

Endpoint Security Utilities Reference

Novell® ZENworks® 11

Support Pack 1

August 08, 2011

www.novell.com



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 \(http://www.novell.com/info/exports/\)](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 © 2011 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 \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

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

Contents

About This Guide	7
Part I Device Scanner	9
1 Overview	11
1.1 Supported ZENworks Endpoint Security Management Versions	11
1.2 Device Scanner Application	11
1.3 Device Scanner CLI	13
1.4 Scan Files	13
1.5 ZENworks 11 Import Files	13
1.6 ZENworks 3.5/4.1 Import Files	14
2 Installing the Device Scanner	15
2.1 Supported Windows Operating Systems	15
2.2 Downloading the Device Scanner	15
2.3 Installing the Device Scanner Application	15
2.4 Distributing the Device Scanner CLI	16
3 Scanning Devices	17
3.1 Initiating a Scan	17
3.2 Updating a Scan	18
4 Modifying Device Data	19
4.1 Reasons to Modify Device Data	19
4.2 Editing Data	19
4.3 Deleting Data	20
4.3.1 Deleting a Device	20
4.3.2 Deleting All Devices	20
4.3.3 Deleting Data from a Cell	21
4.4 Adding a New Device	21
5 Saving, Opening, and Merging Scan Files	23
5.1 Saving Data to a Scan File	23
5.2 Opening a Scan File	24
5.3 Merging Scan Files	24
6 Finding Data	27
7 Importing Device Data to Security Policies	29
7.1 Importing to ZENworks 11 Security Policies	29
7.2 Importing to ZENworks 3.5/4.1 Security Policies	29

8	Using the Device Scanner CLI	31
8.1	Distributing the Device Scanner CLI	31
8.2	Initiating a Scan	31
8.2.1	Usage	31
8.2.2	Examples	32
9	Field Descriptions	33
9.1	USB Devices List	33
9.2	Removable Drives List	35
	Part II File Decryption Utility	37
10	Overview	39
11	Installing the User Version of the Utility	41
11.1	Installing the Utility through the Endpoint Security Agent	41
11.2	Installing the Utility via a Data Encryption Policy	41
11.3	Installing the Utility from a ZENworks Server	42
12	Installing the Administrator Version of the Utility	43
13	Encrypting Files	45
13.1	Encrypting a Single File	45
13.2	Encrypting Multiple Files	46
14	Decrypting Files	47
14.1	Decrypting a Single File	47
14.2	Decrypting Multiple Files	48
15	Recovering Key-Encrypted Files	49
15.1	Exporting the Encryption Keys	49
15.2	Loading the Encryption Keys	49
15.3	Decrypting Files	49
	Part III Override Password Key Generator	51
16	Overview	53
16.1	The Override Password	53
16.2	Override Password Key Generator	54
17	Generating an Override Password Key	55
18	Applying an Override Password Key	57

About This Guide

This guide provides information about the following Novell ZENworks 11 SP1 Endpoint Security Management utilities:

- ♦ [Part I, “Device Scanner,” on page 9](#)
- ♦ [Part II, “File Decryption Utility,” on page 37](#)
- ♦ [Part III, “Override Password Key Generator,” on page 51](#)

Audience

This guide is written for ZENworks Endpoint Security Management 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 Endpoint Security 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 SP1 documentation Web site \(http://www.novell.com/documentation/zenworks11\)](http://www.novell.com/documentation/zenworks11).

Device Scanner

The Device Scanner collects data about USB devices for use in USB Connectivity and Storage Device Control policies.

- ♦ [Chapter 1, “Overview,” on page 11](#)
- ♦ [Chapter 2, “Installing the Device Scanner,” on page 15](#)
- ♦ [Chapter 3, “Scanning Devices,” on page 17](#)
- ♦ [Chapter 4, “Modifying Device Data,” on page 19](#)
- ♦ [Chapter 5, “Saving, Opening, and Merging Scan Files,” on page 23](#)
- ♦ [Chapter 6, “Finding Data,” on page 27](#)
- ♦ [Chapter 7, “Importing Device Data to Security Policies,” on page 29](#)
- ♦ [Chapter 8, “Using the Device Scanner CLI,” on page 31](#)
- ♦ [Chapter 9, “Field Descriptions,” on page 33](#)

Overview

1

The Device Scanner collects data about USB devices connected to computers. This includes removable storage devices, printers, mice, keyboards, and other types of USB devices.

After you collect device data, you can review the data and make modifications as necessary. The device data can then be imported into Storage Device Control policies and USB Connectivity policies. The following sections provide an overview of the Device Scanner:

- ♦ [Section 1.1, “Supported ZENworks Endpoint Security Management Versions,” on page 11](#)
- ♦ [Section 1.2, “Device Scanner Application,” on page 11](#)
- ♦ [Section 1.3, “Device Scanner CLI,” on page 13](#)
- ♦ [Section 1.4, “Scan Files,” on page 13](#)
- ♦ [Section 1.5, “ZENworks 11 Import Files,” on page 13](#)
- ♦ [Section 1.6, “ZENworks 3.5/4.1 Import Files,” on page 14](#)

1.1 Supported ZENworks Endpoint Security Management Versions

You can use the Device Scanner with the following ZENworks Endpoint Security Management versions:

Version	Storage Control Device Policy	USB Connectivity Policy
Version 11	Yes	Yes
Version 4.1 or later	Yes	No
Version 3.5 IR8 or later	Yes	No

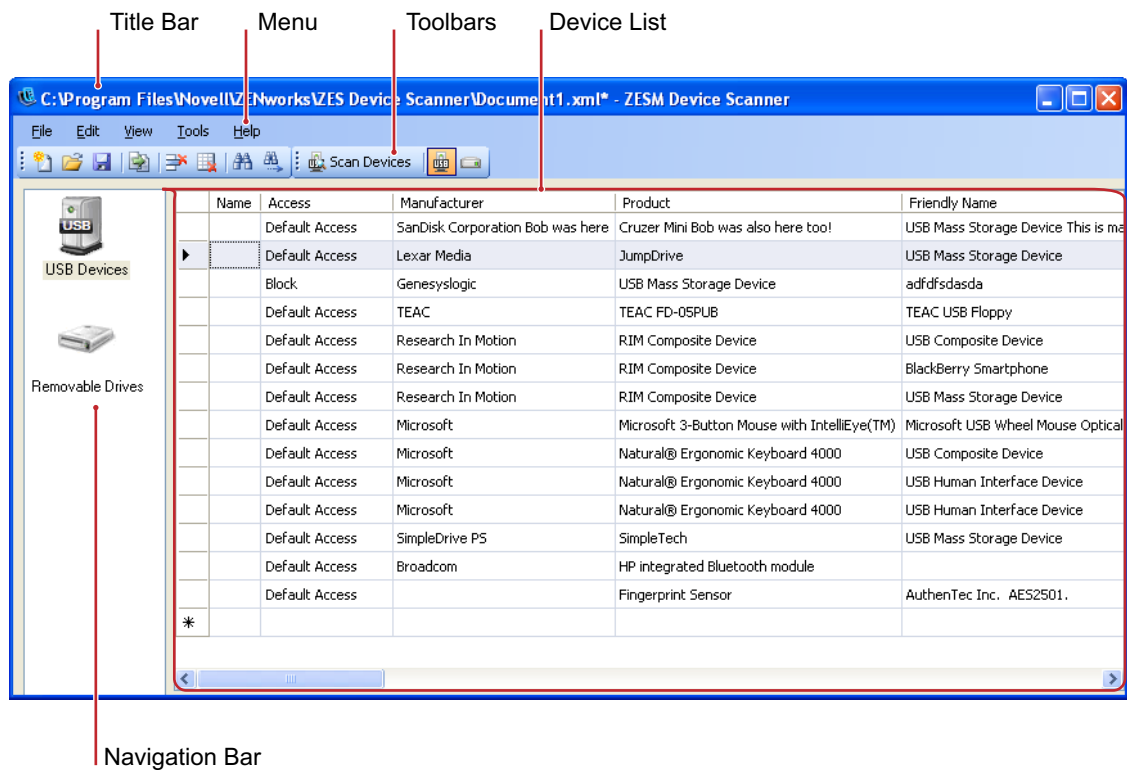
Both the Storage Control Device policy and the USB Connectivity policy in all three versions contain device lists.

In versions 3.5 and 4.1, you can only import devices into the Storage Control Device policy. The USB Connectivity policy does not support device data import.

In version 11, you can import devices into both policies.

1.2 Device Scanner Application

The Device Scanner application (referred to simply as the Device Scanner) is a graphical user interface through which you scan devices, manipulate the scan data, and save the data.



Typically, you should restrict use of the Device Scanner application to the administrators who are responsible for collecting device data and preparing it for import into security policies. If you want users to scan their devices, we recommend that you give them the Device Scanner [command line interface \(CLI\)](#).

Device List

The Device List displays a row for each detected device. The device data can come from a new scan, from a scan file, or from a combination of both.

There are two different lists that you can view:

- ♦ **USB Devices:** Displays all classes of USB devices, such as removable storage devices, keyboards, and printers. The list includes all device properties that are used when defining USB devices in a USB Connectivity policy.
- ♦ **Removable Drives:** Displays only the USB devices that are removable storage devices. This list is a subset of the devices displayed in the USB Devices list. It includes all device properties that are used when defining removable drives in a Storage Device Control policy.

The Device List is your workspace. Use the options available on the toolbars and menu to scan devices, view the scan data, and modify the data as needed to prepare it for use in security policies.

Navigation Bar

The Navigation bar lets you switch between the *USB Devices* list and the *Removable Drives* list.

Menu and Toolbars

The menu provides access to all Device Scanner options. The two toolbars provide quick access to the commonly used menu options:

- ♦ **Standard toolbar:** Provides standard options such as *New Document*, *Open Document*, *Save Document*, *Merge*, and *Find*.
- ♦ **Device toolbar:** Provides options to scan devices and toggle between the *USB Devices* list and *Removable Drives* list.

You can use the *View* menu to display or hide the toolbars.

Title Bar

The title bar displays the name of the scan file that is currently open in the Device List. An asterisk (*) next to the filename indicates that the file is a new file with unsaved data.

If you have just launched the Device Scanner or started a new file, a number (Document1, Document2, Document3, and so forth) is displayed. The number increments each time you open a new (clean) file during the current Device Scanner session.

1.3 Device Scanner CLI

The Device Scanner CLI (command line interface) provides scanning capabilities only. Unlike the [Device Scanner application](#), the CLI cannot be used to view or modify scan data.

Users typically do not need access to the data editing features provided by the Device Scanner application. Therefore, the CLI provides an easy way for users to scan their devices and return the resulting files to you (or another administrator).

For example, you could distribute a batch file that runs the CLI and saves the scan file to a shared network directory. You, or another administrator, could then retrieve the scan file, open it in the Device Scanner application, modify it as needed, and merge it with other scan data.

Unlike the Device Scanner application, which must be installed, the CLI is a single executable that you copy to the target computer.

1.4 Scan Files

The Device Scanner saves data to XML files called *scan files*.

You can use the Device Scanner application to modify the data in a scan file. Different scan files can be merged to reconcile device data and prepare it for use in security policies. For example, if you scan multiple computers, you can merge the scan files for each computer and remove duplicate or invalid device data.

1.5 ZENworks 11 Import Files

You can import the Device Scanner's .xml scan files directly into ZENworks Control Center in ZENworks 11 Endpoint Security Management.

You can import device data to both the Storage Device Control policy and the USB Connectivity policy. The Storage Device Control policy uses only a subset of the device data required by the USB Connectivity policy. This is why the Device Scanner provides both the *USB Devices* list and the *Removable Drives* list to view the data.

If you plan to import the device data into a Storage Device Control policy, you should ensure that the device data displayed in the *Removable Drives* list is accurate and complete. Likewise, if you plan to import the device data into a USB Connectivity policy, you should ensure that the device data displayed in the *USB Devices* list is accurate and complete.

1.6 ZENworks 3.5/4.1 Import Files

The Management Console in ZENworks Endpoint Security Management 4.1 requires import files to be formatted as `.suf` files. The Device Scanner lets you save `.xml` scan files in `.suf` import file format.

A `.suf` import file cannot be opened in the Device Scanner, so you should keep the original `.xml` scan file in case you need to modify the data again.

The Storage Device Control policy is the only 3.5/4.1 policy to which you can import device data. The Storage Device Control policy uses the removable drives data stored in a `.suf` file to add the removable drives to the Preferred Devices list. The imported removable drives receive whatever access level is defined for the Preferred Devices list.

Installing the Device Scanner

2

The Device Scanner application or CLI must reside on the computer hosting the USB devices you want to scan.

- ♦ [Section 2.1, “Supported Windows Operating Systems,” on page 15](#)
- ♦ [Section 2.2, “Downloading the Device Scanner,” on page 15](#)
- ♦ [Section 2.3, “Installing the Device Scanner Application,” on page 15](#)
- ♦ [Section 2.4, “Distributing the Device Scanner CLI,” on page 16](#)

2.1 Supported Windows Operating Systems

The Device Scanner runs on the following Microsoft Windows operating systems:

- ♦ Windows XP Service Pack 1(or later)
- ♦ Windows Vista (any release)
- ♦ Windows 7 (any release)
- ♦ Windows Server 2003 (any release)
- ♦ Windows Server 2008 (any release)

The operating system must have .NET 2.0 Framework installed. The Device Scanner installation program checks for .NET 2.0 Framework and prompts you if it is not installed.

2.2 Downloading the Device Scanner

The Device Scanner installation program is included on the ZENworks Server. You can access the installation program in the following ways:

- ♦ On the ZENworks Server, locate the `ZESMDeviceScannerUtilitySetup.exe` file in the following directory:
`\Novell\ZENworks\install\downloads\tools`
- ♦ In ZENworks Control Center, click *Home*. Under the *Common Tasks* list (in the left navigation pane), click *Download ZENworks Tools* to display the download page. Click *Administrative Tools*, then click *ZESMDeviceScannerUtilitySetup.exe* to download the installation program.
- ♦ In a Web browser, enter the following URL to display the download page:

`https://ZENworks_Server_address/zenworks-setup`

Click *Administrative Tools*, then click *ZESMDeviceScannerUtilitySetup.exe* to download the installation program.

2.3 Installing the Device Scanner Application

The Device Scanner application provides a graphical user interface that enables you to scan, view, modify, and save device data.

We recommend the following approach to installing the Device Scanner:

- ♦ Install the Device Scanner application on your computer and the computers of any administrators who are responsible for collecting device data and preparing it for import into Management Console security policies. These are the individuals who need access to the data editing features available in the application.
- ♦ Use the administrators' computers to scan USB devices by using either the Device Scanner application or the Device Scanner CLI. For example, connect one set of USB devices, scan them, then connect another set.
- ♦ If you don't have access to all of the USB devices that need to be scanned, distribute the Device Scanner CLI to users and have them use it to scan the devices (see [Section 2.4, "Distributing the Device Scanner CLI,"](#) on page 16).

You must use the Device Scanner installation program (ZESMDeviceScannerUtilitySetup.exe) to install the Device Scanner application to each computer where you want to run the application. You cannot install the Device Scanner application to one computer and then copy it to another; the application does not run if you do so.

To install the Device Scanner application:

- 1 Distribute the installation program (ZESMDeviceScannerUtilitySetup.exe) to the target computer.
- 2 Double-click ZESMDeviceScannerUtilitySetup.exe to launch the installation program.
- 3 Select the language version to install.
- 4 Follow the prompts to complete the installation.

The Device Scanner executable (ZESScan.exe) and support files are installed to the following directory:

```
c:\Program Files\Novell\ZENworks\ZES Device Scanner
```

A Device Scanner shortcut is added to the *Start* menu in the following location:

```
Start > Programs > Novell > ZENworks > ZES Device Scanner
```

For information about using the Device Scanner application to scan devices, see [Chapter 3, "Scanning Devices,"](#) on page 17.

For information about working with device data after you scan devices, see [Chapter 4, "Modifying Device Data,"](#) on page 19.

2.4 Distributing the Device Scanner CLI

The Device Scanner CLI (ZESScanCLI.exe) is installed at the same time and in the same location as the Device Scanner application. By default, this location is:

```
c:\Program Files\Novell\ZENworks\ZES Device Scanner\ZESScanCLI.exe
```

To use the Device Scanner CLI on another computer, you must copy the executable to the computer; do not use the installation program unless you want to also install the Device Scanner application. For information about using the Device Scanner CLI to scan devices, see [Chapter 8, "Using the Device Scanner CLI,"](#) on page 31.

Scanning Devices

3

The Device Scanner collects data for all USB devices (storage devices, mice, keyboards, printers, and so forth) that are connected to the computer.

The following sections provide instructions for using the Device Scanner application to scan devices. For information about scanning devices with the Device Scanner CLI, see [Chapter 8](#), “Using the Device Scanner CLI,” on page 31

- ♦ [Section 3.1, “Initiating a Scan,” on page 17](#)
- ♦ [Section 3.2, “Updating a Scan,” on page 18](#)

3.1 Initiating a Scan

- 1 Make sure that all USB devices you want to scan are connected to the computer.

Some devices, such as the Compaq iPAQ and Palm OS devices, must be powered on in order to be detected. If you perform a scan and a device is not detected, turn on the device and scan again.

If you have more USB devices to scan than your computer has USB ports, you can connect one set of devices, scan them, replace them with new devices, and scan the new devices. Scans are additive, meaning that the device data from each scan is added to any device data that is already in the Device List. You can also add a device to the list manually instead of scanning it. See [Section 4.4, “Adding a New Device,” on page 21](#) for more information.

- 2 Click the *Start* menu > *Programs* > *Novell* > *ZENworks* > *ZES Device Scanner* > *ZES Device Scanner* to launch the scanner.

or

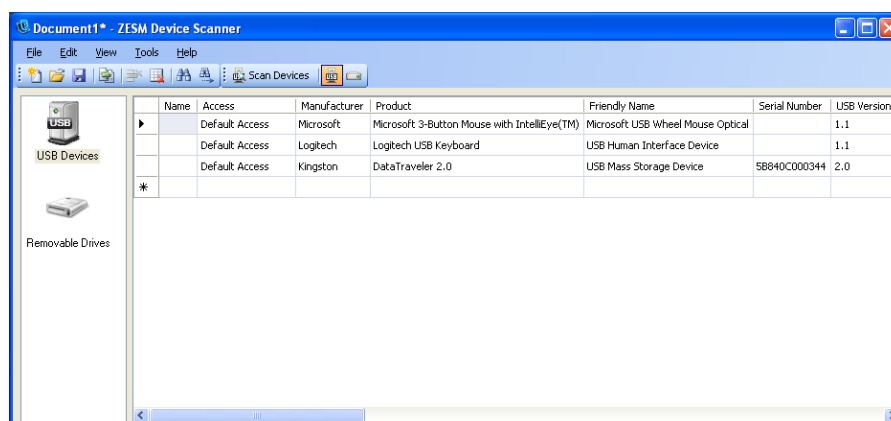
Double-click `ZESScan.exe` located in the `c:\Program Files\Novell\ZENworks\ZES Device Scanner` directory.

- 3 Click *Tools* > *Scan Devices*.

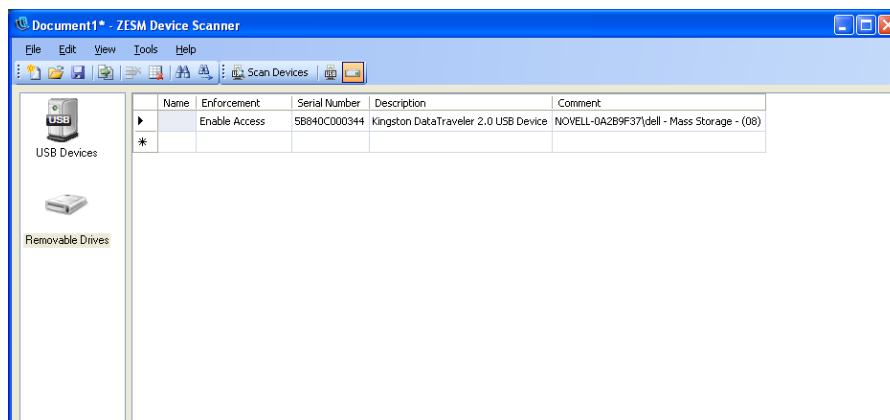
or

Click *Scan Devices* on the toolbar.

When the scan is complete, all detected USB devices are displayed in the *USB Devices* list.



USB devices that are removable storage devices are also displayed in *Removable Drives* list. To qualify as a removable storage device, a USB device must be a mass storage device and have a serial number.



4 Modify the device data as needed or save the file.

After you perform a scan, you must save the data to a scan file before exiting the Device Scanner, or the data is lost. Likewise, when you modify a file, the changes are not saved until you save the file. For information about modifying or saving the data, refer to the following sections:

- ♦ [Chapter 4, “Modifying Device Data,” on page 19](#)
- ♦ [Chapter 5, “Saving, Opening, and Merging Scan Files,” on page 23](#)

3.2 Updating a Scan

The Device Scanner does not perform real-time updates. For example, if you add a USB device to the computer after you perform a scan, the Device Scanner does not automatically detect it and update the scan data. To update a scan, you need to initiate a new scan.

Scans are additive, meaning that if you have data in the Device List, new devices are added to the scan data. However, old devices (those that are no longer present on the computer), are not removed; to remove a device from the list, you must manually [delete](#) it.

Modifying Device Data

4

The Device Scanner lets you add, change, and delete device data to prepare your devices for use in security policies.

- ♦ [Section 4.1, “Reasons to Modify Device Data,” on page 19](#)
- ♦ [Section 4.2, “Editing Data,” on page 19](#)
- ♦ [Section 4.3, “Deleting Data,” on page 20](#)
- ♦ [Section 4.4, “Adding a New Device,” on page 21](#)

4.1 Reasons to Modify Device Data

There are many reasons why you might need to modify your device data, including the following:

- ♦ **Add a name, access level, and enforcement level:** ZENworks 11 security policies require a name to be assigned to the device. You can add a name, or let ZENworks Control Center provide a name during the import. For the USB Connectivity policy, the default format provided by the ZENworks Control Center import is `USBDevice-dd-mm-yyyy hh-mm-ss-x`, where *x* is a sequentially incremented number for each device imported during a single second. For the Storage Device Control policy, the default format provided by the ZENworks Control Center import is `Storage_Device-dd-mm-yyyy hh-mm-ss-x`.

The USB Devices access level (USB Connectivity policy) defaults to *Default Access* and the Removable Drives enforcement level (Storage Device Control policy) defaults to *Enable Access*. You can change the levels as needed.

- ♦ **Create a generic device entry:** When a device is added to a security policy, it serves as a filter against which detected devices are compared. The device data, or fields, make up the filter. If a detected device matches the policy’s device filter, the device is either enabled or disabled according to the policy setting.

The more generic a device filter is, the more devices can match it. For example, assume that your organization allows all SanDisk USB 2.0 devices. Rather than scan each device, you could scan one device, modify the *Manufacturer* field to contain *SanDisk* only, the *Device Class* field to equal 8, and the *USB Version* field to equal 2.0, then delete all of the other fields. The result is a device filter that matches all SanDisk USB 2.0 devices.

- ♦ **Add a device entry:** If you need to add a device that is not available to scan, you can manually add the device data.

4.2 Editing Data

The Storage Device Control policy uses the device data as it is displayed in the *Removable Drives* list. The USB Connectivity policy (ZENworks 11 only) uses the device data as it is displayed in the *USB Devices* list.

If you plan to import the device data into a Storage Device Control policy, you should ensure that the device data displayed in the *Removable Drives* list is accurate and complete. Likewise, if you plan to import the device data into a USB Connectivity policy, you should ensure that the device data displayed in the *USB Devices* list is accurate and complete.

1 In the desired Device List, select the data cell you want to edit.

2 Click the cell to enter Edit mode.

In Edit mode, you can select or specify a value. In addition, you can right-click to access options such as *Undo*, *Cut*, *Copy*, and *Paste*.

3 If the cell provides a list, select a value from the list.

or

If the cell does not have a selection list or the list does not contain the desired value, specify the value.

For cells that include a selection list, if you decide to specify a new value, you must specify the value in the correct hexadecimal format. For example, if you specify a Vendor ID, you must use a four-character hexadecimal value. If you specify a Device Class, you must use a two-character hexadecimal value. You can refer to the other values in the list to see the correct format. If you use the incorrect format, you receive an error message that explains the correct format.

For descriptions of each of the cells, see [Appendix 9, “Field Descriptions,” on page 33](#).

4 Click another cell or press the *Tab* key to save the change.

4.3 Deleting Data

You can delete entire device rows or individual device data cells.

- ♦ [Section 4.3.1, “Deleting a Device,” on page 20](#)
- ♦ [Section 4.3.2, “Deleting All Devices,” on page 20](#)
- ♦ [Section 4.3.3, “Deleting Data from a Cell,” on page 21](#)


4.3.1 Deleting a Device

1 Display the list (*USB Devices* or *Removable Drives*) that contains the device you want to delete.

A removable storage device that is displayed in both lists is treated as two different devices. If you delete the removable storage device from one list, it remains in the other list.

2 Click the first cell of the device row, then click *Edit > Delete > Rows*.

or

Click the first cell of the device row, then click  on the toolbar.

You can Ctrl+click and Shift+click to select multiple device rows.


4.3.2 Deleting All Devices

1 Display the list (*USB Devices* or *Removable Drives*) that contains the devices you want to delete.

Removable storage devices that display in both lists are treated as different devices. If you delete a removable storage device from one list, it remains in the other list.

2 Click *Edit > Delete > All*.

or

Click  on the toolbar.

4.3.3 Deleting Data from a Cell

1 To delete the contents from a cell, double-click the cell, then do one of the following:

- ♦ Press the Delete key.
- ♦ Right-click, then select *Delete*.

4.4 Adding a New Device

The Device List provides a row that you can use to manually add a new device. The row, which is distinguished by an asterisk (*) in the first column, is always the last row in the Device List.

To add a device:

- 1 Select the list (*USB Devices* or *Removable Drives*) where you want to add the device.
- 2 In the new row (located at the bottom of the Device List), select a cell where you want to add a value, then click the cell to enter Edit mode.

In Edit mode, you can select or specify a value. In addition, you can right-click to access options such as *Undo*, *Cut*, *Copy*, and *Paste*.

- 3 If the cell provides a list, select a value from the list.

or

If the cell does not have a selection list or the list does not contain the desired value, specify the value.

For cells that include a selection list, if you decide to specify a new value, you must specify the value in the correct hexadecimal format. For example, if you specify a Vendor ID, you must use a four-character hexadecimal value. If you specify a Device Class, you must use a two-character hexadecimal value. You can refer to the other values in the list to see the correct format. If you use the incorrect format, you receive an error message that explains the correct format.

For descriptions of each of the cells, see [Appendix 9, “Field Descriptions,”](#) on page 33.

- 4 Click another cell or press the Tab key to save the change.
- 5 Continue until you have added all desired data for the device.

The Device Scanner does not require you to enter data in all fields. However, you should provide enough data to allow the device to be accurately identified.

Saving, Opening, and Merging Scan Files

5

The following sections provide instructions to help you save scan files, open scan files, and merge scan files:


- ♦ [Section 5.1, “Saving Data to a Scan File,” on page 23](#)
- ♦ [Section 5.2, “Opening a Scan File,” on page 24](#)
- ♦ [Section 5.3, “Merging Scan Files,” on page 24](#)

5.1 Saving Data to a Scan File

After you perform a scan, you must save the data to a scan file before exiting the Device Scanner, or the data is lost. Likewise, when you modify a file, the changes are not saved until you save the file.

The Device Scanner supports a variety of save options. You can save the entire Device List, the *USB Devices* list only, the *Removable Drives* list only, or selected data. If you modify data in an existing file, you can save it to the same file or to a new file.

To save data:

- 1 If you want to save selected data only, select the data.
You can select an entire row, an entire column, or a single cell. Ctrl+click and Shift+click to select multiple rows, columns, and cells.
- 2 Select the appropriate Save option:
 - ♦ *File > Save* (or 

Saving, Opening, and Merging Scan Files 23

- ♦ **Selection:** Saves only the currently selected data.

7 Click *Save*.

5.2 Opening a Scan File

When you open a scan file, the file replaces any data (saved or unsaved) that is already displayed in the Device List.

1 Click *File > Open*.

or

Click .

2 (Conditional) If the Device List contains unsaved data, you are prompted to save the data before continuing. Click *Yes* to save the data or click *No* to discard the data.

3 In the Open File dialog box, browse for and select the file you want to open.

4 Click *Open*.

5.3 Merging Scan Files

You can combine the contents of two or more scan files by merging the files. The merge results show any devices with invalid data; you can correct the invalid data or discard the device entry.

If two devices are duplicates, only one device entry is kept. To determine if two devices are duplicates, the merge compares all device properties except the Comment property and the OS properties (OS Device Class, OS Device ID, and OS Device Parent).


To merge files:

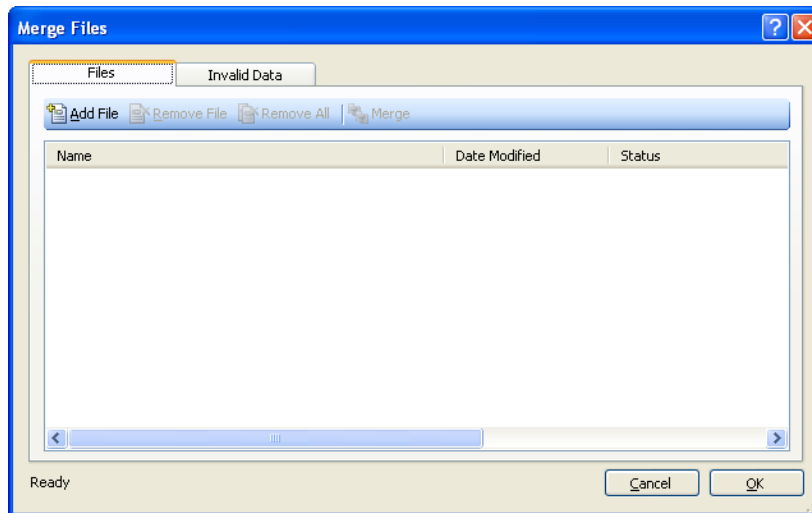
1 If the Device List includes devices you don't want included in the merge, clear the devices.

The merge includes any devices that are displayed in the Device List, either from a scan or from a scan file. If you don't want the Device List data included in the merge, discard the scan data or close the scan file.

2 Click *File > Merge* to display the Merge Files dialog box.

or

Click  on the toolbar.





3 On the *Files* tab, click *Add File*, select the files you want included in the merge, then click *Open* to add them to the list of files to be merged.

You can Shift+click and Ctrl+click to select multiple files.

4 Click *Merge* to merge the files.

The files are processed from top to bottom in the list. If the Device List includes devices, it is considered to be the first file and is processed before the files in the *Merge Files* list.

When the merge is finished, the status for each file is displayed:

- ◆  **Success:** No merge errors. All devices are included in the merge.
- ◆  **Invalid Data:** The file contains devices with data that is not valid. The devices are listed on the *Invalid Data* tab.

5 If invalid data was found, click the *Invalid Data* tab to display the devices.

The list includes each device from which invalid data was removed during the merge process. You can choose to merge the devices (minus the invalid data) or exclude the devices from the merge.

- ◆ **USB Devices:** Displays the *USB Devices* list.
- ◆ **Removable Drives:** Displays the *Removable Drives* list.
- ◆ **Merge:** Includes the devices in the merge. After the merge is complete, you can edit the device in the Device List to add valid data.

6 When you are finished, click *OK* to accept the merge and populate the Device List.

or

Click *Cancel > Yes* to discard the merge file.

Finding Data

6

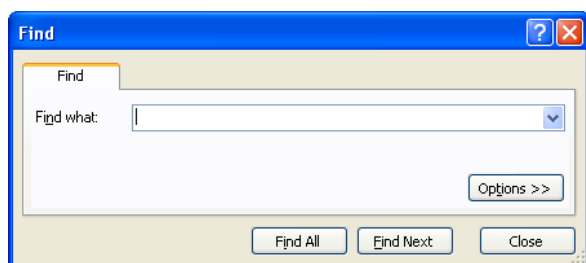
You can search the Device List to find specific data. For example, you can find USB Version entries equal to 2.0, or you can find all Manufacturer entries that contain SanDisk.

To find data:

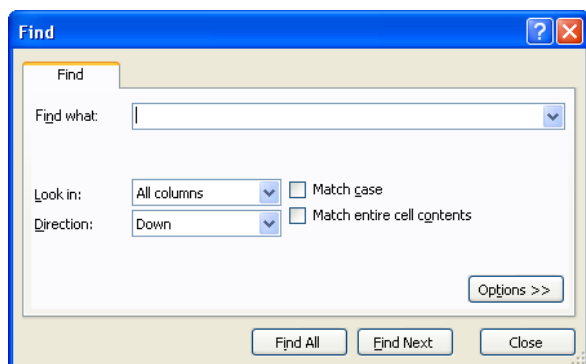
- 1 Display the list (*USB Devices* or *Removable Drives*) that contains the data you want to find.
- 2 Click *Edit > Find*.

or

Click .



- 3 In the *Find What* field, type the text you want to find.
You can enter a partial word, a complete word, or multiple words.
- 4 (Conditional) Click *Options* to display the advanced Find options, or skip to [Step 6](#).



- 5 Fill in the following fields:

Look in: Select the column to search. To search all columns, select *All columns*.

Direction: Select the search direction (*Up* or *Down*). The default is *Down*.

Match case: Select this option to find only occurrences that match the capitalization used in the *Find What* field. For example, if you specify *USB*, *Usb* and *usb* are not found.

Match entire cell contents: Select this option to require the cell contents to exactly match the text in the *Find What* field. The cell cannot contain more or less text than the *Find What* text. For example, if you specify *USB*, *USB1.1* and *USB Micro* are not matched. Capitalization is ignored unless you turn on the *Match case* option.

- 6 Click *Find Next* to find the next occurrence that matches the criteria.
or
Click *Find All* to find all matching occurrences.

Importing Device Data to Security Policies

7

The following sections provide instructions for importing device data to security policies:

- [Section 7.1, “Importing to ZENworks 11 Security Policies,” on page 29](#)
- [Section 7.2, “Importing to ZENworks 3.5/4.1 Security Policies,” on page 29](#)

7.1 Importing to ZENworks 11 Security Policies

- 1 Save the device data to a scan file.

You can save all device data to the scan file. Or, if you are importing data to a Storage Device Control policy, you can save only the *Removable Drives* list. Likewise, if you are importing data to a USB Connectivity policy, you can save only the *USB Devices* list. For instructions, see [Section 5.1, “Saving Data to a Scan File,” on page 23](#).

- 2 Use ZENworks Control Center to import the device data to the desired security policy. For instructions, see “Storage Device Control Policy” and “USB Connectivity Policy” in the *ZENworks 11 SP1 Endpoint Security Policies Reference*.

7.2 Importing to ZENworks 3.5/4.1 Security Policies

- 1 Save the device data to a .suf import file:

- 1a Retrieve the desired data into the Device List by performing a device scan or by opening an existing .xml scan file.
- 1b Click *File > Save As*.
- 1c In the *File name* field, type a name for the file.
- 1d In the *Save as type* field, select *3.5/4.1 Scan Files (*.suf)*.
- 1e Click *Save*.

- 2 Use the Management Console to import the .suf file into the desired Storage Device Control policy.

All imported devices receive the access level that is defined for the Preferred Devices list.

For import instructions, see [Storage Device Control \(http://www.novell.com/documentation/zesm41/zesm_admin/data/bbjlf89.html\)](http://www.novell.com/documentation/zesm41/zesm_admin/data/bbjlf89.html) in the *ZENworks Endpoint Security Management 4.1 Administration Guide*.

Using the Device Scanner CLI

8

The Device Scanner CLI (command line interface) provides scanning capabilities only; it cannot be used to view or modify scan data.

The following sections provide information about using the Device Scanner CLI:

- ♦ [Section 8.1, “Distributing the Device Scanner CLI,” on page 31](#)
- ♦ [Section 8.2, “Initiating a Scan,” on page 31](#)

8.1 Distributing the Device Scanner CLI

The Device Scanner CLI (`ZESScanCLI.exe`) is a different executable than the Device Scanner application (`ZESScan.exe`). When you run the Device Scanner installation program, the CLI executable is copied to the same location as the application executable. By default, this location is:

```
c:\Program Files\Novell\ZENworks\ZES Device Scanner\ZESScanCLI.exe
```

Copy the Device Scanner CLI executable (`ZESScanCLI.exe`) to the computer you want to scan. Do not use the Device Scanner installation program unless you also want to install the Device Scanner application on the computer.

IMPORTANT: The Device Scanner CLI requires .NET 2.0 Framework. If .NET 2.0 Framework is not installed on the computer being scanned, the CLI does not run.

8.2 Initiating a Scan

The Device Scanner CLI can be launched without any arguments, in which case it uses default settings to scan the device and save the scan file. If you want to customize the scan settings, you can distribute a batch or script file that starts the Device Scanner CLI executable with the desired arguments. The following sections explain the command line usage and provide examples:

- ♦ [Section 8.2.1, “Usage,” on page 31](#)
- ♦ [Section 8.2.2, “Examples,” on page 32](#)

8.2.1 Usage

```
zesscancli [/all] [/usb] [/rsd] [/c | /comment] [/f | /filename] [/s | /silent]
```

The arguments, which are optional, can be placed in any order. You can also substitute a dash (-) for the forward slash (/). For example, `/all` or `-all`.

/all: Scans all device types. Stores the results in USB Devices format and Removable Drives format in the scan file. This is equivalent to populating the *USB Devices* and *Removable Drives* lists in the Device Scanner application.

/usb: Scans USB devices. Stores the results, including removable storage devices, in USB Devices format only. This is equivalent to populating only the *USB Devices* list in the Device Scanner application.

/rsd: Scans removable drives. Stores the results in *Removable Drives* format only. This is equivalent to populating only the *Removable Drives* list in the Device Scanner application.

/c or /comment: Adds a comment to each scanned device. If no comment is specified, the default is *computer\user - device class* for USB devices and *computer\user* for removable drives.

/f or /filename: Saves the scan file with the specified path and filename. You can use any combination of path and filename:

- ♦ Filename only: Saves the file, with the specified filename, to the default directory.
- ♦ Path and filename: Saves the file, with the specified filename, to the specified directory.
- ♦ Path only: Saves the file, with the default filename, to the specified directory. You must append a backslash to the final directory in the path (for example, *c:\scanfiles*).

The default filename is *zesscan-machine_name-MMddyyyyHHmmssffff.xml* and the default path is the Device Scanner CLI executable directory.

/s or /silent: Suppresses error messages.

8.2.2 Examples

Example 1: `zesscancli`

This scan uses the default settings. All devices are scanned. A default comment (*computer\user - device class* for USB devices and *computer\user* for removable drives) is added to each device. The scan data is saved with the default filename (*zesscan-machine_name-MMddyyyyHHmmssffff.xml*) in the `zesscancli` executable directory.

Example 2: `zesscancli /usb /f myscan.xml`

Scans all USB devices and saves the data in USB device format to the `myscan.xml` file in the `zesscancli` executable directory.

Example 3: `zesscancli -rsd -c "removable drive"`

Scans all removable storage devices, adds `removable drive` as a comment on all devices, and saves the data with the default filename in the `zesscancli` executable directory.

Example 4: `zesscancli /filename s:\scans\ /silent`

Scans all devices, suppresses any scanning error messages, and saves the data to the default filename in the `s:\scans` directory.

Field Descriptions

9

The following sections provide descriptions of the fields in the *USB Devices* list and the *Removable Drives* list.

- ♦ [Section 9.1, “USB Devices List,” on page 33](#)
- ♦ [Section 9.2, “Removable Drives List,” on page 35](#)

9.1 USB Devices List

The *USB Devices* list is used for providing device definitions (or filters) for the USB Connectivity policy in ZENworks 11. Devices cannot be imported into the USB Connectivity policy in ZENworks 3.5 or 4.1

The more generic a device filter is, the more devices can match it. For example, assume that your organization allows all SanDisk USB 2.0 devices. Rather than scan each device, you could scan one device, modify the *Manufacturer* field to contain *SanDisk* only, the *Device Class* field to equal 8, and the *USB Version* field to equal 2.0, then delete all of the other fields. The result is a device filter that matches all SanDisk USB 2.0 devices.

Name

Specify a display name to be used for the device when it is added as an object in ZENworks Control Center. The name is for display purposes only; it is not part of the device filter used to match detected devices.

Access

Select the access level to assign to the device:

- ♦ **Always Block:** Always block the device. This setting cannot be overridden.
- ♦ **Always Allow:** Always allow access unless the device also matches an *Always Block* filter.
- ♦ **Block:** Block access unless the device also matches an *Always Allow* filter.
- ♦ **Allow:** Allow access unless the device also matches an *Always Block* filter or a *Block* filter.
- ♦ **Default Access:** Give the device the default access defined in the USB Connectivity policy to which the device data is imported.

Manufacturer

Specify the name of the manufacturer, such as Canon. This is a substring match field, meaning that both *C* and *Can* would match *Canon*. The more generic the string, the more devices that can match it. For example, *Canon* matches more devices than *Canon imageCLASS 2200 PCL 5e*.

Product

Specify the name of the product. This is a substring match field, meaning that both *D* and *Data* would match *DataTraveler*. The more generic the string, the more devices that can match it. For example, *DataTraveler* matches more devices than *DataTraveler 2.0*.

Friendly Name

Specify the friendly name of the device. This is a substring match field, meaning that both *W* and *Wheel* would match *Optical Wheel Mouse*. The more generic the string, the more devices that can match it. For example, *Mouse* matches more devices than *Optical Wheel Mouse*.

Serial Number

Specify the serial number of the device. Be aware that not all USB devices have unique serial numbers. To guarantee a unique match based on a serial number, you must also use the *USB Version*, *Vendor ID*, *Production ID*, and *BCD Device* fields. *Serial Number* is an exact match field.

USB Version

Select a version from the list, or specify a new version in *XX.XX* hexadecimal format (for example, 1.1 or 01.10).

Device Class

Select a class from the list, or specify a new device class in *XX* hexadecimal format.

Device Sub Class

Select a subclass from the list, or specify a new subclass in *XX* hexadecimal format.

Device Protocol

Select a device protocol from the list, or specify a new protocol in *XX* hexadecimal format.

Vendor ID

Select a vendor ID from the list, or specify a new vendor ID in *XXXX* hexadecimal format.

Product ID

Select a product ID from the list, or specify a new product ID in *XXXX* hexadecimal format.

Product Version

Select a product version from the list, or specify a new version in *XX.XX* hexadecimal format.

OS Device Class

Select an OS device class from the list, or specify a new class in {XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX} hexadecimal format.

OS Device ID

Specify an OS Device ID.

Comment

Specify a comment. This field is not used to match devices, so it can include any text you want.

9.2 Removable Drives List

The *Removable Drives* list is used for providing device definitions (or filters) for the Storage Device Control policy.

Name

This field is only used with ZENworks 11 security policies. Specify a display name to be used for the device when it is added as an object in ZENworks Control Center. The name is for display purposes only; it is not part of the device filter used to match detected devices.

Enforcement

This field is only used with ZENworks 11 security policies. Select the enforcement level to assign to the device:

- ♦ **Enable Access:** Read and write access is allowed.
- ♦ **Disable Access:** All access is prevented. When users attempt to access files on the device, they receive an error message from the operating system or from the application attempting to access the local storage device, indicating that the action has failed
- ♦ **Read-Only Access:** Read-only access is allowed. When users attempt to write to the device, they receive an error message from the operating system or from the application attempting to access the local storage device, indicating that the action has failed
- ♦ **Default Access:** Give the device the default access defined in the Storage Device Control policy to which the device data is imported.

Serial Number

Specify the serial number of the device. This is an exact match field. Serial numbers are unique to specific removable storage devices. If you want to match specific devices, use this field.

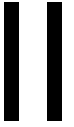
Description

Specify a description for the device. This is a substring match field. If you want to match multiple devices, use this field without using the *Serial Number* field. For example, to match all SanDisk USB drives, specify *SanDisk*.

Comment:

Specify a comment. This field is not used to match devices, so it can include any text you want.

File Decryption Utility



The ZENworks File Decryption utility enables users to password-encrypt files. It also enables ZENworks administrators to recover encrypted files from fixed disks and removable storage devices if the Endpoint Security Agent is removed before the files are decrypted.

- ♦ [Chapter 10, “Overview,” on page 39](#)
- ♦ [Chapter 11, “Installing the User Version of the Utility,” on page 41](#)
- ♦ [Chapter 12, “Installing the Administrator Version of the Utility,” on page 43](#)
- ♦ [Chapter 13, “Encrypting Files,” on page 45](#)
- ♦ [Chapter 14, “Decrypting Files,” on page 47](#)
- ♦ [Chapter 15, “Recovering Key-Encrypted Files,” on page 49](#)

The ZENworks File Decryption utility provides both encryption and decryption of files. There are two versions of the utility:

- ♦ **User Version:** The User version, `ZESDecrypt.exe`, is intended for end-users. It enables users to encrypt files using a password. It also enables users to decrypt password-encrypted files created with either the File Decryption utility or the Endpoints Security Agent.
- ♦ **Administrator Version:** The Administrator version, `ZESDecryptAdmin.exe`, provides the same functionality as the User version plus the ability to recover key-encrypted files from devices where the Endpoint Security Agent has been removed and from removable storage devices.

Installing the User Version of the Utility

11

By default, the File Decryption utility is not installed on managed devices or on encrypted removable storage devices.

The following sections provide information about the methods that can be used to install the User version of the utility.


- ♦ [Section 11.1, “Installing the Utility through the Endpoint Security Agent,” on page 41](#)
- ♦ [Section 11.2, “Installing the Utility via a Data Encryption Policy,” on page 41](#)
- ♦ [Section 11.3, “Installing the Utility from a ZENworks Server,” on page 42](#)

11.1 Installing the Utility through the Endpoint Security Agent

You, or your users, can use the Endpoint Security Agent to install the File Decryption utility on encrypted removable storage devices. This ensures that the utility is always available to decrypt any password-protected files on the device.

- 1 At the Windows device, plug in the removable storage devices on which you want to install the utility.

The utility will be installed on any USB removable storage device that is plugged in to the Windows device. Make sure to unplug any USB removable storage devices on which you do not want to install the utility.

- 2 On the Windows device, right-click the  icon in the notification area, then click *Show Properties*.
- 3 Click *Endpoint Security* to display the Endpoint Security properties page.
- 4 Under *Endpoint Security Agent Actions*, click *Encryption* to display the Encryption dialog box.
- 5 Click *Copy Decrypt Tool*.

The utility is copied to the `Novell Decrypt Tool` folder on the removable storage device.

11.2 Installing the Utility via a Data Encryption Policy

You can configure the Data Encryption policy to automatically install the File Decryption utility on encrypted removable storage devices. With this policy setting in place, the Endpoint Security Agent installs the utility in an `Novell Decrypt Tool` folder when the removable storage device is first encrypted.

You enable this policy setting by turning on the *Copy standalone decryption tool to removable storage devices* option in the Data Encryption policy.

☒ Enable encryption for removable storage devices

☒ Enable encryption via user-defined password

Folder name: *

☐ Require strong password

☐ Copy standalone decryption tool to removable storage devices

For information about creating or modifying a Data Encryption policy, see the *ZENworks 11 SP1 Endpoint Security Policies Reference*.

11.3 Installing the Utility from a ZENworks Server

The installation program for the File Decryption utility is included on the ZENworks Server. You can download and install the utility on any device you want to use to decrypt files

- 1 Download the utility from a ZENworks Server, using one of the following methods:
 - ♦ On the ZENworks Server, locate the `ZESMStandAloneDecrypt.exe` file in the following directory:


```
\Novell\ZENworks\install\downloads\tools
```
 - ♦ In the ZENworks Control Center, click *Home*. Under the *Common Tasks* list (in the left navigation pane), click *Download ZENworks Tools* to display the download page. Click *Administrative Tools*, then click *ZESMStandAloneDecrypt.exe* to download the installation program.
 - ♦ In a Web browser, enter the following URL to display the download page:

`https://ZENworks_Server_address/zenworks-setup`

Click *Administrative Tools*, then click *ZESMStandAloneDecrypt.exe* to download the installation program.

- 2 Copy the `ZESMStandAloneDecrypt.exe` file to the device where you want to install it.
- 3 Double-click the executable to launch the installation program.
- 4 Follow the prompts to install the utility.

Installing the Administrator Version of the Utility

12

The installation program for the Administrator version of the File Decryption utility is included on the ZENworks Server. You can download and install the utility on any device you want to use to decrypt files.

1 Download the utility from a ZENworks Server, using one of the following methods:

- ♦ On the ZENworks Server, locate the `ZESMStandAloneDecryptAdmin.exe` file in the following directory:
`\Novell\ZENworks\install\downloads\tools`
- ♦ In the ZENworks Control Center, click *Home*. Under the *Common Tasks* list (in the left navigation pane), click *Download ZENworks Tools* to display the download page. Click *Administrative Tools*, then click *ZESMStandAloneDecryptAdmin.exe* to download the installation program.
- ♦ In a Web browser, enter the following URL to display the download page:

`https://ZENworks_Server_address/zenworks-setup`

Click *Administrative Tools*, then click *ZESMStandAloneDecryptAdmin.exe* to download the installation program.

- 2** Copy the `ZESMStandAloneDecryptAdmin.exe` file to the device where you want to install it.
- 3** Double-click the executable to launch the installation program.
- 4** Follow the prompts to install the utility.

Encrypting Files

13

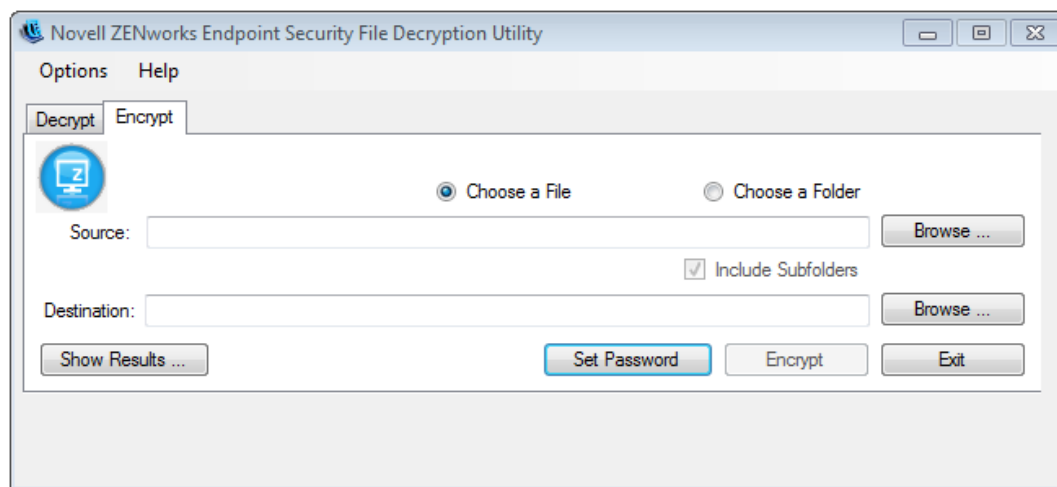
This functionality is available in both the User version (ZESDecrypte.exe) and the Administrator version (ZESDecryptAdmin.exe) of the File Decryption utility.

The File Decryption utility, like the Endpoint Security Agent, provides password-encryption of files. During encryption, a password must be provided that is then required to decrypt the file.

- ♦ [Section 13.1, “Encrypting a Single File,” on page 45](#)
- ♦ [Section 13.2, “Encrypting Multiple Files,” on page 46](#)

13.1 Encrypting a Single File

- 1 Launch the File Decryption utility (ZESDecrypt.exe).

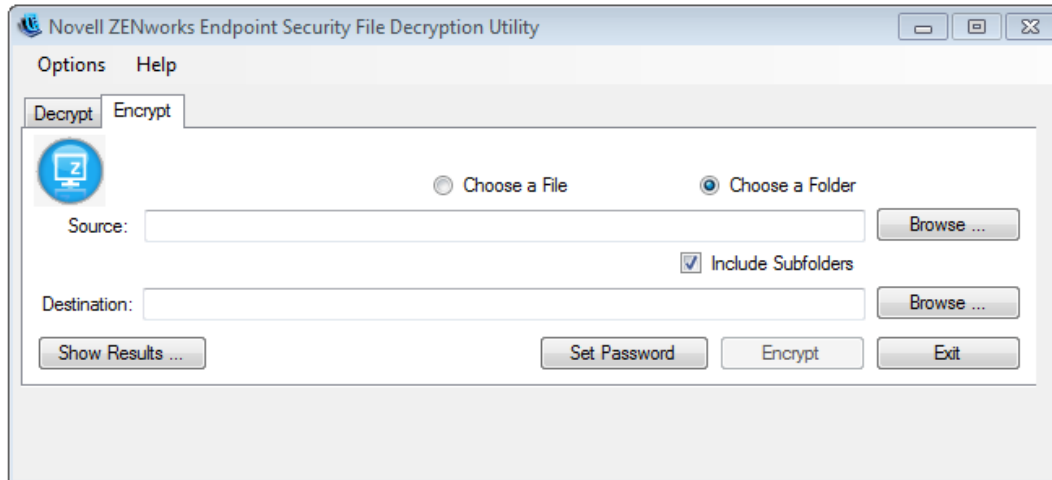


- 2 Click the *Encrypt* tab.
- 3 Make sure the *Choose a File* option is selected.
- 4 In the *Source* field, click *Browse*, select the desired file, then click *Open*.
- 5 In the *Destination* field, click *Browse*, select the location for the decrypted file, then click *OK*.
When you select the destination, no filename is included. By default, the utility uses the source filename as the destination file. If you want a different destination filename, you can add it to the destination path.
- 6 Click *Set Password*, specify the encryption password, provide a password hint (optional), then click *OK*.
- 7 Click *Encrypt*.
- 8 Click *Show Results* to view the encryption results.

13.2 Encrypting Multiple Files

You decrypt multiple files by selecting a folder rather than an individual file.

- 1 Launch the File Decryption utility (ZESDecrypt.exe).



- 2 Select the *Choose a Folder* option.
- 3 In the *Source* field, click *Browse*, select the desired folder, then click *Open*.
- 4 If the folder includes subfolders with files you want to encrypt, select *Include Subfolders*.
- 5 In the *Destination* field, click *Browse*, select a folder in which to place the encrypted files, then click *OK*.

If you included subfolders when selecting the source, the encryption process preserves the subfolder structure under the destination folder.

- 6 If desired, click the *Options* menu to change what happens to the original files after they are encrypted and how file conflicts are resolved.

Select options: By default, the original, unencrypted file is retained after the encrypted copy is created. Select *Delete Original File after Copy* if you want the utility to delete the original file from the source folder after copying the encrypted file to the destination folder.

File conflict options: By default, you are prompted if a file has the same name as a file in the destination folder. Select *Skip if Replacing* if you want the utility to automatically skip the file without prompting you. Select *Always Replace* if you want the utility to automatically overwrite the existing file without prompting you.

- 7 Click *Set Password*, specify the encryption password, provide a password hint (optional), then click *OK*.
- 8 Click *Encrypt*.
- 9 Click *Show Results* to monitor the encryption progress.

Decrypting Files

14

This functionality is available in both the User version (ZESDecrypte.exe) and the Administrator version (ZESDecryptAdmin.exe) of the File Decryption utility.

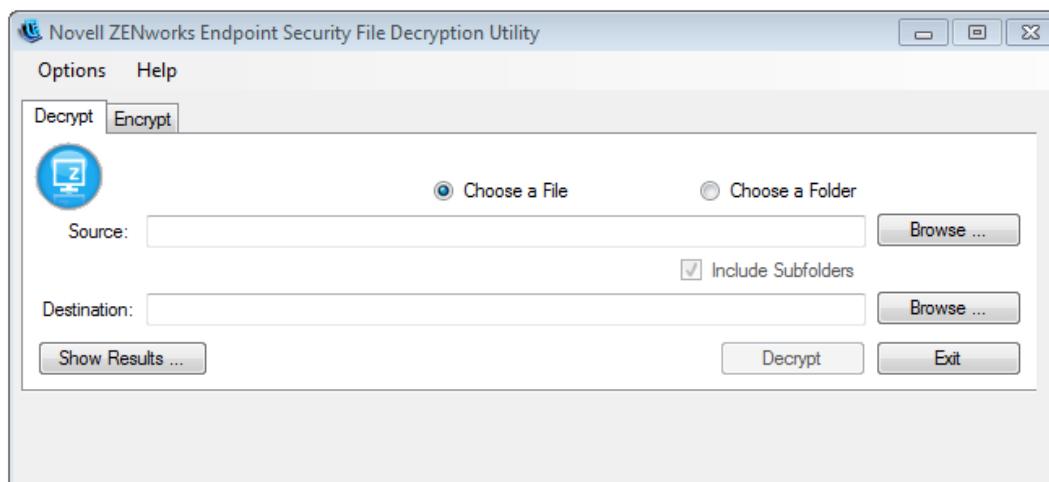
The File Decryption utility provides decryption of password-encrypted files. You can decrypt files that were password-encrypted with either the File Decryption utility or the Endpoint Security Agent.

To decrypt a password-protected file you must know the location of the file on the removable storage device and the password used to encrypt it.

- ♦ [Section 14.1, “Decrypting a Single File,” on page 47](#)
- ♦ [Section 14.2, “Decrypting Multiple Files,” on page 48](#)

14.1 Decrypting a Single File

- 1 Plug the removable storage device into your computer.
- 2 Launch the File Decryption utility (ZESDecrypt.exe).

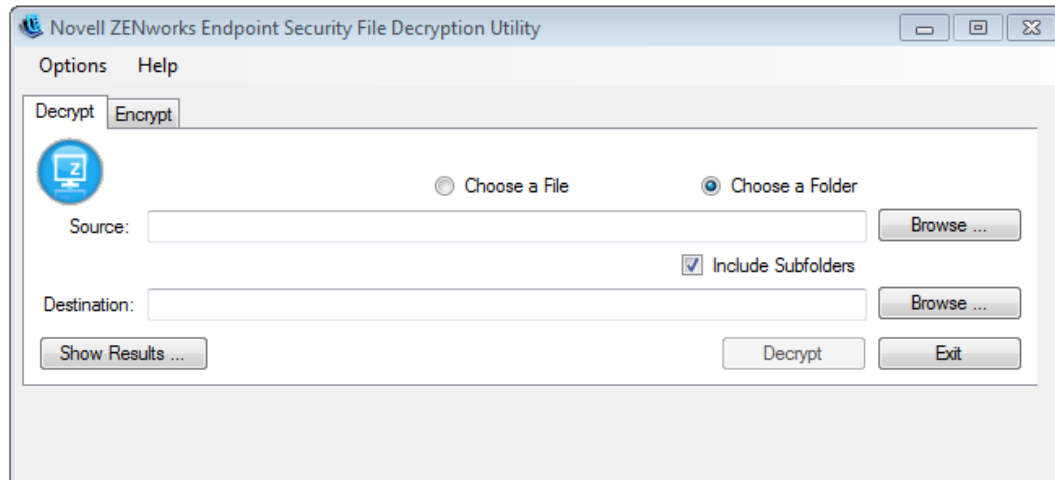


- 3 Make sure the *Choose a File* option is selected.
- 4 In the *Source* field, click *Browse*, select the password-encrypted file, then click *Open*.
- 5 In the *Destination* field, click *Browse*, select a folder in which to place the decrypted file, then click *OK*.
- 6 Click *Decrypt*.
- 7 When prompted, specify the decryption password, then click *OK*.
- 8 Click *Show Results* to view the decryption results.

14.2 Decrypting Multiple Files

You decrypt multiple files by selecting a folder rather than an individual file.

- 1 Plug the removable storage device into your computer.
- 2 Launch the File Decryption utility (ZESDecrypt.exe).



- 3 Select the *Choose a Folder* option.
- 4 In the *Source* field, click *Browse*, select the folder containing the password-encrypted files, then click *Open*.
- 5 If the folder includes subfolders with files you want to decrypt, select *Include Subfolders*.
- 6 In the *Destination* field, click *Browse*, select a folder in which to place the decrypted files, then click *OK*.

If you included subfolders when selecting the source, the decryption process preserves the subfolder structure under the destination folder.

- 7 If desired, click the *Options* menu to change which files are copied to the destination folder and how file conflicts are resolved.

Copy options: By default, only the password-encrypted files that are decrypted are copied to the destination folder. Select *Copy All Files* if you want the utility to copy all files from the source folder to the destination folder.

File conflict options: By default, you are prompted if a file has the same name as a file in the destination folder. Select *Skip if Replacing* if you want the utility to automatically skip the file without prompting you. Select *Always Replace* if you want the utility to automatically overwrite the existing file without prompting you.

- 8 Click *Decrypt*.

You can click *Show Results* to monitor the decryption progress.

- 9 When prompted, specify the decryption password. then click *OK*.

It is possible that all files do not have the same decryption password. You are prompted each time the utility attempts to open a file that has a different password.

Recovering Key-Encrypted Files

15

This functionality is available only in the Administrator version (ZESDecryptAdmin.exe) of the File Decryption utility.

The Endpoint Security Agent uses encryption keys to encrypt files on a device's fixed disk and on removable storage devices (except in the *Password-Encrypted Files* folder). The files are referred to as key-encrypted files.

If the Endpoint Security Agent is removed from a device before all of the key-encrypted files are decrypted, you can use the Administrator version of the File Decryption utility to decrypt the orphaned files.

- ♦ [Section 15.1, “Exporting the Encryption Keys,” on page 49](#)
- ♦ [Section 15.2, “Loading the Encryption Keys,” on page 49](#)
- ♦ [Section 15.3, “Decrypting Files,” on page 49](#)

15.1 Exporting the Encryption Keys

The File Decryption utility requires an encryption key file in order to decrypt files. You export the encryption key file from your Management Zone. For information, see the *ZENworks 11 SPI Endpoint Security Policies Reference*.

15.2 Loading the Encryption Keys

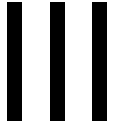
The encryption keys must be loaded from the file into the File Decryption utility. The keys remain loaded until you exit the utility.

- 1** Launch the utility (ZESDecryptAdmin.exe).
- 2** Load the key file:
 - 2a** Click the *Load Keys* button to open the Import Key dialog box.
 - 2b** In the *File* field, click *Browse* to select the key file.
 - 2c** In the *Password* field, specify the password associated with the key file.
 - 2d** Click *Load*.

15.3 Decrypting Files

After you have loaded the encryption keys, you select key-encrypted files that you want to decrypt the same way that you select password-encrypted files. For details, see [“Decrypting a Single File” on page 47](#) and [“Decrypting Multiple Files” on page 48](#).

Override Password Key Generator



The Override Password Key Generator lets you generate an override password key that can be used to disable the current policies on a device.

- ♦ [Chapter 16, “Overview,” on page 53](#)
- ♦ [Chapter 17, “Generating an Override Password Key,” on page 55](#)
- ♦ [Chapter 18, “Applying an Override Password Key,” on page 57](#)

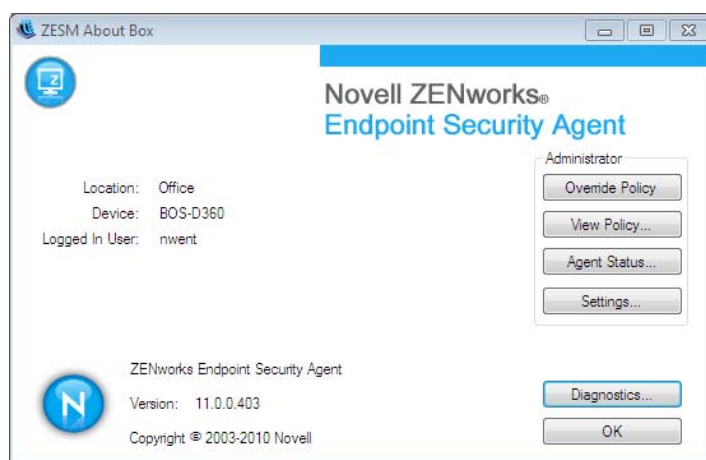
Occasionally, you might need to remove a device's security restrictions. For example, the user might need temporary access to a blocked application or might need less restrictive firewall access. You can use the Override Password Key Generator to provide the user with a password key that temporarily overrides the security policies.

The following sections provide an overview of the override password and the Override Password Key Generator:

- ♦ [Section 16.1, “The Override Password,” on page 53](#)
- ♦ [Section 16.2, “Override Password Key Generator,” on page 54](#)

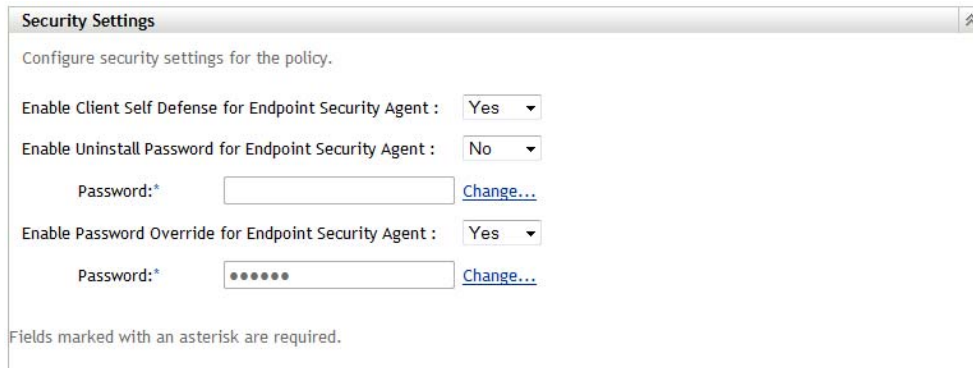
16.1 The Override Password

The Endpoint Security Agent includes an *Override Policy* option that removes the current security policies and restores the agent's default policies.



The default policies are typically non-restrictive, as if no security policies are applied. The Data Encryption policy is not removed; if a Data Encryption policy is being enforced, it continues to be enforced.

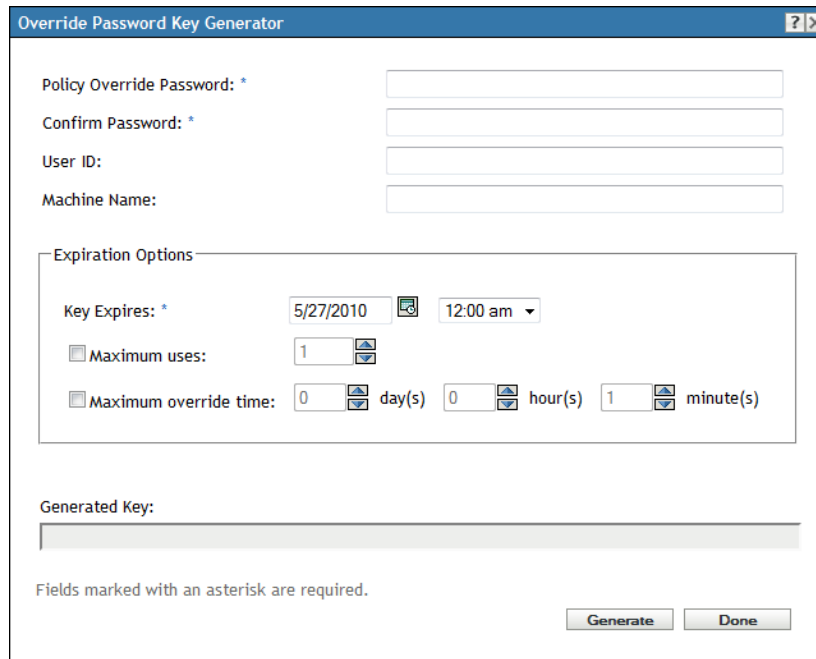
The Override Policy option is displayed in the Endpoint Security Agent only if the applied Security Settings policy is configured with an override password, as shown in the following policy example. For information about creating and assigning Security Settings policies, see “Policy Deployment” in the *ZENworks 11 SP1 Endpoint Security Policies Reference*.



16.2 Override Password Key Generator

The override password is intended to be shared only among ZENworks administrators to troubleshoot issues on devices. You should not distribute the override password to users.

If a user needs to override the currently enforced policies, you can use the Override Password Key Generator to generate an override password key. The key functions the same as the override password but allows you to specify who can use the key, what machine it can be used on, and when the key expires.



The Override Password Key Generator is included in ZENworks Control Center. For instructions explaining how to use the generator, see [Chapter 17, “Generating an Override Password Key,” on page 55](#).

Generating an Override Password Key

17

If a user needs to override the currently enforced policies, you can use the Override Password Key Generator to generate an override password key. The key functions the same as the override password but allows you to specify who can use the key, what machine it can be used on, and when the key expires.

- 1 In ZENworks Control Center, click *Endpoint Security*.
- 2 Under *Common Tasks* (in the left navigation pane), click *Override Password Key Generator* to display the following dialog box:

Override Password Key Generator

Policy Override Password: *

Confirm Password: *

User ID:

Machine Name:

Expiration Options

Key Expires: * 5/27/2010 12:00 am

Maximum uses: 1

Maximum override time: 0 day(s) 0 hour(s) 1 minute(s)

Generated Key:

Fields marked with an asterisk are required.

Generate Done

- 3 Fill in the following fields:
 - Policy Override Password:** Specify the password defined in the Security Settings policy that is assigned to the user or device.
 - Confirm Password:** Specify the password again.
 - User ID:** To restrict the key to a single user, specify the user's ZENworks login ID. The ZENworks login ID is the same as the user's LDAP directory user ID (Novell eDirectory or Microsoft Active Directory).
 - Machine Name:** To restrict the key to a single device, specify the device's computer name. This is the computer name defined in Windows System Properties on the device.
- 4 Fill in the expiration options:
 - Key Expires:** Click to select the expiration date, then select the expiration time. After the specified date and time, the key no longer works.

Maximum Uses: The override password key must be supplied each time the Endpoint Security Agent begins a new session. A new session occurs whenever the computer starts (or reboots). To restrict the key so that it can only be used a certain number of times, select *Maximum uses*, then select the number of uses. After the maximum use has been reached, the key no longer works, even if the expiration date and time have not been reached.

Maximum Override Time: To restrict the amount of time the key can be used, select *Maximum override time*, then select the number of days, hours, and minutes. For example, if you want the key to provide a maximum of 36 hours of override time, select 1 day and 12 hours.

The usage time can occur over multiple Endpoint Security Agent sessions. After the maximum time has been reached, the key no longer works, even if the expiration date and time have not been reached.

5 Click *Generate*.


The generated key is displayed in the *Generated Key* field. Copy the key and give it to the user.

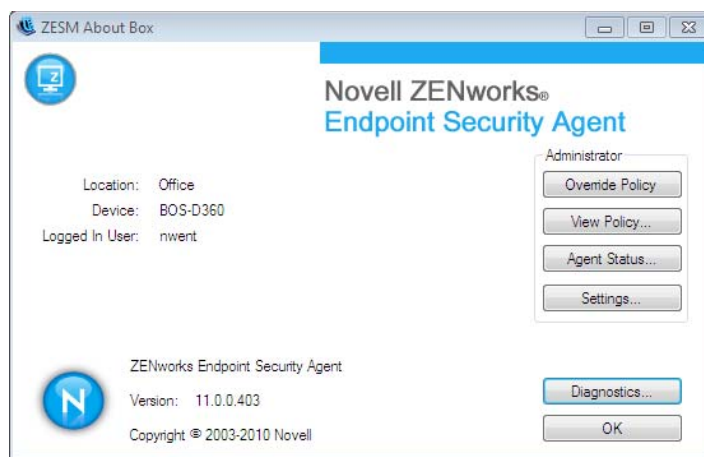
6 After you finish generating keys, click *Done*.

Applying an Override Password Key

18

The following instructions assume that an override password key is already generated. If a key is not yet generated, see [Chapter 17, “Generating an Override Password Key,” on page 55](#).

- 1 On the Windows device, right-click the  icon in the notification area, then click *Show Properties*.
- 2 Click *Endpoint Security* to display the Endpoint Security properties page.
- 3 Under *Endpoint Security Agent Actions*, click *About* to display the ZESM About dialog box.



- 4 Click the *Override Policy* button, specify the override password key, then click *Override*.

The override results in the following:

- ♦ The Data Encryption policy continues to be enforced.
- ♦ The Firewall policy behavior is set to Open.
- ♦ All other policies are removed.

The override occurs immediately and stays in effect until one of the following occurs:

- ♦ The device reboots.
- ♦ The maximum override time expires.
- ♦ The key expires.
- ♦ The *Load Policy* button is clicked.

