

ZENworks 11 SP2 Full Disk Encryption

Beta 1 Test Scenarios

This document contains test scenarios for the Beta 1 release of Novell ZENworks 11 SP2 Full Disk Encryption.

Purpose of the Test Scenarios

The purpose of these exercises is to familiarize you with the new Full Disk Encryption capability added to ZENworks 11 SP2.

Assumptions

We assume that you have:

- Installed a ZENworks 11 SP2 system.
- Deployed the ZENworks Adaptive Agent and ZENworks Full Disk Encryption Agent to a Windows device. The ZFDE Agent is installed automatically with the ZENworks Adaptive Agent as long as you activated ZENworks Full Disk Encryption during installation of your ZENworks Server and subsequently have not disabled the agent by using the Agent Features options in ZENworks Control Center.

New Scenarios in Beta 1

The following scenarios are new in this beta. All other scenarios were published with the Alpha release.

6. [Configure Full Disk Encryption with Pre-Boot Authentication and smart card User Capturing](#)
7. [Configure Full Disk Encryption with Pre-Boot Authentication, smart card User Capturing, and pre-defined smart card certificates](#)
8. [Configure single sign-on between the ZENworks PBA and Windows using a smart card](#)
9. [Add or remove smart card certificates from the Certificates list](#)

Test Scenarios

There are 10 test scenarios in this document.

Part 1: Full Disk Encryption Only

1. [Configure Full Disk Encryption without Pre-Boot Authentication](#)

Part 2: Full Disk Encryption with Pre-Boot Authentication (User ID/Password)

2. [Configure Full Disk Encryption with Pre-Boot Authentication and User Capturing](#)
3. [Configure Full Disk Encryption with Pre-Boot Authentication, User Capturing, and pre-defined PBA user accounts](#)
4. [Configure single sign-on between the ZENworks PBA and Windows login](#)
5. [Add or remove users from the PBA Users list](#)

Part 3: Full Disk Encryption with Pre-Boot Authentication (Smart Card)

6. [Configure Full Disk Encryption with Pre-Boot Authentication and smart card User Capturing](#)

7. [Configure Full Disk Encryption with Pre-Boot Authentication, smart card User Capturing, and pre-defined smart card certificates](#)
8. [Configure single sign-on between the ZENworks PBA and Windows using a smart card](#)
9. [Add or remove smart card certificates from the Certificates list](#)

Part 4: Full Disk Encryption Imaging and Removal

10. [Take and restore an image of an encrypted hard disk](#)
11. [Remove disk encryption from a device](#)

Part 5: Appendixes

- A. [Supported Smart Cards and Smart Card Readers](#)
- B. [Supported PKCS#11 Middleware](#)

Part 1: Full Disk Encryption Only

ZENworks Full Disk Encryption includes two components: disk encryption and pre-boot authentication. The following scenario explains how to encrypt a disk only. The pre-boot authentication component is not installed, so authentication occurs through the Windows login client.

Test Scenario #1: Configure Full Disk Encryption without Pre-Boot Authentication

Objective

To encrypt a volume on a Windows device and require Windows login only (no ZENworks Pre-Boot Authentication) to access the encrypted volume.

Prerequisites

The target Windows device must meet the following requirements:

- Windows XP SP3 (32-bit) or Windows 7 (32-bit or 64-bit).
- For software-based encryption: IDE or SATA hard drive; SCSI drives are not supported in physical or virtual machines.
- For hardware-based encryption: Seagate Momentus FDE.x drive; no other drives are supported.
- The hard drive must have no more than 3 primary partitions. Windows supports 4 primary partitions, but ZENworks Full Disk Encryption must be able to create a 100MB primary partition to support ZENworks Pre-Boot Authentication, encryption key storage, and Emergency Recovery Information (ERI) file storage.
- (Recommended): A small, non-system volume (partition) to encrypt. You can encrypt the system volume or larger volumes if desired, but the test scenario will be faster if you use a small, non-system volume.

Steps

1. In ZENworks Control Center, click *Policies*.
2. In the Policies panel, click *New > Policy*.
3. In the policy category, select *General Endpoint Security Policies*, then click *Next*.
4. Select *Disk Encryption Policy* as the policy type, then click *Next*.
5. On the Define Details page, specify a policy name and description, then click *Next*.
6. On the Configure Disk Encryption – Volumes and Algorithm page:
 - a) Select *Encrypt specific local fixed volumes*, then click *Add* to specify the volume to encrypt.
 - b) In the Encryption Settings section, select the algorithm and key length you want to use. If you don't have a preference, you should keep the default (AES and 256).
 - c) Deselect the *Encrypt only the used sectors of the drive* if you want all sectors of the drive to be encrypted, even if they are not currently being used.
7. Click *Next*.
8. On the Configure Disk Encryption – Admin Password and Encryption Initialization page:
 - a) In the Admin Password section, click *Change* to assign an Admin password to the Full Disk Encryption Agent.
 - b) In the Reboot Options section, select *Display predefined message to user before rebooting*, then select *Override predefined message with custom message*. Enter “Disk Encryption Reboot” as the title, then enter “The device is being rebooted for disk encryption” in the message body.
 - c) In the CheckDisk Options section, select *Do not run Windows check disk*. This will save time during the reboot process; if you think the target disk might have errors, you should run Windows check disk.
9. Click *Next*.

10. On the Configure Pre-Boot Authentication – Authentication Methods page, select *Disable pre-boot authentication (use Windows authentication only)*. This turns off ZENworks Pre-Boot Authentication.
11. Click *Next*.
12. On the Configure Logging page, leave the default settings, then click *Next*.
13. Review the selected details in the Summary page, then click *Finish* to create the policy.
14. Assign the policy to a device.
15. Refresh the ZENworks Adaptive Agent on the device to apply the policy.
16. Follow the prompts to reboot.

Expected Results

- 1) The Reboot prompt is launched and displays the custom message you entered.
- 2) During the reboot, if the device is Windows XP, you will see a 100MB primary partition being created. This partition, referred to as the ZFDE partition, is used for the PBA Linux kernel, storage of the encryption keys, and temporary storage of the Emergency Recovery Information (ERI) file.
- 3) After reboot, when you log in to Windows on the device, you have access to the encrypted volume.
- 4) You can access the Full Disk Encryption About box (Z-icon > Properties > Full Disk Encryption > About) to see that the policy is enforced and the drive encrypted.

Part 2: Full Disk Encryption with Pre-Boot Authentication (User ID/Password)

ZENworks Pre-Boot Authentication provides increased security for encrypted hard disks. Rather than relying on Windows login to secure access to the encrypted volumes, you can install the ZENworks PBA to a Linux partition that is hardened and protected from alteration through the use of MD5 checksums. In addition, the PBA uses strong encryption for authentication keys.

The ZENworks PBA supports two authentication methods: user ID/password and smart card. The following scenarios explain how to use the user ID/password method. See ??? for scenarios that use the smart card method.

Test Scenario #2: Configure Full Disk Encryption with Pre-Boot Authentication and User Capturing

Objective

To encrypt a volume on a Windows device, using ZENworks Pre-Boot Authentication (with User Capturing enabled) to access the volume.

The ZENworks PBA is a Linux-based component. When the Disk Encryption policy is applied to a device, a small Linux partition containing the ZENworks PBA is created on the hard disk. During normal operation, the device boots to the Linux partition and loads the ZENworks PBA. As soon as the user provides the appropriate credentials (user ID/password or smart card), the PBA terminates and the Windows operating system boots, providing access to the encrypted data on the previously hidden and inaccessible Windows drives.

The Linux partition, and ZENworks PBA software, is hardened and protected from alteration through the use of MD5 checksums, and the PBA uses strong encryption for authentication keys.

To log in through the ZENworks PBA and gain access to the encrypted drive, a user must have a PBA account. As part of the ZENworks Pre-Boot Authentication configuration, you can enable User Capturing so that the first user to log in to Windows is automatically given a ZENworks PBA account.

Prerequisites

The target Windows device must meet the following requirements:

- Windows XP SP3 (32-bit) or Windows 7 (32-bit or 64-bit).
- For software-based encryption: IDE or SATA hard drive; SCSI drives are not supported in physical or virtual machines.
- For hardware-based encryption: Seagate Momentus FDE.x drive; no other drives are supported.
- The hard drive must have no more than 3 primary partitions. Windows supports 4 primary partitions, but ZENworks Full Disk Encryption must be able to create a 100MB primary partition to support ZENworks Pre-Boot Authentication, encryption key storage, and Emergency Recovery Information (ERI) file storage.
- (Recommended): A small, non-system volume (partition) to encrypt. You can encrypt the system volume or larger volumes if desired, but the test scenario will be faster if you use a small, non-system volume.

Steps

1. In ZENworks Control Center, click *Policies*.
2. In the Policies panel, click *New > Policy*.
3. In the policy category, select *General Endpoint Security Policies*, then click *Next*.
4. Select *Disk Encryption Policy* as the policy type, then click *Next*.
5. On the Define Details page, specify a policy name and description, then click *Next*.
6. On the Configure Disk Encryption – Volumes and Algorithm page:
 - a) Select *Encrypt specific local fixed volumes*, then click *Add* to specify the volume to encrypt.
 - b) In the Encryption Settings section, select the algorithm and key length you want to use. If you don't have a preference, you should keep the default (AES and 256).
 - c) Deselect the *Encrypt only the used sectors of the drive* if you want all sectors of the drive to be encrypted, even if they are not currently being used.
 - d) Click *Next*.
7. On the Configure Disk Encryption – Admin Password and Encryption Initialization page:
 - a) In the Admin Password section, click *Change* to assign an Admin password to the Full Disk Encryption Agent.
 - b) In the Reboot Options section, select *Display predefined message to user before rebooting*, then select *Override predefined message with custom message*. Enter “Disk Encryption Reboot” as the title, then enter “The device is being rebooted for disk encryption” in the message body.
 - c) In the CheckDisk Options section, select *Do not run Windows check disk*. This will save time during the reboot process; if you think the target disk might have errors, you should run Windows check disk.
 - d) Click *Next*.
8. On the Configure Pre-Boot Authentication – Authentication Methods page:
 - a) In the Authentication Methods section, select *Enable User ID/Password Authentication*.
 - b) In the User ID/Password Authentication Settings section, select *Create PBA account for first user who logs in to Windows after the policy is applied (User Capturing)*.
 - c) Click *Next*.
9. On the Configure Pre-Boot Authentication – Reboot and Lockout page:
 - a) In the Reboot Options section, select *Display predefined message to user before rebooting*, then select *Override predefined message with custom message*. Enter “PBA Reboot” as the title, then enter “The device is being rebooted for Pre-Boot Authentication” in the message body.
 - b) In the Lockout Settings section, leave the default settings.
 - c) Click *Next*.
10. On the Configure Logging page, leave the default settings, then click *Next*.
11. Review the selected details in the Summary page, then click *Finish* to create the policy.
12. Assign the policy to a device.
13. Refresh the ZENworks Adaptive Agent on the device to apply the policy.
14. Follow the prompts to reboot.

Expected Results

- 1) The Disk Encryption Reboot prompt is launched and displays the custom message you entered.
- 2) During the reboot, if the device is Windows XP, you will see a 100MB primary partition being created. This partition, referred to as the ZFDE partition, is used for the PBA Linux kernel and temporary storage of the Emergency Recovery Information (ERI) file.
- 3) After the Disk Encryption reboot, you are prompted to log in to Windows. These login credentials are captured and added as a ZENworks PBA account.
- 4) After logging in to Windows, the PBA Reboot prompt is displayed.
- 5) After the PBA reboot, pre-boot authentication is enforced. You must log in to the ZENworks PBA using the Windows credentials.
- 6) After the PBA login, you are prompted with the Windows login. Scenario 4 shows how to use single-sign on so that you only have to log in to the ZENworks PBA.

- 7) You can access the Full Disk Encryption About box (Z-icon > Show Properties > Full Disk Encryption > About) to see that the policy is enforced and the drive encrypted.

Test Scenario #3: Configure Full Disk Encryption with Pre-Boot Authentication, User Capturing, and pre-defined PBA user accounts

Objective

To enable user to log in to the ZENworks PBA using a pre-defined account and gain access to the encrypted drive.

To log in through the ZENworks PBA and gain access to the encrypted drive, a user must have a PBA account. The account can be captured during first log in (as done in Scenario 2), or it can be defined in the Disk Encryption policy in ZENworks Control Center. This scenario has you use an account defined in the policy.

Prerequisites

- Completion of [Scenario 2](#).

Steps

1. In ZENworks Control Center, click *Policies*.
2. In the Policies panel, click the Disk Encryption policy created in [Scenario 2](#).
3. Click the policy's *Details* tab
4. Click the *Pre-Boot Authentication* sub tab.
5. In the User ID/Password Authentication Settings section:
 - a) Select the *Allow access for the following users* option to activate it.
 - b) In the PBA Users list, click *Add*.
 - c) In the *User Name* field, specify the user name of the user for whom you want to create the PBA account. This can be any user name you want; it does not have to match a Windows user name. To log in this scenario, you will need to enter both the ZENworks PBA credentials and a valid Windows credentials (during Windows login). They can be the same credentials or different credentials. Scenario 4 explains how to use single-sign on to enable one login for the ZENworks PBA and Windows.
 - d) In the *Password* and *Confirm Password* fields, specify a password.
 - e) Click *OK* to add the user to the PBA Users list.
6. Click *Apply* (at the bottom of the page).
7. Next to the displayed version, click *Publish*, make sure *Publish as new version* is selected, then click *Finish*.
8. Refresh the ZENworks Adaptive Agent on the device to apply the policy changes.
9. Reboot the device and log in using the PBA user account you added.

Expected Results

- 1) You can use the new PBA user account and a valid Windows login to access the encrypted volume.
- 2) To see the PBA Users list on the device, you can access the Full Disk Encryption About box (Z-icon > Show Properties > Full Disk Encryption > About), click Agent Status, specify the FDE Admin Password, click the PBA tab, then scroll down to the PBA Users List.

Test Scenario #4: Configure single sign-on between the ZENworks PBA and Windows login

Objective

To enable a user to enter Windows credentials one time to authenticate to both the ZENworks PBA and Windows login.

Prerequisites

- Completion of [Scenario 3](#).
- If you want single sign-on to apply not only to the ZENworks PBA and Windows login but also to the ZENworks user login, you can define the user's directory (user source) in ZENworks Control Center.

Steps

1. In ZENworks Control Center, click *Policies*.
2. In the Policies panel, click the Disk Encryption policy used in [Scenario 3](#).
3. Click the policy's *Details* tab
4. Click the *Pre-Boot Authentication* sub tab
5. In the Authentication Methods section, select the *Activate single sign-on for ZENworks PBA and Windows login* option.
6. If you want to use the credentials for the captured user ([Scenario 2](#)) to log in, skip to step 7.
or
To use credentials for another user you add to the PBA user list ([Scenario 3](#)):
 - a) In the PBA Users list, click *Add*.
 - b) In the *User Name* field, specify the user name of the user for whom you want to create the PBA account. The user name must be a valid Windows user.
 - c) In the *Domain* field, specify the user's Windows domain or workgroup.
 - d) In the *Password* and *Confirm Password* fields, specify a password.
 - e) Click *OK* to add the user to the PBA Users list.
7. Click *Apply* (at the bottom of the page).
8. Next to the displayed version, click *Publish*, make sure *Publish as new version* is selected, then click *Finish*.
9. Refresh the ZENworks Adaptive Agent on the device to apply the policy changes.
10. Reboot the device and log in using the captured user's credentials or the PBA user account credentials you added.

Expected Results

- 1) After entering the Windows login credentials in the ZENworks PBA, you are not prompted to log in to Windows.

Test Scenario #5: Add or remove users from the PBA Users list

Objective

To modify the PBA user list in order to add user access or remove user access.

Prerequisites

- Completion of [Scenario 3](#) or [Scenario 4](#).
or
A Disk Encryption policy that has at least one user in the PBA User list; the policy must have already been applied to a device.

Steps

1. In ZENworks Control Center, click *Policies*.
2. In the Policies panel, click a Disk Encryption policy that has at least one user in the PBA User list.
3. Click the policy's *Details* tab
4. Click the *Pre-Boot Authentication* sub tab
5. In the User ID/Password Authentication Settings section:
6. If you want to add a PBA user account:
 - a) In the PBA Users list, click *Add*.
 - b) In the *User Name* field, specify the user name of the user for whom you want to create the PBA account. If you are using single sign-on for the ZENworks PBA and Windows login, the user name must be a valid Windows user.
 - c) In the *Domain* field, specify the user's Windows domain or workgroup. This is only necessary if you are using single sign-on.
 - d) In the *Password* and *Confirm Password* fields, specify the password.
 - e) Click *OK* to add the user to the PBA Users list.
7. If you want to remove a PBA user account:
 - a) In the PBA Users list, click the check box next to the user you want to remove, click *Remove*, then click *OK* to confirm the removal.
 - b) Select the *Remove existing users from PBA if not in this list* option. If you do not select this option, the user is not removed. You should also be aware that this removes the captured user, so you need to have at least one user in the PBA Users list to log in, or you need to have the *Create PBA account for first user who logs in to Windows after the policy is applied* option enabled.
8. Click *Apply* (at the bottom of the page).
9. Next to the displayed version, click *Publish*, make sure *Publish as new version* is selected, then click *Finish*.
10. Refresh the ZENworks Adaptive Agent on the device to apply the policy changes.

Expected Results

- 1) If you added a PBA user account, you can now log in using that account.
- 2) If you removed a PBA user account, you can no longer log in using that account.
- 3) To see the PBA Users list on the device, you can access the Full Disk Encryption About box (Z-icon > Show Properties > Full Disk Encryption > About), click Agent Status, specify the FDE Admin Password, click the PBA tab, then scroll down to the PBA Users List.

Part 3: Full Disk Encryption with Pre-Boot Authentication (Smart Card)

ZENworks Pre-Boot Authentication provides increased security for encrypted hard disks. Rather than relying on Windows login to secure access to the encrypted volumes, you can install the ZENworks PBA to a Linux partition that is hardened and protected from alteration through the use of MD5 checksums. In addition, the PBA uses strong encryption for authentication keys.

The ZENworks PBA supports two authentication methods: user ID/password and smart card. The following scenarios explain how to use the smart card method. See [Part 2](#) for scenarios that use the user ID/password method.

Test Scenario #6: Configure Full Disk Encryption with Pre-Boot Authentication and smart card User Capturing

Objective

To encrypt a volume on a Windows device, using ZENworks Pre-Boot Authentication (with Smart Card User Capturing enabled) to access the volume.

The ZENworks PBA is a Linux-based component. When the Disk Encryption policy is applied to a device, a small Linux partition containing the ZENworks PBA is created on the hard disk. During normal operation, the device boots to the Linux partition and loads the ZENworks PBA. As soon as the user provides the appropriate credentials (user ID/password or smart card), the PBA terminates and the Windows operating system boots, providing access to the encrypted data on the previously hidden and inaccessible Windows drives.

The Linux partition, and ZENworks PBA software, is hardened and protected from alteration through the use of MD5 checksums, and the PBA uses strong encryption for authentication keys.

To log in through the ZENworks PBA and gain access to the encrypted drive, a user must have a PBA account. As part of the ZENworks Pre-Boot Authentication configuration, you can enable Smart Card User Capturing so that the first user to log in to the ZENworks PBA is automatically given a ZENworks PBA account.

Prerequisites

The target Windows device must meet the following requirements:

- Windows XP SP3 (32-bit) or Windows 7 (32-bit or 64-bit).
- For software-based encryption: IDE or SATA hard drive; SCSI drives are not supported in physical or virtual machines.
- For hardware-based encryption: Seagate Momentus FDE.x drive; no other drives are supported.
- The hard drive must have no more than 3 primary partitions. Windows supports 4 primary partitions, but ZENworks Full Disk Encryption must be able to create a 100MB primary partition to support ZENworks Pre-Boot Authentication, encryption key storage, and Emergency Recovery Information (ERI) file storage.
- (Recommended): A small, non-system volume (partition) to encrypt. You can encrypt the system volume or larger volumes if desired, but the test scenario will be faster if you use a small, non-system volume.

- A smart card reader and PKCS#11 middleware that is listed in [Appendix A: Supported Tokens and Smart Card Readers](#) and [Appendix B: Supported PKCS#11 Middleware](#).

Steps

1. In ZENworks Control Center, click *Policies*.
2. In the Policies panel, click *New > Policy*.
3. In the policy category, select *General Endpoint Security Policies*, then click *Next*.
4. Select *Disk Encryption Policy* as the policy type, then click *Next*.
5. On the Define Details page, specify a policy name and description, then click *Next*.
6. On the Configure Disk Encryption – Volumes and Algorithm page:
 - a) Select *Encrypt specific local fixed volumes*, then click *Add* to specify the volume to encrypt.
 - b) In the Encryption Settings section, select the algorithm and key length you want to use. If you don't have a preference, you should keep the default (AES and 256).
 - c) Deselect the *Encrypt only the used sectors of the drive* if you want all sectors of the drive to be encrypted, even if they are not currently being used.
 - d) Click *Next*.
7. On the Configure Disk Encryption – Admin Password and Encryption Initialization page:
 - a) In the Admin Password section, click *Change* to assign an Admin password to the Full Disk Encryption Agent.
 - b) In the Reboot Options section, select *Display predefined message to user before rebooting*, then select *Override predefined message with custom message*. Enter “Disk Encryption Reboot” as the title, then enter “The device is being rebooted for disk encryption” in the message body.
 - c) In the CheckDisk Options section, select *Do not run Windows check disk*. This will save time during the reboot process; if you think the target disk might have errors, you should run Windows check disk.
 - d) Click *Next*.
8. On the Configure Pre-Boot Authentication – Authentication Methods page:
 - a) In the Authentication Methods section, select *Enable Smart Card Authentication*.
 - b) In the Smart Card Authentication Settings section, select the device's Smart Card Reader and PKCS#11 Provider.
 - c) In the Smart Card Authentication Settings section, select *Create PBA account for first smart card user who logs in to the ZENworks PBA after the policy is applied (User Capturing)*.
 - d) Click *Next*.
9. On the Configure Pre-Boot Authentication – Reboot and Lockout page:
 - a) In the Reboot Options section, select *Display predefined message to user before rebooting*, then select *Override predefined message with custom message*. Enter “PBA Reboot” as the title, then enter “The device is being rebooted for Pre-Boot Authentication” in the message body.
 - b) In the Lockout Settings section, leave the default settings.
 - c) Click *Next*.
10. On the Configure Logging page, leave the default settings, then click *Next*.
11. Review the selected details in the Summary page, then click *Finish* to create the policy.
12. Assign the policy to a device.
13. Refresh the ZENworks Adaptive Agent on the device to apply the policy.
14. Follow the prompts to reboot.

Expected Results

- 1) The Disk Encryption Reboot prompt is launched and displays the custom message you entered.
- 2) During the reboot, if the device is Windows XP, you will see a 100MB primary partition being created. This partition, referred to as the ZFDE partition, is used for the PBA Linux kernel and temporary storage of the Emergency Recovery Information (ERI) file.
- 3) After the Disk Encryption reboot, you are prompted to log in to the ZENworks PBA. The smart card is captured and added as a ZENworks PBA account.

- 4) After logging in, the PBA Reboot prompt is displayed.
- 5) After the PBA reboot, pre-boot authentication is enforced. You must log in to the ZENworks PBA using the smart card.
- 6) After the PBA login, you are prompted with the Windows login. Scenario 8 shows how to use single-sign on so that you only have to log in to the ZENworks PBA.
- 7) You can access the Full Disk Encryption About box (Z-icon > Show Properties > Full Disk Encryption > About) to see that the policy is enforced and the drive encrypted.

Test Scenario #7: Configure Full Disk Encryption with Pre-Boot Authentication, smart card User Capturing, and pre-defined smart card certificates

Objective

To enable a user to log in to the ZENworks PBA using a pre-defined account and gain access to the encrypted drive.

To log in through the ZENworks PBA and gain access to the encrypted drive, a user must have a PBA account. The account can be captured during first log in (as done in Scenario 6), or it can be defined in the Disk Encryption policy in ZENworks Control Center. This scenario has you use an account defined in the policy.

Prerequisites

- Completion of [Scenario 6](#).

Steps

1. In ZENworks Control Center, click *Policies*.
2. In the Policies panel, click the Disk Encryption policy created in [Scenario 6](#).
3. Click the policy's *Details* tab
4. Click the *Pre-Boot Authentication* sub tab.
5. In the Smart Card Authentication Settings section:
 - a) Select the *Allow certificate content to be used for authentication* option to activate it.
 - b) In the *Certificates* list, click *Add*.
 - c) In the *Certificate Name* field, specify a name for the certificate. This can be any name; it is used only for display purposes in ZENworks Control Center.
 - d) In the *Certificate Content* fields, paste the contents of the smart card certificate to be used for authentication. You must use an X.509 certificate (*.cer; DER-encoded).
 - e) Click *OK* to add the certificate to the list.
6. In the Smart Card Authentication Settings section:
 - a) In the *Key Usages* list, click *Add* to specify the key usages that must be present in the certificate to allow authentication.
or
Select *Allow certificate labels to be used for authentication*, click *Add*, then add the certificate's label to the list.
The key usages or certificate labels further identify the certificate. This adds a second layer of security to the certificate authentication. For more information about these two options, refer to the ZENworks Control Center Help.
7. Click *Apply* (at the bottom of the page).
8. Next to the displayed version, click *Publish*, make sure *Publish as new version* is selected, then click *Finish*.
9. Refresh the ZENworks Adaptive Agent on the device to apply the policy changes.
10. Reboot the device and log in using the smart card whose certificate you added.

Expected Results

- 1) You can use the new smart card certificate and a valid Windows login to access the encrypted volume.
- 2) To see the PBA Users list on the device, you can access the Full Disk Encryption About box (Z-icon > Show Properties > Full Disk Encryption > About), click Agent Status, specify the FDE Admin Password, click the PBA tab, then scroll down to the PBA Users List.

Test Scenario #8: Configure single sign-on between the ZENworks PBA and Windows using a smart card

Objective

To enable a user to provide the smart card and PIN one time to authenticate to both the ZENworks PBA and Windows.

Prerequisites

- Completion of [Scenario 7](#).
- The device must use the CryptoVision, Gemalto, or RSA SID smart card reader and middleware listed in [Appendix A: Supported Tokens and Smart Card Readers](#) and [Appendix B: Supported PKCS#11 Middleware](#). Other solutions might work with single sign-on but have not been tested and are not supported.
- If you want single sign-on to apply not only to the ZENworks PBA and Windows login but also to the ZENworks user login, you can define the user's directory (user source) in ZENworks Control Center.

Steps

1. In ZENworks Control Center, click *Policies*.
2. In the Policies panel, click the Disk Encryption policy used in [Scenario 7](#).
3. Click the policy's *Details* tab
4. Click the *Pre-Boot Authentication* sub tab
5. In the Authentication Methods section, select the *Activate single sign-on for ZENworks PBA and Windows login* option.
6. Click *Apply* (at the bottom of the page).
7. Next to the displayed version, click *Publish*, make sure *Publish as new version* is selected, then click *Finish*.
8. Refresh the ZENworks Adaptive Agent on the device to apply the policy changes.
9. Reboot the device and log in using the captured smart card or another smart card certificate you defined in the policy.

Expected Results

- 1) After logging in to the ZENworks PBA, you are not prompted to log in to Windows.

Test Scenario #9: Add or remove smart card certificates from the Certificates list

Objective

To modify the Certificates list in order to add smart card user access or remove smart card user access.

Prerequisites

- Completion of [Scenario 7](#) or [Scenario 8](#).
or
A Disk Encryption policy that has at least one certificate in the Certificates list; the policy must have already been applied to a device.

Steps

1. In ZENworks Control Center, click *Policies*.
2. In the Policies panel, click a Disk Encryption policy that has at least one certificate in the Certificates list.
3. Click the policy's *Details* tab
4. Click the *Pre-Boot Authentication* sub tab
5. In the Smart Card Authentication Settings section:
6. If you want to add a smart card certificate:
 - a) In the *Certificates* list, click *Add*.
 - b) In the *Certificate Name* field, specify a name for the certificate. This can be any name; it is used only for display purposes in ZENworks Control Center.
 - c) In the *Certificate Content* fields, paste the contents of the smart card certificate to be used for authentication. You must use an X.509 certificate (*.cer; DER-encoded).
 - d) Click *OK* to add the certificate to the list.
7. If you want to remove a certificate:
 - a) In the Certificates list, click the check box next to the certificate you want to remove, click *Remove*, then click *OK* to confirm the removal.
 - b) Select the *Remove existing certificates from PBA if not in this list* option. If you do not select this option, the certificate is not removed from the PBA. You should also be aware that this removes the captured smart card certificates, so you need to have at least one smart card certificate in the Certificates list to log in, or you need to have the *Create PBA account for first smart card user who logs in to the ZENworks PBA after the policy is applied* option enabled.
8. Click *Apply* (at the bottom of the page).
9. Next to the displayed version, click *Publish*, make sure *Publish as new version* is selected, then click *Finish*.
10. Refresh the ZENworks Adaptive Agent on the device to apply the policy changes.

Expected Results

- 1) If you added a smart card certificate, you can now log in using that smart card.
- 2) If you removed a smart card certificate, you can no longer log in using that smart card.
- 3) To see the PBA Users list on the device, you can access the Full Disk Encryption About box (Z-icon > Show Properties > Full Disk Encryption > About), click Agent Status, specify the FDE Admin Password, click the PBA tab, then scroll down to the PBA Users List.

Part 4: Full Disk Encryption Imaging and Removal

The following scenarios provide instructions for taking and restoring an image of an encrypted disk and for decrypting an encrypted disk by removing ZENworks Full Disk Encryption from a device.

Test Scenario #10: Take and restore an image of an encrypted hard disk

Objective

To take an image of an encrypted hard disk and restore the image on the same device using raw imaging.

Prerequisites

- The device must have a Disk Encryption policy enforced, with the ZENworks PBA enabled. See [Scenario 2](#) if necessary.
- A standard hard disk. Imaging of self-encrypting drives is not supported.
- The image cannot include any add ons. Add-on imaging is not supported with encrypted disks.

Steps

1. On the device, use the ZFDE About box (Z-icon > Show Properties > Full Disk Encryption > About) to verify that the disk is encrypted.
2. In ZENworks Control Center, locate the device in the Workstations list.
3. Select the check box next to the device, then click *Action > Take an image*.
4. Complete the wizard to take the image.
5. Create a ZENworks Imaging Preboot bundle that includes the new image.
6. Assign the bundle to the same device from which the image was taken. The image is restored completely.
7. Replace the device's hard disk with a new hard disk and restore the image.

Expected Results

- 1) The image is restored to the device. Note: You cannot restore an image to a different device. It must be the same device with either the same hard disk or a new hard disk.
- 2) If you are unable to successfully perform the scenario, send us the imglog and novell-pbserv.log.

Test Scenario #11: Remove disk encryption from a device

Objective

To remove a Disk Encryption policy, decrypt the encrypted drives, and remove ZENworks Pre-Boot Authentication.

Prerequisites

- A Disk Encryption policy, with the ZENworks PBA enabled, applied to a device. See [Scenario 2](#).

Steps

1. In ZENworks Control Center, click *Policies*.
2. In the Policies panel, click the Disk Encryption policy.
3. Click the policy's *Relationships* tab
4. In the Device Assignments list, click the check box next to the device from which you want to remove the policy, then click *Remove*.
5. Refresh the ZENworks Adaptive Agent on the device to apply the policy changes.
6. Follow the reboot prompts that are displayed as the Disk Encryption policy and ZENworks PBA are removed.

Expected Results

- 1) After the ZENworks Adaptive Agent refresh, the drive is decrypted, the policy is removed, and you receive a reboot prompt.
- 2) After the reboot, you should not be prompted to authenticate to the ZENworks PBA and the Disk Encryption policy should not be applied. To validate that the policy is not applied, you can access the Full Disk Encryption About box (Z-icon > Show Properties > Full Disk Encryption > About). The status should be “No Policy”.

Part 5: Appendix

Appendix A: Supported Tokens and Smart Card Readers

- Aladdin eToken Pro 32k (issued with RTE 3.6)
- Aladdin eToken Pro 64 k, NG-Flash, NG-OTP (issued with RTE 3.6)
- Common Access Cards (CAC)
- Dell smart card reader keyboard
- Eutron Crypto Identity
- Eutron Crypto Combo
- GemPC Twin
- Gemalto .Net
- 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 ProfessionalKobil 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 V.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

Appendix B: Supported PKCS#11 Middleware

- 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 SID 800
- SECUDE 1.3.0
- SECUDE TCOS 1.7.0
- Siemens CardOS HiPath 5.0.12
- Schlumberger Axalto 5.2
- Telesec 3.0.5