

March 17, 2009

These are the release notes for the Sentinel 6.1.1.0 (6.1 SP1) Release.

- ◆ [Section 1, “Overview,” on page 1](#)
- ◆ [Section 2, “New Features in Sentinel 6.1,” on page 2](#)
- ◆ [Section 3, “Prerequisites,” on page 2](#)
- ◆ [Section 4, “Installation,” on page 3](#)
- ◆ [Section 5, “Sentinel Database Patch Installation,” on page 4](#)
- ◆ [Section 6, “Post-Installation,” on page 7](#)
- ◆ [Section 7, “Defects Fixed in Sentinel 6.1 Release,” on page 8](#)
- ◆ [Section 8, “Known Issues in Sentinel 6.1.1.0 Release,” on page 12](#)
- ◆ [Section 9, “Documentation Conventions,” on page 12](#)
- ◆ [Section 10, “Legal Notices,” on page 13](#)

1 Overview

The information in this Release Note file pertains to Novell Sentinel™ 6.1.1.0, which provides a real-time, holistic view of security and compliance activities, while helping customers monitor, report, and respond automatically to network events across the enterprise.

This Service Pack will apply the latest software fixes and enhancements to an existing installation of Sentinel 6.1, including the updates in Sentinel 6.1 Hotfix 1 (6.1.0.1). Sentinel 6.1 must already be installed before applying this Service Pack.

The Service Pack must be installed on all existing Sentinel 6.1 installation machines, client and server. This includes machines with Sentinel Server the Correlation Engine, Sentinel Database, Collector Manager, Sentinel Control Center, Collector Builder, and Sentinel Data Manager.

This Service Pack is mandatory for all users who subscribe to the Advisor data service.

1.1 Prerequisites

- ◆ If Sentinel is not yet installed, it must be installed using the Sentinel 6.1.0.0 installer. Please see the Sentinel Installation Guide for instructions.
- ◆ If Sentinel 5.x is installed, it must be upgraded to Sentinel 6.1.0.0 using the upgrade installer. Please see the Patch Installation Guide for instructions.
- ◆ If Sentinel 4.x is installed, Sentinel 6.1.0.0 must be installed using the Sentinel 6.1.0.0 installer. Some data can be migrated to the Sentinel 6.1.0.0 installation. Please see the Patch Installation Guide for instructions.

The full product documentation and the most recent version of this file are available at the [Novell Sentinel Documentation Web site \(http://www.novell.com/documentation/sentinel61\)](http://www.novell.com/documentation/sentinel61).

2 New Features in Sentinel 6.1

This section explains the new features available in Sentinel 6.1.

- ♦ [Section 2.1, “New Features in Sentinel 6.1.1.0,” on page 2](#)
- ♦ [Section 2.2, “New Features in Sentinel 6.1 Hotfix 1,” on page 2](#)

2.1 New Features in Sentinel 6.1.1.0

Sentinel 6.1.1.0 is a maintenance release for Sentinel 6.1. In addition to bug fixes, it contains enhanced Advisor feature.

2.1.1 Advisor update

The 6.1.1.0 service pack installer deletes the old Advisor data, which has erroneous Advisor mappings, and enables you to start downloading the new Advisor data.

With the Sentinel 6.1.1.0 release, the existing Advisor download URL will be redirected to a server containing the new Advisor data. In order to continue to receive automatic updates of the latest Advisor data, you need to upgrade to Sentinel 6.1.1.0.

2.2 New Features in Sentinel 6.1 Hotfix 1

This section lists the features available in Sentinel 6.1 Hotfix 1 Release.

- ♦ **AUDIT_RECORD Table Partitioning** - The AUDIT_RECORD table is configured for partitioning and archiving for better table management.
- ♦ **Customizing Data and Time Format in Sentinel Control Center** - This feature gives the ability to customize the date/time format that is displayed in event tables in SCC. These event tables are the ones seen in Active Views, Historical Event Query, Offline Query, etc. By default, the date/time format will be based on the locale of the machine running SCC; however, the user can override this default by adding a property to the SentinelPreferences.properties file found in \$ESEC_HOME/config.

3 Prerequisites

The prerequisites depend on the Sentinel system version and platform. Read each section below carefully to determine whether the steps apply to your environment.

3.1 Back Up Sentinel System

This prerequisite applies to all Sentinel systems, regardless of version or platform.

It is highly recommended that a complete backup be made of the machines on which you are installing the service pack, including the Sentinel database. If this is not possible, then at a minimum a backup of the contents of the ESEC_HOME directory should be made. This will help protect your system against unexpected installation errors.

3.2 Back Up AUDIT_RECORD Table

This prerequisite is not necessary if you have already applied Sentinel 6.1 Hotfix 1 (6.1.0.1). It is necessary if Hotfix 1 has not been applied yet.

Starting with Sentinel 6.1 Hotfix 1, the AUDIT_RECORD table, which contains internal audit events for the Sentinel system, is configured for partitioning and archiving for better table management. Because the existing table is not partitioned or archived, the PatchDB script may fail if the AUDIT_RECORD table is too large relative to the amount of temporary tablespace available.

There are two approaches to ensure the PatchDB script runs successfully, depending on whether it is critical to your organization to preserve the data in the AUDIT_RECORD table.

- ♦ If the AUDIT_RECORD data is not important, truncate the AUDIT_RECORD table using the following SQL command:

```
TRUNCATE TABLE AUDIT_RECORD
```

- ♦ If the AUDIT_RECORD data is important and needs to be preserved, add more space to the temporary tablespace. The amount of space to be added depends on your environment; consult your Database Administrator (DBA) for adequate settings.

4 Installation

The instructions provided in this section are for installing Sentinel 6.1.1.0 Service Pack only. This Service Pack can be run against an existing installation of Sentinel™ 6.1.

Follow the below listed instructions to install the Service Pack for software and database:

- 1 Login to any machine which has Sentinel installed.
 - ♦ On Linux/Solaris, log in as root.
 - ♦ On Windows Vista, log in as any user unless User Access Control is disabled. If User Access Control is disabled, you must log in as an Administrator.
 - ♦ On other (non-Vista) Windows systems, log in as an Administrator.
- 2 Verify that the environment variables for Sentinel are set by running one of the following commands:
 - ♦ On Linux/Solaris, echo \$ESEC_HOME
 - ♦ On Windows, echo %ESEC_HOME%
- 3 Extract the Service Pack zip file.
- 4 Close all Sentinel applications running on this machine, including:
 - ♦ Sentinel Control Center
 - ♦ Sentinel Collector Builder
 - ♦ Sentinel Data Manager
 - ♦ Solution Designer
- 5 Shut down the Sentinel services running on this machine:
 - ♦ On Windows, use *Windows Service Manager* to stop the “Sentinel” services.
 - ♦ On Linux/Solaris, run \$ESEC_HOME/bin/sentinel.sh stop

- 6 Open a command prompt. For most Windows systems and Linux/Solaris, you can use any method to open the prompt. For Windows Vista, you must open the command prompt as an administrator using the following instructions.
 - 6a Go to *Start > All Programs > Accessories*.
 - 6b Right-click *Command Prompt* and select *Run as administrator*.
 - 6c If User Access Control is enabled and you are logged in as a user with administrator privileges, a *User Access Control* window appears to notify you that “Windows needs your permission to continue”.
 - 6d Click *Continue*. If you are logged in as a user without administrative privileges, you will be prompted to authenticate as an administrative user.
- 7 On the command line, return to the extracted Service Pack top level directory and run the `service_pack` script to start the Service Pack installer:
 - ♦ On Windows: `.\service_pack.bat`
 - ♦ On Unix: `./service_pack.sh`
- 8 Press the <ENTER> key when prompted to start the Service Pack installation procedure.
- 9 After the installation completes, log out and log back in to apply environmental variable changes.
- 10 Repeat the above steps on every machine with Sentinel software installed. This is required for all machines with any Sentinel software, including both Sentinel server and client software.
- 11 Restart the Sentinel services on all machines:
 - ♦ On Windows, use *Windows Service Manager* to start the “Sentinel” services.
 - ♦ On *NIX, run `$ESEC_HOME/bin/sentinel.sh start`
- 12 This Service Pack also contains a mandatory patch for the Sentinel Database. Apply the database patch by performing the appropriate steps in the section below for the database platform you are using.

5 Sentinel Database Patch Installation

In addition to patching the Sentinel components, you must run a script to patch the database. The instructions are different depending on which database you have.

- ♦ [Section 5.1, “Sentinel Database Patch Installation on Oracle,” on page 4](#)
- ♦ [Section 5.2, “Sentinel Database Patch Installation on SQL Server,” on page 6](#)

5.1 Sentinel Database Patch Installation on Oracle

There are several prerequisites for applying the Oracle database patch. The machine and account from which the database patch is run must meet the following requirements:

- ♦ User has the Oracle client application `sqlplus` in its `PATH`.
- ♦ User has the environment variable `ORACLE_HOME` set to the directory where the Oracle software is installed.
- ♦ User must be a member of the Oracle "dba" group.
- ♦ User has the Java 1.5 executable `java` in its `PATH`.

TIP: The easiest way to apply the patch is to run the PatchDB script directly on the database server machine after logging in as a user that meets the requirements above. However, in some environments, local policies prohibit this (for example, you cannot install Java on the database server). In this situation, the script can be run from any other machine that meets the requirements stated above.

Any Sentinel 6.1 machine will already have the necessary version of Java, but the default Java installation done by Sentinel does not allow the oracle user access to the \$ESEC_HOME/jre directory. You can add the Oracle user to the esec group (for example, `groupmod -A oracle esec`), temporarily modify the permissions on the directory (for example, `chown -R oracle $ESEC_HOME/jre`), or install a second instance of Java.

If using a non-Sentinel machine, the Java version and PATH variable settings can be verified by running the `java -version` command from a command line:

If necessary, the PATH environment variable can be updated to include the java installation directory, for example:

```
export PATH=/opt/novell/sentinel6/jre/bin:$PATH
```

If Java is not installed on the non-Sentinel machine, the correct Java version [Java Runtime Environment (JRE) 5.0] can be downloaded from the [Sun Web site \(http://java.sun.com/javase/downloads/index_jdk5.jsp\)](http://java.sun.com/javase/downloads/index_jdk5.jsp).

After the prerequisites are met, use the following instructions to apply the database patch.

- 1 Log in to the database server or another machine with connectivity to the Sentinel Database as a user who meets the above installation prerequisites.
- 2 Verify that your machine meets the Java prerequisites.
- 3 Extract the Service Pack zip file.
- 4 On the command line, go into the Service Pack top level directory that was just extracted.
- 5 Change directories to the following directory under extracted top level directory:
 - ◆ db_patch/bin
- 6 Enter the `./PatchDb.sh` command.
- 7 Follow the prompts and enter the following information:
 - ◆ Hostname or static IP address of the Oracle Sentinel Database that you want to patch.
 - ◆ Port number of the Oracle Sentinel Database that you want to patch.
 - ◆ Database net service name.
 - ◆ Database service name of the Oracle Sentinel Database that you want to patch.
 - ◆ esecdba user password.

After you press *Enter* the final time, the script verifies the entered information and begins the database patch.

- 8 After the script is done applying the patch, check for any errors. If there are no errors, you are done with the Sentinel Database patch. If there are errors, resolve the errors and re-run the PatchDb utility.

9 Restart the Sentinel services on all machines:

- ♦ On Windows, use *Windows Service Manager* to start the “Sentinel” services.
- ♦ On *NIX, run `$ESEC_HOME/bin/sentinel.sh start`

5.2 Sentinel Database Patch Installation on SQL Server

The following steps must be performed on the machine with a Microsoft SQL Server database to prepare the database for 6.1.1.0. There is one main patch script for SQL Server (PatchDb.bat).

There are several prerequisites for applying the SQL Server patch.

- ♦ The patch must be copied to the machine that is running the Sentinel database.
- ♦ The patch must be run by using the Sentinel Database User credentials, or esecdba if you are using SQL Authentication.

Use the appropriate instructions depending on whether the database uses Windows authentication or SQL Server authentication.

- ♦ [“Installing Database Patch with Windows Authentication” on page 6](#)
- ♦ [“Installing Database Patch with SQL Server Authentication” on page 7](#)

5.2.1 Installing Database Patch with Windows Authentication

To install the database patch with Windows authentication, you need the credentials for the Sentinel Database User.

- 1** Log into the database machine as the Windows Domain user who is the Sentinel Database User.
- 2** Shut down the Sentinel Server processes (if this has not already been done).
- 3** Extract the Service Pack zip file (if this has not already been done).
- 4** Open a command prompt.
- 5** Change directories to the following directory under the extracted Service Pack directory:
 - ♦ `db_patch\bin`
- 6** Enter the `.\PatchDb.bat` command.
- 7** Follow the prompts and enter the following information:
 - ♦ Hostname or static IP address of the SQL Server Sentinel Database machine.
 - ♦ SQL Server Database instance name, if any.
 - ♦ Port number of the SQL Server database.
 - ♦ Name of the SQL Server database to patch (*ESEC* by default).
 - ♦ 1 for the Windows Authentication option.

After you press *Enter* the final time, the script verifies the entered information and proceeds if authentication is successful.
- 8** After the script has done applying the patch, check for any errors. If there are errors, resolve the errors and re-run the PatchDb utility.
- 9** After the patch runs with no errors, “Sentinel” services should be restarted.

5.2.2 Installing Database Patch with SQL Server Authentication

To install the database patch with SQL Server authentication, you need the credentials for the Sentinel Database User.

- 1 Log into the database machine as the Windows Domain user who is the Sentinel Database User.
- 2 Shut down the Sentinel Server processes (if this has not already been done).
- 3 Extract the Service Pack zip file (if this has not already been done).
- 4 Open a command prompt.
- 5 Change directories to the following directory under the extracted directory:
 - ♦ db_patch\bin
- 6 Enter the .\PatchDb.bat command.
- 7 Follow the prompts and enter the following information:
 - ♦ Hostname or static IP address of the SQL Server Sentinel Database machine.
 - ♦ SQL Server Database instance name, if any.
 - ♦ Port number of the SQL Server database.
 - ♦ Name of the SQL Server database to patch (ESEC by default).
 - ♦ 2 for the SQL Authentication option.
 - ♦ esecdba user password.

After you press *Enter* the final time, the script verifies the entered information and proceeds if authentication is successful.

- 8 After the script is done applying the patch, check for any errors. If there are errors, resolve the errors and re-run the PatchDb utility.
- 9 After the patch runs with no errors, “Sentinel” services should be restarted.

6 Post-Installation

After running the installer, some additional updates may be necessary.

By default, the Sentinel Control Center (SCC) uses a date and time format that is appropriate for the locale for which the Sentinel Control Center is configured, but that default can be overridden. For formatting details on customizing the date and time format in event field in Sentinel Control Center, see the [Java Web site \(http://java.sun.com/j2se/1.5.0/docs/api/java/text/SimpleDateFormat.html\)](http://java.sun.com/j2se/1.5.0/docs/api/java/text/SimpleDateFormat.html).

- 1 Edit the SentinelPreferences.properties file.

On Windows:

```
%ESEC_HOME%\config\SentinelPreferences.properties
```

On *NIX:

```
$/ESEC_HOME/config/SentinelPreferences.properties
```

- 2 Uncomment the following line and modify to customize date and time format for Sentinel Control Center event date/time fields.

```
com.eSecurity.Sentinel.event.datetimeformat=yyyy-MM-dd'T'HH:mm:ss.SSSZ
```

7 Defects Fixed in Sentinel 6.1 Release

This section lists the defects fixed in the Sentinel 6.1 Hotfix 1 and Sentinel 6.1.1.0 Release.

- ◆ [Section 7.1, “Defects Fixed in Sentinel 6.1.1.0 Release,” on page 8](#)
- ◆ [Section 7.2, “Defects Fixed in Sentinel 6.1 Hotfix 1,” on page 10](#)

7.1 Defects Fixed in Sentinel 6.1.1.0 Release

This section lists the defects fixed in the Sentinel 6.1.1.0 Release.

- ◆ [“Advisor fixes” on page 8](#)
- ◆ [“Performance enhancements” on page 9](#)
- ◆ [“General fixes” on page 9](#)

7.1.1 Advisor fixes

Table 1 *Defects fixed in Sentinel 6.1.1.0 Release*

Defects Number	Description
452478 and 452476	Issue: Advisor server is not downloading the latest CVE. FIXED: Data quality issues in the Advisor data feed have been fixed to provide more complete data and more accurate CVE information.
452473	Issue: Advisor feed failed to be processed by the client. FIXED: Advisor data feed have been fixed to provide complete data.
451602	Issue: Cannot reliably download feed files. FIXED: Improved error handling of corrupted file downloads in Advisor.
451723	Issue: A manual clean up of the partially downloaded file is required, If the Advisor download is interrupted in the middle (like downloading partial feed file). FIXED: Partial or corrupted feed files are re-downloaded by Advisor client and all feed files will be then processed.
451601	Issue: Cannot reliably download feed files. FIXED: Partial or corrupted feed files are re-downloaded by Advisor client and all feed files will be then processed.

7.1.2 Performance enhancements

Table 2 Defects fixed in Sentinel 6.1.1.0 Release

Defects Number	Description
465935	<p>Issue: Slow performance when querying mssql.</p> <p>FIXED: The file jtdsoverride.properties has been added, which contains JDBC driver properties that increase query performance on SQL Server. This properties file is only enabled in the configuration.xml file when using SQL Server. This fix does not affect Oracle.</p>
463818	<p>Issue: Sentinel Control Center (SCC) User Preferences time-out setting configurable.</p> <p>FIXED: A configurable setting has been added to SentinelPreferences.properties to set the user preferences load time-out in milliseconds. Increasing this value will fix login time-out issues over slow connections. This file includes comments with more information.</p>
452093	<p>Issue: Improve the performance of repeated javascript action execution.</p> <p>FIXED: Javascript actions are cached to improve performance.</p>
452092	<p>Issue: Improve the metadata manager performance for mapping and event transformations.</p> <p>FIXED: Performance improvements have been added to the mapping service.</p>

7.1.3 General fixes

Table 3 Defects fixed in Sentinel 6.1.1.0 Release

Defects Number	Description
470664	<p>Issue: HIST_EVENTS view is not updated when archived partition is imported back to database.</p> <p>FIXED: The HIST_EVENTS view is updated with the data from the imported partitions.</p>
468193	<p>Issue: Imported archived partitions are unsearchable.</p> <p>FIXED: The HIST_EVENTS SQL Server database view did not include data imported from archived event files. Therefore, imported data did not show up in reports. The stored procedure that generates the database view has been fixed so imported data is available in these scenarios.</p> <p>NOTE: The event data will still not show up in Historical Query or Offline Query.</p>

Defects Number	Description
474567	<p>Issue: javascripts end mail action only substitutes replacement strings on first execution of action.</p> <p>FIXED: Variable inputs to JavaScript plugin actions retained the variable input from the first correlated event to trigger the action. The action framework has been fixed to correctly accept variable input from all correlated events.</p>
468118	<p>Issue: Emailing large report results takes a very long time.</p> <p>FIXED: Errors sending email with large attachments (for example, incidents with associated data) have been resolved.</p>
468130	<p>Issue: Intermittent unique constraint violation on EVENTS table, particularly during startup. Improper shutdown resulted in attempts to insert duplicate events into the database, which resulted in the message "ERROR: duplicate key value violates unique constraint 'events_p_[date]_events_p_max_pk'"</p> <p>FIXED: Duplicate events are cleared from the buffer and no errors are generated.</p>
452471	<p>Issue: Collector debugger Upload function does not properly update the Package object of the Plugin object store in the DB.</p> <p>FIXED: Uploading a Collector through the Collector debugging interface properly loads information from the Collector's package.xml file.</p>
452112	<p>Issue: Instructions are needed to verify that Advisor and exploit detection are working from start to finish.</p> <p>FIXED: Advisor is now working properly. A section has been added to the "Testing the Installation" chapter of the Installation Guide to describe how to test Advisor.</p>
475280	<p>Issue: Active Views does not work properly if client time is not in sync with server time.</p> <p>FIXED: Client will now properly sync with server time.</p>

7.2 Defects Fixed in Sentinel 6.1 Hotfix 1

This table lists the defects fixed in the Sentinel 6.1 Hotfix 1 Release.

Table 4 Defects fixed in Sentinel 6.1 Hotfix 1 Release

Defects Number	Description
SEN-8471	<p>Issue: Moving through raw data tap events with keyboard does not update details in lower half of window.</p> <p>Fixed. Raw data tap now updates correctly.</p>
SEN-8467	<p>Issue: <i>Sentinel Data Manager</i> login screen hangs up throwing exception if any table space (used,free,total) exceeds 2,147,483,647 MB.</p> <p>Fixed. SDM login works properly.</p>

Defects Number	Description
SEN-8032	Issue: <i>Sentinel Data Manager</i> does not work with [enter] key to login. Fixed. SDM now work with [enter] key to login.
SEN-8113	Issue: Selecting checkboxes in Dynamic List inconsistent. Fixed. Selecting checkboxes in Dynamic List now are consistent.
SEN-8080	Issue: <i>Sentinel Data Manager</i> "History Status" window is limited in size. Fixed. Provided text area with scrollbar so that lengthy messages can be displayed.
SEN-7947	Issue: Moving through raw data tap events with keyboard does not update details in lower half of window. Fixed. Details are updated properly.
SEN-7156	Issue: Offline Query doesn't stop its execution when the "Stop" link is clicked. Fixed. Offline Query now stops properly.
SEN-8501	Issue: Correlation Engine errors when running JavaScript. Fixed. Correlation Engine work properly.
SEN-8463	Issue: Cannot debug JS correlation actions that create incidents. Fixed. Debugging JS correlation actions work properly.
SEN-8440	Issue: Linux environment variables should not be set directly in /etc/profile. Fixed. Linux environment variables are moved to /etc/profile.d/
SEN-8210	Issue: <i>Sentinel Data Manager</i> (SDM) does not ever finish loading when it encounters an error from the database. Fixed. SDM finishes loading properly.
SEN-8039	Issue: PatchDB fails on non-English install. Fixed. PatchDB now installs on non-English system properly.

Defects Number	Description
SEN-7062	<p>Issue: Customer would like to customize the way date/time is formatted in event tables.</p> <p>Fixed. Please follow the following manual steps to take advantage of this feature.</p> <p>To customize date and time format in event time stamp fields in the <i>Sentinel Control Center</i> and related exports to .csv or .html files, modify %ESEC_HOME%\config\SentinelPreferences.properties on Windows, \$ESEC_HOME/config/SentinelPreferences.properties on Solaris and Linux to the format you desire.</p> <p>Uncomment the following line in the file:</p> <pre>#com.eSecurity.Sentinel.event.datetimeformat=yyyy-MM-dd'T'HH:mm:ss.SSSZ</pre> <p>The date and time format can be modified using the formatting information on the following web page: Class SimpleDateFormat (http://java.sun.com/j2se/1.5.0/docs/api/java/text/SimpleDateFormat.html)</p> <p>By default, the <i>Sentinel Control Center</i> will use a pattern appropriate for the locale for which it is configured. This property gives the user the ability to override this default.</p>
DAT-366	<p>Issue: Inability to manage SENT_AUDITD tablespace probably causing Sentinel to lock up.</p> <p>Fixed. Perform partitioning and archiving of data in the SENT_AUDITD tablespace.</p>

8 Known Issues in Sentinel 6.1.1.0 Release

This table lists the known defects in the Sentinel 6.1.1.0 Release.

Table 5 *Known defects in Sentinel 6.1.1.0 Release*

Defects Number	Description
DAT-375	<p>Issue: PatchDB fails when Audit Record table is large. When AUDIT_RECORD table is large, there might not be enough of temporary table space available to constraints in order to support AUDIT_TABLE partition management.</p>

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

10 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 \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2009 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc. 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 \(http://www.novell.com/company/legal/patents/\)](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 \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

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