

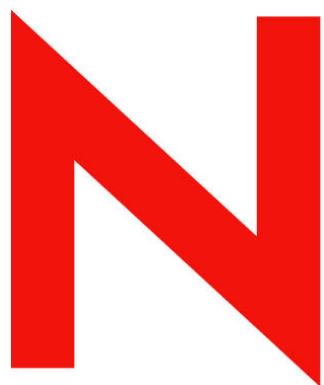
Novell[®] Sentinel[™]

6.0

July 25, 2007

Volume VI - PATCH INSTALLATION GUIDE

www.novell.com



Novell[®]

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.

Copyright © 1999-2007 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 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

Online Documentation: To access the online documentation for this and other Novell products and to get updates, see www.novell.com/documentation.

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>.

NOTE: As of the publication of this documentation, the above links were active. In the event you find that any of the above links are broken or the linked web pages are inactive, please contact Novell, Inc., 404 Wyman Street, Suite 500, Waltham, MA 02451 U.S.A.

Preface

The Sentinel Technical documentation is general-purpose operation and reference guide. This documentation is intended for Information Security Professionals. The text in this documentation is designed to serve as a source of reference about Sentinel's Enterprise Security Management System. There is additional documentation available on the Sentinel web portal.

Sentinel Technical documentation is broken down into five different volumes. They are:

- Volume I – Sentinel™ Install Guide
- Volume II – Sentinel™ User's Guide
- Volume III – Sentinel™ Collector User's Guide
- Volume IV – Sentinel™ User's Reference Guide
- Volume V – Sentinel™ 3rd Party Integration
- Volume VI – Sentinel™ Patch Installation Guide

Volume I – Sentinel Install Guide

This guide explains how to install:

- Sentinel Server
- Sentinel Console
- Sentinel Correlation Engine
- Sentinel Crystal Reports
- Collector Builder
- Collector Manager
- Advisor

Volume II – Sentinel User's Guide

This guide discusses:

- Sentinel Console Operation
- Sentinel Features
- Sentinel Architecture
- Sentinel Communication
- Shutdown/Startup of Sentinel
- Vulnerability assessment
- Event monitoring
- Event filtering
- Event correlation
- Sentinel Data Manager
- Event Configuration for Business Relevance
- Mapping Service
- Historical reporting
- Collector Host Management
- Incidents
- Cases
- User management
- Workflow

Volume III – Collector User's Guide

This guide discusses:

- Collector Builder Operation
- Collector Manager
- Collectors
- Collector Host Management
- Building and maintaining Collectors

Volume IV - Sentinel User's Reference Guide

This guide discusses:

- Collector scripting language
- Collector parsing commands
- Collector administrator functions
- Sentinel correlation engine
- Correlation command line options
- Sentinel database schema

- Collector and Sentinel meta-tags
- User Permissions

Volume V - Sentinel 3rd Party Integration Guide

- Remedy
 - HP Service Desk
- HP OpenView Operations

Volume VI - Sentinel Patch Installation Guide

- Patching from Sentinel 4.x to 6.0
 - Patching from Sentinel 5.1.3 to 6.0

Contents

1 Migrate from Sentinel 4.2 to Sentinel 6	1-1
Overview	1-1
Comparing Sentinel 4.2 and Sentinel 6	1-1
Functionality removed or replaced in Sentinel 6	1-1
Functionality enhanced or included between Sentinel 4.2 and Sentinel 6	1-1
Data Migration from Sentinel 4.2 to Sentinel 6	1-4
Java Version	1-4
Backup Systems	1-5
Exporting Sentinel 4.2 Correlation Rules	1-6
Uninstalling Sentinel 4.2	1-6
Installing Sentinel 6 Database	1-6
Creating Sentinel Database Administrator User	1-8
Migrating Data	1-9
Install and Configure Sentinel 6 Components	1-11
Post-Migration Procedures	1-11
Configure User Permissions	1-11
User Interface Display Preferences	1-12
Importing Correlation Rules	1-12
Import and Deploy Collectors and Connectors	1-13
Configuring Reports	1-13
Creating Filters in Sentinel 6	1-13
2 Patching from Sentinel 5.1.3 to Sentinel 6.0	2-1
Overview	2-1
Notes on Upgrade to Sentinel 6.0	2-1
Pre-requisites for patching to Sentinel 6.0	2-4
Related Topics	2-5
Exporting Correlation Rules in Sentinel 5.1.3	2-5
Patching to Sentinel 6.0	2-5
Patching to Sentinel 6.0 Database When Using Oracle	2-7
Patching to Sentinel 6.0 Database When Using Microsoft SQL Server	2-9
Post-Patch Procedures	2-11
Updating Sentinel User Permissions	2-11
Importing Sentinel 5.1.3 Correlation Rules	2-12
Migrating Sentinel 5.1.3 Collector Port Configurations	2-12
Updating Default Filters	2-13
Updating Menu Configuration Executables	2-14
Importing Crystal Reports	2-15
Enabling AES 256-bit Message Bus Encryption	2-15
Customized Sentinel Server Data Directories	2-15

1

Migrate from Sentinel 4.2 to Sentinel 6

Topics included in this chapter:

	<u>Topic</u>	<u>Page</u>
	Overview	1-1
	Comparing Sentinel 4.2 and Sentinel 6	1-1
	Data Migration from Sentinel 4.2 to Sentinel 6	1-4
	Uninstalling Sentinel 4.2	1-6
	Installing Sentinel 6 Database	1-6
	Install and Configure Sentinel 6	1-11
	Components	
	Post-Migration Procedures	1-11

Overview

Caution: Sentinel 4.2 and Sentinel 6.0 have different database schemas and system requirements. Confirm that the hardware and software platforms meet the Sentinel 6.0 requirements before starting the upgrade.

A Sentinel data migration utility is provided to copy data from Sentinel 4.2 to Sentinel 6. This utility is provided with the Sentinel 6 installer. For Microsoft SQL Server, the data migration utility supports migration from the Sentinel 4.2.1 database on a SQL Server 2000 instance to the Sentinel 6 database on a SQL Server 2005 instance. The SQL Server instances can be on the same or two different machines. For Oracle, the data migration utility supports migration from the Sentinel 4.2.1 database instance to the Sentinel 6 database instance on the same machine or on two different machines.

Comparing Sentinel 4.2 and Sentinel 6

This section lists out the Functional and User Interface updates in Sentinel 6.0 and refers to different documents related to these updates for your understanding and analysis. It is recommended that you read through this section before performing the migration.

Functionality removed or replaced in Sentinel 6

- Case-related functionality has been removed.
- Real Time Summary Displays has been replaced by Active Views.
- Wizard Monitoring permissions have been replaced by View Collectors, Control Collectors, and Collector Administration permissions.
- System Overview functionality has been removed.

Functionality enhanced or included between Sentinel 4.2 and Sentinel 6

- User Permissions
- Correlation
- Incidents
- iTRAC

- Offline Query
- Collectors, Collector Builder and ESM
- Mapping
- Server View
- Aggregation
- Auto-Archive Partitions
- Platform & Database Support
- Reports

User Permissions

The following permissions are new or changed in Sentinel 6:

- iTRAC (all settings)
- Incidents > Incident Administration
- Collector Management > Collector Administration
- Administration > DAS Statistics
- Administration > User Session Management
- Administration > iTRAC Role Management
- Server View (all settings)
- Roles (all settings)

For more information on User Permissions, see [Sentinel Control Center User Permissions](#) in *Sentinel 6.0 User's Reference Guide*.

Correlation

Correlation in Sentinel 6 may have many Functional and User Interface updates when compared to Sentinel 4.2. Moreover, you may want to re-write some of the existing rules for more efficient results. For information on Correlation Functionality updates, see [Sentinel Correlation Engine RuleLG Language](#) in *Sentinel 6.0 User's Reference Guide*.

For information on User Interface updates, see [Correlation Tab](#) in *Sentinel 6.0 User's Guide*.

Incidents

A Case in Sentinel 4.x is referred to as an Incident in Sentinel 6.0. An incident is a set of events (events that require attention, for example, a possible attack) grouped together. An Incident in 'open' state alerts you to investigate and close the events that resulted in the incident. For more information, see [Incident Tab](#) in *Sentinel 6.0 User's Guide*.

iTRAC

In Sentinel 6.0, iTRAC Workflow is a new functionality designed to provide a simple, flexible solution for automating and tracking an enterprise's incident response processes. Through Sentinel's internal incident system, it tracks security or system problems and identifies and resolves the problem. For more information, see [iTRAC Workflows](#) in *Sentinel 6.0 User's Guide*.

Offline Query

Offline Query is introduced in Sentinel 6.0. They are often used to run queries against large amounts of data. Offline Query will continue to run even after the user logs out of the Sentinel Control Center, if necessary. For more information, see [Offline Query](#) in *Sentinel 6.0 User's Guide*.

Collectors, Collector Builder and ESM

Agents in Sentinel 4.x are referred to as Collectors in Sentinel 6.0, and Wizard as Collector Builder. In Sentinel 4.0 Collectors were configured and managed using Wizard. But, in Sentinel 6.0 the Collectors are configured in Collector Builder, but are managed using the Event Source Management in Sentinel Control Center.

Event Source Management (ESM) panel provides a set of tools to manage and monitor connections between Sentinel and its event sources. For more information, see [Event Source Management](#) in *Sentinel 6.0 User's Guide*.

For other Collectors, including custom Collectors or modified Tier 1 Collectors, there are several reference documents available:

- [Using 5.x Collectors with Sentinel 6](#) (also applies to Sentinel 4.x collectors)
- [DB Connector Differences in Sentinel 6](#)
- [File Connector Differences in Sentinel 6](#)
- [Syslog Connector Differences in Sentinel 6](#)
- [WMI Connector Differences in Sentinel 6](#)

Mapping

Mapping is a new functionality introduced in Sentinel 5 and enhanced in Sentinel 6. Mapping allows you to add, edit, delete and update mapping configurations. For more information, see [Administration](#) in *Sentinel 6.0 User's Guide*.

Server View

Server Views allows you to monitor the status of all Sentinel Server processes across the system. Through Server view you can Start/Stop/Restart the processes that get installed on the product installation. For more information, see [Server View](#) in [Administration](#) in *Sentinel 6.0 User's Guide*.

Aggregation

Aggregation is the process of calculating the running count for all active summaries as events flow through the system. These running counts are saved to the database in the respective summary tables. For more information, see [Reporting Data](#) in [Administration](#) in *Sentinel 6.0 User's Guide*.

Auto-Archive Partitions

Auto-archiving is a new functionality in Sentinel 6.0. The Partition Configuration tab in the SDM allows you to set parameters to auto-archive partitions. The Auto-Archive Partition functionality allows you to auto-add partitions. For more information, see [Sentinel Data Manager](#) in *Sentinel 6.0 User's Guide*.

Platform & Database Support

The platform and database support is significantly improved for Sentinel 6.0. For more information on the Platform and Database support in Sentinel 6.0, see [Supported Platforms and Best Practices](#) in *Sentinel 6.0 Installation Guide*.

Reports

The Crystal Reports version has been updated from 9 to XI R2 between Sentinel 4.2 and Sentinel 6. Use the upgrade procedures recommended by Business Objects to upgrade the report server and update the ODBC Data Source Name to point to the new Sentinel 6 database. In addition, the Sentinel database schema has changed significantly. For more information, see [Crystal Reports on Linux/Solaris or Windows](#) in *Sentinel 6.0 Installation Guide*.

Data Migration from Sentinel 4.2 to Sentinel 6

There are several steps to be performed for migration from Sentinel 4.2 to Sentinel 6. Most of these prerequisites are described in more detail in the following sections. Follow the links to perform each of these actions in the order given below for successful migration.

WARNING: To avoid mistakes, read through all instructions carefully before beginning the upgrade and migration.

- Verify hardware and software platform requirements for Sentinel 6. For more information, see [Hardware Recommendations](#) in [Supported Platforms and Best Practices](#) in *Sentinel 6.0 Installation Guide*.
- [“Check Java Version”](#) installed on your system
- [“Backup components”](#) of the Sentinel system, as required
- [“Export Sentinel v4.2 correlation rules”](#)
- [“Uninstall Sentinel 4.2”](#), except for the Database Component
- [“Install Sentinel 6 database”](#) only
- [“Verify/Add Sentinel Administrator User”](#) (esecdba) to the Database.
- [“Install and configure Sentinel Components”](#) (except Database)

On successful migration, the following data is migrated from the Sentinel 4.2.x system to Sentinel 6:

- Users and assigned permissions
- Filters
- Right-click menu configuration options
- Renamed CV tags
- Partition and archive configurations
- Cases from Sentinel 4.2 are copied into Sentinel 6 as incidents
- Incidents
- Incident-related events (Only viewable using Crystal Reports or SQL queries. The Sentinel 4.2 events cannot be viewed in the Sentinel Control Center.)

NOTE: The data migration utility **will not** migrate event data, except for event data associated with incidents in Sentinel 4.2.

NOTE: All data migration should be completed before using Sentinel 6. Do not run the data migration utility after creating new incidents.

Java Version

Before migrating any data, the correct version of java (1.5.0_11) must be in your PATH variable.

To check the java version:

1. Log into the Sentinel 6 database machine. For Solaris, login as the root user. For Windows, login as a user with administrative rights.
2. On the command line, enter the following command:

```
java -version
```
3. If the version is not 1.5.0_11, download and install the correct version of java.
4. Update the PATH variable to include the path to the directory with the correct version of java.

For example, on Windows, if the location of java is

```
C:\Program Files\Novell\Sentinel6\jre\
```

then the PATH environment variable should be prepended with:

```
C:\Program Files\Novell\Sentinel6\jre\bin
```

And on Solaris, if the location of java is

```
/opt/novell/sentinel6/jre/Sun-1.5.0_11
```

then the PATH variable should be prepended with:

```
/opt/Novell/sentinel6/ Sun-1.5.0_11/bin:
```

Backup Systems

Before making any updates to the Sentinel system, Novell strongly recommends making a backup of all system components.

Files and Folders

Back up the \$ESEC_HOME (for UNIX) or %ESEC_HOME% (for Windows) directories, the root drives of all machines in the Sentinel system, the Crystal report files, and the database before taking any other actions. Backing up this information will enable you to restore the older version of the software in case there are any unexpected failures during the installation of Sentinel 6 or during the data migration.

There are several pieces of information that are particularly important:

- The root drives may include important configuration information for your servers.
- On the Sentinel Server, the \$ESEC_HOME or %ESEC_HOME% directory includes all custom menu configurations
- On the Collector Manager(s), the \$WORKBENCH_HOME/Agents or %WORKBENCH_HOME%\Agents directory stores all port configurations.
 - These cannot be imported into Sentinel 6 but may be used for reference.
- On the Collector Manager(s), the \$WORKBENCH_HOME/Elements or %WORKBENCH_HOME%\Elements directory stores all collector scripts.
- On the Crystal Server, the files with .rpt extensions include the Novell report library and any custom reports.
 - These cannot be run without modification in Sentinel 6 because of database schema changes, but they may be used for reference.
 - The Novell report library should be replaced by the Sentinel 6 report library.
 - Any custom reports should be adapted to run against the Sentinel 6 database views.
- The database should always be backed up before any major system changes.
 - The database is the only Sentinel component that **will not** be uninstalled.

To Backup Collector scripts and Port configuration:

1. On all Sentinel 4.2 machines running Collector Manager, create a directory to store all Collectors scripts and port configurations for that machine.
2. Create a text file in this directory that lists the name of all the Collectors used by a port configuration on this Collector Manager. Use a Collector Builder to determine the Collectors being used by this Collector Manager. If this Collector Manager is on Solaris, you will need to use a Collector Builder on a Windows machine (Collector Builder is not supported on Solaris).
3. Copy the following directories into the directory you just created:

- %WORKBENCH_HOME%\Agents or \$WORKBENCH_HOME/Agents
- %WORKBENCH_HOME%\Elements or \$WORKBENCH_HOME/Elements

Exporting Sentinel 4.2 Correlation Rules

To Export a Correlation Rule Set:

1. In the Sentinel 4.2 Control Center, go to *Admin > Correlation Rules*.
2. Select a Rule Set. Click *Export*. A file browser window will open.
3. Select a folder location and click OK. The rule set will be exported as an xml file.

Uninstalling Sentinel 4.2

Except for the database, all Sentinel 4.2 components must be uninstalled before installing Sentinel 6. The database should not be removed or uninstalled.

To Uninstall Sentinel v4.2:

1. On your Sentinel 4.2 machines, close all Sentinel Consoles and Collector Builders and stop the Sentinel Server.
2. Login into each machine with Sentinel components as a user with administrative rights (on Windows) or as root user (Solaris).

On Windows:

- a. Click *Start > Programs > e-Security > Uninstall e-Security 4.2*.

On Linux/Solaris:

- a. Go to \$ESEC_HOME/_uninst
- b. Enter ./uninstall.bin

3. Follow the screen prompts. Select all Sentinel components to uninstall.

IMPORTANT:

To perform an upgrade, all components should be selected, including the Database component. Selecting the Database component for uninstall here will cause the uninstaller to remove some database related files the installer placed on the filesystem. In the following step, you may specify that you do not want to remove the data in the database.

4. Click through the screen prompts to the Database Uninstall window. In the Database Uninstall window, select *Perform no action on the database* for Windows uninstallation or *Delete nothing* for Solaris.
-

CAUTION: Do not uninstall the Sentinel database or you will lose your Sentinel 4.2 data

5. Click through the remaining uninstall windows to remove the rest of the Sentinel components.

Installing Sentinel 6 Database

The Sentinel 6 database components should be installed into a database instance that is an Oracle or SQL Server version that is supported by Sentinel 6.

IMPORTANT:

The Sentinel 6 database should be installed before installing the rest of the Sentinel 6 components.

To install Sentinel 6 Database:

1. Before starting the installation, delete the following environmental variables, if present:
 - ESEC_HOME
 - ESEC_VERSION
 - ESEC_JAVA_HOME
 - ESEC_CONF_FILE
 - WORKBENCH_HOME
2. Verify you have performed all of the preceding preparatory steps in this chapter.
3. Log into the database machine as a user with administrative rights (on Windows) or a root user (on Solaris or Linux).
4. Insert the Sentinel installation CD into the CD-ROM drive.
5. Browse to the CD and do one of the following:
 - On UNIX,
 - For GUI mode. enter `./setup.sh`
 - or
 - For textual (“headless”) mode, enter `./setup.sh –console`

NOTE: Installing in console mode is not supported on Windows.

6. After reading the Welcome screen, click *Next*.
7. Read and accept End User License Agreement. Click *Next*.
8. Accept the default install directory or click Browse to specify a different location. Click *Next*.
9. For type of installation, select *Custom* (default). Click *Next*.
10. In the feature selection window, de-select all options and select *Database*. Click *Next*.

NOTE: Ensure that Database is the only component with a check mark.

11. Configure database for installation:
 - On Windows:
 - a. Select the target database server platform.
 - b. Select *Microsoft SQL server 2005*.
 - c. Specify the Database Install log directory. Click *Next*.
 - d. Specify the storage location for:
 - Data Directory
 - Index Directory
 - Summary Data Directory
 - Summary Index Directory
 - Log Directory
 - Click *Next*.
 - e. Select the database character set support option, ASCII only database. Click *Next*.
 - f. Specify the database Size. Click *Next*.
 - g. Configure database partitions.
 - h. You may select *Enable automatic database partitions*.

- i. For data partitions, specify the archive directory; enter Time specifications to add and archive data.

Click *Next*.

On Solaris:

- a. Select the target database server platform.
- b. Select *Oracle 9i / Oracle 10g*.
- c. Select *Create New database with database objects*. Click *Next*.
- d. Specify *Oracle User Name* or accept default user name. Click *OK*.
- e. Select *Oracle JDBC driver* and specify the *Database name*. Click *Next*.
- f. Accept default memory space and listener port or specify new values.
- g. Enter *SYS* and *SYS* credentials and click *Next*.
- h. Specify the Database size. Click *Next*.
- i. Specify the storage location for:
 - Data Directory
 - Index Directory
 - Summary Data Directory
 - Summary Index Directory
 - Log Directory

Click *Next*.

- j. Configure database partitions. You may select *Enable automatic database partitions*.
 - k. If enabled, specify the data partition archive directory.
 - l. Enter time specifications to add and archive data. Click *Next*.
12. Enter Authentication Information for:
- Sentinel Database Administrator User
 - Sentinel Application Database User
 - Sentinel Administrator User
 - Sentinel Report User (only on Windows)

Click *Next*.

13. Summary of Database parameters specified will display. Click *Next*.
14. Installation Summary will display. Click *Install*.
15. On successful installation, select to restart your system and click *Finish*.

Creating Sentinel Database Administrator User

The data migration utility requires that a user named “esecdba” exists in the Sentinel 4.2 database. The procedure given below will add the “esecdba” user to Sentinel 4.2 database to allow data migration from Sentinel 4.2 to Sentinel 6. This user must have the same password in both databases for the data migration.

If this user does not exist or the database is not set up with SQL Authentication, this must be changed before attempting the migration. These changes may be reverted after the successful migration.

To add an esecdba user to the database:

1. For Solaris, login to the database machine as the Oracle software owner. For Windows, login as a user with administrative rights.

On Solaris:

- a. Go to the following directory on the CD-ROM:

```
sentinel/dbsetup/ddl/oracle/Migration
```

- b. Using SQL*Plus, connect to the Sentinel 4.2 database as SYSDBA.
- c. At the SQL prompt (SQL>), enter:

```
@import_add_esecdba.sql
```

2. Exit SQL*Plus.
3. On Windows:
 - a. Start Microsoft SQL Server Query Analyzer.
 - b. Login as the 'sa' user or equivalent Windows Authentication user.
 - c. Click *File > Open*. Navigate to the following directory on the CD-ROM:

```
sentinel\dbsetup\ddl\mssql\Migration
```

- d. Select import_add_esecdba.sql.
- e. Click *Open > Query > Execute*.
- f. After the script has finished, exit Query Analyzer.

NOTE: After successfully performing data migration:

* On Solaris, you may use Oracle Enterprise Manager to delete the recently added esecdba user from the Sentinel 4.2 database.

* On Windows, you can use Microsoft SQL Server Enterprise Manager to delete the recently added esecdba SQL Authentication user from the Sentinel 4.2 database. You may also change the database to Windows Authentication mode, if desired.

Migrating Data

To migrate data:

1. For Solaris, log in to the Sentinel 6 database server as the root user. For Windows, login as a user with administrative rights
2. For Linux and Solaris, mount the Sentinel 6 software installation CD on the database server where Sentinel 6 database resides.
3. At the command prompt, go to the following directory on the Sentinel 6 software installation CD:

```
sentinel\dbsetup\bin (Windows)
```

```
sentinel/dbsetup/bin (UNIX)
```

4. Execute the command:

```
.\MigrateDb.bat (Windows)
```

```
./MigrateDb.sh (Solaris)
```
5. For Oracle, you will be prompted for the following:
 - Destination database host name (server where the Sentinel 6 database is running)
 - Destination database name (Sentinel 6 database name)
 - ESECDBA password (the password must be the same for the Sentinel Database User on the Sentinel v4.2 and Sentinel 6 databases)
 - Source database name (Sentinel 4.2 database net service name. If your Sentinel 4.2 and Sentinel 6 database are on two different machines, you need to add the Sentinel 4.2 database net service entry to

\$ORACLE_HOME/network/admin/tnsnames.ora on your Sentinel 6 database server)

- Oracle software owner ID
- Log directory (where data migration log files will be placed)
- Migration option:
 - System settings
 - Incidents/cases
 - Both
 - Done

For SQL Server, you will be prompted for the following:

- Destination database host name (server where the Sentinel 6 database is running)
- Destination database instance name (Sentinel 6 database instance name)
- Destination database name (Sentinel 6 database name)
- ESECDBA password
- Sentinel 4.2 database host name
- Sentinel 4.2 database instance name
- Sentinel 4.2 database name
- Log directory (where data migration log files will be placed)
- Default password for migrated users

NOTE: For Windows only, the migration utility will migrate all Sentinel 4.2 users to the Sentinel 6 system. The initial password will be set to the default password entered here, so the default password should comply with your Windows password policy. Migrated users should change their passwords as soon as they log into the Sentinel 6 system.

- Migration option:
 - System settings
 - Incidents/cases
 - Both
 - Done

Special Circumstances

If the database migration fails at any point, there are several procedures to follow, depending on the point of failure.

To complete migration if the system settings migration fails:

NOTE: Do not rerun the entire migration if the system settings migration was successful.

1. Run the uninstaller for Sentinel 6.
2. Uninstall the Sentinel 6 database.
3. Choose *Delete database objects only*.
4. Complete the uninstallation process.
5. Run the Sentinel installer to install the Sentinel 6 database.
6. Choose *Add database objects to an existing empty database*.
7. Complete the installation.

8. Retry the data migration instructions with the *System Settings* option.

To complete migration if the incidents/cases migration fails:

1. Retry the data migration instructions with the *Incidents/Cases* option.
2. The migration utility will restart from the point of failure.

Install and Configure Sentinel 6 Components

To Install Sentinel 6:

1. Use the instructions in **Installing Sentinel 6** in *Sentinel 6.0 Installation Guide* to install remaining Sentinel components.

WARNING:

The database for Sentinel 6 is already installed; do not attempt to re-install.

2. Install the latest Sentinel Service Pack, if applicable.

Post-Migration Procedures

After migrating the Sentinel 4.2 data to the Sentinel 6 database, there are a few remaining steps:

- **“Update the User Permissions”** to reflect the functionality changes in the new version.
- **“Import Sentinel 4.2 Correlation Rules”** into Sentinel 6.0
- **“Import and deploy Collectors and Connectors”**
- **“Configuring Reports”**

On successful migration, see **Quick Start Guide** and **Sentinel 6.0 User’s Guide** to get started.

Configure User Permissions

IMPORTANT:

After patching to Sentinel 6, only a user with administrative privileges can modify the User Permissions/grant access to the new functionality introduced in Sentinel 6.

To change user permissions:

1. Ensure Sentinel Server is running.
2. Log into Sentinel Control Center as a user with Administration/User Management permission (For example, esecadm).
3. In Sentinel Control Center, go to *Admin > User Configuration*.
4. Right-click on the user you have to modify User Permissions to (For example, esecadm) and select *User Details*.
5. Click the *Permissions* tab.
6. Expand *iTRAC* and assign permissions as needed.
7. Expand *Incidents* and assign 'Incident Administration' as needed.
8. Expand *Collector Management* and assign 'Collector Administration' as needed.
9. Expand *Administration* and assign 'DAS Statistics', 'User Session Management' or 'iTRAC Role Management' as needed.
10. Expand *Correlation* and assign any or all permissions under Correlation, as needed.

11. Expand *Server View* permissions in the list and grant permissions as needed.
12. Click the *Roles* tab and assign the Admin or Analyst Workflow Role as needed for iTRAC workflows. Click *OK*.

User Interface Display Preferences

You may not have the Correlation or Incidents tab in Sentinel Control Center after patching to Sentinel 6.0.

NOTE: You should have administrative rights to modify user permissions.

To have these tabs, edit your User Permissions and assign Correlation or Incidents permissions as needed.

WARNING: In this case, do not save your preferences when you log out of the system after patching, if you did not update the User Permissions.

If you save your preferences when you log out of the system before the User Permissions are updated, the Correlation and Incidents tabs may not be available when you next logon. Follow the instructions given below to restore default preferences and enable the new tab or tabs.

To restore default preferences:


1. Open and edit `control_center.bat` file located in `%ESEC_HOME%\bin` (Windows) or `$ESEC_HOME/bin` (Linux/Solaris) on the machine with the Sentinel Control Center
2. Add “-nopref” in the last line after `console.jar` and Save.
3. Double-click `control_center.bat` file to open Sentinel Control Center.

NOTE: You must open Sentinel Control Center from `control_center.bat` file, not from the desktop icon, else the “-nopref” argument will not be applied.

4. Enter Login credentials. Sentinel Control Center will open without user preferences and the new tab or tabs will display.
5. After opening the Sentinel Control Center once using the modified `control_center.bat` file, the issue is resolved. You may revert to the original `control_center.bat` file, use the desktop icon to open the Sentinel Control Center, or Save Preferences when you exit the Control Center.

Importing Correlation Rules

To Import a Correlation Rule:

1. Log into Sentinel 6.0 and click the *Correlation* tab.
2. In the menu bar, click *Correlation > Correlation Rule Manager*.
3. In the Correlation Rule Manager window, click . The Import/Export Rule window will display.
4. Select *Import* from the Action pane.
5. Click *Browse* and select the Correlation Rules you want to import; click *Import*. Click *Next*. The Import Rule window will display.

6. Select the destination folder to import the Correlation rule. Click *Finish*.

NOTE: You cannot import a Sentinel 4.2 Correlation rule into Sentinel 6.0, if a Correlation rule with the same name exists in Sentinel 6.0.

Import and Deploy Collectors and Connectors

You may have to modify some of the Sentinel 4.2 Collectors to work with Sentinel 6. It is recommended to download the Add-ons (Sentinel 6.0 Collectors and related Connectors) and deploy in Sentinel Control Center.

To import and deploy Collectors:

1. Download the Sentinel 6.0 Collectors and Connectors from Novell Website (<http://support.novell.com/products/sentinel/>).
2. Import and Deploy Collectors and Connectors following the instructions in [Event Source Management](#) in *Sentinel 6.0 User's Guide*.

Configuring Reports

To publish reports:

1. For the most recent reports, follow the links from <http://support.novell.com/products/sentinel/>.
2. Upgrade Crystal Reports 9 to Crystal Reports XI R2.
3. Apply necessary patches described in [Crystal Reports on Linux/Solaris or Crystal Reports on Windows](#) in *Sentinel 6.0 Installation Guide*.
4. Deploy most recent reports using the information in [Crystal Reports on Linux/Solaris or Crystal Reports on Windows](#) in *Sentinel 6.0 Installation Guide*.

IMPORTANT:

For reports from the Novell library that have been modified or custom reports, it is recommended to modify the report queries based on the information in [Sentinel Database Views for Oracle or Microsoft SQL Server](#) in *Sentinel 6.0 User's Reference Guide*.

Creating Filters in Sentinel 6

A new installation of Sentinel 6.0 provides a set of default filters. These filters can be recreated, if desired, in a system that has been upgraded from Sentinel 4.2 to Sentinel 6.0. The graphic below shows the default filters for Sentinel 6.

Owner	Filter Name	Expression String
PUBLIC	Real_Time	filter(e.SensorType = "T")
PUBLIC	Operating_System_Events	filter(e.DeviceCategory = "OS")
PUBLIC	EventSource_B62672A0-12D3-102A...	filter(e.EventSourceId = "B62672A0-12D3-102A-BCFE-000C29512CF1")
PUBLIC	IDS_Events	filter(e.DeviceCategory = "IDS")
PUBLIC	Database_Events	filter(e.DeviceCategory = "DB")
PUBLIC	High_Severity	filter(e.Severity >= 3)
PUBLIC	EventSource_B62672A0-12D3-102A...	filter(e.EventSourceId = "B62672A0-12D3-102A-BD78-000C29512CF1")
PUBLIC	Low_Severity	filter(e.Severity <= 2)
PUBLIC	Firewall_Events	filter(e.DeviceCategory = "FW")
PUBLIC	Correlation	filter((e.SensorType = "C") or (e.SensorType = "W"))
PUBLIC	Exploit_Detection	filter(e.Vulnerability = 1)
PUBLIC	External_Events	filter(((e.SensorType != "I") and (e.SensorType != "A")) and (e.SensorType != "P...")
PUBLIC	EventSource_B62672A0-12D3-102A...	filter(e.EventSourceId = "B62672A0-12D3-102A-BC3D-000C29512CF1")
PUBLIC	ALL	filter(1=1)
PUBLIC	Scan_Events	filter(e.DeviceCategory = "SCAN")
PUBLIC	Severe_Internal	filter(((e.SensorType = "I") or (e.SensorType = "A")) and (e.Severity >= 3))
PUBLIC	Internal_Events	filter((e.SensorType = "A") or (e.SensorType = "I"))

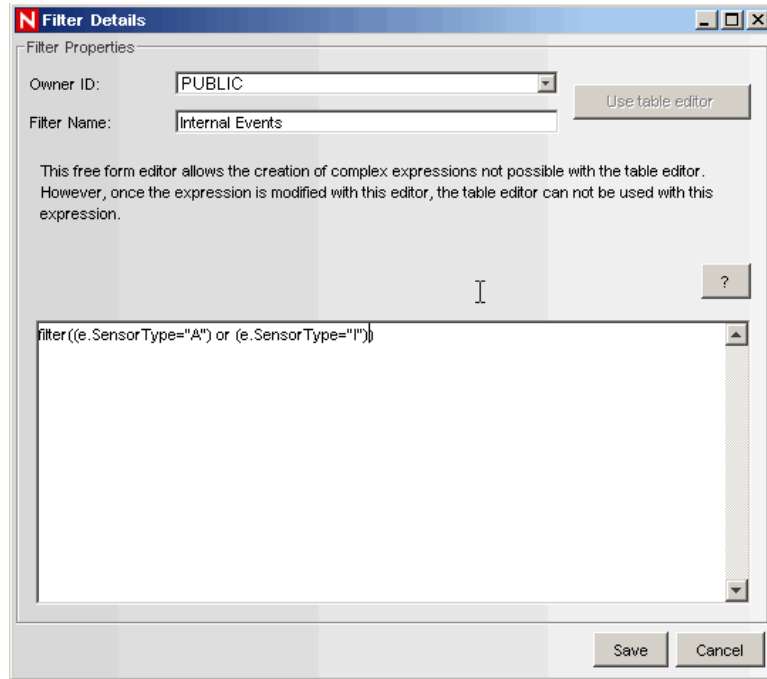
To recreate a Sentinel 6 public filter:

1. Log into the Sentinel Control Center as a user with permissions to create public filters.
2. Click Admin tab.
3. Click Admin > Filter Manager. Alternatively select File Manager under the Filter Configuration folder in the navigator. Click Add.
4. Select an Owner ID (public or private [user owned]).

5. Enter a Filter Name.
6. Click Use free form editor to display a free form editor.

NOTE: The free form editor allows you to create complex expressions not possible with the table editor. However, once the expression is modified with the free form editor, the table editor cannot be used with the expression.

7. Enter a filter expression from the screenshot above to define the new filter.



8. Click *Save*.

For information on creating a Global Filter in Sentinel 6, see [Administration](#) in *Sentinel 6.0 User's Guide*.

2 Patching from Sentinel 5.1.3 to Sentinel 6.0

Topics included in this chapter:

	<u>Topic</u>	<u>Page</u>
	Overview	2-1
	Notes on Upgrade to Sentinel 6.0	2-1
	Pre-requisites for patching to Sentinel 6.0	2-4
	Patching to Sentinel 6.0	2-5
	Post-Patch Procedures	2-9

Overview

Novell provides a Sentinel 6.0 patch installer to upgrade your existing Sentinel 5.1.3 installation to Sentinel 6.0. This patch installer will maintain most of your Sentinel 5.1.3 configuration settings through the patch process, resulting in a Sentinel 6.0 installation that is setup much like your Sentinel 5.1.3 installation.

This patch installer does not support upgrading from a version of Sentinel 5.x previous to 5.1.3. If you are currently on a version of Sentinel 5.x previous to 5.1.3, first run the Sentinel 5.1.3 patch installer to upgrade your system to 5.1.3. Then run the Sentinel 6.0 patch installer to upgrade your system to 6.0.

Additionally, this patch installer does not support upgrading from Sentinel 4.2.x. If you are currently running Sentinel 4.2.x, see [Chapter 1, “Migrate from Sentinel 4.2.x to Sentinel 6”](#).

NOTE: The Sentinel 6.0 patch installer will work fine with any service pack or hotfix you may have applied on top of Sentinel 5.1.3.

IMPORTANT (for Japanese, Traditional Chinese, or Simplified Chinese users):

The patch installer supports migrating from a non-Unicode database to another non-Unicode database. It cannot migrate data from a non-Unicode database to a Unicode database. Since a Unicode database is necessary to achieve the full functionality of Sentinel 6.0 (and future versions) in Japanese, Traditional Chinese, or Simplified Chinese, Novell strongly recommends that customers using these languages perform a new installation of the Sentinel 6 database components using the Unicode database option. For customers using these languages, the patch installer is only recommended for the non-database Sentinel components.

Notes on Upgrade to Sentinel 6.0

On patching to Sentinel 6.0, you will observe that some system settings are updated by the patch installer. Others system settings must be updated manually in order to work with Sentinel 6.0, as described below:

Automatic updates

The items listed below are automatically updated by the Patch Installer. They are either copied to the Sentinel 6.0 installation directory (if they are stored on the file system) or updated in the database.

<u>Item</u>	<u>Description</u>
Communication Server message bus port settings	The message bus application and related configuration files have been updated in Sentinel 6.0. The patch installer will maintain the message bus port used in Sentinel 5.1.3
Events, including Correlated Events	Existing event tables will get updated with the new event tags and indexes that have been added to the event schema.
Users and Roles	The user and role settings stored in the iTRAC schema will be recreated in the new iTRAC schema that is installed when applying the patch.
Event Configurations (for example, event tag name, mapping config)	The default name and mapping configuration of some of the event tags has changed in Sentinel 6.0. Additionally, new event tags have been introduced, for which new event configuration entries will be added.
User Created Filters	Filters that are stored in the database with the “long name” of an event tag in their expression will be modified to only contain the “tag name”. This only affects how the filter is stored in the database. The “long name” will still appear when viewing or editing a filter in Sentinel Control Center.
SDM partition management settings	

The table below gives you an overview of the files that are automatically updated and the source (Sentinel 5.1.3) and destination (Sentinel 6.0) locations of these files, for easy reference.

<u>Item</u>	<u>Sentinel 5.1.3</u>	<u>Sentinel 6.0</u>
Map Source Data	ESEC_HOME\sentinel\bin\map_data	ESEC_HOME\data\map_data
E-mail Server settings (execution.properties)	ESEC_HOME\sentinel\config	ESEC_HOME\config
Sentinel License key (.primary_key)	ESEC_HOME\utilities	ESEC_HOME\config
DAS and Advisor xml	ESEC_HOME\sentinel\config	ESEC_HOME\config

configuration files	ig	
Advisor scheduled task or cron job	ESEC_HOME\sentinel\bin	ESEC_HOME\bin
* HP SD “attach” folder contents	ESEC_HOME\3rdparty\integration\attach	ESEC_HOME\3rdparty\integration\attach
* Aggregation event files (awaiting processing by the Aggregation Service)	ESEC_HOME/sentinel/bin/eventfiles	ESEC_HOME/data/event s/aggregation
* Event insert error files (event files are cached in this directory if there is a database insert error)	ESEC_HOME/sentinel/bin/eventInsertBuffer & ESEC_HOME/sentinel/bin/eventProcessingBuffer	ESEC_HOME/data/event s/insertErrorBuffer & ESEC_HOME/data/event s/processingErrorBuffer
Collector Scripts	ESEC_HOME\wizard\Elements	ESEC_HOME/data/collector_workspace
Sentinel Control Center Local Preferences (Preference file location)	ESEC_HOME/sentinel/console	ESEC_HOME/config
Menu configuration executables on UNIX that are not symbolic links	ESEC_HOME/sentinel/exec	ESEC_HOME/config/exec

NOTE: The location of directories marked with an “*” are customizable. Therefore, the actual location of these directories may not match the default location stated above. If one or more of the directories marked with an “*” have been customized, a few configuration files must be updated manually in order to maintain this custom configuration. Follow the instructions in the section [“Customized Sentinel Server Data Directories”](#) to update your configuration.

Manual Updates

The items listed below are to be updated manually in order for the related existing Sentinel 5.1.3 data to work properly in Sentinel 6.0. Follow the link provided to each item below to see procedures for manual updates.

- [“Sentinel User Permissions”](#)
- [“Collector Port configurations”](#)
- [“Correlation Rules”](#)
- [“Default Filters”](#)
- [“Menu Configuration Executables”](#)
- [“Crystal Reports”](#)
- [“Message Bus Encryption key”](#)
- [“Customized Sentinel Server Data Directories”](#)

Not updatable

These items cannot be updated from Sentinel 5.1.3 to Sentinel 6.0. Any data related to these items will be lost in the patch to Sentinel 6.0.

<u>Item</u>	<u>Description</u>
iTRAC templates, processes, and work items	The iTRAC workflow engine and database has been upgraded. Any existing iTRAC data will be lost.
OCI and ADO event insert strategy settings	These strategies are not supported in Sentinel 6.0. Due to performance

	improvements in the JDBC event insertion strategy, it is likely you will not need these other strategies to handle your event rate. If you find this is not the case, please contact Novell Technical Support to find an appropriate solution.
Asset Data	The asset database schema has been improved. Any asset data already loaded into Sentinel will be removed. This does not affect asset map data loaded directly from the asset.csv file. This also does not affect asset data loaded after applying the Sentinel 5.1.3 "Asset" hotfix.

Not affected by patch

These items are not affected by the patch to Sentinel 6.0. Any data related to these items will not be modified during the patch and will work in Sentinel 6.0.

- Global Filters
- Reporting Configuration
- Incident Categories
- Vulnerabilities
- Incidents
- Advisor Data

Pre-requisites for patching to Sentinel 6.0

The following are several steps that should be taken before upgrading from Sentinel 5.1.3 to Sentinel 6.0.

- Stop Sentinel services before running the patch installer.
- **“Export Sentinel 5.1.3 Correlation Rules”** to file. After the patch to Sentinel 6.0 is complete, you will be able to import these back in.
- Ensure that each machine in the Sentinel system meets the minimum system requirements for Sentinel 6.0. Some of the minimum system requirements have changed between Sentinel 5.1.3 and Sentinel 6.0.
- Ensure that a Sentinel 6-certified operating system is installed.

NOTE: Sentinel 6.0 does not support Windows 2000 for Sentinel Server, so if this version of Windows is currently being used by Sentinel 5.1.3, it must first be upgraded to Windows 2003 before running the Sentinel 6 Patch installer. Use Microsoft’s Windows 2003 upgrade utility to upgrade the operating system.

- Ensure that a Sentinel 6-certified database is installed.

NOTE: Sentinel 6.0 does not support MS SQL Server 2000, so if this version of MS SQL Server is currently being used by Sentinel 5.1.3, it must first be upgraded to MS SQL Server 2005 before running the Sentinel 6 Patch installer. Use Microsoft’s SQL Server 2005 upgrade utility to upgrade the database.

- If you will not be installing directly from the Sentinel 6.0 Patch installer CD-ROM, create a directory with ASCII-only characters (and no special characters) from which to run the installer.

Related Topics:

- For information on System Requirements, Supported Operating Systems and databases, see “[Best Practices](#)” in *Sentinel 6.0 Installation Guide*.
- To export Sentinel 5.1.3 Correlation Rules, see “[Exporting Correlation Rules in Sentinel 5.1.3](#).”

Exporting Correlation Rules in Sentinel 5.1.3

To export Sentinel 5.1.3 Correlation Rules:

1. Login to the Sentinel 5.1.3 Sentinel Control Center.
2. Go to the *Admin* Tab and open *Correlation Rules* by selecting *Correlation Rules* from the *Admin* menu or click the *Display Correlation Rules* button.
3. In the *Correlation Rules* window, right-click on the rule folder you want to export and select *Export Rule Folder*.
4. Browse to the location you want to save this Rule folder and save it as an .xml file.

Patching to Sentinel 6.0

To patch to Sentinel 6.0:

1. Obtain the Sentinel 6.0 Patch installer CD.
2. On Solaris/Linux, login as the root user; On Windows, login as an administrator user.
3. Insert (and mount on Solaris/Linux only) the Sentinel 6.0 Patch installer CD.
4. Start the Sentinel 6.0 Patch installer by executing the following:

- On Windows

```
setup.bat
```

- On Solaris/Linux:

For GUI mode:

```
./setup.sh
```

Or for textual (“headless”) mode:

```
./setup.sh -console
```

NOTE: Windows does not support installation in headless mode.

5. Click the down-arrow and select one of the following language choices:

English	Italian
French	Portuguese (Brazil)
German	Spanish
Simplified Chinese	Japanese
Traditional Chinese	
6. After reading Welcome screen, click *Next*.
7. Read and accept the End User License Agreement and click *Next*.
8. Shutdown all Sentinel applications currently running on this machine.
9. Accept the default install directory or click *Browse* to specify your Sentinel 6.0 installation location. Click *Next*.

IMPORTANT: You cannot install into a directory with special characters or non-ASCII characters.

Also, you cannot install into the same directory where the existing Sentinel 5.1.3 is installed.

10. If Sentinel Control Center is currently installed, the patch installer will prompt for the maximum memory space to be allocated to Sentinel Control Center. Enter the desired JVM heap size (MB). Click *Next*.
11. If the Sentinel Control Center or Communication Server component is currently installed, the patch installer will prompt for the Communication Server proxy server ports. Enter the required information and click *Next*.
 - **Sentinel Control Center Proxy Port:** The port the SSL proxy server (DAS Proxy) is listening to accept username and password based authenticated connections. Since Sentinel Control Center prompts for a username and password, it uses this port to connect to Sentinel Server.
 - **Collector Manager Certificate Authentication Proxy Port:** The port the SSL proxy server (DAS Proxy) is listening to accept certificate based authenticated connections. Since Collector Manager cannot prompt for a username and password, it uses this port to connect to Sentinel Server if it is configured to connect through the proxy. This prompt will not be shown if the Communication Server component is not currently installed on this machine.
12. If DAS, Correlation Engine, Collector Manager, or Communication Server is currently installed, the patch installer will prompt for how to obtain the shared message bus encryption key.
 - **Generate random encryption key:** Selecting this option will generate a new AES 128-bit message bus encryption key.
 - **Import encryption key from keystore file:** You will be prompted to navigate to the location of an existing .keystore file.

NOTE: If you chose to import Sentinel 5.1.3 keystore file, see [“Enabling AES 256-bit Message Bus Encryption”](#).

Click *Next*.

NOTE: All components connecting directly to the message bus must share the same encryption key. Novell recommends generating a random encryption key when installing the Communication Server and importing this key when installing components on other machines. Components that connect through the proxy do not need the shared message bus encryption key.

The .keystore file will be placed at \$ESEC_HOME/config on Linux/Solaris or %ESEC_HOME%\config on Windows.

13. If DAS, Correlation Engine, Collector Manager, or Communication Server are currently installed, the patch installer will prompt for the amount of memory (RAM) to allocate to these Sentinel Server processes. The installer will factor in operating system and database overhead when determining what allocation options to display. There are two ways to specify memory allocation:
 - **Automatic Memory Configuration:** Select the total amount of memory to allocate to Sentinel Server. The installer will automatically determine the optimal distribution of memory across components taking into account estimated operating system and database overhead.

- **Custom Memory Configuration:** Click the *Configure* button to fine-tune memory allocations. This option will not be available if there is too little memory on the machine.

Click *Next*.

14. If DAS is currently installed and the Sentinel Application user (for example, *esecapp*) is a Windows Authentication user, the patch installer will prompt for the Sentinel Application user's username and password. After entering the required information, click *Next*.
15. A summary screen with the features selected for installation will appear. Click *Install*.
16. If you haven't applied Sentinel 6.0 Database Patch already, apply Sentinel 6.0 Database patch by following the instructions in one of the following sections:
 - "Patching to Sentinel 6.0 Database When Using Oracle"
 - "Patching to Sentinel 6.0 Database When Using Microsoft SQL Server"

TIP: When running the Sentinel Database patch, if you run it on a machine where the Sentinel 6 Patch InstallShield was already installed, you will automatically have the Java version 1.5 binaries that are necessary to apply the database patch. Alternately, you can install Java version 1.5 yourself and, therefore, do not require running the InstallShield.

17. On successful installation, you will be prompted to reboot or re-login and start Sentinel Services manually. Click *Finish* close the installer and reboot your system, if selected.

CAUTION: Do not reboot or start Sentinel services until you've applied the Sentinel Database patch. Doing so may result in invalid changes being made to your Sentinel 5.1.3 database.

18. Perform the post patch procedures as described in "Post-Patch Procedures".

Patching to Sentinel 6.0 Database When Using Oracle

The majority of the Sentinel Database patch script for Oracle can be run from any machine that has Java version 1.5 and the Oracle client tools installed. If the script is run on a separate machine than where the Sentinel Database instance is located, the Sentinel Database patch script will remotely connect to the Sentinel Database instance to apply the patch. There is, however, one script that must be run on the machine where the Oracle instance is located. Instructions for running this script are included in the steps below.

NOTE: If the Sentinel 6 Patch InstallShield was run on the machine where you are performing the Sentinel database patch, then it is likely Java version 1.5 is installed in the *\$ESEC_HOME/jre* directory. The permissions on the *\$ESEC_HOME/jre* directory, however, only allow *root* or a user in the *esec* group to access the directory. Therefore, to enable your current user to access this directory, you can add the user to the *esec* group, modify the permissions on the directory, or install a new instance of Java. Alternatively, you can run the Sentinel Database patch as the *esecadm* user, which is a member of the *esec* group.

If you need to install Java version 1.5, you can download it from the Java website http://java.sun.com/javase/downloads/index_jdk5.jsp by clicking on the *Download* button next to the text *Java Runtime Environment (JRE) 5.0*.

To apply database patch when using Oracle:

1. One script must be run before running the main database patch script on the machine where the Oracle Sentinel Database instance is located. This script creates two additional database tablespaces. This script requires that it be run on the machine where the Oracle Sentinel Database instance is located as a user that has Oracle DBA operating system group permissions. To run this script:

NOTE: If you are using Oracle 10g Automatic Storage Management (ASM), do not execute this pre-patch script. Instead, create the tablespaces *SENT_AUDITD* and *SENT_AUDITX* manually.

NOTE: This pre-patch script does not require Java.

- Log into the database machine as a user that is a member of the Oracle DBA group.
- If not already mounted, mount the Sentinel Patch installer CD.
- Change directories to the *sentinel/dbsetup/bin* directory on the Sentinel Patch installer CD.
- If they do not already exist, create one or two directories to place the two new tablespace's data files (the same directory can be used for both). These directories must be owned by the Oracle software operating system user.
- Execute the command:

```
./PrePatchDb_60.sh <audit_data_tablespace_dir>  
<audit_index_tablespace_dir> <database_name>
```

For Example:

```
./PrePatchDb_60.sh /opt/audit_data /opt/audit_index ESEC
```

- After the script completes, continue to the next step to perform the main database patch installation.
2. Login into a machine that is running one of the UNIX operating systems that are supported by Sentinel as a user that has the Oracle client application *sqlplus* in its *PATH* as well as the environment variable *ORACLE_HOME* set appropriately.

TIP: If the *esecadm* user exists on this machine, logging in as this user will provide the easiest access to an already installed instance of Java.

3. Insert the Sentinel Patch installation CD into the CD-ROM drive.
4. Check your environment variables to ensure that java (version 1.5) is in your *PATH*. You can perform this check by executing the following command on the command line:

```
java -version
```

If the above command does not succeed, then either locate where java is installed on your system or download and install java. Then, update your *PATH* environment variable to include the java executable. For example, if java is installed in the directory:

```
/opt/novell/sentinel6/jre
```

Then add the following to the beginning of your *PATH* environment variable:

```
/opt/novell/sentinel6/jre/bin:
```

5. Open a command prompt. On the command prompt, change directories to the following directory on the Sentinel patch installation CD:

```
sentinel/dbsetup/bin
```
6. Execute the command:

```
./PatchDb.sh
```
7. The script will notify you that if there is a lot of event data in your database, the database patch could take a long time. Drop as much event data as possible and enter *Y* to continue.
8. At the prompt, enter the hostname or IP address of the Oracle server running the Sentinel Database that you want to patch.
9. At the prompt, enter the port number of the Oracle listener the patch script should use access the Sentinel Database to patch. The typical port number is *1521*.
10. At the prompt, enter the Oracle Sentinel Database Net Service Name to patch.
11. At the prompt, enter the Oracle Sentinel Database Service Name (that is, Oracle SID) to patch.
12. At the prompt, enter the password for the Sentinel Database Administrator user *esecdba*.
13. At the prompt, enter whether you want to enable automatic database partition management. It is highly recommended you enter *Y*.
14. If you selected to enable automatic partition management, at the prompt, enter the time of day to schedule the *add partition job*.
15. If you selected to enable automatic partition management, at the prompt, enter the time of day to schedule the *archive partition job*. Give at least an hour and a half between the *add partition job* and the *archive partition job* because these operations should not overlap due to the use of shared resources.
16. The script will verify the entered information.
17. The script will begin patching the database to version Sentinel 6.0.

Patching to Sentinel 6.0 Database When Using Microsoft SQL Server

The Sentinel Database patch script for Microsoft SQL Server can be run from any machine that has Java version 1.5 and the Microsoft SQL Server client tools installed. If the script is run on a separate machine than where the Sentinel Database instance is located, the Sentinel Database patch script will remotely connect to the Sentinel Database instance to apply the patch.

NOTE: If the Sentinel 6 Patch InstallShield was run on the machine where you are performing the Sentinel database patch, then it is likely Java version 1.5 is installed in the `%ESEC_HOME%\jre` directory.

If you need to install Java version 1.5, you can download it from the Java website http://java.sun.com/javase/downloads/index_jdk5.jsp by clicking on the *Download* button next to the text *Java Runtime Environment (JRE) 5.0*.

To apply the database patch when using Microsoft SQL Server:

1. If using Microsoft SQL Server and the Sentinel Database Administrator user (for example, *esecdba*) is a Windows Authentication user, login to Windows as the Sentinel Database Administrator user. Otherwise, log in as an Administrator. The

user you log in as must have the Microsoft SQL Server client tool *osql* in its *PATH*.

2. Insert the Sentinel Patch installation CD into the CD-ROM drive.
3. Check your environment variables to ensure that Java (version 1.5) is in your *PATH*. You can perform this check by executing the following command on the command line:

```
java -version
```

If the above command does not succeed, then either locate where java is installed on your system or download and install java. Then, update your *PATH* environment variable to include the java executable. For example, if java is installed in the directory:

```
C:\Program Files\Novell\Sentinel6\jre
```

Then add the following to the beginning of your *PATH* environment variable:

```
C:\Program Files\Novell\Sentinel6\jre\bin;
```

4. Open a command prompt.
5. On the command prompt, change directories to the following directory on the Sentinel patch installation CD:

```
sentinel\dbsetup\bin
```

6. Execute the command:

```
.\PatchDb.bat
```
7. The script will notify you that if there is a lot of event data in your database, the database patch could take a long time. Drop as much event data as possible and enter *Y* to continue.
8. At the prompt, enter the hostname or IP address of the Microsoft SQL Server of the Sentinel Database that you want to patch.
9. At the prompt, enter the port number of the Microsoft SQL Server Sentinel Database to patch. The typical port number is *1433*.
10. At the prompt, enter the name of the SQL Server Sentinel Database to patch.
11. At the prompt, enter the type of authentication mechanism you are using for the Sentinel Database Administrator user (for example, *esecdba*). Enter option 1 for Windows Authentication or option 2 for SQL Authentication. If you enter option 2, the script will prompt for the *esecdba* password.
12. The script will verify the entered information.
13. At the prompt, enter the directory to place the Audit data tablespace database files. This directory must already exist on the machine where the SQL Server instance is located; this script will not create it.
14. At the prompt, enter the directory to place the Audit index tablespace database files. This directory must already exist on the machine where the SQL Server instance is located; this script will not create it.
15. At the prompt, enter whether you want to enable automatic database partition management. It is highly recommended you enter *Y*.
16. At the prompt, enter the time of day to schedule the *add partition job*.
17. At the prompt, enter the time of day to schedule the *archive partition job*. Give at least an hour and a half between the *add partition job* and the *archive partition*

job because these operations should not overlap due to the use of shared resources.

18. The script will begin patching the database to version Sentinel 6.0.

Post-Patch Procedures

After running the patch installer, you may need to perform some additional tasks depending on the version you are patching from and which components are installed.

- All Versions
 - “Update Sentinel User Permissions”
 - “Importing Sentinel 5.1.3 Correlation Rules”
 - “Migrating Sentinel 5.1.3 Collector Port Configurations”
 - “Updating Default Filters”
 - “Update Menu Configuration Executable”
 - “Importing Crystal Reports”
 - “Enabling AES 256-bit Message Bus Encryption”
 - “Customized Sentinel Server data directories”

Updating Sentinel User Permissions

Sentinel 6.0 contains new permissions that control access to new features in Sentinel Control Center. The Sentinel 6 patch installer does not enable these new permissions automatically. Therefore, if a Sentinel user needs to use a new feature, the user must first be granted to the permission. The steps below describe the new permissions and how to enable them for a user.

To update Sentinel User Permissions:

1. Login Sentinel Control Center as a user with Administration/User Management permission (example, *esecadm*).
2. In Sentinel Control Center, click the *Admin* tab. Expand User Configuration in the Navigation pane or from the navigation bar click *Admin > User Configuration*.
3. Right-click on the user that should have one or more of the new permissions (that is, *esecadm*) and select *User Details*.
4. Click the *Permissions* tab.
5. The following are the new permissions in Sentinel 6.0. Select all permissions the currently selected user should possess. For more information on user permissions that are included in Sentinel 6.0, see [Sentinel Control Center User Permissions in Sentinel 6.0 User's Reference Guide](#).
 - iTRAC
 - Work Item Management
 - Incidents
 - Add Notes
 - Event Source Management
 - View Scratch Pad
 - Manage Plugins
 - View Raw Data
 - Debug Collector
 - Admin
 - Event Configuration


- Mapping Configuration
- Reporting Data
- Correlation
 - View Correlation Tab
 - View/Use Correlation Rule Manager
 - View/Use Correlation Engine Manager
 - View/Use Correlation Action Manager
 - View/Use Dynamic Lists

Click *OK* to save the permission changes.

6. Repeat the steps above for every user that requires one or more of the new permissions.

Importing Sentinel 5.1.3 Correlation Rules

To import Correlation Rules:

1. Log into the Sentinel 6.0 Sentinel Control Center.
2. Open the Correlation Rule Manager in the Correlation Tab. To open, select the Correlation Rule Manager from the Correlation Menu or click the *Correlation Rule Manager* button.
3. In the Correlation Rule Manager window, click the *Import/Export* button . The Import/Export rules wizard will display.
4. Select Import from the Action list and browse to the correlation rules xml file you exported before applying the Sentinel 6 patch. Click *Next*.
5. In the Import Rule window, select the rules you want to import and click *Finish*.

Migrating Sentinel 5.1.3 Collector Port Configurations

Sentinel 6 has a new feature called Event Source Management (ESM) that greatly enhances the Collector management capabilities in Sentinel 5.1.3. Some of these enhancements include:

- Configuration wizards
- Configuration stored centrally in the database
- Raw data filter
- Raw data tap
- Configurability through Sentinel Control Center

Some Collectors may need to be updated before they will work in Sentinel 6. For example, collectors that performed log file rotation using the Collector code will no longer work because of changes to the GETCONFIG command.

In addition, Collector port configurations from Sentinel 5.1.3 must be migrated into ESM in order to continue to collect data from your event sources after you've upgraded to Sentinel 6. The following steps are necessary to perform this migration:

To migrate Sentinel 5.1.3 Collector Port Configuration into Sentinel 6 ESM:

NOTE: Ensure that all Sentinel 5.1.3 Collector Scripts that you are using are located on the local machine where you are running Sentinel Control Center. If necessary, copy the Collector Scripts from the ESEC_HOME/wizard/Elements directory of all Collector Manager machines.

1. Log into Sentinel Control Center as the *esecadm* user. Ensure that you have enabled the *Event Source Management -> Manage Plug-ins* user permission as described in the section “**Updating Sentinel User Permissions**”.
2. Select the *Event Source Management -> Live View...* menu bar option.
3. Import all your Collector Scripts by selecting the menu option *Tools->Import Plug-in...* from the ESM view and navigating to the location where the Collector Script you wish to import is stored. Repeat this for every Collector Script you were using in Sentinel 5.1.3.
4. Download all of the Connector Plug-ins you need from <http://support.novell.com/products/sentinel/connectors.html>. Import these plug-ins in the same way you imported the Collector Script in the previous step.
5. See Event Source Management, in the *Sentinel6.0 User's Guide* for information on how to deploy the Collector Scripts and Connector Plug-ins you just imported. Using ESM, you will be able to connect to and start processing data from all of the sources of event data you were receiving data from in Sentinel 5.1.3.

Related Topics:

- For additional information on Event Source Management and related topics, see **Event Source Management** in *Sentinel6.0 User's Guide*.
- For information on deploying Collectors and Connectors for users who are familiar with Sentinel 5.1.3, see the *Migrating to Sentinel 6* collection of documents available on the [Sentinel 6 documentation website](http://www.novell.com/documentation/sentinel6). (<http://www.novell.com/documentation/sentinel6>). These documents also describe differences between collector and connector functionality between Sentinel 5 and Sentinel 6.

Updating Default Filters

Sentinel comes installed with a set of default filters that are useful for analyzing general event data. The default filters in a clean install of Sentinel 6.0 differ from the default filters in Sentinel 5.1.3. The steps below indicate how to update Sentinel 5.1.3 default filters to match the Sentinel 6.0 default filters.

To update Default Filters in Sentinel 6.0:

1. *Internal_Events* – Add a clause to the filter to include events that have a *Sensor Type* set to *A*. The resulting filter expression looks like:


```
filter( ( e.SensorType = "A" ) or ( e.SensorType = "I" ) )
```
2. *Severe_Internal* – Add a clause to the filter to include events that have a *Sensor Type* set to *A*. The resulting filter expression looks like:


```
filter( ( ( e.SensorType = "I" ) or ( e.SensorType = "A" ) ) and ( e.Severity >= 3 ) )
```
3. *External_Events* – Add clauses to the filter to exclude events that have a *Sensor Type* of *A* and *P*. The resulting filter expression looks like:


```
filter( ( ( e.SensorType != "I" ) and ( e.SensorType != "A" ) ) and ( e.SensorType != "P" ) )
```
4. *Real_Time* – This is a new filter in Sentinel 6.0. This filter includes only events that have *Sensor Type* set to *T*. The events included in this filter are only sent to the real-time system and, therefore, are not stored in the database. The resulting filter expression looks like:

```
filter( e.SensorType = "T" )
```

Updating Menu Configuration Executables

In order to launch an executable from the Menu Configuration feature, Sentinel 6.0 requires (for security reasons) that the executable be located in the directory `$ESEC_HOME/config/exec` (UNIX) or `%ESEC_HOME%\config\exec` (Windows). This policy creates a “sandbox” of executables that can be executed from Sentinel Control Center, making all executables not in this directory invisible to the Sentinel Control Center user.

The enforcement of this policy in Sentinel 6.0 requires some manual patch steps are performed in order for Sentinel 5.1.3 Menu Configuration actions to continue to work. The manual patch steps differ depending on which operating system the DAS component is installed. Follow the instructions below that are appropriate for the operating system where the DAS component is installed.

On Unix:

The Sentinel 6.0 Patch installer will automatically copy files from your existing Sentinel 5.1.3 “sandbox” directory located at `$ESEC_HOME/sentinel/exec` to the new Sentinel 6 “sandbox” directory. However, if any of the copied files are symbolic links, Sentinel 6.0 will not allow them to be executed because the symbolic link resolves to a file that is not under the “sandbox” directory.

Therefore, any symbolic link files must be converted to simple scripts that, internally, execute the desired command.

For example:

To convert a symbolic link to the command `/bin/ping` to a script:

1. Create a file with the following text in the `$ESEC_HOME/config/exec` directory:

```
#!/bin/sh
/bin/ping $*
```
2. Set the permissions on the file to be readable and executable by the `esecadm` user.
3. Make sure the name of this file match the name of the symbolic link it is replaces. This avoids having to update the Menu Configuration entry.

On Windows:

Sentinel 5.1.3 did not enforce a “sandbox” directory. Since there was no “sandbox” directory in Sentinel 5.1.3, the Sentinel 6.0 Patch installer will only install the default Menu Configuration executables in the Sentinel 6.0 “sandbox” directory `%ESEC_HOME%\config\exec`.

As a result, all Menu Configuration actions in your Sentinel 5.1.3 installation must either have their binary executable moved to the “sandbox” directory or have a simple script written to execute them from the “sandbox” directory.

For example:

To create a script to launch the executable `ping`:

1. Create a `ping.bat` file with the following text in the `%ESEC_HOME%\config\exec` directory:

```
ping.exe %*
```

2. Log into the Sentinel Control Center.
3. Open the Menu Configuration dialog by navigating to *Admin (tab) -> Menu Configuration*.
4. Update all Menu Configuration entries that execute the command *ping* to now execute the command *ping.bat*.

Importing Crystal Reports

After patching to Sentinel 6.0, you must import the reports from the latest Sentinel Reports Distribution. For more information, see [Crystal Reports on Windows](#) and [Crystal Reports on Linux and Solaris](#) in *Sentinel 6.0 Installation Guide*. To obtain the latest reports, go to <http://support.novell.com/products/sentinel/reports.html>.

Enabling AES 256-bit Message Bus Encryption

Sentinel 6.0, by default, uses AES 128-bit encryption to encrypt messages on the message bus. Sentinel 5.1.3, by default, used AES 256-bit encryption. This change was a result of Sentinel 6.0 switching to the built-in Java JCE.

Due to this change, the Sentinel 6.0 patch installer will prompt you to either generate a new AES 128-bit encryption key or import your Sentinel 5.1.3 AES 256-bit encryption key. If you selected to import your Sentinel 5.1.3 AES 256-bit encryption key, before running Sentinel 6.0 you must enable AES 256-bit encryption in Sentinel 6.0 by following the instructions in the [Enabling Unlimited AES Key Strength in Communication Layer \(iSCALE\)](#), of *Sentinel 6.0 Installation Guide*.

NOTE: If an AES 256-bit encryption key is used in Sentinel 6.0 without AES 256-bit encryption being enabled, Sentinel Server will not work and errors related to encryption keys will appear in the Sentinel Server log files.

Customized Sentinel Server Data Directories

Sentinel Server uses a number of data directories, some of them are customizable for performance or data assurance reasons. The table below lists the data directories that are customizable in Sentinel 5.1.3 and their default locations in Sentinel 5.1.3 and 6.0.

<u>Item</u>	<u>Sentinel 5.1.3</u>	<u>Sentinel 6.0</u>
HP SD “attach” folder contents	ESEC_HOME\3rdparty\integration\attach	ESEC_HOME\3rdparty\integration\attach
Aggregation event files (awaiting processing by the Aggregation Service)	ESEC_HOME/sentinel/bin/eventfiles	ESEC_HOME/data/event s/aggregation
Event insert error files (event files are cached in this directory if there is a database insert error)	ESEC_HOME/sentinel/bin/eventInsertBuffer & ESEC_HOME/sentinel/bin/eventProcessingBuffer	ESEC_HOME/data/event s/insertErrorBuffer & ESEC_HOME/data/event s/processingErrorBuffer

The Sentinel 6.0 patch installer does not account for customizations of the locations of the directories above. It will simply set the location back to the default location. Therefore, if your Sentinel 5.1.3 Server installation contains custom locations for any of the directories above, a few configuration files must be manually updated after the patch installation in order for Sentinel Server to continue accessing the files in their custom location.

To update configuration file for custom HP SD “attach” folder:

1. Backup the *ESEC_HOME/config/das_query.xml* file.
2. Open the file *ESEC_HOME/config/das_query.xml* in a text editor.
3. Search for the property name *attachment_path* and change its value to the custom directory location.
4. Save your changes and verify the xml syntax is correct by, for example, opening the file in a web browser.

To update configuration file for custom Aggregation event files:

1. Backup the *ESEC_HOME/config/das_binary.xml* and *ESEC_HOME/config/das_aggregation.xml* files.
2. Open the file *ESEC_HOME/config/das_binary.xml* in a text editor.
3. Search for the component name *EventFileRedirectService*. Under this component you will find two properties named *directory* and *outputDirectory*. Modify the value of both of these properties to match the custom value used in Sentinel 5.1.3
4. Open the file *ESEC_HOME/config/das_aggregation.xml* in a text editor.
5. Search for the property name *directory* and change its value to the value given for property name *outputDirectory* in the *das_binary.xml* file.
6. Save your changes to both files and verify the xml syntax is correct for example, by opening the file in a web browser.

To update configuration file for custom Aggregation event files:

1. Backup the *ESEC_HOME/config/das_binary.xml* file.
2. Open the file *ESEC_HOME/config/das_binary.xml* in a text editor.
3. Search for the property name *rootDirectory*. You’ll find two occurrences of this property, one under the *EventProcessingErrorHandler* component and the other under the *EventInsertErrorHandler* component. Modify the value of both of these properties to match the custom value used in Sentinel 5.1.3.
4. Save your changes to both files and verify the xml syntax is correct for example, by opening the file in a web browser.