

# Installation Guide

## Novell® Sentinel™

**6.1 SP2**

June 2010

[www.novell.com](http://www.novell.com)



## 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. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 1999-2011 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.  
404 Wyman Street, Suite 500  
Waltham, MA 02451  
U.S.A.  
[www.novell.com](http://www.novell.com)

*Online Documentation:* To access the latest online documentation for this and other Novell products, see the [Novell Documentation Web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

## Novell Trademarks

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

## Third-Party Materials

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

# Contents

<b>Preface</b>	<b>7</b>
<b>1 Introduction</b>	<b>9</b>
1.1 Sentinel Overview	9
1.2 Sentinel User Interfaces	10
1.2.1 Sentinel Control Center	10
1.2.2 Sentinel Data Manager	11
1.2.3 Sentinel Solution Designer	11
1.2.4 Sentinel Collector Builder	11
1.3 Sentinel Server Components	11
1.3.1 Sentinel Server	11
1.3.2 Sentinel Communication Server	12
1.3.3 Sentinel Database	12
1.3.4 Sentinel Collector Manager	12
1.3.5 Correlation Engine	12
1.3.6 iTRAC	12
1.3.7 Crystal Reports Server	12
1.3.8 Sentinel Advisor and Exploit Detection	12
1.4 Sentinel Plugins	13
1.4.1 Collectors	13
1.4.2 Connectors and Integrators	13
1.4.3 Correlation Rules and Actions	13
1.4.4 Reports	14
1.4.5 iTRAC Workflows	14
1.4.6 Solution Packs	14
1.5 Language Support	14
<b>2 System Requirements</b>	<b>15</b>
2.1 Supported Software	15
2.1.1 Patch Levels	15
2.1.2 Database Supported Platforms	16
2.1.3 Sentinel Component Supported Platforms	17
2.1.4 Platform Support Exceptions and Cautions	19
2.2 Hardware Recommendations	19
2.2.1 Architecture Considerations	20
2.2.2 Supported Hardware	21
2.2.3 Proof of Concept Configuration	22
2.2.4 Production Configuration	22
2.2.5 High-Performance Production Configuration	24
2.2.6 Virtual Environments	25
2.3 Recommended Collector Manager Limits	25
<b>3 Installing Sentinel 6.1 SP2</b>	<b>27</b>
3.1 Installer Overview	27
3.2 Sentinel Configurations	28
3.2.1 Linux	28
3.2.2 Solaris	29
3.2.3 Windows	29

3.2.4	High-Performance Configuration .....	29
3.3	Port Numbers Used for Sentinel 6.1 .....	31
3.4	General Installation Prerequisites .....	31
3.4.1	Providing Power User Privileges to Domain Users .....	33
3.4.2	Sentinel Database Installation Prerequisites .....	33
3.4.3	Authentication Mode Settings on SQL .....	36
3.4.4	Sentinel Server Installation Prerequisites .....	37
3.5	Simple Installation .....	37
3.6	Custom Installation .....	39
3.6.1	Starting the Installation .....	40
3.6.2	Configuring the Database on Windows .....	44
3.6.3	Configuring the Database on Linux or Solaris .....	45
3.6.4	Completing the Installation .....	48
3.6.5	Console Installation on Linux or Solaris .....	49
3.7	Installing Sentinel as a Domain user .....	51
3.8	Post-Installation Configuration .....	51
3.8.1	Configuring the SMTP Integrator to Send Sentinel Notifications .....	51
3.8.2	Sentinel Database .....	52
3.8.3	Collector Service .....	52
3.8.4	Starting the Collector Manager Service .....	52
3.8.5	Configuring the Light weight Collector Manager .....	53
3.8.6	Managing Time .....	55
3.8.7	Modifying Oracle dbstart and dbshut scripts .....	55
3.8.8	High-Performance Configuration .....	56
3.9	LDAP Authentication .....	58
3.9.1	Configuring the Sentinel 6.1 Server for LDAP Authentication .....	58
3.9.2	Configuring Multiple LDAP Servers for Failover .....	62
3.9.3	Migrating LDAP User Accounts from Sentinel 6.1 SP1 Hotfix 2 to Sentinel 6.1 SP2 .....	64
3.10	Updating the License Key .....	65
3.10.1	Unix .....	65
3.10.2	Windows .....	65
<b>4</b>	<b>Testing the Installation</b> .....	<b>67</b>
4.1	Testing the Installation .....	67
4.2	Clean Up from Testing .....	75
4.3	Getting Started .....	76
<b>5</b>	<b>Adding Sentinel Components</b> .....	<b>77</b>
5.1	Adding Sentinel Components to an Existing Installation .....	77
5.2	Installing Additional Load Balancing Nodes .....	77
5.2.1	Multiple DAS_Binary Processes .....	78
<b>6</b>	<b>Communication Layer (iSCALE)</b> .....	<b>87</b>
6.1	SSL Proxy and Direct Communication .....	88
6.1.1	Sentinel Control Center .....	88
6.1.2	Collector Manager .....	89
6.2	Changing the Communication Encryption Key .....	90
6.3	Increasing AES Key Strength .....	91
<b>7</b>	<b>Crystal Reports for Windows</b> .....	<b>93</b>
7.1	Overview .....	93

7.2	System Requirements . . . . .	94
7.3	Configuration Requirements . . . . .	95
7.4	Installation Overview . . . . .	95
7.4.1	Installation Overview of Crystal Reports Server with SQL Server 2005 . . . . .	96
7.4.2	Installation Overview of Crystal Reports Server with Oracle . . . . .	97
7.5	Installation . . . . .	97
7.5.1	Installing Microsoft Internet Information Server (IIS) and ASP.NET . . . . .	98
7.5.2	Installing Crystal Reports Server for SQL Server 2005 with Windows Authentication . . . . .	98
7.5.3	Installing Crystal Reports Server for SQL Server 2005 with SQL Authentication . . . . .	102
7.5.4	Installing Crystal Reports Server for Oracle . . . . .	105
7.6	Downloading the Service Packs for Crystal Reports . . . . .	108
7.7	Configuring Crystal Reports Server to Work with the Sentinel Control Center . . . . .	108
7.7.1	Configuring inetmgr . . . . .	108
7.7.2	Patching Crystal Reports . . . . .	109
7.8	Publishing Crystal Report Templates . . . . .	111
7.8.1	Using the Solution Manager to Publish Report Templates . . . . .	112
7.8.2	Using the Crystal Publishing Wizard to Publish Report Templates . . . . .	112
7.8.3	Using the Central Management Console to Publish Report Templates . . . . .	114
7.8.4	Setting a Named User Account . . . . .	115
7.8.5	Configuring Report Permissions and Testing Connectivity . . . . .	115
7.8.6	Disabling the Sentinel Top 10 Reports . . . . .	116
7.8.7	Configuring the Sentinel Control Center to Integrate with Crystal Reports Server . . . . .	117
7.9	High-Performance Configurations for Crystal . . . . .	118
7.9.1	Increasing the Report Refresh Record Limit for Crystal Reports Server . . . . .	118
7.9.2	Using the Aggregation Service for Reports . . . . .	119
7.9.3	Report Development . . . . .	120
7.10	Using Crystal Reports . . . . .	120
7.11	Uninstalling Crystal Reports . . . . .	120

## **8 Crystal Reports for Linux 121**

8.1	Overview . . . . .	122
8.2	Installation . . . . .	122
8.2.1	Pre-Install Crystal Reports Server XI R2 . . . . .	122
8.2.2	Installing Crystal Reports Server XIR2 . . . . .	124
8.2.3	Patching Crystal Reports . . . . .	126
8.3	Downloading the Service Packs for Crystal Reports . . . . .	127
8.4	Publishing Crystal Reports Templates . . . . .	127
8.4.1	Publishing Report Templates using Solution Manager . . . . .	128
8.4.2	Publishing Report Templates – Crystal Publishing Wizard . . . . .	129
8.4.3	Publishing Report Templates – Central Management Console . . . . .	131
8.5	Using the Crystal XI R2 Web Server . . . . .	132
8.5.1	Testing connectivity to the Web Server . . . . .	132
8.5.2	Setting a “Named User” Account . . . . .	132
8.5.3	Configuring Reports Permissions . . . . .	133
8.6	Increasing Crystal Reports Server Report Refresh Record Limit . . . . .	133
8.7	Configuring Sentinel Control Center to Integrate with Crystal Reports Server . . . . .	134
8.8	Utilities and Troubleshooting . . . . .	135
8.8.1	Starting MySQL . . . . .	135
8.8.2	Starting Tomcat . . . . .	135
8.8.3	Starting Crystal Reports Servers . . . . .	135
8.8.4	Crystal Host Name Error . . . . .	135
8.8.5	Cannot Connect to CMS . . . . .	136
8.9	High-Performance Configurations for Crystal . . . . .	136
8.9.1	Reports Using Aggregation Service . . . . .	137
8.9.2	Report Development . . . . .	138

8.10	Using Crystal Reports .....	138
<b>9</b>	<b>Uninstalling Sentinel</b> .....	<b>139</b>
9.1	Uninstalling Sentinel .....	139
9.1.1	Uninstall for Solaris and Linux .....	139
9.1.2	Uninstall for Windows .....	140
9.2	Post-Uninstall .....	140
9.2.1	Sentinel Settings .....	141
<b>A</b>	<b>Pre-installation Questionnaire</b> .....	<b>147</b>
<b>B</b>	<b>Oracle Setup</b> .....	<b>149</b>
B.1	Installing Oracle 11g .....	149
B.1.1	Oracle 11g Installation on SLES 11 .....	149
B.1.2	Oracle 11g Installation on SLES 10 .....	151
B.1.3	Oracle 11g Installation on Red Hat Linux 4 .....	152
B.1.4	Oracle 11g Installation on Solaris 10 .....	154
B.2	Upgrading the Database from Oracle 10g to Oracle 11g .....	156
B.3	Installing Oracle 10g .....	157
B.3.1	Oracle 10g Installation on SLES 10 .....	157
B.3.2	Oracle 10g Installation on Red Hat Linux 4 .....	158
B.3.3	Oracle 10g Installation on Solaris 10 .....	160
B.4	Configuring the System for Oracle Database Installation .....	160
B.4.1	Setting Kernel Values .....	160
B.4.2	Creating Group and User Accounts for Oracle (Solaris Only) .....	163
B.4.3	Setting Environment Variables for Oracle (Solaris Only) .....	163
B.4.4	Installing Oracle .....	163
B.5	Manual Oracle Instance Creation (Optional) .....	164
<b>C</b>	<b>Sentinel with Oracle Real Application Clusters</b> .....	<b>167</b>
C.1	Configuring the Oracle RAC Database .....	167
C.1.1	Creating the RAC Database .....	167
C.1.2	Creating the Sentinel Tablespaces .....	170
C.1.3	Creating the Sentinel Database User .....	171
C.2	Installing the Sentinel Database .....	171
C.3	Configuring the Connection Properties File .....	173
C.4	Configuring the Connection for Sentinel Data Manager .....	174
C.4.1	Known Issue .....	174
C.5	Configuring the Connection for Crystal Enterprise Server .....	174

# Preface

Sentinel is a security information and event management solution that receives information from many sources throughout an enterprise, standardizes it, prioritizes it and presents it to you to make threat, risk and policy related decisions.

This guide describes the installation procedures for Sentinel 6.1 SP2.

- ◆ Chapter 1, “Introduction,” on page 9
- ◆ Chapter 2, “System Requirements,” on page 15
- ◆ Chapter 3, “Installing Sentinel 6.1 SP2,” on page 27
- ◆ Chapter 4, “Testing the Installation,” on page 67
- ◆ Chapter 5, “Adding Sentinel Components,” on page 77
- ◆ Chapter 6, “Communication Layer (iSCALE),” on page 87
- ◆ Chapter 7, “Crystal Reports for Windows,” on page 93
- ◆ Chapter 8, “Crystal Reports for Linux,” on page 121
- ◆ Chapter 9, “Uninstalling Sentinel,” on page 139
- ◆ Appendix A, “Pre-installation Questionnaire,” on page 147
- ◆ Appendix B, “Oracle Setup,” on page 149
- ◆ Appendix C, “Sentinel with Oracle Real Application Clusters,” on page 167

## Audience

This documentation is intended for Information Security Professionals.

## Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation and enter your comments there.

## Additional Documentation

For information on using Sentinel Control Center, see *Sentinel 6.1 User Guide*.

For information on Sentinel event fields, user accounts, permissions, and so on, see *Sentinel 6.1 Reference Guide*.

For information on developing Collectors (proprietary or JavaScript) and JavaScript Correlation actions, go to the Sentinel SDK Web site: [http://developer.novell.com/wiki/index.php?title=Develop\\_to\\_Sentinel](http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel) ([http://developer.novell.com/wiki/index.php?title=Develop\\_to\\_Sentinel](http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel)).

For information on the complete product documentation, see the Sentinel 6.1 Documentation site: <http://www.novell.com/documentation/sentinel61/index.html> (<http://www.novell.com/documentation/sentinel61/index.html>)

## Contacting Novell

- ♦ Web site: <http://www.novell.com> (<http://www.novell.com>)
- ♦ Technical Support: [http://support.novell.com/phone.html?sourceidint=suplnav4\\_phonesup](http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup) ([http://support.novell.com/phone.html?sourceidint=suplnav4\\_phonesup](http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup))
- ♦ Self Support: [http://support.novell.com/support\\_options.html?sourceidint=suplnav\\_supportprog](http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog) ([http://support.novell.com/support\\_options.html?sourceidint=suplnav\\_supportprog](http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog))
- ♦ Patch Download site: <http://download.novell.com/index.jsp> (<http://download.novell.com/index.jsp>)
- ♦ 24x7 support: <http://www.novell.com/company/contact.html> (<http://www.novell.com/company/contact.html>)
- ♦ Sentinel Community Support Forum: <http://forums.novell.com/novell-product-support-forums/sentinel/> (<http://forums.novell.com/novell-product-support-forums/sentinel/>)
- ♦ Sentinel TIDs: <http://support.novell.com/products/sentinel> (<http://support.novell.com/products/sentinel>)
- ♦ Sentinel Plug-in Web site: <http://support.novell.com/products/sentinel/secure/sentinel61.html> (<http://support.novell.com/products/sentinel/secure/sentinel61.html>)
- ♦ Notification E-mail List: Sign up through the Sentinel Plug-in Web site



# Introduction

# 1

- ♦ [Section 1.1, “Sentinel Overview,” on page 9](#)
- ♦ [Section 1.2, “Sentinel User Interfaces,” on page 10](#)
- ♦ [Section 1.3, “Sentinel Server Components,” on page 11](#)
- ♦ [Section 1.4, “Sentinel Plugins,” on page 13](#)
- ♦ [Section 1.5, “Language Support,” on page 14](#)

The following sections will walk you through the product basics. The rest of the *Sentinel User Guide* has more detailed architecture, operation and administrative procedures.

These sections assumes that you are familiar with Network Security, Database Administration, Windows and UNIX operating systems.

## 1.1 Sentinel Overview

Sentinel is a security information and event management solution that receives information from many sources throughout an enterprise, standardizes it, prioritizes it and presents it to you to make threat, risk, and policy-related decisions.

Sentinel automates log collection, analysis, and reporting processes to ensure that IT controls are effective supporting threat detection and audit requirements. Sentinel replaces these labor-intensive manual processes with automated, continuous monitoring of security and compliance events and IT controls.

Sentinel gathers and correlates security and non-security information from across an organization's networked infrastructure, as well as third-party systems, devices, and applications. Sentinel presents the collected data in a more sensible GUI, identifies security or compliance issues, and tracks remediation activities, to streamline previously error-prone processes and build a more rigorous and secure management program.

Automated incident response management enables you to document and formalize the process of tracking, escalating, and responding to incidents and policy violations, and provides two-way integration with trouble-ticketing systems. Sentinel enables you to react promptly and resolve incidents efficiently.

Solution Packs are a simple way to distribute and import Sentinel correlation rules, dynamic lists, maps, reports, and iTRAC workflows into controls. These controls may be designed to meet specific regulatory requirements, such as the Payment Card Industry Data Security Standard, or they may be related to a specific data source, such as user authentication events for an Oracle database.

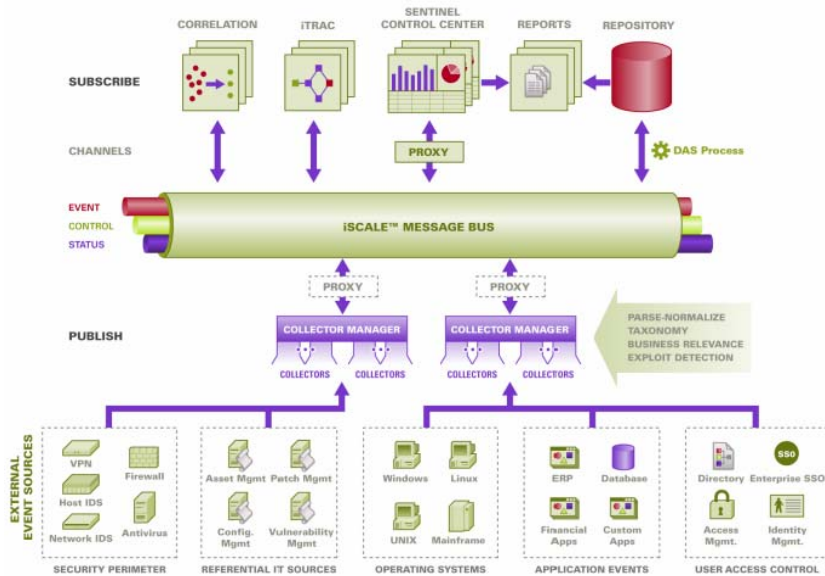
With Sentinel, you get:

- ♦ Integrated, automated real-time security management and compliance monitoring across all systems and networks
- ♦ A framework that enables business policies to drive IT policy and action
- ♦ Automatic documenting and reporting of security, systems, and access events across the enterprise

- ◆ Built-in incident management and remediation
- ◆ The ability to demonstrate and monitor compliance with internal policies and government regulations such as Sarbanes-Oxley, HIPAA, GLBA, FISMA and others. The content required to implement these controls is simply distributed and implemented using Solution Packs.

The following is a conceptual architecture of Sentinel, which illustrates the components involved in performing security and compliance management.

**Figure 1-1** Conceptual Architecture of Sentinel



## 1.2 Sentinel User Interfaces

Sentinel includes several easy-to-use user interfaces:

- ◆ Sentinel Control Center
- ◆ Sentinel Data Manager
- ◆ Sentinel Solution Designer
- ◆ Sentinel Collector Builder

### 1.2.1 Sentinel Control Center

Sentinel Control Center provides an integrated security management dashboard that enables analysts to quickly identify new trends or attacks, manipulate and interact with real-time graphical information, and respond to incidents. Key features of Sentinel Control Center include:

- ◆ **Active Views:** Real-time analytics and visualization
- ◆ **Incidents:** Incident creation and management
- ◆ **Correlation:** Correlation rules definition and management
- ◆ **iTRAC:** Process management for documenting, enforcing, and tracking incident resolution processes

- ♦ **Reporting:** Historical reports and metrics
- ♦ **Event Source Management:** Collector deployment and monitoring

## 1.2.2 Sentinel Data Manager

Sentinel Data Manager (SDM) allows you to manage the Sentinel Database. You can perform the following operations in the SDM:

- ♦ Monitor Database Space Utilization
- ♦ View and Manage Database Partitions
- ♦ Manage Database Archives
- ♦ Import Data into the Database

## 1.2.3 Sentinel Solution Designer

Sentinel Solution Designer is used to create and modify Solution Packs, which are packaged sets of Sentinel content, such as reports, correlation rules, and workflows.

## 1.2.4 Sentinel Collector Builder

Sentinel Collector Builder enables you to build Collectors in the Sentinel proprietary language to process events. You can create and customize the templates so that the Collector can parse the data.

# 1.3 Sentinel Server Components

Sentinel is made up of several components:

- ♦ Data Access Service (DAS)
- ♦ Sentinel Communication Server
- ♦ Sentinel Database
- ♦ Sentinel Collector Manager
- ♦ Correlation Engine
- ♦ iTRAC
- ♦ Crystal Reports Server
- ♦ Sentinel Advisor and Exploit Detection (optional)

## 1.3.1 Sentinel Server

The Data Access Service (DAS) is the primary component used to communicate with the Sentinel database. DAS and other server components work together to store events received from the Collector Managers in the database, filter data, process Active View displays, perform database queries and process results, and manage administrative tasks such as user authentication and authorization.

### **1.3.2 Sentinel Communication Server**

The iSCALE Message Bus is capable of moving thousands of message packets in a second among the components of Sentinel. This allows independent scaling of components and standards-based integration with external applications.

### **1.3.3 Sentinel Database**

The Sentinel product is built around a back-end database that stores security events and all of the Sentinel metadata. The events are stored in normalized form, along with asset and vulnerability data, identity information, incident and workflow status, and many other types of data.

### **1.3.4 Sentinel Collector Manager**

Collector Manager manages data collection, monitors system status messages, and performs event filtering as needed. Main functions of the Collector Manager include transforming events, adding business relevance to events through taxonomy, performing global filtering on events, routing events, and sending health messages to the Sentinel server.

The Sentinel Collector Manager can connect directly to the message bus or it can use an SSL proxy.

### **1.3.5 Correlation Engine**

Correlation adds intelligence to security event management by automating analysis of the incoming event stream to find patterns of interest. Correlation allows you to define rules that identify critical threats and complex attack patterns so that you can prioritize events and initiate effective incident management and response.

### **1.3.6 iTRAC**

Sentinel provides an iTRAC workflow management system to define and automate processes for incident response. Incidents that are identified in Sentinel, either by a correlation rule or manually, can be associated with an iTRAC workflow.

### **1.3.7 Crystal Reports Server**

Comprehensive reporting services within the Sentinel Control Center are powered by Crystal Reports Server by Business Objects. Sentinel comes with predefined reports geared toward the most common reporting requests by organizations monitoring their security and compliance postures. Using the Crystal Reports Developer, new or customized reports can also be developed against the Sentinel published report view schema.

### **1.3.8 Sentinel Advisor and Exploit Detection**

Sentinel Advisor is an optional data subscription service that includes known attacks, vulnerabilities, and remediation information. This data, combined with known vulnerabilities and real-time intrusion detection or prevention information from your environment, provide proactive exploit detection and the ability to immediately act when an attack takes place against a vulnerable system.

## 1.4 Sentinel Plugins

Sentinel supports a variety of plugins to expand and enhance system functionality. Some of these plugins are installed automatically. Additional plugins (and updates) are available for download at the [Sentinel Content Web site \(http://support.novell.com/products/sentinel/sentinel61.html\)](http://support.novell.com/products/sentinel/sentinel61.html).

Some plugins, such as the Remedy Integrator and the IBM Mainframe Connector, require an additional license for download.

### 1.4.1 Collectors

Sentinel collects data from source devices and delivers a richer event stream by injecting taxonomy, exploit detection, and business relevance into the data stream before events are correlated and analyzed and sent to the database. A richer event stream means that data is correlated with the required business context to identify and remediate internal or external threats and policy violations.

Sentinel Collectors can parse data from the types of devices listed below:

---

◆ Intrusion Detection Systems (host)	◆ Anti-Virus Detection Systems
◆ Intrusion Detection Systems (network)	◆ Web Servers
◆ Firewalls	◆ Databases
◆ Operating Systems	◆ Mainframe
◆ Policy Monitoring	◆ Vulnerability Assessment Systems
◆ Authentication	◆ Directory Services
◆ Routers and Switches	◆ Network Management Systems
◆ VPNs	◆ Proprietary Systems

---

JavaScript Collectors can be written and run on Sentinel 6.0 SP1 and above using standard JavaScript development tools and the Collector SDK. Proprietary Collectors can be built or modified using [Section 1.2.4, “Sentinel Collector Builder,” on page 11](#), a standalone application included with the Sentinel system.

### 1.4.2 Connectors and Integrators

Connectors provide connectivity from the Collector Manager to event sources using standard protocols such as JDBC and syslog. Events are passed from the Connector to the Collector for parsing.

Integrators enable remediation actions on systems outside of Sentinel. For example, a correlation action can use the SOAP Integrator to initiate a Novell Identity Manager workflow.

The optional Remedy AR Integrator provides the ability to create a Remedy ticket from Sentinel events or incidents.

### 1.4.3 Correlation Rules and Actions

Correlation rules identify important patterns in the event stream. When a correlation rule triggers, it initiates correlation actions, such as sending email notifications, initiating an iTRAC workflow, or executing an action using an Integrator.

## 1.4.4 Reports

Users can run a wide variety of dashboard and operational reports from the Sentinel Control Center using Crystal Reports Server. In Sentinel 6.1 and later versions, reports are typically distributed via Solution Packs.

## 1.4.5 iTRAC Workflows

iTRAC workflows provide consistent, repeatable processes for managing incidents. In Sentinel 6.1 and later versions, workflow templates are typically distributed via Solution Packs.

## 1.4.6 Solution Packs

Solution Packs are packaged sets of related Sentinel content, such as correlation rules, actions, iTRAC workflows, and reports. Novell provides Solution Packs that focus on specific business needs, such as the PCI-DSS Solution Pack, which addresses compliance with the Payment Card Industry Data Security Standard. Novell also creates “collector packs,” which include content focused on a specific event source, such as Windows Active Directory.

# 1.5 Language Support

Sentinel components are localized for the following languages:

- ◆ English
- ◆ Portuguese (Brazil)
- ◆ French
- ◆ Italian
- ◆ German
- ◆ Spanish
- ◆ Japanese
- ◆ Chinese (Traditional)
- ◆ Chinese (Simplified)

There are several exceptions:

- ◆ The Collector Builder interface and scripting are in English only, although it can run on the non-English operating systems listed above.
- ◆ JavaScript Collectors can be modified to parse either ASCII or Unicode (double-byte) data, but the Collectors posted on the Sentinel Content site are currently written for English data only. Collectors written in the proprietary Collector language are only capable of processing ASCII and extended ASCII data.
- ◆ Internal events (to audit Sentinel operations) are in English only.

# System Requirements

# 2

- ♦ [Section 2.1, “Supported Software,” on page 15](#)
- ♦ [Section 2.2, “Hardware Recommendations,” on page 19](#)
- ♦ [Section 2.3, “Recommended Collector Manager Limits,” on page 25](#)

## 2.1 Supported Software

For best performance and reliability, Novell recommends installing all Sentinel components on the approved software listed in this section. This software is quality assured and certified.

Novell supports Sentinel on the operating system and database versions described in this section. Novell also supports Sentinel on systems with minor updates to these operating system and database versions, such as service packs or hotfixes. However, running Sentinel on systems with major updates to these operating system and database versions is not supported.

- ♦ [Section 2.1.1, “Patch Levels,” on page 15](#)
- ♦ [Section 2.1.2, “Database Supported Platforms,” on page 16](#)
- ♦ [Section 2.1.3, “Sentinel Component Supported Platforms,” on page 17](#)
- ♦ [Section 2.1.4, “Platform Support Exceptions and Cautions,” on page 19](#)

### 2.1.1 Patch Levels

The following table lists the specific patch levels that were used to perform Sentinel testing. For convenience in this document, these platforms are referred to by the short name in the left column.

**Table 2-1** Patch Level Information

Short Name	Full Name and Patch Level
SLES 11 (64-bit)	SUSE Linux Enterprise Server 11 (64-bit)
SLES 10 (32-bit)	SUSE Linux Enterprise Server 10 SP2 (32-bit)
SLES 10 (64-bit)	SUSE Linux Enterprise Server 10 SP2 (64-bit)
RHEL 4 (32-bit)	Red Hat Enterprise Linux 4 Nahant Update-4 (32-bit)
RHEL 4 (64-bit)	Red Hat Enterprise Linux 4 Nahant Update-4 (64-bit)
RHEL 5 (64-bit)	Red Hat Enterprise Linux 5 Nahant Update-5 (64-bit)
<b>NOTE:</b> RHEL 5 is supported only on clean installations of Sentinel 6.1 SP2. Novell does not currently support upgrading an existing Sentinel system from RHEL 4 to RHEL 5.	
Solaris 10 (64-bit)	Sun Solaris 10 6/06 s10s_u2wos_09a (64-bit SPARC)
Windows 2003 (32-bit)	Windows 2003 SP2, Standard or Enterprise Edition (32-bit)

Short Name	Full Name and Patch Level
Windows 2003 (64-bit)	Windows 2003 SP1, Standard or Enterprise Edition (64-bit)
Windows 2008 (64-bit)	Windows 2008 SP1, Standard Edition (64-bit)
SLED 10 (32-bit)	SUSE Linux Enterprise Desktop 10 SP1 (32-bit)
Windows XP (32-bit)	Windows XP SP2 (32-bit)
Windows Vista (32-bit)	Windows Vista SP1 (32-bit)
Oracle 10g (32-bit)	Oracle 10g Enterprise Edition with partitioning (v 10.2.0.4)
Oracle 10g (64-bit)	Oracle 10g Enterprise Edition with partitioning (v 10.2.0.4)
Oracle 11gR2 (64-bit)	Oracle 11g Release 2 Enterprise Edition with partitioning
SQL Server 2005 (32-bit)	SQL Server 2005 SP2, Standard or Enterprise Edition (32-bit)
SQL Server 2005 (64-bit)	SQL Server 2005 SP2, Standard or Enterprise Edition (64-bit)
SQL Server 2008 (64-bit)	SQL Server 2008 (Version 10.0.1600.22)
SLES 9 (32-bit)	SUSE Linux Enterprise Server 9 SP2 (32-bit)

You should check with the vendors for security updates and patches. Hot fixes and security patches typically have no impact on Sentinel operations and are therefore supported. Because major or minor releases of a database or operating system typically involve more substantial changes, only the versions mentioned in [Table 2-1 on page 15](#) are supported for this release.

## 2.1.2 Database Supported Platforms

The following database and operating system combinations are certified or supported. Certified combinations have been tested with Novell Engineering's full test suite. Supported combinations are expected to be fully functional.

**Table 2-2** Database Supported Platforms

Operating System	Oracle 10g (32-bit)	Oracle 10g and Oracle 11g (64-bit)	SQL Server 2005 (32)	SQL Server 2005 (64)	SQL 2008 (64)
SLES 11 (64)	Not Supported	Certified only on Oracle 11g	Not Supported	Not Supported	Not Supported
SLES 10 (32)	Supported	Not Supported	Not Supported	Not Supported	Not Supported
SLES 10 (64)	Not Supported	Certified	Not Supported	Not Supported	Not Supported
RHEL 4 (32)	Supported	Not Supported	Not Supported	Not Supported	Not Supported
RHEL 4 (64)	Not Supported	Supported	Not Supported	Not Supported	Not Supported
RHEL 5 (64)	Supported	Certified only on Oracle 10g	Not Supported	Not Supported	Not Supported
Solaris 10 (32)	Supported	Not Supported	Not Supported	Not Supported	Not Supported
Solaris 10 (64)	Not Supported	Supported	Not Supported	Not Supported	Not Supported



Operating System	Oracle 10g (32-bit)	Oracle 10g and Oracle 11g (64-bit)	SQL Server 2005 (32)	SQL Server 2005 (64)	SQL 2008 (64)
Windows 2003 (32)	Not Supported	Not Supported	Supported	Not Supported	Not Supported
Windows 2003 (64)	Not Supported	Not Supported	Not Supported	Certified	Not Supported
Windows 2008 (64)	Not Supported	Not Supported	Not Supported	Not Supported	Supported

Although 32-bit platforms are supported for the Sentinel database in development or proof-of-concept environments, Novell recommends 64-bit platforms for production databases in order to obtain the best performance results.

**NOTE:** All databases should be installed on an operating system that is certified by the database vendor and also by Novell for use with Sentinel components. Oracle must run on Linux or Solaris (not Windows). When you use the Oracle client to install or load seed data to the Sentinel database, ensure that the Oracle client version is same or later than the Oracle server version.

### 2.1.3 Sentinel Component Supported Platforms

The Sentinel Server components include the Communication Server, Correlation Engine, Data Access Service (DAS), and the Advisor data subscription service (which resides on the same machine as DAS).

The Sentinel user applications that are mentioned in [Table 2-3 on page 17](#) include the Sentinel Control Center (SCC), Sentinel Data Manager (SDM), and Sentinel Solution Designer (SSD).

The Collector Manager, Collector Builder, and Crystal Reports Server also have specific platform requirements.

The following software and operating system combinations are certified or supported. Certified combinations have been tested with Novell Engineering's full test suite. Supported combinations are expected to be fully functional.

**Table 2-3** *Supported and Certified Components*

	Sentinel Server Components	Sentinel User Applications	Collector Manager	Collector Builder	Crystal Reports Server
SLES 11 (64)	Certified	Certified	Supported	Not Supported	Not Supported
SLES 10 (32)	Supported	Supported	Certified	Not Supported	Not Supported
SLES 10 (64)	Certified	Supported	Supported	Not Supported	Not Supported
RHEL 4 (32)	Supported	Supported	Supported	Not Supported	Certified
RHEL 4 (64)	Supported	Supported	Supported	Not Supported	Not Supported
RHEL 5 (64)	Certified	Certified	Supported	Not Supported	Not Supported
Solaris 10 (32)	Supported	Supported	Certified	Not Supported	Not Supported

	Sentinel Server Components	Sentinel User Applications	Collector Manager	Collector Builder	Crystal Reports Server
Solaris 10 (64)	Certified	Supported	Supported	Not Supported	Not Supported
Windows 2003 (32)	Supported	Supported	Certified	Supported	Certified
Windows 2003 (64)	Certified	Supported	Supported	Supported	Not Supported
Windows 2008 (64)	Supported	Supported	Supported	Supported	Not Supported
SLED 10	Not Supported	Certified	Not Supported	Not Supported	Not Supported
Windows XP	Not Supported	Certified	Not Supported	Supported	Not Supported
Windows Vista	Not Supported	Supported	Not Supported	Supported	Not Supported
SLES 9 (32)	Not Supported	Not Supported	Not Supported	Not Supported	Certified

The supported reporting server is Crystal Reports Server XI R2 SP4, which is supported only on 32-bit hardware. The supported Crystal Reports service packs can be downloaded from the [Novell download Web site \(http://download.novell.com/\)](http://download.novell.com/).

- 1 Go to the [Novell download Web site \(http://download.novell.com/\)](http://download.novell.com/).
- 2 Select SIEM/Sentinel from the *Product or Technology* list.
- 3 Specify *crystal* as the *Keyword*, then click *search*.

The download page displays the required service packs for Crystal Reports and also includes the instructions for installing the service packs.

For more information on installing and configuring Crystal Reports, see [Chapter 7, “Crystal Reports for Windows,” on page 93](#) and [Chapter 8, “Crystal Reports for Linux,” on page 121](#).

Crystal requires a Web server and a Central Management Server (CMS) database for operation, in addition to the Sentinel database. The Crystal Reports Server can run on the following platforms in the Sentinel environment:

- ♦ Red Hat Enterprise Linux 4 (32-bit)
  - ♦ Crystal CMS database on MySQL
  - ♦ Web server on Apache Tomcat
  - ♦ Sentinel database on Oracle recommended; other configurations untested
- ♦ SUSE Linux Enterprise Server 9 SP2 (32-bit)
  - ♦ Crystal CMS database on MySQL
  - ♦ Web server on Apache Tomcat
  - ♦ Sentinel database on Oracle recommended; other configurations untested
- ♦ Windows 2003 SP1 Server, Standard or Enterprise Edition (32-bit)
  - ♦ Crystal CMS database on SQL Server 2005
  - ♦ Web server on Microsoft IIS with .NET
  - ♦ Sentinel database on SQL Server recommended; other configurations untested

See the vendor documentation for additional details about system requirements, supported version numbers, and known issues for these platforms.

## 2.1.4 Platform Support Exceptions and Cautions

The RHEL 5 (64-bit) platform is supported only on clean installations of Sentinel 6.1 SP2. Novell does not currently support upgrading an existing Sentinel system from RHEL 4 to RHEL 5.

The following platforms are not supported by their respective vendors and therefore are not supported by Novell:

- ♦ The vendor for Crystal Reports Server XI R2 does not currently support Crystal on Solaris or SUSE Linux Enterprise Server 10.
- ♦ Oracle does not currently support Oracle 10 (32-bit) on 32-bit Solaris 10.

Although the following platform configurations might be supported by their respective vendors, Novell does not recommend these configurations in a Sentinel environment:

- ♦ Sentinel on SUSE Linux Enterprise Server 10 running with the ReiserFS file system
- ♦ Oracle database on Windows
- ♦ Crystal Reports Server on Windows 2000
- ♦ Crystal Reports Server with MSDE as the database

Novell recommends running the Sentinel database and reporting engine on platforms that have been fully quality assured by Novell. However, both the Oracle database and Crystal Reports Server are supported by their respective vendors on additional platforms that are not fully quality assured by Novell. If a customer wants to use one of these additional platforms, Novell support for these platforms includes the following conditions:

- ♦ Because the Sentinel database installation and configuration are platform specific, only Novell Consulting or a qualified partner should be engaged to perform the initial Sentinel installation and setup.
- ♦ The standard installer might not work as expected on an untested platform.
- ♦ When the Sentinel system is functional, any database or reporting issue that cannot be duplicated on Novell in-house supported platforms must be addressed by the appropriate vendor.

Finally, for full functionality, Novell recommends that the database and DAS be installed with the same operating system (although not necessarily on the same machine). For example, Windows Authentication cannot be used if DAS is installed in a mixed environment where DAS is on Windows and the database is Oracle or where DAS is on UNIX or Linux and the database is SQL Server.

Collector Builder runs only on the Windows platform.

## 2.2 Hardware Recommendations

Sentinel has a highly scalable architecture, and if high event rates are expected, components can be distributed across several machines to achieve the best performance for the system. As you plan your system, make sure you take into account the following considerations:

- ♦ [Section 2.2.1, “Architecture Considerations,” on page 20](#)

- ◆ [Section 2.2.2, “Supported Hardware,” on page 21](#)
- ◆ [Section 2.2.3, “Proof of Concept Configuration,” on page 22](#)
- ◆ [Section 2.2.4, “Production Configuration,” on page 22](#)
- ◆ [Section 2.2.5, “High-Performance Production Configuration,” on page 24](#)
- ◆ [Section 2.2.6, “Virtual Environments,” on page 25](#)

## 2.2.1 Architecture Considerations

There are many factors that should be considered when designing a Sentinel system.:

- ◆ Event rate (events per second, or EPS)
- ◆ Geographic/network location of event sources, and bandwidth between networks
- ◆ Available hardware
- ◆ Preferred operating systems
- ◆ Plans for future scalability
- ◆ Amount of event filtering expected
- ◆ Local data retention policies
- ◆ Desired number and complexity of correlation rules
- ◆ Expected number of incidents per day
- ◆ Expected number of workflows to be managed per day
- ◆ Number of users logging in to the system
- ◆ Vulnerability and asset infrastructure

The most significant factor in the Sentinel system design is the event rate; almost every component of the Sentinel architecture is affected by increasing event rates. In a high-event-rate environment, the greatest demand is placed on the database, which is I/O-dependent and might be simultaneously handling inserts of hundreds or thousands of events per second, object creation by multiple users, workflow process updates, simple historical queries from the Sentinel Control Center, and long-term reports from the Crystal Reports Server. Therefore, Novell makes the following recommendations:

- ◆ The database should be installed without any other Sentinel components.
- ◆ The database server should be dedicated to Sentinel operations. Additional applications or Extract Transform Load (ETL) processes might impact database performance.
- ◆ The database server should have a high-speed storage array that meets the I/O requirements based on the event insertion rates.
- ◆ A dedicated database administrator should regularly evaluate and maintain the following aspects of the database:
  - ◆ Size
  - ◆ I/O operations
  - ◆ Disk space
  - ◆ Memory
  - ◆ Indexing
  - ◆ Transaction logs

In low-event-rate environments (for example, EPS < 25), these recommendations can be relaxed, because the database and other components use fewer resources.

This section includes some general hardware recommendations as guidance for Sentinel system design. In general, design recommendations are based on event rate ranges. However, these recommendations are based on the following assumptions:

- ◆ The event rate is at the high end of the EPS range.
- ◆ The average event size is 600 bytes.
- ◆ All events are stored in the database (that is, there are no filters to drop events).
- ◆ Thirty days worth of data is stored online in the database.
- ◆ Storage space for Advisor data is not included in the specifications mentioned in the tables later in this section.
- ◆ The Sentinel Server has a default 5 GB of disk space for temporarily caching event data that fails to insert into the database.
- ◆ The Sentinel Server also has a default 5 GB of disk space for events that fail to be written to aggregation event files.
- ◆ The optional Advisor subscription requires an additional 50 GB of disk space on the database server.

The hardware recommendations for a Sentinel implementation can vary based on the individual implementation, so you should consult Novell Consulting Services prior to finalizing the Sentinel architecture. The recommendations in this section can be used as guidelines.

---

**NOTE:** The Sentinel Server machine with Data Access Server (DAS) must have a local or shared striped disk array (RAID) with a minimum of four disk spindles because of high event loads and local caching.

The distributed hosts must be connected to the other Sentinel Server hosts through a single high-speed switch (GigE) in order to prevent network traffic bottlenecks.

---

Novell recommends that the Crystal Reports Server be installed on its own dedicated machine, particularly if the database is large or reporting usage is heavy. Crystal can be installed on the same machine as the database if the database is small, the reporting usage is light, and the database is installed on either Windows or Linux and not Solaris.

## 2.2.2 Supported Hardware

When you install Sentinel on Linux or Windows, the Sentinel server and database components can run on x86 (32-bit) or x86-64 (64-bit) hardware, with some exceptions based on the operating system, as described in [Section 2.2.1, “Architecture Considerations,” on page 20](#). Sentinel is certified on AMD Opteron and Intel Xeon hardware. Itanium servers are not supported.

For Solaris, the SPARC architecture is supported.

## 2.2.3 Proof of Concept Configuration

The proof of concept configuration supports up to 1350 events per second (EPS). This configuration is suitable for demonstrations or limited proofs of concept and can be installed by using the Simple option in the Sentinel installer. This configuration is not recommended for use in a production system and has been tested only with the configuration described below.

**Table 2-4** Hardware for Proof of Concept

Function	RAM	Model
Sentinel Server + Database (Oracle)	5 GB, Software RAID 5 with 5 SATA hard drives	SLES 10 SP1, two 64-bit dual core processors (tested with two Intel Xeon 5160s, 3.00 GHz)
Collector Manager, Correlation Engine, and Sentinel Control Center	4 GB RAM	Windows 2003 SP2, two 32-bit single-core processors (tested with Intel Xeon, 2.4 GHz)
Crystal Reports Server	4 GB RAM 40 GB disk space	One 32-bit dual core processor (tested with Intel Xeon 5150, 2.66 GHz)

**Table 2-5** System Setup for Proof of Concept

Attribute	Rating	Comments
Collectors deployed per Collector Manager	3	
Rules deployed per correlation engine	10	
Active Views running	10	
Number of simultaneous users	3	
Number of maps deployed	5	The largest map is 40 KB with over 800 rows.

## 2.2.4 Production Configuration

This production configuration supports up to 3200 EPS. The Sentinel components are distributed to enable a higher event rate than the proof of concept configuration.

- ♦ To achieve optimal performance, the Oracle database uses a StorCase disk array (16 disks) to store data files, and a separate local drive to hold the Oracle Redo log.
- ♦ To achieve optimal performance on the Sentinel server, the file directory that holds DAS aggregation data and `insertErrorBuffer` was pointed to a separate local hard drive.

**Table 2-6** *Hardware for Production Configuration*

Function	RAM	Model
Sentinel Server and Correlation Engine	4 GB RAM 90 GB disk space	SLES 10 SP1, two 64-bit dual core processors (tested with two Intel Xeon 5160s, 3.00 GHz)
Database (Oracle)	4 GB RAM 3 TB+ disk space	SLES 10 SP1, two 64-bit dual core processors (tested with two Opteron 275s, 2.2 GHz), StorCase disk array, and software RAID 5
Collector Manager 1	4 GB RAM 20 GB disk space	SLES 10 SP1, two 64-bit dual core processors (tested with two Opteron 275s, 2.2 GHz)
Collector Manager 2	4 GB RAM 20 GB disk space	Windows 2003, one dual core processor (tested with dual core Intel Xeon, 2.50 GHz)
Crystal Reports Server	4 GB RAM 40 GB disk space	One 32-bit dual core processor (tested with Intel Xeon 5150, 2.66 GHz)

**Table 2-7** *System Setup for Production Configuration*

Attribute	Rating	Comments
Collectors deployed per Collector Manager	10	The Collector Manager 1 configuration handles up to 1750 EPS; the Collector Manager 2 configuration handles up to 850 EPS. A typical collector running alone can output up to 600 EPS, but adding more collectors to a Collector Manager or using collectors with more complex parsing will reduce the per-collector output.
Rules deployed per Correlation Engine	20	
Active Views running	20	
Number of simultaneous users	5	
Number of maps deployed	5	The largest map is 40 KB with over 800 rows.

## 2.2.5 High-Performance Production Configuration

The high-performance production configuration supports up to 5000 EPS.

- ♦ To achieve optimal performance, the Oracle database uses a StorCase disk array (16 disks) to store data files and a separate local hard drive to hold the Oracle Redo log.
- ♦ A secondary DAS\_Binary process (which is responsible for event inserts into the database) is installed on a dedicated machine to reduce the CPU utilization on the primary server.
- ♦ To achieve optimal performance on both DAS machines, the file directory that holds DAS aggregation data and `insertErrorBuffer` was pointed to a separate local hard drive.

**Table 2-8** Hardware for High-Performance Production Configuration

Function	Sizing	Model
Sentinel Server (including primary DAS_Binary process) and Correlation Engine	4 GB RAM 90 GB disk space	SLES 10 SP1, two 64-bit dual core processors (tested with two Intel Xeon 5160s, 3.00 GHz)
Database (Oracle)	4 GB RAM 4 TB+ disk space	SLES 10 SP1, two 64-bit dual core processors (tested with two Opteron 275s, 2.2 GHz), StorCase disk array, and software RAID 5
Collector Manager 1 and secondary DAS_Binary process	4 GB RAM 40 GB disk space	SLES 10 SP1, two 64-bit dual core processors (tested with two Opteron 275s, 2.2 GHz)
Collector Manager 2	4 GB RAM 20 GB disk space	Windows 2003, one dual core processor (tested with dual core Intel Xeon, 2.50 GHz)
Crystal Reports Server	4 GB RAM 40 GB disk space	One 32-bit dual core processor (tested with Intel Xeon 5150, 2.66 GHz)

**Table 2-9** System Setup for High-Performance Production Configuration

Attribute	Rating	Comments
Collectors deployed per Collector Manager	10	The Collector Manager 1 configuration handles up to 1750 EPS; the Collector Manager 2 configuration handles up to 850 EPS. A typical collector running alone can output up to 600 EPS, but adding more collectors to a Collector Manager or using collectors with more complex parsing will reduce the per-collector output.
Rules deployed per correlation Engine	20	
Active Views running	20	



Attribute	Rating	Comments
Number of simultaneous users	4	
Number of maps deployed	5	The largest map is 40 KB with over 800 rows.

## 2.2.6 Virtual Environments

Sentinel 6.1 has been tested extensively on VMware ESX Server, and Novell fully supports Sentinel running in this environment. Performance results in a virtual environment can be comparable to the results achieved in tests on a physical machine, the virtual environment should provide the same memory, CPU, disk space, and I/O as the physical machine recommendations.

## 2.3 Recommended Collector Manager Limits

The limits mentioned in this section are recommendations based on the performance testing done at Novell or at customer sites. They are not hard-limits. The recommendations are approximations. In highly dynamic systems, it is a good practice to build in buffers and allow room for growth.

Unless otherwise specified, Collector Manager limits assume 4 CPU cores at 2.2 GHz each, 4 GB of RAM, running on SLES 11.

**Table 2-10** Collector Manager Performance Numbers

Attribute	Limit	Comments
Maximum number of Collector Managers	20	This limit assumes each Collector Manager is running at low EPS (e.g, less than 100 EPS). The limit decreases as the events per second increase.
Maximum number of Connectors (fully utilized) on a single Collector Manager	1 per CPU core, with at least 1 CPU core reserved for the operating system and other processing	A fully utilized Connector is one that is running at the highest EPS possible for that type of Connector.
Maximum number of Collectors (fully utilized) on a single Collector Manager	1 per CPU core, with at least 1 CPU core reserved for the operating system and other processing	A fully utilized Collector is one that is running at the highest EPS possible for that type of Collector.
Maximum number of event sources on a single Collector Manager	2000	The limit of the Sentinel server is also 2000, so if 2000 event sources are on a single Collector Manager, then the limit of event sources for the overall Sentinel system has been reached with that single Collector Manager.
Maximum number of event sources per Sentinel server instance	2000	



- ◆ [Section 3.1, “Installer Overview,” on page 27](#)
- ◆ [Section 3.2, “Sentinel Configurations,” on page 28](#)
- ◆ [Section 3.3, “Port Numbers Used for Sentinel 6.1,” on page 31](#)
- ◆ [Section 3.4, “General Installation Prerequisites,” on page 31](#)
- ◆ [Section 3.5, “Simple Installation,” on page 37](#)
- ◆ [Section 3.6, “Custom Installation,” on page 39](#)
- ◆ [Section 3.7, “Installing Sentinel as a Domain user,” on page 51](#)
- ◆ [Section 3.8, “Post-Installation Configuration,” on page 51](#)
- ◆ [Section 3.9, “LDAP Authentication,” on page 58](#)
- ◆ [Section 3.10, “Updating the License Key,” on page 65](#)

## 3.1 Installer Overview

This section helps you install the major components of the Sentinel system. The Sentinel installer offers the option of a Simple installation or Custom installation. The Simple installation installs all components on one machine and is intended for demonstration or training systems. This is not intended for production use as many minimal default settings are used for a Simple installation. The Custom installation can be used to install one or more Sentinel components at a time and can be used for distributed production installations.

In addition to the Sentinel components, there are several other applications that can be part of the Sentinel system:

- ◆ **Database:** The database stores the events, correlated events, and configuration information. The database must be installed according to the best practices recommended by Oracle and Microsoft for database installation, directory structure, and so on.
- ◆ **Crystal Reports Server:** Crystal (and its associated Web Server and database) is used to generate reports from the Novell report library or custom-designed reports, and has a separate installer for Crystal components. For more information about installing Crystal, see [Chapter 7, “Crystal Reports for Windows,” on page 93](#) and [Chapter 8, “Crystal Reports for Linux,” on page 121](#).
- ◆ **Crystal Reports Developer:** This application is used to create and modify reports.
- ◆ **Advisor:** Advisor provides real-time intelligence about attacks and vulnerabilities, including real-time exploit detection to determine which threats are taking place against vulnerable systems. For more information about Advisor, see [“Advisor Usage and Maintenance” in the \*Sentinel 6.1 User Guide\*](#).
- ◆ **Sentinel Link Solution:** Sentinel Link is a mechanism that provides the ability to hierarchically link multiple Sentinel systems, including Novell Sentinel Log Manager, Novell Sentinel, and Novell Sentinel Rapid Deployment. You can hierarchically link two or more Sentinel systems to forward filtered events from one Sentinel system to another for further evaluation. For more information on Sentinel Link Solution, see [“Sentinel Link Solution” in the \*Sentinel 6.1 User Guide\*](#).

**NOTE:** Remedy Service Desk integration was previously available as an installer option. With the Sentinel 6.1 release, Remedy integration is available separately as an Integrator plug-in and is no longer included in the Sentinel installer. With the proper license, the Remedy Integrator and associated Action can be downloaded at the [Sentinel Content Web site \(http://support.novell.com/products/sentinel/sentinel61.html\)](http://support.novell.com/products/sentinel/sentinel61.html).

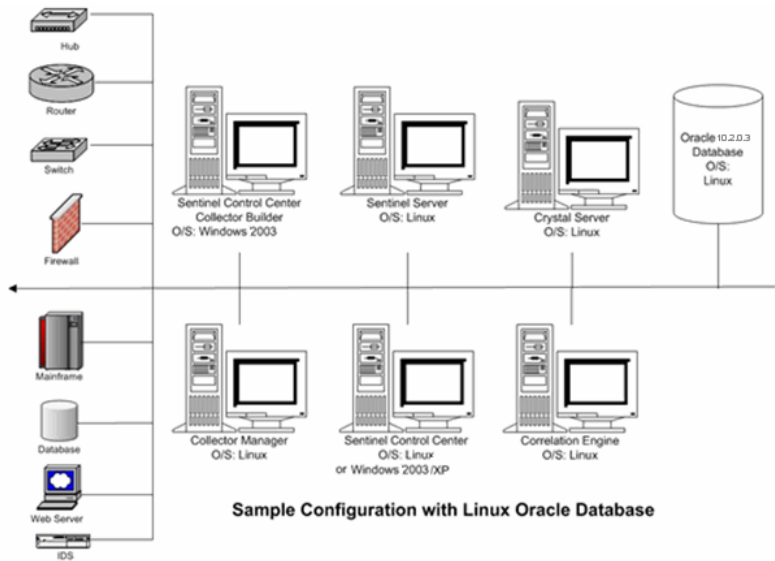
## 3.2 Sentinel Configurations

The following are some typical configurations for Sentinel.

- ♦ Section 3.2.1, “Linux,” on page 28
- ♦ Section 3.2.2, “Solaris,” on page 29
- ♦ Section 3.2.3, “Windows,” on page 29
- ♦ Section 3.2.4, “High-Performance Configuration,” on page 29

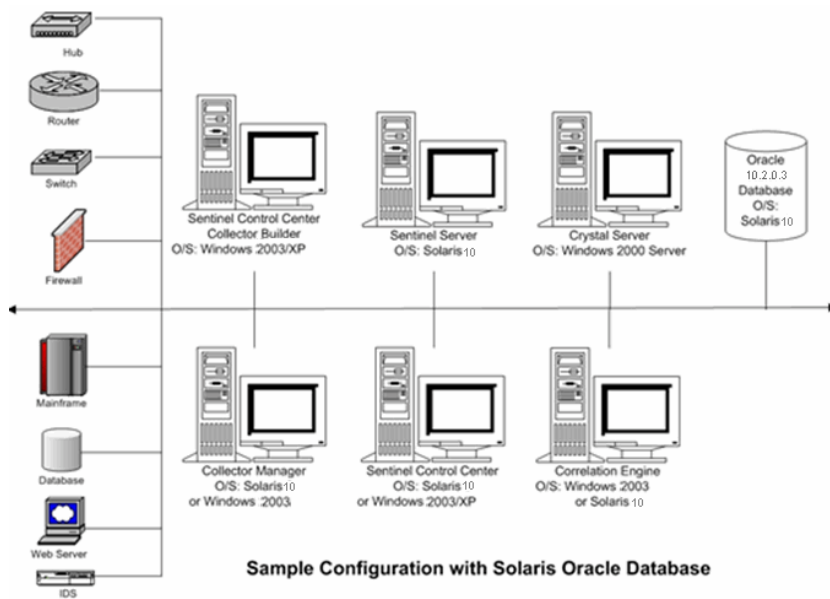
### 3.2.1 Linux

**Figure 3-1** *Sentinel Configuration on Linux*



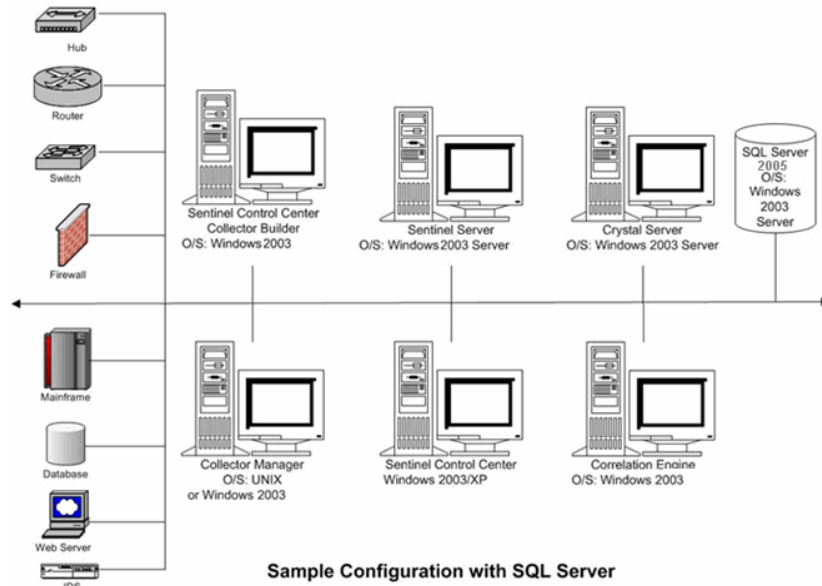
### 3.2.2 Solaris

Figure 3-2 Sentinel Configuration on Solaris



### 3.2.3 Windows

Figure 3-3 Sentinel Configuration on Windows



### 3.2.4 High-Performance Configuration

The 64-bit JVM can allocate much more RAM to Sentinel processes than the 32-bit JVM. The highest Xmx value that can be used by a 32-bit JVM is 1200m, but it is virtually unlimited in a 64-bit JVM. Therefore, a 64-bit JVM is useful if processing requires a lot of RAM and it is available on

the machine. However, performance testing shows that the 64-bit JVM requires nearly double the RAM to perform the same tasks as compared to the 32-bit JVM. So using the 64-bit JVM for a process that does not require this additional RAM wastes memory resources. For example, if a process was allocated 1200m with a 32-bit JVM, there is no benefit to running that process on a 64-bit JVM unless more than double the amount of RAM is allocated to it. In this example, the amount must be more than 2400m.

There are several processes that can benefit from having an additional RAM at their disposal (beyond the 1200m limit of a 32-bit JVM). For example, DAS\_RT can hold more Active Views. A Collector Manager can support more Collectors and Connectors. The Correlation Engine can support more rules. DAS\_Query, DAS\_Binary, and DAS\_Aggregation can also take advantage of additional RAM. However, a few processes such as DAS\_iTRAC, DAS\_Proxy, and Sonic are not likely to make use of memory beyond the 1200m that is supplied with a 32-bit JVM.

To move all the processes on a machine to use the 64-bit JVM:

- 1 Stop the Sentinel services. Select *Start > Control Panel > Administrative Tools > Services*, right-click *Sentinel*, then select *Stop*.
- 2 Back up the `ESEC_HOME/config/configuration.xml` file.
- 3 Modify the `ESEC_JAVA_HOME` path environment variable to point to 64-bit JVM.
  - ♦ **Windows:** Set `ESEC_JAVA_HOME` to `%ESEC_HOME%\jre64\bin`
  - ♦ **Linux:** Set `ESEC_JAVA_HOME` to `$(ESEC_HOME)/jre64/bin`
- 4 Reload the environment variables.
  - ♦ **Windows:** Replace `%ESEC_HOME%\lib\x86` with `%ESEC_HOME%\lib\x86_64` in the path variable.
  - ♦ **Linux:** Log out and log in to Sentinel.
- 5 Open the `ESEC_HOME/config/configuration.xml` file in a text editor.
- 6 Modify the `-Xmx<#>m` setting of every process entry in the `configuration.xml` file for which you want to allocate additional memory.

Start by doubling the value that was already there for every process. This is necessary because of the overhead of the 64-bit JVM as described earlier. Then, for processes that you want to have additional RAM, modify their values again and choose an even higher number.
- 7 Save the `configuration.xml` file and open the file in a Web browser to validate the XML syntax.
- 8 Start the Sentinel services. Select *Start > Control Panel > Administrative Tools > Services*, right-click *Sentinel*, then select *Start*.

To move individual processes on a machine to use the 64-bit JVM:

---

**NOTE:** On Windows, only the Correlation Engine and Collector Manager can be moved individually to 64-bit JVM. This limitation exists because other processes use the dynamic link libraries (DLLs) found in the `PATH` environment variable, and there is only one `PATH` environment variable for both 32-bit and 64-bit processes. Only one type of DLL (32-bit or 64-bit) can appear first in the `PATH`. On UNIX, any process can be moved individually to 64-bit.

---

- 1 Stop the Sentinel services. Select *Start > Control Panel > Administrative Tools > Services*, right-click *Sentinel*, then select *Stop*.
- 2 Back up the `ESEC_HOME/config/configuration.xml` file.

- 3 Open the `ESEC_HOME/config/configuration.xml` file in a text editor.
- 4 Locate the entry for the process to move to 64-bit at the end of the file. For each of these process that should run as 64-bit in the `image` attribute, change the `$(ESEC_JAVA_HOME)/java` environment variable to `$(ESEC_HOME)/jre64/bin/java`.
- 5 Modify the `-Xmx<#>m` setting of the process entries in the `configuration.xml` file for which you want to allocate additional memory.  
  
Start by doubling the value that was already there for the processes that will be running in a 64-bit JVM. This is necessary because of the overhead of the 64-bit JVM as described earlier. Then, modify their values again and choose an even higher number.
- 6 Save the `configuration.xml` file and open the file in a Web browser to validate the XML syntax.
- 7 Start the Sentinel services. Select *Start > Control Panel > Administrative Tools > Services*, right-click *Sentinel*, then select *Start*.

### 3.3 Port Numbers Used for Sentinel 6.1

On the Sentinel 6.1 server, configure the following ports in the firewall to enable communication between Sentinel 6.1 and its components:

**Table 3-1** Port Numbers for Sentinel 6.1 Server

Component	Port Number	Description
Message bus	10012	The port on which the communication server is listening. Components connecting directly to the communication server use this port.
Sentinel Control Center proxy	10013	The port on which the SSL proxy server (DAS Proxy) is listening to accept username and password based authenticated connections. When prompted for a username and password, it uses this port to connect to the Sentinel server.
Collector Manager certificate authentication	10014	The port on which the SSL proxy server (DAS Proxy) is listening to accept certificate-based authenticated connections. Because the 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.

The Sentinel Data Manager (SDM) uses port 1521 to connect to the Oracle database and port 1433 to connect to the SQL database. These are the default ports that are used, however, you can change the port numbers.

### 3.4 General Installation Prerequisites

Perform the following tasks before installing Sentinel. For more information on these prerequisites, including the list of certified platforms, see [Chapter 2, “System Requirements,” on page 15](#).

- ◆ Ensure that each machine in the Sentinel architecture meets the minimum system requirements.

- ◆ Ensure that the operating systems for all components of the system are certified platforms and that the operating system has been hardened by using current best security practices.
- ◆ If you are installing on SUSE Linux Enterprise Server (SLES) 10, ensure that SLES is using the ext3 file system.
- ◆ For a minimal or headless installation, the operating system for the Sentinel Server machine must include at least the Base Server and X Window components of SuSE Linux Enterprise Server.
- ◆ If you are installing the Collector Manager on a 64-bit machine, ensure that the 32-bit libraries are available. The 32-bit libraries are required when running a Collector that is written in the proprietary Collector language (this includes almost all Collectors written before June 2008) as well as when running certain Connectors such as the LEA Connector. JavaScript based Collectors and the plug-ins of Sentinel are 64-bit enabled. Verifying the availability of these libraries is important on Linux platforms, which might not include them by default.
- ◆ You must install SUNWxcu4 package on your Solaris machine before installing Sentinel 6.1.
- ◆ Ensure that a Sentinel-certified database is installed. If you are using Oracle, Enterprise Edition with partitioning is required for the data archive to work. For more information on certified versions, see [Chapter 2, “System Requirements,” on page 15](#).
- ◆ Get the Sentinel, Crystal Reports Server, and Crystal Reports Developer serial numbers and license keys from the [Novell Customer Center \(https://secure-www.novell.com/center/regadmin\)](https://secure-www.novell.com/center/regadmin). If you have purchased the optional Advisor exploit detection data feed, verify in the Customer Center that this data subscription is listed with the rest of your Novell products.
- ◆ Install and configure an SMTP server if you want to send e-mail notifications from Sentinel.
- ◆ Create a directory with ASCII-only characters (and no special characters) from which you want to run the Sentinel installer.
- ◆ Provide Power user privileges to the Domain User. For more information, see [Section 3.4.1, “Providing Power User Privileges to Domain Users,” on page 33](#).

Sentinel installations using the full installer should always take place on a clean system. If Sentinel 6.0 was previously installed on any of the machines, Novell recommends that you follow the uninstallation procedures in [Chapter 9, “Uninstalling Sentinel,” on page 139](#). For information on uninstalling previous versions of Sentinel, see the relevant Installation guides on the [Novell Documentation Web site \(http://www.novell.com/documentation/\)](http://www.novell.com/documentation/).

---

**NOTE:** Instructions for upgrading from a previous version of Sentinel 6.0 to Sentinel 6.1 are included with the patch installer.

---

- ◆ [Section 3.4.1, “Providing Power User Privileges to Domain Users,” on page 33](#)
- ◆ [Section 3.4.2, “Sentinel Database Installation Prerequisites,” on page 33](#)
- ◆ [Section 3.4.3, “Authentication Mode Settings on SQL,” on page 36](#)
- ◆ [Section 3.4.4, “Sentinel Server Installation Prerequisites,” on page 37](#)



## 3.4.1 Providing Power User Privileges to Domain Users

---

**IMPORTANT:** If you install Sentinel as a domain user, where the user is not a part of administrator group in the Active Directory machine and the local machine, then the domain user should be a Power User to start the Sentinel Services.

---

- 1 On the Windows desktop, right-click My Computer and select *Manage*.
- 2 In the Computer Management window, select *Local > Users and Groups > Groups*.
- 3 Double-click *Power User* and add the domain user in `domain/domain user` format in the local system where Sentinel is installed by using this domain user.

## 3.4.2 Sentinel Database Installation Prerequisites

Before installing the Sentinel Database components, you must ensure the following prerequisites are met:

- ♦ [“Linux and Solaris” on page 33](#)
- ♦ [“Windows” on page 35](#)

### Linux and Solaris

- ♦ If you are installing on SLES 10, the file system for the operating system must be ext3.
- ♦ The Oracle database must be installed and running.
- ♦ The Oracle client and the Oracle JDBC client (for Oracle 10g, use `ojdbc14.jar` and for Oracle 11g, use `ojdbc6.jar`) must be installed on the machine from which you are running the installer. If you run the Sentinel installer on the database machine, ensure that a compatible JDBC client is already installed by the database installer. If you run the Sentinel installer on another machine, the database instance must be manually created and the compatible JDBC client must be manually installed on the machine with the installer. Although newer Oracle drivers are backward compatible, Sentinel testing was performed with the drivers that were shipped with the Oracle database (for example, 10.2.0.3 drivers were tested with the 10.2.0.3 database).

---

**NOTE:** Sentinel cannot start the Oracle 10 database because of the errors in the Oracle `dbstart` and `dbshut` scripts. You need to modify the `dbstart` and `dbshut` scripts after installing Sentinel. For more information on modifying these scripts, see [Section 3.8.7, “Modifying Oracle dbstart and dbshut scripts,” on page 55](#).

For performance reasons it is highly recommended that if you are installing in a RAID system and if your RAID environment allows, configure the Sentinel database so that the Transaction Log points are stored on the fastest write disk available. This Transaction log disk is a separate physical disk where the database files are stored.

- 
- ♦ You should allow the Sentinel installer to create the Oracle database instance for Sentinel.
  - ♦ The database instance creation can be performed manually if required. To ensure the compatibility of this instance with Sentinel, see [Section B.5, “Manual Oracle Instance Creation \(Optional\),” on page 164](#). If you chose this option, you must run the Novell `createEsecDBA.sh` script and use the Sentinel installer to add the database objects to the manually created Oracle database instance. For more information, see [Section 3.6, “Custom Installation,” on page 39](#).

---

**NOTE:** If you are using an existing or manually created Oracle database instance, it must be empty except for the Sentinel Database User for successful installation.

---

- ◆ Get the login credentials for the Oracle operating system user (default: `oracle`).
- ◆ Get the login credentials for Oracle users `SYSTEM` and `SYS`.
- ◆ Ensure that the following environment variables are set for the Oracle operating system user:
  - ◆ `ORACLE_HOME` (for example, `echo $ORACLE_HOME` might produce `/opt/oracle/product/10gR2/db`)
  - ◆ `ORACLE_BASE` (for example, `echo $ORACLE_BASE` produces `/opt/oracle`)
  - ◆ `PATH` (must include `$ORACLE_HOME/bin`)
- ◆ Determine an appropriate Oracle listener port number (the default port number is 1521).
- ◆ Create directories for the following storage locations:
  - ◆ Data Directory
  - ◆ Index Directory
  - ◆ Summary Data Directory
  - ◆ Summary Index Directory
  - ◆ Temp and Undo Directory
  - ◆ Redo Log Member A Directory
  - ◆ Redo Log Member B Directory
  - ◆ Archive Directory

---

**NOTE:** The oracle user must have the write permissions for these directories. To provide write permissions for these directories, execute the following commands for each directory as the root user:

```
chown -R oracle:dba <directory_path>
chmod -R 770 <directory_path>
```

---

- ◆ After the Sentinel Database is installed on Oracle, the database contains the following users:

**Table 3-2** Database Users

User	Description	Server Roles	Need for the Role
<code>esecdba</code>	Database schema owner. The DBA privilege is not granted to the Sentinel Database User because of security concerns. To use Enterprise Manager, you must create a user with DBA privileges.	Serveradmin and Sysadmin	<code>esecdba</code> needs <code>serveradmin</code> and <code>sysadmin</code> , because Sentinel Data Manager needs the privilege to use a built-in SQL Server stored procedure to write to the file system.

User	Description	Server Roles	Need for the Role
esecapp	Database application user. This is the application user used to connect to the database.	securityadmin	esecapp needs the securityadmin role, because Sentinel applications run under the esecapp user and this role is required to create new users in Sentinel and the database.
esecadm	Database user. This is the Sentinel Administrator. This is not the same user account as the Sentinel Administrator operating system user.	Not required	
esecrpt	Database report user	Not required	
SYS	SYS database user	Not required	
SYSTEM	SYSTEM database user	Not required	

## Windows

- ♦ The SQL Server database must be installed and running.
- ♦ The Sentinel Database installer requires the SQL Server client tools to be installed on the system where the Sentinel Database installer is run.
- ♦ The `sc` command to start the SQL Server Agent Service must be available on your database operating system. If not, the SQL Server Agent Service must be started manually for partitioning and data archiving to work properly. Also, it must be scheduled to restart after a reboot using another utility.
- ♦ Get the login credentials for the System Administrator database user
  - ♦ If the database uses SQL Authentication mode, the default database administrator user is `sa`.
  - ♦ If the database uses Windows Authentication only mode, you must run the installer when you are logged into Windows as a System Administrator database user.
- ♦ Set the `MSSQLSERVER` service to log in using the Local System Account.
- ♦ Determine the SQL Server Instance Name, if applicable.

---

**NOTE:** If you named your database instance during the SQL Server install, use the same name when prompted for the SQL Server instance name when installing the Sentinel Database and DAS components. If you did not name your database instance during the SQL Server install, leave the instance name blank during installation (if you are typing the hostname, do not add `\<instance_name>` to the database hostname).

---

- ♦ Create directories for the following storage locations:
  - ♦ Data Directory
  - ♦ Index Directory
  - ♦ Summary Data Directory
  - ♦ Summary Index Directory

- ♦ Log Directory
- ♦ Archive Directory
- ♦ Determine the SQL Server Instance port number (the default port number is 1433).

The Sentinel system uses several accounts for installation and system operation. These accounts exist in the Sentinel database and might use SQL Server authentication or Windows authentication. To use Windows authentication for one or more of the Sentinel users during Sentinel installation, the corresponding Windows Domain user must exist before installing the Sentinel Database.

The domain user should have Power User privileges to start the Sentinel services. See [Section 3.4.1, “Providing Power User Privileges to Domain Users,”](#) on page 33 for more information.

The following Sentinel users can be assigned to a Windows Domain User:

- ♦ Sentinel Database Administrator, used as the schema owner (named `esecdba` by default, if using SQL authentication; might be any domain account if using Windows Authentication).
- ♦ Sentinel Application User, used by Sentinel applications to connect to the database (named `esecapp` by default, if using SQL Authentication; might be any domain account if using Windows authentication).
- ♦ Sentinel Administrator, used as the administrator for logging to the Sentinel Control Center (named `esecadm` by default, if using SQL authentication; might be any domain account if using Windows authentication).
- ♦ Sentinel Report User, used for creating reports (named `esecrpt` by default, if using SQL authentication; might be any domain account if using Windows authentication).

---

**NOTE:** The database contains the Sentinel Database Administrator user, Sentinel Application User, and Sentinel Administrator user by default.

Sentinel does not support Microsoft clustering or High Availability for Windows.

---

After installing the Sentinel Database on SQL Server using local authentication, the database contains the following users:

- ♦ **esecdba:** Database schema owner. The DBA privilege is not granted to the Sentinel Database User because of security concerns, so to use Enterprise Manager (the GUI for the SQL database), you must create a user with DBA privileges.
- ♦ **esecapp:** Database application user. This is the application user used to connect to the database.
- ♦ **esecadm:** Database user that is the Sentinel Administrator. This is not the same user account as the Sentinel Administrator operating system user.
- ♦ **esecrpt:** Database report user.
- ♦ **sa:** System administrator database user.

### 3.4.3 Authentication Mode Settings on SQL

On Windows, you need to install SQL Server with mixed mode authentication to log in to the Sentinel Control Center using either Windows or SQL Server authentication. If you install SQL Server with Windows authentication, you can log in through Windows authentication only.

To modify your authentication mode settings:

- 1 In SQL Server Management Studio, right-click the server for which you want to modify the settings.
- 2 Select *Properties*, then click *Security*.
- 3 From the options *SQL Server and Windows Authentication Mode* or *Windows Authentication Mode*, select your option for authentication.

### 3.4.4 Sentinel Server Installation Prerequisites

If you are not installing the Sentinel Database on the same machine as the Sentinel server, you must install the Sentinel Database before installing the other components of Sentinel.

## 3.5 Simple Installation

The Simple Installation option is an all-in-one installation option that installs Sentinel Services, Collector Manager, and Sentinel Applications with the database on the same machine. This installation is only for demonstration or training purposes and should not be used in production environments.

After performing the database installation and meeting the prerequisites mentioned in [Section 3.4, “General Installation Prerequisites,”](#) on page 31 proceed with installing Sentinel. If you choose the Simple Installation, the following default settings are used:

- ♦ On Windows, SQL authentication is allowed on the SQL Server database.
- ♦ The same password is used for the Sentinel Database Administrator, the Sentinel Administrator, the Sentinel Application User, and the Sentinel Report User.
- ♦ The size of the database is 10 GB.

1 Log in as `root` user on Solaris/Linux or `administrator` user on Windows.

2 Extract the `<SENTINEL_6.1.2.zip>` file to a location of your choice.

The files are extracted to `disk1` folder.

3 From the `disk1` folder, run the following script:

- ♦ **Windows:** `setup.bat`

- ♦ **Solaris/Linux:**

For GUI mode:

```
./setup.sh
```

For text-based (serial console) mode:

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

You cannot run the installer on UNIX from a directory path that has special characters such as a space or non-ASCII characters.

4 Click the down-arrow and select one of the following language options:

---

English	Italian
French	Portuguese (Brazil)
German	Spanish
Simplified Chinese	Japanese
Traditional Chinese	

---

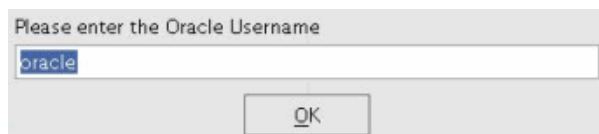
- 5 Read the Welcome screen, then click *Next*.
- 6 Read and accept End User License Agreement, then click *Next*.
- 7 Accept the default installation directory or click *Browse* to specify the installation location. Click *Next*.

---

**IMPORTANT:** You cannot install Sentinel into a directory with special characters or non-ASCII characters. For example, when installing Sentinel 6.1 on Windows x86-64, the default path is C:\Program Files (x86). You must change the default path to avoid the special characters and continue installation.

---

- 8 Select *Simple*, then click *Next*.
- 9 Provide the configuration information and click *Next*.
  - ♦ Serial Number
  - ♦ License Key
  - ♦ SMTP Server  
Sentinel sends e-mail through this server.
  - ♦ E-mail  
E-mail sent by Sentinel displays as sent from this e-mail address.
  - ♦ Global System Password  
The password you enter here is valid for all default users. This includes both the Sentinel Administrator user and the database users. For more information on the list of default database users created during installation, see [Section 3.8.2, “Sentinel Database,” on page 52](#).
- 10 Select the target database platform for database configuration:  
On Solaris/Linux, you are prompted to specify the Oracle username. Specify the username and click *OK*.



- 11 Specify the database name.
  - ♦ **Linux/Solaris:** Specify the path for the Oracle JDBC Driver file.
  - ♦ **Windows:** Specify the database user credentials and SQL Server instance name.
- 12 Click *Next*.

On Linux/Solaris, the installer backs up the existing `tnsnames.ora` and `listener.ora` files in the `$ORACLE_HOME/network/admin` directory. It overwrites the `listener.ora` file with Sentinel Database connection information, and appends the Sentinel Database connection information to the `tnsnames.ora` file.

---

**NOTE:** If you have other databases on the same server as the Sentinel Database, the administrator must manually merge the information from the backed-up `listener.ora` files into the new file and restart the Oracle listener for other applications to continue to connect to the database.

---

A summary of the selected database parameters is displayed.

```
A MSSQL database will be created with the following parameters:
A new database will be created named: ESEC617
This database will have a initial size of 1000 MB.
This database will have a maximum size of 20000 MB.

Data file storage locations are as follows:
Data Files: D:\esecdata
Index Files: D:\esecdata
Summary Data Files: D:\esecdata
Summary Index Files: D:\esecdata
Log Files: D:\esecdata

The schema will be owned by: esecdba
The Sentinel Application user will be: esecapp
The Sentinel Administrator will be: esecadm
The Sentinel Report User will be: esecrpt
```

**13** Click *Next*.

A summary of the installation is displayed.

**14** Click *Install*.

**15** After the install is complete, click *Finish*.

**16** Restart the machine.

## 3.6 Custom Installation

The Custom Installation option allows for a fully distributed installation, with more control over memory and other installation settings. The Custom Installation option can install one or more Sentinel components, including:

- ◆ Sentinel Database Components
- ◆ Sentinel Services
  - ◆ Communication Server
  - ◆ Correlation Engine
  - ◆ Data Access Server (DAS)
  - ◆ Sentinel Collector Service (Collector Manager)
- ◆ Applications
  - ◆ Sentinel Control Center

- ♦ Sentinel Data Manager
- ♦ Sentinel Solution Designer

Ensure that the prerequisites mentioned in [Section 3.4, “General Installation Prerequisites,” on page 31](#) are met before you proceed with installing Sentinel.

The Sentinel Database components should always be installed first. Other components can be installed at the same time if the system architecture includes multiple components on the database machine. The procedure below shows the steps for installing all the components on the same machine; a distributed installation includes a subset of the steps below.

- ♦ [Section 3.6.1, “Starting the Installation,” on page 40](#)
- ♦ [Section 3.6.2, “Configuring the Database on Windows,” on page 44](#)
- ♦ [Section 3.6.3, “Configuring the Database on Linux or Solaris,” on page 45](#)
- ♦ [Section 3.6.4, “Completing the Installation,” on page 48](#)
- ♦ [Section 3.6.5, “Console Installation on Linux or Solaris,” on page 49](#)

### 3.6.1 Starting the Installation

- 1 Log in as the `root` user on Solaris/Linux or the `administrator` user on Windows.

To install the Sentinel Database components on Windows when the target SQL Server instance is in Windows Authentication only mode, you must log in to Windows as a System Administrator database user.

- 2 Extract the `<SENTINEL_6.1.2.zip>` file to a location of your choice.

The files are extracted to `disk1` folder.

- 3 From the `disk1` folder, run the following script:

- ♦ **Windows:** `setup.bat`

- ♦ **Solaris/Linux:**

GUI mode:

```
./setup.sh
```

Textual (headless) mode:

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

You cannot run the installer on UNIX from a directory path that has special characters such as a space or non-ASCII characters.

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

**English**

French

German

Simplified Chinese

Traditional Chinese

Italian



English

Portuguese (Brazil)

Spanish

Japanese

- 5 Read the Welcome screen, then click *Next*.
- 6 Read and accept End User License Agreement. Click *Next*.
- 7 Accept the default install directory or click *Browse* to specify your installation location. Click *Next*.

You cannot install Sentinel in a directory with special characters or non-ASCII characters.

- 8 Select *Custom*, then click *Next*.
- 9 Select the components of Sentinel to install.



The following options are available:

Component	Description
Database	Installs Sentinel database objects (tables, views, stored procedures, and so on) into a database instance. Optionally creates the database instance first.
Communication Server	Installs the message bus (iSCALE) and DAS Proxy.
Correlation Engine	Installs the correlation engine.
Data Access Server (DAS)	Installs the components that communicate with the Sentinel database. Requires a Sentinel license key and serial number. (Required for using Advisor.)
Sentinel Collector Service	Installs the Collector Manager that handles connections to event sources, data parsing, mapping, and so on.
Sentinel Control Center	Installs the main console for security or compliance analysts.

Component	Description
Sentinel Data Manager (SDM)	Installs the SDM that is used for manual database management activities.
Solution Designer	Installs Solution Designer.

There is a time delay in the interface when you select or deselect a component.

If none of the child features of Sentinel Services are selected, make sure that you also deselect the Sentinel Services feature. This option looks like it is disabled (with a white check mark) even if all of its child features are deselected.

As part of the installation of the Sentinel Database component, the installer stores the files in the %ESEC\_HOME%\unist\db folder.

If you are using the console mode, the component selection page only displays a few components. Follow the on-screen instructions to view and edit the selected child components. For more information, see [Section 3.6.5, “Console Installation on Linux or Solaris,” on page 49.](#)

**NOTE:** For SQL (SQL 2005 and 2008) databases, the maximum number of online partitions allowed is 255. You must schedule the offline delete/archive operations so that the online partitions do not exceed 255.

- 10** If you select to install DAS, supply the serial number and license key when you are prompted.
- 11** On Linux/Solaris, specify the Sentinel Administrator username and the location of its home directory. This is the username that owns the installed Sentinel product. If the user does not already exist, the user role is created along with a home directory in the specified directory.
  - ◆ OS Sentinel Administrator username: The default username is `esecadm`
  - ◆ OS Sentinel Administrator user home directory: The default location is `/export/home`. If `esecadm` is the username, the home directory of the user is `/export/home/esecadm`.

To meet stringent security configurations required by the Common Criteria Certification, the `esecadm` user is created without a password. To log in as the `esecadm` user, you must first set a password.

- 12** If you chose to install the Sentinel Control Center, the installer prompts for the maximum memory space to be allocated to the Sentinel Control Center. Specify the maximum JVM heap size (MB) that you want to allocate only for the Sentinel Control Center.

By default, this is 256 MB. The maximum is 1024 MB.

Sentinel Control Center Configuration

Specify the JVM heap size for Sentinel Control Center. The installer has detected 516 MB of physical memory. The allowed range is 64-1024.

JVM Heap Size (MB)

- 13** If you select only Collector Manager and do not select Data Access Server (DAS), select the option for establishing communication between the Sentinel Collector Managers and the Sentinel Server. You can select *Connect to message bus directly* or *Connect to message bus using proxy*.

For more information on these two options, see [Chapter 6, “Communication Layer \(iSCALE\),” on page 87](#).

If you select *Connect to message bus using proxy*, immediately after the installation is complete you are prompted for the information that is required to register this Collector Manager as a trusted client. Before you select this option, ensure that the Communication Server is running.

If the Communication Server is not available, first select *Connect to message bus directly* and later manually configure the Proxy type communication by performing [Step 5 on page 48](#).

Collector Manager Communication Options:

- Connect to message bus directly.
- Connect to message bus using proxy.

- 14** Specify the Communication Server port or host server name information.

The port numbers must be identical on every machine in the Sentinel system to enable communications. For more information on the port numbers used for Sentinel 6.1, see [Section 3.3, “Port Numbers Used for Sentinel 6.1,” on page 31](#). Make a note of these ports for future installations on other systems.

- 15** Click *Next*.

Select how to obtain the message bus encryption key:

- Generate a random message bus encryption key.**  
Generates a random encryption key for message bus communication and stores it in keystore file. This option is typically used only when installing Communication Server.
- Import a message bus encryption key from existing keystore file.**  
Imports message bus encryption key from existing keystore file. Use this option when installing components that connect directly to the message bus and you have already generated a key elsewhere. The imported key must match the key used by the Communication Server.

- 16** If you are installing a component that makes a direct connection to the message bus or if you are installing the Communication Server, specify how to obtain the shared message bus encryption key:

All components connecting directly to the message bus must share the same encryption key. Novell recommends that you generate a random encryption key when you install the Communication Server and import this key when you install components on other machines. Components that connect through the proxy do not require the shared message bus encryption key.

The `.keystore` file is stored at `$ESEC_HOME/config` on Linux/Solaris or `%ESEC_HOME%\config` on Windows.

- 17 Select the target Database Server platform based on the target database version that you have installed, then click *Next*.

If you chose to install DAS and the Sentinel Database components are already installed on a different system, you are prompted for the following Sentinel Database information. This information is used to configure DAS to point to the Sentinel Database.

- ♦ **Database hostname or IP address:** The name or IP address of the existing Sentinel Database where events and configuration information are stored.
- ♦ **Database name:** The name of the Sentinel Database instance that you want to configure for the DAS component (the default name is ESEC).
- ♦ **Database port:** The default port number. For SQL Server, the port number is 1433 and for Oracle it is 1521.
- ♦ **Sentinel Application Database User:** Specify the login for the Sentinel Application User (`esecapp` by default) and the password given for this user during Sentinel Database installation.

- 18 Click *Next*.

- 19 If you chose to install the database component, configure the database for installation:

- ♦ To configure the database on Windows, continue with [Section 3.6.2, “Configuring the Database on Windows,”](#) on page 44.
- ♦ To configure the database on Linux or Solaris, continue with [Section 3.6.3, “Configuring the Database on Linux or Solaris,”](#) on page 45

- 20 Continue with [Section 3.6.4, “Completing the Installation,”](#) on page 48.

## 3.6.2 Configuring the Database on Windows

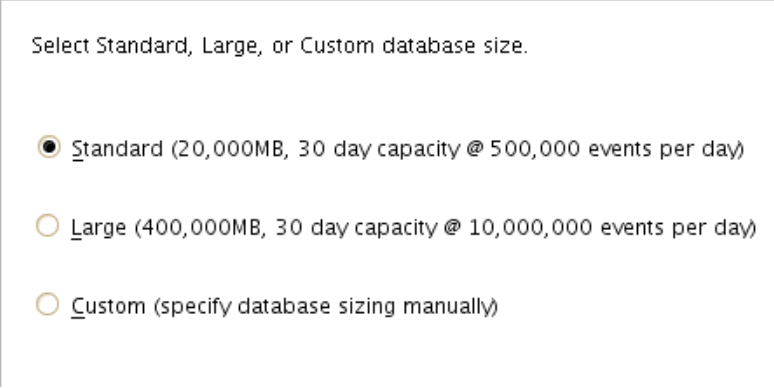
- 1 Complete Step 1 through Step 18 in [Section 3.6.1, “Starting the Installation,”](#) on page 40.
- 2 Select Microsoft SQL Server 2005 or Microsoft SQL Server 2008 as the target database server platform, then select one of the following options:
  - ♦ **Create a new database with database objects:** Creates a new Microsoft SQL database and populates the new database with database objects.
  - ♦ **Add database objects to an existing empty database:** Adds the database objects to an existing Microsoft SQL Server 2005 database. The existing database must be empty.
- 3 Specify the Database Install log directory.
- 4 Click *Next*.
- 5 If you are creating a new database, specify the existing directories to use as storage for:
  - ♦ Data Directory
  - ♦ Index Directory
  - ♦ Summary Data Directory
  - ♦ Summary Index Directory
  - ♦ Log Directory

Continue with [Step 7](#).

- 6 If you chose to add database objects to an existing empty database, continue with [Section 3.6.4, “Completing the Installation,”](#) on page 48.
- 7 Click *Next*.
- 8 Select the database character set support option and click *OK*.

If the installer is running in an Asian language, the Unicode database option is set by default. If the installer is running in a non-Asian language, the system prompts you to select from either ASCII only or Unicode.

The Unicode database installation requires more hard disk space than the ASCII only database installation.



Select Standard, Large, or Custom database size.

- Standard (20,000MB, 30 day capacity @ 500,000 events per day)
- Large (400,000MB, 30 day capacity @ 10,000,000 events per day)
- Custom (specify database sizing manually)

- 9 Select a database size option. If you selected a Custom database size, specify custom database size settings:
  - ♦ **Maximum Database Size:** The maximum amount of disk space the database occupies. The database automatically increases up to this size as it accumulates data. Regardless of the value specified here, the initial size of the database is 1000 MB.
  - ♦ **Log File Size:** The size of the transaction log file.
  - ♦ **Maximum Database File Size:** No single database file grows beyond this size.
- 10 Click *Next*.
- 11 Continue with [Section 3.6.4, “Completing the Installation,”](#) on page 48.

### 3.6.3 Configuring the Database on Linux or Solaris

- 1 Configure the system for Oracle database installation. For more information, see [Section B.4, “Configuring the System for Oracle Database Installation,”](#) on page 160.
- 2 Complete Step 1 through Step 18 in [Section 3.6.1, “Starting the Installation,”](#) on page 40.
- 3 Select the target Oracle database server version, then select whether to use a new database or an existing database.
  - ♦ **Create a new database with database objects:** Creates a new Oracle database instance and populates the new database with database objects.
  - ♦ **Add database objects to an existing empty database:** Adds database objects to an existing Oracle database instance. The existing database must be empty except for the esecdba user.
- 4 Specify the Database Install log directory.

- 5 Click *Next*.
- 6 Specify the Oracle user name or accept the default user name, then click *OK*.
- 7 If you chose to create a new database, specify the following:
  - ♦ **The path for Oracle JDBC driver file:** Specify the path to the jar file (do not use environment variables in this field.)
  - ♦ **Hostname:** The hostname of the local machine, where the Oracle database is installed. The installer only supports creating a new database instance on the local host.
  - ♦ **Database Name:** The name of the database instance to create.

Continue with [Step 9](#).

- 8 If you chose to add database objects to an existing empty Oracle database or perform a remote installation, specify the following information:
  - ♦ **The path for Oracle JDBC driver file:** Specify the path to the jar file (do not use environment variables in this field.)
  - ♦ **Database hostname or IP address:** The hostname or IP address of the machine where the Oracle database is installed. This can be the local hostname or a remote hostname.
  - ♦ **Database name:** The name of the existing empty Oracle database instance (the default name is ESEC). This database name must display as a service name in the `tnsnames.ora` file (in the directory `$ORACLE_HOME/network/admin/`) on the system from which you are running the installation.
  - ♦ **Database port:** The default database port is 1521.
  - ♦ **Password:** For Sentinel Database Administrator User (DBA), specify the password for the `esecdba` user. The Username field in this prompt is not editable.

---

**IMPORTANT:** If the database name is not in the `tnsnames.ora` file, the installer does not give an error at this point in the installation (because it verifies the connection using a direct JDBC connection), but the database installation fails when the database installer tries to connect to the database through SQL Plus. If the Database installation fails at that point, do not exit the installer. Modify the Service Name for this database in the `tnsnames.ora` file on that machine, then go back in the installer one screen and then forward again. This retries the Database installation with the new values in the `tnsnames.ora` file.

---

The installer takes a back up of the existing `tnsnames.ora` and `listener.ora` files in the `$ORACLE_HOME/network/admin` directory. It overwrites the `listener.ora` file with Sentinel database connection information, and appends Sentinel database connection information to the `tnsnames.ora` file. If you have other databases on the same server as the Sentinel database, the administrator must manually merge information from the backed-up `listener.ora` files into the new file and restart the Oracle listener in order for other applications to continue to connect to the database.

Continue with [Section 3.6.4, “Completing the Installation,”](#) on page 48.

- 9 Specify the Oracle memory (RAM) allocation and listener port or accept the default values.
- 10 Specify the passwords to set for the default `SYS` and `SYSTEM` database users, then click *Next*.

Select Standard, Large, or Custom database size.

Standard (20,000MB, 30 day capacity @ 500,000 events per day)

Large (400,000MB, 30 day capacity @ 10,000,000 events per day)

Custom (specify database sizing manually)

**11** Select a database size option. If you selected to use a custom database size, specify the custom database size settings:

- ◆ **Maximum Database Size:** The maximum amount of disk space the database occupies. The database automatically increases to this size as it accumulates data. Regardless of the value specified here, the initial size of the database is 5000 MB.
- ◆ **Log File Size:** The size of each redo log file
- ◆ **Maximum Database File Size:** No single database file grows beyond this size.

**12** Click *Next*.

**13** Specify the existing directories to use for database storage:

- ◆ Data Directory
- ◆ Index Directory
- ◆ Summary Data Directory
- ◆ Summary Index Directory
- ◆ Temp and Undo Directory
- ◆ Redo Log Member A Directory
- ◆ Redo Log Member B Directory

**14** Click *Next*.

---

**IMPORTANT:** For recovery and performance purposes, Novell recommends that these locations be on different I/O devices.

For performance reasons, the Redo Log should point to the fastest write disk you have available.

The installer does not create these directories, so they must be created externally before continuing beyond this step, and they must be writable by the oracle user. For more information, see [Section 3.4.2, “Sentinel Database Installation Prerequisites,” on page 33](#).

---

**15** Continue with [Completing the Installation](#).

## 3.6.4 Completing the Installation

After you have configured the database, perform the following steps to complete the installation.

- 1 If you chose to install the database component, configure the database partitions:
  - 1a Select *Enable automatic partition management* to allow Sentinel Data Manager to handle database partitioning and archiving.
  - 1b For data partitions, specify an existing directory for archive files.
  - 1c Specify start time for adding partitions and archiving data. These operations should not overlap because they use shared resources.
  - 1d Click *Next*.
  - 1e Provide authentication information for the following:
    - ◆ Sentinel Database Administrator User
    - ◆ Sentinel Application Database User
    - ◆ Sentinel Administrator User
    - ◆ Sentinel Report User (only on Windows)

---

**NOTE:** If the DAS component is also being installed, the Sentinel Application Database User password is required even if Windows authentication is selected. This is required to install the Sentinel Service to log in as the Sentinel Application Database User. No other users require a password to be specified if you are using Windows authentication.

On a Windows Server 2008 platform with MS SQL Server 2008 database, the Sentinel installation fails if you enter a weak password that does not meet Windows policy requirements.

---

- 1f Click *Next*.
- 2 A summary of the specified Database parameters displays. Click *Next*.
- 3 If you chose to install any of the Sentinel Server components, specify the amount of memory (RAM) to allocate to these components.

The installer factors 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 automatically determines the optimal distribution of memory across components taking into account the estimated operating system and database overhead.

---

**IMPORTANT:** You can modify the `-Xmx` value in `configuration.xml` file to change the RAM allocated to Sentinel Server processes. The `configuration.xml` file is placed at `$ESEC_HOME/config` on Linux/Solaris or `%ESEC_HOME%\config` on Windows.

---

- ◆ **Custom Memory Configuration:** Click the *Configure* button to allocate memory for specific components. This option is only available if there is sufficient memory on the machine.
- 4 Click *Next*, verify the selected features for installation, then click *Install*.
  - 5 If Collector Manager was selected to be installed and it was configured to use Proxy type communication, you are prompted for username and password of a Sentinel user that has the permission to register to a trusted client (For example, `esecadm`).



To complete this step, the Communication Server must be running and a valid username and password must be specified.

- 5a** Accept the Communication Server SSL certificate and upload the Collector Manager SSL certificate to the Communication Server.

When the connection with the Communication Server is initiated, you are prompted to accept the server certificate.

- 5b** Review the certificate attributes, then select *Accept Permanently*.

The installer automatically uploads the Collector Manager certificate to the Communication Server.

- 6** After installation, you are prompted to reboot or to log in again and start Sentinel services manually. Click *Finish* to reboot the system.

---

**NOTE:** The Sentinel installer, by default, turns off archive logging. For database recovery purposes, it is highly recommended that you enable archive logging after you install and before you begin to receive your production event data. You should also schedule backups for your archive logs to free up space in your archive log destination, or your database might stop accepting events.

---

### 3.6.5 Console Installation on Linux or Solaris

If you are using console mode, the installer's component selection page does not display all of the components together. Follow the on-screen instructions to view and edit the selected child components.

The following is an example of how to navigate the console mode component selection page:

```
Sentinel 6.1 - InstallShield Wizard
```

```
Select the features for "Sentinel 6.1" you would like to install:
```

```
Sentinel 6.1
```

```
To select/deselect a feature or to view its children, type its number:
```

- ```
1. [ ] Database
2. +[x] Sentinel Services
3. +[x] Applications
```

```
Other options:
```

- ```
0. Continue installing
```

```
Enter command [0] 1
```

```
Select the features for "Sentinel 6.1" you would like to install:
```

```
Sentinel 6.1
```

```
To select/deselect a feature or to view its children, type its number:
```

- ```
1. [x] Database
2. +[x] Sentinel Services
3. +[x] Applications
```

Other options:

0. Continue installing

Enter command [0] 2

1. Deselect 'Sentinel Services'
2. View 'Sentinel Services' subfeatures

Enter command [1] 2

Select the features for "Sentinel 6.1" you would like to install:

Sentinel 6.1  
- Sentinel Services

To select/deselect a feature or to view its children, type its number:

1. [ ] Communication Server
2. [x] Correlation Engine
3. [x] Data Access Server
4. [x] Sentinel Collector Service

Other options:

- 1. View this feature's parent
0. Continue installing

Enter command [0] 1

Select the features for "Sentinel 6.1" you would like to install:

Sentinel 6.1  
- Sentinel Services

To select/deselect a feature or to view its children, type its number:

1. [x] Communication Server
2. [x] Correlation Engine
3. [x] Data Access Server
4. [x] Sentinel Collector Service

Other options:

- 1. View this feature's parent
0. Continue installing

Enter command [0] 2

Select the features for "Sentinel 6.1" you would like to install:

Sentinel 6.1  
- Sentinel Services

To select/deselect a feature or to view its children, type its number:

1. [x] Communication Server
2. [x] Correlation Engine

3. [x] Data Access Server
4. [x] Sentinel Collector Service

Other options:

- 1. View this feature's parent
0. Continue installing

## 3.7 Installing Sentinel as a Domain user

- 1 Map a domain user to any of the Sentinel users (esecdba, esecadm, esecrpt).
- 2 Perform the actions in [Section 3.4.1, “Providing Power User Privileges to Domain Users,” on page 33](#) to provide power user privileges.
- 3 Install Sentinel 6.1 as an administrator user. See [Section 3.6, “Custom Installation,” on page 39](#) to install Sentinel.
- 4 When the installer prompts for esecdba, esecadm, and esecrpt user credentials, specify the created domain user in domain\domain user format, provide the password, and continue installation.

## 3.8 Post-Installation Configuration

- ♦ [Section 3.8.1, “Configuring the SMTP Integrator to Send Sentinel Notifications,” on page 51](#)
- ♦ [Section 3.8.2, “Sentinel Database,” on page 52](#)
- ♦ [Section 3.8.3, “Collector Service,” on page 52](#)
- ♦ [Section 3.8.4, “Starting the Collector Manager Service,” on page 52](#)
- ♦ [Section 3.8.5, “Configuring the Light weight Collector Manager,” on page 53](#)
- ♦ [Section 3.8.6, “Managing Time,” on page 55](#)
- ♦ [Section 3.8.7, “Modifying Oracle dbstart and dbshut scripts,” on page 55](#)
- ♦ [Section 3.8.8, “High-Performance Configuration,” on page 56](#)

### 3.8.1 Configuring the SMTP Integrator to Send Sentinel Notifications

In Sentinel 6.1, a JavaScript SendEmail action works with an SMTP integrator to send e-mail messages from various contexts within the Sentinel interface to e-mail recipients. The recipients of the e-mail message and the message contents are configured in the action parameters.

A single action instance of the SendEmail action plug-in is created automatically in every Sentinel installation. This action is used internally by Sentinel to send e-mail in the following situations:

- ♦ When a Correlation rule that is deployed with a Send Email action is triggered. The Send Email action referred to here is the action indicated by the gear icon, which is only valid for correlation (as opposed to the JavaScript SendEmail action, which is indicated by the JS JavaScript icon).
- ♦ If the workflow includes a Mail Step or Activity that is configured to send e-mail.
- ♦ If the user opens an incident and selects to execute an Activity that is configured to send e-mail.

- ♦ If the user right-clicks an event and selects *Email*.
- ♦ If the user opens an incident and selects *Email Incident*.

No configuration is necessary for the SendEmail action, but the SMTP Integrator must be configured with valid connection information before it works.

### 3.8.2 Sentinel Database

Unless the DBA wants to manage database archiving using his or her own procedures, Sentinel database automatic partition management (archiving, dropping, and adding partitions) should be enabled during installation to keep event data within a controlled size. Automatic partition management can also be configured post-installation by using the Sentinel Data Manager (SDM).

By default, the Sentinel Data Manager might not be able to write to the file system in order to archive data. This can be enabled by editing the `init<OracleSID>.ora` file for the database.

---

**NOTE:** By default, the installer sets all tablespaces to autogrow. By default, the file grow size is 200 MB, but the maximum file size depends on the value provided during the installation.

---

To enable Oracle to write to the archive directory:

- 1 Log in to the database machine.
- 2 Navigate to the `$ORACLE_HOME/dbs` directory.
- 3 Open the `init<OracleSID>.ora` file in a text editor.
- 4 Edit the `UTL_FILE_DIR` parameter to specify the directory path to which the archived Sentinel data should be written. You should have one of the following:
  - ♦ `UTL_FILE_DIR = *`
  - or
  - ♦ `UTL_FILE_DIR = [specific directory path]`
- 5 Save the file and exit.

### 3.8.3 Collector Service

During the installation of the Collector Service, a Collector called the General Collector is configured. By default, it creates events at a rate of 5 events per second (eps). This Collector can be used to test the installation. Additional Collectors can be downloaded from the [Sentinel Content Web site \(http://support.novell.com/products/sentinel/collectors.html\)](http://support.novell.com/products/sentinel/collectors.html).

### 3.8.4 Starting the Collector Manager Service

- 1 Start Sentinel 6.1.
- 2 Click *Admin > Servers View*.  
You can also click *Servers View* in the Navigator pane.
- 3 Expand the Servers view.  
The list of processes is displayed.
- 4 Right-click the Collector Manager that you want to start, then select *Actions > Start*.

Alternatively, click *Event Source Management > Live View*. Right-click the Collector Manager that you want to start, then select *Start*.

### 3.8.5 Configuring the Light weight Collector Manager

The EventRouter component of the Collector Manager handles internal functions such as processing maps and applying global filters on the events parsed by the Collector Manager. These processes can cause high CPU and RAM usage on a remote system.

With Sentinel 6.1 SP1 Hotfix 2 and later, you can configure a lightweight version of the Collector Manager on remote systems that have limited CPU and RAM. The internal functions of a Lightweight Collector Manager (LWCM) are handled by the Sentinel server (or whichever system is running DAS), so they consume less CPU and RAM on the remote system.

The EventRouter must be configured to operate in server and client modes on the DAS system and Collector Manager system. The Collector Manager system on which the EventRouter is configured to run in the client mode is referred to as the LWCM.

- ◆ [“Configuring the LWCM on the DAS Machine” on page 53](#)
- ◆ [“Configuring the LWCM on the Collector Manager Machine” on page 54](#)

#### Configuring the LWCM on the DAS Machine

The EventRouter must be configured to run in the server mode. This enables the DAS Query container to provide centralized event routing for multiple LWCMs.

The `das_query.xml` file under the `<ESEC_HOME>/config` folder contains a preconfigured EventRouter. By default, the EventRouter section is commented in the `das_query.xml` file.

Perform the following steps to configure the EventRouter for server mode:

- 1 Open the `das_query.xml` file for edit.

**Windows:** `%ESEC_HOME%\config\das_query.xml`

**Linux:** `$ESEC_HOME/config/das_query.xml`

- 2 Comment the following section:

```
<obj-component id="EventRouter">
  <class>esecurity.ccs.comp.router.EventRouter</class>
  <property name="esecurity.router.mode">standalone</property>
  <property name="esecurity.router.disable.compression">>true</property>
- <obj-component-ref>
  <name>DispatchManager</name>
  <ref-id>DispatchManager</ref-id>
</obj-component-ref>
- <obj-component-ref>
  <name>EventPublisher</name>
  <ref-id>DispatchManager</ref-id>
</obj-component-ref>
</obj-component>
```

- 3 Uncomment the following section:

```

<!--
<obj-component id="DispatchManagerEvents">
  <class>esecurity.ccs.comp.dispatcher.CommDispatcherManager</
class>
  <property name="esecurity.communication.service">Sentinel</
property>
  <property
name="EventPublisher.performanceEventChannel">ewizard_binary_event</
property>
  </obj-component>
  <obj-component id="EventRouterServer">
  <class>esecurity.ccs.comp.dispatcher.CommDispatcherManager</
class>
  <property name="esecurity.communication.service">Sentinel</
property>
  </obj-component>
  <obj-component id="EventRouter">
  <class>esecurity.ccs.comp.router.EventRouter</class>
  <property name="esecurity.router.mode">server</property>
  <property name="esecurity.router.disable.compression">>true</
property>
  <obj-component-ref>
    <name>DispatchManager</name>
    <ref-id>DispatchManager</ref-id>
  </obj-component-ref>
  <obj-component-ref>
    <name>EventPublisher</name>
    <ref-id>DispatchManagerEvents</ref-id>
  </obj-component-ref>
  <obj-component-ref>
    <name>EventRouterServer</name>
    <ref-id>EventRouterServer</ref-id>
  </obj-component-ref>
  </obj-component>
-->

```

4 Restart the Sentinel services.

---

**NOTE:** To return the EventRouter to standalone mode, comment the EventRouter section in the `das_query.xml` file and restart the Sentinel services.

---

### Configuring the LWCM on the Collector Manager Machine

To switch the EventRouter from standalone mode to client mode, rename the default `collector_mgr.xml` file, which is in the `ESEC_HOME/config` folder.

- 1 Change the `collector_mgr.xml` filename to `collector_mgr_standalone.xml`.
- 2 Change the `collector_mgr_lwcm.xml` filename to `collector_mgr.xml`.
- 3 Restart the Collector Manager services.

---

**NOTE:** To return the EventRouter to standalone mode, change the filenames to the original names and restart the Collector Manager services.

---

## 3.8.6 Managing Time

Novell strongly recommends that all Sentinel components, particularly the Correlation Engine and Collector Manager machines, be connected to an NTP (Network Time Protocol) server or other type of time server. If the system time across machines is not synchronized, the Sentinel Correlation Engine and Active Views do not work properly. The events from the Collector Managers are not considered to be real-time and are therefore sent directly to the Sentinel database, bypassing the Sentinel Control Centers and Correlation Engines.

By default, the threshold for real-time data is 120 seconds. This can be modified by changing the value of `esecurity.router.event.realtime.expiration` in the `event-router.properties` file. The Sentinel event time populates based on the Trust Device Time or the Collector Manager Time. You can select the Trust Device Time while configuring a collector. The Trust Device Time is the time when the log was generated by the device and the Collector Manager Time is the local system time of the Collector Manager system.

## 3.8.7 Modifying Oracle dbstart and dbshut scripts

Sentinel cannot start the Oracle 10 database because of errors in the Oracle `dbstart` and `dbshut` scripts. For details on the script errors, see [Oracle Support \(https://metalink.oracle.com\)](https://metalink.oracle.com) for the error numbers 336299.1 with the subject “dbstart errors out when executing in 10.2.0.1.0”, 5183726 and 4665320.

After the installation of Sentinel 6.1, you need to modify the `dbstart` and `dbshut` scripts for Sentinel to start an Oracle 10 database.

To modify the `dbstart` and `dbshut` scripts on Solaris 10:

- 1 In a text editor, open the `dbstart` script from `$ORACLE_HOME/bin/dbstart`.
- 2 Go to line 78 and replace the line with `ORACLE_HOME_LISTNER=$ORACLE_HOME`.
- 3 Add `#!/bin/bash` at the start to request the bash shell.
- 4 Ensure that `ORATAB` is pointing to `ORATAB=/var/opt/oracle/oratab`.  
If `ORATAB` is not in this location on your system, modify the `ORATAB` path manually to the correct location.
- 5 Click *Save*.
- 6 In a text editor, open the `dbshut` script from `$ORACLE_HOME/bin/dbshut`.
- 7 Ensure that `ORATAB` is pointing to `ORATAB=/var/opt/oracle/oratab`.  
If `ORATAB` is not in this location on your system, modify the `ORATAB` path manually to the correct location.
- 8 Click *Save*.

To modify the `dbstart` script on Red Hat Linux ES4:

- 1 In a text editor, open `dbstart` script from `$ORACLE_HOME/bin/dbstart`.
- 2 Ensure that `ORATAB` is pointing to `ORATAB=/etc/oratab`.  
If `ORATAB` is not in this location on your system, modify the `ORATAB` path manually to the correct location.
- 3 Click *Save*.

- 4 Open the dbshut script for edit from `$ORACLE_HOME/bin/dbshut`.
- 5 Ensure that ORATAB pointing is to `ORATAB=/etc/oratab`.

---

**NOTE:** If ORATAB is not in the above specified location on your system, modify the ORATAB path manually to the exact location.

---

- 6 Click *Save*.

After Sentinel is installed, you must install the Crystal Reporting server and the Sentinel Core Solution Pack.

DAS and the Sentinel Database are typically located in a secure area of your network. However, you might want to add another security layer to protect the data being transmitted from DAS to the database. For Oracle, the DBA can use the Advanced Security feature. For SQL Server, the DBA can enable the SSL functionality in the jTDS driver. For more information, go to [jTDS FAQ \(http://jtids.sourceforge.net/faq.html\)](http://jtids.sourceforge.net/faq.html) and search for "ssl".

### 3.8.8 High-Performance Configuration

There are several recommendations for configuring a high-performance Sentinel system.

- ♦ The Sentinel Server machine with Data Access Server (DAS) must have a local or shared striped disk array (RAID) with a minimum of four disk spindles because of high event loads and local caching.
- ♦ The distributed hosts must be connected to the other Sentinel Server hosts through a single high-speed switch (GigE) in order to prevent network traffic bottlenecks.
- ♦ The Crystal Reports Server should be installed on its own dedicated machine, particularly if the database is large or reporting usage is heavy.
- ♦ To achieve optimal performance on systems using an Oracle database, the Oracle database uses a StorCase Disk Array (16 disks) to store data files and a separate local SATA drive to hold the Oracle Redo log.
- ♦ To achieve optimal performance on the Sentinel server, the file directory that holds DAS aggregation data and `insertErrorBuffer` can be pointed to a separate local SATA hard drive.

To change the file directory for aggregation and buffers:

---

**NOTE:** The `esecadm` user or the user running the Sentinel services must have write permission to the file directory that holds the DAS aggregation data and `insertErrorBuffer`.

---

- 1 On the Sentinel server (DAS installed machine), open the `das_binary.xml` file for editing.

**On Windows:** `%ESEC_HOME%\config\das_binary.xml`

**On Linux:** `$ESEC_HOME/config/das_binary.xml`

- 2 Change the `rootDirectory` value in the following component:

```
<obj-component id="EventInsertErrorHandler">
  <class>esecurity.ccs.comp.event.EventInsertErrorHandlerService</class>
  <property
    name="cacheImpl">esecurity.ccs.comp.event.SmallFileMultiDirectoryEventMes
    sageCache</property>
  <property name="rootDirectory">../data/events/insertErrorBuffer</
  property>
```



```

<property name="reportInterval">300</property>
<property name="takeDelaySec">60</property>
<property name="eventTimeoutSec">28800</property>

<property name="onlineCapacity">1000</property>
<property name="capacity">5368709120</property>
</obj-component>

```

- 3** In the same file, change the `rootDirectory` value of the following component:

```

<obj-component id="EventProcessingErrorHandler">
  <class>esecurity.ccs.comp.event.EventInsertErrorHandlerService</class>
  <property
name="cacheImpl">esecurity.ccs.comp.event.SmallFileMultiDirectoryEventMes
sageCache</property>
  <property name="rootDirectory">../data/events/insertErrorBuffer</
property>
  <property name="reportInterval">300</property>
  <property name="takeDelaySec">60</property>
  <property name="eventTimeoutSec">28800</property>

  <property name="onlineCapacity">1000</property>
  <property name="capacity">5368709120</property>
</obj-component>

```

- 4** Change the directory and `outputDirectory` values of the following component:

```

<obj-component id="EventFileRedirectService">
  <class>esecurity.ccs.comp.event.redirect.EventFileRedirectService</
class>
  <property name="status">on</property>
  <property name="handler">esecurity.event.fileredirect</property>
  <property name="directory">../data/events/aggregation</property>
  <property name="outputDirectory">../data/events/aggregation/done</
property>
  <property name="filePrefix">events</property>
  <property name="fileSuffix">dat</property>
  <property name="maxFileSize">500000000</property>
  <property name="maxFileTime">1800</property>
  <property name="notificationChannel">event_file_redirect</property>
  <obj-component-ref>
    <name>Publisher</name>
    <ref-id>DispatchManager</ref-id>
  </obj-component-ref>
</obj-component>

```

- 5** Save the `das_binary.xml` file and exit.

- 6** On the Sentinel server (DAS installed machine), open the `das_aggregation.xml` in the config directory file for editing.

- 7** Change the directory value in the following component to match the directory value in the `EventFileRedirectService` component in the `das_binary.xml` file.

```

<obj-component id="EventAggregationService">
<class>esecurity.ccs.comp.event.transformer.EventAggregationService</
class>
  <property name="directory">c:\test\Aggregation\done</property>
  <property name="reporterChannel">event_aggregation_status</property>
  <property name="updateBatchSize">200</property>
  <property name="updateDB">enabled</property>
  <property name="nullHashValid">>false</property>

```

```

<property name="maxNumberEntries">30000</property>
<property name="maxEntrySize">50</property>
<property name="startOffsetInDays">7</property>
<property name="deleteProcessedFiles">true</property>
<obj-component-ref>
  <name>Publisher</name>
  <ref-id>DispatchManager</ref-id>
</obj-component-ref>
</obj-component>

```

- 8 Save the `das_aggregation.xml` file and exit.
- 9 Restart the Sentinel server for the changes to take effect.

## 3.9 LDAP Authentication

You can enable users to login to Sentinel using their Novell eDirectory or Microsoft Active Directory credentials by configuring a Sentinel 6.1 server for LDAP authentication.

- ♦ [Section 3.9.1, “Configuring the Sentinel 6.1 Server for LDAP Authentication,” on page 58](#)
- ♦ [Section 3.9.2, “Configuring Multiple LDAP Servers for Failover,” on page 62](#)
- ♦ [Section 3.9.3, “Migrating LDAP User Accounts from Sentinel 6.1 SP1 Hotfix 2 to Sentinel 6.1 SP2,” on page 64](#)

### 3.9.1 Configuring the Sentinel 6.1 Server for LDAP Authentication

- 1 Export the self-signed certificate of the Certificate Authority (CA) for the eDirectory/Active Directory server to a Base64-encoded file.

**eDirectory:** For more information on exporting an eDirectory CA certificate, see [Exporting an Organizational CA's Self-Signed Certificate \(http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/a7elxuq.html\)](http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/a7elxuq.html).

To export an eDirectory CA certificate to iManager, the Novell Certificate Server plug-ins for iManager must be installed. For more information on installing an iManager plug-in, see [Downloading and Installing Plug-in Modules \(http://www.novell.com/documentation/imanager27/imanager\\_admin\\_273/?page=/documentation/imanager27/imanager\\_admin\\_273/data/hk42s9ot.html\)](http://www.novell.com/documentation/imanager27/imanager_admin_273/?page=/documentation/imanager27/imanager_admin_273/data/hk42s9ot.html).

**Active Directory:** For more information on exporting an Active Directory CA certificate, see [How to enable LDAP over SSL with a third-party certification authority \(http://support.microsoft.com/kb/321051\)](http://support.microsoft.com/kb/321051).

- 2 Log in as the `root` user to the Sentinel 6.1 server in which DAS is installed.
- 3 Copy the certificate file to the following directory on the Sentinel 6.1 server:
  - ♦ **Windows:** `%ESEC_HOME%\config`
  - ♦ **Linux/Solaris:** `$ESEC_HOME/config`
- 4 Set the ownership and permissions of the certificate file as follows:
  - ♦ **Windows:** Not applicable
  - ♦ **Linux/Solaris:** Run the following commands:

```
chown esecadm:esec <Install_Directory>/config/<cert-file>
chmod 700 <Install_Directory>/config/<cert-file>
```

**5** Switch to esecadm user:

- ♦ **Windows:** Not applicable
- ♦ **Linux/Solaris:** Run the following command:

```
su - esecadm
```

**6** Change to the following directory:

- ♦ **Windows:** %ESEC\_HOME%\bin
- ♦ **Linux/Solaris:** \$ESEC\_HOME/bin

**7** Run the LDAP authentication configuration script:

- ♦ **Windows:** ldap\_auth\_config.bat
- ♦ **Linux/Solaris:** ./ldap\_auth\_config.sh

The script takes a back up of the auth.login and configuration.xml configuration files in the config directory as auth.login.sav and configuration.xml.sav before modifying them for LDAP authentication.

**8** Specify the following information:

Press Enter to accept the default value suggested in the brackets [ ] or specify a new value to override the default value.

Parameter	Description/Action
Sentinel install location	The installation directory on the Sentinel 6.1 server. The default location is: <ul style="list-style-type: none"><li>♦ <b>Windows:</b> %ESEC_HOME%</li><li>♦ <b>Linux/Solaris:</b> \$ESEC_HOME</li></ul>
LDAP server hostname or IP address	The hostname or the IP address of the machine where the LDAP server is installed. The default value is localhost. However, it is not recommended to install the LDAP server on the same machine as the Sentinel 6.1 server.
LDAP server port	The port number for a secure LDAP connection. The default port number is 636.

Parameter	Description/Action
Anonymous searches on LDAP directory	<p>Specify <i>y</i> to perform anonymous searches on the LDAP directory to fetch the LDAP user DN for authentication based on Sentinel username. Otherwise, specify <i>n</i>. The default value is <i>y</i>.</p> <p>You can search the LDAP directory anonymously to fetch the LDAP user DN based on the Sentinel LDAP username to perform LDAP authentication, by using an LDAP connection that does not use a username or password. For more information on anonymous searches, see <a href="http://www.ietf.org/rfc/rfc2829.txt">Section 5 “Anonymous authentication” (http://www.ietf.org/rfc/rfc2829.txt)</a>.</p> <p>For Active Directory, if you specify <i>y</i>, the ANONYMOUS LOGON user object must be given appropriate list permission and read access to <code>sAMAccountName</code> and <code>objectclass</code> attributes. For more information, see <a href="http://support.microsoft.com/kb/320528">Configuring Active Directory to Allow Anonymous Queries (http://support.microsoft.com/kb/320528)</a>.</p> <p>For Windows Server 2003, you must perform additional configuration. For more information, see <a href="http://support.microsoft.com/kb/326690/en-us">Configuring Active Directory on Windows Server 2003 (http://support.microsoft.com/kb/326690/en-us)</a>.</p> <p>If you specify <i>n</i>, complete the LDAP configuration and perform the steps mentioned in the section “<a href="#">LDAP Authentication Without Performing Anonymous Searches</a>” on page 61.</p>
LDAP Directory used	Specify 1 for Novell eDirectory or 2 for Active Directory. The default value is 1.
This parameter is displayed only if you have specified ‘y’ for anonymous searches.	
LDAP subtree to search for users	The subtree in the directory that has the user objects.
This parameter is displayed only if you have specified ‘y’ for anonymous searches.	<p>The following are examples for specifying the subtree in eDirectory and Active Directory:</p> <ul style="list-style-type: none"> <li>◆ eDirectory: <pre>ou=users,o=novell</pre> <hr/> <p><b>NOTE:</b> For eDirectory, if no subtree is specified, then the search is run on the entire directory.</p> </li> <li>◆ Active Directory: <pre>CN=users,DC=TESTAD,DC=provo,DC=novell,DC=com</pre> <hr/> <p><b>NOTE:</b> For Active Directory, the subtree cannot be blank.</p> </li> </ul>
Filename of the LDAP server certificate	The filename of the eDirectory/Active Directory CA certificate that you have copied in <a href="#">Step 3</a> .

- 9 Enter one of the following:
- ♦ y: to accept the entered values
  - ♦ n: to enter new values
  - ♦ q: to quit the configuration

On successful configuration:

- ♦ The LDAP server certificate is added to a keystore named `<Install_Directory>/config/ldap_server.keystore`.
- ♦ The `auth.login` and `configuration.xml` configuration files in the `<Install_Directory>/config` directory are updated to enable LDAP authentication.

- 10 Enter y to restart the Sentinel service.

---

**IMPORTANT:** If there are any errors, revert the changes made to the `auth.login` and `configuration.xml` configuration files in the `config` directory:

```
cp -p auth.login.sav auth.login
cp -p configuration.xml.sav configuration.xml
```

---

## LDAP Authentication Without Performing Anonymous Searches

- 1 Ensure that you have performed Step 1 through Step 10 in section “[Configuring the Sentinel 6.1 Server for LDAP Authentication](#)” on page 58, and you specified n for [Anonymous searches on LDAP directory](#).
- 2 Specify the *LDAP user DN* that is used for non anonymous LDAP authentication, while creating the LDAP user account in Sentinel Control Center. For more information, see “[Creating an LDAP User Account for Sentinel](#)” in the *Sentinel 6.1 User Guide*.

Alternatively, for Active Directory, you can perform LDAP authentication without anonymous searches by using the `userPrincipalName` attribute:

- 1 Ensure that you have performed Step 1 through Step 10 in section “[Configuring the Sentinel 6.1 Server for LDAP Authentication](#)” on page 58, and you specified n for [Anonymous searches on LDAP directory](#).

- 2 Ensure that the `userPrincipalName` attribute is set to `<sAMAccountName@domain>` for the Active Directory user.

For more information, see [User-Principal-Name Attribute \(http://msdn.microsoft.com/en-us/library/ms680857\(VS.85\).aspx\)](http://msdn.microsoft.com/en-us/library/ms680857(VS.85).aspx).

- 3 On the Sentinel server, edit the `LdapLogin` section in the `<Install Directory>/config/auth.login` file:

```
LdapLogin {
    com.sun.security.auth.module.LdapLoginModule required
    userProvider="ldap://LDAP server IP:636/DN of the Container that
contains the user objects"
    authIdentity="{USERNAME}@Domain Name"
    userFilter="(&(sAMAccountName={USERNAME}))(objectclass=user)"
    useSSL=true;
};
```

For example:

```
LdapLogin {
  com.sun.security.auth.module.LdapLoginModule required
  userProvider="ldap://137.65.151.12:636/DC=Test-
AD,DC=provo,DC=novell,DC=com"
  authIdentity="{USERNAME}@Test-AD.provo.novell.com"
  userFilter="(&(sAMAccountName={USERNAME})(objectclass=user))"
  useSSL=true;
};
```

#### 4 Restart the Sentinel service:

```
/etc/init.d/sentinel stop
/etc/init.d/sentinel start
```

You have successfully configured the Sentinel 6.1 server for LDAP authentication, and now you can create Sentinel LDAP user accounts in the Sentinel Control Center. For more information on creating LDAP user accounts, see “[Creating an LDAP User Account for Sentinel](#)” in the *Sentinel 6.1 User Guide*.

---

**NOTE:** To modify an existing LDAP configuration, run the `ldap_auth_config` script again and specify the new values for the parameters.

---

## 3.9.2 Configuring Multiple LDAP Servers for Failover

You can configure multiple LDAP servers for failover only on Windows and Linux platforms.

To configure one or more LDAP servers as failover servers for LDAP authentication:

#### 1 Log in to the Sentinel server as `esecadm`.

#### 2 Stop the Sentinel service.

```
/etc/init.d/sentinel stop
```

#### 3 Change to the `<Install_Directory>/config` directory:

```
cd <Install_Directory>/config
```

#### 4 Open the `auth.login` file for editing.

```
vi auth.login
```

#### 5 Update the `userProvider` in the `LdapLogin` section to specify multiple LDAP URLs. Separate each URL by a blank space.

For example:

```
userProvider="ldap://ldap-url1 ldap://ldap-url2"
```

---

**NOTE:** For Active Directory, ensure that the subtree in the LDAP URL is not blank.

---

For more information on specifying multiple LDAP URLs, see the description of the `userProvider` option in [Class LdapLogin Module \(http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html\)](http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html).

#### 6 Save the changes.

#### 7 Export the certificate of each failover LDAP server and copy the certificate file to the `<Install_Directory>/config` directory on the Sentinel 6.1 server.

For more information, see [Step 1](#) in section “[Configuring the Sentinel 6.1 Server for LDAP Authentication](#)” on page 58.

- 8 Ensure that you set the necessary ownership and permissions of the certificate file for each failover LDAP sever.

**Windows:** Not applicable.

**Linux/Solaris:** Run the following commands:

```
chown esecadm:esec <Install_Directory>/config/<cert-file>
```

```
chmod 700 <Install_Directory>/config/<cert-file>
```

- 9 Add each failover LDAP server certificate to the keystore `ldap_server.keystore` that is created in [Step 9](#) in section “[Configuring the Sentinel 6.1 Server for LDAP Authentication](#)” on [page 58](#).

**Windows:**

```
"%ESEC_HOME%\jre64\bin\keytool.exe" -importcert -noprompt -trustcacerts -file <certificate-file> -alias <alias_name> -keystore ldap_server.keystore -storepass sentinel
```

**Linux/Solaris:**

```
$(ESEC_HOME)/jre64/bin/keytool -importcert -noprompt -trustcacerts -file <certificate-file> -alias <alias_name> -keystore ldap_server.keystore -storepass sentinel
```

where `<certificate-file>` is the LDAP certificate filename in Base64-encoded format and `<alias_name>` is the alias name for the certificate to be imported.

---

**IMPORTANT:** Ensure that you specify the alias. If no alias is specified, the keytool takes `mykey` as the alias by default. When you import multiple certificates into the keystore without specifying an alias, the keytool reports an error that the alias already exists.

---

- 10 Start the Sentinel service.

```
/etc/init.d/sentinel start
```

## Additional Configuration for Linux Platform

In Linux, the Sentinel 6.1 server times out before it finds that the primary LDAP server is down, and hence does not connect to the failover LDAP server. To ensure that the Sentinel 6.1 server connects to the failover LDAP server without timing out, perform the following steps:

- 1 Log in to the Sentinel 6.1 server as `root` user.
- 2 Open the `sysctl.conf` file for editing:

```
vi /etc/sysctl.conf
```
- 3 Ensure that the `net.ipv4.tcp_syn_retries` value is set to 3. If the entry does not exist, add the entry. Save the file:

```
net.ipv4.tcp_syn_retries = 3
```
- 4 Execute the following commands for the changes to take effect:

```
/sbin/sysctl -p  
/sbin/sysctl -w net.ipv4.route.flush=1
```
- 5 Set the Sentinel 6.1 server time out value by adding the `-Desecurity.remote.timeout=60` parameter in `control_center.sh` and `solution_designer.sh` in the `$(ESEC_HOME)/bin` directory:

**control\_center.sh:**

```
"$ESEC_HOME/jre/bin/java" $MEMORY -
Dcom.esecurity.configurationfile=$ESEC_CONF_FILE -
Desecurity.cache.directory="$ESEC_HOME/data/control_center.cache" -
Desecurity.communication.service="sentinel_client" -Dfile.encoding=UTF8 -
Desecurity.dataobjects.config.file="/xml/BaseMetaData.xml,/xml/
WorkflowMetaData.xml,/xml/ActMetaData.xml" -
Djava.util.logging.config.file="$ESEC_HOME/config/
control_center_log.prop" -Djava.security.auth.login.config="$ESEC_HOME/
config/auth.login" $SENTINEL_LANG_PROP $SENTINEL_CTRY_PROP -
Dice.pilots.html4.baseFontFamily="Arial Unicode MS" -
Desecurity.remote.timeout=60 -jar ../lib/console.jar
```

#### **solution\_designer.sh:**

```
"$ESEC_HOME/jre/bin/java" -classpath $LOCAL_CLASSPATH $MEMORY -
Dcom.esecurity.configurationfile="$ESEC_CONF_FILE" -
Dsentinel.installer.jar.location="$ESEC_HOME/lib/contentinstaller.jar" -
Desecurity.communication.service="sentinel_client" -Dfile.encoding=UTF8 -
Desecurity.dataobjects.config.file="/xml/BaseMetaData.xml,/xml/
WorkflowMetaData.xml,/xml/ActMetaData.xml" -
Djava.util.logging.config.file="$ESEC_HOME/config/
solution_designer_log.prop" -
Djava.security.auth.login.config="$ESEC_HOME/config/auth.login"
$SENTINEL_LANG_PROP $SENTINEL_CTRY_PROP -Desecurity.cache.directory=../
data/solution_designer.cache -Desecurity.remote.timeout=60
com.esecurity.content.exportUI.ContentPackBuilder
```

### **3.9.3 Migrating LDAP User Accounts from Sentinel 6.1 SP1 Hotfix 2 to Sentinel 6.1 SP2**

In Sentinel SP1 Hotfix 2, LDAP users are created by using the *Domain* authentication option in the User Manager window of Sentinel Control Center. In Sentinel 6.1 SP2, LDAP users are created by using a new option called *LDAP Authentication*.

Use the following procedure to ensure that the existing LDAP users created in SP1 Hotfix 2 function properly in SP2:

- 1** Run the LDAP Authentication configuration script.
- 2** Log in to Sentinel Control Center, select *Admin* tab, then open the User Manager window.
- 3** For each existing LDAP user, right-click and select *User Details*.

The LDAP user who was created by using the *Domain* option is displayed as *LDAP* type.

- 4** If you specified *n* for “[Anonymous searches on LDAP directory](#)” parameter while configuring LDAP authentication, specify the fully qualified DN of the LDAP user in the *LDAP User DN* field.

For more information, see “[Creating an LDAP User Account for Sentinel](#)” in the *Sentinel 6.1 User Guide*.

- 5** Click *OK*.



## 3.10 Updating the License Key

If you purchase the product after evaluation, follow the procedure given below to update your license key in the system to avoid re-installation.

- ♦ [Section 3.10.1, “Unix,” on page 65](#)
- ♦ [Section 3.10.2, “Windows,” on page 65](#)

### 3.10.1 Unix

- 1 As the Sentinel Administrator operating system user, log in to the machine where the DAS component is installed (The default is `esecadm`).
- 2 In the command prompt, change the directory to `$ESEC_HOME/bin`.
- 3 Enter the following command:  

```
./softwarekey.s h
```
- 4 Specify number 1 to set your primary key, then press Enter.

### 3.10.2 Windows

- 1 As a user with administrative rights, log in to the machine where the DAS component is installed.
- 2 In the command prompt, change directory to `%ESEC_HOME%\bin`.
- 3 Enter the following command:  

```
.\softwarekey.bat
```
- 4 Specify number 1 to set your primary key, then press Enter.



# Testing the Installation

# 4

- ♦ Section 4.1, “Testing the Installation,” on page 67
- ♦ Section 4.2, “Clean Up from Testing,” on page 75
- ♦ Section 4.3, “Getting Started,” on page 76

## 4.1 Testing the Installation

Sentinel is installed with a demonstration collector that can be used to test many of the basic functions of the system. Using this collector, you can test Active Views, Incident creation, Correlation rules, and Reports. The following procedure describes the steps to test the system and the expected results. You might not see the exact events, but your results should be similar to the results below.

At a basic level, these tests allow you to confirm the following:

- ♦ Sentinel Services are up and running
- ♦ Communication over the message bus is functional
- ♦ Internal audit events are being sent
- ♦ Events can be sent from a Collector Manager
- ♦ Events are being inserted into the database and can be retrieved using either Historical Event Query or the Crystal Reports
- ♦ Incidents can be created and viewed
- ♦ The Correlation Engine is evaluating rules and triggering correlated events
- ♦ The Sentinel Data Manager can connect to the database and read partition information

If any of these tests fail, review the installation log and other log files, and contact [Novell Technical Support](http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup) ([http://support.novell.com/phone.html?sourceidint=suplnav4\\_phonesup](http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup)), if necessary.

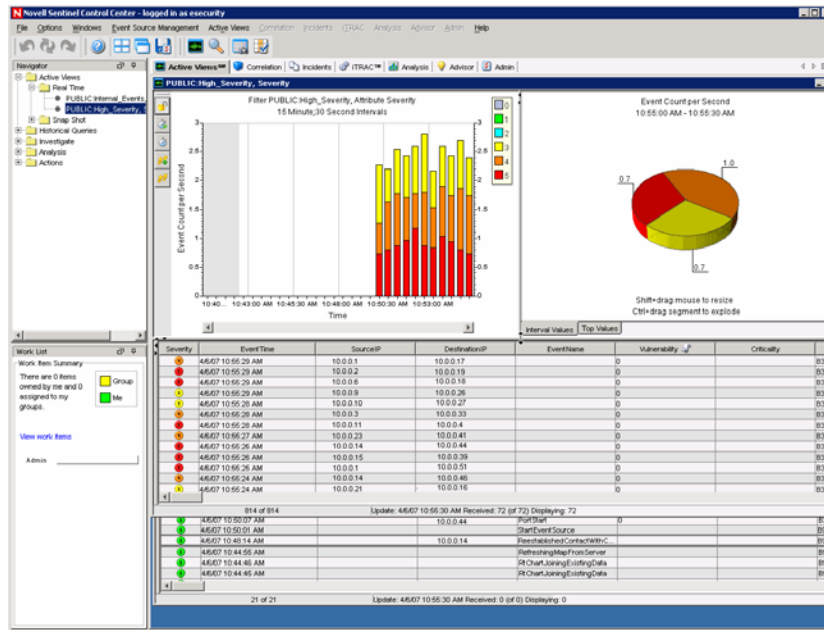
### To test the installation:

1 Start the Sentinel Control Center:

- ♦ **Windows:** Double-click the Sentinel Control Center icon on the desktop.
- ♦ **Linux/Solaris:** Log in as an admin user (esecadm), change the directory to `$ESEC_HOME/bin` and run `./control_center.sh` from the command prompt. Specify the credentials and press Enter.

2 Log in to the system as an admin user (esecadm by default).

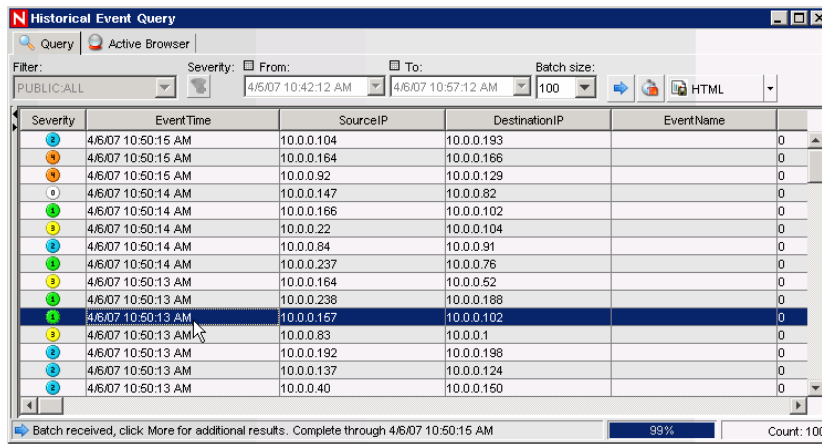
The Sentinel Control Center opens and you can see the events in the Active Views filtered by public filters: `Internal_Events` and `High_Severity`.



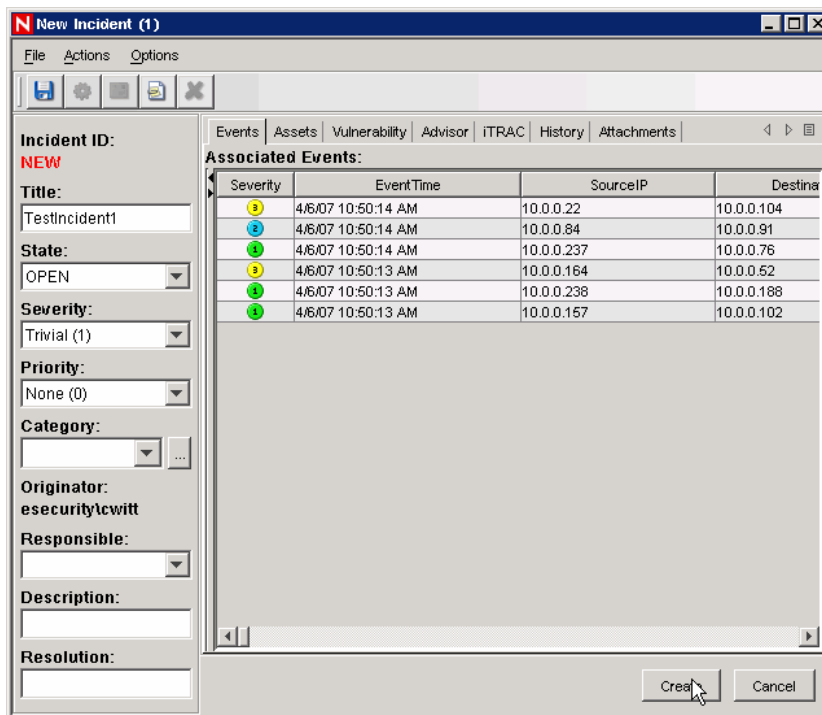
- 3 Click the *Event Source Management* menu, and select *Live View*.
- 4 In the Graphical view, right-click 5 eps event source and select *Start*.
- 5 Close the *Event Source Management Live View* window.
- 6 Click the *Active Views* tab.

The Active window titled PUBLIC: High\_Severity, Severity. The collector might take some time to start and send the data to get displayed in the Active View window.

- 7 Click the *Event Query* button in the toolbar.  
The *Historical Event Query* window is displayed.
- 8 In the *Historical Event Query* window, click the *Filter* drop-down arrow to select the filter. Highlight Public: All filter and click Select.
- 9 Select a time period that covers the time that the Collector has been active. Select the date range from the *From* and *To* drop-down list.
- 10 Select a batch size from the Batch size drop-down list.
- 11 Click the *Magnifying Glass* icon to run the query.

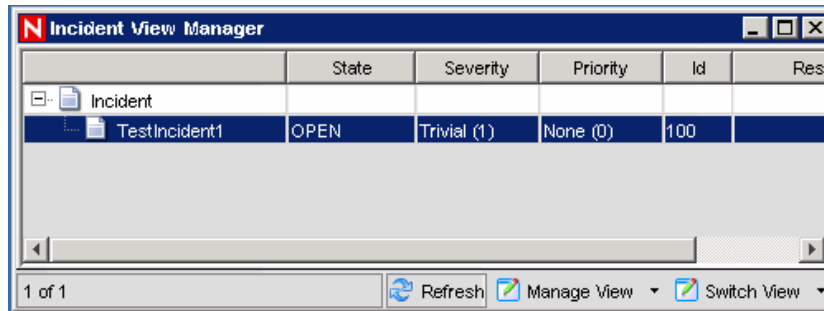


- 12 Hold down the Ctrl or Shift key, and select multiple events from the *Historical Event Query* window.
- 13 Right-click and select *Create Incident*.

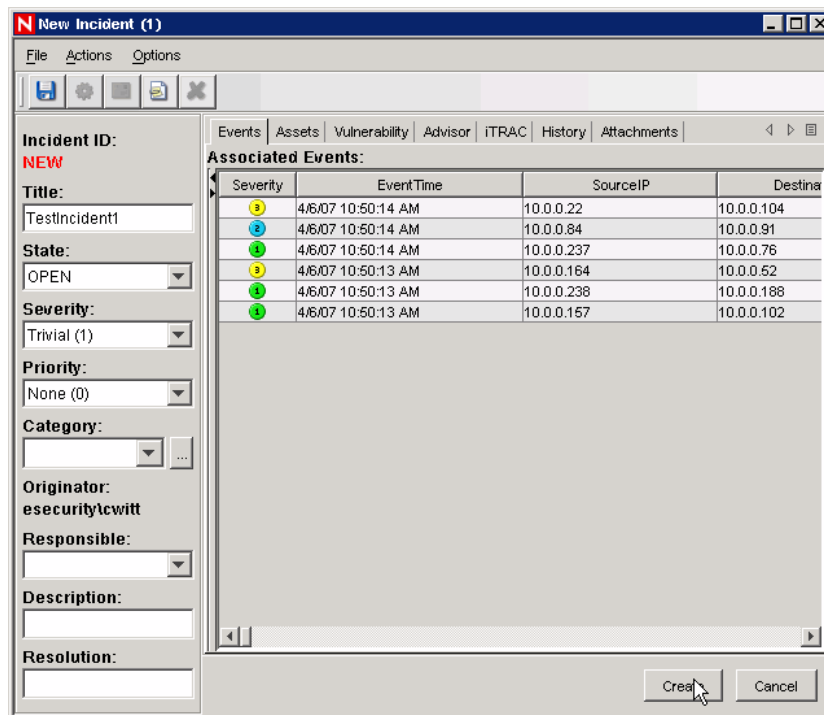


- 14 Enter a name for the incident TestIncident1 and click *Create*. A success notification displays.
- 15 Click *OK*.
- 16 Click the *Incident* tab.

The *Incident View Manager* window is displayed that lists the incident that you created.



17 Double-click the incident to display.



18 Click *File > Exit* or click the X button on the upper right corner of the window to close the *Incident* window.

19 Click the *Analysis* tab.

The *Analysis Navigator* window with the *Events* folder is displayed.

20 Click *Historical Event Queries*.

21 Click *Analysis > Create Report* or click the *Create Report* icon.

An *Event Query* window is displayed. Set the following:

- ◆ time frame
- ◆ filter
- ◆ severity level
- ◆ batch size (this is the number of events to view – events display from oldest events to newer events)

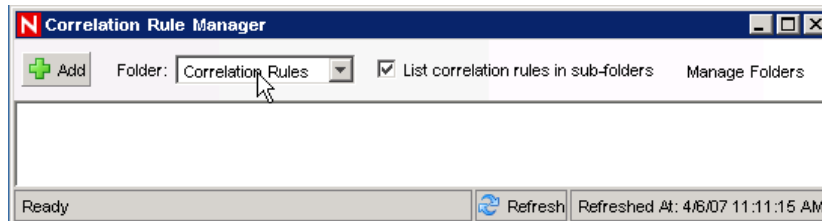
22 Click the *Begin Searching* icon.

- 23** To view the next batch of events, click *More*.
- 24** Rearrange the columns by dragging and dropping them, and sort the events as required by clicking the respective column heading.

When the query is complete, it gets added to the list of quick queries in the Navigator.

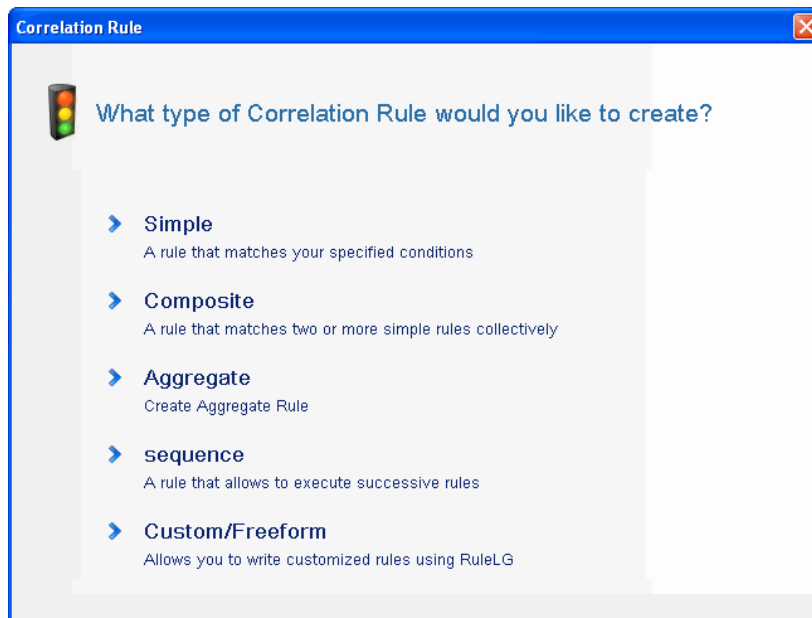
- 25** Click the *Correlation* tab.

The *Correlation Rule Manager* window is displayed.



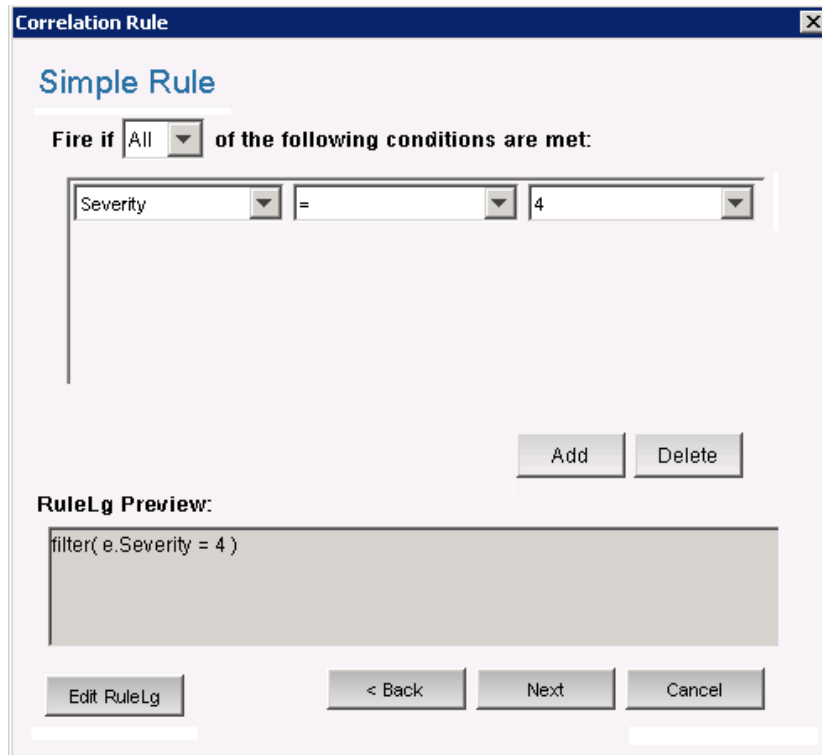
- 26** Click *Add*.

The *Correlation Rule* wizard is displayed.

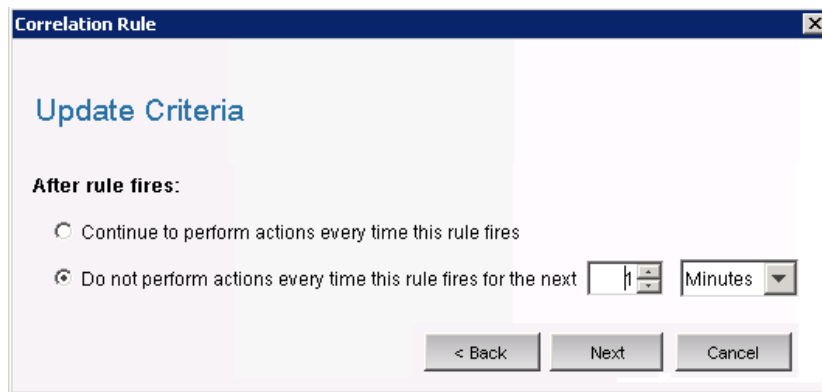


- 27** Click *Simple*.

The *Simple Rule* window is displayed.



- 28 Use the drop-down menus to set the criteria to Severity 4. Click *Next*. The *Update Criteria* window is displayed.



- 29 Select *Do not perform actions every time this rule fires for the next* and set the time period to 1 Minute using the drop-down menu. Click *Next*. The *General Description* window displays.



**Correlation Rule**

**General Description**

**Name**

**Namespace**

**Description**

< Back    Next    Cancel

**30** Enter a name and description for the rule, and click *Next*.

**31** Select *No, do not create another rule* and click *Next*.

**32** Create an action to associate the rule that you have created:

**32a** Perform either of the following:

- ◆ Select *Tools > Action Manager > Add*.
- ◆ In the Deploy Rule window, click *Add Action*. For more information, see [Step 33](#) thru [Step 34](#) on page 74.

The Configure Action window is displayed.

**Configure Action**

Action Name

CorrelatedEvent Action

Action

Name	Value
<b>Action Parameters</b>	
Event Options	Do not copy fields from trigger event
<b>Attribute Values</b>	
Severity	5
EventName	CorrelatedEvent
Message	
Resource	
SubResource	

Help    Add Action Plugin    Save    Cancel

**32b** In the Configure Action window, specify the following:

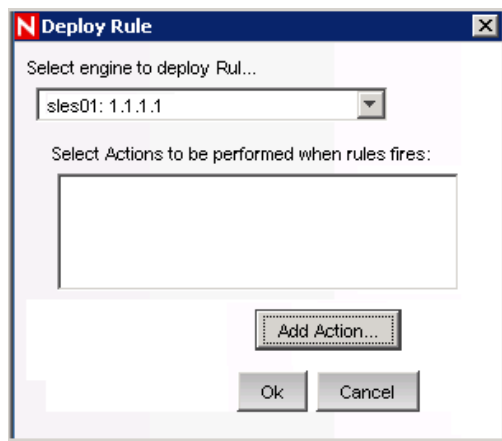
- ◆ Specify the action name. For example, CorrelatedEvent Action.
- ◆ Select *Configure Correlated Event* from the *Action* drop-down list.
- ◆ Set the *Event Options*.
- ◆ Set the *Severity* to 5.
- ◆ Specify the *EventName*. For example, CorrelatedEvent.
- ◆ Specify a message if required.

**32c** Click *Save*.

**33** Open the Correlation Rule Manager window.

**34** Select a rule and click the *Deploy rules* link.

The Deploy Rule window is displayed.



**35** In the Deploy rule window, select the Engine to deploy the rule from the drop-down list.

**36** Select the action that you created in [Step 32 on page 73](#) to associate with the rule and click *OK*.

**37** Select *Correlation Engine Manager*.

In the Correlation engine, you can see the rule is deployed/enabled.



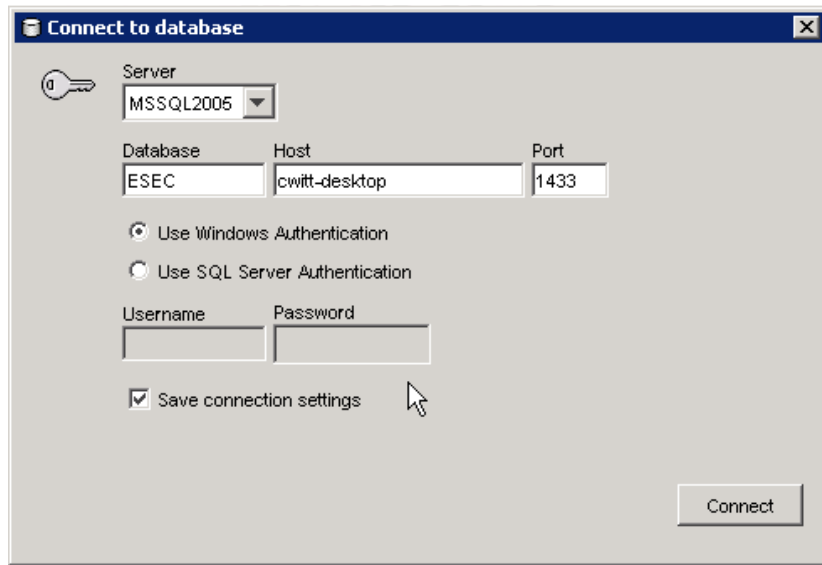
**38** Click the *Active Views* tab and verify that the Correlated Event is generated.

Severity	EventTime	EventName	Message	XDATA: EconomyName
5	8/17/09 11:43:34 AM	Authentication--Failed	User dd has failed Authentication to Sentinel/Wizard; reqId(ABA0BSA0-6D21-102...	
5	8/17/09 11:43:34 AM	AuthenticationFailed--Failed	Authentication of user dd with OS name BLR-PRADHIKA/pradhi from 169.254...	
5	8/17/09 11:43:34 AM	CorrelatedEvent		
5	8/17/09 11:43:34 AM	CorrelatedEvent		

**39** Close the Sentinel Control Center.

**40** Double-click the Sentinel Data Manager (SDM) icon on the desktop.

**41** Log in to SDM using the Database Administrative User specified during installation (esecdba by default).



**42** Click each tab to verify that you can access them.

**43** Close Sentinel Data Manager.

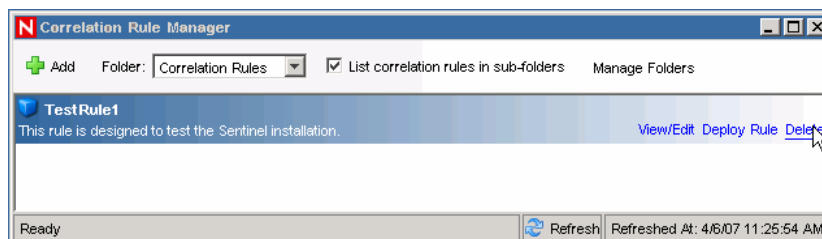
If you were able to proceed through all of these steps without errors, you have completed a basic verification of the Sentinel system installation.

## 4.2 Clean Up from Testing

After completing the system verification, you should remove the objects that were created for the tests.

### To perform a clean up after system testing:

- 1** Log in to the system as an admin user (esecadm by default).
- 2** Click the *Correlation* tab.
- 3** Open *Correlation Engine Manager*.
- 4** Right-click `TestRule1` in the Correlation Engine Manager and select *Undeploy*.
- 5** Open *Correlation Rule Manager*.
- 6** Select `TestRule1` and click *Delete*.



**7** Click the *Event Source Management* menu, and select *Live View*.

**8** In the Graphical event source hierarchy, right-click *General Collector* and select *Stop*.

- 9 Close the Event Source Management window.
- 10 Click the *Incidents* tab.
- 11 Open the Incident View Manager.
- 12 Select `TestIncident1`, right-click and select *Delete*.

## 4.3 Getting Started

To get started with real data, import and configure the Collectors that are appropriate for your environment, configure your own rules, build iTRAC workflows, and so on. The Sentinel Solution Packs help you get started quickly.

# Adding Sentinel Components

# 5

- ♦ [Section 5.1, “Adding Sentinel Components to an Existing Installation,” on page 77](#)
- ♦ [Section 5.2, “Installing Additional Load Balancing Nodes,” on page 77](#)

## 5.1 Adding Sentinel Components to an Existing Installation

It might be necessary, at times, to install additional Sentinel components on a machine that already has a Sentinel installation. For example, you may need to install Collector Builder where Sentinel Control Center is already installed.

The Sentinel installer makes it simple to perform this kind of installation. Ensure that you met the prerequisites of the additional component being installed as specified in [Chapter 3, “Installing Sentinel 6.1 SP2,” on page 27](#). The requirements on the machine are likely to increase when installing additional components. Then run the Sentinel installer on the target machine just as if you were installing on a “clean” machine. When running in add component mode, the installer slightly changes its behavior in the following ways:

- ♦ The installer will automatically detect the existing Sentinel installation and displays a screen indicating the location of the existing install and which components are already installed.
- ♦ The installer will not prompt for the destination directory. The destination directory of the existing installation will be used.
- ♦ The install will not prompt to select Simple or Custom install type. The Custom install type is assumed.

---

**NOTE:** Only one instance of Advisor and the Communication Server can exist in a distributed Sentinel installation.

---

## 5.2 Installing Additional Load Balancing Nodes

Occasionally, it might be necessary to add an additional Sentinel processing node to the Sentinel distributed environment in order to load balance across machines. For example, if the memory usage is high on a machine running a Correlation Engine, you might decide to add another machine running Correlation Engine. (This may require an additional license.) You can then redeploy your correlation rules across these two engines in order to decrease the load on a single machine if all the rules were deployed on it.

To do this, simply run the installer on the new machine as described in [Chapter 3, “Installing Sentinel 6.1 SP2,” on page 27](#). As you step through the installer, select only the components you want to add additional load balancing nodes for. The following components can be load balanced:

- ♦ Correlation Engine
- ♦ Collector Manager
- ♦ DAS\_Binary process

The DAS\_Binary process is responsible for event database insertion. Because event database insertions can be an event flow bottleneck, load balancing the DAS\_Binary process typically results in a significant performance gain, in terms on events per second throughput. Additionally, the Correlation Engine and Collector Manager components can be load balanced by installing instances of these components on additional machines

## 5.2.1 Multiple DAS\_Binary Processes

Although not true load-balancing, it is possible to configure multiple DAS\_Binary instances in a Sentinel system to improve performance of event insertion. This should only be considered after analyzing the system for bottlenecks and finding that DAS\_Binary has fully utilized the CPU. DAS\_Binary is the process that manages event insertion into the database, and the highest event rates Novell has achieved in internal testing were with multiple DAS\_Binary processes.

For more information on the Sentinel 6.1 performance test results, see the [Novell Documentation site \(http://www.novell.com/documentation/sentinel61\)](http://www.novell.com/documentation/sentinel61).

Multiple DAS\_binary processes can be installed on the same machine or distributed across multiple machines.

### Distributing Multiple DAS\_binary Instances Across Different Machines

---

**IMPORTANT:** Before you proceed, ensure that you have installed the Sentinel Server including the DAS. This installation is referred to as the Sentinel Server or the primary DAS\_Binary.

---

- 1** Run the Sentinel installer to install the DAS component on the machines that you want to run a DAS\_Binary process. All DAS\_Binary should connect to the same database; therefore, during installation provide the same database connection information you provided for the initial DAS installation.
- 2** On all machines where you want to run the DAS\_Binary, including the primary DAS\_Binary, make the following modifications:
  - 2a** Log in as `esecadm` (UNIX) or an Administrator (Windows) to any one of the machines that run an instances of the DAS\_Binary process and locate the `configuration.xml` file in the `$ESEC_HOME/config` (`%ESEC_HOME%\config` on Windows) directory.
  - 2b** Add the following information to services section of the `configuration.xml` file:

```
<service name="DAS_Binary_EventStore" plugins=""
strategyid="sentinel_client" subscriptiongroup="dasbin" />
```
  - 2c** Save the `configuration.xml` file.
- 3** On the machines that are running secondary DAS\_Binary processes, make the following modifications. A secondary DAS\_Binary is the one that is not running on the main Sentinel Server.
  - 3a** Remove the file `sentinelhost.id` from the `$ESEC_HOME/data` (`%ESEC_HOME%\data` on Windows) directory. This will force the Collector Manager on this machine to generate a new ID rather than using the same one that Sentinel Server's Collector Manager is using.
  - 3b** The other DAS processes should be disabled. To do this, in the process section of the `configuration.xml` file on the DAS\_Binary-only machines, set the `min_instances` attribute as follows:

```
min_instances="0"
```

for the following process entries:

- ◆ DAS\_RT
- ◆ DAS\_Aggregation
- ◆ DAS\_Query
- ◆ DAS\_ITRAC

**3c** The secondary Sentinel service should be used. Therefore, the `sentinel.conf` in the `ESEC_HOME/config` directory must be modified by uncommenting the following line by removing the `#` character from the beginning of the line:

```
wrapper.app.parameter.1=../config/sentinel.xml
```

and commenting out the following line by inserting the `#` character at the beginning of the line:

```
#wrapper.app.parameter.1=../config/sentinel_primary.xml
```

**4** Make the following changes to the `das_binary.xml` file on one of the machines that run a DAS\_Binary process:

---

**NOTE:** The `das_binary.xml` file will later be copied to other DAS\_Binary installations.

---

**4a** Make a copy of the entire `DispatchManager` component and change the new component's id from `DispatchManager` to `EventStoreDispatchManager`. After making this change, you should have one component with the id `DispatchManager` and another component with the id `EventStoreDispatchManager`. See the example below of what the new `EventStoreDispatchManager` component should look like.

**4b** Update the value of the property named `esecurity.communication.service` of the `EventStoreDispatchManager` component to `DAS_Binary_EventStore`.

**4c** Remove the property with name `handler:esecurity.event.create` from the `DispatchManager` component.

**4d** Remove all properties with a name that starts with "handler:\*" except for `handler:esecurity.event.create` from the `EventStoreDispatchManager` component. The handler `handler:esecurity.event.create` should be the only handler defined in the `EventStoreDispatchManager` component.

**4e** Add the following XML element to the `EventStoreService` component:

```
<obj-component-ref>
<name>DispatchManager</name>
<ref-id>EventStoreDispatchManager</ref-id>
</obj-component-ref>
```

When the `DAS_BINARY` processes are installed on different remote machines, there is only one instance of the aggregation process that runs on the primary DAS server. Hence, all the remote (secondary) `DAS_BINARY` processes should write their event files to a common location that can be used by the `EventAggregationService` (running on the primary DAS server) to pick up the event files from the remote (secondary) `DAS_BINARY` processes.

**4f** The `outputDirectory` property in the `EventFileRedirect` component in each of the secondary `das_binary.xml` files should point to the common location where the `EventAggregationService` on the primary `DAS_BINARY` is writing to.

The value (directory location) of the `directory` property in the `EventAggregationService` component of the `das_aggregation.xml` file on the primary DAS server should be shared with all the machines that are running the secondary `das_binary` process.

Use the map drive option for Windows and the mount option for Unix to share the location of primary DAS\_BINARY with the secondary DAS\_BINARY.

---

**NOTE:** You must ensure that the user who owns the Sentinel service has permissions to access the shared folder. Use the UNC path to specify the output directory for the EventFileRedirect service. For example, \\<ipaddress of the machine having the shared drive>\events\aggregation.

---

- 4g** Save the `das_binary.xml` file.
- 5** Copy the modified `das_binary.xml` file to all machines that run a DAS\_Binary process, including the primary DAS\_Binary.

Following is a sample excerpt from the `das_binary.xml` file showing the `EventStoreDispatchManager` component.

```
<obj-component id="EventStoreDispatchManager">
<class>esecurity.ccs.comp.dispatcher.CommDispatcherManager</class>
<property name="esecurity.communication.service">DAS_Binary_EventStore</
property>
<property name="dependencies">DAS_Query</property>
<property
name="handler:esecurity.event.create">esecurity.ccs.cracker.EventCracker@
ewizard_binary_event,correlation_binary_event,database_binary_event,datab
ase_tagged_event,correlation_binary_event_update</property>
<obj-component id="DispatcherStatsService">
<class>esecurity.ccs.comp.dispatcher.stats.DispatcherStatsManager</class>
<property name="ReportIntervals">900,3600,14400,86400</property>
<property name="MinLogReportInterval">900</property>
<property name="MinPublishReportInterval">86400</property>
<property name="ReportByServiceName">true</property>
<property name="ReportByMethodName">true</property>
<obj-component-ref>
<name>EventPublisher</name>
<ref-id>DispatchManager</ref-id>
</obj-component-ref>
<obj-component-ref>
<name>DispatchManager</name>
<ref-id>DispatchManager</ref-id>
</obj-component-ref>
</obj-component>
</obj-component>
```

Here is a sample excerpt from the `das_binary.xml` file showing the `EventStoreService` component:

```
<obj-component id="EventStoreService">
<class>esecurity.ccs.comp.event.EventStoreService</class>
<property name="handler">esecurity.event.create</property>
<property name="waitBlocked">true</property>
<property name="maxThreads">6</property>
<property name="minThreads">6</property>
<property name="maxThreadsQueued">10</property>
<property name="queueSize">1000000</property>
<obj-component-ref>
<name>ThreadPool</name>
<ref-id>EventStoreThreadPool</ref-id>
</obj-component-ref>
<obj-component-ref>
<name>DispatchManager</name>
```



```

<ref-id>EventStoreDispatchManager</ref-id>
</obj-component-ref>
<obj-component id="Persistor">
<class>esecurity.ccs.comp.event.jdbc.JDBCEventStore</class>
<property name="insert.batchsize">600</property>
<property
name="insert.strategy">esecurity.ccs.comp.event.jdbc.JDBCLoadStrategy</
property>
<property name="insert.oci.workerCount">5</property>
<property name="insert.oci.queueWaitTime">1</property>
<property name="insert.oci.highWatermark">10000000</property>
<property name="insert.oci.lowWatermark">9000000</property>
<property name="insert.oci.optimizationFlag">on</property>
<property name="insert.pmaxWarningTime">300</property>
<property name="insert.pminWarningTime">300</property>
</obj-component>
<obj-component-ref>
<name>EventRedirect</name>
<ref-id>EventFileRedirectService</ref-id>
</obj-component-ref>
</obj-component>

```

**6** Delete the unneeded durable subscription.

After the system is restarted, the multiple DAS\_Binary processes share a new, single, durable shared subscription to the Sentinel message bus event channels. In order to avoid the message bus cache from growing indefinitely and filling up the hard drive, the durable subscription that was initially created by the primary DAS\_Binary must be deleted.

**6a** Open the Sonic Management Console.

**6b Windows:** Select *Start > Programs > Sentinel > SonicMQ > SonicMQ 7.0 > Management Console*

**Unix:** Open a terminal console and run the following command:

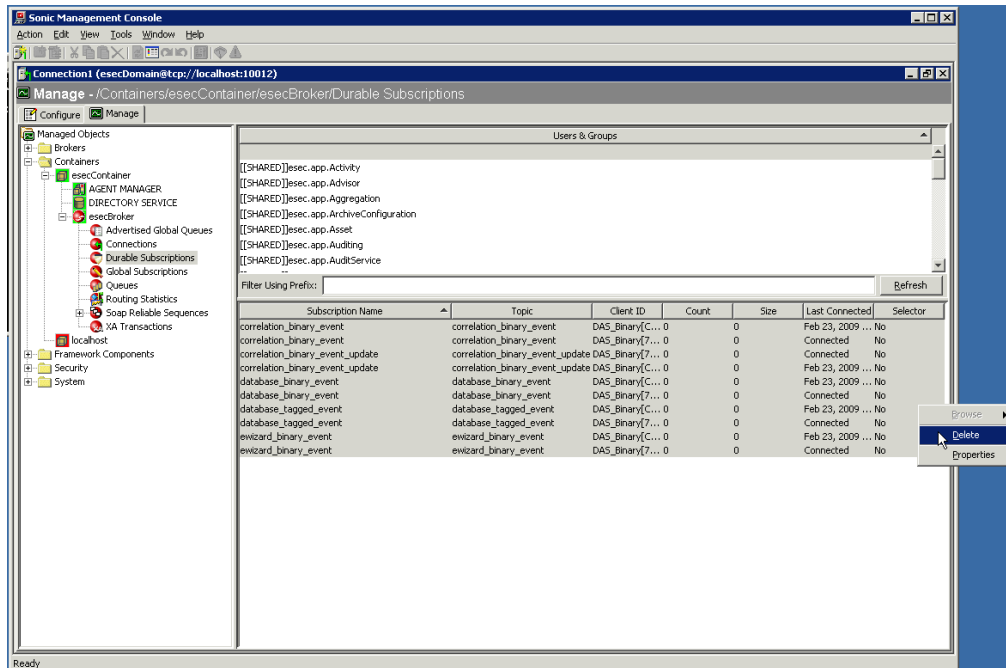
```
$ESEC_HOME/3rdparty/SonicMQ/MQ7.0/bin/startmc.sh
```

**6c** Specify the following to log in to the management console:

Options	Description
Connection Name	Leave as default
Domain Name	esecDomain
Connection URL	tcp://localhost:10012
User Name	Leave as default
Password	Leave as default

**6d** In the management console, select *Manage tab > Containers > esecContainer > esecBroker > Durable Subscriptions*.

**6e** Select the first empty row in the Users & Groups table on the right side of the GUI.



When you select the empty row at top of this table, view the details of the DAS\_Binary durable subscriptions below the empty row.

- 6f Select all durable subscriptions, right click, and then select *Delete*.
- 7 To activate your changes, restart the Sentinel service on all machines where you have made the modifications.

**UNIX:** Run the following command:

```
$ESEC_HOME/bin/sentinel.sh restart
```

**Windows:** Restart the "Sentinel" service using the Windows Service Manager.

### Configuring Multiple DAS\_binary Instances on the Same Machine

- 1 Log in as esecadm (UNIX) or an Administrator (Windows) to the machine that will run multiple instances of the DAS\_Binary processes and locate the `configuration.xml` file in the `$ESEC_HOME/config` (`%ESEC_HOME%\config` on Windows) directory.
- 2 In the `configuration.xml` file, locate the section of the xml file that defines the services entries (see example below). Make a copy of the DAS\_Binary service entry for every instance of DAS\_Binary you want to run. For example, to run two DAS\_Binary processes, make two copies of the DAS\_Binary service entry. Delete the `uuid` attribute for each of the service entries (the `uuid` attribute will automatically be regenerated when Sentinel is started). The following is an example of one DAS\_Binary service entry.

```
<service name="DAS_Binary" plugins="" strategyid="sentinel_client"
uuid="4DA52BE0-E7A4-1029-BB2F-00132168CBDF" />
```

- 3 In the `configuration.xml` file, create a copy of the following DAS\_Binary\_EventStore service entry xml for every instance of DAS\_Binary you want to run. This service does not exist in the `configuration.xml` file, so you should copy it from the example below. For example, to run two DAS\_Binary processes, make two copies of the following DAS\_Binary\_EventStore service entry:

```
<service name="DAS_Binary_EventStore" plugins=""
strategyid="sentinel_client" subscriptiongroup="dasbin" />
```

- 4 Give each copy of the DAS\_Binary and DAS\_Binary\_EventStore service entry a unique name. For example, the service names might be DAS\_Binary1, DAS\_Binary\_EventStore1, DAS\_Binary2, and DAS\_Binary\_EventStore2.
- 5 Locate the section of the configuration.xml file that defines the processes entries (see example below). Make a copy of the DAS\_Binary process entry for every instance of DAS\_Binary you want to run. For example, to run two DAS\_Binary processes, make two copies of the DAS\_Binary process entry. For each DAS\_Binary process entry, modify sections of the entry as described below:
  - ♦ **DAS\_Binary Dsrv\_name:** Change to match the DAS\_Binary service names defined in step 4, such as DAS\_Binary2.
  - ♦ **DAS\_Binary communication service name:** Insert the following text into the process entry's image attribute at the location shown in bold in the process entry example below. For each DAS\_Binary process entry, replace the DAS\_Binary part of the text below with the associated service name, such as DAS\_Binary2.  

```
-Desecurity.communication.service=DAS_Binary
```
  - ♦ **das\_binary.xml file name:** Use any unique name(s), such as das\_binary\_2.xml. These names are used in a later step.
  - ♦ **das\_binary\_log\_prop file name:** Use any unique name(s), such as das\_binary\_log\_2.prop. These names are used in a later step.
  - ♦ **das\_binary.cache directory name:** Use any unique name(s), such as das\_binary2.cache. Each instance of DAS\_Binary must use a different das\_binary.cache directory.
  - ♦ **DAS\_Binary process name:** Change the value of the process entry's name attribute to match the DAS\_Binary service names defined in step 4, such as DAS\_Binary2.

The following xml is an example of a process entry as discussed in the instructions above:

```
process component="DAS" depends="UNIX Communication Server,Windows
Communication Server" image="&quot;$(ESEC_JAVA_HOME)/java&quot;; -server -
Dsrv_name=DAS_Binary -Xmx160m -Xms64m -XX:+UseParallelGC -
XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=../log/DAS_Binary.hprof -
Xss136k -Xrs -Desecurity.communication.service=DAS_Binary -
Duser.language=en -Djava.net.preferIPv4Stack=true -Dfile.encoding=UTF8 -
Desecurity.cache.directory=../data/das_binary.cache -
Desecurity.dataobjects.config.file=/xml/BaseMetaData.xml -
Djava.util.logging.config.file=../config/das_binary_log.prop -
Dcom.esecurity.configurationfile=../config/configuration.xml -
Djava.security.auth.login.config=../config/auth.login -
Djava.security.krb5.conf=../config/krb5.conf -jar ../lib/ccsbase.jar ../
config//das_binary.xml" min_instances="1" name="DAS_Binary"
post_startup_delay="20" type="container" working_directory="$(ESEC_HOME)/
data"/>
```

- 6 Save the configuration.xml file.
- 7 Locate the das\_binary.xml file in the \$ESEC\_HOME/config (%ESEC\_HOME%\config on Windows) directory.
- 8 Create a copy of the das\_binary.xml file for each instance of DAS\_Binary you want to run. For example, to run two instances of DAS\_Binary, create two copies of das\_binary.xml.
- 9 Rename the copied das\_binary.xml files to match the names selected in step 5.

**10** Make the following changes to each of the `das_binary.xml` files:

- ◆ Make a copy of the entire `DispatchManager` component and change the new component's id from `DispatchManager` to `EventStoreDispatchManager`. After making this change, you should have one component with the id `DispatchManager` and another component with the id `EventStoreDispatchManager`.
- ◆ Update the value of the property named `esecurity.communication.service` of the `DispatchManager` component with the appropriate unique name for `DAS_Binary`, such as `DAS_Binary2`.
- ◆ Update the value of the property named `esecurity.communication.service` of the `EventStoreDispatchManager` component with the appropriate unique name for `DAS_Binary_EventStore`, such as `DAS_Binary_EventStore2`.
- ◆ Remove the property with name `handler:esecurity.event.create` from the `DispatchManager` component.
- ◆ Remove all properties with a name that starts with "handler:\*" except for `handler:esecurity.event.create` from the `EventStoreDispatchManager` component. The handler `handler:esecurity.event.create` should be the only handler defined in the `EventStoreDispatchManager` component.
- ◆ Add the following XML element to the `EventStoreService` component.

```
<obj-component-ref>
  <name>DispatchManager</name>
  <ref-id>EventStoreDispatchManager</ref-id>
</obj-component-ref>
```

- ◆ The `outputDirectory` property in the `EventFileRedirect` component of the `das_binary.xml` file must have the same value as the `directory` property in the `EventAggregationService` component of the `das_aggregation.xml` file. This allows the `DAS_Aggregation` to pick up the event files from a secondary `DAS_Binary`.
  - ◆ Save the `das_binary.xml` file.
- 11** Locate the `das_binary_log.prop` file in the `$ESEC_HOME/config(%ESEC_HOME%\config` on Windows) directory.
- 12** Create a copy of the `das_binary_log.prop` file for each instance of `DAS_Binary` you want to run. For example, to run two instances of `DAS_Binary`, create two copies of `das_binary_log.prop`.
- 13** Rename the `das_binary_log.prop` files to match the names selected in step 5.
- 14** Delete the unneeded durable subscription.

After the system is restarted, the multiple `DAS_Binary` processes share a new, single, durable shared subscription to the Sentinel message bus event channels. In order to avoid the message bus cache from growing indefinitely and filling up the hard drive, the durable subscription that was initially created by the primary `DAS_Binary` must be deleted.

**14a** Open the Sonic Management Console.

**14b Windows:** Select *Start > Programs > Sentinel > SonicMQ > SonicMQ 7.0 > Management Console*

**Unix:** Open a terminal console and run the following command:

```
$ESEC_HOME/3rdparty/SonicMQ/MQ7.0/bin/startmc.sh
```

**14c** Specify the following to log in to the management console:

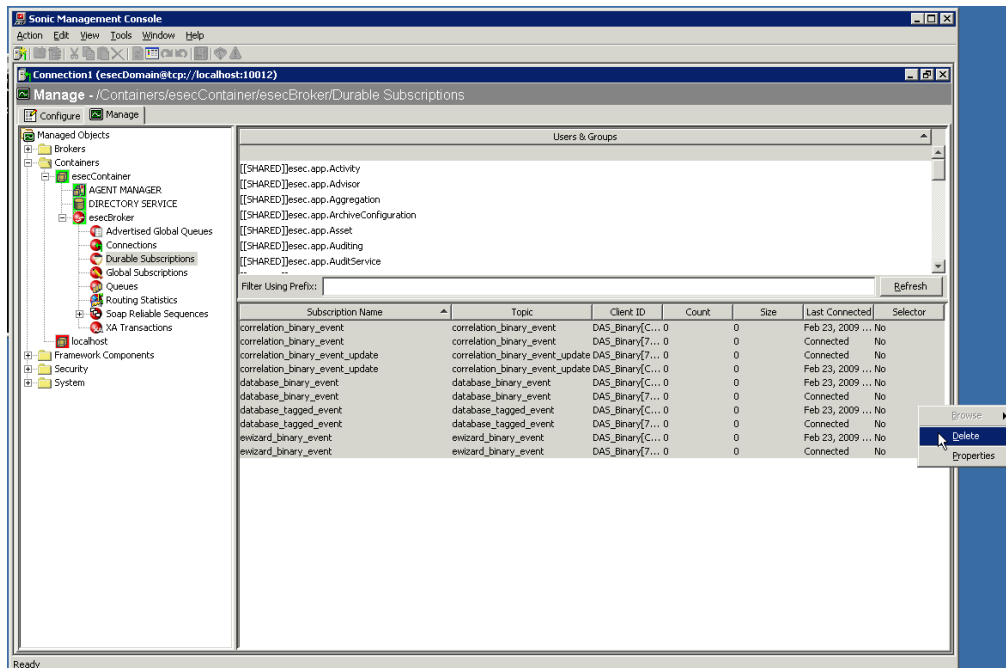
---

Connection Name	Leave as default
Domain Name	esecDomain
Connection URL	tcp://localhost:10012
User Name	Leave as default
Password	Leave as default

---

**14d** In the management console, select *Manage tab > Containers > esecContainer > esecBroker > Durable Subscriptions*.

**14e** Select the first empty row in the Users & Groups table on the right side of the GUI.



When you select the empty row at top of this table, view the details of the DAS\_Binary durable subscriptions below the empty row.

**14f** Select all durable subscriptions, right click, and then select *Delete*.

**15** Restart the Sentinel services to activate your changes.

**UNIX:**

`$ESEC_HOME/bin/sentinel.sh restart`

**Windows:** Restart the Sentinel service using the Windows Service Manager.



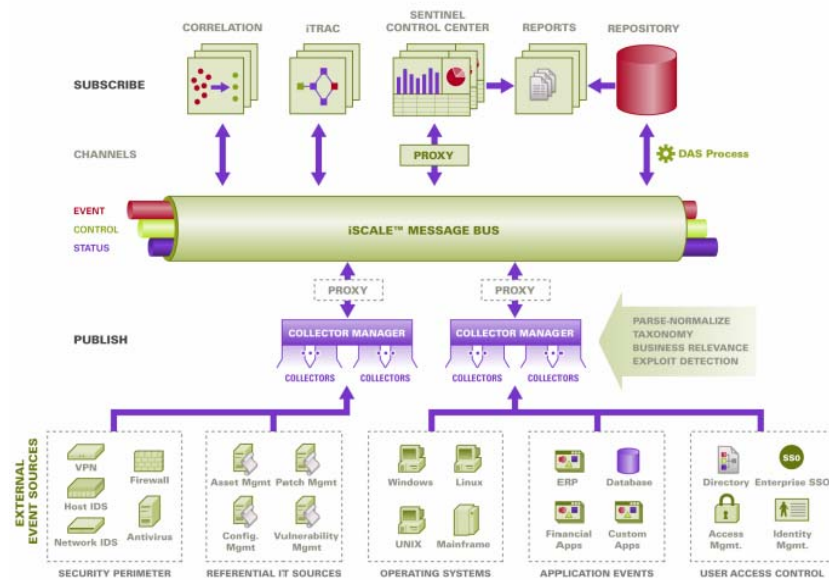
# Communication Layer (iSCALE)

# 6

- ◆ Section 6.1, “SSL Proxy and Direct Communication,” on page 88
- ◆ Section 6.2, “Changing the Communication Encryption Key,” on page 90
- ◆ Section 6.3, “Increasing AES Key Strength,” on page 91

The communication layer (iSCALE) connecting all components of the architecture is an encrypted TCP/IP based connection built on a JMS (Java Messaging Service) backbone. With Sentinel 6, an optional SSL proxy has been added to secure the Collector Manager and Sentinel Control Center components if they are installed outside the firewall.

Figure 6-1 Sentinel Architecture



There are two communication options available when installing the Collector Manager:

- ◆ **Connect directly to the message bus (default):** This is a simplest and fastest option. It requires the Collector Manager to know the shared message bus encryption key, however, which can be a security risk if the Collector Manager is running on a machine that is exposed to security threats (for example, a machine in the DMZ). This option will encrypt communications using AES 128-bit encryption based on the data in a file called `.keystore`.
- ◆ **Connect to the message bus through the proxy:** This option adds an additional layer of security by configuring the Collector Manager to connect through an SSL proxy server. In this case, certificate-based authentication and encryption will be used, so the `.keystore` does not need to be stored on the Collector Manager machine. This is a good option when the Collector Manager is installed in a less secure environment.

Either of these options can be selected when installing the Collector Manager. The Sentinel Control Center uses the proxy by default.

## 6.1 SSL Proxy and Direct Communication

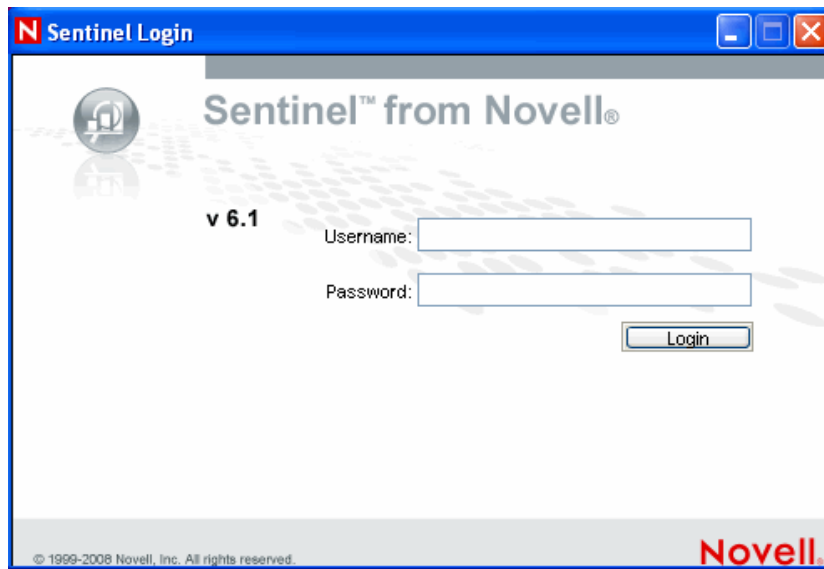
The Sentinel components that might use the SSL proxy are the Sentinel Control Center and the Collector Manager.

### 6.1.1 Sentinel Control Center

The Sentinel Control Center uses the SSL proxy by default. The Sentinel Control Center connects to SSL through the `proxied_client` port. This port is setup to use server-side SSL certificate authentication only. The client side authentication uses the Sentinel Control Center user's username and password.

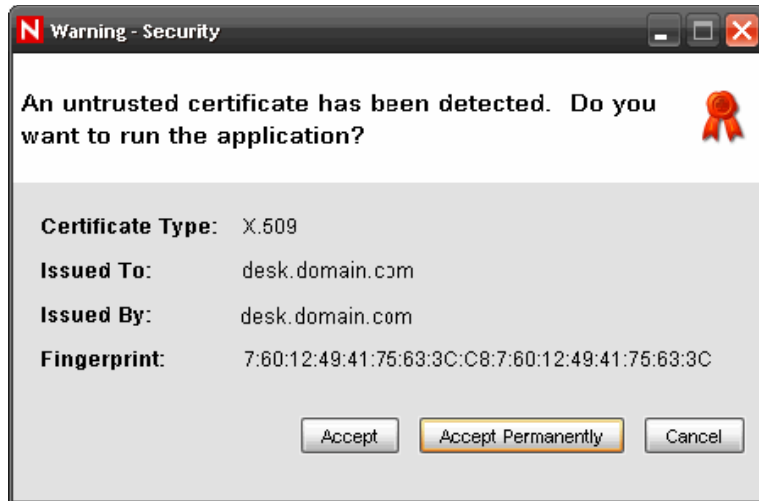
#### To Log into Sentinel Control Center for the First Time:

- 1 Go to Start > Programs > Sentinel and select Sentinel Control Center. Sentinel Login window displays.



- 2 Provide the user credentials you are provided with to log-in to Sentinel Control Center.
  - ♦ Username and password, if using SQL Server authentication, OR
  - ♦ Domain\username and password, if using Windows authentication
- 3 Click Login.
- 4 A warning message displays as shown in the figure below, for the first logon attempt.





- 5 If you select Accept, this message displays every time you try to open Sentinel on your system. To avoid this, you can select Accept permanently.

#### To Start the Sentinel Control Center on Linux and Solaris:

- 1 As the Sentinel Administrator User (esecadm), change directory to:  
`$ESEC_HOME/bin`
- 2 Run the following command:  
`control_center.sh`
- 3 Provide your username and password and click OK.
- 4 A Certificate window displays, click Accept.

The Sentinel Control Center users will need to repeat the procedure above to accept a new certificate under these circumstances:

- ♦ The Sentinel communication server is reinstalled
- ♦ The Sentinel communication server is moved to a new server

### 6.1.2 Collector Manager

Collector Manager can be installed in either proxy mode (using the SSL proxy) or direct mode (connecting directly to the message bus).

- ♦ For Collector Managers that could be more easily compromised (for example, a machine in the DMZ), the SSL proxy is the more secure method of communication.
- ♦ For Collector Managers in a more secure environment or where high event throughput is important or installed on the same machine as the Data Access Service (DAS), direct communication to the message bus is recommended.

The Collector Manager connects to SSL through the `proxied_trusted_client`. To enable Collector Manager to restart without human intervention after a reboot, this port is set up to use both server and client SSL certificate authentication. A trust relationship is established between the proxy and Collector Manager (certificate exchange), with future connections using the certificates to authenticate. This trust relationship is set up automatically during installation.

The trust relationship will need to be reset for every Collector Manager using the SSL proxy if the following circumstances apply:

- ♦ The Sentinel communication server is reinstalled
- ♦ The Sentinel communication server is moved to a new server

This procedure can also be used to change a Collector Manager from direct mode to proxy mode.

### To Reset Trust Relationship for a Collector Manager:

- 1 Log into the Collector Manager server as the Sentinel Administrator (esecadm by default).
- 2 Open the `configuration.xml` file in `$ESEC_HOME/config` or `%ESEC_HOME%\config` in a text editor.
- 3 Modify "Collector\_Manager", "agentmanager\_events", and "Sentinel" services in `configuration.xml` to use "proxied\_trusted\_client" strategy ID. Here is an excerpt from a sample file:

```
<service name="Collector_Manager" plugins=""
strategyid="proxied_trusted_client"/>
<service name="agentmanager_events" plugins=""
strategyid="proxied_trusted_client"/>
<service name="Sentinel" plugins="" strategyid="proxied_trusted_client"/>
```

- 4 Save the file and exit.
- 5 Run `%ESEC_HOME%\bin\register_trusted_client.bat` (or `.sh` file if on UNIX). You will see output similar to this:

```
E:\Program Files\novell\sentinel6>bin\register_trusted_client.bat
Please review the following server certificate:
Type: X.509
Issued To: foo.bar.net
Issued By: foo.bar.net
Fingerprint (MD5): A8:DF:BA:B2:F3:21:C9:27:28:48:13:B3:FE:F8:B4:AD
Would you like to accept this certificate? [Y/N] (defaults to N): Y
Please enter a Sentinel username and password that has permissions to
register a trusted client.
Username: esecadm
Password:*****
*Writing to keystore file: E:\Program
Files\Novell\Sentinel6\config\.proxyClientKeystore
```

- 6 Restart the Sentinel Service on the server hosting the Collector Manager.
- 7 Repeat these steps on all Collector Managers using the proxy communication.

## 6.2 Changing the Communication Encryption Key

The Sentinel installation allows the administrator to generate a new, random encryption key (stored in the `.keystore` file) or import an existing `.keystore` file. With either approach, the `.keystore` file must be the same on every machine that has a Sentinel Server component installed in order for communication to work properly.

---

**NOTE:** The `.keystore` file is not necessary on the database machine if the database is the only Sentinel component installed on that machine. It is also not necessary on machines with only the Sentinel Control Center, Collector Builder, Sentinel Data Manager, or Collector Manager (using a proxy) installed.

---

The encryption key can be changed after installation using the `keymgr` utility. This utility generates a file containing a randomly generated encryption key. This file must be copied to every machine that has a Sentinel Server component installed.

### To change the encryption key for Direct Communication:

**1** For UNIX, log in as the Sentinel Administrator User (`esecadm` by default). For Windows, login as a user with administrative rights.

**2** Go to:

**For UNIX:**

`$ESEC_HOME/lib`

**For Windows:**

`%ESEC_HOME%\lib`

**3** Run the following command:

**On UNIX:**

```
keymgr.sh --keyalgo AES --keysize 128 --keystore <output filename, usually .keystore>
```

**On Windows:**

```
keymgr.bat --keyalgo AES --keysize 128 --keystore <output filename, usually .keystore>
```

**4** Copy `.keystore` to each machine with a Sentinel Server component installed (unless it is using proxy communication). The file should be copied to:

**For UNIX:**

`$ESEC_HOME/config`

**For Windows:**

`%ESEC_HOME%\config`

---

**NOTE:** If you are using Advisor in Direct Download mode, you must update the Advisor password stored in Advisor's configuration files. This password is encrypted using the information in `.keystore` and must be recreated using the new `.keystore` value. To update the password, follow the instructions in .

---

## 6.3 Increasing AES Key Strength

Sentinel uses AES encryption for Communication over Sonic and Encryption passwords stored in config files and sent over Sonic. By default, Sentinel uses the AES 128-bit encryption algorithm because of certain import restrictions. If these import restrictions do not apply to you, you can configure Sentinel to use a stronger AES 256-bit algorithm.

---

**NOTE:** It is highly recommended that you review the “Understanding the Export/Import Issues” section of the Java `Readme.txt` file before enabling 256-bit encryption.

---

**To configure AES 256-bit encryption:**

- 1** Download Unlimited Encryption policies from Sun ([http://java.sun.com/javase/downloads/index\\_jdk5.jsp](http://java.sun.com/javase/downloads/index_jdk5.jsp)). In the Other Downloads section, download “Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 5.0”.
- 2** Apply the above mentioned policy file to all the JRE's that run processes that connect directly to Sonic (DAS, Correlation Engine, Communication Server, Collector Manager if used in Direct to Sonic mode). To understand how to apply policy files, go through the `Readme.txt` available in the policy you downloaded.
- 3** Use the `keymgr` utility to generate a 256-bit AES `.keystore` file by follow the instructions in [Section 6.2, “Changing the Communication Encryption Key,” on page 90](#).
- 4** Copy this `.keystore` file to all machines in step #2 and place in the `$ESEC_HOME/config` or `%ESEC_HOME%\config` directory.

---

**NOTE:** If you are using Advisor in Direct Download mode, you must update the Advisor password stored in Advisor’s configuration files. This password is encrypted using the information in `.keystore` and must be recreated using the new `.keystore` value. For more information on updating a password, see “Certificate Management for DAS\_Proxy” section in [Sentinel 6.1 Reference Guide](#).

---

# Crystal Reports for Windows

# 7

Business Objects Crystal Reports Server is [Section 7.10, “Using Crystal Reports,” on page 120](#) the reporting tool used with Sentinel. This section discusses the installation and configuration of Crystal Reports Server for Sentinel on Windows platform. For more information on supported platforms for Crystal Reports Server in a Sentinel environment, see [Chapter 2, “System Requirements,” on page 15](#).

On Windows, Sentinel has been tested with Crystal Reports Server XI R2 SP4. For more information on downloading the latest service packs, see [Section 7.6, “Downloading the Service Packs for Crystal Reports,” on page 108](#).

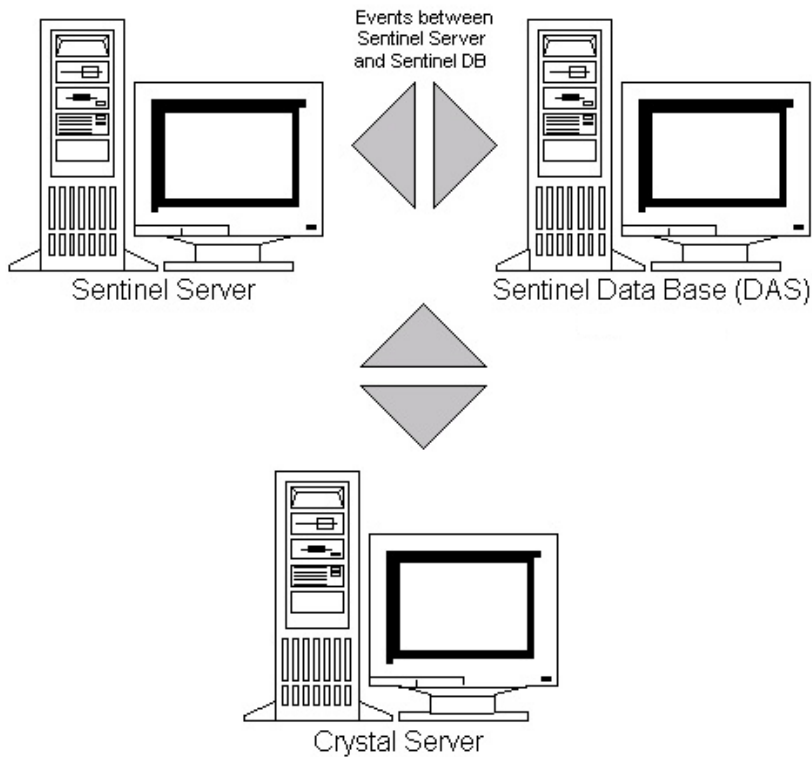
- ◆ [Section 7.1, “Overview,” on page 93](#)
- ◆ [Section 7.2, “System Requirements,” on page 94](#)
- ◆ [Section 7.3, “Configuration Requirements,” on page 95](#)
- ◆ [Section 7.4, “Installation Overview,” on page 95](#)
- ◆ [Section 7.5, “Installation,” on page 97](#)
- ◆ [Section 7.6, “Downloading the Service Packs for Crystal Reports,” on page 108](#)
- ◆ [Section 7.7, “Configuring Crystal Reports Server to Work with the Sentinel Control Center,” on page 108](#)
- ◆ [Section 7.8, “Publishing Crystal Report Templates,” on page 111](#)
- ◆ [Section 7.9, “High-Performance Configurations for Crystal,” on page 118](#)
- ◆ [Section 7.10, “Using Crystal Reports,” on page 120](#)
- ◆ [Section 7.11, “Uninstalling Crystal Reports,” on page 120](#)

For information on running Crystal Reports Server on Linux and Solaris, see [Chapter 8, “Crystal Reports for Linux,” on page 121](#).

## 7.1 Overview

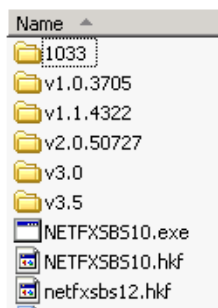
Crystal Reports Server uses Central Management Server (CMS) database to store information about the Crystal Reports Server system and its users. Other components of Crystal Reports Server can access this information as required.

You must set up the CMS database on top of a local SQL Server 2005 database for a Crystal installation on Windows. Although the Crystal Reports Server installer allows you to set up the CMS database on top of an MSDE database, this configuration is not tested or supported with Sentinel.



## 7.2 System Requirements

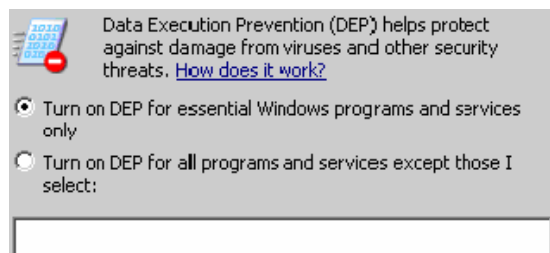
- Windows Server 2003 SP1 with an NTFS-formatted partition, with IIS (Microsoft Internet Information Server) and ASP.NET installed. Sentinel does not support Crystal XI R2 on Windows Server 2000.
- .NET Framework 1.1 or 2.0 is installed by default on Windows Server 2003. However, you can also install .NET Framework 3.5 manually. To determine which version of .NET Framework is on your machine, go to %SystemRoot%\Microsoft.NET\Framework. The version is listed as shown in the figure below:



For more information on supported platforms for Crystal Reports Server in a Sentinel environment, see [Chapter 2, “System Requirements,”](#) on page 15.

## 7.3 Configuration Requirements

- ◆ Ensure that a local administrator account is used to install Crystal Reports Server.
- ◆ Set Data Execution Prevention (DEP) to run on essential Windows programs and services only.
  1. Go to *Control Panel > System > Advanced tab > Performance Settings > Data Execution Prevention*.
  2. Select *Turn on DEP for essential Windows programs and services only*.

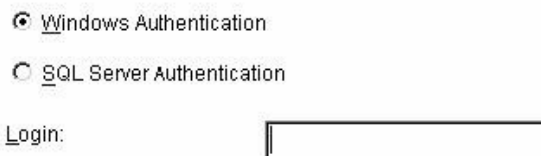


---

**NOTE:** This is required to avoid Error 1920. Service Crystal Report Cache Server on Windows Server 2003.

---

- ◆ Ensure that the Sentinel server and database is already installed.
- ◆ Ensure that you know the authentication mode that was chosen for the Sentinel Report User. If you are using the local database authentication, `escript` is the username. If you are using Windows authentication, the username can be anything of your choice. The authentication mode is set during the Sentinel installation process, as shown in the screen below. For more information on the Sentinel installation process, see [Chapter 3, “Installing Sentinel 6.1 SP2,” on page 27](#).



---

**NOTE:** The `escript` password can be explicitly set in Windows.

---

- ◆ Video resolution should be set to 1024 x 768 or higher.
- ◆ Ensure that Microsoft Internet Information Server (IIS) and ASP.NET are installed. For more information, see [Section 7.5.1, “Installing Microsoft Internet Information Server \(IIS\) and ASP.NET,” on page 98](#).

## 7.4 Installation Overview

- 1 Install Microsoft IIS and ASP.NET.
- 2 Install SQL (depending on whether you are using Windows authentication or SQL Server authentication).
- 3 Install Asian fonts (for example, Arial Unicode MS).

---

**NOTE:** This is required only for Chinese (traditional and simple) and Japanese users so they can view the reports in these languages.

---

- 4 Install Crystal Reports Server:
  - ♦ Configuring Open Database Connectivity (ODBC)
  - ♦ Installing and configuring Oracle Client Software
- 5 Configure inetmgr.
- 6 Patch Crystal Reports.
- 7 Publish (import) Crystal Reports.
- 8 Set a named user account.
- 9 Test the connectivity to the Web server.
- 10 Increase the Crystal Reports Server report refresh record limit (recommended)
- 11 Configure Sentinel Control Center to integrate with Crystal Reports Server.

This section includes the following topics:

- ♦ [Section 7.4.1, “Installation Overview of Crystal Reports Server with SQL Server 2005,” on page 96](#)
- ♦ [Section 7.4.2, “Installation Overview of Crystal Reports Server with Oracle,” on page 97](#)

For more information on installing Crystal Reports, see [Crystal Reports Server documentation \(http://help.sap.com/businessobject/product\\_guides/boexir2SP4/en/xir2\\_sp4\\_install\\_win\\_unix\\_en.pdf\)](http://help.sap.com/businessobject/product_guides/boexir2SP4/en/xir2_sp4_install_win_unix_en.pdf).

## 7.4.1 Installation Overview of Crystal Reports Server with SQL Server 2005

The following are the high-level steps for installing Crystal Reports Server with a SQL Server 2005 Sentinel database, using Windows authentication or SQL authentication.

- 1 Install Crystal Reports Server XI R2.
  - ♦ If you selected Windows Authentication for the Sentinel Report user when installing Sentinel, see [Section 7.5.2, “Installing Crystal Reports Server for SQL Server 2005 with Windows Authentication,” on page 98](#).
  - ♦ If you selected SQL Authentication for the Sentinel Report user when installing Sentinel, see [Section 7.5.3, “Installing Crystal Reports Server for SQL Server 2005 with SQL Authentication,” on page 102](#).
- 2 Configure Open Database Connectivity (ODBC). For more information, see [“Configuring Open Database Connectivity \(ODBC\)” on page 103](#).
- 3 Map Crystal Reports for use with Sentinel. For more information, see [Section 7.7, “Configuring Crystal Reports Server to Work with the Sentinel Control Center,” on page 108](#).
- 4 Patch Crystal Reports. For more information, see [Section 7.7.2, “Patching Crystal Reports,” on page 109](#).
- 5 Publish the reports. For more information, see [Section 7.8, “Publishing Crystal Report Templates,” on page 111](#).



- 6 Set the Named User Account. For more information on setting, see [Section 7.8.4, “Setting a Named User Account,”](#) on page 115.
- 7 Create a Crystal Web page. For more information, see [Section 7.8.5, “Configuring Report Permissions and Testing Connectivity,”](#) on page 115.
- 8 Configure Sentinel for Crystal Reports Server. For more information, see [Section 7.8.7, “Configuring the Sentinel Control Center to Integrate with Crystal Reports Server,”](#) on page 117.

## 7.4.2 Installation Overview of Crystal Reports Server with Oracle

The following are the high-level steps for installing Crystal Reports Server with an Oracle Sentinel database.

- 1 Install the Oracle client and configure the Oracle native driver. For more information, see [“Installing and Configuring Oracle Client Software”](#) on page 107.
- 2 Install Asian fonts (for example, Arial Unicode MS).  
This is required only for Chinese (traditional and simple) and Japanese users so they can view the reports in these languages.
- 3 Install Crystal Reports Server XI R2. For more information, see [Section 7.5.4, “Installing Crystal Reports Server for Oracle,”](#) on page 105.
- 4 Map Crystal Reports for use with Sentinel. For more information, see [Section 7.7, “Configuring Crystal Reports Server to Work with the Sentinel Control Center,”](#) on page 108
- 5 Import Crystal Reports templates. For more information, see [Section 7.8, “Publishing Crystal Report Templates,”](#) on page 111.
- 6 Create a Crystal Web page. For more information, see [Section 7.8.5, “Configuring Report Permissions and Testing Connectivity,”](#) on page 115.
- 7 Configure Sentinel for Crystal Reports Server. For more information, see [Section 7.7, “Configuring Crystal Reports Server to Work with the Sentinel Control Center,”](#) on page 108.

## 7.5 Installation

This topic provides the Crystal Reports Server installation instructions for the following:

- ♦ [Section 7.5.1, “Installing Microsoft Internet Information Server \(IIS\) and ASP.NET,”](#) on page 98
- ♦ [Section 7.5.2, “Installing Crystal Reports Server for SQL Server 2005 with Windows Authentication,”](#) on page 98
- ♦ [Section 7.5.3, “Installing Crystal Reports Server for SQL Server 2005 with SQL Authentication,”](#) on page 102
- ♦ [Section 7.5.4, “Installing Crystal Reports Server for Oracle,”](#) on page 105

## 7.5.1 Installing Microsoft Internet Information Server (IIS) and ASP.NET

If the IIS and ASP.NET are not installed on your Sentinel 6.1 server, use the following procedure to install. You might need the Windows Server 2003 installation CD to add these Windows components.

- 1 On the Windows desktop, go to *Control Panel > Add/Remove Programs*.
- 2 In the left pane, click *Add/Remove Windows Components*.
- 3 Select *Application Server*.



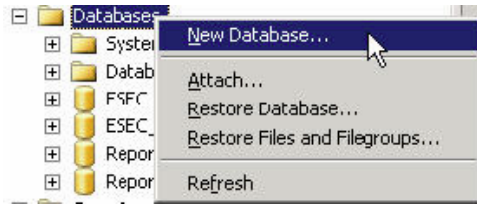
- 4 Click *Details*.
- 5 Select *ASP.NET* and *Internet Information Services (IIS)*.



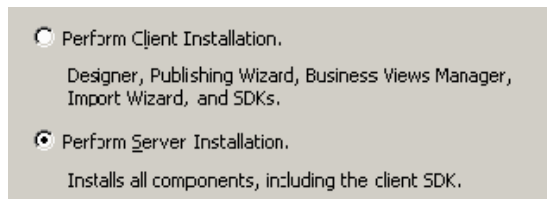
- 6 Click *OK*.
- 7 Click *Next*.
- 8 (Conditional) If you are prompted for the Windows Server 2003 installation CD, insert it into the CD drive.
- 9 Click *Finish*.
- 10 Continue with one of the following sections:
  - ♦ If you are using SQL Server 2005 with Windows authentication, see [Section 7.5.2, “Installing Crystal Reports Server for SQL Server 2005 with Windows Authentication,”](#) on page 98.
  - ♦ If you are using SQL Server 2005 with SQL authentication, see [Section 7.5.3, “Installing Crystal Reports Server for SQL Server 2005 with SQL Authentication,”](#) on page 102.
  - ♦ If you are using Oracle, see [Section 7.5.4, “Installing Crystal Reports Server for Oracle,”](#) on page 105.

## 7.5.2 Installing Crystal Reports Server for SQL Server 2005 with Windows Authentication

- 1 Install SQL Server 2005 in mixed mode.
- 2 Launch Microsoft SQL Server Management Studio.
- 3 In the navigation pane, expand *Databases*.
- 4 Right-click *Database*, then select *New Database* to create the Crystal CMS database.



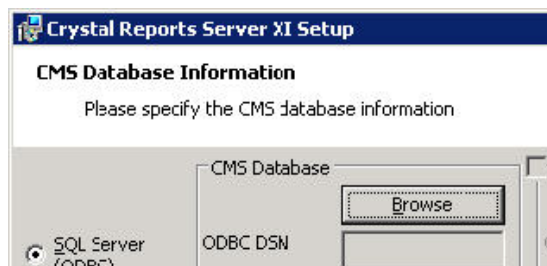
- 5 In the *Database name* field, specify BOE115 and click *OK*.
- 6 Exit Microsoft SQL Server Management Studio.
- 7 Insert the Crystal Reports XI R2 Server CD into the CD-ROM drive.
- 8 If Autoplay is enabled on your machine, the installation begins. Continue with [Step 9](#).  
or  
If Autoplay is disabled on your machine, run `setup.exe` and follow the prompts.
- 9 Select the Crystal Reports setup language.
- 10 In the Select Client or Server Installation window, select *Perform Server Installation*.



- 11 Specify the Crystal license key that you received from the [Novell Customer Center \(https://secure-www.novell.com/center/regadmin\)](https://secure-www.novell.com/center/regadmin).  
Novell provides two Crystal license keys, one for Crystal Reports Server and the other for the Crystal Reports Developer (to modify or create new reports). Ensure that you use the Crystal Reports Server key when installing Crystal Reports Server.
- 12 Specify a destination folder.
- 13 For the install type, select *Use an existing database server*.

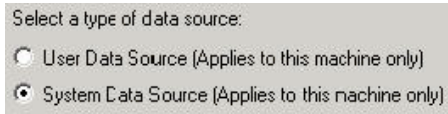


- 14 In the *CMS Database* pane, click *Browse*.



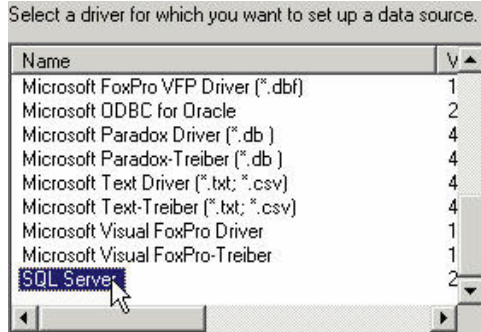
15 Click the *Machine Data Source* tab, then click *New*.

16 Select *System Data Source*, then click *Next*.

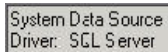


17 Scroll down and select *SQL Server*, then click *Next*.

A new source displays.

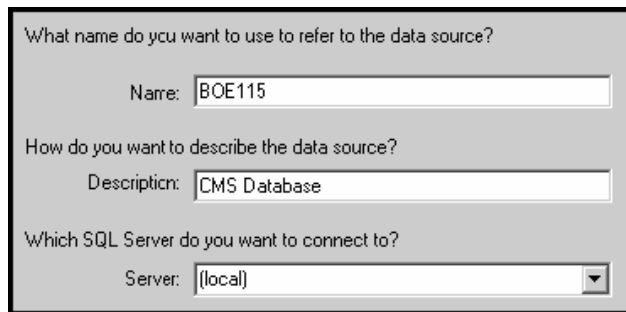


18 Click *Finish*.



19 Right-click *Databases*, then select *Create New Database*.

20 In the *New Data Source to SQL Server* window, specify the name of your data source (for example, BOE115) and an optional description.



21 For *Server*, click the down-arrow and select *(local)*, then click *Next*.

22 Ensure that *With Windows NT authentication using the network Login ID* is selected, then click *Next*.



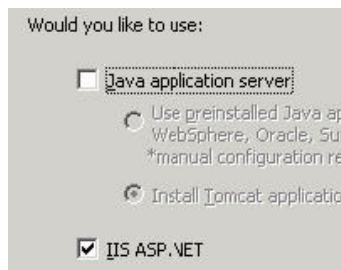
The Login ID that is displayed in this window is your Windows login name.

- 23** Select the *Change the default database to* check box. Change your default database to BOE115, then click *Next*.
- 24** In the *Create a New Data Source to SQL Server* window, click *Finish*.
- 25** Click *Test Data Source* and test the data source. After testing the data source, click *OK*.
- 26** In the *Select Data Source* window, select the new data source (BOE115) and follow the prompts until you get to the *SQL Server Login*. Ensure that *Use Trusted Connection* is selected, then click *OK*.

The Login ID that is displayed in this window is your Windows login name.

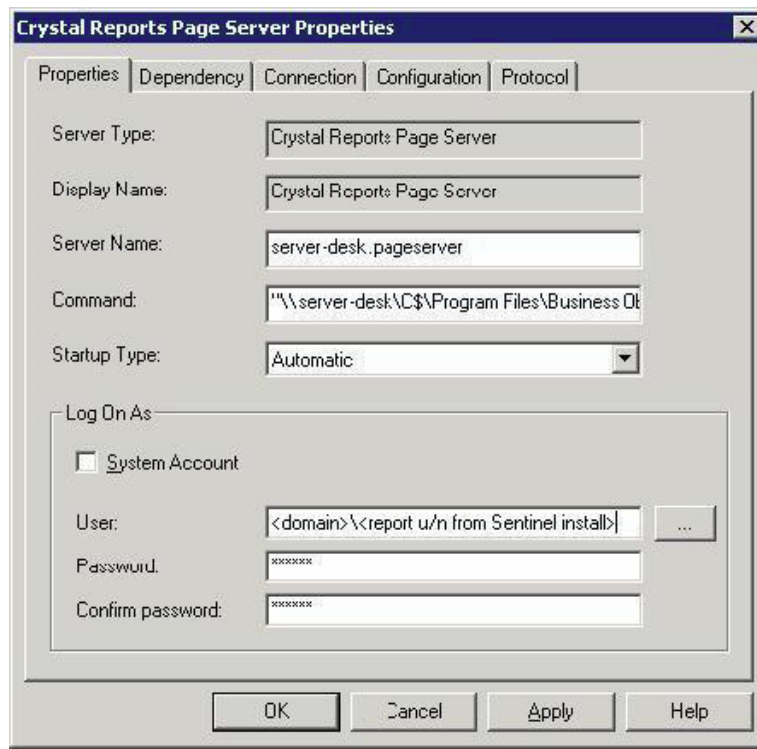
- 27** In the *Web Component Adapter Type* window, select *IIS ASP.NET*.

If you have not installed IIS and ASP.NET through *Control Panel > Add Remove Programs > Add/Remove Windows Components*, IIS ASP.NET is disabled.



- 28** After installation, change the login account for Crystal Reports Page Server and Crystal Reports Job Server to the Sentinel Report User domain account:
  - 28a** Click *Start > Programs > BusinessObjects > Crystal Reports Server > Central Configuration Manager*.
  - 28b** Right-click *Crystal Reports Page Server*, then select *stop*.
  - 28c** Right-click *Crystal Reports Page Server* again, then click *Properties*.

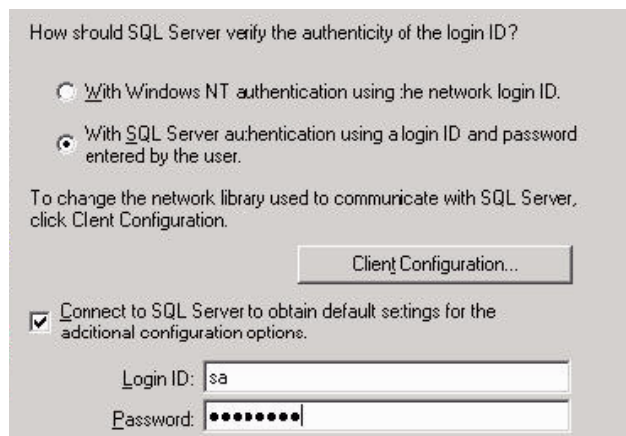
- 28d** In the *Log On As* pane, deselect the *System Account*, specify the Sentinel Report User domain account username and password that was used for the Sentinel Report User during your Sentinel install, then click *OK*.



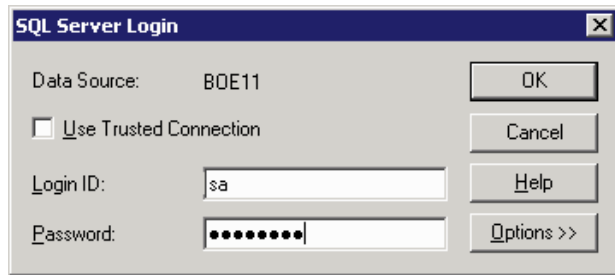
- 29** Right-click Crystal Reports Page Server, then click *start*.

### 7.5.3 Installing Crystal Reports Server for SQL Server 2005 with SQL Authentication

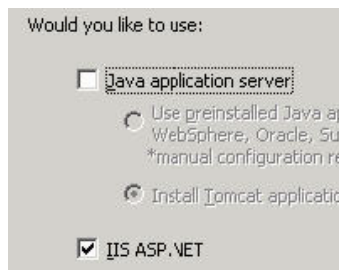
- 1 Complete [Step 1](#) through [Step 20](#) in [Section 7.5.2, "Installing Crystal Reports Server for SQL Server 2005 with Windows Authentication,"](#) on page 98.
- 2 When you are prompted for an authentication method, select *With SQL Server authentication*.



- 3 Specify the *Login ID* as *sa* and specify a password, then click *Next*.
- 4 Select *Change the default database to*. Change your default database to *BOE115*, then click *Next*.
- 5 In the *Create a New Data Source to SQL Server* window, click *Finish*.
- 6 Click *Test Data Source*, then click *OK*.
- 7 In the *Select Data Source* window, select *BOE115* and continue to click *OK* until you get to the *SQL Server Login* window.
- 8 Ensure that *Use Trusted Connection* is not selected. Click *OK*, then click *Next*.



- 9 In the *Web Component Adapter Type* window, select *IIS ASP.NET*.  
If you have not installed IIS and ASP.NET through *Control Panel > Add Remove Programs > Add/Remove Windows Components*, IIS ASP.NET is disabled.



## Configuring Open Database Connectivity (ODBC)

This procedure sets up an ODBC data source name to allow Crystal Reports Server to connect to the Sentinel database on Windows and SQL Server. These steps must be performed on the Crystal Reports Server machine.

- 1 On the Windows desktop, go to *Control Panel > Administrative Tools > Data Sources (ODBC)*.
- 2 Click *System DSN*, then click *Add*.
- 3 Select *SQL Server*, then click *Finish*.  
A window displays prompting for driver configuration information.
- 4 Specify the following information:
  - Data Source name:** The default data source name is *esecuritydb*
  - Description:** Description of the data source (optional)
  - Server:** Host-name or the IP address of the Sentinel server

Name:

How do you want to describe the data source?  
 Description:

Which SQL Server do you want to connect to?  
 Server:  ▼

5 Click *Next*.

6 Select how SQL Server should verify the authenticity of the login ID:

**For Windows NT Authentication:** Select *With Windows NT authentication using the network Login ID*

How should SQL Server verify the authenticity of the login ID?

With Windows NT authentication using the network login ID.

With SQL Server authentication using a login ID and password entered by the user.

To change the network library used to communicate with SQL Server, click Client Configuration.

Connect to SQL Server to obtain default settings for the additional configuration options.

Login ID:

Password:

The *Login ID* that is displayed in this window is your Windows login name.

**For SQL Authentication:** Select *With SQL Server authentication using a login ID and password entered by the user*, specify the *Login ID* as *esecrpt*, then provide a password.

How should SQL Server verify the authenticity of the login ID?

With Windows NT authentication using the network login ID.

With SQL Server authentication using a login ID and password entered by the user.

To change the network library used to communicate with SQL Server, click Client Configuration.

Connect to SQL Server to obtain default settings for the additional configuration options.

Login ID:

Password:

7 Click *Next*.

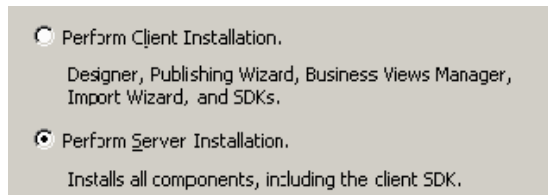
8 In the next window, select *Change the Sentinel database (Default name is ESEC)*, and leave all the other settings as the defaults.



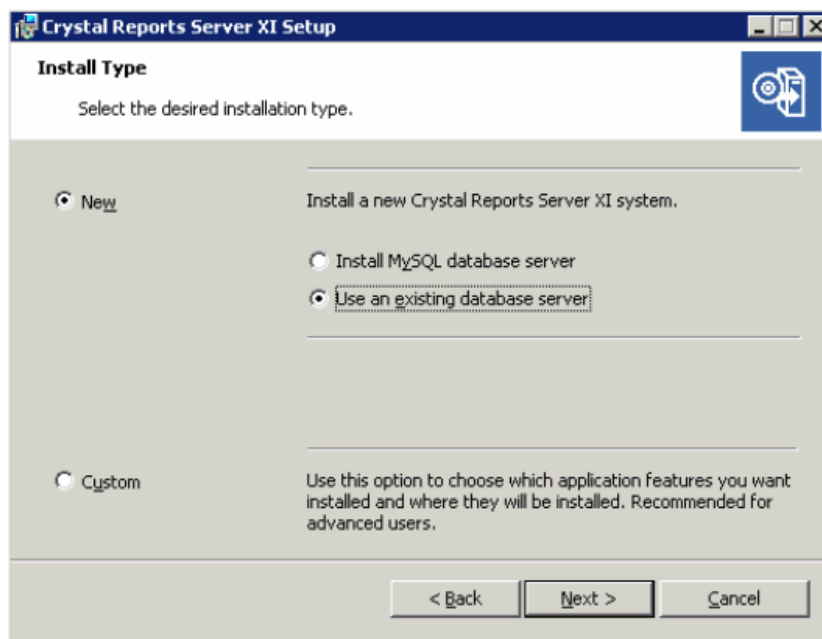
- 9 Click *Next*, then click *Finish*.
- 10 Click *Test Data Source*. After testing, click *OK* until you exit.

## 7.5.4 Installing Crystal Reports Server for Oracle

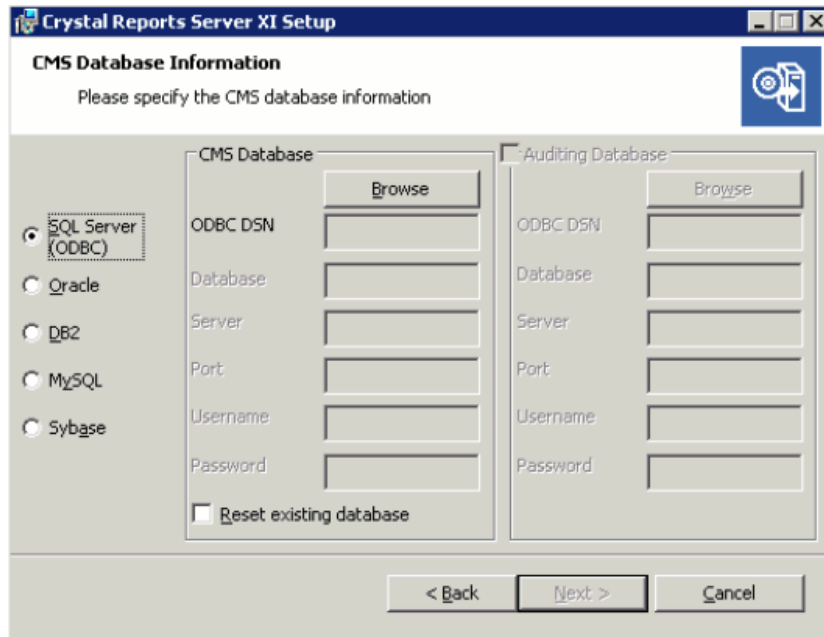
- 1 Insert the Crystal Reports XI R2 Server CD into the CD-ROM drive.
- 2 Select the Crystal Reports setup language.



- 3 In the Select Client or Server Installation window, select *Perform Server Installation*.



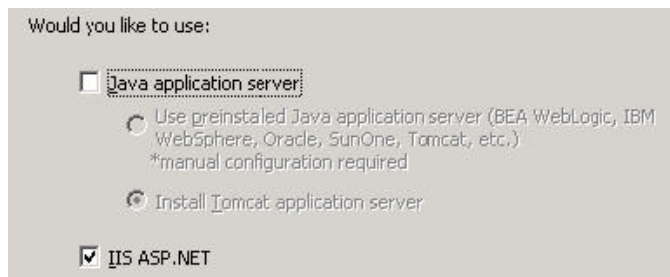
- 4 Select *Use an existing database server*.  
The CMS Database Information window displays.



- 5 Select *SQL Server (ODBC)*, then click *Browse* to select a DSN.
- 6 After you select a DSN, you are prompted for a username and password. Specify the required information and click *Next*.

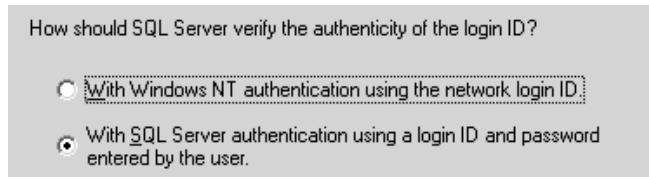
Crystal Reports Server and SQL Server 2005 must reside on the same machine.

- 7 Select *IIS ASP.NET*.



If you have not installed IIS and ASP.NET through *Control Panel > Add Remove Programs > Add/Remove Windows Components*, IIS ASP.NET is disabled. Installing IIS and ASP.NET is a prerequisite to this installation.

- 8 Select *SQL Server authentication*.



The Crystal Reports Server supports direct access to a Sentinel database on Oracle. This accessibility is provided by the `crdb_oracle.dll` translation file. This file communicates with the Oracle database driver, which works directly with Oracle databases and clients, retrieving the data you need for your report.

## Installing and Configuring Oracle Client Software

---

**NOTE:** In order for Crystal Reports Server to use Oracle databases, the Oracle client software must be installed on your system, and the location of the Oracle client must be in the `PATH` environment variable.

---

When installing Oracle Client, perform the following:

- ◆ Accept the default install location.
- ◆ Select *No* for Perform Typical Configuration.
- ◆ Select *No* for Directory Service.
- ◆ Select *Local*.
- ◆ Specify the TNS Service Name as `ESEC`.
- ◆ (Optional) Specify the Username (optional) as `esecrpt`.

After the installation, create a local Net Service Name configuration.

The following procedure is for the Oracle native driver, but the procedure should be similar for Oracle 10.

To create Net Service Name configuration for an Oracle native driver:

- 1 Select *Oracle-OraHome92 > Configuration and Migration Tools > Net Manager*.
- 2 In the navigation pane, expand *Local* and select *Service Naming*.
- 3 Click the plus sign on the left to add a Service Name.
- 4 In the Service Name window, specify the *Net Service Name* as `ESECURITYDB`, then click *Next*.
- 5 In the Select Protocols window, select *TCP/IP (Internet Protocol)*, then click *Next*.
- 6 Specify the hostname or IP address of the machine that has the Sentinel database.
- 7 Select the Oracle port (the default 1521 on install), then click *Next*.
- 8 Identify the Sentinel database or service:
  - 8a Select (Oracle8i or later), specify the *Service Name* (this is the Oracle instance name).
  - 8b For connection type, select *Database Default*.
  - 8c Click *Next*.
- 9 In the Test window, click *Test*, then click *Next*.

The test might fail because the test uses a database ID and password.

- 10 If the test fails:
  - 10a In the Connection Test window, click *Change Login*.
  - 10b Specify the *Sentinel Oracle ID* (use `esecrpt`) and password then click *Test*
- 11 If the test fails again:
  - 11a Ping the Sentinel Server.
  - 11b Verify that the hostname of the Sentinel Server is in the hosts file on Crystal Reports Server. The hosts file is located at `%SystemRoot%\system32\drivers\etc\`
- 12 Click *Close*, then click *Finish*.

## 7.6 Downloading the Service Packs for Crystal Reports

- 1 Go to the [Novell download Web site \(http://download.novell.com\)](http://download.novell.com).
- 2 In the Patches section, click *search patches*.
- 3 Select SIEM-Sentinel from the *Product* list.
- 4 Specify `crystal` as the keyword, then click *Search*.

A list of Sentinel patches that include the Sentinel Crystal XI R2 SP4 patch is displayed.
- 5 Click the appropriate Sentinel version installed on your system, then click *Sentinel Crystal XI R2 SP4*.
- 6 In the Sentinel Crystal XI R2 SP4 page, click *proceed to download*.
- 7 Refer to the `Crystal_Reports_patchinstallation.pdf` for installation instructions.

## 7.7 Configuring Crystal Reports Server to Work with the Sentinel Control Center

The following procedures are required for Crystal Reports Server to work with Sentinel Control Center:

- ♦ [Section 7.7.1, “Configuring inetmgr,” on page 108](#)
- ♦ [Section 7.7.2, “Patching Crystal Reports,” on page 109](#)

### 7.7.1 Configuring inetmgr

- 1 Copy the `web.config` file from `c:\Program Files\Business Objects\BusinessObjects Enterprise 11.5\Web Content` to `c:\Inetpub\wwwroot`
- 2 Launch the Internet Service Manager by clicking *Start > Run*.
- 3 Specify `inetmgr`, then click *OK*.
- 4 Expand (local computer) > *Web Sites > Default Web Site > businessobjects*.
- 5 Right-click *businessobjects*, then click *properties*.
- 6 In the *Virtual Directory* tab, click *Configuration*.
- 7 Ensure that you have the following mappings. If not, add them. If you are adding a mapping, do not click the *businessobjects* or *crystalreportsviewer11* nodes.

Extension	Executable
.csp	C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll
.cwr	C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll
.cri	C:\Windows\Microsoft.NET\Framework\v1.1.4322\aspnet_isapi.dll
.wis	...\BusinessObjects Enterprise 11.5

**8** Click *OK* to close the window.

**9** Restart IIS:

**9a** Expand (local computer) > *Web Sites* > *Default Web Site*.

**9b** Right-click *Default Web Site*, then click *Stop*.

**9c** Right-click *Default Web Site* again, then click *Start*.

---

**NOTE:** After Crystal Reports Server is installed, you must download and install the Sentinel Core Solution Pack, which includes both report templates and the necessary files to patch Crystal Reports. The installation instructions are provided in the Solution Pack documentation on the [Sentinel Content Web site](http://support.novell.com/products/sentinel/secure/sentinel61.html) (<http://support.novell.com/products/sentinel/secure/sentinel61.html>).

---

## 7.7.2 Patching Crystal Reports

To view Crystal Reports from the *Analysis* tab of the Sentinel Control Center and to publish the reports from Solution Manager, several Crystal Enterprise files need to be updated to make them compatible with the browser.

The following table lists the Crystal Reports Enterprise files and describes the purpose of each file. The Crystal Reports Enterprise files can be extracted from the *crystal\_patch.zip* file, which is available as an attachment in the Sentinel Core Solution Pack under the *Global Setup* control.

**Table 7-1** *Crystal Enterprise Files*

File name	Description
calendar.js	Displays a pop-up calendar when you select a date as a parameter to a report.
calendar.html	
grouptree.html	Displays a Loading message when the reports are loading.
exportframe.html	Displays a window that allows you to export a report for saving or for printing.
exportIce.html	File used by Sentinel when exporting a report for saving or for printing.
GetInfoStore.asp	File used to query the Crystal server.
GetReports.asp	File used by the Sentinel Control Center to establish a connection with Crystal Server and display the report list.
GetReportURL.asp	File used to support hyperlinks between reports.

File name	Description
helper_js.asp	A call file used by GetInfoStore.asp.
publish_report.aspx	Used to publish reports directly from a Solution Pack to the Crystal server when a control is installed.  This file is also included in the SP2 patch distribution.
delete_report.aspx	Used to remove reports directly from the Crystal server when a control is uninstalled.  This file is also included in the SP2 patch distribution.

To patch Crystal Reports:

**NOTE:** Ensure that you have read the Sentinel Reports Release Notes before performing this task, because there can be updated files, scripts, and additional steps that need to be completed.

- 1 Log in to Crystal Reports Server machine as a user who is a member of BusinessObjects NT Users group.
- 2 Extract the Crystal Enterprise files from the `crystal_patch.zip` file to a local directory.
- 3 In the patch directory of Sentinel Reports Distribution, copy the following files:
  - ♦ Copy all \*.html and \*.js files to the viewer file location. The default location is:  

```
C:\Program Files\Business Objects\BusinessObjects Enterprise 11.5\Web Content\Enterprise115\viewer\en
```
  - ♦ Copy all \*.asp and \*.js files to:  

```
C:\inetpub\wwwroot
```

Your Web folder might be on a different drive or location.
- 4 In the Crystal installation directory, create a subdirectory for Sentinel. In a default installation, the path is:  

```
C:\Program Files\BusinessObjects Enterprise 11.5\Web Content\Enterprise115\WebTools\Sentinel
```
- 5 Place the `publish_report.aspx` and `delete_report.aspx` files in the Sentinel directory.  
The `publish_report.aspx` and `delete_report.aspx` files are available in the `reports_patch\IIS` directory of the Sentinel 6 SP2 distribution or in the [Sentinel Reports distribution \(http://support.novell.com/products/sentinel/sentinel61.html\)](http://support.novell.com/products/sentinel/sentinel61.html).
- 6 Open the `web.config` file from the Crystal install directory.
- 7 Add two new entries to the `<assemblies>` section of the `web.config` file for `Enterprise.PluginManager` and `Enterprise.Desktop.Report`. The following example shows a sample `<assemblies>` section:

```
<assemblies>
<add assembly="CrystalDecisions.CrystalReports.Engine,
Version=11.5.3300.0, Culture=neutral, PublicKeyToken=123abcd1234a1234" />
<add assembly="CrystalDecisions.ReportSource, Version=11.5.3300.0,
Culture=neutral, PublicKeyToken=123abcd1234a1234" />
<add assembly="CrystalDecisions.Shared, Version=11.5.3300.0,
Culture=neutral, PublicKeyToken=123abcd1234a1234" />
<add assembly="CrystalDecisions.Web, Version=11.5.3300.0, Culture=neutral,
PublicKeyToken=123abcd1234a1234" />
```

```
<add assembly="CrystalDecisions.Enterprise, Version=11.5.3300.0,
Culture=neutral, PublicKeyToken=123abcd1234a1234" />
<add assembly="CrystalDecisions.Enterprise.Framework, Version=11.5.3300.0,
Culture=neutral, PublicKeyToken=123abcd1234a1234" />
<add assembly="CrystalDecisions.Enterprise.InfoStore, Version=11.5.3300.0,
Culture=neutral, PublicKeyToken=123abcd1234a1234" />
<add assembly="CrystalDecisions.Enterprise.Shared, Version=11.5.3300.0,
Culture=neutral, PublicKeyToken=123abcd1234a1234" />
<add assembly="CrystalDecisions.Enterprise.PluginManager,
Version=11.5.3300.0, Culture=neutral, PublicKeyToken=123abcd1234a1234" />
<add assembly="CrystalDecisions.Enterprise.Desktop.Report,
Version=11.5.3300.0, Culture=neutral, PublicKeyToken=123abcd1234a1234" />
</assemblies>
```

---

**IMPORTANT:** The new entries should use the same Version, Culture, and PublicKeyToken values as the other entries in your file.

---

- 8 Restart the Web server and the Crystal Reports server.

## 7.8 Publishing Crystal Report Templates

Many report templates have been created by Novell for use in the *Analysis* and *Advisor* tabs of the Sentinel Control Center. The most recent reports can be downloaded from the [Sentinel 6 content Web pages \(http://support.novell.com/products/sentinel/sentinel61.html\)](http://support.novell.com/products/sentinel/sentinel61.html).

The core set of Sentinel reports are distributed in the Sentinel Core Solution Pack.

Use any of the following methods to add reports to the system:

- ◆ Download a Solution Pack from the *Solution Packs* tab and use the Solution Manager to install one or more controls that include reports.
- ◆ Download a Collector Pack from the *Collectors* tab and use the Solution Manager to install one or more controls that include reports.
- ◆ Use the Crystal Publishing Wizard to add one or more report templates (.rpt files).
- ◆ Use the Crystal Reports Central Management Console to add one or more report templates (.rpt files).

---

**IMPORTANT:** To run any Top 10 reports, aggregation must be enabled and the `EventFileRedirectService` in the `DAS_Binary.xml` must be set to ON. This is already configured in a default Sentinel installation. For information on how to enable aggregation, see the “Report Data Configuration” section of “Admin” in the *Sentinel 6.1 User Guide*.

---

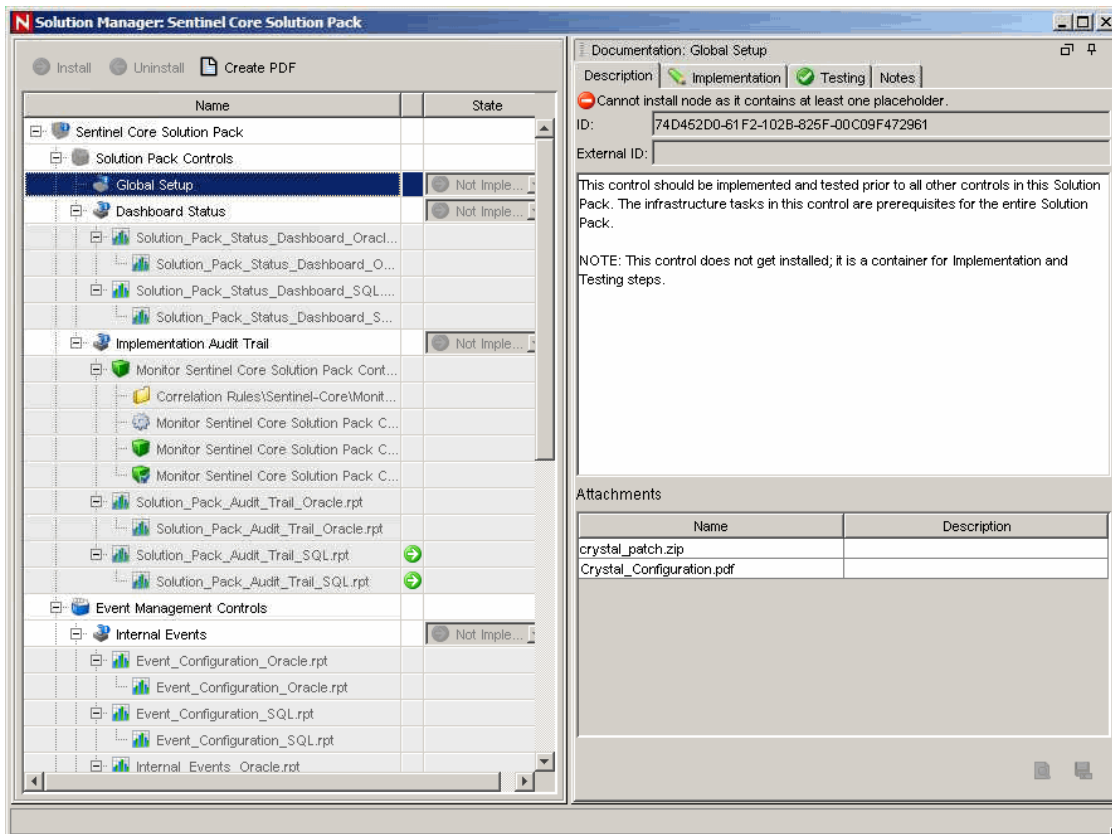
- ◆ [Section 7.8.1, “Using the Solution Manager to Publish Report Templates,” on page 112](#)
- ◆ [Section 7.8.2, “Using the Crystal Publishing Wizard to Publish Report Templates,” on page 112](#)
- ◆ [Section 7.8.3, “Using the Central Management Console to Publish Report Templates,” on page 114](#)
- ◆ [Section 7.8.4, “Setting a Named User Account,” on page 115](#)
- ◆ [Section 7.8.5, “Configuring Report Permissions and Testing Connectivity,” on page 115](#)
- ◆ [Section 7.8.6, “Disabling the Sentinel Top 10 Reports,” on page 116](#)
- ◆ [Section 7.8.7, “Configuring the Sentinel Control Center to Integrate with Crystal Reports Server,” on page 117](#)

## 7.8.1 Using the Solution Manager to Publish Report Templates

If the Web server and Crystal Reports Server are configured properly, you can use the Solution Manager to directly publish the reports included in a Solution Pack or Collector Pack to the Crystal Reports Server. To configure the system, you must download the Sentinel Core Solution Pack, available in the *Solution Packs* tab at *Sentinel 6.1 Content Web site* (<http://support.novell.com/products/sentinel/secure/sentinel61.html>).

The Sentinel Core Solution Pack includes auxiliary files that must be applied to both the Web server and the Crystal Reports server. These auxiliary files are available in the Solution Manager after you import the Core Solution Pack. When you select the Global Setup control, the auxiliary file attachments are available in the lower right corner of the screen.

**Figure 7-1** Core Solution Pack in Solution Manager Showing Crystal Auxiliary Files



## 7.8.2 Using the Crystal Publishing Wizard to Publish Report Templates

Sentinel reports are now distributed through Solution Packs, but the method in this section can be used to publish report templates that are from a source other than a Solution Pack.



---

**NOTE:** If you want to publish your report templates again, delete your previous import of the report templates.

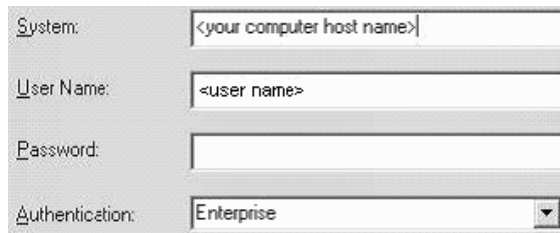
---

- 1 Click *Start > Programs > BusinessObjects > Crystal Reports Server > Publishing Wizard*, then click *Next* and log in.

*System* should be the hostname of the machine where Crystal is installed, and *Authentication* should be *Enterprise*. *User Name* can be *Administrator*.

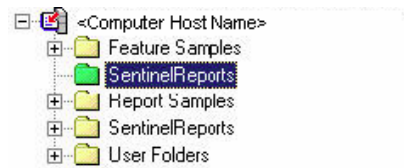
- 2 For security reasons, you should create a new user instead of using *Administrator*. Specify your password and click *Next*.

Publishing reports as an *Administrator* user allows all users to access the reports.

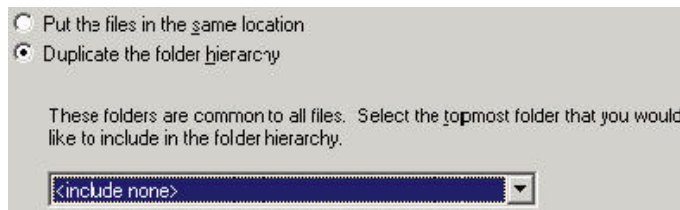


A screenshot of the Publishing Wizard login form. It contains four fields: 'System:' with a text box containing '<your computer host name>', 'User Name:' with a text box containing '<user name>', 'Password:' with an empty text box, and 'Authentication:' with a dropdown menu set to 'Enterprise'.

- 3 Click *Add Folder*.
- 4 (Optional) Select *Include Subfolders*.
- 5 Navigate to the location of the report templates. Click *OK*, then click *Next*.
- 6 In the Specify Location window, click *New Folder* at the upper right corner and create a folder called *SentinelReports* if it does not exist already. Click *Next*.



- 7 Select *Duplicate the folder hierarchy*, then click the down-arrow and select *<include none>*.



A screenshot of a dialog box for folder duplication. It has two radio buttons: 'Put the files in the same location' (unselected) and 'Duplicate the folder hierarchy' (selected). Below the radio buttons is a text box containing '<include none>'. A message reads: 'These folders are common to all files. Select the topmost folder that you would like to include in the folder hierarchy.'

- 8 Click *Next*.
- 9 In the Confirm Location window, click *Next*.
- 10 In the Specify Categories window, specify a category name (for example, *sentinel*), select the name, then click the + button.



**11** Click *Next*.

After you click *Next*, only the first report displays in the category.

**12** In the Specify Schedule window, ensure that *Let users update the object* is selected, then click *Next*.

**13** In the Specify Repository Refresh window, click *Enable All to enable repository refresh*, then click *Next*.

**14** In the Specify Keep Saved Data window, click *Enable All to keep saved data when publishing reports*, then click *Next*.

**15** In the Change Defaults Values window, ensure that *Publish reports without modifying properties* is selected, then click *Next*.

**16** Click *Next* to add your objects.

A published list displays.

**17** Click *Finish*.

When the Sentinel templates for Crystal Reports are published to Crystal Reports Server, the templates must reside within the `SentinelReports` directory, or they are not displayed in the Sentinel Control Center.

### 7.8.3 Using the Central Management Console to Publish Report Templates

Sentinel reports are now distributed through Solution Packs, but the method in this section can be used to publish report templates that are from a source other than a Solution Pack.

**1** Open a Web browser and provide the following URL:

```
http://<hostname_or_IP_of_web_server>/businessobjects/enterprise115/  
WebTools/adminlaunch
```

**2** Click *Central Management Console*.

**3** Log in to your Crystal Reports Server.

**4** In the *Organize* pane, click *Folders*.

**5** On the upper right corner, click *New Folder*.

**6** Create a `SentinelReports` folder (if it does not exist already), then click *OK*.

Ensure that the folder name is `SentinelReports`.

**7** Click *SentinelReports*.

**8** Click *Subfolders* and create subfolders if required. If you are manually adding the Sentinel core reports, create the following subfolders:

- ◆ `Advisor_Vulnerability`
- ◆ `Dashboards`
- ◆ `Incident Management`

- ♦ Internal Events
  - ♦ Security Events
  - ♦ Top 10
- 9 Click *Home > Objects > New Object*.
  - 10 On left side of the page, select *Report*.
  - 11 Click *Browse* and browse to the location of the report templates you want to add. Pick a folder and select a report.
  - 12 Select *SentinelReports*, then click *Show Subfolders*.
  - 13 Select the appropriate folder for the report, then click *Show Subfolders*.
  - 14 Click *Submit*.
  - 15 To add the remaining reports, repeat [Step 9](#) through [Step 14](#) until all reports have been added.

## 7.8.4 Setting a Named User Account

The license key supplied with Crystal Reports Server is a Named User account key. The Guest account must be changed from Concurrent User to Named User.

- 1 On the Windows desktop, click *Start > Programs > BusinessObjects > Crystal Reports Server > .NET Administration Launchpad*.
- 2 Click *Central Management Console*.  
The *System Name* should be your host computer name. The *Authentication Type* should be Enterprise.
- 3 Specify *Administrator* as the User Name. Specify your password (by default, this is blank).
- 4 Click *Log On*. In the *Organize* pane, click *Users*.
- 5 Click *Guest*.
- 6 Change the connection type from *Concurrent User* to *Named User*.

---

**IMPORTANT:** You should use the Named User License account to generate unlimited reports.

---

- 7 Click *Update*.

## 7.8.5 Configuring Report Permissions and Testing Connectivity

- ♦ [“Configuring Permissions” on page 115](#)
- ♦ [“Testing the Web Server Connection to the Sentinel Database” on page 116](#)
- ♦ [“Testing Connectivity to the Web Server” on page 116](#)

### Configuring Permissions

You use the .NET Administration Launchpad to configure the permissions to allow you to view and modify reports on demand.

- 1 On the Windows desktop, click *Start > Programs > BusinessObjects > Crystal Reports Server > .NET Administration Launchpad*.

If you see an HTTP 404- File or Directory not found error when you launch the .NET Administration Launchpad, see <http://support.microsoft.com/kb/315122> for resolution (<http://support.microsoft.com/kb/315122> for resolution).

**2** Click *Central Management Console*.

The *System Name* should be your host computer name. The *Authentication Type* should be Enterprise.

**3** Specify Administrator as the User Name. Specify your password (by default, this is blank).

**4** Click *Log On*. In the *Organize* pane, click *Folders*.

**5** Click *SentinelReports*, then select *All*.

**6** Click *Rights*.

**7** From *Access Level*, select *View on Demand*.

**8** Click *Update*.

### Testing the Web Server Connection to the Sentinel Database

**1** On your Windows desktop, click *Start > Programs > BusinessObjects > Crystal Reports Server > .NET Administration Launchpad*.

**2** Click *Central Management Console*.

**3** Specify Administrator as the User Name. Specify your password (by default, this is blank).

**4** Click *Log On*.

**5** Navigate to *Folders > SentinelReports > Internal Events*.

**6** Select *Column Display Details*, then click *Preview*.

**7** Depending on your system, login as esecrpt or as the Sentinel Report User.

**8** From the *Sort field* drop-down menu, select *Tag*.

**9** Click *OK* to display a report.

### Testing Connectivity to the Web Server

**1** Go to another machine that is on the same network as your Web server.

**2** Open a Web browser and provide the following URL:

```
http://<hostname_or_IP_of_web_server>/businessobjects/enterprise115/  
WebTools/adminlaunch/default.aspx
```

You should see a Crystal BusinessObjects Web page.

## 7.8.6 Disabling the Sentinel Top 10 Reports

By default, the Sentinel Top 10 Reports are enabled. If you do not want to use these reports, you can reduce database storage and CPU usage by disabling them.

To disable the Sentinel Top 10 Reports, you must turn off aggregation and disable EventFileRedirectService.

- ♦ “Turning Off Aggregation” on page 117
- ♦ “Disabling EventFileRedirectService” on page 117

## Turning Off Aggregation

- 1 Log in to Sentinel Control Center.
- 2 Click *Admin*, then click *Reporting Data*.
- 3 Disable the following summaries:
  - ◆ EventDestSummary
  - ◆ EventSevSummary
  - ◆ EventSrcSummary
- 4 In the *Status* column, click *Active* until it changes to *InActive*.

Summary Name	Time	Attributes	Source	Status
EventDestSummary	← 1 hour	CUST_ID.RSRC_IC...	TransformedEvent	→ Active
EventSevDestTxnmy...	1 hour	CUST_ID.DEST_EV...	TransformedEvent	InActive
EventSevDestEvtSu...	1 hour	CUST_ID.DEST_EV...	TransformedEvent	InActive
EventSevDestPortSu...	1 hour	SEV_DEST_PORT.C...	TransformedEvent	InActive
EventSevSummary	← 1 hour	CUST_ID.SEV.EVT...	TransformedEvent	→ Active
EventSrcSummary	← 1 hour	CUST_ID.RSRC_IC...	TransformedEvent	→ Active

## Disabling EventFileRedirectService

- 1 At your DAS machine, using the text editor, open the following file:  
**For UNIX:**  
`$/SEC_HOME/config/das_binary.xml`  
**For Windows:**  
`%SEC_HOME%\config\das_binary.xml`
- 2 For EventFileRedirectService, change the status to off:  
`<property name="status">off</property>`
- 3 Restart the DAS component:  
**On Windows:** Use the Service Manager to stop and start the Sentinel service

## 7.8.7 Configuring the Sentinel Control Center to Integrate with Crystal Reports Server

You can view Crystal Reports from Sentinel Control Center by integrating Crystal Reports Server to the Sentinel Control Center

To enable Sentinel Control Center integration with Crystal Reports Server, perform the following instructions:

---

**NOTE:** This configuration must be performed only after Crystal Reports Server has been installed and Crystal Reports have been published to it.

---

- 1 Log in to Sentinel Control Center as a user who has privileges to access the *Admin* tab.
- 2 In the *Admin* tab, select *Crystal Report Configuration*.
- 3 In the *Analysis URL* field, provide the following:  
`http://<hostname_or_IP_of_web_server>/GetReports.asp?APS=<hostname>&user=Guest&password=&tab=Analysis`

<hostname\_or\_IP\_of\_web\_server> must be replaced with the IP address or hostname of Crystal Reports Server. The URL does not work as expected if the Automated Process Scheduler (APS) is set to the IP address. It must be the host name of Crystal Reports Server.

4 Click *Refresh*, which is next to the *Analysis URL* field.

5 If you have Advisor installed, provide the following in the *Advisor URL* field:

```
http://<hostname_or_IP_of_web_server>/  
GetReports.asp?APS=<hostname>&user=Guest&password=&tab=Advisor
```

<hostname\_or\_IP\_of\_web\_server> must be replaced with the IP address or hostname of Crystal Reports Server. The URL above does not work as expected if the APS is set to the IP address. It must be the host name of Crystal Reports Server.

6 Click *Refresh*, which is next to the *Advisor URL* field, then click *Save*.

7 Log out and log in to the Sentinel Control Center. The Crystal Report trees in the *Analysis* tab and *Advisor* tab (if Advisor is installed) are displayed in the Navigator window.

## 7.9 High-Performance Configurations for Crystal

- ♦ [Section 7.9.1, “Increasing the Report Refresh Record Limit for Crystal Reports Server,” on page 118](#)
- ♦ [Section 7.9.2, “Using the Aggregation Service for Reports,” on page 119](#)
- ♦ [Section 7.9.3, “Report Development,” on page 120](#)

### 7.9.1 Increasing the Report Refresh Record Limit for Crystal Reports Server

Depending on the number of events that Crystal Reports is querying, you might get an error on the maximum processing time or maximum record limit. To set your server to process a higher number or an unlimited number of records, you must reconfigure the Crystal Page Server by using either the Central Configuration Manager or the Crystal Web Page.

- ♦ [“Using the Central Configuration Manager to reconfigure the Crystal Page Server” on page 118](#)
- ♦ [“Using the Central Management Console to reconfigure the Crystal Page Server” on page 118](#)

#### Using the Central Configuration Manager to reconfigure the Crystal Page Server

1 Click *Start > All Programs > BusinessObjects 11 > Crystal Reports Server > Central Configuration Manager*.

2 Right-click *Crystal Reports Page Server*, then select *Stop*.

3 Right-click *Crystal Reports Page Server*, then select *properties*.

4 In the *Command* field in the *Properties* tab, at the end of the command line add:

```
maxDBResultRecords <value greater than 20000 or 0 to disable the default  
limit>
```

5 Restart the Crystal Page Server.

#### Using the Central Management Console to reconfigure the Crystal Page Server

1 Click *Start > All Programs > BusinessObjects 11 > Crystal Reports Server > .Net Administration Launchpad*. Alternatively, open a Web browser and provide the following URL:

http://<hostname\_or\_IP\_of\_web\_server>/businessobjects/enterprise115/  
WebTools/adminlaunch/default.aspx

- 2 Click *Central Management Console*.
- 3 The *System Name* should be your host computer name. The *Authentication Type* should be Enterprise. If not, select Enterprise.
- 4 Specify your username and password, then click *Log On*. Click *Servers*.
- 5 Click <server name>.pageserver.
- 6 In Database Records to Read When previewing or Refreshing a report, select *Unlimited records*. Click *Apply*.  
A prompt to restart the page server displays
- 7 Click *OK*.  
You might be prompted for a login name and password to access the operating system service manager.

## 7.9.2 Using the Aggregation Service for Reports

To improve performance, the Top 10 reports that are included in the Sentinel Core Solution Pack query the summary tables instead of the events table. The summary tables contain counts over time for combinations of fields in the event data. This provides a much smaller data set for certain types of queries and results in much faster queries and report run time.

The Aggregation service is responsible for populating the summary tables with summarizations of all of the events in the events table. The Aggregation service only generates summarized data for summaries that are active. The following summaries are required by the Top 10 reports and are enabled by default:

- ♦ EventDestSummary
- ♦ EventSevSummary
- ♦ EventSrcSummary

Summaries can be activated or disabled by using the Reporting Data configuration window in the *Admin* tab of Sentinel Control Center.

The Aggregation service also depends on the `EventFileRedirectService` component in the DAS Binary to feed the event data that it summarizes. Therefore, this component must be enabled in order for the Aggregation service to run properly. This component is enabled or disabled by modifying the `status` attribute of the `EventFileRedirectService` component in the `das_binary.xml` file to ON or OFF. By default, this component is ON.

For more information about `EventFileRedirectService` and the three aggregation summaries, see “Report Data Configuration” in Admin in the *Sentinel 6.1 User Guide*.

---

**NOTE:** Reports that query a large date range might take sometime to run. They can be scheduled instead of running interactively. For information about scheduling Crystal Reports, see [Crystal BusinessObjects Enterprise 11 documentation \(http://www.sap.com/search/index.epx?q1=SCHEDULING+CRYSTAL+REPORT&num=10\)](http://www.sap.com/search/index.epx?q1=SCHEDULING+CRYSTAL+REPORT&num=10) and click the CRYSTAL REPORTS SERVER.pdf.

The above mentioned URL was current at the time of publication of the document.

---

### 7.9.3 Report Development

The Crystal Reports Developer can be used to create or modify Crystal reports. For custom developed reports, the following is recommended:

- ♦ If the reports can utilize predefined aggregate tables, select the aggregate table that results in processing of the least amount of data.
- ♦ Try to move most of the data processing to the database engine.
- ♦ To reduce processing overhead on the Crystal server, minimize the amount of data to retrieve to the Crystal server.
- ♦ Always write reports against the database views provided by Novell, instead of writing reports against the base tables.

## 7.10 Using Crystal Reports

For more information on using Crystal Reports Server for Sentinel Reporting, see “[Crystal Report Configuration](#)” in the *Sentinel 6.1 User Guide*.

## 7.11 Uninstalling Crystal Reports

- 1 On the Windows desktop, go to *Start > Control Panel > Add/Remove Programs*.
- 2 Select Crystal Reports, then click *Remove*.



# Crystal Reports for Linux

# 8

Business Objects Crystal Reports Server is the reporting tool used with Sentinel. This section discusses the installation and configuration of Crystal Reports Server for Sentinel on Linux platform. For more information on supported platforms for Crystal Reports Server in a Sentinel environment, see [Chapter 2, “System Requirements,” on page 15](#).

On Linux, Sentinel has been tested with Crystal Reports Server XI R2 SP4. For more information on downloading the latest service packs, see [Section 8.3, “Downloading the Service Packs for Crystal Reports,” on page 127](#).

- ◆ [Section 8.1, “Overview,” on page 122](#)
- ◆ [Section 8.2, “Installation,” on page 122](#)
- ◆ [Section 8.3, “Downloading the Service Packs for Crystal Reports,” on page 127](#)
- ◆ [Section 8.4, “Publishing Crystal Reports Templates,” on page 127](#)
- ◆ [Section 8.5, “Using the Crystal XI R2 Web Server,” on page 132](#)
- ◆ [Section 8.6, “Increasing Crystal Reports Server Report Refresh Record Limit,” on page 133](#)
- ◆ [Section 8.7, “Configuring Sentinel Control Center to Integrate with Crystal Reports Server,” on page 134](#)
- ◆ [Section 8.8, “Utilities and Troubleshooting,” on page 135](#)
- ◆ [Section 8.9, “High-Performance Configurations for Crystal,” on page 136](#)
- ◆ [Section 8.10, “Using Crystal Reports,” on page 138](#)

This section discusses running Crystal Reports Server on Linux. For more information on running Crystal Reports Server on Windows, see [Chapter 7, “Crystal Reports for Windows,” on page 93](#).

---

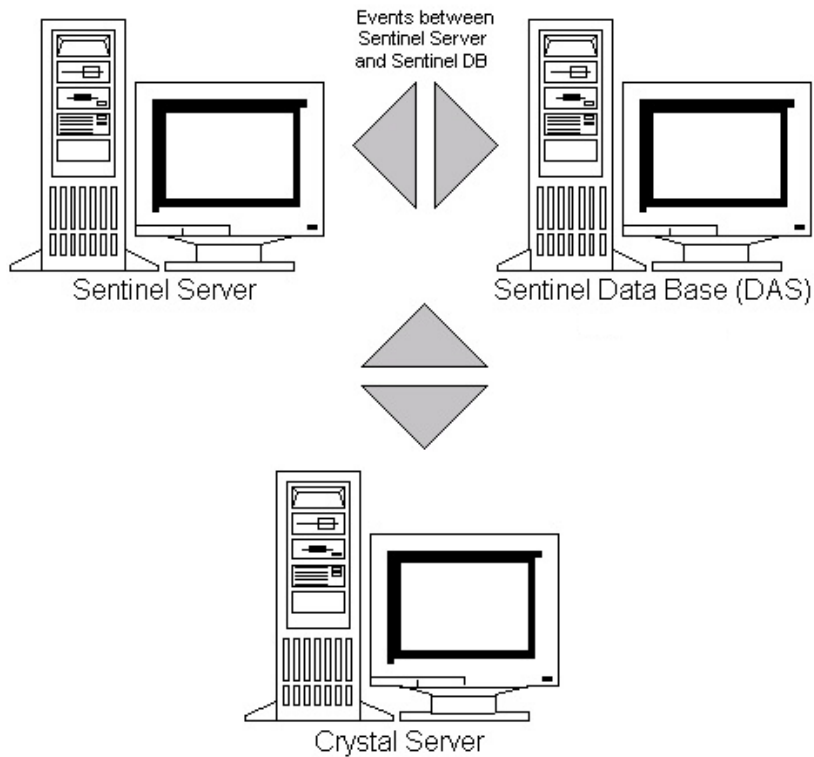
**IMPORTANT:** The installation should be done in the order presented below.

---

## **Installing the Crystal Reports Server involves the following:**

- 1** Installing the Crystal Reports Server XI R2
- 2** Patching the Crystal Reports Server
- 3** Publishing (importing) Crystal reports
- 4** Setting a “Named User” account
- 5** Testing connectivity to the Web Server
- 6** Enabling Top 10 reports (optional)
- 7** Increasing Crystal Reports Server Report Refresh Record Limit (recommended)

## 8 Configuring Sentinel Control Center to Integrate with Crystal Reports Server



### 8.1 Overview

Crystal Report Server requires a database to store information about the system and its users. This database is known as the Central Management Server (CMS) database. The CMS is a server that stores information about the Crystal Reports Server system. Other components of Crystal Reports Server can access this information as required.

### 8.2 Installation

The following procedures must be followed for Crystal Reports Server to work with the Sentinel Control Center:

- ◆ [Section 8.2.1, “Pre-Install Crystal Reports Server XI R2,” on page 122](#)
- ◆ [Section 8.2.2, “Installing Crystal Reports Server XIR2,” on page 124](#)
- ◆ [Section 8.2.3, “Patching Crystal Reports,” on page 126](#)

#### 8.2.1 Pre-Install Crystal Reports Server XI R2

- 1 If the Sentinel Database is not on the same machine as the Crystal Reports Server, then you must install the Oracle Client software on the Crystal Reports Server machine. This additional step is not needed if the Sentinel Database is on the same machine as the Crystal Reports Server because in this case the required Oracle software is already installed during the Oracle database installation.

**2** Login to the Crystal Reports Server machine as the root user

**3** Create bobje group

```
groupadd bobje
```

**4** Create Crystal user (the home directory in this example is /export/home/crystal, change if needed; the /export/home part of the path must already exist).

```
useradd -g bobje -s /bin/bash -d /export/home/crystal -m crystal
```

**5** Create directory for Crystal Software:

```
mkdir -p /opt/crystal_xir2
```

**6** Change the ownership of the Crystal Software directory (recursively) to crystal/bobje:

```
chown -R crystal:bobje /opt/crystal_xir2
```

**7** You must grant permissions to the crystal user on the \$ORACLE\_HOME directory using an Access Control List (ACL). Assuming the crystal user is crystal and \$ORACLE\_HOME is /opt/oracle/product/10.2/db\_1, the command to perform this is:

```
setfacl -m u:crystal:rx -R /opt/oracle/product/10.2/db_1
```

To verify that the ACL was set correctly, run the following command and check for “crystal” in the output:

```
getfacl /opt/oracle/product/10.2/db_1
```

**8** Add the crystal user to the oracle group using the following command:

```
groupmod -A crystal oinstall
```

This enables the crystal user to communicate with the Oracle database and execute Oracle utilities like sqlplus and tnsping.

**9** Change to the crystal user:

```
su - crystal
```

**10** The ORACLE\_HOME environment variable must be set in the crystal user’s environment. To do this, modify the crystal user’s login script to set the ORACLE\_HOME environment variable to the base of the Oracle software. For example, if the crystal user’s shell is bash and the Oracle software is installed in the directory /opt/oracle/product/10.2/db\_1, then open the file ~crystal/.bash\_profile (.profile on SLES) and add the following line to the end of the file:

```
export ORACLE_HOME=/opt/oracle/product/10.2/db_1
```

**11** The LD\_LIBRARY\_PATH environment variable in the crystal user’s environment must contain the path to the Oracle software libraries. To do this, modify the crystal user’s login script to set the LD\_LIBRARY\_PATH environment variable to include the Oracle software libraries. For example, if the crystal user’s shell is bash, then open the file ~crystal/.bash\_profile and add the following line to the end of the file (below where the ORACLE\_HOME environment variable is set):

```
export LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH
```

**12** The PATH environment variable in the crystal user’s environment must contain the path to the Oracle software executables. To do this modify the crystal user’s script to set the PATH environment variable to include the Oracle software executables. For example if the crystal user’s shell is bash, then open the file ~crystal/.bash\_profile and add the following line to the end of the file.

```
export PATH=$PATH:$ORACLE_HOME/bin
```

**13** An entry must be added to the Oracle `tnsnames.ora` file with the Service Name `esecuritydb` that points to the Sentinel Database. To do this on the Crystal Reports Server machine:

**13a** Log in as the oracle user.

**13b** Change directories to `$ORACLE_HOME/network/admin`

**13c** Make a backup of the file `tnsnames.ora`.

**13d** Open the file `tnsnames.ora` for editing.

**13e** If the Sentinel Database is on the Crystal Reports Server machine, then there should already be an entry in the `tnsnames.ora` file to the Sentinel Database. For example, if the Sentinel Database is named `ESEC`, then an entry similar to the following will exist:

```
ESEC =
(DESCRIPTION =
  (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = TCP)(HOST = dev-linux02)(PORT = 1521))
  )
  (CONNECT_DATA =
    (SID = ESEC)
  )
)
```

**13f** If the Sentinel Database is not on the Crystal Reports Server machine, open the `tnsnames.ora` file on the Sentinel Database machine to find the entry described above.

**13g** Make a copy of that entire entry and paste it at the bottom of the `tnsnames.ora` file on the Crystal Reports Server machine. The Service Name part of the entry must be renamed to `esecuritydb`. For example, when the entry above is copied and renamed properly, it will look like:

```
esecuritydb =
(DESCRIPTION =
  (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = TCP)(HOST = dev-linux02)(PORT = 1521))
  )
  (CONNECT_DATA =
    (SID = ESEC)
  )
)
```

**13h** Make sure the `HOST` part of the entry is correct (for example, make sure it is not set to `localhost` if the Crystal Reports Server and Sentinel Database are on different machines).

**13i** Save the changes to the `tnsnames.ora` file.

**13j** Execute the following command to check that the `esecuritydb` Service Name is configured properly:

```
tnsping esecuritydb
```

**13k** After the command is executed, you will get a message saying the connection is OK.

## 8.2.2 Installing Crystal Reports Server XIR2

The Crystal Reports Server installer consists of two `.iso` files. During the installation, you will be prompted for the location of the second disk.

### To Install Crystal Reports Server:

**1** Log in as crystal user.

- 2** Change directories into disk1 of the Crystal installer.
- 3** Execute:  
`./install.sh`
- 4** Select Language: English
- 5** Select New Installation.
- 6** Read and accept License Agreement.
- 7** Provide Product Keycode.
- 8** Provide install directory:  
`/opt/crystal_xir2`
- 9** Select: User install.
- 10** Select: New Install.
- 11** Select: Install MySQL unless you plan to install the Crystal CMS database into an existing database.
- 12** Specify configuration information for MySQL:
  - 12a** Use default port 3306
  - 12b** Admin password
- 13** Specify more configuration information for MySQL:
  - 13a** Default DB Name: BOE115
  - 13b** User id: mysqladm
  - 13c** Password
- 14** Specify more configuration information for MySQL:
  - 14a** Local Name Server: <local machine's hostname>
  - 14b** Default CMS Port Number: 6400
- 15** Select: Install Tomcat
- 16** Specify Tomcat configuration information:
  - 16a** Default Receive HTTP requests port: 8080
  - 16b** Default Redirect jsp requests port: 8443
  - 16c** Default Shutdown Hook port: 8005
- 17** Press Enter to confirm the default directory.
- 18** Press Enter to start installation.
- 19** Note the link to the CMS server, which will probably be something similar to this:  
`http://<hostname>:8080/businessobjects/enterprise115/adminlaunch/launchpad.html`

---

**NOTE:** After Crystal Reports Server is installed, you must download and install the Sentinel Core Solution Pack, the Sentinel Core Solution Pack includes both report templates and files necessary to patch Crystal. The installation instructions are included in the Solution Pack documentation on the [Sentinel Content Web site \(http://support.novell.com/products/sentinel/secure/sentinel61.html\)](http://support.novell.com/products/sentinel/secure/sentinel61.html).

---

## 8.2.3 Patching Crystal Reports

To view Crystal Reports from the *Analysis* tab of the Sentinel Control Center and to publish the reports from Solution Manager, several Crystal Enterprise files need to be updated to make them compatible with the browser.

The following table lists the Crystal Reports Enterprise files and describes the purpose of each file. The Crystal Reports Enterprise files can be extracted from the `crystal_patch.zip` file, which is available as an attachment in the Sentinel Core Solution Pack under the *Global Setup* control.

**Table 8-1** Crystal Enterprise Files

File name	Description
<code>calendar.js</code>	Displays a pop-up calendar when you are selecting a date as a parameter to a report.
<code>calendar.html</code>	
<code>groupTree.html</code>	Displays the Loading... message when the reports are loading.
<code>exportframe.html</code>	Displays the window that allows you to export a report for saving or for printing.
<code>exportIce.html</code>	File used by Sentinel when exporting a report for saving or for printing.
<code>GetReports.jsp</code>	File used by Sentinel Control Center to establish a connection with Crystal Server and display the report list.
<code>GetReportURL.jsp</code>	File used to support hyperlinks between reports.
<code>publish_report.jsp</code>	Used to publish reports directly from a Solution Pack to the Crystal server when a control is installed.  This file is also included in the SP2 patch distribution.
<code>delete_report.jsp</code>	Used to remove reports directly from the Crystal server when a control is uninstalled.  This file is also included in the SP2 patch distribution.

To patch crystal reports server:

**NOTE:** Ensure that you have read the Sentinel Reports Release Notes before performing this task as there can be updated files, scripts, and additional steps that need to be completed.

- 1 Log in to the Crystal Reports Server machine as `crystal` user.
- 2 Extract the Crystal Enterprise files from the `crystal_patch.zip` file to a local directory.
- 3 Create the directory structure `esec-script/WEB-INF/lib` at the following location:  
`/opt/crystal_xir2/bobje/tomcat/webapps/`
- 4 In the patch directory under Sentinel Reports Distribution, copy all `*.html` and `*.js` files to the viewer file location, the default location is:
  - ♦ Copy all `*.html` and `*.js` files to the viewer file location, the default location is:  
`/opt/crystal_xir2/bobje/webcontent/enterprise115/viewer/en/`
  - ♦ Copy all `*.jsp` files at:

```
/opt/crystal_xir2/bobje/tomcat/webapps/esec-script/
```

---

**NOTE:** The `publish_report.aspx` and `delete_report.aspx` files are available in the `reports_patch\Tomcat` directory of the Sentinel 6 SP2 distribution or in the [Sentinel Reports distribution \(http://support.novell.com/products/sentinel/sentinel61.html\)](http://support.novell.com/products/sentinel/sentinel61.html).

---

- 5 Set the permissions and ownership for the `publish_report.jsp` and `delete_report.jsp` files as following:

```
-rwxr-xr-x 1 crystal bobje
```

- 6 Copy all `*.jar` files:

From:

```
/opt/crystal_xir2/bobje/tomcat/webapps/jsfadmin/WEB-INF/lib/
```

To:

```
/opt/crystal_xir2/bobje/tomcat/webapps/esec-script/WEB-INF/lib
```

- 7 If Crystal was installed in a non-default location or as system install, modify the String `BOBJHome` setting in `publish_report.jsp` and `delete_report.jsp` files to the Crystal Reports installation path. For example:.

```
String BOBJHome = "/opt/crystal_xir2/bobje/enterprise115"
```

If Crystal was installed as the designated Crystal user into the default location, no changes should be necessary to this parameter.

- 8 Restart the Web Server and the Crystal Reports server.

## 8.3 Downloading the Service Packs for Crystal Reports

- 1 Go to the [Novell download Web site \(http://download.novell.com\)](http://download.novell.com).
- 2 In the Patches section, click *search patches*.
- 3 Select `SIEM-Sentinel` from the *Product* list.
- 4 Specify `crystal` as the keyword, then click *Search*.  
A list of Sentinel patches that include the Sentinel Crystal XI R2 SP4 patch is displayed.
- 5 Click the appropriate Sentinel version installed on your system, then click *Sentinel Crystal XI R2 SP4*.
- 6 In the Sentinel Crystal XI R2 SP4 page, click *proceed to download*.
- 7 Refer to the `Crystal_Reports_patchinstallation.pdf` for installation instructions.

## 8.4 Publishing Crystal Reports Templates

---

**NOTE:** It is strongly encouraged that the Sentinel Reports Release Notes be reviewed before performing this task. There can be updated files, scripts and additional steps.

---

Many report templates are created by Novell for use in the Sentinel Control Center Analysis tab and Advisor tab. The most recent reports can be downloaded from the [Sentinel 6.1 Plugins Web site \(http://support.novell.com/products/sentinel/sentinel61.html\)](http://support.novell.com/products/sentinel/sentinel61.html).

The core set of Sentinel reports are distributed in the Sentinel Core Solution Pack.

There are four ways to add reports to the system:

- ◆ Download a Solution Pack from the Solution Packs tab and use the Solution Manager to install one or more controls that include reports
- ◆ Download a Collector Pack from the Collectors tab and use the Solution Manager to install one or more controls that include reports
- ◆ Add one or more report templates (.rpt files) using the Crystal Publishing Wizard
- ◆ Add one or more report templates (.rpt files) using the Crystal Reports Central Management Console

---

**IMPORTANT:** To run any Top 10 reports, aggregation must be enabled and [EventFileRedirectService](#) in `DAS_Binary.xml` must be set to on. For information on how to enable aggregation, see “Report Data Configuration” section of “Admin” in [Sentinel 6.1 User Guide](#).

---

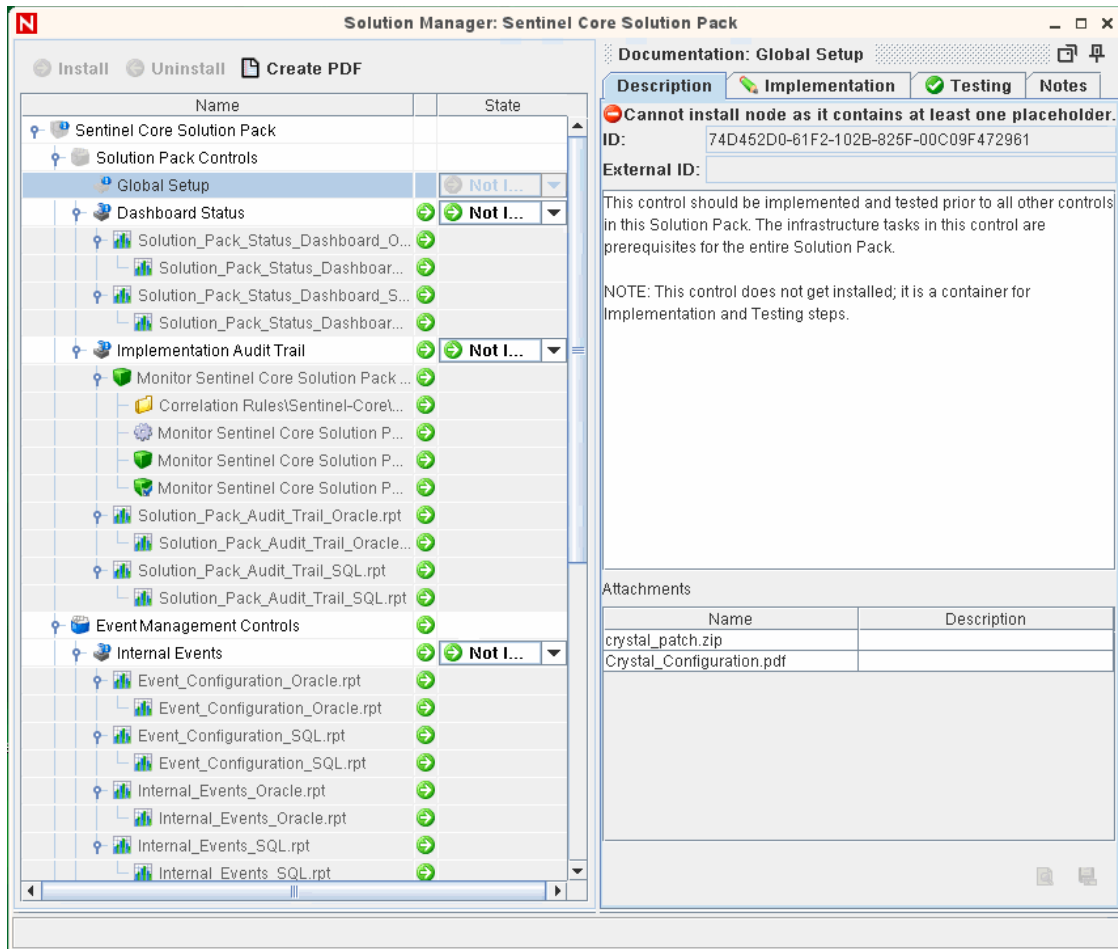
### 8.4.1 Publishing Report Templates using Solution Manager

If the Web Server and Crystal Reports server are configured properly, reports included in a Solution Pack or Collector Pack can be published directly to the Crystal Reports Server using the Solution Manager. To configure the system, you must download the Sentinel Core Solution Pack, available on the Solution Packs tab at [Sentinel 6.1 Content Web site \(http://support.novell.com/products/sentinel/secure/sentinel61.html\)](http://support.novell.com/products/sentinel/secure/sentinel61.html).

The Sentinel Core Solution Pack includes auxiliary files that must be applied to both the Web Server and the Crystal Reports server. These auxiliary files are available in the Solution Manager after you import the Core Solution Pack. When you select the Global Setup control, the auxiliary file attachments (and instructions for applying them) are available in the lower right corner of the screen.



**Figure 8-1** Core Solution Pack in Solution Manager Showing Crystal Auxiliary Files



## 8.4.2 Publishing Report Templates – Crystal Publishing Wizard

Sentinel reports are now distributed using Solution Packs, but this method can be used to publish report templates that are from a source other than a Solution Pack.

**NOTE:** A Windows platform is required to run Crystal Publishing Wizard.

### To import Crystal Reports templates:

**NOTE:** If you import (publish) your Reports Templates again, delete your previous import of Report Templates.

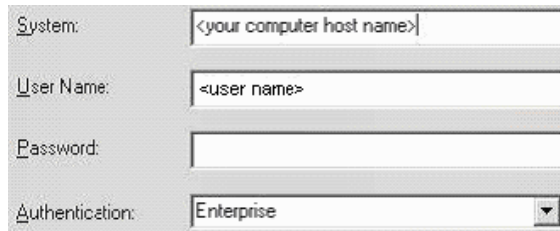
- 1 Click Start > All Programs > BusinessObjects 115 > Crystal Reports Server > Publishing Wizard.
- 2 Click Next.

Login. System should be your host computer name and Authentication should be Enterprise. User Name can be Administrator. For security reasons, you should use another user other than Administrator. Provide your password and click Next.

---

**NOTE:** Publishing reports under user Administrator allows all users access to the reports.

---

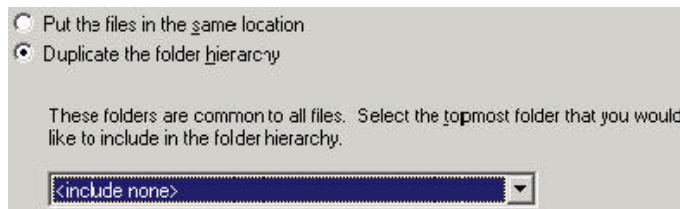


System: <your computer host name>  
User Name: <user name>  
Password:  
Authentication: Enterprise

- 3 Click Add Folder. [Optional] Click Include Subfolders.
- 4 Navigate to the location of the report template(s). Click OK. Click Next.
- 5 In the Specify Location window, click New Folder (upper right corner) and create a folder called SentinelReports (if it does not already exist). Click Next.



- 6 Select:
  - ♦ Duplicate the folder hierarchy.
  - ♦ Click the down arrow and select <include none>



Put the files in the same location  
 Duplicate the folder hierarchy

These folders are common to all files. Select the topmost folder that you would like to include in the folder hierarchy.

<include none>

Click Next.

- 7 In the Confirm Location window, click Next.
- 8 In the Specify Categories window, provide a category name (such as sentinel), highlight the name, and click the + button.



---

**NOTE:** Only the first report displays under the category after clicking Next.

---

Click Next.

- 9 In the Specify Schedule window, click Let users update the object (this should be default). Click Next.
- 10 In the Specify Repository Refresh window, click Enable All to enable repository refresh. Click Next.
- 11 In the Specify Keep Saved Data window, click Enable All to keep saved data when publishing reports. Click Next.
- 12 In the Change Defaults Values window, click Publish reports without modifying properties (this should be default). Click Next.
- 13 Click Next to add your objects.
- 14 Click Next. Click Finish.

When the Sentinel templates for Crystal Reports are published to the Crystal Reports Server, the templates must reside within the SentinelReports directory or they will not display in the Sentinel Control Center.

### 8.4.3 Publishing Report Templates – Central Management Console

Sentinel reports are now distributed using Solution Packs, but this method can be used to publish report templates that are from a source other than a Solution Pack.

#### To import Crystal Reports Templates:

- 1 Open a Web browser and provide the following URL:  
`http://<hostname_or_IP_of_web_server>:<port_number_for_webserver_port>/businessobjects/enterprise115/WebTools/adminlaunch`
- 2 Click Central Management Console.
- 3 Login to your Crystal Reports Server.
- 4 Under the Organize pane, click Folders.
- 5 In the upper right-hand corner, click New Folder.
- 6 Create a folder SentinelReports (if it does not already exist). Click OK.

---

**NOTE:** You must exactly name the folder SentinelReports.

---

- 7 Click SentinelReports.
- 8 Click the Subfolders tab and create subfolders if desired. If adding the Sentinel core reports manually, create the following subfolders:
  - ◆ Advisor\_Vulnerability
  - ◆ Dashboards
  - ◆ Incident Management
  - ◆ Internal Events
  - ◆ Security Events
  - ◆ Top 10
- 9 Click Home > Objects > New Object.
- 10 On left side of the page, highlight Report.

- 11 Click Browse and browse to the location of the report templates you want to add. Pick a folder and select a report.
- 12 Highlight SentinelReports, click Show Subfolders.
- 13 Select the appropriate folder for the report, click Show Subfolders.
- 14 Click Submit.
- 15 To add the remaining reports, repeat steps 9 to 17 until all reports have been added.

## 8.5 Using the Crystal XI R2 Web Server

Crystal Reports Server XI on Linux installs a Web Server through which you can perform administrative tasks as well publish and view reports.

The administrative portal is accessed through your browser at the following URL:

```
http://<hostname_or_IP_of_web_server>:<port_number_for_webserver_port>/  
businessobjects/enterprise115/WebTools/adminlaunch
```

The non-administrative (general use) portal is accessed through your browser at the following URL:

```
http://<hostname_or_IP_of_web_server>:<port_number_for_webserver_port>/  
businessobjects/enterprise115/WebTools/adminlaunch
```

### 8.5.1 Testing connectivity to the Web Server

**To test connectivity to the Web Server:**

- 1 Go to another machine that is on the same network as your Web Server.
- 2 Provide

```
http://<hostname_or_IP_of_web_server>:<port_number_for_webserver_port>/  
businessobjects/enterprise115/WebTools/adminlaunch
```

You should get a Crystal BusinessObjects Web page.

### 8.5.2 Setting a “Named User” Account

The license key supplied with Crystal Reports Server is a Named User account key. The Guest account has to be changed from Concurrent User to Named User.

**To set the Guest Account as Named User:**

- 1 Open a Web browser and provide the following url:  

```
http://<hostname_or_IP_of_web_server>:<port_number_for_webserver_port>/  
businessobjects/enterprise115/WebTools/adminlaunch
```
- 2 Click Central Management Console.
- 3 The System Name should be your host computer name. Authentication Type should be Enterprise. If not, select Enterprise.
- 4 In the Organize pane, click Users > Guest.
- 5 Change connection type from Concurrent User to Named User; Click Update.  
Logoff and close window.

## 8.5.3 Configuring Reports Permissions

This procedure discusses how to use the Administration Launchpad to configure the permissions on reports to allow you to view and modify reports on demand.

### To Configure Reports Permissions:

- 1 Open a Web browser and provide the following URL:  
`http://<hostname_or_IP_of_web_server>:<port_number_for_webserver_port>/businessobjects/enterprise115/WebTools/adminlaunch`
- 2 Click Central Management Console.  
The System Name should be your host computer name. Authentication Type should be Enterprise. If not, select Enterprise.
- 3 Provide your user name, password and click Log On.
- 4 In the Organize pane, click Folders.
- 5 Single-click SentinelReports; Select All.
- 6 Click the Rights tab.
- 7 For Everyone, in the drop-down menu to the right select View on Demand.
- 8 Click Update; Logoff and close the window.

## 8.6 Increasing Crystal Reports Server Report Refresh Record Limit

If Crystal attempts to process an extremely large number of events, it might give an error about maximum processing time or maximum record limit. To set your server to process a higher number or an unlimited number of records you will need to reconfigure the Crystal Page Server.

### To Reconfigure the Crystal Page Server:

- 1 Open a Web browser and provide the following URL:  
`http://<hostname_or_IP_of_web_server>:<port_number_for_webserver_port>/businessobjects/enterprise115/WebTools/adminlaunch`
- 2 Click Central Management Console.
- 3 The System Name should be your host computer name. Authentication Type should be Enterprise. If not, select Enterprise.
- 4 Provide your user name, password and click Log On.
- 5 Click Servers; Click <server name>.pageserver.
- 6 Under Database Records to Read When Previewing Or Refreshing a report, click Unlimited records; Click Apply.
- 7 A prompt to restart the page server displays, click OK.
- 8 You might be prompted for a logon name and password to access the operating system service manager.

## 8.7 Configuring Sentinel Control Center to Integrate with Crystal Reports Server

The Sentinel Control Center can be configured to integrate with the Crystal Reports Server, allowing you to view Crystal Reports from within Sentinel Control Center.

To enable Sentinel Control Center integration with Crystal Reports Server, follow the instructions below.

---

**NOTE:** This configuration must be performed only after the Crystal Reports Server has been installed and Crystal Reports have been published to it. For more information on supported platforms for Crystal Reports Server in a Sentinel environment, [Chapter 2, “System Requirements,” on page 15](#).

---

### To Configure Sentinel to Integrate with Crystal Reports Server:

- 1 Log into Sentinel Control Center as a user that has privileges to the Admin tab.
- 2 On the Admin tab, select Crystal Report Configuration.
- 3 In the Analysis URL field, provide the following:

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/  
esec-script/  
GetReports.jsp?APS=<hostname>&user=Guest&password=&tab=Analysis
```

---

**NOTE:** <hostname\_or\_IP\_of\_web\_server> must be replaced with the IP address or hostname of the Crystal Reports Server.

---

---

**NOTE:** The URL above will not work properly if the APS is set to the IP Address. It must be the host name.

---

---

**NOTE:** <web\_server\_port\_default\_8080> must be replaced with the port the Crystal Web Server is listening on.

---

- 4 Click Refresh next to the Analysis URL field.
- 5 If you have Advisor installed, provide the following in the Advisor URL field:

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/  
esec-script/  
GetReports.jsp?APS=<hostname>&user=Guest&password=&tab=Advisor
```

---

**NOTE:** <hostname\_or\_IP\_of\_web\_server> must be replaced with the IP address or hostname of the Crystal Reports Server.

---

---

**NOTE:** The URL above will not work properly if the APS is set to the IP Address. It must be the host name.

---

---

**NOTE:** <web\_server\_port\_default\_8080> must be replaced with the port the Crystal Web Server is listening on.

---

- 6 Click Refresh next to the Advisor URL field;  
Click Save.

7 Logout and log back in to the Sentinel Control Center.

The Crystal Reports trees in the Analysis and Advisor (if Advisor is installed) tabs should now display in the Navigator window.

## 8.8 Utilities and Troubleshooting

- ♦ [Section 8.8.1, “Starting MySQL,” on page 135](#)
- ♦ [Section 8.8.2, “Starting Tomcat,” on page 135](#)
- ♦ [Section 8.8.3, “Starting Crystal Reports Servers,” on page 135](#)
- ♦ [Section 8.8.4, “Crystal Host Name Error,” on page 135](#)
- ♦ [Section 8.8.5, “Cannot Connect to CMS,” on page 136](#)

### 8.8.1 Starting MySQL

To make sure MySQL is running:

- 1 Log in as crystal user.
- 2 `cd /opt/crystal_xir2/bobje`
- 3 `./mysqlstartup.sh`

### 8.8.2 Starting Tomcat

To make sure Tomcat is running:

- 1 Log in as crystal user
- 2 `cd /opt/crystal_xir2/bobje`
- 3 `./tomcatstartup.sh`

### 8.8.3 Starting Crystal Reports Servers

To make sure Crystal Reports Servers are running:

- 1 Log in as crystal user
- 2 `cd /opt/crystal_xir2/bobje`
- 3 `./startservers`

### 8.8.4 Crystal Host Name Error

To resolve Host Name error

- 1 If you get the following error:

```
Warning: ORB::BOA_init: hostname lookup returned `localhost' (127.0.0.1)
Use the -Oahost option to select some other hostname
```

Make sure your IP and hostname are in the `/etc/hosts` file. For example,

```
10.0.0.1    linuxCE02
```

## 8.8.5 Cannot Connect to CMS

If the system reports that it cannot connect to the CMS, try executing the following commands.

### To Troubleshoot CMS connection failure:

- 1 If the command `netstat -an | grep 6400` does not return any results, try the following:
  - ♦ Provide MySQL connection information again:
    1. Login as crystal user
    2. `cd /opt/crystal_xir2/bobje`
    3. `./cmsdbsetup.sh`
    4. Press Enter when [ <hostname>.cms ] displays.
    5. Select `select` and provide all your MySQL DB info that was entered during install time. For more information, see install instructions in [Chapter 3, “Installing Sentinel 6.1 SP2,”](#) on page 27.
    6. When done, quit `cmsdbsetup.sh`
    7. `./stopservers`
    8. `./startservers`
  - ♦ Re-initialize MySQL DB:
    1. Login as crystal user
    2. `cd /opt/crystal_xir2/bobje`
    3. `./cmsdbsetup.sh`
    4. Press Enter when [ <hostname>.cms ] displays.
    5. Select `reinitialize` and follow instructions.
    6. When done, quit `cmsdbsetup.sh`
    7. `./stopservers`
    8. `./startservers`
- 2 Make sure all CCM servers are enabled:
  - 2a Login as crystal user
  - 2b `cd /opt/crystal_xir2/bobje`
  - 2c `./ccm.sh -enable all`

## 8.9 High-Performance Configurations for Crystal

Depending on the number of events that Crystal is querying, you might get an error on maximum processing time or maximum record limit. To set your server to process a higher number or an unlimited number of records you must reconfigure the Crystal Page Server. This can be done by using either the Central Configuration Manager or the Crystal Web Page.

### To Reconfigure the Crystal Page Server through the Central Configuration Manager:

- 1 Click Start > All Programs > BusinessObjects 11 > Crystal Reports Server > Central Configuration Manager.



- 2 Right-click Crystal Reports Page Server and select Stop.
- 3 Right-click Crystal Reports Page Server and select properties.
- 4 In the Command field under the Properties tab, at the end of the command line add:

```
maxDBResultRecords <value greater than 20000 or 0 to disable the default limit>
```

- 5 Restart Crystal Page Server.

### To Reconfigure the Crystal Page Server through the Central Management Console:

- 1 Click Start > All Programs > BusinessObjects 11 > Crystal Reports Server > .Net Administration Launchpad. Alternatively, open a Web browser and provide the following URL:  
`http://<hostname_or_IP_of_web_server>:<port_number_for_webserver_port>/businessobjects/enterprise115/WebTools/adminlaunch`
- 2 Click Central Management Console.
- 3 The System Name should be your host computer name. Authentication Type should be Enterprise. If not, select Enterprise.
- 4 Provide your user name, password and click Log On. Click Servers.
- 5 Click <server name>.pageserver.
- 6 Under Database Records to Read When previewing or Refreshing a report, click Unlimited records. Click Apply.
- 7 A prompt to restart the page server will display, click OK.

You might be prompted for a logon name and password to access the operating system service manager.

## 8.9.1 Reports Using Aggregation Service

To improve performance, the Top 10 reports included in the Sentinel Core Solution Pack query summary tables instead of the events table. The summary tables contain counts over time for combinations of fields in the event data. This provides a much smaller data set for certain types of queries and results in much faster queries and report run time.

The Aggregation service is responsible for populating the summary tables with summarizations of all of the events in the events table. The Aggregation service will only generate summarized data for summaries that are active. The following summaries are required by the Top 10 reports and are enabled by default:

- ◆ EventDestSummary
- ◆ EventSevSummary
- ◆ EventSrcSummary

Summaries can be activated or inactivated using the Report Data Configuration window under the Admin tab of Sentinel Control Center.

The Aggregation service also depends on the `EventFileRedirectService` component in DAS Binary to feed it the event data that it will summarize. Therefore, this component must be enabled in order for the Aggregation service to run properly. This component is enabled or disabled by modifying the "status" attribute of the `EventFileRedirectService` component in the `das_binary.xml` file to "on" or "off". By default, this component is "on".

---

**NOTE:** For information about EventFileRedirectService and the three aggregation summaries, see “Report Data Configuration” in Admin in the *Sentinel 6.1 User Guide*.

---

**NOTE:** Reports that query a large date range might take sometime to run. They can be scheduled instead of running interactively. For information about scheduling Crystal Reports, go to [Crystal Reports Server XI R2 documentation \(http://www.sap.com/search/index.epx?q1=SCHEDULING+CRYSTAL+REPORT&num=10\)](http://www.sap.com/search/index.epx?q1=SCHEDULING+CRYSTAL+REPORT&num=10) and click the CRYSTAL REPORTS SERVER.pdf.

The above mentioned URL was current at the time of publication of the document.

---

## 8.9.2 Report Development

The Crystal Reports Developer can be used to create or modify Crystal reports. For custom developed reports, the following is recommended:

- ◆ If the reports can utilize pre-defined aggregate tables, select the aggregate table that result in the processing of the least amount of data.
- ◆ Try to push most of the data processing to the database engine.
- ◆ To reduce processing overhead in Crystal Server, minimize the amount of data to retrieve to the Crystal Server.
- ◆ Always write reports against the database views provided by Novell instead of writing reports against the base tables.

## 8.10 Using Crystal Reports

For more information on using Crystal Reports Server for Sentinel Reporting, see “[Crystal Report Configuration](#)” in the *Sentinel 6.1 User Guide*.

# Uninstalling Sentinel

- ♦ [Section 9.1, “Uninstalling Sentinel,” on page 139](#)
- ♦ [Section 9.2, “Post-Uninstall,” on page 140](#)

To remove a Sentinel installation, uninstallers are provided for Linux, Solaris, and Windows. Several files, including log files, are preserved and can be manually removed if desired. Before performing a new installation, it is highly recommended that you perform all of the following steps to ensure there are no files or system settings remaining from a previous installation.

---

**WARNING:** These instructions involve modifying operating system settings and files. If you are not familiar with modifying these system setting and/or files, please contact your System Administrator.

---

## 9.1 Uninstalling Sentinel

- ♦ [Section 9.1.1, “Uninstall for Solaris and Linux,” on page 139](#)
- ♦ [Section 9.1.2, “Uninstall for Windows,” on page 140](#)

### 9.1.1 Uninstall for Solaris and Linux

**To use the Sentinel Uninstaller for Solaris and Linux:**

- 1 Login as user root.
- 2 Stop the Sentinel Server.
- 3 Go to:  
`$ESEC_HOME/_uninst`
- 4 Provide:  
**For GUI mode:**  
`./uninstall.bin`  
Or  
**For text-based (“serial console”) mode:**  
`./uninstall.bin -console`
- 5 Select a language and click OK.
- 6 The Sentinel Install Shield Wizard displays. Click Next.
- 7 Select the components you want to uninstall and click Next.
- 8 Ensure any running Sentinel applications are stopped and click Next.
- 9 If you have selected to uninstall the Database component, you are prompted to select one of the following options:
  - ♦ **Delete the entire database instance:** Removes the database instance and frees up disk space used by the database.

- ♦ **Delete only the database objects:** Removes the contents of the database except for the esecdba user. The database instance can then be repopulated using the Sentinel installer. This option does not free up disk space.
- 10 If you selected to Delete only the database objects, you will be prompted to provide the esecdba password. Click Next.
  - 11 A summary of the features selected for uninstall will be displayed. Click Uninstall.
  - 12 Click Finish.

## 9.1.2 Uninstall for Windows

### To use the Sentinel Windows Uninstaller:

- 1 Login as an Administrator.
- 2 Stop the Sentinel Server.
- 3 Select Start > All Programs (Win XP) or Programs (WIN 2000)> Sentinel > Uninstall Sentinel. You can also type %Esec\_home%\\_uninst in Start > Run, and double-click `uninstall.exe`.
- 4 Select a language and click OK.
- 5 The Sentinel 6.1 - InstallShield Wizard displays. Click Next.
- 6 Select the components you want to uninstall and click Next.
- 7 Ensure any running Sentinel applications are stopped and click Next.
- 8 If you have selected to uninstall the Database component, you are prompted to select one of the following options:
  - ♦ **Delete the entire database:** Removes the database and frees up disk space used by the database.
  - ♦ **Delete only the database objects:** Removes the contents of the database except for the esecdba user. The database can then be repopulated using the Sentinel installer. This option does not free up disk space.
- 9 If you have selected to uninstall the Database component, you are also prompted to select one of the following:
  - ♦ **Windows Authentication:** To use Windows Authentication, you must be logged into Windows as a user that is a MS SQL Server instance System Administrator.
  - ♦ **SQL Authentication:** Provide the sa (or equivalent) user's username and password.Click Next.
- 10 A summary of the features selected for uninstall will be displayed. Click Uninstall.
- 11 Select to Reboot the system and click Finish.

## 9.2 Post-Uninstall

- ♦ [Section 9.2.1, "Sentinel Settings," on page 141](#)

## 9.2.1 Sentinel Settings

After uninstalling Sentinel, certain systems settings remain, which can be manually removed. These settings should be removed before performing a “clean” installation of Sentinel, particularly if the Sentinel uninstallation encountered errors.

---

**NOTE:** On Solaris and Linux, uninstalling Sentinel Server will not remove the Sentinel Administrator User from the operating system. You will need to manually remove that user, if desired.

---

### Remove Sentinel System Settings on Linux

#### To Manually Cleanup Sentinel on Linux:

- 1 Login as root.
- 2 Ensure that all Sentinel processes are stopped.
- 3 Remove contents of `/opt/novell/sentinel6` (or wherever the Sentinel software was installed).
- 4 Remove Sentinel Service startup files:

**On SLES:**

```
chkconfig --del sentinel
```

**On RedHat:**

```
rm /etc/rc.d/rc0.d/K02sentinel
rm /etc/rc.d/rc3.d/S98sentinel
rm /etc/rc.d/rc5.d/S98sentinel
```

- 5 Remove the following files in the `/etc/rc.d/rc0.d` directory, if they exist:
  - ♦ `K01wizard`
  - ♦ `K01esdee`
  - ♦ `K01esyslogserver`
- 6 Remove the following files in the `/etc/rc.d/rc3.d` directory, if they exist:
  - ♦ `S99wizard`
  - ♦ `S99esyslogserver`
  - ♦ `S99esdee`
- 7 Remove the following files in the `/etc/rc.d/rc5.d` directory, if they exist:
  - ♦ `S99wizard`
  - ♦ `S99esyslogserver`
  - ♦ `S99esdee`
- 8 Remove the following files in the `/etc/init.d` directory, if they exist:
  - ♦ `sentinel`
  - ♦ `wizard`
  - ♦ `esdee`
  - ♦ `esyslogserver`

- 9 Make sure nobody is logged in as the Sentinel Administrator operating system user (esecadm by default), then remove the user (and home dir) and esec group.
  - ♦ Run: `userdel -r esecadm`
  - ♦ Run: `groupdel esec`
- 10 Remove the directory `/root/InstallShield`
- 11 Remove the file `/root/vpd.properties`
- 12 Remove InstallShield section of `/etc/profile` and `/etc/.login`
- 13 Remove the Sentinel Oracle database. For more information, see [“Remove Sentinel Oracle Database on Linux and Solaris” on page 143](#).
- 14 Restart the operating system.

## Remove Sentinel System Settings on Solaris

### To Manually Cleanup Sentinel on Solaris:

- 1 Login as root.
- 2 Ensure that no Sentinel processes are running.
- 3 Remove contents of `/opt/novell/sentinel6` (or wherever the Sentinel software was installed).
- 4 Remove the following files in the `/etc/rc0.d` directory, if they exist:
  - ♦ `K01wizard`
  - ♦ `K02sentinel`
  - ♦ `K01esdee`
  - ♦ `K01esyslogserver`
- 5 Remove the following files in the `/etc/rc3.d` directory, if they exist:
  - ♦ `S98sentinel`
  - ♦ `S99wizard`
  - ♦ `S99esyslogserver`
  - ♦ `S99esdee`
- 6 Remove the following files in the `/etc/init.d` directory, if they exist:
  - ♦ `sentinel`
  - ♦ `wizard`
  - ♦ `esdee`
  - ♦ `esyslogserver`
- 7 Remove the following files from `/usr/local/bin`, if they exist:
  - ♦ `stop_wizard.sh`
  - ♦ `restart_wizard.sh`
  - ♦ `start_wizard.sh`

- 8 Make sure nobody is logged in as Sentinel Administrator operating system user, then remove the user (and home dir) and esec group.
  - ♦ Run: `userdel -r esecadm`
  - ♦ Run: `groupdel esec`
- 9 Remove Installshield section of `/etc/profile` and `/etc/.login`
- 10 Remove the `/InstallShield` directory, if one exists.
- 11 Clean up InstallShield references in `/var/sadm/pkg`. If the following files exist, remove the following files from the `/var/sadm/pkg` directory:
  - ♦ All files that begin with IS (IS\* on the command line)
  - ♦ All files that begin with ES (ES\* on the command line)
  - ♦ All files that begin with MISCwp (MISCwp\* on the command line)
- 12 Remove the Sentinel Oracle database. For more information, see [“Remove Sentinel Oracle Database on Linux and Solaris” on page 143](#).
- 13 Restart the operating system.

## Remove Sentinel Oracle Database on Linux and Solaris

### To Manually Cleanup Sentinel Oracle Database on Linux and Solaris:

---

**NOTE:** Make sure no other applications are using this database before removing it.

---

- 1 Log in as oracle.
- 2 Stop Oracle Listener:
  - ♦ Run: `lsnrctl stop`
- 3 Stop Sentinel database:
  - ♦ Set the `ORACLE_SID` environment variable to the name of your Sentinel database instance (default ESEC).
  - ♦ Run: `sqlplus "/ as sysdba"`
  - ♦ At sqlplus prompt, run: `shutdown immediate`
- 4 Remove entry for Sentinel database in the `oratab` file located at:
 

On Linux:

```
/etc/oratab
```

On Solaris:

```
/var/opt/oracle/oratab
```
- 5 Remove `init<your_instance_name>.ora` (default `initESEC.ora`) file from the directory `$ORACLE_HOME/dbs`.
- 6 Remove entries for your Sentinel database from the following files in the `$ORACLE_HOME/network/admin` directory:
  - ♦ `tnsnames.ora`
  - ♦ `listener.ora`
- 7 Delete the database data files from the location you have selected to install them.
- 8 Delete the database archive files from the location you have selected to create them.

## Remove Sentinel System Settings on Windows with MS SQL Server

### To Manually Cleanup Sentinel on Windows:

- 1 Delete the folder %CommonProgramFiles%\InstallShield\Universal and all of its contents.
- 2 Delete the %ESEC\_HOME% folder (by default: C:\Program Files\Novell\Sentinel6).
- 3 Right-click My Computer > Properties > Advanced tab.
- 4 Click the Environment Variables button.
- 5 If they exist, delete the following variables:
  - ◆ ESEC\_HOME
  - ◆ ESEC\_VERSION
  - ◆ ESEC\_JAVA\_HOME
  - ◆ ESEC\_CONF\_FILE
  - ◆ WORKBENCH\_HOME
- 6 Remove any entries in the PATH environment variable that point to the Sentinel installation.

---

**WARNING:** Do not remove paths to anything other than the old Sentinel installation. This could result in your system not functioning properly.

---

- 7 Delete all Sentinel shortcuts from the Desktop.
- 8 Delete the shortcut folder Start >Programs > Sentinel from the Start menu.
- 9 Restart the operating system.

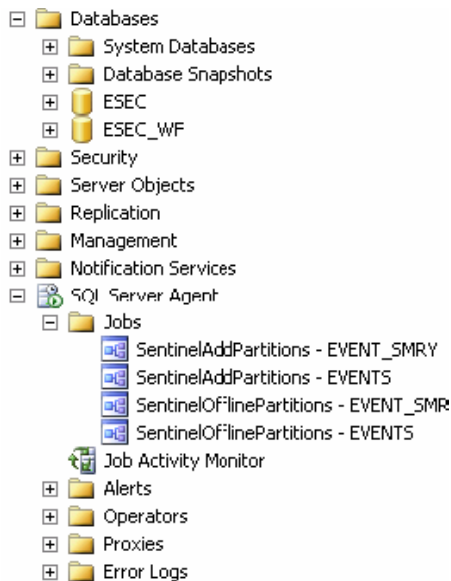
### To Manually Cleanup Sentinel Microsoft SQL Server database on Windows:

---

**NOTE:** Make sure no other applications are using this database before removing it.

---

- 1 Open Microsoft SQL Server Management Studio and connect to the SQL Server instance where you've installed your Sentinel database.





- 2** Expand the SQL Server Agent > Jobs tree and remove the Sentinel jobs.
- 3** Expand the Databases tree and locate your Sentinel database. There should be a Sentinel database (by default called ESEC) and an iTRAC database (by default called ESEC\_WF). Right-click each and select Delete.
- 4** When prompted, select Yes to delete the database.
- 5** Expand the Security > Login tree and remove the Sentinel database users, if they exist.
  - ◆ esecdba
  - ◆ esecapp
  - ◆ esecadm
  - ◆ esecrpt
- 6** Delete the database archive files from the location you have selected to create them.



# Pre-installation Questionnaire



Answering these questions can be helpful in planning your own installation or preparing for consultants to install your Sentinel system.

## Pre-Install Questions

- 1 What is your goal or purpose of using Novell Sentinel?
  - 1a Compliance
  - 1b Security Event Management
  - 1c Other \_\_\_\_\_
- 2 What hardware has been allocated for the installation of Sentinel? Is it in accordance with hardware specifications provided in the Sentinel Installation Guide?
- 3 Have you validated Sentinel hardware and operating system requirements described in the Sentinel Installation Guide against your configuration?
  - ♦ OS patch levels
  - ♦ Service Patches
  - ♦ Hot Fixes and so on.
- 4 Does your DAS machine meet the necessary OS and hardware requirements?
- 5 What is the network architecture for the source devices with respect to the security segment where the Sentinel and Collector hardware is to be located?

---

**NOTE:** This is important to understand the hierarchy of Collector data collection and to identify any firewalls that must be penetrated to enable Collector to Sentinel communication or Sentinel to DB communication or Crystal Server to DB communication.

---

Provide information below (text and/or drawing) or link to information.

**6** What reports do you want out of the system? This is important to ensure that your Collectors collect the correct data to be passed to the Sentinel database.

**6a** \_\_\_\_\_

**6b** \_\_\_\_\_

**6c** \_\_\_\_\_

**6d** \_\_\_\_\_

**6e** \_\_\_\_\_

**6f** \_\_\_\_\_

**7** What source devices do you want to collect data from (IDS, HIDS, Routers, Firewalls and so on), event rate (EPS – events per second), versions, connection methods, platforms and patches?

Device (mfr/ model)	Event Rate (EPS)	Version	Connection Method	Platform	Patches

Can you provide sample data of what you want the Sentinel Collectors to collect and parse? Sentinel can be configured to provide the desired output based on the information provided here.

- 8** What security model/standards exist at your site?
- ◆ What is your stance on local accounts versus domain authentication?
    - ◆ For Windows with domain authentication, proper domain account settings must be created to ensure that Sentinel can be installed.
    - ◆ For Solaris install, this is not applicable. However, Sentinel does not support NIS.
- 9** What is the required data retention in terms of days?
- 10** Based on the data retention information and EPS, what disk size will you be using? Use 500 to 800 bytes/event for sizing estimates.
- 11** What event patterns do you want to identify in your data?
- 12** Does the current data available from your event sources support the event patterns you want to detect, or will event enrichment using the mapping service be needed?
- 13** If the mapping service is needed, what is the source of the enrichment data, and what key will be used to perform the mapping? How will the maps be kept up to date?
- 14** When a security or compliance violation is detected, what processes will be used to remediate?

# Oracle Setup

# B

- ◆ [Section B.1, “Installing Oracle 11g,” on page 149](#)
- ◆ [Section B.2, “Upgrading the Database from Oracle 10g to Oracle 11g,” on page 156](#)
- ◆ [Section B.3, “Installing Oracle 10g,” on page 157](#)
- ◆ [Section B.4, “Configuring the System for Oracle Database Installation,” on page 160](#)
- ◆ [Section B.5, “Manual Oracle Instance Creation \(Optional\),” on page 164](#)

---

**IMPORTANT:** The instructions provided in this document are not intended to replace Oracle documentation. This section is an example of only one setup scenario for each platform. This documentation assumes that the Oracle users’ home directory is `/home/oracle` and that Oracle is installed into `/opt/oracle`. Your exact configuration might vary. Refer to the documentation of the operating system and Oracle for more information.

For more information on Oracle installations and the patch levels that are certified or supported for Sentinel, see [Chapter 2, “System Requirements,” on page 15](#).

---

## B.1 Installing Oracle 11g

- ◆ [Section B.1.1, “Oracle 11g Installation on SLES 11,” on page 149](#)
- ◆ [Section B.1.2, “Oracle 11g Installation on SLES 10,” on page 151](#)
- ◆ [Section B.1.3, “Oracle 11g Installation on Red Hat Linux 4,” on page 152](#)
- ◆ [Section B.1.4, “Oracle 11g Installation on Solaris 10,” on page 154](#)

### B.1.1 Oracle 11g Installation on SLES 11

**1** Follow the installation instructions provided in the SUSE Linux Enterprise Server (SLES) 11 installation manual. Install SLES 11 and the default packages along with the Oracle Server Base and the C/C++ Compiler and Tools.

**2** Log in as `root`.

**3** The account for the oracle user is disabled. Enable the account by changing the shell for the oracle user from `/bin/false` to `/bin/bash` by using YaST or by editing the `/etc/passwd` file.

If the oracle user account does not exist, create an account by using the following commands:

To add a dba group:

```
groupadd -G dba
```

To add an oracle user:

```
useradd -G dba -d <home_directory> -m oracle -p <passwd>
```

**4** Set a new password for the oracle user by using YaST or by using the following command:

```
/usr/bin/passwd oracle
```

**5** Change the default Oracle environment settings set by `oracore`, if required:

**5a** Change the Oracle home directory by editing the `ORACLE_HOME` variable in `/etc/profile.d/oracle.sh` file.

**5b** The default `ORACLE_SID` value is set to `orcl`. Change it to `ESEC` in the `/etc/profile.d/oracle.sh` file.

**6** Set the kernel parameters by using the following command:

```
/usr/sbin/rcoracle start
```

Required kernel parameter settings:

```
fs.file-max = 512 * PROCESSES
kernel.shmall = 2097152
kernel.shmmax = 2147483648
kernel.shmni = 4096
kernel.sem = 250 32000 100 128
net.ipv4.ip_local_port_range = 1024 65000
net.core.rmem_default = 4194304
net.core.rmem_max = 4194304
net.core.wmem_default = 262144
net.core.wmem_max = 262144
```

**7** Ensure that the packages are installed correctly by using the following command:

```
rpm -q <package_name>
```

List of packages:

```
binutils-2.19
gcc-4.3
gcc-32bit-4.3
gcc-c++-4.3
glibc-2.9
glibc-32bit-2.9
glibc-devel-2.9
glibc-devel-32bit-2.9
ksh-93t
libaio-0.3.104
libaio-32bit-0.3.104
libaio-devel-0.3.104
libaio-devel-32bit-0.3.104
libstdc++33-3.3.3
libstdc++33-32bit-3.3.3
libstdc++43-4.3.3_20081022
libstdc++43-32bit-4.3.3_20081022
libstdc++43-devel-4.3.3_20081022
libstdc++43-devel-32bit-4.3.3_20081022
libgcc43-4.3.3_20081022
libstdc++-devel-4.3
make-3.81
sysstat-8.1.5
```

**8** Change to the oracle user:

```
su -oracle
```

**9** Change to database directory, then run `./runinstaller`.

The Oracle Universal Installer screen is displayed.

**10** From the *Configuration* options, select *Install Database Software only*, then click *Next*.

**11** Accept the default inventory directory or browse and select a new directory, then click *Next*.

- 12 From the *Installation* types, select *Enterprise Edition*, then click *Next*.
- 13 Review your selections, then click *Install*.
- 14 Execute the specified scripts as the `root` user and click *OK* on completion.
- 15 After the installation is complete, click *Exit*.

## B.1.2 Oracle 11g Installation on SLES 10

- 1 Follow the installation instructions provided in the SLES 10 installation manual. Install SLES 10 with the `ext3` filesystem and the default packages along with Oracle Server Base, C/C++ Compiler and Tools.
- 2 Log in as `root`.
- 3 Install SLES 10 Service pack. Verify the service pack information by using the following command:

```
SPident
or
cat /etc/SuSE-release
```

- 4 The account for the oracle user is disabled. Enable the account by changing the shell for the oracle user from `/bin/false` to `/bin/bash` by using YaST or by editing the `/etc/passwd` file.

If the oracle user account does not exist, create an account by using the following commands:

To add a dba group:

```
groupadd -G dba
```

To add an oracle user:

```
useradd -G dba -d <home_directory> -m oracle -p <passwd>
```

- 5 Set a new password for the oracle user by using YaST or by using the following command:

```
/usr/bin/passwd oracle
```

- 6 Change the default Oracle environment settings set by `orarun`, if required:

**6a** Change the Oracle home directory by editing the `ORACLE_HOME` variable in `/etc/profile.d/oracle.sh` file.

**6b** The default `ORACLE_SID` value is set to `orcl`. Change it to `ESEC` in `/etc/profile.d/oracle.sh` file.

- 7 Set the kernel parameters by using the following command:

```
/usr/sbin/rcoracle start
```

Required kernel parameter settings:

```
fs.file-max = 512 * PROCESSES
kernel.shmall = 2097152
kernel.shmmax = 2147483648
kernel.shmmni = 4096
kernel.sem = 250 32000 100 128
net.ipv4.ip_local_port_range = 1024 65000
net.core.rmem_default = 4194304
net.core.rmem_max = 4194304
net.core.wmem_default = 262144
net.core.wmem_max = 262144
```

- 8 Ensure that the packages are installed correctly by using the following command:

```
rpm -q <package_name>
```

List of packages:

```
binutils-2.16.91.0.5
compat-libstdc++-5.0.7
glibc-2.4-31.2
glibc-devel-2.4-31.2
gcc-4.1.0
ksh-93r-12.9
libaio-0.3.104
libaio-devel-0.3.104
libelf-0.8.5
libgcc-4.1.0
libstdc++-4.1.0
libstdc++-devel-4.1.0
make-3.80
sysstat-6.0.2
unixODBC-2.2.11
unixODBC-devel-2.2.11
```

- 9 Change to the oracle user:

```
su - oracle
```

- 10 Change to database directory, then run `./runinstaller`.

The Oracle Universal Installer screen is displayed.

- 11 From the *Configuration* options, select *Install Database Software only*, then click *Next*.

- 12 Accept the default inventory directory or browse and select a new directory, then click *Next*.

- 13 From the *Installation* types, select *Enterprise Edition*, then click *Next*.

The Installation summary is displayed.

- 14 Review the settings, then click *Install*.

- 15 Execute the specified scripts as the `root` user and click *OK* on completion.

- 16 After the installation is complete, click *Exit*.

### B.1.3 Oracle 11g Installation on Red Hat Linux 4

- 1 Log in as `root`.

- 2 Set the kernel parameters as follows:

```
fs.file-max = 512 * PROCESSES
kernel.shmall = 2097152
kernel.shmmax = 2147483648
kernel.shmmni = 4096
kernel.sem = 250 32000 100 128
net.ipv4.ip_local_port_range = 1024 65000
net.core.rmem_default = 4194304
net.core.rmem_max = 4194304
net.core.wmem_default = 262144
net.core.wmem_max = 262144
```

- 3 Run the following command to ensure that the required packages are installed on your server.

```
rpm -q <package name>
```

List of packages:



```

binutils-2.15.92.0.2-18
compat-libstdc++-33.2.3-47.3
elfutils-libelf-0.97-5
elfutils-libelf-devel-0.97-5
glibc-2.3.9.4-2.19
glibc-common-2.3.9.4-2.19
glibc-devel-2.3.9.4-2.19
gcc-3.4.5-2
gcc-c++-3.4.5-2
libaio-devel-0.3.105-2
libaio-0.3.105-2
libgcc-3.4.5
libstdc++-3.4.5-2
libstdc++-devel-3.4.5-2
make-3.80-5
sysstat-5.0.5
unixODBC-2.2.11
unixODBC-devel-2.2.11

```

- 4** Create a UNIX group and UNIX user account for the Oracle database owner by using the following commands:

Add dba group (as root):

```

groupadd oinstall
groupadd dba

```

- 5** Add an Oracle user (as root):

```

useradd -g oinstall -G dba -d /opt/oracle/product/<10.2.0.3>/db_1 -m
oracle
passwd oracle

```

- 6** Change to the oracle user:

```

su - oracle

```

- 7** Create directories for ORACLE\_HOME and ORACLE\_BASE.

- 8** Open the `.bash_profile` file (in the oracle user's home directory) for editing, and append the following:

```

# User specific environment and startup programs
ORACLE_BASE=/opt/oracle; export ORACLE_BASE
ORACLE_HOME=$ORACLE_BASE/product/10.2.0/db_1; export ORACLE_HOME
ORACLE_TERM=xterm; export ORACLE_TERM
PATH=$ORACLE_HOME/bin:$PATH; export PATH
ORACLE_SID=oracle; export ORACLE_SID
LD_LIBRARY_PATH=$ORACLE_HOME/lib; export LD_LIBRARY_PATH
CLASSPATH=$ORACLE_HOME/jre:$ORACLE_HOME/jlib:$ORACLE_HOME/rdbms/jlib
CLASSPATH=$CLASSPATH:$ORACLE_HOME/network/jlib; export CLASSPATH
LD_ASSUME_KERNEL=2.4.19; export LD_ASSUME_KERNEL
TMP=/tmp; export TMP
TMPDIR=$TMP; export TMPDIR
PATH=$PATH:$HOME/bin
export PATH

unset USERNAME

```

---

**IMPORTANT:** This set of environment variables must only be used for the oracle user. These variables should not be set in the system environment or in the Sentinel Administrator User environment.

---

- 9 Run the `.bash_profile` to set the environment variables, and check the values by using the following command:

```
set | more
```

- 10 If you are using X emulation, set the `DISPLAY` environmental variable:

```
DISPLAY=<machine-name>:0.0; export DISPLAY
```

- 11 Change to database directory, then run the following script:

```
./runInstaller
```

- 12 When you proceed through the installation, leave all the prompts with their default values except the ones specified below:

**12a** In the Welcome window, click *Next*.

**12b** In the *File Locations* window, select `ORACLE_BASE` and `ORACLE_HOME` from the drop-down list for the *Destination Name*, then click *Next*.

**12c** Install only the Oracle software, and deselect the *Default Database Creation* option.

**12d** In the *Installation Types* window, select *Enterprise Edition*, then click *Next*.

**12e** In the *Summary* window, review the installation summary, then click *Install*.

**12f** In the *End of Installation* window, click *Exit*.

## B.1.4 Oracle 11g Installation on Solaris 10

- 1 Log in as `root`.

- 2 Set the kernel parameters according to the following standards:

```
set noexec_user_stack=1
set semsys:seminfo_semmni=100
set semsys:seminfo_semmns=1024
set semsys:seminfo_semmsl=256
set semsys:seminfo_semvmx=32767
set shmsys:shminfo_shmmax=4294967296
set shmsys:shminfo_shmmni=100
```

- 3 Run the following command to ensure that the required packages are installed on your server.

```
rpm -q <package name>
```

List of packages:

```
SUNWarc
SUNWbtool
SUNWhea
SUNWlibC
SUNWlibm
SUNWlibms
SUNWsprot
SUNWtoo
SUNWilof
SUNWilcs
SUNWi15cs
SUNWxfnt
SUNWsprox
```

- 4 Create a UNIX group and UNIX user account for the Oracle database owner by using the following commands:

Add dba group (as `root`):

```
groupadd oinstall
groupadd dba
```

**5** Add an Oracle user (as root):

```
useradd -g oinstall -G dba -d /opt/oracle/product/<10.2.0.3>/db_1 -m
oracle
passwd oracle
```

**6** Change to the oracle user:

```
su - oracle
```

**7** Create directories for ORACLE\_HOME and ORACLE\_BASE.

**8** Open the `.bash_profile` file (in the oracle user home directory) for editing, and append the following:

```
# User specific environment and startup programs
ORACLE_BASE=/opt/oracle; export ORACLE_BASE
ORACLE_HOME=$ORACLE_BASE/product/10.2.0/db_1; export ORACLE_HOME
ORACLE_TERM=xterm; export ORACLE_TERM
PATH=$ORACLE_HOME/bin:$PATH; export PATH
ORACLE_SID=oracle; export ORACLE_SID
LD_LIBRARY_PATH=$ORACLE_HOME/lib; export LD_LIBRARY_PATH
CLASSPATH=$ORACLE_HOME/jre:$ORACLE_HOME/jlib:$ORACLE_HOME/rdbms/jlib
CLASSPATH=$CLASSPATH:$ORACLE_HOME/network/jlib; export CLASSPATH
LD_ASSUME_KERNEL=2.4.19; export LD_ASSUME_KERNEL
TMP=/tmp; export TMP
TMPDIR=$TMP; export TMPDIR
PATH=$PATH:$HOME/bin
export PATH

unset USERNAME
```

---

**IMPORTANT:** This set of environment variables must only be used for the oracle user. These variables should not be set in the system environment or in the Sentinel Administrator User environment.

---

**9** Run the `.bash_profile` to set the environment variables, and check the values by using the following command:

```
set | more
```

**10** If you are using X emulation, set the `DISPLAY` environmental variable by using the following command:

```
DISPLAY=<machine-name>:0.0; export DISPLAY
```

**11** Change to database directory, then run the following script:

```
./runInstaller
```

**12** When you proceed through the installation, leave all the prompts with their default values except the ones specified below:

**12a** In the Welcome window, click *Next*.

**12b** In the *File Locations* window, select `ORACLE_BASE` and `ORACLE_HOME` from the drop-down list for the *Destination Name*, then click *Next*.

**12c** Install only the Oracle software, and deselect the *Default Database Creation* option.

**12d** In the *Installation Types* window, select *Enterprise Edition*, then click *Next*.

**12e** In the *Summary* window, review the install summary, then click *Install*.

**12f** In the *End of Installation* window, click *Exit*.

## B.2 Upgrading the Database from Oracle 10g to Oracle 11g

---

**NOTE:** There are several methods to upgrade the database from Oracle 10g to Oracle 11g. This section provides instructions on upgrading the database manually.

---

- 1 Shut down all the Sentinel applications.
- 2 Install the Oracle 11g software on a new ORACLE\_HOME and ORACLE\_BASE directory. For more information, refer to the [Oracle Documentation Web site \(http://www.oracle.com/technology/documentation/database.html\)](http://www.oracle.com/technology/documentation/database.html).
- 3 Verify the database for upgrading to Oracle 11g by using the pre-upgrade information tool (utlu111i.sql).

The SQL script is available at the Oracle 11g location, oracle\_home/rdbms/admin/utlu111i.sql. Run the script from the source database (Oracle 10g).

- 4 Connect to the database sysdba and run the following script:  

```
SQL>spool upgrade_info.log
SQL>@/11g_oracle_home/rdbms/admin/utlu111i.sql
```
- 5 Open the upgrade.info log file and check for any errors. If there are any errors, download and install the required patch files from the [Oracle Web site \(https://support.oracle.com/\)](https://support.oracle.com/).
- 6 Specify the following parameters in the initialization parameter file:

```
diagnostic_dest= $ORACLE_BASE/diag
memory_max_target=1GB
memory_target= 800m
compatible= 11.1.0
```

- 7 Shut down the Oracle 10g database:  

```
SQL>shutdown immediate
```
- 8 Set the ORACLE\_HOME and ORACLE\_BASE environment variables to the Oracle 11g software.
- 9 Use the new parameter values to Connect to Oracle 11g.
- 10 Start the database in the upgrade mode:  

```
SQL> startup upgrade
```
- 11 Use the catupgrd.sql script to upgrade the database:  

```
SQL> spool upgrade.log
SQL> @/rdbms/admin/catupgrd.sql
```
- 12 Open the upgrade.log file and check for errors. If there are any errors, download and install the required patch files from the [Oracle Web site \(https://support.oracle.com/\)](https://support.oracle.com/).
- 13 Run the utlu111s.sql post upgrade script:  

```
SQL>startup
SQL>@/rdbms/admin/utlrp.sql
```
- 14 Check the status of database components and ensure that all components are using the Oracle 11g version.

```
SQL>select comp_name,version,status from dba_registry
```

- 15 Copy the `tnsnames.ora`, `listener.ora`, `sqlnet.ora` files from the Oracle 10g source `ORACLE_HOME` to the Oracle 11g `ORACLE_HOME`.
- 16 Shut down the database and start the database, database listener, Sentinel, and all other services.

## B.3 Installing Oracle 10g

- ♦ [Section B.3.1, “Oracle 10g Installation on SLES 10,” on page 157](#)
- ♦ [Section B.3.2, “Oracle 10g Installation on Red Hat Linux 4,” on page 158](#)
- ♦ [Section B.3.3, “Oracle 10g Installation on Solaris 10,” on page 160](#)

### B.3.1 Oracle 10g Installation on SLES 10

- 1 Follow the installation instructions provided in the SLES 10 installation manual. Install SLES 10 with the `ext3` filesystem and default packages along with Oracle Server Base, C/C++ Compiler and Tools.
- 2 Log in as root.
- 3 Install the SLES 10 Service pack. Verify the service pack information by using the following command:  

```
SPident
```

or  

```
cat /etc/SuSE-release
```

The following result is expected:  

```
CONCLUSION: System is up-to-date!  
Found      SLES-10-x86_64-current
```
- 4 The account for the oracle user is disabled. Enable the account by changing the shell for the oracle user from `/bin/false` to `/bin/bash` by using YaST user administration or by editing the `/etc/passwd` file.
- 5 Set a new password for the oracle user by using YaST or by using the following command:  

```
/usr/bin/passwd oracle
```
- 6 Change the default Oracle environment set by `orarun`, if required:
  - 6a Change the Oracle home directory by editing the `ORACLE_HOME` variable in `/etc/profile.d/oracle.sh` file.
  - 6b The default `ORACLE_SID` value is set to `orcl`. Change it to `ESEC` in `/etc/profile.d/oracle.sh` file.
- 7 Set the kernel parameters by using the following command:  

```
/usr/sbin/rcoracle start
```
- 8 Change to the oracle user:  

```
su - oracle
```
- 9 Change to the database directory and run `./runinstaller`.  
The Oracle Universal Installer screen is displayed.
- 10 Accept the default inventory directory or browse and select a new directory, then click *Next*.

- 11 From the *Installation types*, select *Enterprise Edition*, then click *Next*.
- 12 For checking Network configuration requirements, select *User Verified*, then click.
- 13 From the Configuration options, select *Install Database Software only*, then click *Next*.  
The Installation summary is displayed.
- 14 Review the selections, then click *Install*.
- 15 Execute the specified scripts as *root* and click *OK* on completion.
- 16 After the installation is complete, click *Exit*.

## B.3.2 Oracle 10g Installation on Red Hat Linux 4

- 1 Log in as *root*.
- 2 Run the following command to ensure that the required packages are installed on your server.

```
rpm -q make
```

List of packages:

```
binutils-2.15.92.0.2-13.EL4
compat-db-4.1.25-9
compat-libstdc++-296-2.96-132.7.2
control-center-2.8.0-12
gcc-3.4.3-22.1.EL4
gcc-c++-3.4.3-22.1.EL44
glibc-2.3.4-2.9
glibc-common-2.3.4-2.9
gnome-libs-1.4.1.2.90-44.1
libstdc++-3.4.3-22.1
libstdc++-devel-3.4.3-22.1
make-3.80-5
numactl-0.6.4.i386
pdksh-5.2.14-30
sysstat-5.0.5-1
xscreensaver-4.18-5.rhel4.2
setarch-1.6-1
```

- 3 Create a UNIX group and UNIX user account for the Oracle database owner by using the following commands:

Add a *dba* group (as *root*):

```
groupadd oinstall
groupadd dba
```

- 4 Add the Oracle user (as *root*):

```
useradd -g oinstall -G dba -d /opt/oracle/product/<10.2.0.3>/db_1 -m
oracle
passwd oracle
```

- 5 Create directories for *ORACLE\_HOME* and *ORACLE\_BASE* as the *oracle* user:

```
mkdir -p /opt/oracle/product/<10.2.0.3>
```

- 6 Open the *.bash\_profile* file (in *oracle* user home directory) for editing, and append the following:

```

# User specific environment and startup programs
ORACLE_BASE=/opt/oracle; export ORACLE_BASE
ORACLE_HOME=$ORACLE_BASE/product/10.2.0/db_1; export ORACLE_HOME
ORACLE_TERM=xterm; export ORACLE_TERM
PATH=$ORACLE_HOME/bin:$PATH; export PATH
ORACLE_SID=oracle; export ORACLE_SID
LD_LIBRARY_PATH=$ORACLE_HOME/lib; export LD_LIBRARY_PATH
CLASSPATH=$ORACLE_HOME/jre:$ORACLE_HOME/jlib:$ORACLE_HOME/rdbms/jlib
CLASSPATH=$CLASSPATH:$ORACLE_HOME/network/jlib; export CLASSPATH
LD_ASSUME_KERNEL=2.4.19; export LD_ASSUME_KERNEL
TMP=/tmp; export TMP
TMPDIR=$TMP; export TMPDIR
PATH=$PATH:$HOME/bin
export PATH

unset USERNAME

```

---

**IMPORTANT:** This set of environment variables must only be used for the oracle user. These variables should not be set in the system environment or in the Sentinel Administrator User environment.

---

**7** Save the `.bash_profile` and exit.

**8** Log in as oracle user to load the environment variables you added in [Step 6](#).

```

exit
su - oracle

```

**9** Check the environment variables by using the following command:

```

set | more

```

**10** Log in as the oracle user. If you are using X emulation, set the `DISPLAY` environmental variable:

```

DISPLAY=<machine-name>:0.0; export DISPLAY

```

**11** Change to database directory and run the following script:

```

./runInstaller

```

**12** When you proceed through the installation, leave all the prompts at their default values except the ones specified below:

**12a** In the Welcome window, click *Next*.

**12b** In the File Locations window, select `ORACLE_BASE` and `ORACLE_HOME` from the drop-down list for the *Destination Name*, then click *Next*.

**12c** In the Select Product to Install window, select either the Oracle 10g Database or 10.2.0.1, then click *Next*.

**12d** In the Installation Types window, select *Enterprise Edition*, then click *Next*.

**12e** In the Database Configuration window, select *General Purpose*, then click *Next*.

**12f** In the Summary window, review the installation summary, then click *Install*.

**12g** In the End of Installation window, click *Exit*.

**13** To apply the Oracle 10.2.0.3 patch, change to database directory and run the following script:

```

./runInstaller

```

**14** Follow the prompts in the Installation windows. In the Summary window, review the installation summary and click *Install*. In the End of Installation window, click *Exit*.

## B.3.3 Oracle 10g Installation on Solaris 10

---

**NOTE:** For more information on kernel parameter settings in Solaris 10, see [Section B.4.1, “Setting Kernel Values,”](#) on page 160.

---

- 1 Log in as `root`.
- 2 Start the installation

```
# su - oracle
# < Installation directory or CD mount>/ .runInstaller
```
- 3 In the Welcome window:
  - 3a Select *Basic Installation*.
  - 3b Deselect the *Create Starter Database* option.
  - 3c Specify the Oracle Home Location.
  - 3d Specify the oracle DBA group, then click *Next*.
- 4 In the Product-Specific Prerequisite window, verify that all systems checks were successful, then click *Next*
- 5 In the Summary window, review the install summary and click *Install*.
- 6 In the End of Installation window, click *Exit*.

## B.4 Configuring the System for Oracle Database Installation

An experienced DBA should install Oracle. In addition to the recommendations from the DBA, Novell also has some recommendations for installing Oracle. These recommendations are in the following areas:

- ♦ [Section B.4.1, “Setting Kernel Values,”](#) on page 160
- ♦ [Section B.4.2, “Creating Group and User Accounts for Oracle \(Solaris Only\),”](#) on page 163
- ♦ [Section B.4.3, “Setting Environment Variables for Oracle \(Solaris Only\),”](#) on page 163
- ♦ [Section B.4.4, “Installing Oracle,”](#) on page 163

### B.4.1 Setting Kernel Values

---

**IMPORTANT:** The kernel values suggested in this section are minimum values only. These settings should be changed only if your system settings are lower than the recommended minimum values, and only after consulting your system administrator and Oracle documentation. For more information, see [the Oracle Web site \(http://www.oracle.com/technology/documentation/database.html\)](http://www.oracle.com/technology/documentation/database.html). This URL was current at the time of publishing the document.

---

- ♦ [“Linux”](#) on page 160
- ♦ [“Solaris 10”](#) on page 161

#### Linux

- 1 Log in as `root`.



- 2 Back up `/etc/sysctl.conf`.
- 3 Using a text editor, change the kernel parameters by appending the following text to the `/etc/sysctl.conf` file:

The kernel settings below are minimal recommended settings. These settings can be increased if the machine hardware can support it.

To determine your current setting for a particular kernel parameter, execute the command:

```
sysctl <kernel_parameter>
```

For example, to check the current value of the kernel parameter `kernel.sem`, execute the command: `sysctl kernel.sem`

On SUSE Linux 10 SP2:

```
# Oracle requires MLOCK privilege for hugetlb memory.
vm.disable_cap_mlock=1
```

On Red Hat Linux 4:

```
# Kernel settings for Oracle
kernel.core_uses_pid = 1
kernel.shmall = 2097152
kernel.shmmax = 2147483648
kernel.shmmni = 4096
kernel.sem = 250 32000 100 128
fs.file-max = 65536
net.ipv4.ip_local_port_range = 1024 65000
net.core.rmem_default = 262144
net.core.rmem_max = 262144
net.core.wmem_default = 262144
net.core.wmem_max = 262144
```

- 4 Execute the following command to load the modifications to the `/etc/sysctl.conf` file:

```
sysctl -p
/sbin/sysctl -p (on Red Hat Linux4)
```

- 5 Set the file handles and process limits by appending the following text to the `/etc/security/limits.conf` file. `nproc` is the maximum limit on the number of processes and `nofile` is the maximum limit on the number of open files. These are the recommended values, but they can be modified if needed. The following is an example if your Oracle userid is `oracle`.

```
# Settings added for Oracle
oracle      soft    nofile   65536
oracle      hard    nofile   65536
oracle      soft    nproc    16384
oracle      hard    nproc    16384
```

## Solaris 10

Oracle 10g

---

```
noexec_user_stack=1                semsys:seminfo_semvmx=32767
semsys:seminfo_semmni=100          shmsys:shminfo_shmmax=4294967295
semsys:seminfo_semmns=1024        shmsys:shminfo_shmmni=100
semsys:seminfo_semmsl=256
```

---

- 1 By default, Oracle instances are run as the `oracle` user of the `dba` group. A project with the `group.dba` name is created to serve as the default project for the `oracle` user. Run the `id` command to verify the default project for the `oracle` user.

```
# su - oracle
$ id -p
uid=100(oracle) gid=100(dba) projid=100(group.dba)
$ exit
```

- 2 To set the maximum shared memory size to 2 GB, run the `projmod` command

```
# projmod -sK "project.max-shm-memory=(privileged,2G,deny)" group.dba
```

Alternatively, add the `project.max - shm-memory=(privileged,2147483648,deny)` resource control to the last field of the project entries for the Oracle project.

- 3 After these steps are complete, the `/etc/project` file should contain the following:

```
# cat /etc/project
```

The following is the output of the command:

```
system:0::::
user.root:1::::
noproject:2::::
default:3::::
group.staff:10::::
group.dba:100:Oracle default
project:::project.max-shmmemory=(privileged,2147483648,deny
```

- 4 To verify that the resource control is active, run the `id` and `prctl` commands:

```
# su - oracle
$ id -p
uid=100(oracle) gid=100(dba) projid=100(group.dba)
$ prctl -n project.max-shm-memory -i process $$
process: 5754: -bash
NAME PRIVILEGE VALUE FLAG ACTION RECIPIENT
project.max-shm-memory
privileged 2.00GB - deny
```

## Oracle 11g

For information on setting the kernel values for Oracle 11g, see [Section B.1, “Installing Oracle 11g,”](#) on page 149 in [Appendix B, “Oracle Setup,”](#) on page 149.

---

**NOTE:** For additional information, see the [Oracle documentation for Solaris 10 installation \(http://www.oracle.com/technology/documentation/database.html\)](http://www.oracle.com/technology/documentation/database.html). This URL was current at the time of publication of the document.

---

## B.4.2 Creating Group and User Accounts for Oracle (Solaris Only)

- 1 Log in as root.
- 2 Create a UNIX group and UNIX user accounts for the Oracle database owner.
  - ♦ Add a dba group (as root):

```
groupadd -g 400 dba
```
  - ♦ Add the oracle user (as root) for the csh shell:

```
useradd -g dba -d /export/home/oracle -m -s /bin/csh oracle
```
  - ♦ Add the oracle user (as root) for the bash shell:

```
useradd -g dba -d /export/home/oracle -m -s /bin/bash oracle
```

## B.4.3 Setting Environment Variables for Oracle (Solaris Only)

- 1 Log in as root.
- 2 To set the necessary environment variables for Oracle in the csh shell, add the following information to the local.cshrc file:

```
setenv ORACLE_HOME /opt/oracle
setenv ORACLE_SID ESEC
setenv LD_LIBRARY_PATH ${ORACLE_HOME}/lib
setenv DISPLAY :0.0
set path=(/bin /bin/java /usr/bin /usr/sbin ${ORACLE_HOME}/bin /usr/ucb/
etc.)
if ( $?prompt ) then
set history=32
endif
```

- 3 To set the necessary environment variables for Oracle in the bash shell, add the following information to the .profile file in the \$ORACLE\_HOME directory:

```
setenv ORACLE_HOME /opt/oracle
setenv ORACLE_SID ESEC
setenv LD_LIBRARY_PATH ${ORACLE_HOME}/lib
setenv DISPLAY :0.0
set path=(/bin /bin/java /usr/bin /usr/sbin ${ORACLE_HOME}/bin /usr/ucb/
etc.)
if ( $?prompt ) then
set history=32
endif
```

## B.4.4 Installing Oracle

To install Oracle, see [Appendix B, “Oracle Setup,” on page 149](#). This section describes installation settings recommended for Sentinel operations. It also describes the procedures for creating the Oracle instance. (Novell recommends creating the instance by using the Sentinel installer, but provides instructions if corporate policy requires that the DBA create the instance manually.)

## B.5 Manual Oracle Instance Creation (Optional)

Novell recommends using the Sentinel installer to create the Oracle instance during the Sentinel database components installation. Sentinel 6.1 supports both dedicated server and shared server connection with Oracle. However, performance is better in a dedicated server connection when compared to a shared server connection. This procedure is applicable if it is a corporate policy that the DBA create the Oracle instance. The tablespaces must be named exactly as specified.

- 1 Log in as an Oracle user.
- 2 Use the Oracle Database Assistant GUI to create the following:

The database initialization parameter values might vary depending on your system configuration and requirements. Consult your DBA.

Oracle 11g Parameters	Value
memory_max_target	700MB
memory_target	650MB
open_cursors	500
cursor_sharing	SIMILAR
optimizer_index_caching	50
optimizer_index_cost_adj	55
nls_length_semantics	CHAR
job_queue_processes	10

Oracle 10g Parameters	Value
db_cache_size	1 GB
java_pool_size	33,554,432
large_pool_size	8,388,608
shared_pool_size	100 MB
pga_aggregate_target	150,994,944
sort_area_size	109,051,904
open_cursors	500
cursor_sharing	SIMILAR
optimizer_index_caching	50
optimizer_index_cost_adj	55
nls_length_semantics	CHAR
job_queue_processes	10

- 3 Create Sentinel tablespaces.

For more information, see [Section C.1.2, “Creating the Sentinel Tablespaces,”](#) on page 170.

- 4** Run the `createEsecdba.sh` script found in the `sentinel\dbsetup\bin` directory on the Sentinel Installation CD.

This script creates the user `esecdba`, which is required to add the database objects through the Sentinel installer.

- 5** Back up the database.

For more information on installing the Sentinel database on Oracle database, see [Section 3.6, “Custom Installation,”](#) on page 39.



# Sentinel with Oracle Real Application Clusters



Sentinel 6.1 is certified to run on an Oracle database with Real Application Clusters (RAC). The supported Oracle database versions are Oracle 10g and Oracle 11g Release 2 (64-bit) with Real Application Clusters (RAC).

In addition to the standard installation procedures for Sentinel, there are a few additional steps to install and configure Sentinel to use Oracle RAC:

- ♦ [Section C.1, “Configuring the Oracle RAC Database,” on page 167](#)
- ♦ [Section C.2, “Installing the Sentinel Database,” on page 171](#)
- ♦ [Section C.3, “Configuring the Connection Properties File,” on page 173](#)
- ♦ [Section C.4, “Configuring the Connection for Sentinel Data Manager,” on page 174](#)
- ♦ [Section C.5, “Configuring the Connection for Crystal Enterprise Server,” on page 174](#)

---

**NOTE:** Before installing Sentinel 6.1 software, use the Oracle RAC tools and ensure that the Oracle cluster is up and running.

---

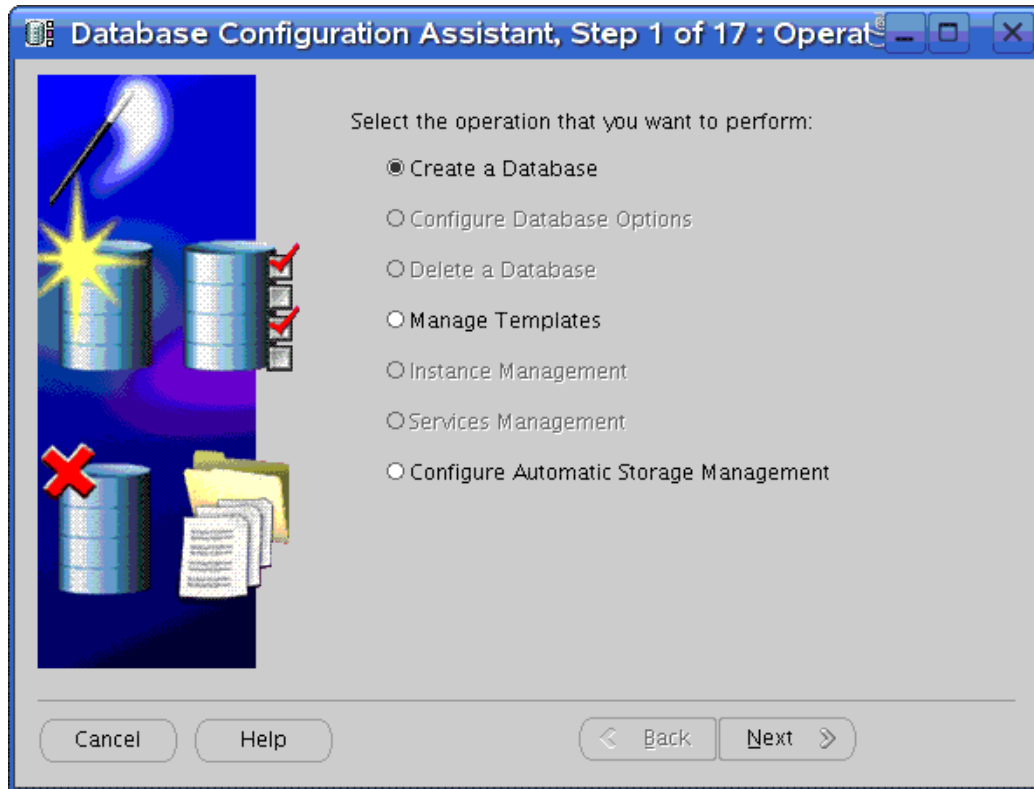
## C.1 Configuring the Oracle RAC Database

- ♦ [Section C.1.1, “Creating the RAC Database,” on page 167](#)
- ♦ [Section C.1.2, “Creating the Sentinel Tablespaces,” on page 170](#)
- ♦ [Section C.1.3, “Creating the Sentinel Database User,” on page 171](#)

### C.1.1 Creating the RAC Database

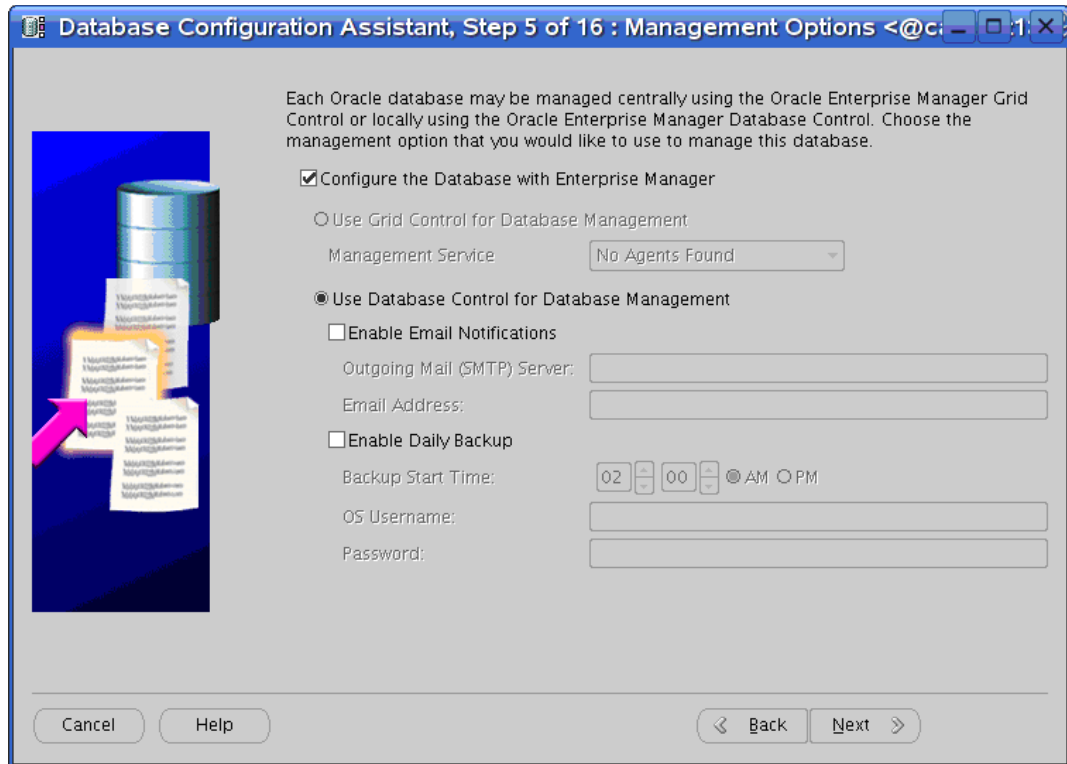
Perform the following steps to create an empty Oracle RAC database by using the Oracle Database Configuration Assistant (DBCA) utility for installing the Sentinel components.

- 1 Run the DBCA utility.
- 2 Select the *Oracle Real Application Clusters* database under *Database Configuration Assistant*. Click *Next*.
- 3 Select *Create a database*, then click *Next*.

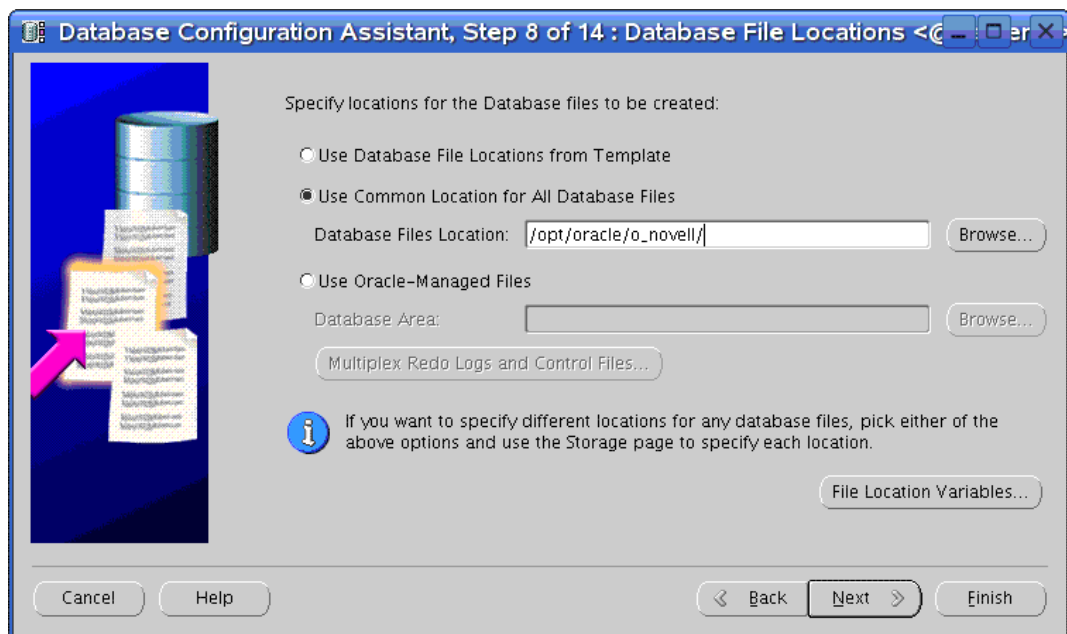


- 4 To select all the nodes to create a cluster database, click *Select All*, then click *Next*.
- 5 From the list of templates, select a template. By default, *General Purpose* is selected. Click *Next*.
- 6 Specify the database name and SID (Oracle System Identifier), then click *Next*.
- 7 Make sure the *Configure the Database with Enterprise Manager* option is selected, then click *Next*.





- 8 You can use the same passwords for all user accounts or you can use different passwords. Select your option and specify the passwords, then click *Next*.
- 9 From the three storage mechanisms offered by the system (*Cluster File System*, *Automatic Storage Management*, and *Raw Devices*), select your option. If you chose *Raw Devices*, specify the path to the Raw Devices mapping file. Click *Next*.
- 10 Specify a directory to store the database files on the storage system, then click *Finish*.



11 Retain the default selection in the *Recovery options* and *Sample Schemas* windows, then click *Next*.

You can create a Database Service or you can create the service later by using DBCA.

12 In the *Database storage* window, retain the default selection, then click *Next*.

13 From the *Database creation* options, select *Create Database*, then click *Finish*.

## C.1.2 Creating the Sentinel Tablespaces

---

**IMPORTANT:** The Sentinel installation will be successful only if all the tablespaces mentioned in [Table C-1 on page 170](#) are created. You can use Oracle Enterprise Manager or an SQL query to verify the existence of these tablespaces.

---

**Table C-1** *Minimum Recommended Tablespace Size*

Tablespace	Minimum Recommended Size with Autoextend Enabled	Comments
REDO	3 x 100MB	You should create larger redo logs if the event rate is high. A minimum of three redo log groups is required.
SYSTEM	500MB	Stores information about internal tables and indexes of the database.
TEMP	1GB	Used for temporary operations like sorting and storing temporary information of a session.
UNDO	1GB	Stores the information required for rollback and undo operations.
ESENTD	5GB	Stores the event data.
ESENTD2	500MB	Stores information about configuration, assets, vulnerability, and associations.
ESENTWFD	250MB	Stores information about iTRAC data
ESENTWFX	250MB	Stores information about iTRAC indexes
ESENTX	3GB	Stores information about event indexes
ESENTX2	500MB	Stores information about indexes for configuration, assets, vulnerability, and associations.
SENT_ADVISORD	15GB	Stores information about the Advisor data
SENT_ADVISORX	15GB	Stores information about the Advisor indexes
SENT_AUDITD	250MB	Stores information about the Sentinel audit data
SENT_AUDITX	250MB	Stores information about the Sentinel audit indexes

Tablespace	Minimum Recommended Size with Autoextend Enabled	Comments
SENT_LOBS	100MB	Stores information about the database large objects This is the minimum value in a basic installation.
	2GB	This is the minimum value if the Sentinel installation is integrated with the identity management system enabled.
SENT_SMRYD	3GB	Stores the summary data for aggregation
SENT_SMRYX	2GB	Stores the summary indexes for aggregation
SYSAUX	100MB	Stores information about internal tables and indexes of the database for performance and other statistics. This tablespace is for Oracle 10g/11g (not Sentinel specific).

### C.1.3 Creating the Sentinel Database User

The username for the Sentinel schema owner is `esecdba`. Most of the objects that are created by the Sentinel installer are owned by this user.

- 1 Locate the Sentinel `createEsecdba.sh` script on the Sentinel installation disk at `disk1/sentinel/dbsetup/bin`.
- 2 Run this script from any machine with the Oracle client installed.

You must set the `ORACLE_SID` value to the instance value of a particular node on which you are running the script. For example, in a two-node cluster, you can set `ORACLE_SID = ESEC1`. You might also need to edit the script to properly set the Oracle environment variables and the `CONNECT AS` string (by default, the script connects as `sysdba`).

```

oracle@ca-sent1:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
oracle@ca-sent1:~> ksh createEsecdba.sh
Please enter esecdba password: novell
Please enter temporary tablespace name: TEMP
"Creating ESECDBA database user..."

User created.

Grant succeeded.

Grant succeeded.

Grant succeeded.

Grant succeeded.

```

## C.2 Installing the Sentinel Database

After the Oracle database is configured, you must install the Sentinel database. The database is installed to a single-cluster node as if it is a non-RAC Oracle instance.

You can run the Sentinel installer from any machine with the Oracle client installed, as long as the system has the proper Oracle environment variables set for the `oracle` user (`ORACLE_HOME`, `ORACLE_BASE`). If the machine is a Sentinel server, you can install the Sentinel components as mentioned in [Step 9 on page 172](#).

- 1** Log in to the installation server as the `root` user.
- 2** Insert and mount the Sentinel installation CD or fileset.
- 3** Browse to the CD:
  - For GUI mode, double-click:

```
./setup.sh
```
  - For textual (headless) mode, run:

```
./setup.sh -console
```
- 4** Select the language and click *OK*.
- 5** Read the Welcome screen, then click *Next*.
- 6** Read and accept the End User License Agreement, then click *Next*.
- 7** Accept the default installation directory or click *Browse* to specify a different location, then click *Next*.
- 8** Specify the type of installation, select *Custom* (default), then click *Next*.
- 9** In the Feature Selection window, deselect the options that are not required, select *Database*, then click *Next*.
- 10** Select the target database server platform:
  - 10a** Select *Oracle 10g* or *Oracle 11g* from the drop-down list.
  - 10b** Select *Add database objects to an existing database*.
- 11** Click *Next*.
- 12** Provide the authentication information for creating the Sentinel Application Database User and the Sentinel Administration User, then click *Next*.

A summary of the Database parameters is displayed.
- 13** Click *Next*.

The Installation Summary is displayed.
- 14** Click *Install*.
- 15** After the installation is complete, click *Finish*.
- 16** Install the rest of the Sentinel system components, including Collector Services, DAS, and the Communication Server.

For more information on installing these components, see [Chapter 3, “Installing Sentinel 6.1 SP2,” on page 27](#).

## C.3 Configuring the Connection Properties File

You need to manually create a database connection property file with the RAC database connection information. The database connection property file should be created on the same machine where DAS (Data Access Services) is installed. Some of the necessary information can be found in the `$ORACLE_HOME/network/admin/tnsnames.ora` file on the cluster nodes.

- 1 Log in to the machine where the Sentinel Data Access Service (DAS) components are installed.
- 2 Change to the `$ESEC_HOME/config` directory.
- 3 Create the `RACconnect.properties` file.

The following is a sample configuration for a service called OLTP with three nodes:

```
driver=esecurity.base.db.driver.OracleProxyDriver
dburl=jdbc:esecurity:oracleproxy:@
realdriver=oracle.jdbc.driver.OracleDriver
realdburl=jdbc:oracle:thin:@
fatalvendorstates=28,600,1012,1014,1033,1034,1035,1089,1090,1092,1094,239
6,3106,3111,3113,3114
advancedconnectionstring=(DESCRIPTION=
(AADDRESS= (PROTOCOL=TCP) (HOST=ca-sent1.novell.com) (PORT=1521))
(AADDRESS= (PROTOCOL=TCP) (HOST=ca-sent2.novell.com) (PORT=1521))
(AADDRESS= (PROTOCOL=TCP) (HOST=ca-sent3.novell.com) (PORT=1521))
(LOAD_BALANCE=yes)
(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=OLTP)
(FAILOVER_MODE=(TYPE=SELECT)(METHOD=BASIC)(RETRIES=180)(DELAY=5))))
```

---

**NOTE:** The entire `advancedconnectionstring` should be on a single line.

---

- 4 Edit the `configuration.xml` file in `$ESEC_HOME/config` and add the following argument to the process components:

```
-Desecurity.connect.config.file=../config/RACconnect.properties
```

The process components that need changes are:

- ♦ DAS\_Aggregation
- ♦ DAS\_Binary
- ♦ DAS\_iTRAC
- ♦ DAS\_Query
- ♦ DAS\_RT

For example:

```
<process component="DAS"depends="UNIX Communication Server,Windows
Communication Server" image="$(ESEC_JAVA_HOME)/java" -server -
Dsrv_name=DAS_Query
-Xmx256m -Xms85m -XX:+UseParallelGC -Xss136k -Xrs
-Duser.language=en -Dfile.encoding=UTF8
-Desecurity.dataobjects.config.file=/xml/BaseMetaData.xml,
/xml/WorkflowMetaData.xml
-Djava.util.logging.config.file=../config/das_query_log.prop
-Djava.security.auth.login.config=../config/auth.login
```

```
-Djava.security.krb5.conf=../config/krb5.conf
-Desecurity.execution.config.file=../config/execution.properties -
Dcom.esecurity.configurationfile=../config/configuration.xml
-Desecurity.connect.config.file=../config/RACconnect.properties
-jar ../lib/ccsbase.jar ../config//das_query.xml" min_instances="1"
name="DAS_Query" post_startup_delay="20" type="container"
working_directory="$(ESEC_HOME)/data" />
```

- 5 Restart the Sentinel services for the database connection changes to take effect.

## C.4 Configuring the Connection for Sentinel Data Manager

The `advancedconnectionstring` value from the `RACconnect.properties` file enables you to log in to Sentinel Data Manager.

To log in to Sentinel Data Manager:

- 1 Launch Sentinel Data Manager from `$ESEC_HOME/bin/sdm`.
- 2 Specify the username and password for the Sentinel Database Administrator (`esecdba` by default).
- 3 Copy the `advancedconnectionstring` value from the `RACconnect.properties` file.
- 4 Paste the `advancedconnectionstring` value into the `Connection String` field.
- 5 Select *Save connection settings*.
- 6 Click *Connect*.

### C.4.1 Known Issue

**Issue:** Unable to connect to Oracle RAC database through Sentinel Data Manager.

**Workaround:** When you log in to Sentinel Data Manager for the first time, select *Oracle* as the *Server* option, and select *Save connection settings*, using any of the RAC node information. After the login succeeds, select *OracleRAC* as the *Server* option and connect to Sentinel Data Manager.

## C.5 Configuring the Connection for Crystal Enterprise Server

For Crystal Enterprise Server to use the Oracle RAC database, you must edit the `tnsnames.ora` file.

---

**NOTE:** The steps in the standard installation for Crystal Enterprise Server must be followed before performing this step. For more information on installing Crystal Enterprise Server, see [Chapter 8, “Crystal Reports for Linux,”](#) on page 121.

---

To edit the `tnsnames.ora` file:

- 1 Log in to the server with Crystal Enterprise Server installed and locate the `tnsnames.ora` file.
- 2 Modify the `ESECURITYDB` service to show the TNS information for all of the nodes. The IP address must be the virtual IP address.

A sample file for a system with three nodes is shown below:

```
ESECURITYDB =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = 10.0.0.1)(PORT = 1521))
    (ADDRESS = (PROTOCOL = TCP)(HOST = 10.0.0.2)(PORT = 1521))
    (ADDRESS = (PROTOCOL = TCP)(HOST = 10.0.0.3)(PORT = 1521))
    (LOAD_BALANCE = yes)
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = REPORT.novell.com)
      (FAILOVER_MODE =
        (TYPE = SELECT)
        (METHOD = BASIC)
        (RETRIES = 180)
        (DELAY = 5)
      )
    )
  )
)
```

