

ZENworks® 2017

Full Disk Encryption Pre-Boot Authentication Reference

December 2016

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.novell.com/company/legal/>.

Copyright © 2016 Micro Focus Software, Inc. All Rights Reserved.

Third-Party Materials

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

Contents

About This Guide	5
1 Introduction	7
The ZENworks PBA	7
Security	7
Implementation	7
Authentication Methods	8
The PBA Boot Process	8
2 PBA Management	11
Activating Pre-Boot Authentication	11
Enabling User Capturing	11
Using a ZENworks Control Center Quick Task	11
Using the Full Disk Encryption Agent	12
Manually Adding Users	12
Using a ZENworks Control Center Quick Task	13
Using the Full Disk Encryption Agent	13
Enabling Single Sign-On with Windows	14
Activating Single Sign-On in the Disk Encryption Policy	14
Configuring Windows Login	15
Using the Client for Open Enterprise	16
Synchronizing PBA and Windows Credentials	17
Using the Windows Login	17
Using a ZENworks Control Center Quick Task	18
Using the Full Disk Encryption Agent	18
Customizing the PBA Login Screen	19
Creating a Custom Background Image File	19
Adding the Custom Background Image File to the FSEBRAND.BIN File	20
Distributing the Rebranded FSEBRAND.BIN File to Devices	20
Upgrading to a new ZENworks version	21
3 PBA Override	23
PBA Override Versus Emergency Recovery	23
Using the ZENworks PBA Helpdesk for PBA Override (User)	24
Generating a Response Sequence for PBA Override (Administrator)	26
Assigning the Administrator Rights Needed for PBA Override	26
Generating a Response with the Zone Key	28
Generating a Response with a PBA Override File	29
Overriding the PBA with an ERI File	30

About This Guide

This *ZENworks Full Disk Encryption Pre-Boot Authentication Reference* provides information to help you understand, manage, and override ZENworks Pre-Boot Authentication.

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 Introduction

The sections in this chapter explain how ZENworks Pre-Boot Authentication (PBA) works.

The ZENworks PBA

Pre-boot authentication is the process of authenticating a user to a device before the device boots to the primary operating system. For ZENworks Full Disk Encryption, the ZENworks Pre-Boot Authentication module, referred to as the **ZENworks PBA**, performs this operation on a device.

Security

The ZENworks PBA is hosted by a fully functional Linux system installed on the device. At device startup, the Linux system boots and displays the ZENworks PBA login.

The primary advantage of the ZENworks PBA is increased security over the standard Windows login. The Linux system is hardened, meaning that it has been explicitly configured for security and reliability. The ZENworks PBA is protected against alteration through the use of MD5 checksums, and the ZENworks PBA applies strong encryption for the keys used in the authentication process.

With standard hard disks encrypted by ZENworks Full Disk Encryption, the ZENworks PBA does not prevent intruders from seeing the encrypted partitions. However, because the partitions are encrypted, none of the data is accessible until ZENworks PBA login is successful.

With self-encrypting hard disks, the ZENworks PBA prevents intruders from seeing the disks. The disks remain hidden and locked until ZENworks PBA login is successful.

Implementation

The ZENworks PBA implementation differs for a standard hard disk and a self-encrypting hard disk. Read below for more information.

Standard Hard Disk

A standard hard disk is an IDE, SATA, or PATA disk that is not self-encrypting and therefore can be encrypted by ZENworks Full Disk Encryption.

With a standard hard disk, a 100 MB primary partition is created for the Linux system and the ZENworks PBA. When the device boots, the ZENworks PBA login is displayed. After the user enters valid credentials (see [“Authentication Methods” on page 8](#)), the PBA terminates, the Windows operating system is booted, and the encrypted drives become accessible.

Self-Encrypting Hard Disk

A self-encrypting hard disk does its own encryption through the use of a dedicated encryption chip. It cannot be encrypted by ZENworks Full Disk Encryption, but the ZENworks PBA can be used to provide extra security for the disk.

With a self-encrypting disk, a Linux system and ZENworks PBA are installed to the MBR shadow, which is a protected partition of the hard disk. When the device boots, the ZENworks PBA login is displayed. At this time, the MBR shadow is visible to the system but the Windows partition (with the self-encrypted drive) is not. After the user enters valid credentials (see [“Authentication Methods” on page 8](#)), the ZENworks PBA terminates, the Windows partition is unlocked, the Windows operating system is booted, and the encrypted drive becomes accessible.

Authentication Methods

The ZENworks PBA supports the following authentication methods:

- ♦ Standard user ID/password authentication
- ♦ Smart card authentication based on the X.509, PKCS#11, and PC/SC standards

Both methods support the user capturing and single sign-on functionality discussed in the next two sections.

User Capturing

A user's credentials (either user ID/password or smart card) must be added to the ZENworks PBA. You can add credentials via the Disk Encryption policy applied to the device, or you can enable the credentials to be captured by the ZENworks PBA the first time it starts after installation. This second method, referred to as **user capturing**, is the recommended method, especially when using smart card authentication, because it increases the accuracy of correctly defining the user's credentials.

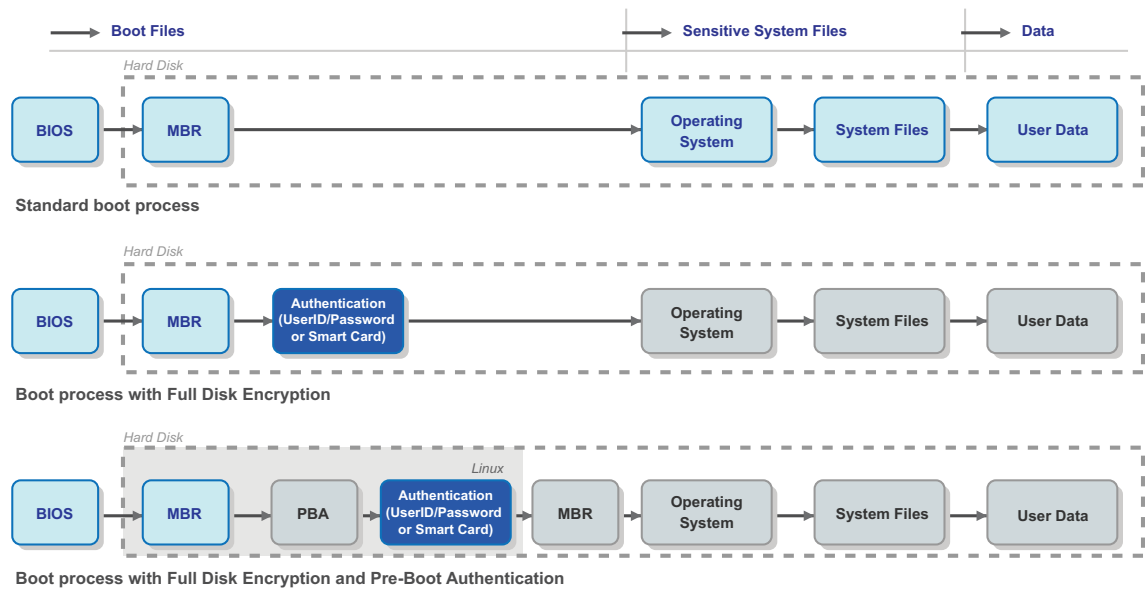
Single Sign-On

The ZENworks PBA login does not replace the Windows login. A user must log in to the ZENworks PBA and in to Windows. You can, however, enable single sign-on so that the user only enters credentials during the ZENworks PBA login and is automatically logged in to Windows with those same credentials. This requires that the ZENworks PBA credentials match the Windows credentials.

The PBA Boot Process

When the ZENworks PBA is installed, it changes the standard boot process. The following illustration shows the standard boot process (no disk encryption or pre-boot authentication), the boot process with disk encryption (no pre-boot authentication), and the boot process with disk encryption and pre-boot authentication.

The gray boxes represent protected components and data and the light blue boxes represent unprotected components and data.



Standard Boot Process

The standard Windows boot process provides no data protection. The Windows login can be easily broken or the drive can be removed and installed as a secondary drive on another device to gain access to the data.

Boot Process With Full Disk Encryption

With full disk encryption applied to a device, the drive data is encrypted, and thus protected, until successful authentication to Windows occurs. The drive data cannot be accessed by removing the drive and installing it as a secondary drive on another device. The primary security weakness is the Windows login.

Boot Process with Full Disk Encryption and Pre-Boot Authentication

With full disk encryption and pre-boot authentication applied to a device, the drive data is encrypted until successful authentication to the ZENworks PBA occurs. This eliminates the Windows login as the key component to gaining access to the encrypted drives.

To protect the ZENworks PBA, the PBA's Linux system includes only the components needed to complete the secure authentication. The system includes no networking components. USB and CD drivers are enabled to provide emergency recovery of the device if necessary. All ZENworks PBA components are protected against manipulation.

If the device is using self-encrypting drives, the ZENworks PBA provides additional protection by locking the drive when the device shuts down. This means that the drive is completely hidden and the data is inaccessible. If the drive is connected as a secondary drive on another device, it remains hidden. The only way to unlock the drive is to provide valid authentication through the ZENworks PBA.

2 PBA Management

The following sections help you manage ZENworks Pre-Boot Authentication.

Activating Pre-Boot Authentication

ZENworks Pre-Boot Authentication is activated on a device by deploying a Disk Encryption policy to the device. The policy also defines the supported authentication methods (user ID/password or smart card) for the device and enables options such as user capturing and single sign-on.

Creation and deployment of Disk Encryption policies is covered in the [ZENworks Full Disk Encryption Policy Reference](#).

Enabling User Capturing

The ZENworks PBA can be enabled to capture the credentials (user ID/password or smart card) of the next user who logs in to the device. This process is referred to as *user capturing*.

If a Disk Encryption policy has user capturing enabled, the ZENworks PBA captures the credentials of the first user to log in after the policy is applied. You can also enable user capturing after the policy is applied through a ZENworks Control Center Quick Task or through the ZENworks Full Disk Encryption Agent. After user capturing is enabled, the ZENworks PBA captures the credentials of the next user to log in and adds them to any other captured credentials.

The following sections cover both methods of enabling user capturing.

Using a ZENworks Control Center Quick Task

To use a ZENworks Full Disk Encryption Quick Task in ZENworks Control Center, a ZENworks administrator must be assigned the **Manage Endpoint Security Settings and Tasks** privilege. This privilege is configured through the Quick Tasks rights for administrators and administrator groups. For help configuring Quick Tasks rights, see the [ZENworks Administrator Accounts and Rights Reference](#).

For user capturing to be enabled on a device through a Quick Task, the device must be running and have a network connection to the ZENworks Server. Otherwise, the ZENworks Server cannot deliver the Quick Task to the device.

To enable user capturing on a device:

- 1 In ZENworks Control Center, click **Devices**.
- 2 In the **Devices** panel, locate the device for which you want to enable user capturing.
- 3 Select the check box next to the device, click **Quick Tasks**, click **FDE: Enable Additive User Capturing**, then click **OK** to confirm the task.
- 4 In the Quick Task Status dialog box, click **Start** if you want to use the default options.
or
Configure the options as desired, then click **Start**.


For information about the options, click the Help icon in the Quick Task Status dialog box.

- 5 As soon as the Quick Task is complete, have the user restart the device.

Until the device restarts and the correct user's credentials are captured, the device's security is compromised. Having the user immediately restart the device minimizes this possible security threat.

Using the Full Disk Encryption Agent

To use the ZENworks Full Disk Encryption Agent to enable user capturing on a device, you must know the FDE Administrator password for the policy assigned to the device, or you must know the ZENworks Agent override password or key.

- 1 On the device, right-click the ZENworks icon  in the notification area, and select **Technician Application**.
- 2 Click **Full Disk Encryption** in the ZENworks Agent navigation menu.
- 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 (in the About dialog box) and looking at the **PBA Self Initialization Mode** value. If user capturing is enabled, the value is `WINDOWS_CRED_SELFINIT`.

- 7 Exit the Full Disk Encryption Agent and restart the device.

Until the device restarts and the correct user's credentials are captured, the device's security is compromised. Immediately restarting the device minimizes this possible security threat.

Manually Adding Users

In addition to having the ZENworks PBA automatically capture users (see [Chapter , "Enabling User Capturing," on page 11](#)), you can manually add users to the ZENworks PBA for a device. You cannot manually add smart cards.

As with captured users, users that you manually add exist only on the device; they are not added to the Disk Encryption policy's user list. Therefore, 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 add users through a ZENworks Control Center Quick Task or through the ZENworks Full Disk Encryption Agent. The following sections cover both methods.

Using a ZENworks Control Center Quick Task

To use a ZENworks Full Disk Encryption Quick Task in ZENworks Control Center, a ZENworks administrator must be assigned the **Manage Endpoint Security Settings and Tasks** privilege. This privilege is configured through the Quick Tasks rights for administrators and administrator groups. For help configuring Quick Tasks rights, see the [ZENworks Administrator Accounts and Rights Reference](#).

For a user to be added to a device through a Quick Task, the device must be running and have a network connection to the ZENworks Server. Otherwise, the ZENworks Server cannot deliver the Quick Task to the device.

- 1 In ZENworks Control Center, click **Devices**.
- 2 In the **Devices** panel, locate the device for which you want to add a user.
- 3 Select the check box next to the device, click **Quick Tasks > FDE: Update PBA User** to display the Update PBA User dialog box.
- 4 Fill in the following fields:

Replace password if user already exists in PBA: Ignore this option. It only applies if you are updating an existing user's password.

User Name: Specify a user name for the PBA user. If single sign-on is active on the device, this user name must be the same as the Windows user name. If single sign-on is not active, the user name does not need to match the Windows user name.

Domain: Specify a domain name for the PBA user. If single sign-on is active, this must be the Windows domain name (or computer name if the user is not a domain member). If single sign-on is not active, this field is optional. You can leave it blank or use it as another component to distinguish the PBA user name.

Password: Specify a password for the PBA user. If single sign-on is active, this must be the Windows password. If single sign-on is not active, you can specify any password.

- 5 Click **OK** to display the Quick Task Status dialog box.
- 6 In the Quick Task Status dialog box, click **Start** if you want to use the default options.

or

Configure the options as desired, then click **Start**.


For information about the options, click the Help icon in the Quick Task Status dialog box.

As soon as the Quick Task is complete, the new user can authenticate to the ZENworks PBA on the device.

Using the Full Disk Encryption Agent

You can use the Full Disk Encryption Agent to add users to or remove users from the ZENworks PBA.

To add or remove a PBA user, you must know the FDE Administrator password for the policy assigned to the device, or you must know the ZENworks Agent override password or key.

- 1 On the device, right-click the ZENworks icon  in the notification area, and select **Technician Application**.
- 2 Click **Full Disk Encryption** in the ZENworks Agent navigation menu.
- 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.

User Name: Specify a user name for the PBA user. If single sign-on is active on the device, this user name must be the same as the Windows user name. If single sign-on is not active, the user name does not need to match the Windows user name.

User Password: Specify a password for the PBA user. If single sign-on is active, this must be the Windows password. If single sign-on is not active, you can specify any password.

User Domain: Specify a domain name for the PBA user. If single sign-on is active, this must be the Windows domain name (or computer name if the user is not a domain member). If single sign-on is not active, this field is optional. You can leave it blank or use it as another component to distinguish the PBA user name.

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**.

Enabling Single Sign-On with Windows

Users authenticate to both the ZENworks PBA and the Windows operating system. You can enable single sign-on so that the user logs in to the ZENworks PBA and the PBA handles the login to the Windows operating system. This, of course, requires that the user's PBA and Windows credentials are the same. Single sign-on applies to both authentication methods (user ID/password or smart card).

If you are using ZENworks login to enable policies and bundles to be applied to users as well as devices, and you have configured ZENworks login for single sign-on with your Windows login, single sign-on works for all three logins. When a user logs in to the ZENworks PBA, the credentials are passed to the Windows login and then the ZENworks login.

Refer to the following sections for information on enabling single sign-on.

Activating Single Sign-On in the Disk Encryption Policy

Single sign-on is activated through the Disk Encryption policy assigned to a device:

- ♦ To create a new policy with single sign-on activated and assign it to a device, see [Policy Deployment](#) in the [ZENworks Full Disk Encryption Policy Reference](#).
- ♦ To modify an existing policy to activate single sign-on and republish it to a device, see [Policy Management](#) in the [ZENworks Full Disk Encryption Policy Reference](#).

Configuring Windows Login

Single sign-on supports both the classic Logon screen mode (left screen shot) and the Welcome screen mode (right screen shot). As long as a device is using one of these two modes, single sign-on works as soon it is activated in the policy and the policy is applied to the device. Windows 7 is used in the example screen shots below, but Windows Vista and Windows XP also provide the classic Logon screen and Welcome screen modes.



Single sign-on also supports Secure Logon (shown below) in both of these modes. However, as with the standard Windows login process, the user must press Ctrl+Alt+Delete to dismiss the Secure Logon screen before the single sign-on process can continue.



If single sign-on is failing on a device, we recommend that you set the device to use the classic Logon screen without Secure Logon. In addition, we recommend that you set the **Do Not Display Last User Name** option to Enabled so that the Logon screen is not automatically populated with the user name of the last person to successfully log in.

To configure these settings locally on a Windows XP device:

- 1 Log on to the device as an administrator.
- 2 Set classic Logon screen mode:
 - 2a Click the **Start** menu, click **Run**, type `gpedit.msc`, then click **OK** to open the Local Group Policy Editor.
 - 2b In the editor, expand **Local Computer Policy > Computer Configuration > Administrative Templates > System > Logon**.

- 2c Double-click **Always Use Classic Logon**.
- 2d Select **Enabled**, then click **OK**.
- 3 Disable Secure Logon:
 - 3a Click the **Start** menu, click **Run**, type `control userpasswords2`, then click **OK** to open the User Accounts dialog box.
 - 3b Click the **Advanced** tab.
 - 3c In the Secure logon section, deselect **Require users to press Ctrl+Alt+Delete**.
 - 3d Click **OK**.
- 4 Enable the Do Not Display Last User Name setting:
 - 4a Click the **Start** menu, click **Run**, type `secpol.msc`, then click **OK** to open the Local Security Settings.
 - 4b Expand **Local Policies > Security Options**.
 - 4c Double-click **Interactive logon: Do not display last user name**.
 - 4d Select **Enabled**, then click **OK**.

To configure these settings locally on a Windows Vista or Windows 7 device:

- 1 Log on to the device as an administrator.
- 2 Set classic Logon screen mode:
 - 2a Click the **Start** menu, type `gpedit.msc` in the search box, then click **OK** to open the Local Group Policy Editor.
 - 2b In the editor, expand **Local Computer Policy > Computer Configuration > Administrative Templates > System > Logon**.
 - 2c Double-click **Always Use Classic Logon**.
 - 2d Select **Enabled**, then click **OK**.
- 3 Disable Secure Logon:
 - 3a Click the **Start** menu, type `netplwiz` in the search box, then click **OK** to open the User Accounts dialog box.
 - 3b Click the **Advanced** tab.
 - 3c In the Secure logon section, deselect **Require users to press Ctrl+Alt+Delete**.
 - 3d Click **OK**.
- 4 Enable the Do Not Display Last User Name setting:
 - 4a Click the **Start** menu, click **Run**, type `secpol.msc`, then click **OK** to open the Local Security Settings.
 - 4b Expand **Local Policies > Security Options**.
 - 4c Double-click **Interactive logon: Do not display last user name**.
 - 4d Select **Enabled**, then click **OK**.

Using the Client for Open Enterprise

If a device is using the Client for Open Enterprise (formerly called the Novell Client) for Windows login, be aware of the following requirements:

- ♦ Novell Client 2 SP3 IR5 or later is required on Windows Vista/7/8.

- ◆ When using user ID/password authentication with the Client for Open Enterprise and DLU, the user needs to log in to the Client for Open Enterprise once before single sign-on will work. During single sign-on, the ZENworks PBA passes the user ID and password to the Client for Open Enterprise. 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 Client for Open Enterprise, NESCM (Novell Enhanced Smart Card Method) and DLU, the user needs to be the last user to have logged in to the Client. During single sign-on, the ZENworks PBA passes the pin to the 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 Client for Open Enterprise, NESCM, and **Disconnected Workstation Only** mode is not supported.

Synchronizing PBA and Windows Credentials

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 as long as 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.

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.

Using a ZENworks Control Center Quick Task

To use a ZENworks Full Disk Encryption Quick Task in ZENworks Control Center, a ZENworks administrator must be assigned the **Manage Endpoint Security Settings and Tasks** privilege. This privilege is configured through the Quick Tasks rights for administrators and administrator groups. For help configuring Quick Tasks rights, see the [ZENworks Administrator Accounts and Rights Reference](#).

Using a Quick Task to synchronize a user's PBA password with his or her Windows password requires you to know the Windows password.

- 1 In ZENworks Control Center, click **Devices**.
- 2 In the **Devices** panel, locate the user's device.
- 3 Select the check box next to the device, then click **Quick Tasks > FDE: Update PBA User** to display the Update PBA User dialog box.
- 4 Fill in the following fields:
 - Replace password if user already exists in PBA:** Make sure this option is selected.
 - User Name:** Specify the Windows user name.
 - 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.
 - Password:** Specify the user's Windows password.
- 5 Click **OK** to display the Quick Task Status dialog box.
- 6 In the Quick Task Status dialog box, click **Start** if you want to use the default options.

or

Configure the options as desired, then click **Start**.


For information about the options, click the Help icon in the Quick Task Status dialog box.

As soon as the Quick Task is complete, the user can authenticate to the ZENworks PBA using the new password.

Using the Full Disk Encryption Agent

You can use the Full Disk Encryption Agent to change the user's PBA password to match the Windows password.

To change the user's PBA password, you must know the FDE Administrator password for the policy assigned to the device, or you must know the ZENworks Agent override password or key.

- 1 On the device, right-click the ZENworks icon  in the notification area, and select **Technician Application**.
- 2 Click **Full Disk Encryption** in the ZENworks Agent navigation menu.
- 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 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 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.

Customizing the PBA Login Screen

The Pre-Boot Authentication login screen appears each time the device starts. The default background image for the login screen looks like the following:



The background image is a single file, `pba_bkgd_image.png`. If desired, you can replace the default image with your own custom image. Refer to the next three sections for more information.

IMPORTANT: If you want to customize the background image, you should do so before applying a Disk Encryption policy with Pre-Boot Authentication to devices. When the PBA is initialized, the PBA Linux partition is created and the background image is added to it. The only way to replace the background image after it is in the Linux partition is to remove the ZENworks PBA and reinstall it; this requires you deactivate the PBA in the Disk Encryption policy, update the policy on the device so that the PBA is removed, and then reactivate the PBA in the policy and reapply the policy to the device.

Creating a Custom Background Image File

A custom background image must meet the following two requirements:

- ♦ **Filename:** `pba_bkgd_image.png`
- ♦ **Size:** 800 pixels wide by 600 pixels high (800x600)

If you want to customize the default `pba_bkgd_image.png` rather than create a new file, complete the following steps to retrieve a copy of the default image file:

- 1 On a managed device that has ZENworks Full Disk Encryption enabled (no policy needs to be applied), locate the `fsesbrand.bin` file:

C:\Program Files (x86)\Novell\ZENworks\FDE\fsebrand.bin

- 2 Make a copy of the `fsebrand.bin` file and rename it to `fsebrand.zip`.
- 3 Extract the contents of the zip file to a location outside of the `c:\windows\nac\sbs` directory.
The contents are extracted to an `fsebrand` folder. The `pba_bkgd_image.png` file is located in that folder.

Adding the Custom Background Image File to the FSEBRAND.BIN File

After you create the custom background image file you want to use with the PBA login screen, you need to add the custom file to the `fsebrand.bin` file.

- 1 Extract the `fsebrand.bin` file to a temporary folder. If you already did this in order to get a copy of the `pba_bkgd_image.png` file (see [“Creating a Custom Background Image File” on page 19](#)), you can use that set of extracted files. Otherwise, complete the following steps to extract the `fsebrand.bin` file:

- 1a On a managed device that has ZENworks Full Disk Encryption enabled (no policy needs to be applied), locate the `fsebrand.bin` file:

C:\Program Files (x86)\Novell\ZENworks\FDE\fsebrand.bin

- 1b Make a copy of the `fsebrand.bin` file and rename it to `fsebrand.zip`.

- 1c Extract the contents of the zip file to a folder to a location outside of the `C:\Program Files (x86)\Novell\ZENworks\FDE` directory.

The contents are extracted to an `fsebrand` folder.

- 2 In the `fsebrand` folder, replace the default `pba_bkgd_image.png` file with your custom `pba_bkgd_image.png` file.
- 3 In the `fsebrand` folder, select all of the files and subfolders, right-click the selected files and folders, then select **Send To Compressed (zipped) Folder**.

Do not select the `fsebrand` folder itself, only its contents. Including the `fsebrand` folder nests the files too deep in the structure.

- 4 Rename the zip file to `fsebrand.bin`.

Distributing the Rebranded FSEBRAND.BIN File to Devices

After you add your custom background image file to the `fsebrand.bin` file (see [“Adding the Custom Background Image File to the FSEBRAND.BIN File” on page 20](#)), you need to distribute the `fsebrand.bin` file to devices that have ZENworks Full Disk Encryption enabled.

- 1 On a managed device, copy the `fsebrand.bin` file to the following directory:

C:\Program Files (x86)\Novell\ZENworks\FDE

If you have many devices for which you need to do this, you can use ZENworks Configuration Management to distribute the file as a Windows bundle to the devices. For information about creating a Windows bundle that copies a file to a device, see [“Creating Bundles”](#) in the *ZENworks 2017 Software Distribution Reference*.

- 2 Apply a Disk Encryption policy to the device.

After the policy is applied and the PBA login screen appears, your custom background image is displayed.

IMPORTANT: If you want to apply the custom background image to a device that already has ZENworks Pre-Boot Authentication installed, you must uninstall and reinstall the PBA. The background image is added to the PBA Linux partition (from the `fsebrand.bin` file) when the PBA is installed and cannot be changed after installation.

To uninstall and reinstall the PBA, modify the Disk Encryption policy to deactivate the PBA, then republish the policy to the device to remove the PBA. After the PBA is removed, make sure the rebranded `fsebrand.bin` file is in the `C:\Program Files (x86)\Novell\ZENworks\FDE` directory, then reactivate the PBA in the policy and reapply the policy to the device.

Upgrading to a new ZENworks version

When upgrading to a new version of ZENworks, a new `fsebrand.bin` file is created, and the background image for the PBA login screen reverts to the default system image. Maintaining a customized PBA login screen during upgrade is currently not supported. To customize the login screen after upgrade, follow the same procedure used in the initial customization. See [Customizing the PBA Login Screen](#).

NOTE: Do not copy the `fsebrand.bin` file from the older version and replace the `fsebrand.bin` file in the upgraded version of ZENworks. This file has functions that are specific to the current installed version, and replacing the file could cause issues after the upgrade.

3 PBA Override

The following sections provide information about overriding ZENworks Pre-Boot Authentication in cases such as a forgotten password or lost smart card.

PBA Override Versus Emergency Recovery

ZENworks Full Disk Encryption provides both authentication override for ZENworks Pre-Boot Authentication and emergency recovery of devices and their encrypted hard disks.

Pre-Boot Authentication Override (or PBA Override) is used in situations where the ZENworks PBA is still functional but the user cannot authenticate for reasons such as:

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

PBA Override cannot be used in the following situations. Instead, you need to perform an emergency recovery:

- ♦ 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.

This *ZENworks Full Disk Encryption Pre-Boot Authentication Reference* does not provide information about emergency recovery. For information about emergency recovery, see the [ZENworks Full Disk Encryption Emergency Recovery Reference](#).

Using the ZENworks PBA Helpdesk for PBA Override (User)

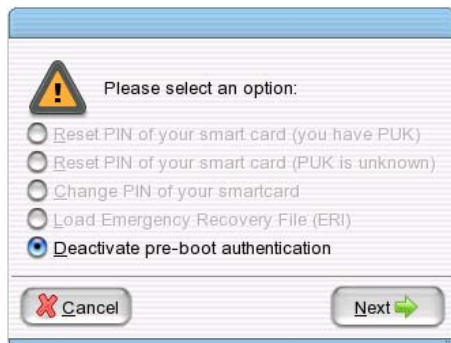
PBA Override uses the *challenge-response* methodology. The device user must provide a ZENworks administrator with a **request ID** and *challenge sequence* that can be used to generate a *response sequence* in ZENworks Control Center. When the response sequence is entered at the device, it authorizes the user to bypass the PBA for a set number of times.

The following steps explain how to use the ZENworks PBA Helpdesk to override the PBA. The steps must be performed on the device where the override is required. In addition, the ZENworks administrator must perform the steps in [Chapter , “Generating a Response Sequence for PBA Override \(Administrator\),” on page 26](#) to provide the user with the required response sequence.

- 1 Start the device so that it boots to the ZENworks PBA login screen.



- 2 Click **Helpdesk**.
- 3 Make sure that **Deactivate pre-boot authentication** is selected, and click **Next**.



- 4 Contact your ZENworks administrator who is running the FDE Pre-boot authentication override. Then, click **Next** to display the Request ID dialog box.

Helpdesk procedure step 2 of 4

Please relay the Request-ID below to your helpdesk officer and click 'Next'!

Request-ID

a | 0x160 | b | HVVMH | c | | d | | e | |

- 5 Give the request ID to your ZENworks administrator. Then, click **Next** to display the Challenge Sequence dialog box.

Helpdesk procedure step 3 of 4

Relay the Challenge sequence below (fields a to p) to your helpdesk officer and click 'Next'.

Challenge sequence

a | TGV69 | b | W4CMW | c | | d | | e | | f | | g | | h | | i | | j | | k | | l | | m | | n | | o | | p | |

[Click here to display the input guide.](#)

- 6 Give the challenge sequence to your ZENworks administrator. Then, click **Next** to display the Response Sequence dialog box.

Helpdesk procedure step 4 of 4

Carefully enter the response sequence from the helpdesk officer in these fields:

Response sequence

a | | b | | c | | d | | e | | f | | g | | h | |

- 7 Enter the response sequence you receive from your ZENworks administrator.

If you enter a value incorrectly, the box is outlined in red. Enter the value again before proceeding with the next value.

8 Click [Finish](#).

The device boots to Windows.

Generating a Response Sequence for PBA Override (Administrator)

PBA Override uses the *challenge-response* methodology. The user provides you with a *request ID* and *challenge sequence* that you use to generate a *response sequence* in ZENworks Control Center. You then provide the user with the response sequence that authorizes the user to bypass the PBA for a set number of times.

By default, the response sequence is calculated by using the Management Zone's unique override key. Therefore, it works only with devices registered in the zone. If you need to generate a response for a device registered in another zone, you must export a PBA Override file from that zone and use the PBA Override file to generate the correct response. The next three sections provide instructions for both methods.

Assigning the Administrator Rights Needed for PBA Override

Super Administrators have rights to perform all tasks in ZENworks Control Center. If a ZENworks administrator is not a Super Administrator, the administrator must be assigned the **Manage FDE PBA Override** privilege to use the PBA Override feature. If the administrator does not have this privilege, he or she is restricted to view rights for the PBA Override page.

This **Manage FDE PBA Override** privilege is configured through the Zone rights for individual administrators or administrator groups.

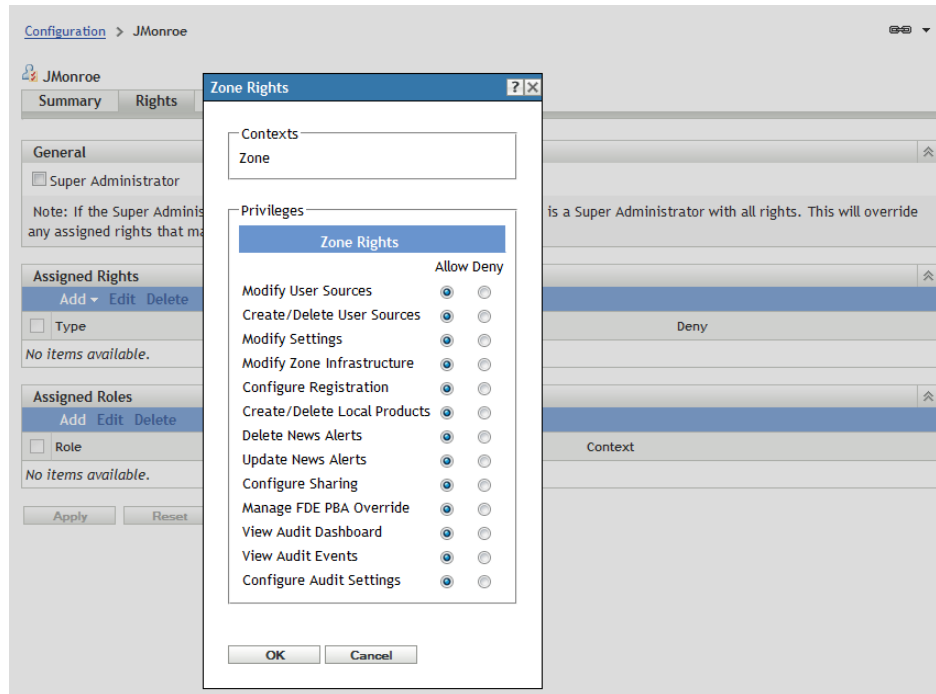
1 In ZENworks Control Center, click **Configuration**.

2 In the Administrators panel, click the administrator or administrator group to which you want to assign the privilege.

You can also use roles to assign the privilege to administrators. For instructions, see "[Managing Administrator Roles](#)" in the *ZENworks Administrator Accounts and Rights Reference*.

3 Click the **Rights** tab.

- 4 In the Assigned Rights panel, click **Add > Zone Rights** to display the Zone Rights dialog box.



- 5 By default, all privileges are set to **Allow**. Change any privileges you don't want the administrator to have to **Deny**, then click **OK**.
- 6 Click **Apply** to apply the changes to the administrator.

Generating a Response with the Zone Key

- 1 In ZENworks Control Center, click **Full Disk Encryption**, and then click **Pre-Boot Authentication Override**.

The screenshot shows the 'Pre-Boot Authentication Override' configuration page. At the top, there are three tabs: 'Workflow', 'Pre-Boot Authentication Override', and 'Emergency Recovery'. Below the tabs, there is a description of PBA Override and its methodology. The form contains several sections: 'Request ID' with two input fields labeled 'a' and 'b'; 'Challenge' with two input fields labeled 'a' and 'b'; 'Overrides Allowed' with a dropdown menu set to '1'; 'Generate Response' and 'Clear Values' buttons; a 'Response' text area; and 'PBA Override File' with a checkbox, a text field for the file name, and a password field.

- 2 In the **Request ID** fields, specify the request ID sequence supplied to you by the user.
The request ID sequence must be identical to the sequence presented to the user on his or her device. Your **Request ID** field A corresponds directly to the user's **Request ID** field A and your **Request ID** field B corresponds to the user's **Request ID** field B. Incorrect characters or order cause a sequence mismatch, resulting in an error when generating the response sequence.
- 3 In the **Challenge** fields, specify the challenge sequence supplied to you by the user.
As with the request ID sequence, the challenge sequence you enter must exactly match (characters and order) the user's challenge sequence.
- 4 In the **Overrides Allowed** field, specify the number of times you want to allow the user to boot the device without providing PBA authentication.
- 5 Click **Generate Response**.
- 6 Supply the response sequence to the user.
As with the request ID and challenge sequences you entered earlier, the user must enter the response sequence to exactly match (characters and order) the generated response sequence.

Generating a Response with a PBA Override File

The following instructions assume that you have exported the PBA Override file from another zone and want to use it to create a response for a device from that zone. The PBA Override file contains the override key from the other zone, which is needed to create the correct response for that zone's devices.

To generate a response:

- 1 In ZENworks Control Center, click **Full Disk Encryption**, then click **Pre-Boot Authentication Override**.

The screenshot shows the 'Pre-Boot Authentication Override' configuration page in ZENworks Control Center. At the top, there are three tabs: 'Workflow', 'Pre-Boot Authentication Override' (which is selected), and 'Emergency Recovery'. Below the tabs, there is a descriptive text about PBA Override. The main form contains three sections: 'Request ID' with two input fields labeled 'a' and 'b'; 'Challenge' with two input fields labeled 'a' and 'b'; and 'Overrides Allowed' with a label 'Number of PBA overrides allowed: *' and a single input field containing the number '1'. Below these sections are two buttons: 'Generate Response' and 'Clear Values'. The 'Response' section is a large empty text area. The 'PBA Override File' section includes a checkbox labeled 'Use PBA Override file to generate response', which is currently unchecked. Below the checkbox are two input fields: 'PBA Override File:' and 'PBA Override File Password:'.

- 2 In the **Request ID** section, specify the request ID sequence supplied to you by the user.

The request ID sequence must be identical to the sequence presented to the user on his or her device. Your **Request ID** field A corresponds directly to the user's **Request ID** field A and your **Request ID** field B corresponds to the user's **Request ID** field B. Incorrect characters or order cause a sequence mismatch, resulting in an error when generating the response sequence.

- 3 In the **Challenge** section, specify the challenge sequence supplied to you by the user.

As with the request ID sequence, the challenge sequence you enter must exactly match (characters and order) the user's challenge sequence.

- 4 In the **Overrides Allowed** section, specify the number of times you want to allow the user to boot the device without providing PBA authentication.

- 5 In the **PBA Override File** section, select the **Use PBA Override file to generate response** option, select the PBA Override (*.hdf) file, then specify the password for the file.
- 6 Click **Generate Response**.
- 7 Supply the response sequence to the user.
As with the request ID and challenge sequences you entered earlier, the user must enter the response sequence to exactly match (characters and order) the generated response sequence.

Overriding the PBA with an ERI File

A device's emergency recovery information (ERI) file can be used to perform a PBA override on self-encrypting hard disks. This method does not apply to standard hard disks.

Rather than use the challenge-response methodology, a user can load the ERI file for his or her device (including the ERI password) to bypass the ZENworks PBA. The bypass can unlock the disk one time, so the PBA remains active, locks the disk the next time the device powers off, and enforces pre-boot authentication on the next start up. Or, the bypass can deactivate the PBA, so the disk remains unlocked and no pre-boot authentication takes place on subsequent device startups.

- 1 Make sure the media (for example, a USB drive) containing the ERI file is inserted in the device.
- 2 Start the device so that it boots to the ZENworks PBA login screen.



- 3 Click **Helpdesk**.
- 4 Select **Load Emergency Recovery File**, and then click **Next**.



- 5 Use the file browser to locate and select the ERI file.
- 6 Choose the action you want performed when the ERI is loaded:
 - ♦ **Unlock disk temporarily:** This bypasses the PBA one time.

- ◆ **Deactivate pre-boot authentication:** This bypasses the PBA permanently.
- 7 Click **OK** to display the ERI password dialog box.
 - 8 Provide the ERI password, then click **OK**.

Pre-boot authentication is bypassed and the device boots to the Windows operating system. This process can take several minutes.

