AUTHORIZED DOCUMENTATION

Security Client for Windows* Vista* and Windows 7 User Guide

Novell®
ZENworks® Endpoint Security Management

4.1

January 27, 2010

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/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide

This *User Guide* provides information to help you use the Security Client for Windows Vista and Windows 7. The Security Client is a component of Novell® ZENworks® Endpoint Security Management.

The information in this guide is organized as follows:

Audience

This guide is intended for any users of the Security Client for Windows Vista and Windows 7. A separate guide is available for users of the Security Client for Windows 2000 and Windows XP. See the ZENworks Endpoint Security Management 4.1 documentation Web site (http://www.novell.com/documentation/zesm41).

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, or go to the Novell Documentation Feedback site (http://www.novell.com/documentation/feedback.html) and enter your comments there.

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 Endpoint Security Management 4.1 documentation Web site (http://www.novell.com/documentation/zesm41).

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

Introduction

1

The Novell® ZENworks® Endpoint Security Client, referred to as the *Security Client*, secures your computer against intruder attacks that can result in lost data, stolen data, and computer damage. The following sections introduce the Security Client:

1.1 What the Security Client Does

The Security Client enforces security policies created by your ZENworks Endpoint Security Management administrator. Security policies are a collection of security settings that determine the following on your computer:

- The wireless networks to which you can connect.
- The firewall configuration, such as allowed ports, protocols, network addresses, and applications.
- The communication hardware (Bluetooth*, 1394 FireWire*, Serial/Parallel) that is active.
- The storage devices (CD/DVD, floppy drives, removable storage devices) that are active.
- The locations (network environments) in which a VPN connection is required.
- The hard drive folders that provide data encryption of files, and whether or not removable storage devices (such as USB thumb drives) are encrypted.

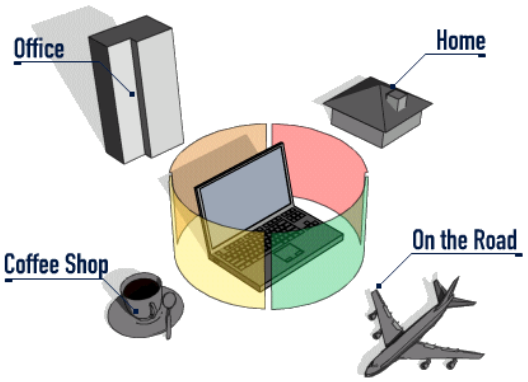
Your administrator determines the security policies assigned to you (or your computer) and distributes the policies to your computer. The Security Client enforces the settings and provides reports to the administrator.

1.2 Locations

A security policy includes both global settings and location settings. Global settings are applied regardless of your location. Location settings are applied only when the Security Client detects that its current network environment meets a location defined by your administrator.

A security policy might have a few defined locations or it might have many. For each location, the Security Client applies the security settings defined for that location. For example, an Office location might have one set of firewall settings while a Remote location has another.

Figure 1-1 *The Security Client Adjusts Security Settings Based on the Detected Location*



Your administrator defines locations that you commonly visit, such as your office location or home location. Whenever you visit a location that is not defined, the Security Client applies the Unknown location. The Unknown location includes the following default security settings:

- Change Locations = Permitted
- Change Firewall Settings = Not permitted
- Save Location = Not permitted
- Update Policy = Permitted
- Default Firewall settings = All Adaptive (all ports open for inbound and outbound traffic)

Your administrator can change the Unknown location's security settings, so your settings might be different than the ones listed above.

1.3 Security Policy Updates

The Security Client is installed in *managed mode* or *unmanaged mode*.

If your Security Client is running in managed mode, updated security policies are automatically distributed to the Security Client when it checks in with the ZENworks Endpoint Security Management system. Check-in occurs automatically whenever you start your computer or manually whenever you initiate a check in.

If your Security Client is running in unmanaged mode, your administrator must distribute updated security policies to your computer. Depending on the distribution methods available to your administrator, this might require you to receive the updated policy and manually copy it to the appropriate Security Client directory.

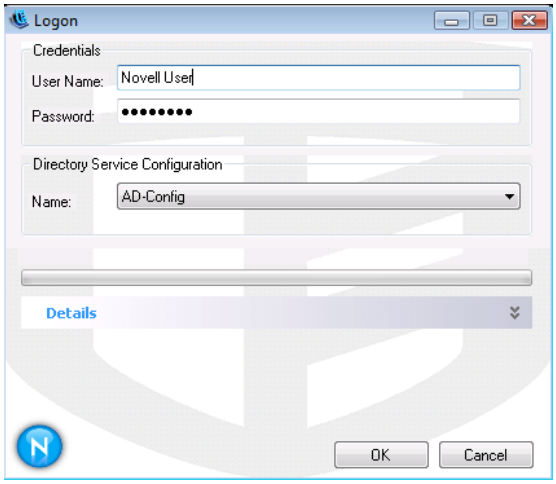
Instructions for manually initiating a policy update (managed mode) and manually copying a policy update to the Security Client directory (unmanaged mode) are provided in Chapter 5, "Policy Updates," on page 23.

Log In

2

If the Security Client is running in managed mode, you must log in to connect the Security Client to the ZENworks® Endpoint Security Management system.

Depending on how your administrator has configured your system for login, you might be logged in automatically when you log in to your directory service (Microsoft* Active Directory* or Novell eDirectory™). If not, the Security Client displays a Login dialog box.



If you receive the Security Client login prompt:

1. Fill in the following fields:

   User Name: Specify the username you enter to log in to your Active Directory domain or eDirectory tree. Specify the username only (without the domain or tree context).

   Password: Specify the password associated with the username you entered.

   Directory Service Configuration Name: Select the configuration name that represents your Active Directory domain or eDirectory tree.

2. Click *OK*.

Locations

3

As you move from one location to another, your computer might require different security measures to protect it. Your ZENworks® Endpoint Security Management administrator defines common locations (Office, Home, Remote, and so forth) and assigns security settings to each of the locations. When the Security Client detects that it is in one of the defined locations (based on specific network environment parameters established by your administrator), it applies the security settings for the location.

The following sections provide instructions for using the Security Client to manage locations. Your administrator controls options you have access to. If a Security Client option is not available, your administrator has removed access to the option.

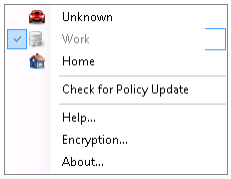
3.1 Changing Locations

By default, the Security Client attempts to detect the current network environment and to change the location automatically. In some cases, you might want to change locations manually to apply different security settings to your computer.

If you cannot perform the following steps, your ZENworks Endpoint Security Management administrator has prevented you from changing locations manually.

To change a location:

1 Right-click the *Endpoint Security Client* icon in the taskbar to display a menu of choices.



2 Click the appropriate location.

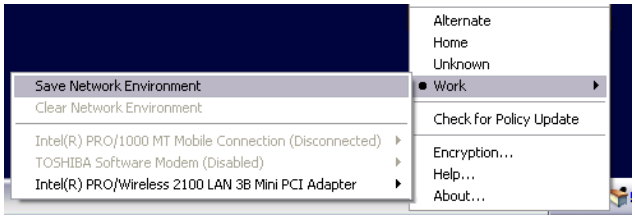
3.2 Saving a Network Environment

You can save a network environment to a location. This allows the Security Client to automatically switch to that location the next time you enter the network environment. For example, your administrator might have defined a Home location. You can save your home network environment to the Home location so that each time your computer detects your home network environment it applies the Home location’s security settings.

If you cannot perform the following steps, your ZENworks Endpoint Security Management administrator has prevented you from saving network environments.

To save an environment:

1. Right-click the *Endpoint Security Client* icon in the taskbar to display the menu.
2. Click the location you want to change to.
3. Right-click the *Endpoint Security Client* icon, mouse over the current location to display the submenu, then click *Save Network Environment* to save the environment.



   If this network environment was saved at a previous location, the Security Client asks if you want to save the new location. Select *Yes* to save the environment to the current location and clear the environment from its prior location, or select *No* to leave the environment in the prior location.

Additional network environments can be further saved to a location. For example, if a location defined as Airport is part of the current policy, each airport you visit can be saved as a network environment for this location. This way, every time you return to a saved airport environment, the Security Client automatically switches to the Airport location.

3.3 Saving a Wi-Fi Environment

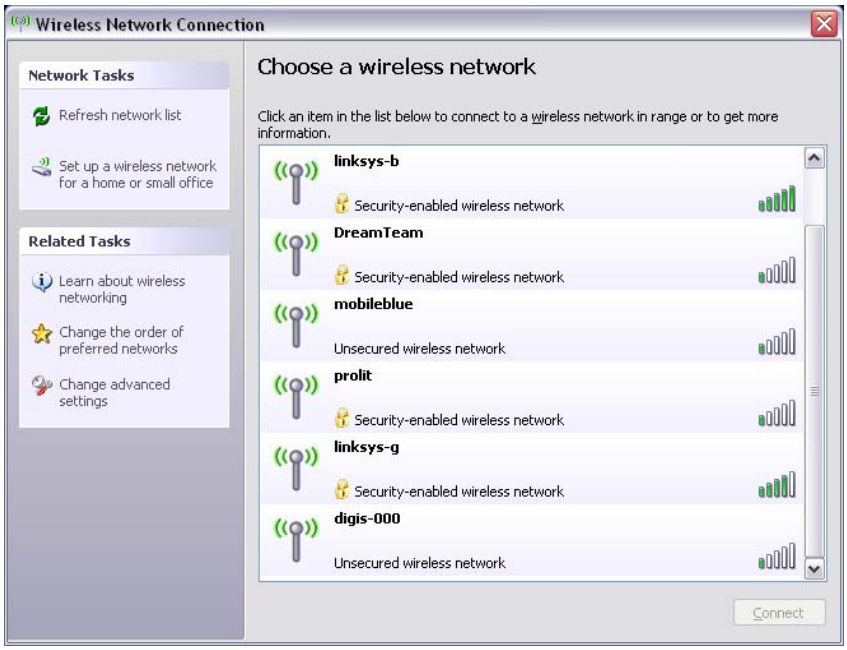
At any single location, your Wi-Fi adapter might detect many available wireless access points. The Wi-Fi adapter might lock on to a single access point at first, but if too many access points are within proximity of the adapter, the adapter might drop the associated access point and switch to another access point with a stronger signal. When this occurs, current network activity is halted, often forcing the resending of certain packets and reconnecting of the VPN to the corporate network.

You can resolve this situation by locking on to a specific access point for a location. If an access point is saved as a network environment parameter at a location, the adapter locks on to that access point and does not lose connectivity until you physically move away from the access point. When you return to the access point, the adapter automatically associates with the access point, the location changes, and all other access points are no longer visible through wireless connection management software.

If you cannot perform the following steps, your ZENworks Endpoint Security Management administrator has prevented you from saving network environments.

To save a Wi-Fi environment:

1. Open the connection management software and select the desired access point.



2 Specify any necessary security information (WEP or other security key), then click *Connect*.

3 Complete the steps outlined in Section 3.2, “Saving a Network Environment,” on page 13 to save this environment.

3.4 Removing a Saved Network Environment

You can remove any network environments that you’ve saved to a location. When you do so, all of the saved network environments for the location are removed.

If you cannot perform the following steps, your ZENworks Endpoint Security Management administrator has prevented you from saving and deleting network environments.

To remove the saved network environments from a location:

1 Make sure the location is the current location:

1a Right-click the *Endpoint Security Client* icon in the taskbar to display the menu.

1b Change to the appropriate location.

2 Right-click the *Endpoint Security Client* icon, then select the current location to display the submenu.

3 Click *Clear Network Environment* to clear all of the saved network environments.

Data Encryption

4

The Security Client can manage the encryption of files placed in specific directories on your computer and on removable storage devices such as thumb drives. Data encryption is available only if your ZENworks® Endpoint Security Management administrator has enabled it.

The following sections provide information about encrypting files on your computer:

4.1 Managing Files on Fixed Disks

Fixed disks are defined as all non-system volume drives installed on the computer, as well as any partitions of a hard-disk drive. Each fixed disk on the endpoint has an `Encrypted Files` folder placed at the root directory of each non-system volume or drive. All files placed in this folder are encrypted with the current encryption key. Only authorized users on the computer can decrypt these files. `Encrypted Files` is the default name for the folder; your administrator might have changed the name.

When you save a file, select the `Encrypted Files` folder from the available folders on the desired drive.

4.2 Managing Files on Removable Storage

Removable storage is defined as any storage device that is connected to a computer. This includes (but is not limited to) USB thumb drives, flash memory cards, and PCMCIA memory cards, along with traditional Zip, floppy, and external CDR drives, digital cameras with storage capacity, and MP3 players.

When you connect a removable storage device to your computer, the Security Client prompts you to encrypt the files on the device. This protects you from accidentally encrypting a device. After you initially encrypt the device, any files you add to the device (from a computer that has the Security Client installed) are automatically encrypted. If you then connect the storage device to a computer that does not have the Security Client installed, the files remain encrypted and cannot be decrypted.

The following sections contain more information:

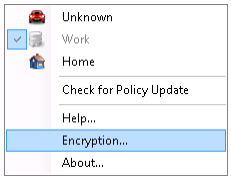
4.2.1 Encrypting Files

When you connect an unencrypted removable storage device to your computer, the Security Client prompts you to encrypt the files on the device. Thereafter, as you add files to the removable storage device, the Security Client automatically encrypts the files.

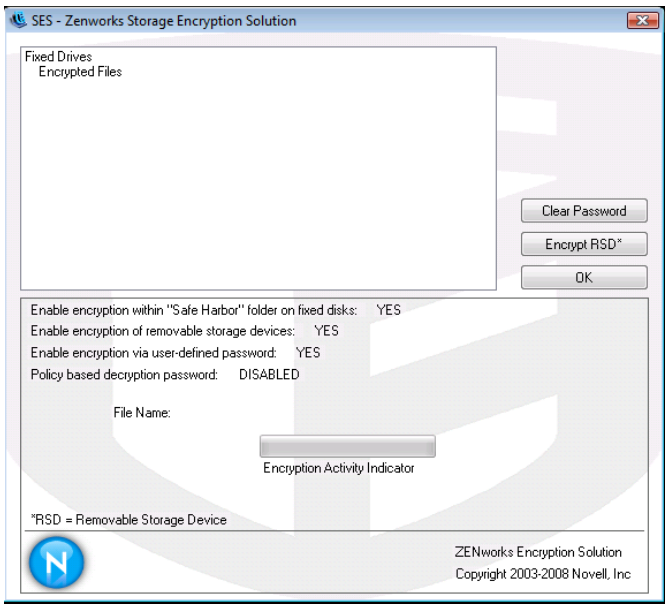
In some cases, you might need to manually encrypt a file. For example, if you connect your removable storage device to a computer that does not have the Security Client installed, any files you add to the device are not encrypted (because the Security Client does the encrypting). To encrypt the files, you need to connect the removable storage device to a computer that has the Security Client installed and then manually encrypt them.

To manually encrypt added files on a removable storage device:

1. Plug the storage device into the appropriate port on a computer that has the Security Client installed.
2. Right-click the *Endpoint Security Client* icon in the taskbar.
3. Select *Encryption* from the menu.



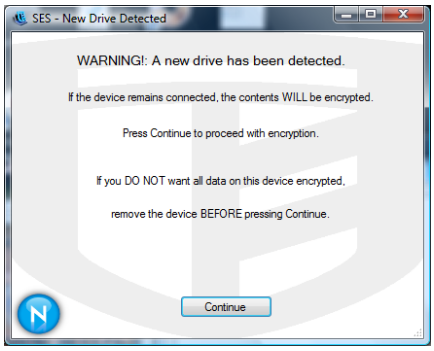
4. Click *Encrypt RSD* to use the current encryption key to encrypt all files on the removable storage device.



The amount of time needed to encrypt the files depends upon the amount of data stored on the device.

4.2.2 What If I Don't Want the Device Encrypted?

When you insert a removable storage device, the Security Client prompts, asking if you want the drive encrypted, or if you prefer to remove it and not encrypt all files.



To prevent encryption, remove the drive before clicking *Continue*. Click *Continue* to either encrypt the drive or to close the window after removing the device.

4.2.3 Password Encrypting Files

Your administrator can enable the Security Client to create a Password Encrypted Files folder on any removable storage device that connects to your computer. This folder is named by your administrator; therefore, it might be named *Password Encrypted Files* or some other name.

When you add files to this folder, they are encrypted with a password that you supply. You can then access the files from any device that is not running the Security Client. To decrypt the files, you need the ZENworks File Decryption utility and the encryption password. You must get the utility from your administrator.

For example, assume that you are working on encrypted files at work. You want to take the files home to work on them, but your home computer does not have the Security Client installed. You copy the files to the Password Encrypted Files folder on your USB thumb drive, take the files home, then access them by using the ZENworks File Decryption utility you got from your administrator.

To use the Password Encrypted Files folder:

1. Move or save a file to the folder.
2. At the password prompt, enter a password and confirmation password.
3. Enter a hint for the password.

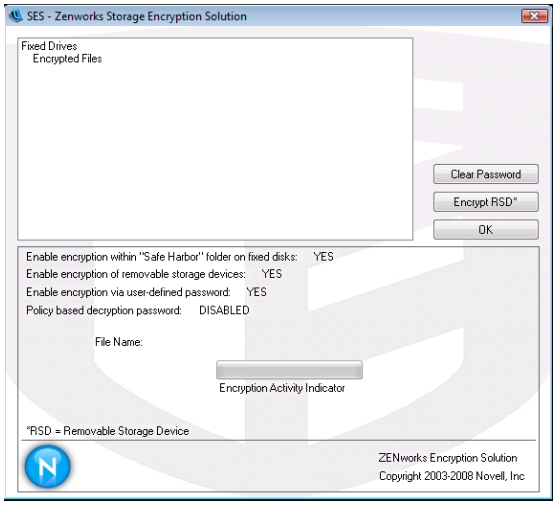
The Security Client remembers the password and applies it to any new files that you add to the folder until you reboot your computer. Any time your computer reboots, you are again prompted to supply a password the first time you add a file to the folder.

4.2.4 Changing the Password for the Password Encrypted Files Folder

After you enter a password for the Password Encrypted Files folder on your removable storage devices, the Security Client uses the same password until you reboot your computer. If you want to change the password without rebooting, you can do so manually. However, this does not change the password for existing files, just the password assigned to future files.

To change the password:

1. Plug the storage device into the appropriate port on your computer.
2. Right-click the *Endpoint Security Client* icon in the taskbar.
3. Select *Encryption* from the menu.
4. Click *Clear Password*.



5. Drag a file to the Password Encrypted Files folder and enter the new password and hint.

All new files added to the folder now require the new password for access.

4.2.5 Decrypting Password Encrypted Files

The File Decryption utility lets you decrypt files stored in the Password Encrypted Files folder on a removable storage device.

Your ZENworks Endpoint Security Management administrator must give you the File Decryption utility.

To use the File Decryption utility:

1. Plug the storage device into the appropriate port on your computer.
2. Open the File Decryption Utility (`stdecrypt.exe`).
3. Click the *Advanced* button.
4. In the Source panel, select *Password Protected Only*.

5. In the Source panel, click *Browse*, navigate to the storage device's Password Encrypted Files directory, select the desired file, then click *Save*.

   or

   To decrypt the entire Password Encrypted Files directory rather than a single file, select *Directories*, then browse to and select the appropriate directory.

6. In the Destination panel, click *Browse* to select the folder on the local machine where you want to store the decrypted files.
7. Click *Decrypt*.
8. Enter the password to decrypt the file.

   If you selected the entire directory, all files might not have the same password. You are prompted each time the utility attempts to open a file that has a different password.

The transaction can be monitored by clicking the *Show Progress* button.

Policy Updates

5

Occasionally, your ZENworks® Endpoint Security Management administrator might update the security policy that determines the security settings on your computer.

If your Security Client is running in managed mode, updated security policies are automatically distributed to the Security Client when it checks in with the ZENworks Endpoint Security Management system. Check-in occurs automatically whenever you start your computer or manually whenever you initiate a check for policy updates. To see if your Security Client is running in managed mode, right-click the Security Client icon located in the Windows notification tray. If the menu includes a *Check for Policy Update* option, your Security Client is managed.

If your Security Client is running in unmanaged mode, your administrator must distribute updated security policies to your computer. Depending on the distribution methods available to your administrator, this might require you to receive the updated policy and manually copy it to the appropriate Security Client directory.

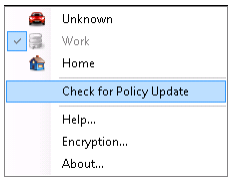
The following sections provide instructions for manually initiating a policy update (managed mode) and manually copying a policy update to the Security Client directory (unmanaged mode):

- Section 5.1, “Checking for Policy Updates,” on page 23
- Section 5.2, “Manually Applying a Policy Update,” on page 24

5.1 Checking for Policy Updates

The Security Client automatically receives updates at intervals determined by your administrator. However, you can manually check for policy updates:

1. Right-click the *Endpoint Security Client* icon in the taskbar to display the menu.
2. Click *Check for Policy Update*.



The Security Client notifies you if the policy has been updated.

NOTE: Switching wireless access cards occasionally displays the `Policy Has Been Updated` message. The Policy has not been updated; the Security Client is simply comparing the device to any restrictions in the current policy.

5.2 Manually Applying a Policy Update

If your Security Client is running in unmanaged mode, your administrator might deliver policy updates to you and ask you to apply them. To do so:

1. Copy the policy file (or files) to the following directory on your computer:

   ```
   \Program Files\Novell\ZENworks Security Client
   ```

Password Override

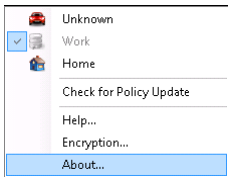
6

The Security Client is equipped with a Password Override feature that temporarily disables the current security policy. This can be helpful if your security policy is adversely affecting the work or activities you need to perform in a specific location.

To use the Password Override feature, you must obtain a password key from your ZENworks® Endpoint Security Management administrator. The password key expires when you reboot your computer or when you reach the administrator-determined time limit. After the password key expires, the security policy protecting your computer is restored.

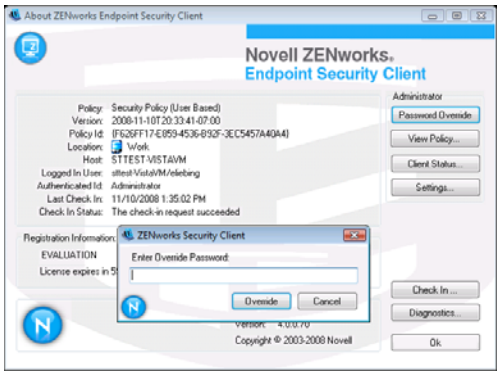
To activate the password override:

1. Contact your administrator to get the password key.
2. Right-click the *Endpoint Security Client* icon in the taskbar to display the menu, then click *About*.



3. Click *Password Override* to display the password window.

   If the *Password Override* button is not displayed on this screen, your current policy does not have a password override.



4. Type the password key provided by your administrator.
5. Click *OK*. The current policy is replaced with a default All Open policy for the designated time.

Clicking *Load Policy* (which replaces the *Password Override* button) in the *About* window restores the previous policy. If your administrator has updated your policy to resolve existing issues, you should use *Check for Policy Update* to immediately download the new policy.

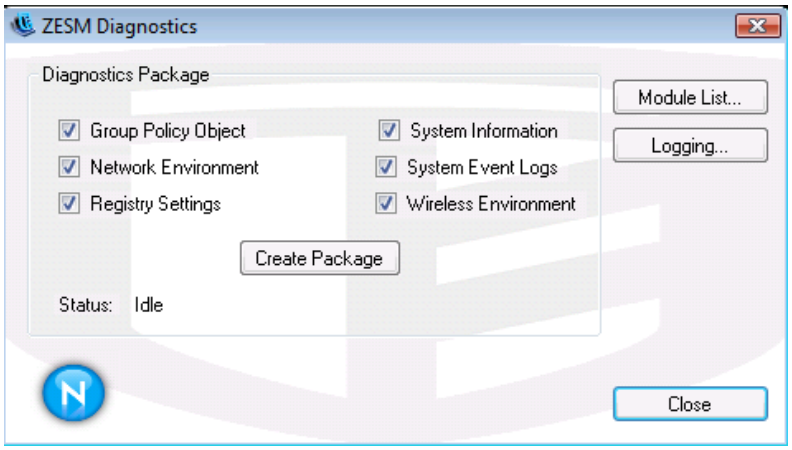
Diagnostics

7

The Security Client provides diagnostics tools to enable your administrator to troubleshoot Security Client issues. If this becomes necessary, your administrator will guide you through the diagnostics process.

You might be asked for a diagnostics package. Your administrator will tell you what to include in it. To create a diagnostics package:

1. Right-click the *Endpoint Security Client* icon in the taskbar to display the menu, then click *About*.
2. Click the *Diagnostics* button.



3. Check everything in the Diagnostics Package pane, or check only the items that your administrator requests, then click *Create Package*.

   The Security Client creates a `zesmdiagnostics*.enc` file on your desktop, which you can then send to the administrator.