Sentinel™ 6 from Novell

Updated June 23, 2007

The information in this ReadMe file pertains to Sentinel 6 from Novell®, 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.

The most current ReadMe file for Sentinel 6 is available in the following languages: English, German, French, Italian, Spanish, Brazilian Portuguese, Japanese, Chinese Traditional, and Chinese Simplified. To view or download any of these ReadMe files, go to the Novell documentation site at http://www.novell.com/documentation/sentinel6.

What's New in Sentinel 6

Sentinel 6 includes many new features and enhancements to make it more powerful, more flexible, and easier to use. This section describes what's new in Sentinel 6.

New Correlation Features and Language Constructs

Sentinel 6 Correlation has been enhanced with new constructs that allow for nested, sequenced, and cause and effect rule types as well as powerful wizards to assist in creating new rules. Other correlation enhancements include a new rule deployment model, more options for reacting to repeated attacks, new correlation actions, and reduced administrative overhead for managing rules.

Correlation using Dynamic Lists

An important new Sentinel 6 feature is the ability to correlate against Dynamic Lists, which are used to correlate against targeted historical event data and important referential data from external sources. Dynamic Lists can be created manually through the provided management interface or automatically by adding and removing elements through actions as correlation rules are triggered. New correlation language constructs then allow rules to be triggered based whether or not a particular attribute exists in a list.

New Global Filter options

Filters can now be created to send events to the data store only, to all Sentinel components, or only to the Sentinel User Interface and Correlation Engine. This provides users with the option to analyze large amounts of data and store only the correlated events, to avoid the expense of storing large amounts of unimportant data.

Next Generation iTRAC Incident Management System

The iTRAC Incident Management System in Sentinel 6 has been dramatically improved to provide for greater capability, performance, and flexibility. It now allows for complete customization of the incident response workflow processes to match an organization's existing incident remediation policies. In Sentinel 6, iTRAC supports variables, attachments, notes, time-based and conditional escalation, improved worklist handling, and additional administrative options.

New Event Source Management Framework

Sentinel 6 includes an all-new Event Source Management framework for deploying, managing, and troubleshooting event collectors from within the Sentinel console. This

framework allows for management of all event collection components from within an intuitive, graphical interface that replaces functionality previously in the Sentinel Collector Builder and provides a number of new features not available in previous versions of Sentinel. Collectors and connectors are now stored within a central repository in the Sentinel system and are configured and deployed through a simple, wizard based interface. Other ESM features include a collector debugger, the ability to open filters on a single data source with a single mouse click, and integrated right click actions for analysis and management tasks such as viewing the raw data or creating a Sentinel Active View.

Expanded Platform Support

Platform support has been expanded and now includes selected 64-bit operating systems, SUSE Linux Enterprise Server 10, and Oracle 10, including Oracle Real Application Clusters (RAC). See the Sentinel Installation Guide for a complete list of supported platforms. The Java Virtual Machine and Sonic Message Bus included in Sentinel have also been updated to the latest versions available to improve performance and reliability.

SSL Proxy Connection Option for Product Components

Sentinel 6 now allows Collector Managers and the Sentinel Control Center to communicate with the Sentinel message bus using an SSL Proxy, allowing Sentinel components to be placed in a remote network without the need to modify router and firewall settings.

Offline Query

Sentinel 6 now includes a tool for retrieving a set of data from the event store as system resources become available, without negatively impacting the performance of the running Sentinel system or the database.

Active Browser

The Sentinel 6 Active Browser allows users to quickly and accurately parse through a set of events to expose specific events and detect trends without needing to write SQL statements or create reports.

Database and User Interface Support for Double-Byte Characters

The Sentinel database and User Interface now allow the manual entry and storage of double-byte characters.

Event Hashing

Sentinel 6 supports storing and hashing the original event to ensure data integrity.

Improved Internal Auditing

More events and detail are provided for actions taken within the Sentinel system.

Migration and Upgrade Tools

Installation tools and database scripts are provided to ease facilitate upgrades from Sentinel 5 to Sentinel 6, and migrations from Sentinel 4 to Sentinel 6.

Known Issues and Limitations

Help files for the Sentinel Control Center are not included in this release. To install up-to-date help files, follow this procedure:

1. Go to http://www.novell.com/documentation/sentinel6
2. Download the most recent help files, which are contained in a .jar file called eSentinelHelp.jar.
3. Browse to the following directory on the Sentinel Control Center machine:
   $ESEC_HOME/lib or %ESEC_HOME%\lib
4. Back up the old version of eSentinelHelp.jar.
5. Copy the new eSentinelHelp.jar into the directory.
6. Close and reopen the Sentinel Control Center.

Installation Issues

SEN-5895 – Sentinel installation fails if the installer is run from a directory which contains a special character in its path. The workaround is to copy the installer directory to a directory that does not contains spaces in its path.

SEN-3394, SEN-5524 – The Sentinel Control Center and Uninstall shortcuts do not work if Sentinel is installed into a directory that contains non-ASCII characters. The workaround for Sentinel Control Center is to launch the application from %ESEC_HOME%\sentinel\console\console.exe or $ESEC_HOME/sentinel/console/console.exe. The workaround for uninstalling is to follow the manual procedures for uninstallation in the Install Guide.

SEN-5610 – Uninstalling the Sentinel Database on SLES 10 does not remove all database files that were created during installation (*.dbf, *.ctl, *.log). The workaround is to remove these files manually using the instructions in the Installation Guide.

SEN-5843 –When installing a Collector Manager with a proxy connection to the Sentinel system, the DAS Proxy must be restarted in order to load the new trusted certificate so the Collector Manager can connect. The workaround is to restart the entire Sentinel Service on the machine with DAS installed or kill the DAS Proxy process, which will automatically be restarted.

SEN-5843 - When installing the Collector Manager with it set connect to Sentinel Server via the proxy, the installer will configure everything required to establish the proxy connection automatically. However, the Collector Manager will not be able to connect to the proxy until the DAS Proxy process is restarted in order to allow it to load the new trusted certificate. The workaround is to either restart the entire Sentinel Service where DAS Proxy is running or just kill the DAS Proxy process (which will automatically be restarted by the Sentinel Service watchdog).

SEN-6041 – Sentinel cannot start the Oracle 10 database due to errors in the Oracle dbstart and dbshut scripts. The instructions for modifying the two scripts for Oracle 10 on Solaris 10 and Red Hat 3 can be found in the Install Guide. No modifications are necessary on SUSE Linux Enterprise Server 10.

SEN-6542 – On Oracle only, when installing DAS and the Sentinel Database, the language you run the installer in must be supported by the installed Oracle software. For example, if the Sentinel installer is run in French to install DAS and the Sentinel Database and the Oracle database is installed with English support only, there will be NLS errors in the das_query_*.log file.

SEN-6881 – If the user clicks “Back” from the Communication port prompt until the feature selection page and unchecks some components to be installed, the installer may continue to prompt for Communication ports that are not necessary. The workaround is to specify the correct

ports even though they may not be used by the components currently selected to be installed. If additional components are installed later, the ports will be used at that time.

SEN-6882 – When the wrong hostname or port is entered when installing Collector Manager with it set to connect to Sentinel Server via the proxy, continuing the installation until the prompt for the "Sentinel username and password that has permissions to register the trusted client" causes errors. If you go back and edit hostname or port in the installer, the configuration.xml is not updated with the new information and the trusted client registration will not succeed. The workaround is when the installer is on the screen with the register trusted client prompt, manually edit the hostname or ports in the ESEC_HOME/config/configuration.xml file. When the register trusted client username and password are re-entered, the installer will pick up the change to the configuration.xml file and continue properly.

SEN-6884 – When installing a Collector Manager with a proxy connection and with the installer in GUI mode, the user will be prompted with three options to make the trust registration with the DAS Proxy. The user must choose “Accept Permanently” (not “Accept”) in order for the Collector Manager to work.

SEN-6885 - On Windows only, using Windows Authentication for the Sentinel Application user (esecapp), if the database and other non-DAS process are installed, the Sentinel service will be set to install as the Windows Authentication user but the necessary password will not be set. Therefore, the service will not start up. The workaround is to set the service to run as the "Local System" account using the Windows Service Manager. The service does not need to run as the Sentinel Application user (esecapp) if it is not running DAS.

SEN-6886 - On Windows only, if the DAS component is added to a machine with other Sentinel Server components already installed on it and if the Sentinel Application user (esecapp) uses Windows Authentication, after the installation of DAS completes the Sentinel Service will incorrectly still be set to run as the "Local System" user. The workaround is to manually set the Sentinel Service to run as the Sentinel Application user using the Window Service Manager.

SEN-6920 – During installation, some screens (particularly the user authentication screens) may not paint completely. The workaround is to go back and forward in the InstallShield wizard or minimize and then maximize the window to force it to redraw the wizard screen.

SEN-6932 – 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.

SEN-7225 – On SUSE Linux Enterprise Server only, Sentinel will not autostart on a machine that does not have Oracle and RAW services installed. The workaround is to edit the chkconfig file and change the line

```
# Required-Start: network oracle raw
```

to

```
# Required-Start: network +oracle +raw
```

Then, as root, run the command `chkconfig --add sentinel`.

Other Issues

DAT-160 – On SQL Server 2005 only, import summary table partitions fails with “Invalid object name” in the sdm.log file.

DAT-216 – On SQL Server 2005 only, summary table insertion fails when online current partition is P_MAX. The workaround is to ensure that there are always future partitions available so the system never writes to P_MAX.

DAT-284 – On Oracle only, partition management jobs (e.g., adding or taking partitions offline) may fail if multiple jobs are running concurrently or if a partition management job is running at the same time as partition listing is refreshed in the Sentinel Data Manager GUI. The workaround

is to schedule partition management jobs to avoid overlap and to avoid using the SDM while the partition management jobs are running.

DAT-294 – On SQL Server 2005 only, if partitions are archived and then the user attempts to “archive and drop” the same partitions, the job will fail and generate a primary key violation error.

DAT-305 – On SQL Server 2005 only, if the event rate is high (>200 events per second), the aggregation service cannot update the aggregation tables quickly enough. Until the aggregation service catches up, reports based on the aggregation tables may not show the most recent data.

SEN-3515 – Users can terminate iTRAC processes even though they have not been given permission.

SEN-3897 – The Server View Manager will display processes that are not installed a particular machine with a state of NOT_INITIALIZED. For example, Sentinel on Windows will show the "UNIX Communication Server" process as NOT_INITIALIZED and Sentinel on UNIX will show the "Windows Communication Server" process as NOT_INITIALIZED. The processes that are displayed with a state of NOT_INITIALIZED should be ignored.

SEN-4066 – Users with only View Status permissions for Event Source Management are able to start and stop nodes if multiple nodes are selected simultaneously.

SEN-4617 – On UNIX only, only the Sentinel Administrative User (esecadm) is able to run the Sentinel Control Center. To enable other users to run the Sentinel Control Center, please refer to the knowledge base of Technical Information Documents (TIDs) on the Novell Technical Services web site.

SEN-5284 – If an Event Source, Connector, or Collector node is set to “Run” by editing the node's configuration and clicking OK, the "Run" setting of the parent nodes is not updated to also be set to run. Therefore, if an Event Source is set to “Run” but its Collector is not, events will not be processed by the system. The workaround is to right-click on the node and select Start. This defect also affects the system when a node's "Run" setting is unchecked. In this case, the node's child nodes will not be updated to also not run. The workaround is right-click on the node and select Stop

SEN-5524 – On Windows, if the Sentinel components are installed into a directory with non-ASCII characters, the Sentinel Control Center and Sentinel Uninstall shortcuts do not work. The workaround for Sentinel Control Center is to execute the %ESEC_HOME%\bin\control_center.bat. The workaround for the Sentinel Uninstall is to perform the Manual Uninstall steps as described in the Sentinel Install Guide.

SEN-5931 – If a Collector reaches a Stop state in the debugger mode, the Step Into, Pause, and Stop buttons are still enabled but will not have any effect. The workaround is to close the debugger and reopen it.

SEN-6182 – If a running Collector Script reaches a Stop state, the child nodes of the Collector will not stop. Therefore, the Collector may be stopped, but its Connectors and Event Sources will still appear to be running in the Live View for Event Source Management. No events will be processed. The workaround is to right click on the Collector and stop it manually.

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. The workaround is to edit the package.xml file for the collector and add the element <DefaultTrustEventSourceTime>1</DefaultTrustEventSourceTime> under the element CollectorPackage.

SEN-6397 - When setting Formatter Name to “xml” in a Send Email action in the Correlation Action Manager, the body of the email is sent in name value pair format.

SEN-6398 - When the Send Email action is triggered for a correlation rule, the email attachment is blank.

SEN-6429 - If you create two role names in the Role Manager on the Admin tab that differ only in case (e.g., Admin and admin), user additions and deletions to one role will also impact the other role. The workaround is to ensure that all role names differ by more than just case.

SEN-6473 – In the Event Source Management Live View, when a filter condition is added to a node from a raw data tap and then the OK button is selected to save the new filter condition, the state of the node will be set back to what it was before the raw data tap was opened.

SEN-6532 – Users can import scripts into the Plug-in Repository with only “View Scratch Pad” permissions.

SEN-6573 – If all attributes are selected in the Attribute List as “group by” fields in a composite, aggregate, or sequence rule, an “invalid RuleLg” message is displayed.

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 not rolled back.

SEN-6608 – Maps added to the top level "Maps" folder in the Mapping Service GUI are not visible until a refresh occurs. The workaround is to create new maps in a subfolder.

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 not immediately updated. The result is that the Collector will not function properly if the Collector is restarted (which causes the Collector to use the updated Collector Script). The workaround is to open the Collector for edit and click OK to save.

SEN-6701 – Moving or cloning a node that is related to an Event Source Server, either directly or through a parent or child, fails. The workaround is to export the node and then import it.

SEN-6703 – After using the Connector edit dialog to modify the Event Source Server to which a Connector is associated, the Event Source Management GUI shows child Event Sources of that Connector connected to both the previous Event Source Server and the new Event Source Server. Some nodes’ status will change from “On” to “Off.” The workaround is to click the Refresh button and restart the Event Source.

SEN-6732 – The “Help” button does not work from the “Connect To Event Source” wizard. The workaround is to click on the “Help” button from within one of the other dialogs (e.g., Add Collector wizard or Edit Collector dialog).

SEN-6747 – When importing collectors from 511_SP2_06_GA, the Collector Details Screen does not appear and a ClassCastException is displayed in control_center0.0.log file. The workaround is to remove the package.xml file from the collector package and retry the import.

SEN-6779 – The correlation rule syntax checker does not prevent users from creating a sequence rule without subrules.

SEN-6783 – Windows Authentication user creation in Sentinel Control Center fails if the user is already in the SQL Server 2005 list of user logins.

SEN-6784 – By design, deployed correlation rules cannot be edited. The Correlation RuleLG cannot be selected or copied either. The error message "Deployed rule can not be edited" is displayed.

SEN-6800 – Correlation rules containing an inlist operator referring to a dynamic list are not functional after they are imported into Sentinel. The workaround is to recreate correlation rules with inlist instead of importing them.

SEN-6818 – The "Error" checkbox in the "Attribute Filter" does not properly display nodes with an error status set..

SEN-6821 – The UpdateMapdata command in the Sentinel Data Manager command line interface does not update the maps. The workaround is to update maps from the Sentinel Control Center->Admin->Mapping Configuration GUI.

SEN-6698 – The correlation rule language does not support the e.all operator. Rules imported from previous versions of Sentinel that use e.all will not work.

SEN-6895 – On Windows only, if a non-Unicode database is selected at install time, there is no enforcement of Latin characters in the GUI.

SEN-6896 – Mnemonics (hotkeys) do not exist for most buttons.

WIZ-1839 – The ALERT command in the collector scripting language does not automatically send the ConnectorID (RV23), EventSourceID (RV24), and TrustDeviceTime fields. The workaround is to append these fields to the alert message in any Collectors that use the ALERT command or to update Collectors to use the EVENT command. For code samples, see the Sentinel Reference Guide.

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 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 at 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.

Novell, Inc.

404 Wyman Street, Suite 500

Waltham, MA 02451

U.S.A.

www.novell.com

Novell Trademarks

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

Third-Party Materials

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

Third Party Legal Notices

This product may include the following open source programs that are available under the LGPL license. The text for this license can be found in the Licenses directory.

- edtFTPj-1.2.3 is licensed under the Lesser GNU Public License. For more information, disclaimers and restrictions see http://www.enterprisedt.com/products/edtftpj/purchase.html.
- Esper. Copyright © 2005-2006, Codehaus.
- jTDS-1.2.jar is licensed under the Lesser GNU Public License. For more information, disclaimers and restrictions see http://jtds.sourceforge.net/.
- MDateSelector. Copyright © 2005, Martin Newstead, licensed under the Lesser General Public License. For more information, disclaimers and restrictions see http://web.ukonline.co.uk/mseries.
- Enhydra Shark, licensed under the Lesser General Public License available at: http://shark.objectweb.org/license.html.
- Tagish Java Authentication and Authorization Service Modules, licensed under the Lesser General Public License. For more information, disclaimers and restrictions see http://free.tagish.net/jaas/index.jsp.

This product may include software developed by The Apache Software Foundation (http://www.apache.org/) and licensed under the Apache License, Version 2.0 (the "License"); the text for this license can be found in the Licenses directory or at http://www.apache.org/licenses/LICENSE-2.0. Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

The applicable open source programs are listed below.

- Apache Axis and Apache Tomcat, Copyright © 1999 to 2005, Apache Software Foundation. For more information, disclaimers and restrictions, see http://www.apache.org/licenses/
- Apache Lucene, Copyright © 1999 to 2005, Apache Software Foundation. For more information, disclaimers and restrictions, see http://www.apache.org/licenses/
- Skin Look and Feel (SkinLF). Copyright © 2000-2006 L2FProd.com. Licensed under the Apache Software License. For more information, disclaimers and restrictions see https://skinlf.dev.java.net/.
- Xalan and Xerces, both of which are licensed by the Apache Software Foundation Copyright © 1999-2004. For more information, disclaimers and restrictions see http://xml.apache.org/dist/LICENSE.txt.

This product may include the following open source programs that are available under the Java license.

- JavaBeans Activation Framework (JAF). Copyright © Sun Microsystems, Inc. For more information, disclaimers and restrictions see http://www.java.sun.com/products/javabeans/glasgow/jaf.html and click download > license
- Java 2 Platform, Standard Edition. Copyright © Sun Microsystems, Inc. For more information, disclaimers and restrictions see http://java.sun.com/j2se/1.5.0/docs/relnotes/SMICopyright.html
- JavaMail. Copyright © Sun Microsystems, Inc. For more information, disclaimers and restrictions see http://www.java.sun.com/products/javamail/downloads/index.html and click download > license.

This product may also include the following open source programs.

- ANTLR. For more information, disclaimers and restrictions, see http://www.antlr.org
- Boost. Copyright © 1999, Boost.org.
- Concurrent, utility package. Copyright © Doug Lea. Used without CopyOnWriteArrayList and ConcurrentReaderHashMap classes
- Java Ace, by Douglas C. Schmidt and his research group at Washington University. Copyright © 1993-2005. For more information, disclaimers and restrictions see http://www.cs.wustl.edu/~schmidt/ACE-copying.html and http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html
- JLDAP. Copyright 1998-2005 The OpenLDAP Foundation. All rights reserved. Portions Copyright © 1999 - 2003 Novell, Inc. All Rights Reserved.
- OpenSSL, by the OpenSSL Project. Copyright © 1998-2004. For more information, disclaimers and restrictions, see http://www.openssl.org.
- Tao (with ACE wrappers) by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine and Vanderbilt University. Copyright © 1993-2005. For more information, disclaimers and restrictions see http://www.cs.wustl.edu/~schmidt/ACE-copying.html and http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html
- Tinyxml. For more information, disclaimers and restrictions see http://grinninglizard.com/tinyxmldocs/index.html.
- Java Service Wrapper. Portions copyrighted as follows: Copyright © 1999, 2004 Tanuki Software and Copyright © 2001 Silver Egg Technology. For more information, disclaimers and restrictions, see http://wrapper.tanukisoftware.org/doc/english/license.html.