Novell ZENworks Endpoint Security Client 4.0

Novell®

January 15, 2009

1 Overview

The issues included in this document are identified for Novell® ZENworks® Endpoint Security Client 4.0, which is a client release to support Microsoft* Windows* Vista* with Support Pack 1 running in 32-bit mode.

◆ For installing the Endpoint Security Client 4.0, see the *ZENworks Endpoint Security Client 4.0 User Guide*.

The Endpoint Security Client 4.0 uses the ZENworks Endpoint Security Management 3.5 Server and Management Console. You can now manage Windows XP with the 3.5 client and Windows Vista with the 4.0 client.

◆ For ZENworks Endpoint Security Management Server installation instructions, see the *ZENworks Endpoint Security Management Installation Guide*.

◆ For ZENworks Endpoint Security Management administrative tasks, see the *ZENworks Endpoint Security Management Administration Guide*.

2 Features That Are Not Supported in the Endpoint Security Client 4.0

The following features that are available in Security Client 3.5 are not supported in Security Client 4.0:

◆ Client Self Defense (except stopping of client through service manager)

◆ USB Connectivity policy

◆ ZENworks Security Client (ZSC) Update policy

◆ Application Control (both Network Access and Application Execution)

◆ Encryption of My Documents folder

◆ Scripting

◆ Integrity and Remediation Rules

◆ Compliance Reporting and Alerts

◆ Modem/dialup settings for access control (Communication Hardware policy) and location awareness (Network Environments)

◆ Wireless control except ad hoc enforcement (Wireless Control policy) and approved wireless adapters (Communication Hardware policy)

◆ Managed access points (Wi-Fi Management)

- Authentication Timeout and Adapters (VPN Enforcement policy)
- Manual change, by user, of firewalls in a location (Location settings)
- Multiple firewalls visible for a single location; only default firewall available to user (Location setting)

The following features work differently in Security Client 4.0 than in Security Client 3.5:

- System Tray Icon: The mouse-over information for the icon shows only policy and location information.
- Connection Management: Wired connections are not valued above wireless connections.

3 Known Issues

This section contains information about Endpoint Security Client 4.0 issues that might occur.

3.1 ZENworks Endpoint Security Client 4.0

This section contains information about the issues that might occur when using the ZENworks Endpoint Security Client 4.0 on a Windows Vista managed device.

3.1.1 Vista Firewall Is Not Disabled

Endpoint Security Client 4.0 does not disable Windows Vista's firewall configurations. It is recommended to use either the ZENworks Endpoint Security Management firewall or native Vista, not both. Vista's firewall can be disabled through GPO policies, or simply set the Vista firewall to "All Open." See TID #7002061 on the Novell Support Web Site (http://www.novell.com/support/microsites/microsite.do).

3.1.2 Incorrect Information In the Encryption Dialog Box

With an encryption policy, the encryption client dialog box does not initially display correct information about the Safe Harbor folders in the policy. This is because of a location change. It displays incorrect information for about two minutes. While this is happening, encryption is working properly, and only the display is incorrect.

After the client synchronizes, the information is correctly displayed. See TID #7002060 on the Novell Support Web Site (http://www.novell.com/support/microsites/microsite.do).

3.1.3 After Installing the Endpoint Security Client 4.0, the User Is Prompted To Log In To the Client

Users might be prompted to enter credentials to log in to the ZENworks Endpoint Security Management Server. This happens only once after installing the Endpoint Security Client 4.0. The causes include the following:

- The back-end server is on Novell eDirectory.
- The user logs on locally to the computer and not through the domain.
- The user logs on through NetWare®, not Microsoft Windows.
- The administrator has not configured the search context correctly on the infrastructure's Authentication Directories setup to include containers where the user or computer resides.
- The computer or user SID is no longer valid and a new one needs to be created.
- You are using Directory Services for Windows instead of communicating directly with eDirectory or Active Directory*.
- If the ZENworks Configuration Management Client uses the Dynamic Local User (DLU) feature with Volatile User enabled.

NOTE: If more than one eDirectory user is logging into a machine with the same local administrator user account, all users receive the same policy. Each eDirectory user must have his or her own local user account.

3.2 Installation

Novell Endpoint Security Client 4.0 is the client release to support Microsoft Vista Support Pack 1 running in 32-bit mode.

This section contains information about the issues that might occur when you install Endpoint Security Client 4.0.

- "Windows Server 2008 Is Not Supported" on page 3
- "The Windows Vista 64-bit Operating System Is Not Supported" on page 3

3.2.1 Windows Server 2008 Is Not Supported

Endpoint Security Client 4.0 components do not support Microsoft Windows Server* 2008.

3.2.2 The Windows Vista 64-bit Operating System Is Not Supported

ZENworks Endpoint Security Management does not run on the Windows Vista 64-bit operating system. We do support a 64-bit CPU on a 32-bit OS.

3.3 Controlling Communications Hardware

This section contains information about the issues that might occur when you use Endpoint Security Client 4.0 to control communications hardware.

- ◆ "Supported Devices" on page 4
- ◆ "Determining If a Device Is Supported" on page 4

3.3.1 Supported Devices

Most Widcom-based Bluetooth* solutions are supported. Supported devices include the following:

- ◆ Devices using the Microsoft standard Type GUID {e0cbf06cL-cd8b-4647-bb8a263b43f0f974}
- ◆ Devices using the Dell* USB Bluetooth module with the Dell Type GUID {7240100F-6512-4548-8418-9EBB5C6A1A94}
- ◆ Devices using the HP*/Compaq* Bluetooth Module with the HP Type GUID {95C7A0A0L-3094-11D7-A202-00508B9D7D5A}

3.3.2 Determining If a Device Is Supported

1 Open Regedit.

2 Navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class`.

3 Search for the type GUID Keys listed in Section 3.3.1, "Supported Devices," on page 4. The Microsoft key must have more than one subkey to be valid.

3.4 Data Encryption and Performance

Data encryption is only supported on "non-system" volumes and removable storage devices. This section contains information about the performance issues that might occur when you use data encryption in Endpoint Security Client 4.0.

- ◆ "Copying Folders To a Removable Storage Device with Encryption Enabled" on page 4
- ◆ "Applications Saving Directly To an Encrypted RSD Cause Performance Issues" on page 4
- ◆ "Copying Multiple Files from an RSD-encrypted Drive To a Safe Harbor Encrypted Fixed Drive" on page 5

3.4.1 Copying Folders To a Removable Storage Device with Encryption Enabled

Copying folders containing multiple files and folders to a removable storage device (RSD) with encryption enabled takes longer for the copy. For example, in our testing, a 38 MB folder took between five and six minutes to copy.

3.4.2 Applications Saving Directly To an Encrypted RSD Cause Performance Issues

A potential machine performance impact exists when applications save directly to an encrypted RSD (depending on the file write size used by the application).

3.4.3 Copying Multiple Files from an RSD-encrypted Drive To a Safe Harbor Encrypted Fixed Drive

Copying multiple files from an RSD-encrypted drive to a Safe Harbor encrypted fixed drive can take considerable time.

3.5 Firewalls

This section contains information about the issues that might occur when you use a firewall and Endpoint Security Client 4.0.

- "Using Dynamically Assigned Ports" on page 5
- "Using FTP Sessions" on page 5

3.5.1 Using Dynamically Assigned Ports

In most modes, the ZENworks firewall does not allow incoming connections to dynamically assigned ports. If an application requires an incoming connection, the port must be static and a firewall setting of *Open* must be created to allow the incoming connection. If the incoming connection is from a known remote device, an ACL can be used.

3.5.2 Using FTP Sessions

The default *All Adaptive (Stateful)* firewall setting does not allow an active FTP session; you must use passive FTP instead. A good reference to explain active versus passive FTP is the Slacksite Web site (http://slacksite.com/other/ftp.html).

3.6 Localization

This section contains information about the localization issues in Endpoint Security Client 4.0.

- The client uninstall if an encryption policy is active and the MSI property is set (SESMSG=1).

3.7 Network Environments

This section contains information about the issues that might occur when you use Endpoint Security Client 4.0 to manage networks.

3.7.1 Using adapter-specific network environments

Adapter-specific network environments that become invalid can cause the client to continue to switch between the location the environment is assigned to, and Unknown. To prevent this, set the adapter type of the network environment to an adapter that is enabled at the location.

3.8 Storage Devices

This section contains information about the issues that might occur when you use Endpoint Security Client 4.0 to manage storage devices.

- "Controlling USB Devices" on page 6
- "Controlling CD/DVD Devices" on page 6

3.8.1 Controlling USB Devices

Not all USB disk drives have serial numbers, some disk drive serial numbers depend on the port and drive combination, and some are not unique. Most thumb drives have what appears to be a unique serial number.

3.8.2 Controlling CD/DVD Devices

If a CD/DVD burning device is added after the ZENworks Security Client is installed, policies specifying Read Only to that device are not enforced if you are using third-party burning software such as Roxio* or Nero*.

You can also have a conflict if GPO policies try to control the CD/DVD burning device, so use only one method to control devices. This also applies to floppy drive controllers.

3.9 VPN Connections

This section contains information about the issues that might occur when you use Endpoint Security Client 4.0 to manage VPN connections.

3.9.1 Configuring VPN settings

- ZENworks Endpoint Security Management does not support using a split tunnel when configuring VPN settings.
- ZENworks Endpoint Security Management does not automatically add a VPN IP to the firewall ACL. You must manually add it to the "VPN Switch To" location firewall.

4 Documentation Conventions

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

A trademark symbol ($^{\circledR}$, ™, etc.) denotes a Novell trademark; an asterisk (*) denotes a third-party trademark

5 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