Novell Sentinel™ 6.0.3.0

April 1, 2009

These are the release notes for the Sentinel 6.0.3.0 (6.0 SP3) Release.

1 Overview

The information in this Release Note file pertains to Novell Sentinel™ 6.0.3.0, 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 6.0 or Sentinel 6.0 SP1 or Sentinel 6.0 SP2. Sentinel 6.0.0.0 must already be installed before applying this Service Pack, but SP1 and SP2 is not necessary; 6.0.3.0 is inclusive of all fixes and feature that are in SP1 and SP2.

The Service Pack must be installed on all existing Sentinel 6.0 or Sentinel 6.0 SP1 or 6.0 SP2 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.

IMPORTANT: If you install this service pack, you must use the Novell Sentinel™ 6.1.1.0 Upgrade Installer to upgrade from Novell Sentinel™ 6.0.3.0 to Novell Sentinel™ 6.1.1.0. Using an earlier version of the upgrade installer will not work..

The instructions for upgrading the Novell Sentinel™ 6.0.3.0 to Novell Sentinel™ 6.1.1.0 are described in the Novell Sentinel™ 6.1.1.0 Upgrade Installer document.

1.1 Prerequisites

- If Sentinel is not yet installed, it must be installed using the Sentinel 6.0.0.0 installer. Please see the Sentinel Installation Guide for instructions.
- If Sentinel 5.x is installed, it must be upgraded to Sentinel 6.0.0.0 using the upgrade installer. Please see the Patch Installation Guide for instructions.
- If Sentinel 4.x is installed, Sentinel 6.0.0.0 must be installed using the Sentinel 6.0.0.0 installer. Some data can be migrated to the Sentinel 6.0.0.0 installation. Please see the Patch Installation Guide for instructions.

The full product documentation and the most recent version of this file are available at Product Documentation (http://www.novell.com/documentation/sentinel6/).

2 What's New in Sentinel 6.0 SPs

This section explains the new features available in Sentinel 6.0 SPs.

- Section 2.1, “What's New in Sentinel 6.0.3.0,” on page 2
- Section 2.2, “What's Included in Previous Sentinel 6.0 Service Packs,” on page 2

2.1 What's New in Sentinel 6.0.3.0

Sentinel 6.0.3.0 is a maintenance release for Sentinel that is inclusive of Sentinel 6.0 SP1 and SP2. In addition to bug fixes, it contains enhanced Advisor feature.

2.1.1 Advisor update

The 6.0.3.0 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 6.0.3.0 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 6.0.3.0.

Increased data storage requirements: Because the Advisor feed now supports a much larger set of devices and signatures the data storage requirements have increased. Novell recommends approximately 20 gigabytes dedicated to store Sentinel Advisor data.

IMPORTANT: Previously downloaded Advisor tables are no longer used and are dropped during patch installation.

2.2 What's Included in Previous Sentinel 6.0 Service Packs

The following fixes may also be applied, depending on the current patch level of your Sentinel system:

- “Solution Designer (added in SP2)” on page 3
- “Solution Manager (added in SP2)” on page 3
- “JavaScript-based Correlation Actions (added in SP2)” on page 3
- “JavaScript-based Correlation Actions (added in SP2)” on page 3

2.2.1 Solution Designer (added in SP2)

Sentinel 6.0 SP2 introduces the Sentinel Solution Designer, a new application that is used to package a set of Sentinel content, organized into controls that address common regulatory concerns. The Solution Designer packages Sentinel correlation rules, dynamic lists, maps, reports, and iTRAC workflows along with a description of the requirement the control was designed to fulfill, implementation instructions, and testing steps to ensure that the control is working as expected. The Solution Designer packages all of this information into a single, easily-installed Solution Pack, creating an integrated solution to solve a specific business problem.

Solution Designer functionality is described in detail in the "Solution Packs" chapter of the Sentinel User Guide.

2.2.2 Solution Manager (added in SP2)

The Sentinel Solution Manager is a new interface in the Sentinel Control Center, designed to install and manage Solution Packs created using Solution Designer. Solution Packs may be custom or provided by Novell. Combinations of Sentinel content are managed as integrated controls, simplifying the process of installing, implementing, and testing the Sentinel system.

Solution Designer functionality is described in detail in the "Solution Packs" chapter of the Sentinel User Guide.

2.2.3 JavaScript-based Correlation Actions (added in SP2)

Sentinel 6.0 SP2 includes the ability to create powerful and flexible correlation actions using JavaScript. These scripts can make calls to the Sentinel correlation API and can be debugged in the Sentinel Control Center.

JavaScript Correlation Action functionality is described in detail in the "Correlation Rules and Actions" section of the "Solution Packs" chapter of the Sentinel User Guide.

2.2.4 JavaScript-based Correlation Actions (added in SP2)

Documentation on the correlation API can be found under Sentinel JavaScript Correlation Action API on the Novell documentation site: Correlation API Documentation (http://www.novell.com/documentation/sentinel6/).

2.2.5 Advisor Updates

Sentinel 6.0 SP2 includes a new release of the Advisor vulnerability and exploit data feed. This new release expands the devices and signatures that are supported. Current Advisor users will need to be aware of several issues as they move to the new Service Pack:

- Integration with Novell Login: The new Advisor system uses a Novell eLogin account associated with the customer's purchase information to connect to the Advisor server, the same account used to log into the Novell Customer Care portal. The previous credentials supplied with the Advisor license are not valid after the SP2 patch is applied. Contact Novell Technical Support for any questions about creating a Novell eLogin account with the appropriate entitlements to Sentinel.

Advisor functionality is described in detail in the “Advisor Configuration” chapter of the Sentinel Installation Guide.

2.2.6 Significant Connector Updates (added in SP2)

Several of the Sentinel Connectors have been updated in Service Pack 2. In addition to bug fixes, the following enhancements have been made:

- WMI (Windows): Now includes the ability to retrieve a list of servers from Active Directory via LDAP /LDAPS for use in auto-configuration. A new MSI package is provided to simplify setup of source servers.
- Database: The connector now includes the ability to use stored procedures rather than SQL statements built into the collector itself. This is useful if corporate policy prohibits running SQL statements from an external source against the database. Existing collectors will need to be customized to use this functionality.
- Novell Audit and Syslog: These connectors can now use certificates signed by a third party CA.
- Sentinel Mainframe Connector (SMC): Rearchitected to improve stability, security, and supportability. This optional connector requires a special license from Novell.
- SDEE: Improved certificate handling.

To download the latest connectors go to the Sentinel Connector Web site (http://support.novell.com/products/sentinel/secure/sentinel6.html).

2.2.7 Red Hat Enterprise Linux 4 Support (added in SP1)

Sentinel 6 supports Red Hat Enterprise Linux 4 on x86_64 hardware.

2.2.8 Enhancements to the ESM Framework (added in SP1)

The new Event Source Management framework in Sentinel 6 has been enhanced to improve performance and usability. The Graphical view now automatically contracts child nodes into the parent if more than 20 children are present, and adds a dedicated frame to manage child nodes. This prevents performance degradation and display clutter that can occur with large numbers of nodes. A new "Magnifying Glass" option is also included that enlarges a portion of the screen without changing the overall view.

2.2.9 Export Raw Events to a File (added in SP1)

A new configuration option on all Connector nodes allows the raw data from that connector to be saved to a text file. This can be used to store the raw data in unaltered form. This also is useful for debugging and testing Sentinel data collection.

2.2.10 New JavaScript Based Collector Engine (added in SP1)

Sentinel 6.0 includes a new technology that allows collector development using JavaScript based event collectors in addition to the existing proprietary Sentinel collectors. This provides a platform for Novell's customers and partners to build high quality, feature-rich collectors using an industry standard programming language. Collectors written in JavaScript are available on request from Novell Technical Support.

To know more about the Sentinel Plug-in SDK, refer to the Sentinel Plug-in SDK (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel).

3 Prerequisites

The prerequisites depend on the Sentinel system version and platform. Read the below section 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.

4 Installation

The instructions provided in this section are for installing this Sentinel 6.0.3.0 Service Pack only. This Service Pack can be run against an existing installation of Sentinel™ 6.0 or Sentinel™ 6.0 SP1 or Sentinel™ 6.0 SP2.

This Service Pack comes with an automated installer that will backup the existing software components that will be replaced. The backup files are placed in a directory named "SP<id>_<date>_bak" under the ESEC_HOME directory, where <id> is the numeric identifier of the service pack and <date> is the date of the Service Pack (for example, "SP3_2008-10-30-GMT_bak").

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 Sentinel services running on this machine:

- On Windows, use *Windows Service Manager* to stop the “Sentinel” services.
- On UNIX, run $ESEC_HOME/sentinel/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 to 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 7
- Section 5.2, "Sentinel Database Patch Installation on SQL Server," on page 8

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 6.0 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).

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 Service Pack 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 SP2. 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 using the Sentinel Database User credentials, esecdba if 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 8
- "Installing Database Patch with SQL Server Authentication" on page 9

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 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.

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 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).
- 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 Updates

There are several configuration steps needed after updating the Sentinel system.

- Section 6.1, "Updating Permissions for Solution Designer and Manager," on page 10
- Section 6.2, "Resetting Advisor Authentication (Direct Download Only)," on page 10

6.1 Updating Permissions for Solution Designer and Manager

If updating from Sentinel 6.0 SP1 or earlier, you must update the permissions for any users who will use Solution Designer or Manager. If updating from Sentinel 6.0 SP2 this does not apply because the permissions are already set correctly.

To grant permissions for the Solution Pack:

1. Log into the Sentinel Control Center as a user with permissions to use the User Manager.
2. Go to the *Admin* tab.
3. Open the *User Configuration* folder.
4. Open the *User Manager* window.
5. Click the *Permissions* tab.
6. Select Solution Designer, Solution Manager, or Solution Pack (which will automatically select both child permissions). The new permissions will be applied the next time the user logs in.

6.2 Resetting Advisor Authentication (Direct Download Only)

If you were running Advisor in Direct Download mode in Sentinel 6.0 SP2 or before, the credentials used for Advisor authentication must be updated after applying the 6.0.3.0 service pack.

There is no need to update the password if you are running Advisor in a Standalone configuration. In this mode, the password is entered manually and not stored in a file.

To reset the password for automatic Advisor downloads:

1. For UNIX, log into the machine where Advisor is installed as the Sentinel Administrator User (esecadm by default). For Windows, login as a user with administrative rights.
2. Go to the following location:
   - For UNIX: $ESEC_HOME/bin
   - For Windows: %ESEC_HOME%\bin
3. Execute the following command:
   - For UNIX: ./adv_change_passwd.sh <newpassword>
   - For Windows: adv_change_passwd.bat <newpassword>

   where <newpassword> is the updated Advisor password.

To reset the username for automatic Advisor downloads:

1. For UNIX, log into the machine where Advisor is installed as the Sentinel Administrator User (esecadm by default). For Windows, login as a user with administrative rights.

2 Edit the advisor_client.xml file in the follwing directory:

- For UNIX: $ESEC_HOME/config
- For Windows: %ESEC_HOME%\config

3 Change the username value to the Novell eLogin username. For example: <property name="username">BobJones</property>

4 Save the file.

7 Defects Fixed in Sentinel 6.0 Releases

This section lists the defects fixed in the Sentinel 6.0.3.0, Sentinel 6.0 SP2, and Sentinel 6.0 SP1 Releases.

- Section 7.1, “Defects Fixed in Sentinel 6.0.3.0 Release,” on page 11
- Section 7.2, “Defects Fixed in Sentinel 6.0 SP2 Release,” on page 13
- Section 7.3, “Defects Fixed in Sentinel 6.0 SP1 Release,” on page 14

7.1 Defects Fixed in Sentinel 6.0.3.0 Release

The following table lists the defects fixed in the Sentinel 6.0.3.0 Release.

- “Advisor fixes” on page 11
- “Performance enhancement” on page 12
- “General fixes” on page 12

7.1.1 Advisor fixes

Table 1 *Defects fixed in Sentinel 6.0.3.0 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.
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 enhancement

Table 2 *Defects fixed in Sentinel 6.0.3.0 Release*

Defects Number	Description
466081	Issue: Slow performance when querying mssql. FIXED: Change the jdbc properties to query mssql.

7.1.3 General fixes

Table 3 *Defects fixed in Sentinel 6.0.3.0 Release*

Defects Number	Description
468716	Issue: HIST_EVENTS view is not updated when archived partition is imported back to database. FIXED: The HIST_EVENTS view is updated with the data from the imported partitions.
452875	Issue: Crystal XIR2 does not work on Linux install. FIXED: To make the crystal reports work, it is mandatory to add the "crystal" user to the group of Oracle (oinstall).
452098	Issue: Sentinel bar graphs show incorrect percentages graphically. FIXED: The graphical and numerical values are displaying properly.
452101	Issue: dbconfig options are incorrect. FIXED: dbconfig options are displaying correctly.
452721	Issue: Correlation Engine errors when running JavaScript. FIXED: The correlation engine is not showing error on deploying the correlation rule of the form window(...) flow trigger | gate | sequence | ... and the java script actions are executed.
452479	Issue: Another non-resizable window for no reason... Correlation Rule Import. FIXED: While importing correlation rule error messages are displaying completely in more than one line, and scroll bars are provided in order to view the message completely.
452124	Issue: Need install instructions to enable Advisor after SP2 is installed. FIXED: The instruction are documented in the Enabling Advisor document.
452488	Issue: Advisor server could create lots of feed files with no vuln/exploit information in it. FIXED: Advisor server is not crating empty files and releases the connections to the databases properly.

Defects Number	Description
452928	Issue: Unable to open the closed `Debug Collector` window of a collector running in debug mode, if its event source is started. FIXED: Able to open the debug connector window on right clicking and selecting the debug option. Debug option was disable earlier.
452122	Issue: Typo in error message. FIXED: The Advisor log currently shows “handleRecognizable” instead of “handleRecoganizable”.
451805	Issue: Improper error messages are logged in Advisor log, if the Advisor credentials are given incorrectly. FIXED: Appropriate error messages are displaying when the user credentials are given incorrectly.
452103	Issue: Resuming processing of feed files after fixing them results in e-mail with Java error upon successful completion. FIXED: Provides appropriate error messages on wrong user credentials.
452111	Issue: Instructions are needed to verify that Advisor and exploit detection are working from start to finish. 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.

7.2 Defects Fixed in Sentinel 6.0 SP2 Release

The following table lists the defects fixed in the Sentinel 6.0 SP2 Release.

Table 4 *Defects fixed in Sentinel 6.0 SP2 Release*

Defects Number	Description
DAT-325	Issue: On Oracle only, when the time of scheduled partition jobs is changed, the job will run at the scheduled time once and then revert to the time specified during installation. FIXED. The job runs consistently at the newly scheduled time.
SEN-3515	Issue: If the parent permission Process Management is granted but the child permission Control Processes is not granted, users are still able to terminate iTRAC processes. FIXED. Users must have the Control Processes permission in order to terminate an iTRAC process.

Defects Number	Description
SEN-6572, SEN-6891	Issue: Correlation Rule deployments with more than one configured Create Correlated Event action generate a unique constraint violation in the DAS Binary log file: ORA-00001: unique constraint (ESECDBA.CORRELATED_EVENTS_ABC) Also, triggered events cannot be viewed. FIXED. Only the first Create Correlated Event action configured is executed by the correlation engine. This situation can be avoided by associating only one Create Correlated Event action with a Correlation Rule.
SEN-6732	Issue: The Sentinel Control Center viewer configuration for attachments is stored by user in the database, but attachment associations and viewer information for attachments may vary for a user between one machine and another. FIXED. The viewer information for attachments is now stored locally.
SEN-6932	Issue: The embedded browser in the Sentinel Control Center does not format reports properly. The workaround is to configure the Sentinel Control Center to use an external browser. FIXED. The embedded browser is removed and all reports are run through an external browser.
SEN-7246	Issue: Running a right-click command from an event table (such as in the Active View or Historical Event Query) that opens in a browser generates a run-time exception. FIXED. The embedded browser is removed and all reports run in an external browser.
SEN-7190	Issue: Imported correlation rules that contain new line characters cannot be deployed or read by the correlation engine manager. FIXED. The correlation rule import process strips extraneous new line characters.
SEN-7413	Issue: When debugging a JavaScript Collector with the FILE Connector, the debugger throws a “RuntimeException - Sentinel-EOF” when the end of the input file is reached. FIXED. When the end of the input file is reached, a notification appears.

7.3 Defects Fixed in Sentinel 6.0 SP1 Release

The following table lists the defects fixed in the Sentinel 6.0 SP1 Release.

Table 5 *Defects fixed in Sentinel 6.0 SP1 Release*

Defects Number	Description
DAT-160	Import summary table partitions function has been fixed for SQL Server 2005.

Defects Number	Description
DAT-216	Summary table insertions are now successful even if SQL Server 2005 is writing to P_MAX.
DAT-284	Multiple Sentinel Data Manager jobs may now run simultaneously with no conflict.
DAT-294	Attempting to “archive and drop” partitions that are already archived on SQL Server 2005 will now archive the selected unarchived partitions and then drop all selected partitions.
DAT-305	On SQL Server 2005, aggregation functions properly at high event rates.
DAT-306	On SQL Server 2005, attempting to archive and drop partitions when the archive destination is invalid will now result in an error. The partitions will not be dropped without being archived in this situation.
SEN-4066	Users with only View Status permissions for Event Source Management are now unable to start and stop nodes, even if multiple nodes are selected simultaneously.
SEN-5284	Starting a child node in Event Source Management will now start its parent node(s) also. Stopping a parent node in Event Source Management will not stop its child node(s).
SEN-5843	When installing the Collector Manager with it set connect to Sentinel Server via the proxy, it is no longer necessary to restart DAS.
SEN-6198	With Collectors that do not have an Event Source (e.g., ODBC collectors), “Trust Event Source Time” cannot be set in the Event Source Management GUI. Now “Trust EventSource Time” may be set at the Collector level and will apply to all child nodes.
SEN-6532	Users can no longer import scripts into the Plug-in Repository with only “View Scratch Pad” permissions.
SEN-6591	When modifications or deletions are performed on a subrule during the creation of a composite rule and the Cancel button is clicked, the modifications or deletions are now rolled back.
SEN-6629	When the parameters of a Collector Script plug-in are changed and the changes are imported into Sentinel, the parameters for any deployed Collectors using that plug-in are now immediately updated.
SEN-6703	Event Sources used to show connections to both the Event Source Server and the Connector. For clarity when there are a large number of Event Sources, connections are now shown between Event Sources and their Connector and between the Event Source Server and its Connector. Event Source Servers are no longer connected to Event Source nodes in the interface.
SEN-6747	Collector imports from 511_SP2_06_GA now work properly.
SEN-6779	Users are now prevented from creating a sequence rule without subrules.
SEN-6783	Windows Authentication users may now be created in Sentinel Control Center even if the user is already in the SQL Server 2005 list of user logins.

Defects Number	Description
SEN-6784	Deployed correlation rules can now be selected or copied. By design, deployed correlation rules still may not be edited.
SEN-6800	Users are now warned if they attempt to import a correlation rule that refers to a dynamic list that doesn't exist in the target system.
SEN-6818	The "Error" checkbox in the "Attribute Filter" in Event Source Management now displays filtered nodes properly.
SEN-6821	The updateMapData command in the Sentinel Data Manager command line interface has been removed. Maps may be updated using the Sentinel Control Center->Admin->Mapping Configuration GUI or using either %ESEC_HOME%\MapUpdateUtility.bat or $ESEC_HOME/MapUpdateUtility.sh.
SEN-7239	Switch View in the Servers View now works as expected.

8 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

9 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.