_YYYYMMDD_HHMMSS_NNNN.txt: This log contains any Full Disk Encryption messages generated by the ZESZid.dll process. This agent process communicates policy data between the Adaptive Agent and the ZESService.exe process.

The log files are stored in the following hidden directories:

- Windows XP: \Documents and Settings\All Users\Application Data\Novell\ZES\Logs
- Windows Vista/7: \ProgramData\Novell\ZES\Logs

Each process creates a new log file when the process starts or when the log file reaches approximately 1 MB. A maximum of 10 log files are kept for ZESService.exe, ZESCommand.exe, and ZESZid.dll, and a maximum of 50 log files are kept for ZESUser.exe.

The Full Disk Encryption Agent drivers also generate two log files: FDE.log and PBA.log. These logs are stored in the same directory as the process logs. These are low-level logs that provide information for Novell Support if needed.
14.2 Accessing the Logging Settings

The ZESService.exe, ZESCommand.exe, ZESUser.exe, and ZESZid.dll processes are shared processes used by the ZENworks Full Disk Encryption Agent, the ZENworks Endpoint Security Agent, and the ZENworks Location Decider. Because of this, the logging settings are accessed through the ZENworks Endpoint Security Agent if it is enabled, or through the ZENworks Location Decider if the Endpoint Security Agent is not enabled.

1. On the device, double-click the icon in the notification area, then click Agent (under the Status heading).

2. In the Agent Security Settings section, click Policy Override.

   If ZENworks Endpoint Security Management is enabled, the ZENworks Endpoint Security Agent dialog box is displayed. If it is not enabled, the ZENworks Location Decider dialog box is displayed.

3. Click the Diagnostics button

4. Click Logging.
14.3 Changing the Logging Level

By default, the logging level is set to Warning. If necessary, you can change it to Debug, Informational, or Error to gather more or less information. For troubleshooting, you should set logging according to the directions of Novell Support and re-create the circumstances that led to the error to see if it can be repeated.

To change the logging level:

1. Access the Logging dialog box. If you need instructions, see Section 14.2, “Accessing the Logging Settings,” on page 50.

2. Change the Full Disk Encryption logging level as desired:
   - **Debug**: Turns on every possible message and includes Informational, Warning, and Error messages.
   - **Informational**: Records all events when they occur, such as when a network connection event begins and ends.
   - **Warning**: Records errors that have occurred but are solvable and do not prevent the client from running.
   - **Error**: Records errors that have occurred and prevent the client from running.

3. If you want to save the settings as the default settings, select Save as Defaults. Otherwise, the settings are used only for the current session for each process (ZESCommand.exe, ZESService.exe, and ZESUser.exe).

4. If you change settings, you can click Restore Defaults to reset them to the stored defaults.

5. Click OK to exit the dialog box.

14.4 Viewing Log Files

1. Access the Logging dialog box. If you need instructions, see Section 14.2, “Accessing the Logging Settings,” on page 50.
2 Click one of the following buttons to display the log file you want:

- **View Service Log**: This log contains any Full Disk Encryption messages generated by the ZESService.exe process. This agent process performs the majority of activities for Full Disk Encryption.

- **View User Log**: This log contains any Full Disk Encryption messages generated by the ZESUser.exe process. This agent process executes agent commands (such as creating diagnostic packages) through the user interface.

- **View Interface Log**: This log contains any Full Disk Encryption messages generated by the ZESZid.exe process. This agent process communicates policy data between the Adaptive Agent and the ZESService.exe process.

3 When you are finished viewing log files, click OK to exit the dialog box.

### 14.5 Inserting a Comment in the Log Files

You can add your own comment to the Service (Log_*.txt) and User (User_*.txt) logs. The comment is inserted at the current line in both of the log files.

1 Access the Logging dialog box. If you need instructions, see Section 14.2, “Accessing the Logging Settings,” on page 50.

2 Click Add Comment to display the Comment dialog box.

3 Type your comment, then click OK to add it to the log files.

4 View the log files, or click OK to exit the Logging dialog box.
14.6 Deleting All Log Files

You can delete all log files from a managed device. The current log files and any saved log files are deleted.

1 Access the Logging dialog box. If you need instructions, see Section 14.2, “Accessing the Logging Settings,” on page 50.

![Logging dialog box](image)

2 Click Clear Log Files.

3 Click OK to exit the dialog box.
15 Creating a Diagnostics Package

If Novell Support is helping you resolve an Full Disk Encryption Agent issue on one of your devices, you might be asked to generate a diagnostic package for Support to review. This package contains information about the device’s Group Policy object, registry settings, system, and system events.

To create a diagnostics package:

1. On the device, double-click the icon in the notification area, then click Full Disk Encryption.
2. In the Full Disk Encryption Agent Actions section, click About to display the About dialog box.

3. Click Diagnostics, then follow the prompts to create the package.

The Full Disk Encryption Agent creates an fdediagnostics*.enc file on your desktop. This can take a while. During the creation time, the Diagnostics button is disabled.

After the file is created, send it to Novell Support.
Viewing the List of Agent Modules

You can view a list of the Full Disk Encryption Agent modules that are currently loaded on a device. The list displays each module with its date and version.

1. On the device, double-click the icon in the notification area, then click Full Disk Encryption.
2. In the Full Disk Encryption Agent Actions section, click About to display the About dialog box.

3. Click Module List.
4. After you finish viewing the module list, click Close to exit the dialog box.
Appendixes

- Appendix A, “Supported Smart Card Terminals and Tokens,” on page 61
- Appendix B, “Administrator Passwords,” on page 63
- Appendix C, “Documentation Updates,” on page 65
A Supported Smart Card Terminals and Tokens

The following sections list the smart card terminals and tokens supported by ZENworks Full Disk Encryption based on the middleware that is integrated with the ZENworks Pre-Boot Authentication component:

- Section A.1, “Supported Smart Card Terminals and Tokens,” on page 61
- Section A.2, “Integrated PKCS#11 Middleware,” on page 62

A.1 Supported Smart Card Terminals and Tokens

The following smart card terminals and tokens are supported by the PKCS#11 middleware integrated with the Pre-Boot Authentication component:

- Aladdin eToken Pro 32k (issued with RTE 3.6)
- Aladdin eToken Pro 64k, NG-Flash, NG-OTP (issued with RTE 3.6)
- ACS ACR83 (without PIN-pad and display support)
- Common Access Cards (CAC)
- Dell smart card reader keyboard
- Eutron CryptoIdentity
- Eutron CryptoCombo
- Gemalto .Net
- GemPC Twin
- IDpendant Token 100
- IDpendant Token 200
- IDpendant Token 1000
- Kobil B1 Professional
- Kobil Kaan Advanced
- Kobil Kaan Base
- Kobil Kaan CT B1 S
- Kobil Kaan Professional Kobil mIDentity (Product Ids: 4000, 4081)
- O2micro CCID USB
- Omnikey Cardman Desktop USB 3021
- Omnikey Cardman 3121
- Omnikey Cardman Desktop USB 3621
- Omnikey Cardman Desktop USB 3821
- Omnikey Cardman 4000
- Omnikey Cardman 4040
- Omnikey Cardman 4321
- Omnikey Cardman 6121
- ReinerSCT cyberjack pinpad
- RICOH Smartcard Reader V1.0.2
- RSA SID 800 (issued with RAC 2.x)
- SCM SCR 335
- SCM SCR 531
- SCM SCR 532
- SCM SCR 3310
- SCM SCR 3311 USB
- SCM SCR 3320 USB
- SCM SCR 3340
- Vasco Smartcard Reader

A.2 Integrated PKCS#11 Middleware

The following PKCS#11 middleware is integrated into the Linux-based Pre-Boot Authentication component:

- A.E.T SafeSign v.3.0.43
- A-Trust 1.0.0.68
- Aladdin 5.00
- Charismathics v.4.7 r13
- CryptoVision v.5.0
- D-Trust 1.0.0.68
- Gemalto .NET v.2.00
- Kobil 2.11
- Nexus 4.10.2.16
- Oberthur opensc 2.0.0
- RSA SecurID 800 PKCS#11
- SECUDE 1.3.0
- SECUDE TCOS 1.7.0
- Siemens CardOS HiPath 5.0.12
- Schlumberger Axalto 5.2
- Telesec 3.0.5

...with the following CCID and PCSC-lite versions:

- CCID 1.3.8
- PCSC-lite 1.4.4
The Full Disk Encryption Agent provides several features that are intended for use only by a ZENworks administrator or by a user under the direction of a ZENworks administrator. These features are grouped together in the Full Disk Encryption Agent’s About dialog box.

In order to use the Administrator features, you must provide the FDE Admin password for the Full Disk Encryption policy assigned to the device, or you must have enabled a ZENworks Adaptive Agent override password. If you use an override password on a device, we recommend the following practice:

- If you are the one using the override password on a device, you can use the password as defined in the ZENworks Agent Security settings in ZENworks Control Center.
- If you are allowing a user to access the Administrator options, you should generate an override password key for the user. The key functions like the override password but allows you to specify who can use the key, what device it can be used on, and when the key expires. Using a key enables you to maintain the security of your override password and impose override restrictions on the key. For information about generating an override password key, see “Password Key Generator” in the ZENworks 11 SP2 Endpoint Security Utilities Reference.
This section contains information on documentation content changes that were made in this Full Disk Encryption Agent Reference since its initial publication.

The documentation was updated on the following dates:

- Section C.1, “October 2013: Update to ZENworks 11 SP2 (11.2.4),” on page 65
- Section C.2, “March 2013: Update to ZENworks 11 SP2 (11.2.3),” on page 65

C.1 October 2013: Update to ZENworks 11 SP2 (11.2.4)

<table>
<thead>
<tr>
<th>Location</th>
<th>Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, “System Requirements,” on page 9</td>
<td>Updated the system requirements as follows:</td>
</tr>
<tr>
<td></td>
<td>- Added Windows 8 as a supported platform.</td>
</tr>
<tr>
<td></td>
<td>- Stated that UEFI firmware is not supported on any devices; BIOS firmware is required.</td>
</tr>
<tr>
<td></td>
<td>- Stated that disks must be using an MBR partition table; GPT partition tables are not supported.</td>
</tr>
<tr>
<td>Chapter 2, “Installing the Full Disk Encryption Agent,” on page 13</td>
<td>Updated the installation section to explicitly state that the Full Disk Encryption Agent will not be installed on Windows devices that use UEFI firmware. BIOS firmware is required.</td>
</tr>
</tbody>
</table>

C.2 March 2013: Update to ZENworks 11 SP2 (11.2.3)

<table>
<thead>
<tr>
<th>Location</th>
<th>Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, “System Requirements,” on page 9</td>
<td>Updated the system requirements to explicitly state that Windows 8 is not a supported platform for ZENworks Full Disk Encryption.</td>
</tr>
<tr>
<td>Chapter 2, “Installing the Full Disk Encryption Agent,” on page 13</td>
<td>Updated the installation section to explicitly state that the Full Disk Encryption Agent will not be installed on Windows 8 devices.</td>
</tr>
</tbody>
</table>