

ZENworks 11 SP3

Test Scenarios for *Full Disk Encryption*

This document contains test scenarios for ZENworks 11 SP3 Beta.

Purpose of the Test Scenarios

The purpose of these scenarios is to help you get familiar with some of the new features included in ZENworks 11 SP3 Full Disk Encryption.

Assumptions

- You have installed ZENworks 11 SP3. For instructions, see the *ZENworks 11 SP3 Installation Guide* (<http://www.novell.com/documentation/zenworks113/>).

Test Scenarios

1. [Apply a Disk Encryption Policy that Blocks the 1394 \(FireWire\) Port](#)
2. [Audit Changes to Disk Encryption Policies](#)

Test Scenario #1: Apply a Disk Encryption Policy that Blocks the 1394 (FireWire) Port

Objective

To enable you to apply a Disk Encryption policy to a Windows device that encrypts a single volume and blocks any devices connected to the 1394 (FireWire) port.

The 1394 interface provides direct memory access, or DMA. Direct access to system memory can compromise security by providing read and write access to stored sensitive data, including encryption and authentication data used by ZENworks Full Disk Encryption. Prevent direct access to memory through the 1394 port increases security for the device information.

Prerequisites

The target Windows device must meet the following requirements:

- Windows XP SP3 (32-bit), Windows Vista (32-bit or 64-bit), Windows 7 (32-bit or 64-bit), or Windows 8.
- 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.

Procedure

1. In ZENworks Control Center, click *Policies*.
2. In the Policies panel, click *New > Policy*.
3. In the Platform list, select *Windows*, then click *Next*.
4. In the Policy Category list, select *Windows Full Disk Encryption Policies*, then click *Next*.
5. Select *Disk Encryption Policy* as the policy type, then click *Next*.
6. On the Define Details page, specify a policy name (for example, *DiskEncryptionPolicy*), then click *Next*.

7. On the Configure Disk Encryption – Volumes, Algorithm, and Emergency Recovery 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) Select the *Block 1394 (FireWire) port* option.
 - d) Click *Next*.
8. On the Configure Disk Encryption – Admin Password and Encryption Initialization page:
 - a) In the Admin Password section, click *Set* to assign an Admin password to the Full Disk Encryption Agent.
 - b) 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.
 - c) Click *Next*.
9. On the Configure Pre-Boot Authentication – Authentication Methods page, leave the *Enable pre-boot authentication* option disabled, then click *Next*.
10. Review the selected details in the Summary page, then click *Finish* to create the policy.
11. Assign the policy to a device.
12. Refresh the ZENworks Adaptive Agent on the device to apply the policy.
13. Follow the prompts to reboot.

Expected Results

- After reboot, when you log in to Windows on the device, you have access to the encrypted volume.
- When you plug a device into the 1394 port, you cannot access the device. If you open Device Manager, the 1394 device is disabled. Note that the 1394 port itself is not disabled; the 1394 port cannot be disabled. However, any devices plugged into the 1394 port are disabled.

Test Scenario #2: Audit Changes to Disk Encryption Policies

Objective

To turn on auditing of Disk Encryption policies so that changes to the policies are recorded.

Prerequisites

- At least one existing Disk Encryption policy. For help creating a Disk Encryption policy, see the [ZENworks 11 SP3 Full Disk Encryption Policies Reference](#).

Procedure

Complete the steps in the following sections to enable the audit change event, make changes to a Disk Encryption policy, and view the generated audit change event.

Enable the Audit Change Event for Security Policies

1. In the left navigation pane of ZENworks Control Center, click *Configuration*.
2. In the *Configuration* tab, under *Management Zone Settings*, click *Audit Management*.
3. Click *Events Configuration*.
4. Under *Change Events*, click *Add* to display the *Add Change Events* dialog box.
5. Expand the Change Events tree and select *Full Disk Encryption Policy Modified*.
6. In the *Event Settings* section, set the *Event Classification* to *Informational*.
7. Specify the *Days to Keep* as 30.
8. Click *OK* to add the event and close the *Add Change Events* dialog box.

Modify a Security Policy Setting

1. In the left navigation pane of ZENworks Control Center, click *Policies*.
2. In the Policies list, double-click a Disk Encryption policy to display its properties.
3. Click *Details* to display the policy's settings.
4. Change one of the settings, then click *Apply* to save the changes.

View the Change Event

1. In the left navigation pane of ZENworks Control Center, click *Dashboard*.
2. In the *Top 5 Change Events by Administrator* section, click *Full Disk Encryption Policy Modified*.

If *Full Disk Encryption Policy Modified* is not in the list, wait a few minutes and click the Refresh icon in the menu bar.

3. Click the Full Disk Encryption Policy Modified event in the list to display its details.

Expected Results

- The change event is displayed in the Dashboard.