Novell ZENworks Endpoint Security Management 3.5

Novell®

March 31, 2009

1 Overview

The issues included in this document were identified for Novell® ZENworks® Endpoint Security Management 3.5.

- For installation instructions, see the *ZENworks Endpoint Security Management Installation Guide*.
- For administrative tasks, see the *ZENworks Endpoint Security Management Administration Guide*.

2 Known Issues

This section contains information about ZENworks Endpoint Security Management issues that might occur.

- Section 2.1, "Installation," on page 2
- Section 2.2, "Application Blocking," on page 3
- Section 2.3, "Client Self Defense," on page 4
- Section 2.4, "Controlling Communications Hardware," on page 4
- Section 2.5, "Data Encryption and Performance," on page 5
- Section 2.6, "Using the New Directory Service Wizard," on page 6
- Section 2.7, "Configuring the Directory Service for Novell eDirectory," on page 7
- Section 2.8, "Configuring the Directory Service for Microsoft Active Directory," on page 8
- Section 2.9, "Ensuring Endpoint Security," on page 8
- Section 2.10, "Firewalls," on page 8
- Section 2.11, "Localization," on page 9
- Section 2.12, "Management Console," on page 9
- Section 2.13, "Network Environments," on page 10
- Section 2.14, "Reports," on page 10
- Section 2.15, "Storage Devices," on page 11
- Section 2.16, "Uninstalling," on page 11
- Section 2.17, "Upgrading," on page 12
- Section 2.18, "VPN Connections," on page 13

- Section 2.19, “Wi-Fi Connectivity,” on page 13
- Section 2.20, “Endpoint Security Client 3.5,” on page 14

2.1 Installation

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

- “Windows Server 2008 is not supported” on page 2
- “Installing the Management Console on a device in Active Directory” on page 2
- “The Windows XP 64-bit operating system is not supported” on page 2
- “Using SQL 2005 and SQL 2008 with the ZENworks Endpoint Security Management Server” on page 2
- “SQL Server Express 2005 and SQL Server Express 2008 are not supported” on page 2
- “Using special characters in the password for the DS_STDSDB_User account” on page 3
- “If you use SQL Server 2005, ensure that the Domain Security policy has disabled the Password policy that ensures that the “Password must meet complexity requirements”” on page 3
- “ZENworks Endpoint Security Management does not work with Novell’s Directory Services for Windows” on page 3

2.1.1 Windows Server 2008 is not supported

ZENworks Endpoint Security Management Server components will not install on Microsoft* Windows Server* 2008 because of the newer IIS version.

2.1.2 Installing the Management Console on a device in Active Directory

The device you install the Management Console on must be a member of the Active Directory* domain you are configuring or at least have a trust relationship with the domain.

2.1.3 The Windows XP 64-bit operating system is not supported

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

2.1.4 Using SQL 2005 and SQL 2008 with the ZENworks Endpoint Security Management Server

For information about using SQL 2005 and SQL 2008 with ZENworks Endpoint Security Management, see TID 3466284 (http://www.novell.com/support/supportcentral/supportcentral.do?id=m1).

2.1.5 SQL Server Express 2005 and SQL Server Express 2008 are not supported

ZENworks Endpoint Security Management servers and the stand-alone Management Console are not supported on SQL Server* Express 2005 and SQL Server Express 2008.

2.1.6 Using special characters in the password for the DS_STDSDB_User account

If you use special characters in the password for the DS_STDSDB_User account, the special characters are changed in the configuration files. For example, an @ gets changed to an A in the configuration files. The communication between the server and the database works as expected. However, when you troubleshoot with OSQL, you must use the configuration file passwords, not the ones you specified with special characters.

2.1.7 If you use SQL Server 2005, ensure that the Domain Security policy has disabled the Password policy that ensures that the "Password must meet complexity requirements"

When connecting to SQL Server 2005, ensure that the Domain Security policy has disabled the Password policy that ensures that the password must meet complexity requirements. After installation, you can re-enable this policy because the accounts created in ZENworks Endpoint Security Management for SQL do not have expiration dates.

This policy causes SQL accounts being created in SQL Server 2005 to fail because of the restriction. You cannot install ZENworks Endpoint Security Management unless this policy is disabled. If this policy is not disabled when the DS_STDSDB_User account is created, you receive a message indicating that the password entered for STDSDB is incorrect.

Workaround: You can manually create the user accounts by using the configuration files.

2.1.8 ZENworks Endpoint Security Management does not work with Novell's Directory Services for Windows

For further information, contact Novell Support.

2.2 Application Blocking

This section contains information about the issues that might occur when you use application blocking in ZENworks Endpoint Security Management.

- "Blocking an active application" on page 3
- "Blocking network access" on page 3
- "Blocking an application that is using a network share" on page 4
- "Blocking an application started from a network drive share" on page 4
- "Blocking applications and Safe Mode" on page 4

2.2.1 Blocking an active application

Blocking an application from execution does not shut down an application that is already open on the endpoint.

2.2.2 Blocking network access

Blocking network access to an application does not stop access to an application that is actively streaming network data to the endpoint.

2.2.3 Blocking an application that is using a network share

Blocking network access to an application does not stop access to an application that is getting data from a network share.

2.2.4 Blocking an application started from a network drive share

Blocking execution of an application still launches if it is started from a network drive share that has System blocked from read access.

2.2.5 Blocking applications and Safe Mode

Network Application Control does not function if the device is booted to Safe Mode with Networking.

2.3 Client Self Defense

This section contains information about the issues that might occur when you use Client Self Defense in ZENworks Endpoint Security Management.

- "Client Self Defense requires an uninstall password" on page 4
- "GPO Security policies and third-Party software might cause CPU spiking" on page 4

2.3.1 Client Self Defense requires an uninstall password

For full Client Self Defense to be in effect, an uninstall password must be implemented.

2.3.2 GPO Security policies and third-Party software might cause CPU spiking

It is possible that an interaction with GPO security policies or third-party software that controls access to the registry, files and folders, WMI, and process or service information could produce CPU spiking. GPO security policies that prohibit the ZENworks Endpoint Security Management Client from reading and resetting registry keys the product requires could produce CPU spiking. Antivirus and spyware software might need to allow `STEngine.exe` and `STUser.exe` to run unrestricted.

2.4 Controlling Communications Hardware

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

- "Supported devices" on page 4
- "Determining if a device is supported" on page 5

2.4.1 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; the Dell Type GUID {7240100F-6512-4548-8418-9EBB5C6A1A94}
- Devices using the HP*/Compaq* Bluetooth Module; the HP Type GUID {95C7A0A0L-3094-11D7-A202-00508B9D7D5A}

2.4.2 Determining if a device is supported

1. Open Regedit.
2. Navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class`.
3. Search for the listed type GUID Keys (listed in Section 2.4.1, "Supported devices," on page 4). The Microsoft key must have more than one subkey to be valid.

2.5 Data Encryption and Performance

This section contains information about the performance issues that might occur when you use data encryption in ZENworks Endpoint Security Management.

- "Using data encryption on Windows 2000 SP4 and Windows XP SP1" on page 5
- "Using the ZENworks File Decryption Utility" on page 5
- "Copying folders to a removable storage device with encryption enabled" on page 5
- "Applications saving directly to an encrypted RSD cause performance issues" on page 6
- "Selecting safe harbors on the system volume" on page 6
- "Encrypting the My Documents folder" on page 6
- "Copying multiple files from an RSD-encrypted drive to a safe harbor encrypted fixed drive" on page 6
- "Enabling safe harbor causes two reboots" on page 6
- "Safely Removing a Busy RSD" on page 6

2.5.1 Using data encryption on Windows 2000 SP4 and Windows XP SP1

ZENworks Endpoint Security Management is supported on Windows XP SP2 because of required Filter Manager support. ZENworks Endpoint Security Management installs on Windows 2000 SP4 and XP SP1, but when those operating systems receive an encryption policy, the encryption requests are ignored and an alert is sent to the administrator.

2.5.2 Using the ZENworks File Decryption Utility

The ZENworks File Decryption Utility is used to extract protected data from the `Shared Files` folder on encrypted removable storage devices. This simple tool can be sent by the user (although it cannot be placed on the removable storage device) to a third party so the third party can access the files in the `Shared Files` folder.

The utility is found on the product DVD or on the Novell ZENworks Endpoint Security Management Web site (ftp://ftp.novell.com/outgoing/STDECRYPT-NOVELL-Release-3.5.zip).

For more information, see "Using the ZENworks File Decryption Utility" in the *ZENworks Endpoint Security Management Administration Guide*.

2.5.3 Copying folders to a removable storage device with encryption enabled

Copying folders containing multiple files and folders to a removable storage device 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.

2.5.4 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).

2.5.5 Selecting safe harbors on the system volume

A potential machine performance impact exists if safe harbors are selected on the system volume.

2.5.6 Encrypting the My Documents folder

Encryption of the `My Documents` folder gives only the active user access to decrypt files in his or her `My Documents` folder (not anyone else's folder).

2.5.7 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.

2.5.8 Enabling safe harbor causes two reboots

Two reboots are required when encryption is first activated in a policy, and again when either safe harbor or removable storage encryption is activated (if activated separately from encryption activation). For example, when an encryption policy is applied for the first time, two reboots are required: one reboot to initialize the drivers and another reboot to put any safe harbors into encryption. If additional safe harbors are subsequently selected after the policy has been applied, only one reboot is required to put the safe harbor into policy.

2.5.9 Safely Removing a Busy RSD

If you try to safely remove a removable storage device and you receive a message stating that the device is busy, go ahead and remove the device. No data loss will occur. The message is caused by resident encryption processes.

2.6 Using the New Directory Service Wizard

This section contains general information that is general to configuring directory services using the New Directory Service Wizard.

For specific information about configuring ZENworks Endpoint Security Management for Novell eDirectory™ or Microsoft Active Directory*, see Section 2.7, “Configuring the Directory Service for Novell eDirectory,” on page 7 or Section 2.8, “Configuring the Directory Service for Microsoft Active Directory,” on page 8.

2.6.1 Using the Back button in the New Directory Service Wizard

Using the *Back* button in the New Directory Service Configuration Wizard currently causes you to lose data and causes the synchronization to fail. You should start over if you make a mistake.

2.7 Configuring the Directory Service for Novell eDirectory

This section contains information about configuring directory services for Novell eDirectory by using the New Directory Service Wizard. For more information, see "Configuring the Directory Service for Novell eDirectory" in the *ZENworks Endpoint Security Management Administration Guide*.

- "Use ports 389 or 636 with Novell eDirectory" on page 7
- "Using Directory Services for Windows with ZENworks Endpoint Security Management and eDirectory" on page 7
- "Clients can be deployed with user-based but not computer-based policies" on page 7
- "Clients prompted to log in to the Server for their first check-in" on page 7
- "Using ZENworks Configuration Management with eDirectory and DLU causes the ZENworks Endpoint Security Management Client to prompt for a password" on page 7
- "Moving a user in the eDirectory tree causes problems" on page 7

2.7.1 Use ports 389 or 636 with Novell eDirectory

During configuration of the directory service for eDirectory, you must use ports 389 or 636 if you are using encryption with TLS/SSL.

2.7.2 Using Directory Services for Windows with ZENworks Endpoint Security Management and eDirectory

You cannot currently use ZENworks Endpoint Security Management with eDirectory using Directory Services for Windows.

2.7.3 Clients can be deployed with user-based but not computer-based policies

During Endpoint Security Client 3.5 installation, if you are using Novell eDirectory as your directory service, use the User-Based Policy option.

2.7.4 Clients prompted to log in to the Server for their first check-in

Clients are prompted to log in to the ZENworks Endpoint Security Management Server for their first check-in. Users must specify the username and password but not the context.

2.7.5 Using ZENworks Configuration Management with eDirectory and DLU causes the ZENworks Endpoint Security Management Client to prompt for a password

If you are using ZENworks Configuration Management with Novell eDirectory and DLU with Volatile User enabled, the clients are prompted for a credential from the ZENworks Endpoint Security Management Server each time they log into their Windows device. This is because the users' unique numbers (like a SID in Windows) change on each boot.

2.7.6 Moving a user in the eDirectory tree causes problems

Currently, the ZENworks Endpoint Security Management Server does not have the ability to follow a user if it is moved in the eDirectory tree.

Workaround: Configure a new user in ZENworks Endpoint Security Management.

2.8 Configuring the Directory Service for Microsoft Active Directory

This section contains information about configuring the directory service for Microsoft Active Directory by using the New Directory Service Wizard. For more information, see "Configuring the Directory Service for Microsoft Active Directory".

- "Domain Controller for Active Directory configuration requirements" on page 8
- "Ensure that you are logged in to the domain before configuration" on page 8
- "Moving a user or computer in the domain causes problems" on page 8

2.8.1 Domain Controller for Active Directory configuration requirements

The Domain Controller for Active Directory configurations must be running Windows Server 2000 with SP4, Windows Server 2003, or Windows Server 2008.

If a Windows Server 2008 Domain Controller is down when you run the Directory Services Wizard, the wizard might error out. If this occurs, you set the port to 389 when running the wizard.

2.8.2 Ensure that you are logged in to the domain before configuration

You must be logged in to the domain before configuring the directory service for Active Directory.

2.8.3 Moving a user or computer in the domain causes problems

Currently, the ZENworks Endpoint Security Management Server does not have the ability to follow a user or computer if it is moved in the Active Directory domain.

Workaround: Configure a new user or computer in ZENworks Endpoint Security Management.

2.9 Ensuring Endpoint Security

This section contains information about the issues that might occur when you use antivirus and spyware rules in ZENworks Endpoint Security Management.

2.9.1 Using Antivirus and Spyware rules

Some of ZENworks Endpoint Security Management preinstalled antivirus and spyware rules might need to be modified for a specific or custom-installed version of the antivirus or spyware software.

2.10 Firewalls

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

- "Using dynamically assigned ports" on page 9
- "Using FTP sessions" on page 9

2.10.1 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.

2.10.2 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).

2.11 Localization

This section contains information about the localization issues in ZENworks Endpoint Security Management.

- There are untranslated items and descriptions in Endpoint Auditing Reporting.
- There are untranslated strings in the Reports dialog box in *Endpoint Auditing:Reporting*.
- There is untranslated text in the tree view under the *Reporting* tab.
- There is a truncated radio button when selecting the type of installation in the Management Service installer.
- There are truncated reports in the management console.
- The Policy Distribution Service default install path includes Chinese characters.
- There is an untranslated tab when canceling installation of the Endpoint Security Client 3.5.
- The description of application event logs for `STEngine` is null in Chinese Traditional and Chinese Simplified.
- The uninstall password prompt is in English.

2.12 Management Console

This section contains information about the issues that might occur when you use the Management Console in ZENworks Endpoint Security Management.

2.12.1 Using the Management Console in Active Directory

If you are using Microsoft Active Directory as your directory service, you must be logged in to the domain to use the Management Console.

2.12.2 Viewing error messages

Clicking an error message in the Management Console does not always display the correct screen. This limitation manifests itself on screens with multiple tabs.

2.12.3 Potential exception related to associating an existing integrity rule

A potential exception related to associating an existing integrity rule occurs if you do not verify all the triggers, events, firewalls, etc, before publishing the policy. The policy fails and the following error displays:

```
"Senforce.PolicyEditor.Bll.FatalErorException:component_value table in
unknown state" "at
Senforce.PolicyEditor.UI.Forms.PolicyForm.SavePolicy()" "at
Senforce.PolicyEditor.UI.Forms.MainForm.PublishPolicy()"
```

Workaround: Ensure that all options are configured and click *Save Policy* on each page in the Management Console before continuing to the next page.

2.12.4 Network devices that install as dual devices might not have the policy applied

Network devices that install as dual devices (for example, Modem and Wireless (802.11)) might not appear in the `HKLM\\Software\Microsoft\Windows NT\\Network Cards` registry entry and consequently do not have a policy applied to them (firewall or adapter control).

2.12.5 The Permissions options and controls are not available within the Management Console

The Permissions options and controls are not currently working correctly, so the Permissions options and controls have been removed. Removing Management Console permissions from a user does not take effect until the user's Management Console session is terminated.

Workaround: Control permissions by setting a password to control user access to the computer running the Management Console.

2.13 Network Environments

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

2.13.1 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.

2.14 Reports

This section contains information about using reports in ZENworks Endpoint Security Management.

- Adherence reports have incorrect or missing data.
- Policy reports have missing data.

2.15 Storage Devices

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

2.15.1 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.

2.15.2 Controlling CD/DVD devices

If a CD/DVD burning device is added after the Endpoint Security Client 3.5 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*.

2.15.3 Not able to save Storage Device Control settings by location in the Management Console

If you are configuring Storage Device Control settings on the *Locations* tab, you cannot save your settings. Contact your support representative for a patch and instructions to fix this problem. This problem does not exist when setting Storage Device Control settings on the *Global Policy Settings* tab.

2.15.4 Problem with FreeUSB Drive

At insertion of a FreeUSB 4GB (or larger) drive, the Windows operating system flashes a blue screen and shuts down. Novell has received one reported issue of this problem but has been unable to reproduce it. If you encounter this issue, please contact Novell Technical Services.

2.16 Uninstalling

This section contains information about the issues that might occur when uninstalling ZENworks Endpoint Security Management.

2.16.1 Uninstalling ZENworks Endpoint Security Management with safe harbor enabled

With safe harbor enabled and uninstalling with a policy, you will be prompted on uninstall to decrypt files on a fixed disk. After clicking *OK*, you might get a message that says `Remove Directory Failed`. This message does not go away.

Workaround: You must reboot the device and rerun the uninstallation program.

2.17 Upgrading

This section contains information about the issues that might occur when you upgrade ZENworks Endpoint Security Management from a previous version of the software.

2.17.1 Contact Customer Support before upgrading

You should contact your support representative for assistance with any upgrade.

2.17.2 No support for server upgrades

Because of fixes and new features in this release, upgrading the ZENworks Endpoint Security Server is not supported. Contact your support representative for help in upgrading your system. The support representative can help you retain security policies from your previous version.

2.17.3 Previous versions of the Senforce Endpoint Security Suite's Policy Editor Is not supported in version 3.5

Previous versions of the Senforce® Endpoint Security Suite's Policy Editor cannot run against a ZENworks Endpoint Security Management 3.5 Server installation.

2.17.4 Upgrading a Senforce 3.2 policy loses the password override

Upgrading an existing Senforce Endpoint Security Suite 3.2 policy to a 3.5 version policy loses the password override. If a 3.2 policy has a password override, it must be re-entered in the 3.5 policy before it is published. This is by design.

2.17.5 Upgrading the Endpoint Security Client on managed devices

To manually upgrade the Endpoint Security Client on managed devices, use the `-stupgrade` switch, as in the following example:

```
setup.exe /V"STUPGRADE=1"
```

If you upgrade the Endpoint Security Client 3.5 by using a ZENworks Endpoint Security Management policy, this switch is not needed.

2.17.6 No support for client upgrades from Senforce client builds

You cannot upgrade a Senforce Endpoint Security client to a Novell Endpoint Security Client 3.5.

2.18 VPN Connections

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

2.18.1 Configuring VPN settings

ZENworks Endpoint Security Management does not support Split Tunnel when configuring VPN settings.

2.19 Wi-Fi Connectivity

This section contains information about the issues that might occur when you use ZENworks Endpoint Security Management to manage Wi-Fi connections.

- "Displaying Wi-Fi transmissions and Disable Adapter Bridging custom messages to users" on page 13
- "Using WPA access points" on page 13
- "Controlling cellular phones" on page 13
- "Not able to save Wi-Fi settings by location in the Management Console" on page 13
- "Unsupported Wi-Fi devices" on page 14

2.19.1 Displaying Wi-Fi transmissions and Disable Adapter Bridging custom messages to users

Disable Wi-Fi transmissions and Disable Adapter Bridging messages are only shown if the end user tries to bypass the enforcement. They are enforced without a warning message.

2.19.2 Using WPA access points

WPA access points can be identified for filtering (we do not differentiate between WPA and WPA2). ZENworks Endpoint Security Management distributes WEP keys only.

2.19.3 Controlling cellular phones

You might not be able to control Wireless connections made through cellular phones by using Wi-Fi control features in the Management Console. These devices are generally treated as modems by the operating system and, therefore, need corresponding policy changes to control them (for example, disable modems when wired through scripting).

2.19.4 Not able to save Wi-Fi settings by location in the Management Console

If you are configuring Wi-Fi settings on the *Locations* tab, you cannot save your settings. Contact your support representative for a patch and instructions to fix this problem. This problem does not exist when setting Wi-Fi settings on the *Global Policy Settings* tab.

2.19.5 Unsupported Wi-Fi devices

Certain outdated wireless adapters do not function correctly when managed by ZENworks Endpoint Security Management. These include the following devices:

- Orinoco* 8470-WD Gold
- 3Com* 3CRWE62092B
- Dell True Mobile 1180
- Proxim* Orinoco 802.11bg combo card

2.20 Endpoint Security Client 3.5

This section contains information about the issues that might occur when using the Endpoint Security Client 3.5 on a managed device. For issues when using the Endpoint Security Client 4.0 with Windows Vista, see the Novell ZENworks Endpoint Security Client 4.0 Readme.

- "Two Endpoint Security Client icons display in the Windows Taskbar" on page 14
- "After installing the Endpoint Security Client 3.5, the user is prompted to log in to the client" on page 14

2.20.1 Two Endpoint Security Client icons display in the Windows Taskbar

When you boot your Endpoint Security Client 3.5 machine, you might see two Endpoint Security Client icons in the Windows taskbar. Mouse over one of the icons and it disappears.

2.20.2 After installing the Endpoint Security Client 3.5, the user is prompted to log in to the client

The users might be prompted to enter credentials (username or short or full LDAP context) to log in to the ZENworks Endpoint Security Management Server. This happens only once and only after installing the Endpoint Security Client 3.5. The causes for this issue 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 set up 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 get the same policy. Each eDirectory user must have his or her own local user account.

3 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 (® , ™, etc.) denotes a Novell trademark; an asterisk (*) denotes a third-party trademark

4 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. Please refer to 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.

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

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