ZENworks Endpoint Security Management

Version 3.2

ZENworks Security Client
User's Manual

June 14, 2007

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

PN: UM300MWE

Document Version 1.0 - supporting Novell ESM 3.2 and subsequent version 3 releases

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

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, 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

ZENworks Security Client User's Manual

Introduction

Novell' ZENworks Endpoint Security Management (ESM) is designed to protect corporate data assets, through a centrally managed tool called the ZENworks Security Client (ZSC). The ZSC is installed on enterprise PCs and enforces security policies written and sent down through the ESM management and distribution system. This allows large enterprises and small businesses to create, deploy, enforce and monitor computer security policies on computers inside and outside of the corporate security perimeter.

Security Enforcement for Mobile Computers

Security is enforced both globally and by network location. Each location listed in a security policy determines the user's permissions in that network environment and which firewall settings are activated. The firewall settings determine which networking ports, network addresses, and applications are granted network access and how that access is permitted.

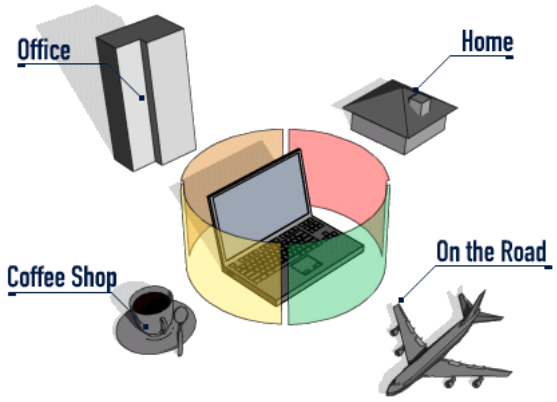

Figure 1: ESM Adjusts Security Settings Based on the Detected Network Environment

Normal operations of the ZSC are transparent to the user, once the network environments have been defined. Occasionally, ZSC protective measures can interrupt normal operation, when this occurs, messages and hyperlinks display to notify the user about the security policy, what protective steps have been taken, and refer them to additional information to help correct the issue.

NDIS Layer Firewall Protection

In securing mobile devices, ESM is superior to typical personal firewall technologies which operate only in the application layer or as a firewall-hook driver. ESM client security is integrated into the Network Driver Interface Specification (NDIS) driver for each network interface card (NIC), providing security protection from the moment traffic enters the PC. Differences between ESM and application-layer firewalls and filter drivers are illustrated in Figure 2.

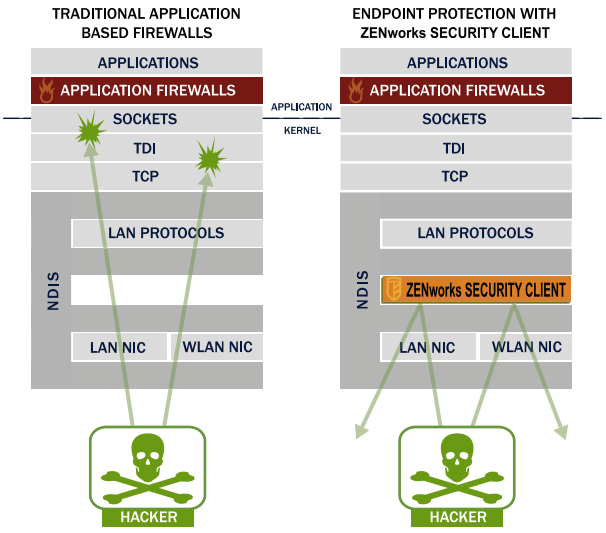

Figure 2: Effectiveness of a NDIS-Layer Firewall

Security decisions and system performance are optimized when security implementations operate at the lowest appropriate layer of the protocol stack. With the ZENworks Security Client, unsolicited traffic is dropped at the lowest levels of the NDIS driver stack by means of Adaptive Port Blocking (stateful packet inspection) technology. This approach protects against protocol-based attacks including unauthorized port scans, SYN Flood attacks, and others.

It is recommended that you follow all operation and maintenance recommendations reflected this document, in order to ensure the endpoint security environment is assured.

ESM Terminology

Locations - Locations are simple definitions which help users identify the network environment they are in, provide immediate security settings (defined by the administrator), and can permit the user to save the network environment and/or change the applied firewall settings.

Each location is given unique security settings, denying access to certain networking and/or hardware in more hostile network environments, and permitting broader access within trusted environments. Locations define the following information:

- The frequency the ZSC will check for a policy update in this location
- The location management permissions granted to a user
- The firewall settings that will be used at this location
- Which communication hardware will be permitted connectivity?
- How Wi-Fi connectivity and security will be handled at this location
- At what level the user is permitted to use removable storage devices (such as thumb-drives and memory cards) and/or their CD/DVD-RW drive
- Any Network Environments that can help to define the location

Firewall Settings - Firewall Settings control the connectivity of all networking ports (1-65535), network packets (ICMP, ARP, etc.), network addresses (IP or MAC), and which network applications (file sharing, instant messenger software, etc.) are permitted to get a network connection, when the setting is applied. Three firewall settings are included as defaults for ESM, and may be implemented at a location. The ESM Administrator can also create specific firewall settings, which cannot be listed here.

- **All Adaptive** - This firewall setting sets all networking ports as stateful (all unsolicited inbound network traffic is blocked. All outbound network traffic is allowed), ARP and 802.1x packets are permitted, and all network applications are permitted a network connection, all.
- **All Open** - This firewall setting sets all networking ports as open (all network traffic is allowed), all packet types are permitted. All network applications are permitted a network connection
- **All Closed** - This firewall setting closes all networking ports, and restricts all packet types.

Adapters - Refers to three communication adapters normally found on an endpoint, Wired Adapters (LAN connections), Wi-Fi Adapters (PCMCIA Wi-Fi cards, and built-in Wi-Fi radios), and Dialup Adapters (both internal and external modems). Also refers to other communication hardware that may be included on a PC, such as Infrared, Bluetooth, Firewire, and serial and parallel ports.

Storage Devices - refers to external storage devices that can pose a security threat when data is copied to, or introduced from, these devices on an endpoint. USB "thumb-drives," Flash memory cards, and SCSI PCMCIA memory cards, along with traditional zip, floppy, and external CDR drives and the installed CD/DVD drives (including CD-ROM, CD-R/RW, DVD, DVD R/RW), can all be blocked, permitted, or rendered to Read-Only at a single location.

Network Environments - A network environment is the collection of network services and service addresses required to identify a network location (see Saving Network Environments).

ZENworks Security Client Overview

The ZENworks Security Client (ZSC) secures PCs from data invasion attacks at home, at work, and while traveling through the enforcement of security policies created by the enterprise ESM administrator. The firewall settings assigned at individual locations, are automatically adjusted when laptop users move from the corporate network to their home network or go on-the-road and log-on to a public or open network.

Security levels are applied to various user locations without requiring user expertise in (or understanding of) network security, port configurations, hidden shared files, or other technical details Immediate information on which location and firewall setting the ZSC is in and which adapters are presently active and/or permitted is available by simply mousing-over the task tray icon to view the ZSC tool-tip (see Figure 3).

Figure 3: ZENworks Security Client Tool-tip

Logging-In to the ZSC

If you are a member of the corporate domain, the ZSC will use your windows username and password to log you in to the Policy Distribution Service (no pop-up window will display). If you are not a member of the domain that the Policy Distribution Service is hosted on, the ZSC will prompt you for your username and password for that domain (see Figure 4).

Figure 4: ZENworks Security Client Login

Enter your username and password for the domain, and click OK.

Note:

It is not necessary to log-in to the ZSC when the ZSC is running as Unmanaged. The ESM Administrator will have a different method to deliver policies to unmanaged users.

Using the ZENworks Security Client

Right-click the ZSC icon in the task tray to display the menu (see Figure 5).

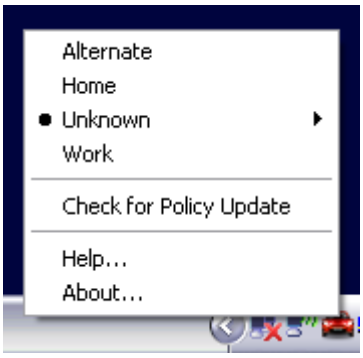

Figure 5: Right-click Menu

The menu gives the user access to:

- Changing Locations (page 11)
- Saving a Network Environment (page 12)
- Remove a Saved Environment (page 14)
- Changing Firewall Settings (page 15)
- Update Policies (page 16)
- View Help (page 17)
- Password Override (page 18)

Note:

The actions listed above can be restricted by the administrator at any location.

Moving Between Network Environments

Each network an end-user travels to may require different security measures. The ZENworks Security Client provides security and protection in locations identified by available network connections. The ZSC detects the network environment parameters and switches to the appropriate location, applying the needed protection levels according to the current security policy.

Network Environment information is either Stored or Preset within a location. This allows the ZSC to switch to a location automatically when the environment parameters are detected.

- **Stored Environments** - defined by the user (see Saving a Network Environment)
- **Preset Environment** - defined by the enterprise ESM Administrator through a published security policy

When the user enters a new network environment, the client compares the detected network environment to any Stored and Preset values in the security policy. If a match is found, the ZSC activates the assigned location. When the detected environment cannot be identified as a Stored or Preset environment, the client activates the default Unknown location.

The Unknown location has the following presets:

- Change Locations = Permitted
- Change Firewall Settings = Not permitted
- Save Location = Not permitted
- Update Policy = Permitted
- Default Firewall settings = All Adaptive

The three adapter types, wi-fi, wired, and dialup are permitted in the Unknown location. This allows the PC to interface peripherally with its network environment, and attempt to associate a location policy as described above.

Changing Locations

At startup, the ZENworks Security Client will switch to the Unknown location. It will then attempt to detect the current network environment, and change the location automatically. In a case where the network environment is either unrecognized, or has not been preset or saved (see Saving a Network Environment), the location will need to be changed manually.

To change a location, perform the following steps:

Step 1: Right-click the ZSC icon in the task tray to display the menu

Step 2: Highlight the appropriate location (see Figure 6)

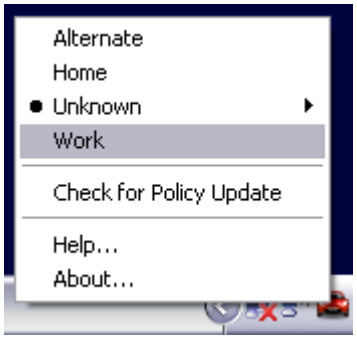

Figure 6: Changing Locations

Step 3: Left-click the selection to change the location

Saving a Network Environment

A network environment will need to be either preset in the security policy or saved by the end-user, before the ZENworks Security Client can automatically change locations. Saving a network environment saves the network parameters to the current location, and allows the ZSC to automatically switch to that location the next time the user enters the network environment. When applied in a Wi-Fi network environment, the ZSC will LockOn™ to the single, selected access point.

To save an environment, perform the following steps:

Step 1: Right-click the ZSC icon in the task tray to display the menu

Step 2: Change to the appropriate location as described above

Step 3: Open the menu again, and highlight the current location to display the sub-menu (see Figure 7)

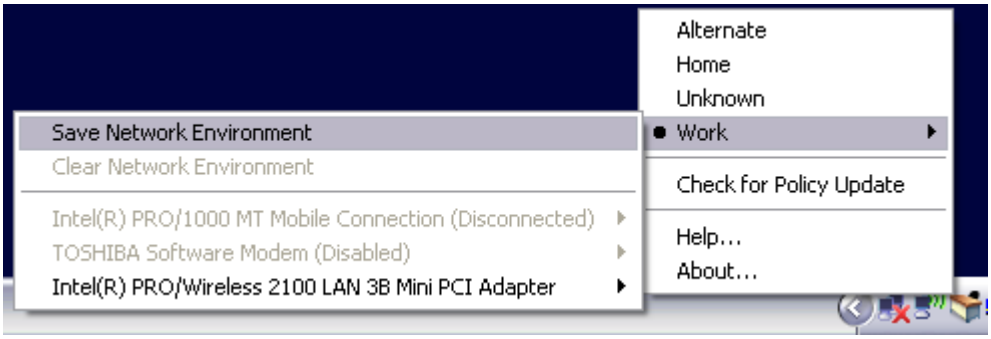

Figure 7: Saving a Network Environment

Step 4: Highlight *Save Network Environment* and left-click the selection to save

If this network environment was saved at a previous location, the ZSC will ask if the user wants to save the new location. Select *Yes* to save the environment to the current location and clear the environment from its prior location, or *No* to leave the environment in the prior location.

Note:

The Save Network Environment function can be restricted by the ESM Administrator at any location.

Additional Network Environments may be further saved to a location. For example, if a location defined as Airport is part of the current policy, each airport visited by the mobile user can be saved as a network environment for this location. This way, every time a mobile user returns to a saved airport environment, the ZSC will automatically switch to the Airport location.

Saving a Wi-Fi Environment

When a user activates their Wi-Fi adapter, they may see dozens of access points available. A Wi-Fi adapter may lock on to a single AP at first, but if too many APs are within proximity of the adapter, the associated AP may be dropped and the wireless connection manager could prompt the adapter to switch to the access point with the strongest signal. When this occurs, current network activity is halted; often forcing a user to resend certain packets and re-connect their VPN to the corporate network.

If an access point is saved as a network environment parameter at a location, the user will LockOn™ to that AP and will not lose connectivity until they physically move away from the access point. Upon returning to the AP, the adapter will automatically associate with the access point, the location will change, and all other APs will no longer be visible through wireless connection management software.

To save a Wi-Fi Environment, perform the following steps:

Step 1: Open the connection management software and select the desired access point (see Figure 8)

Note:

Connection Management Software can be overridden by location when the ESM Security Policy is set to managed your wireless connectivity.

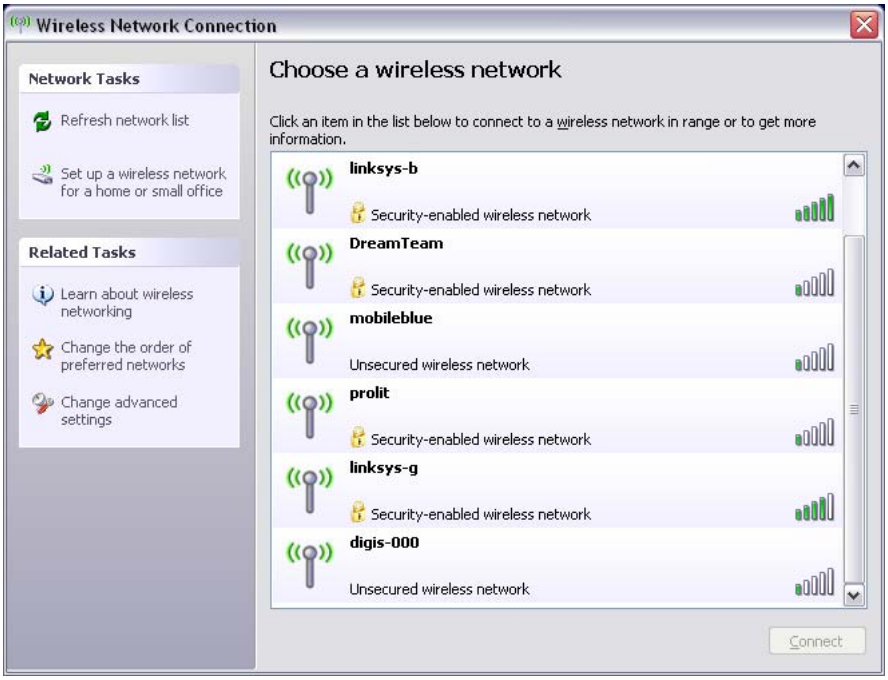

Figure 8: Selecting a Wireless Access Point

Step 2: Enter any necessary security information (WEP or other security key), and click Connect

Step 3: Complete the steps outlined on the previous page to save this environment

Remove a Saved Environment

Step 1: To remove a saved network environment from a location, perform the following steps:

Step 2: Right-click the ZSC icon in the task tray to display the menu.

Step 3: Change to the appropriate location.

Step 4: Open the menu again, and highlight the current location to display the sub-menu.

Step 5: Highlight *Clear Network Environment* and left-click to clear.

Note:

This will clear ALL saved network environments for this location.

Changing Firewall Settings

Each Location can be assigned more than one firewall setting. Changing the firewall setting can open or close networking ports and allow or disallow certain types of networking in a given location.

To change the firewall settings, perform the following steps:

Step 1: Right-click the ZSC icon in the task tray to display the menu

Step 2: Highlight the current location to display the submenu (see Figure 9)

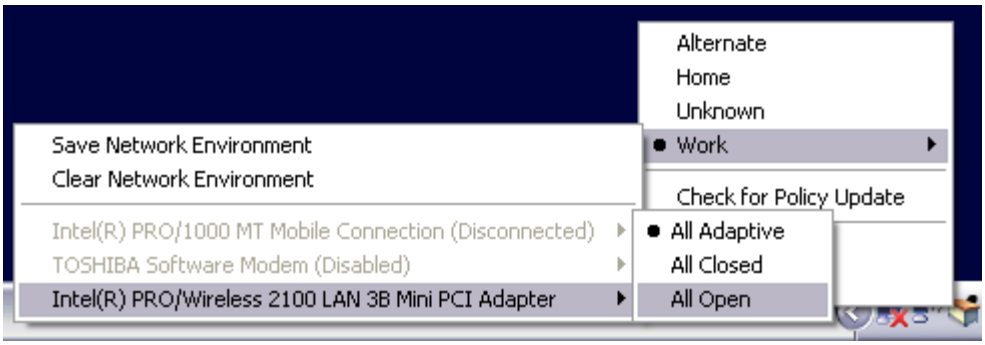

Figure 9: Changing the Firewall Setting

Step 3: Highlight the desired firewall setting

Step 4: Left-click the selection to change the firewall setting

---

Note:

The number of firewall settings available in a location is determined by policy.

Update Policies

New security policies are released to managed users as they are published. The ZSC will automatically receive updates at intervals determined by the ESM administrator. However, the managed user can check for policy updates when entering a new location. Perform the following steps:

Step 1: Right-click the ZSC icon in the task tray to display the menu

Step 2: Highlight *Check for Policy Update* (see Figure 10)

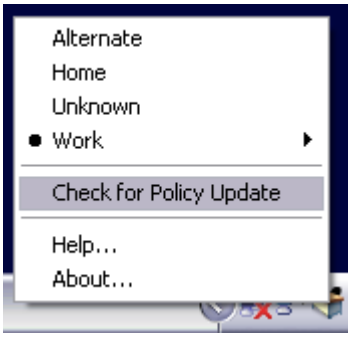

Figure 10: Check for Policy Update

Step 3: Left-click the selection to have the Client look for a new Security Policy

---

Note:

Automatic updates and checking for policy update are not available features when the ZSC is running as Unmanaged. The ESM Administrator will have a different method to deliver policy updates to these users.

The ZSC will notify if the Policy has been updated

Note:

Switching wireless access cards out will occasionally display the "Policy Has Been Updated" message. The Policy has not been updated, the ZSC is simply comparing the device to any restrictions in the current policy.

View Help

The ZSC Help screen may be viewed at any time by:

Step 1: Right-clicking the ZSC icon in the task tray to display the menu

Step 2: Highlight *Help…*(see Figure 11)

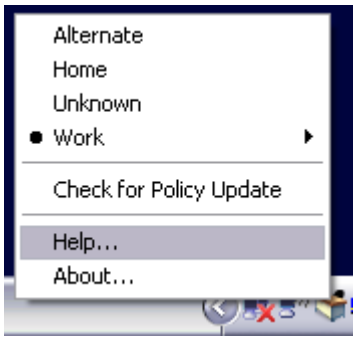

Figure 11: View Help

Step 3: Left-clicking the selection to launch Help

Password Override

Productivity interruptions that a user may experience due to restrictions to connectivity, software, or thumb-drives are likely caused by the security policy the ZSC is enforcing. Changing locations or firewall settings will most often lift these restrictions and restore the interrupted functionality. However, in some cases the restriction could be implemented in such a way that they are restricted in all locations and/or firewall settings. When this is the case the restrictions will need to be temporarily lifted to allow productivity.

The ZSC is equipped with a Password Override feature which temporarily disables the current security policy to permit the necessary activity. The Security Administrator distributes a single-use password key only when needed, and should be informed of any problems with a security policy. Once the password key's time limit has expired the security policy protecting the endpoint will be restored. Rebooting the endpoint will also restore the security settings.

To activate the password override, perform the following steps:

Step 1: Contact your company's ESM Administrator to get the password key

Step 2: Right-click the ZSC icon in the task tray to display the menu

Step 3: Highlight *About...* (see Figure 12)

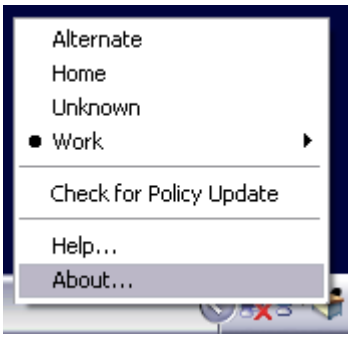

Figure 12: Open About

Step 4: Left-click to display the About window

Step 5: Click *Password Override* to display the password window (see Figure 13)

Note:

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

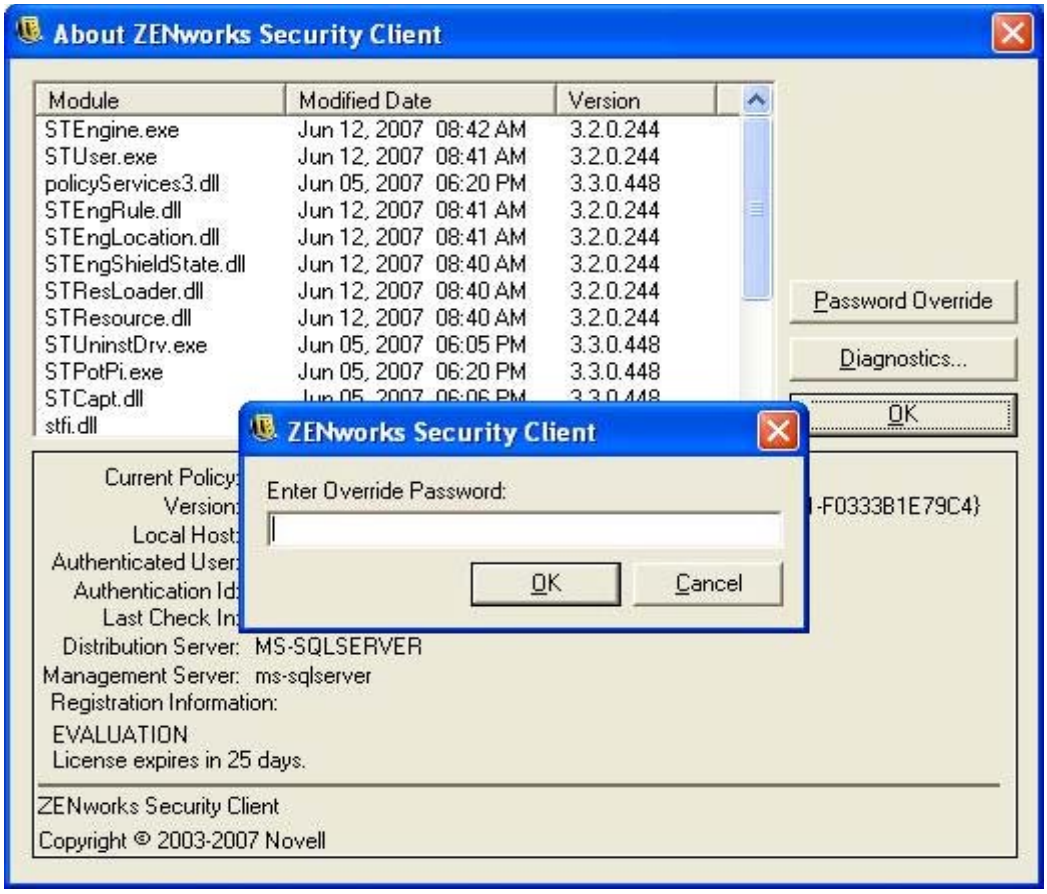

Figure 13: Password Window

Step 6: Enter the password key provided by your ESM Administrator.

Step 7: Click OK. The current policy will be replaced with a default, All Open policy for the designated time.

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

Diagnostics

Novell provides diagnostics tools to allow the administrator to troubleshoot ZSC issues. Your ESM administrator will guide you through the diagnostics process.