Novell® Sentinel™

6.0.3

www.novell.com

Volume I - INSTALLATION GUIDE

November 2009

Novell®

Legal Notices

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

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

Novell Trademarks

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

Third-Party Materials

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

Third Party Legal Notices

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

- edtFTPj-1.2.3 is licensed under the Lesser GNU Public License. For more information, disclaimers and restrictions see http://www.enterprisedt.com/products/edtftpj/purchase.html.
- Enhydra Shark, licensed under the Lesser General Public License available at: http://shark.objectweb.org/license.html.
- Esper. Copyright © 2005-2006, Codehaus.
- FESI is licensed under the Lesser GNU Public License. For more information, disclaimers and restrictions, see http://www.lugrin.ch/fesi/index.html.
- jTDS-1.2.2.jar is licensed under the Lesser GNU Public License. For more information, disclaimers and restrictions see http://jtds.sourceforge.net/.
- MDateSelector. Copyright © 2005, Martin Newstead, licensed under the Lesser General Public License. For more information, disclaimers and restrictions see http://web.ukonline.co.uk/mseries.
- Tagish Java Authentication and Authorization Service Modules, licensed under the Lesser General Public License. For more information, disclaimers and restrictions see http://free.tagish.net/jaas/index.jsp.

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

- Apache Axis and Apache Tomcat, Copyright © 1999 to 2005, Apache Software Foundation. For more information, disclaimers and restrictions, see http://www.apache.org/licenses/.
- Apache FOP.jar, Copyright 1999-2007, Apache Software Foundation. For more information, disclaimers and restrictions, see http://www.apache.org/licenses/.
- Apache Lucene, Copyright © 1999 to 2005, Apache Software Foundation. For more information, disclaimers and restrictions, see http://www.apache.org/licenses/.
- Bean Scripting Framework (BSF), licensed by the Apache Software Foundation Copyright © 1999-2004. For more information, disclaimers and restrictions see http://xml.apache.org/dist/LICENSE.txt.
- Skin Look and Feel (SkinLF). Copyright © 2000-2006 L2FProd.com. Licensed under the Apache Software License. For more information, disclaimers and restrictions see https://skinlf.dev.java.net/.
- Xalan and Xerces, both of which are licensed by the Apache Software Foundation Copyright © 1999-2004. For more information, disclaimers and restrictions see http://xml.apache.org/dist/LICENSE.txt.

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

- JavaBeans Activation Framework (JAF). Copyright © Sun Microsystems, Inc. For more information, disclaimers and restrictions see http://www.java.sun.com/products/javabeans/glasgow/jaf.html and click download > license.

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

Preface

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

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

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

Volume I – Sentinel Install Guide

This guide explains how to install:

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

Volume II – Sentinel User Guide

This guide discusses:

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

Volume III – Collector Builder User Guide

This guide discusses:

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

Volume IV - Sentinel User Reference Guide

This guide discusses:

- Collector scripting language
- Collector parsing commands
- Collector administrator functions
- Collector and Sentinel meta-tags
- Sentinel correlation engine
- User Permissions
- Correlation command line options
- Sentinel database schema

Volume V - Sentinel 3rd Party Integration Guide

- Remedy
- HP OpenView Operations
- HP Service Desk

Volume VI - Sentinel Patch Installation Guide

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

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

The other manuals on this product are available at http://www.novell.com/documentation. The additional documentation available on Sentinel:

- Sentinel 6.0 Installation Guide
- Sentinel 6.0 Patch Installation Guide
- Sentinel 6.0 Reference Guide

Documentation Conventions

The following are the conventions used in this manual:

- Notes and Warnings

NOTE: Notes provide additional information that may be useful or for reference.

WARNING:

Warnings provide additional information that helps you identify and stop performing actions in the system that cause damage or loss of data.

- Commands appear in courier font. For example:

```
useradd –g dba –d /export/home/oracle –m –s
/bin/csh oracle
```

- Go to Start > Program Files > Control Panel to perform this action: Multiple actions in a step.
- References
  - For more information, see "Section Name" (if in the same Chapter).
  - For more information, see Chapter number, "Chapter Name" (if in the same Guide).
  - For more information, see Section Name in Chapter Name, *Name of the Guide* (if in a different Guide).

Other Novell References

The following manuals are available with the Sentinel install CDs.

- Sentinel User Guide
- Sentinel Collector Builder User Guide
- Sentinel User Reference Guide
- Sentinel 3rd Party Integration Guide
- Release Notes

Contacting Novell

- Website: http://www.novell.com
- Novell Technical Support: http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup
- Self Support: http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog
- Patch Download Site: http://download.novell.com/index.jsp
- 24x7 support: http://www.novell.com/company/contact.html.
- For Collectors/Connectors/Reports/Correlation/Hotfixes/TIDS: http://support.novell.com/products/sentinel.

Contents

1 Introduction

The following sections will walk you through a basic installation. 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.

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 incorporate Sentinel correlation rules, dynamic lists, maps, reports, and iTRAC workflows into controls. These controls are typically designed to meet specific regulatory requirements, such as the Payment Card Industry Data Security Standard.

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 Management.

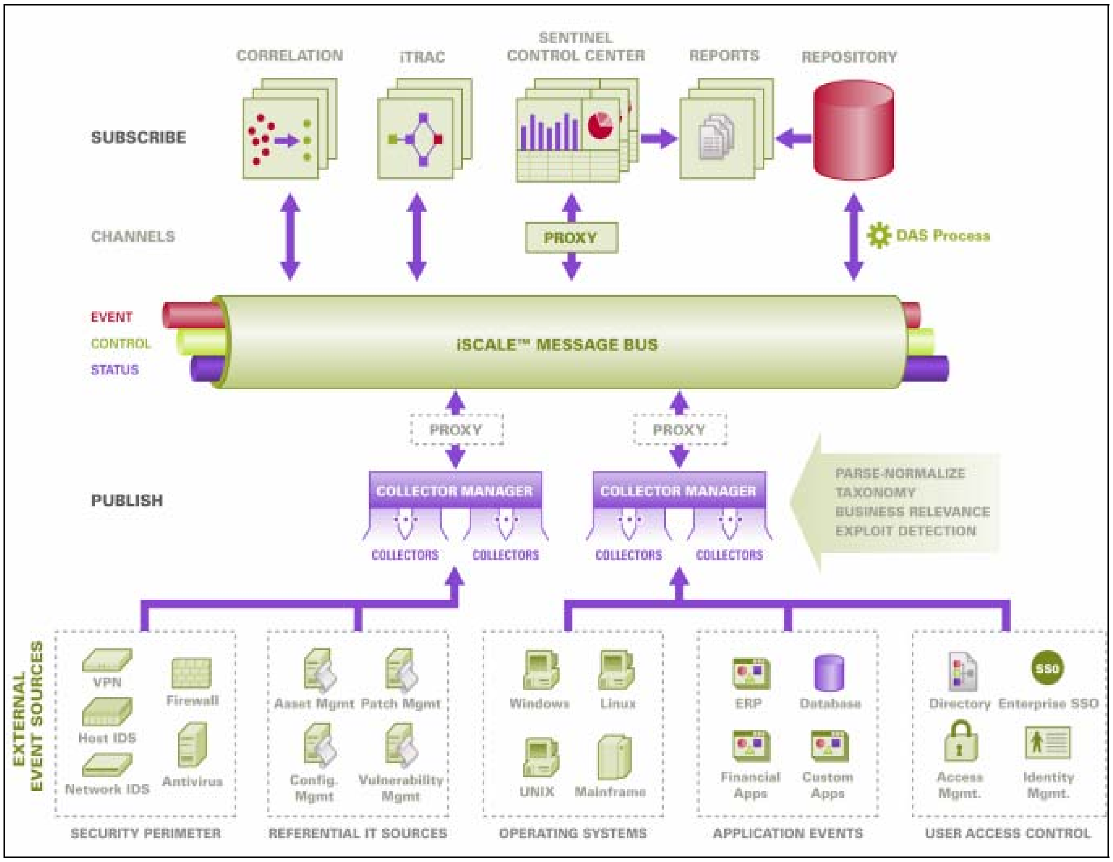


Figure 1-1: *Conceptual Architecture of Sentinel*

Sentinel is composed of multiple components:

- Sentinel Server
- Sentinel Communication Server
- Correlation Engine
- iTRAC™
- Sentinel Database
- Sentinel Collector Manager

- Sentinel Collectors
- Sentinel Control Center
- Sentinel Collector Builder
- Sentinel Data Manager
- Crystal Reports Server*
- Sentinel Advisor
- Third-Party Integration
  - HP* OpenView *Operations
  - HP* Service Desk
  - Remedy *

Sentinel Server

Sentinel Server is made up of several components that perform the core event-processing services. This includes receiving events from the *Collector Managers*, storing them in the database, filtering, processing *ActiveView* displays, performing database queries and processing results, and managing administrative tasks such as user authentication and authorization.

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.

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.

iTRAC Workflow

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.

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.

Sentinel Collector Manager

Collector Manager manages the Collectors, 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.

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

You can download existing device-specific Collectors from the Novell Product site (http://support.novell.com/products/sentinel/collectors.html). Collectors can be built or modified in "Collector Builder", a standalone application included with the Sentinel system.

Sentinel Control Center

The 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

Sentinel Collector Builder

The Sentinel Collector Builder enables you to build Collectors. You can create and customize the templates so that the Collector can parse the data.

Sentinel Data Manager

The 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

Crystal Reporting Server

Comprehensive reporting services within the Sentinel Control Center are powered by Crystal Enterprise and Crystal Report 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 Report Developer, new customized reports can also be developed against the Sentinel published report view schema.

Sentinel Advisor

Sentinel Advisor is an optional add-on module that cross-references the Sentinel real-time alert data with known vulnerabilities and remediation information.

Third-Party Integration

Sentinel uses third-party API plug-ins to integrate with the following systems:

- HP OpenView Operations
- HP Service Desk
- Remedy AR

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.
- At this time, the *Collector Managers* can only process ASCII and extended ASCII data (that is, not double-byte or unicode data).
- Collectors built by Novell are designed to parse English events.
- Internal events (to audit Sentinel operations) are in English only.

2 Supported Platforms and Best Practices

Supported Software

For best performance and reliability, Novell strongly recommends that customers install all Sentinel components on approved software, as listed below, that have been fully quality assured and certified. For the most up-to-date information, see documentation at the Novell Documentation site (http://www.novell.com/documentation).

Operating Systems

Sentinel components (including the database) are certified to run on the following operating systems. Novell recommends that you check with the respective vendors for security updates and patches.

- SUSE® Linux Enterprise Server 9 (32-bit)
- SUSE Linux Enterprise Server 10 (32- or 64-bit)
- Red Hat* Enterprise* Linux 3 Update 5 ES (32-bit)
- Red Hat Enterprise Linux 4 (64-bit)
- Sun* Solaris* 9 (64-bit SPARC*)
- Sun Solaris 10 (64-bit SPARC)
- Windows 2003, Standard or Enterprise Edition (32-bit)
- Windows XP (32-bit) (for Sentinel Control Center, Collector Builder, and Sentinel Data Manager only)
- Windows 2000, Standard or Enterprise Edition (32-bit) (for Sentinel Control Center, Collector Builder, and Sentinel Data Manager only)

Databases

Sentinel is certified to run with the following databases:

- Oracle* 10g Enterprise Edition with partitioning (v 10.2.0.3 with Oracle critical patch #5881721) (32- or 64-bit)
- Oracle 9i Enterprise Edition with partitioning (v 9.2.0.7 p. 5490841) (64-bit)
- Microsoft* SQL Server* 2005 SP1 (v.9.00.2047), Standard or Enterprise Edition (32-bit)
- Microsoft SQL Server 2005 SP1 (v.9.00.2047), Standard or Enterprise Edition (64-bit)

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).

Report Server

The supported reporting server is Crystal Enterprise Server XI R2, which can be run on any of the following platforms in the Sentinel environment:

- Windows 2003 SP1 Server, Standard or Enterprise Edition (32-bit)
    - Crystal database on Microsoft SQL 2005
    - Web server on Microsoft IIS with .NET
- Red Hat Enterprise Linux 4 (32-bit)
    - Crystal database on MySQL
    - Web server on Apache Tomcat
- SuSE Linux Enterprise Server 9 SP2 (32-bit)
    - Crystal database on MySQL
    - Web server on Apache Tomcat

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

Platform Support Exceptions

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

- Business Objects does not currently support Crystal Reports Server XI R2 on Solaris or SUSE Linux Enterprise Server 10
- Oracle does not currently support Oracle 9 (32-bit) on SUSE Linux Enterprise Server 10 (32-bit or 64-bit)
- Oracle does not currently support Oracle 10 (32-bit) on 32-bit Solaris (9 or 10)

Although the following platform configurations might be supported by their respective vendors, Novell recommends against these configurations in a Sentinel environment:

- Sentinel 6 on SUSE Linux Enterprise Server 9 or 10 running with the ReiserFS filesystem
- Oracle database on Microsoft Windows
- Crystal Reports Server on Microsoft 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 may or may not be able to support that configuration.

- Because the Sentinel database installation and configuration are platform specific, 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.

- Once the Sentinel system is functional, any database or reporting issue that cannot be duplicated on our 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 (though 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 on Windows platform only.

Hardware Recommendations

When installing 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 operating system, as described above. Sentinel is certified on AMD Opteron and Intel Xeon hardware. Itanium servers are not supported.

For Solaris, the SPARC architecture is supported.

Architecture

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.

There are many factors that should be considered when designing a Sentinel system. Here is a partial list of factors to be considered when developing a design:

- 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 that will 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 will be affected by increasing event rates. In a high event rate environment, the greatest demand will be placed on the database, which is very IO dependent and might be simultaneously handling inserts of hundreds or thousands of events per second, object creation by multiple users, workflow process updates, and simple historical queries from the Sentinel Control Center, and long-term reports from the Crystal Enterprise 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 will meet the I/O requirement based on the event insertion rates.
- A dedicated Database Administrator should regularly evaluate the following aspects of the database:
  - Size
  - I/O operations
  - Disk space
  - Memory
  - Indexing

In low event-rate environments (For example, eps < 25), the above 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 will be stored online in the database.
- Storage space for Advisor data is not included in the specifications in the tables below.
- 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.

NOTE: 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 it is recommended that Novell Consulting Services be consulted prior to finalizing the Sentinel architecture. The recommendations below can be used as a guideline.

NOTE: Because of high event loads and local caching, the Sentinel Server machine with Data Access Server (DAS) is required to have a local or shared striped disk array (RAID) with a minimum of 4 disk spindles.

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 Enterprise 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.

NOTE: The following numbers are based on testing for Sentinel 5.1.3. For updated information, see the Novell Documentation site (http://www.novell.com/documentation/index.html).

1-500 EPS: Two Machine Configuration (Sentinel 5.1.3)			
Components	**RAM**	**Space**	**CPU**
Machine 1: Sentinel Server / Collector Manager ▪ Correlation Engine ▪ DAS ▪ Communication Server ▪ Advisor ▪ Collector Manager / Collectors ▪ Database ▪ Crystal Server (optional for Windows/Linux)	6 GB	300 GB	Windows or Linux - 2 x Dual Core Intel® Xeon® 5150 (2.66 GHz) or Sun Solaris - 4 x UltraSPARC IIIi (1.5 GHz)
Machine 2: Report Server ▪ Crystal Server	2 GB	20 GB	Windows or Linux - 1 x Dual Core Intel® Xeon® 5150 (2.66 GHz)

Table 2-1: *Two Machine Configuration (Sentinel 5.1.3)*

500 – 1500 EPS: Three Machine Configuration (Sentinel 5.1.3)			
Components	**RAM**	**Space**	**CPU**
Machine 1: Sentinel Server / Collector Manager ▪ Correlation Engine ▪ DAS ▪ Communication Server ▪ Advisor ▪ Collector Manager / Collectors	4 GB	90 GB	Windows or Linux - 2 x Dual Core Intel® Xeon® 5160 (3.0 GHz) or Sun Solaris - 2 x 1.8 GHz UltraSPARC IV+
Machine 2: Database ▪ Database ▪ Crystal Server (optional for Windows/Linux)	4 GB+	1 TB+	Windows or Linux - 2 x Dual Core Intel® Xeon® 5160 (3.0 GHz) or Sun Solaris - 2 x 1.8 GHz UltraSPARC IV+
Machine 3: Report Server (needed only if Sentinel/DB are on Solaris) ▪ Crystal Server	2 GB	20 GB	Windows or Linux - 1 x Dual Core Intel® Xeon® 5150 (2.66 GHz)

Table 2-2: *Three Machine Configuration (Sentinel 5.1.3)*

1500 - 3000 EPS: 4-5 Machine Configuration (Sentinel 5.1.3)			
Components	**RAM**	**Space**	**CPU**
Machine 1: Sentinel Server ▪ Correlation Engine ▪ DAS ▪ Communication Server ▪ Advisor	4 GB	90 GB	Windows or Linux - 2 x Dual Core Intel® Xeon® 5160 (3.0 GHz) or Sun Solaris - 2 x 1.8 GHz UltraSPARC IV+
Machine 2: Database	8 GB+	3 TB+	Windows or Linux - 2 x

1500 - 3000 EPS: 4-5 Machine Configuration (Sentinel 5.1.3)

Components	RAM	Space	CPU
▪ Database ▪ Crystal Server (optional for Windows/Linux)			Dual Core Intel® Xeon® 5160 (3.0 GHz) or Sun Solaris - 2 x 1.8 GHz UltraSPARC IV+
Machine 3: Collector Manager ▪ Collector Manager/Collectors	2 GB	20 GB	Windows or Linux - 2 x Dual Core Intel® Xeon® 5160 (3.0 GHz) or Sun Solaris - 2 x 1.8 GHz UltraSPARC IV+
Machine 4: Report Server ▪ Crystal Server	4 GB	20 GB	Windows or Linux - 1 x Dual Core Intel® Xeon® 5150 (2.66 GHz)
Machine 5: Additional instance of DAS_Binary (needed if EPS > 2000) For configuration instructions, see "Adding Sentinel Components."	2 GB	40 GB	Windows or Linux - 2 x Dual Core Intel® Xeon® 5160 (3.0 GHz) Sun Solaris - 2 x 1.8 GHz UltraSPARC IV+

Table 2-3: *4-5 Machine Configuration (Sentinel 5.1.3)*

Performance Benchmarks

The following tables describe several representative configurations and testing results.

These ratings are intended as a reference point to determine architectural design and do not represent hard limits. In these tests, system loads did not exceed 75% utilization, and the event rates represent steady state performance.

NOTE: The benchmarking tests focused on Sentinel event insertions, correlation, and the mapping service. Additional activities, such as reporting or historical data queries, were not included in the testing.

All of the testing below was performed on a system with RAID 5 with striping with a 4+1 configuration.

Proof of Concept or Demonstration Configuration

This single-machine configuration is suitable for demonstrations or limited proofs of concept and can be installed using the "simple" option in the Sentinel installer. This configuration is strongly discouraged for use in a production system.

NOTE: The following numbers are based on testing on Sentinel 5.1.3. For updated information, see the Novell Documentation site (http://www.novell.com/documentation/index.html).

Function	RAM	MODEL
▪ Sentinel Server + DB + Collector Manager	5 GB, 5x36 GB RAID	SLES9 - 2 x Dual Core Intel Xeon 5150 2.66 GHz

Table 2-4: *Single-Machine Configuration*

The following performance metrics were observed on this system.

Attribute	Rating	Comments
▪ Events Per Day (partially processed)	1.7 billion	Includes events that are preprocessed and filtered in addition to events fully processed and stored in the database.
▪ Events Processed and Stored Per Day (in Database)	86 million	
▪ Events Processed Per Second (Collector Manager)	1000	A single CPU (dual core) Xeon was used for the Collector Manager
▪ Events Processed Per Second (Collector Engine)	300	PIX, Snort, and other devices were used with this test
▪ Events Processed Per Second (SYSLOG)	300	One Syslog server was run on the Collector Manager host with 1 Engine
▪ Collectors deployed per Collector Manager	3	One Collector utilized syslog; others were using a File Connector
▪ Number of Collector Managers	1	20 is the maximum number of Collector Managers supported per Sentinel Server
▪ Number of Correlation Engines Deployed	1	Runs on the Sentinel Server machine
▪ Rules deployed per correlation engine	10	
▪ Active Views running	10	
▪ Number of simultaneous users	3	
▪ Number of views per Active View Instance	2	
▪ Number of maps deployed	2	
▪ Size of the largest map in the mapping service	1.5 MB	
▪ Number of rows in the largest map	1.5 million	

Table 2-5: *Performance Metrics*

Production System Configuration – Option 1

This configuration includes three machines and handles approximately 2000 events per second.

NOTE: The following numbers are based on testing on Sentinel 5.1.3. For updated information, see the Novell Documentation site (http://www.novell.com/documentation/index.html).

Function	RAM	MODEL
▪ Sentinel Server	4 GB, 5x36 GB RAID	SLES9 - 2 x Dual Core Intel Xeon 5150 2.66 GHz
▪ Database	4 GB, 5x250 GB RAID	SLES9 - 2 x Dual Core Intel Xeon 5150 2.66 GHz
▪ Collector Manager	2 GIG, 72 GIG	SLES9 - 1 x Dual Core Intel Xeon 5150 2.66 GHz

Table 2-6: *Three Machine Configuration*

The following performance metrics were observed on this system:

Attribute	Rating	Comments
▪ Events Per Day (partially processed)	3.4 billion	Includes events that are preprocessed and filtered in addition to events fully processed and stored in the database.
▪ Events Per Day (fully processed and stored in the database)	173 million	Includes events that are fully parsed and normalized and stored in the database.
▪ Events Per Second (Collector Manager)	2000	A single CPU (dual core) Xeon was used for the Collector Manager
▪ Events Per Second (Collector Engine)	1200	PIX, Snort, and other devices were used with this test
▪ Events Per Second (SYSLOG)	1200	One Syslog server was running on the Collector Manager host with 1 Engine
▪ Collectors deployed per Collector Manager	10	One Collector utilized syslog; others were using a File Connector
▪ Number of Collector Managers	1	20 is the maximum number of Collector Managers supported per Sentinel Server
▪ Correlation Engines Deployed	1	Runs on the Sentinel Server machine
▪ Rules deployed per correlation Engine	20	
▪ Active Views running	20	
▪ Number of simultaneous users	5	
▪ Number of views per Active View Instance	4	
▪ Number of maps deployed	4	
▪ Size of the largest Map	1.5 MB	
▪ Number of rows in the largest map	1.5 million	

Table 2-7: *Performance Metrics*

Production System Configuration – Option 2

This configuration requires four machines and handles approximately 3000 events per second.

NOTE: The following numbers are based on testing on Sentinel 5.1.3. For updated information, see the Novell Documentation site (http://www.novell.com/documentation/index.html).

Function	RAM	MODEL
▪ Sentinel Server	4 GB, 5x36 GB RAID	SLES9 - 2 x Dual Core Intel Xeon 5160 3.0 GHz
▪ Database	8 GB, 5x250 GB RAID	SLES9 - 2 x Dual Core Intel Xeon 5160 3.0 GHz
▪ Collector Manager	2 GB, 72 GB	SLES9 - 2 x Dual Core Intel Xeon 5160 3.0 GHz
▪ Sentinel Server (DAS - node 2)	2 GB, 5x36G B RAID	SLES9 - 2 x Dual Core Intel Xeon 5160 3.0 GHz

Table 2-8: *Four Machine Configuration*

The following performance metrics were observed on this system:

Attribute	Rating	Comments
▪ Events Per Day (partially processed)	5.2 billion	Includes events that are preprocessed and filtered in addition to events fully processed and stored in the database.
▪ Events Per Day (fully processed and stored in the database)	260 million	Includes events that are fully parsed and normalized and stored in the database.
▪ Events Per Second (Collector Manager)	3000	A dual CPU (dual core) Xeon was used for the Collector Manager
▪ Events Per Second (Collector Engine)	1200	PIX, Snort, and other devices were used with this test
▪ Events Per Second (SYSLOG)	2500	One Syslog server was run on the Collector Manager host
▪ Collectors deployed per Collector Manager	10	Three Collector utilized syslog; others were using a File Connector
▪ Number of Collector Managers	1	
▪ Correlation Engines Deployed	1	Runs on the Sentinel Server machine
▪ Rules deployed per correlation Engine	20	
▪ Active Views running	20	
▪ Number of simultaneous users	5	
▪ Number of views per Active View Instance	4	
▪ Number of maps deployed	4	
▪ Size of the largest Map	1.5 MB	
▪ Number of rows in the largest map	1.5 million	

Table 2-9: *Performance Metrics*

WARNING:

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

Disk Array Configuration

The Novell Sentinel server in a production setting requires a high-speed disk array for the database and sentinel hosts. This section covers typical disk (RAID) configuration recommendations. The following features are affected by the performance of the disk hardware:

- **Database component (Microsoft SQL/Oracle):** The event rate (events per second) and query features are impacted (including Historical Event Query, Offline Query, and Crystal reporting).
- **DAS-RT (Data Access Service Real Time Component):** The Active Views feature is impacted.
- **DAS-Aggregation:** The number of summaries that can be activated are impacted.

Minimum Requirement for Installing Enterprise (1000 EPS or more)

At a minimum, it is recommended to use a RAID 5 configuration. RAID 5 can be the most cost effective. This configuration does sacrifice some performance and redundancy for cost. These are only recommendations and are to be used as a guide. Most production large-scale enterprise installations require a more detailed analysis of speed, throughput, and redundancy requirements.

- RAID Group 1 – Database (Data, Indexes, transaction logs, and so on)
- RAID Group 2 – Sentinel Server DAS (data directory, temporary directory)
- Minimum disks: 13 per RAID group
- Disk Type: 12K+ RPM, Fibre Channel or SCSI
- LUN 1 (RAID Group 1): 5GB – 144GB+ per disk
- LUN 2 (RAID Group 2): 5GB – 144GB+ per disk

Optimal Configuration

For an optimal performance and redundancy configuration a RAID 1+0 can be utilized with the same settings. However, additional RAID Groups and LUNs following the same guidelines as above might be required to achieve more parallelism and I/O for certain databases.

NOTE: For more information on how to point the DAS TEMP DIR to a different location, see "Installing Sentinel 6" section.

Example Storage Configuration for a Microsoft SQL Install

This example uses an EMC^{2*} CLARiiON* storage subsystem with:

- 1 TB of storage
- 60 drives, 36 GB, 15K RPM

RAID Groups

Array	RAID Group	Number of Drives	Drives Assigned (bus-enclosure-disk)	Name
1	0	8	0-0-13, 0-0-14, 1-0-13, 1-0-14, 2-0-13, 2-0-14, 3-0-13, 3-0-13	RAID Group 0
1	1	8	0-0-11, 0-0-12, 1-0-11, 1-0-12, 2-0-11, 2-0-12, 3-0-11, 3-0-12	RAID Group 1
1	2	8	0-0-9, 0-0-10, 1-0-9, 1-0-10, 2-0-9, 2-0-10, 3-0-9, 3-0-10	RAID Group 2
1	3	8	0-0-7, 0-0-8, 1-0-7, 1-0-8, 2-0-7, 2-0-8, 3-0-7, 3-0-8	RAID Group 3
1	4	8	0-0-5, 0-0-6, 1-0-5, 1-0-6, 2-0-5, 2-0-6, 3-0-5, 3-0-6	RAID Group 4
1	5	8	0-0-3, 0-0-4, 1-0-3, 1-0-4, 2-0-3, 2-0-4, 3-0-3, 3-0-4	RAID Group 5
1	6	12	0-0-0, 0-0-1, 0-0-2, 1-0-0, 1-0-1, 1-0-2, 2-0-0, 2-0-1, 2-0-2, 3-0-0, 3-0-1, 3-0-2	RAID Group 6

***Table 2-10:** Storage Configuration for a Microsoft SQL Install*

LUN Assignments

Array	LUN	RAID Type	RAID Group	Size (GB)	Storage Processor	Name
1	0	0	0	263	A	LUN 0
1	1	0	1	263	B	LUN 1
1	2	0	2	263	A	LUN 2
1	3	0	3	263	B	LUN 3
1	4	0	4	263	A	LUN 4
1	5	0	5	214	B	LUN 5
1	6	0	6	160	A	LUN 6
1	7	0	6	160	B	LUN 7

***Table 2-11:** LUN Assignments*

Storage Groups

Array	Storage Group	LUN	Host	Drive Letter	Name
1	Sentinel	0	E2P0 (E3P0)	E:	SQLData1
1	Sentinel	1	E2P0 (E3P0)	F:	SQLData2
1	Sentinel	2	E2P0 (E3P0)	G:	SQLData3
1	Sentinel	3	E2P0 (E3P0)	H:	SQLData4
1	Sentinel	4	E2P0 (E3P0)	I:	SQLIndex1
1	Sentinel	5	E2P0 (E3P0)	J:	SQLIndex2
1	Sentinel	6	E2P0 (E3P0)	L:	SQLLog
1	Sentinel	7	E2P0 (E3P0)	T:	TempDB

Table 2-12: Storage Groups

Example Storage Configuration for an Oracle Install

volume 1	RAID 1	Oracle home
volume 2	RAID 1	redo log member a
volume 3	RAID 1	redo log member b
volume 4	RAID 0+1 or RAID 5	undo and temp tablespaces
volume 5	RAID 0+1 or RAID 5	Sentinel data tablespaces
volume 6	RAID 0+1 or RAID 5	Sentinel index tablespaces
volume 7	RAID 0+1 or RAID 5	Sentinel summary data tablespaces

volume 8	RAID 0+1 or RAID 5	Sentinel summary index tablespaces
volume 9	RAID 1	archive log files

Table 2-13: *Storage Configuration for an Oracle Install*

Network Configuration

Sentinel Server side components: These should be connected to each other through a single 1 GB switch. This includes the database, Communication Server, Advisor, Base Sentinel Services, Correlation Engine, and DAS.

Sentinel Control Center, Collector Builder and Collector Service (Collector Manager): These must be connected to the Sentinel Server through at least 100Mbit-FULL DUPLEX switches.

AES Configuration

Sentinel uses 128-bit AES encryption by default. AES 256-bit encryption can be configured to provide better security. For more information about AES configuration, see "Communication Layer (iSCALE)" section.

Best Practice: Database Installation/Configuration

NOTE: Most database install parameters can be changed after the database install through database management tools or the command line.

- Sentinel uses a predefined archive strategy to manage the tables that grow quickly (the EVENTS table, for instance). These tables are partitioned, and older partitions can be archived and dropped without affecting more recent data. Tables other than EVENTS, Correlated Event and the six summary tables are not covered by this partitioning and archiving scheme, and will need to be managed separately.
- For performance reasons, if you are installing in RAID and if your RAID environment allows, the following logs should be installed on the fastest write disk you have available.
  - **Redo Log (Oracle)**
  - **Transaction Log (Microsoft SQL)**
- To more accurately determine your database size, you can initially start with a small database and extend your database size after having the system up and running for a short period. This will allow you observe your database growth based on your event insertion rate to determine your system database space requirements.
- For recovery purposes, a DBA should perform regularly scheduled backups of the non-partitioned tables in the database.
- For Oracle installations, the Sentinel installer turns off Archive Logging by default. For database recovery purposes, it is highly recommended that you enable Archive Logging before you begin to receive your production event data. You should also schedule to backup your archive logs to free up space in your archive log destination; otherwise, your database will stop accepting events when the archive log destination reaches full capacity.
- For performance reasons in high-event rate environments, the storage locations should point to different locations (For example, different disk controllers) to avoid IO contentions.

- Data directory
- Index directory
- Summary Data directory
- Summary Index directory
- Log Directory (Microsoft SQL Only)
- Temporary and Undo Tablespace directory (Oracle Only)
- Redo Log Member A directory (Oracle Only)
- Redo Log Member B directory (Oracle Only)

Sentinel Database Patches

For Microsoft SQL only, when Sentinel Database patches are applied, the installer will only add new indexes to *_P_MAX only. Already existing partitions are not updated. You must manually add indexes to already existing partitions if you want the new indexes to improve performance for queries running against existing partitions.

Recommended UNIX Kernel Settings for Oracle

The following are suggested minimum values. For more information, see Oracle documentation (http://www.oracle.com/technology/documentation/index.html).

Minimum Kernel Parameter Values for Linux

For more information on how to view and set kernel parameters on Linux, see "Installing Sentinel 6" section.

```
shmmax=2147483648 (minimum value)
shmmni=4096
semmns=32000
semmni=1024
semmsl=1024
semopm=100
```

Minimum Kernel Parameter Values for Solaris

Check UNIX kernel parameters for Oracle in `/etc/system` and set the following:

```
shmmax=4294967295
shmmin=1
shmseg=50
shmmni=400
semmns=14000
semmni=1024
semmsl=1024
shmopm=100
shmvmx=32767
```

Configuring Parameters when Creating Your Own Database Instance

You can create the database structure (to the tablespace level) manually instead of through the Sentinel installer, if desired. Then, during installation, you can select the *Add database objects to an existing database* option. The following settings are recommended when creating your own database instance. Your settings can vary depending on your system configuration and requirements.

In the Oracle instance, you must create:

- Oracle initialization parameters (these values are dependent on your system size and configuration)
- Sentinel required tablespaces configuration parameters for Solaris and Linux

Minimum Recommended Configuration Parameters

Parameters	Size (bytes or otherwise specified)
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
hash_join_enabled	TRUE
optimizer_index_caching	50
optimizer_index_cost_adj	55

Table 2-14: *Configuration Parameters*

Minimum Recommended Tablespace Size

Tablespace	Example Size	Notes
REDO	3 x 100M	This is a minimum value. You should create larger redo logs if you have a high EPS.
SYSTEM	500M	Minimum value.
TEMP	1G	Minimum value.
UNDO	1G	Minimum value.
ESENTD	5G	Minimum value for event data.
ESENTD2	500M	Minimum value for configuration, assets, vulnerability and associations.
ESENTWFD	250M	For iTRAC data.
ESENTWFX	250M	For iTRAC index.
ESENTX	3G	Minimum value for the event index.
ESENTX2	500M	Minimum value for the configuration, assets, vulnerability and associations.
SENT_ADVISORD	35G	Minimum value for the Advisor data.
SENT_ADVISORX	100M	Minimum value for the Advisor index.
SENT_LOBS	100M	Minimum value for the database large objects.
SENT_SMRYD	3G	Minimum value for the Aggregation, summary data.
SENT_SMRYX	2G	Minimum value for the Aggregation, summary index.

Table : *Minimum Recommended Tablespace Size*

NOTE: All the tablespaces are “auto-enabled”, by default.

Sentinel Installation and Configuration

When installing Sentinel, for performance and backup reasons, the following should be considered:

1. When performing a clean installation of Sentinel after having a previous version of Sentinel installed, it is highly recommended that you remove certain files and system settings from the previous installation. Not removing these files could cause a new, clean installation to fail. This should be done on every machine you are performing a clean installation. For more information about which files to remove, see “Uninstalling Sentinel” section.
2. The performance of Active Views and Mapping can improve dramatically if you point the `temp` directory of the DAS_RT and DAS_Query processes to a fast disk (For example, a disk array). To point the temp directory of these processes to a fast disk, do the following on the machine where DAS is installed:

   a. Create a directory on the fast disk to place the temp files. If on UNIX, this directory must be owned and writable by the Sentinel Administrator User and the group esec.

NOTE: Installer automatically creates a backup of `configuration.xml` at `%ESEC_HOME%\config\configuration.xml`.

   b. Open the file `%ESEC_HOME%\config\configuration.xml` in a text editor.

   c. For the DAS_RT and DAS_Query processes, add the JVM argument java.io.tmpdir, setting it to the directory you just created.

   d. To make this change to the DAS_RT process, look for the line containing the text

```
-Dsrv_name=DAS_RT
```

and add the argument mentioned below next to it.

```
-Djava.io.tmpdir=<tmp_directory>
```

An example of what the line should like (your –Xmx, -Xms, and –XX args might look different) is:

```
<process component="DAS"
   image="&quot;$(ESEC_JAVA_HOME)/java&quot; -
   server -Dsrv_name=DAS_RT -
   Djava.io.tmpdir=/opt/Temp2 -Xmx310m -
   Xms103m -XX:+UseParallelGC -Xss128k -Xrs -
   Desecurity.dataobjects.config.file=/xml/Bas
   eMetaData.xml -
   Djava.util.logging.config.file=../config/da
   s_rt_log.prop -
   Dcom.esecurity.configurationfile=../../conf
```

```
    iguration.xml -
    Djava.security.auth.login.config=../config/
    auth.login -
    Djava.security.krb5.conf=../../lib/krb5.con
    f -jar ../../lib/ccsbase.jar
    ..//config//das_rt.xml" min_instances="1"
    post_startup_delay="5"
    shutdown_command="cmd //C
    &quot;$(ESEC_HOME)/bin/stop_container.bat&q
    uot; localhost DAS_RT"
    working_directory="$(ESEC_HOME)/bin"/>
```

e. To make this change to the DAS_Query process, look for the line containing the text

```
-Dsrv_name=DAS_Query
```

and add the argument mentioned below next to it.

```
-Djava.io.tmpdir=<tmp_directory>
```

An example of what the line should like (your –Xmx, -Xms, and –XX args might look different) is:

```
<process component="DAS"
    image="&quot;$(ESEC_JAVA_HOME)/java&quot; -
    server -Dsrv_name=DAS_Query -
    Djava.io.tmpdir=/opt/Temp2 -Xmx256m -Xms85m
    -XX:+UseParallelGC -Xss128k -Xrs -
    Desecurity.dataobjects.config.file=/xml/Bas
    eMetaData.xml,/xml/WorkflowMetaData.xml -
    Djava.util.logging.config.file=../config/da
    s_query_log.prop -
    Djava.security.auth.login.config=../config/
    auth.login -
    Djava.security.krb5.conf=../../lib/krb5.con
    f -
    Desecurity.execution.config.file=../config/
    execution.properties -
    Dcom.esecurity.configurationfile=../../conf
    iguration.xml -jar ../../lib/ccsbase.jar
    ..//config//das_query.xml"
    min_instances="1" post_startup_delay="5"
    shutdown_command="cmd //C
    &quot;$(ESEC_HOME)/bin/stop_container.bat&q
    uot; localhost DAS_Query"
    working_directory="$(ESEC_HOME)/bin"/>
```

Setting Passwords

To meet stringent security configurations required by Common Criteria Certification:

- Choose passwords of at least 8 characters in length that includes at least one UPPER CASE, one lower case, one special symbol (!@#$%^&*()_+), and one numeric (0-9).
- Your password should not contain your e-mail name or any part of your full name.
- Your password should not be a "common" word (for example, it should not be a word in the dictionary or slang in common use).
- Your password should not contain words from any language, because numerous password-cracking programs exist that can run through millions of possible word combinations in seconds.
- You must select a password you can remember and yet is complex. For example, Msi5!YOld (My son is 5 years Old) OR IhliCf5#yN (I have lived in California for 5 years now).

Reporting Configuration

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 Crystal Web Page:

1. Click *Start > All Programs > BusinessObjects 11 > Crystal Reports Server > .Net Administration Launchpad*.
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.

To Reconfigure the Crystal Page Server (Linux or Windows Crystal Servers):

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

   For Linux Crystal Servers:

   http://<DNS or IP of Crystal Server>:8080/businessobjects/enterprise11/adminlaunch

   For Window Crystal Servers:

   http://<DNS name or IP address of your web server>/businessobjects/enterprise11/WebTools/adminlaunch/default.aspx

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*, select *Unlimited records*. Click *Apply*.
7. A prompt to restart the page server will display, click *OK*.
8. You might be prompted for a logon name and password to access the operating system service manager.

Sentinel Provided Reports

To improve performance, the Top 10 reports 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 *Reporting 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 Sentinel Data Manager in the *Sentinel User*

Guide or "Crystal Reports for Windows" and "Crystal Reports for Linux and Solaris" section.

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://support.businessobjects.com/documentation/product_guides/default.asp).

Tips When Developing Custom 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.

High Performance Configuration

The 64-bit JVM can allocate much more RAM to the process than the 32-bit JVM. This is useful if processing requires a lot of RAM and that is available with the machine. Performance testing has shown that the 64-bit JVM requires more RAM to perform the same tasks as compared to 32 bit JVM. However using the 64-bit JVM for a process that will not require this additional RAM will actually waste memory resources. The highest Xmx value that can be safely used by a 32-bit JVM is 1200m and virtually unlimited in 64-bit JVM.

If you want to move all the processes on a machine to use 64-bit JVM, follow these steps:

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

1. Stop Sentinel Service. Select *Start* > *Control Panel* > *Administrative Tools* > *Services*. Right-click *Sentinel* and select *Stop*.
2. Modify ESEC_JAVA_HOME to point to the 64-bit JVM.
   - **On Windows:**

   Set ESEC_JAVA_HOME to %ESEC_HOME%\jre64\bin
   - **On Unix:**

   Set ESEC_JAVA_HOME to $ESEC_HOME/jre64/bin
3. **Windows:** Prepend (must appear before %ESEC_HOME%\lib\x86) the following to the PATH: %ESEC_HOME%\lib\x86_64
Unix: Log out, then log back in to reload environment variables.
4. Take backup of `ESEC_HOME/config/configuration.xml file`.
5. Open the `ESEC_HOME/config/configuration.xml` file in a text editor.

6. Modify the -Xmx<#>m setting of the process entries in the `configuration.xml` file that you will like to give additional memory to.
7. Save the `configuration.xml` file and open it in a Web browser to make sure the xml syntax is correct.
8. Start Sentinel Service. Select *Start* > *Control Panel* > *Administrative Tools* > *Services*. Right-click *Sentinel* and select *Start.*

If you want to move individual processes on a machine to use 64-bit JVM, follow these steps:

NOTE: On Windows only Correlation Engine and Collector Manager can individually be moved to 64-bit. This limitation exists because other processes require the use of dll's found in the PATH. Because there is only one PATH environment variable for both 32-bit and 64-bit processes, only one type of dll (32/64 bit) can appear first in the PATH at one time. On UNIX any process can individually be moved to 64-bit.

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

1. Stop Sentinel Service. Select *Start* > *Control Panel* > *Administrative Tools* > *Services*. Right-click *Sentinel* and select *Stop*.
2. Take backup of `ESEC_HOME/config/configuration.xml` file.
3. Open the `ESEC_HOME/config/configuration.xml` file in a text editor. 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 “$(ESEC_JAVA_HOME)/java” to “$(ESEC_HOME)/jre64/bin/java”
4. Modify the -Xmx<#>m setting of the process entries in the `configuration.xml` file that you will like to give additional memory to.
5. Save the `configuration.xml` file and open it in a Web browser to make sure the xml syntax is correct.
6. Start Sentinel Service. Select *Start* > *Control Panel* > *Administrative Tools* > *Services*. Right-click *Sentinel* and select *Start*.

Database Maintenance

Sentinel uses its backend database to store all events as well as configuration data. This database must be carefully managed to ensure that it continues to run efficiently.

Event Information in Database

The bulk of the database consists of normalized and summarized event data. To ease management of this ever-growing set of data, Novell partitions those tables and provides a management tool, the Sentinel Data Manager, to archive and delete older partitions. You can develop an archiving plan which can be automated to minimize user interaction.

NOTE: For more information on Sentinel Data Manager, see Sentinel Data Manager in *Sentinel User Guide*.

Other Information in Database

The Sentinel database includes lots of other information, such as user accounts, configuration information, incidents, workflows, asset data, vulnerability data, and so on. All this data must be backed up using normal database tools for recovery in case of failure. Novell recommends that a comprehensive backup strategy be developed for the entire Sentinel database (as well as the servers), excepting the partitioned tables above.

For SQL Server, by default, Sentinel databases are created under full recovery model. Under full recovery model, used transaction log space is not freed up until a transaction log backup is run. To prevent the transaction log from becoming full, log backups should be scheduled in SQL Server throughout the day (3 to 4 times a day depending upon your event rate). If your organization does not require the ability to perform point-of-failure recovery, you can switch the database recover model to simple. Under the simple database recovery model, transaction log space will be freed up automatically by SQL Server without any log backups.

Additional Database Maintenance

In addition to backup, the database should be regularly checked for internal consistency. Novell provides some automated tools to help with this task.

These utilities include:

- **Analyze Partitions:** Gathers partition statistics for partitions that have recently been populated.
- **Database Health Check:** Gathers database information. It reports:
  - Checks if database instance is up
  - Checks if Oracle Listener is up
  - Displays space usage
  - Checks for unusable indexes
  - Checks for invalidate database objects
  - Checks for database analyze

NOTE: These utilities are not a substitute for regular database maintenance by a qualified DBA.

Database Analyze for Oracle

As events are inserted continuously into the Sentinel database, database statistics should be updated regularly to ensure good query performance. The Database Analyze Utility updates database statistics for event data in Oracle. For optimum performance, this utility should be scheduled to run regularly.

NOTE: This utility includes a required SQL script that can be updated periodically. It is recommended to periodically check the Novell Technical Support site (http://support.novell.com/techselect/index.html) for any updates.

Analyze Partitions

The `AnalyzePartitions.sh` script analyzes partitions that have recently been populated. This script should be scheduled daily through cron or other scheduler to update database statistics on partitions that were populated the previous day. It is recommended to run this script at a time of day when the database usage is low.

This script is located in $ESEC_HOME/bin. It should run locally on the server where Sentinel database is installed. The UNIX user account that runs the script must be able to connect to the database as sysdba (For example, oracle).

> **NOTE:** If you have downloaded a new version of this utility than is currently installed on your machine, you must install sp_esec_dba_utl.sql.

To Install sp_esec_dba_utl.sql:

1. Login as the Oracle software owner.
2. Using SQL*Plus, connect to the database as Sentinel Database User.
3. Install ESEC_DBA_UTL package. At the SQL prompt (SQL>), enter:

```
@sp_esec_dba_utl.sql
```

4. Exit SQL*Plus.

To Run AnalyzePartitions.sh:

1. On your Oracle database server machine, go to:

```
$ESEC_HOME/bin/
```

   or go to the location where you downloaded the latest file.

2. At the command prompt, enter:

   For Solaris:

```
./AnalyzePartitions.sh <ORACLE_SID> >>
   <LogFileName>
```

   For Linux:

```
ksh ./AnalyzePartitions.sh <ORACLE_SID> >>
<LogFileName>
```

   - **ORACLE_SID:** the Oracle instance name for your database**.**
   - **LogFileName:** the full path name to the file you want the log messages to be written to.

   If the script is successful, it will exit with a return code of 0. If it fails, it will exit with a return code of 1. Schedule your jobs accordingly to check for the return code. If the analyze job fails, check the log file for detailed error messages.

Database Health Check for Oracle

`dbHealthCheck.sh` is a script that gathers information about your Sentinel Oracle Database. The dbHealthCheck.sh script is located in $ESEC_HOME/bin directory. The script checks for:

- Checks if database instance is up
- Checks if Oracle Listener is up
- Displays space usage
- Checks for unusable indexes
- Checks for invalidate database objects
- Checks for database analyze

This script should be run regularly through cron or other scheduler.

NOTE: This utility tool including a required SQL script can be periodically updated. It is recommended to periodically check the Novell Technical Support site (http://support.novell.com/techselect/index.html) for any updates.

NOTE: If you have downloaded a new version of this utility than is currently installed on your machine, you must install sp_esec_dba_utl.sql.

To install "sp_esec_dba_utl.sql":

1. Login as the Oracle software owner.
2. On your database server, make sure $ORACLE_HOME and $ORACLE_SID is set in your environment.
3. Using SQL*Plus, connect to the database as Sentinel Database User.
4. Install ESEC_DBA_UTL package. At the SQL prompt (SQL>), enter:

   ```
   @sp_esec_dba_utl.sql
   ```

5. Exit SQL*Plus.

To run 'dbHealthCheck.sh':

NOTE: The script must be run using Oracle software owner account or any other account that can connect "AS SYSDBA"

NOTE: `dbHealthCheck.sh` must be run locally on the database server.

1. On your database server, make sure $ORACLE_HOME and $ORACLE_SID are set in your environment.
2. On your Oracle database Server machine, go to:

   ```
   $ESEC_HOME/utilities/db/
   ```

   or go to the location where you downloaded the latest file.
3. At the command prompt, enter:

   For Solaris:

   ```
   ./dbHealthCheck.sh
   ```

   Information about your Sentinel database will display on screen or you can write the results to a file.

   ```
   ./dbHealthCheck.sh >> <filename>
   ```

   For Linux:

   ```
   ksh ./dbHealthCheck.sh
   ```

   Information about your Sentinel database will display on screen or you can write the results to a file.

   ```
   ksh ./dbHealthCheck.sh >> <filename>
   ```

Database Maintenance

Database partitioning is automatically configured when Sentinel is installed. It is recommended that the administrator review the settings in the Sentinel Data Manager and adjust as necessary. For more information about Sentinel Data Manager, see Sentinel Data Manager in *Sentinel User Guide*.

Correlation Engine

Time Synchronization

The Sentinel Correlation Engine is very time-sensitive, so Novell strongly recommends that all Correlation Engine and Collector Manager machines be connected to an NTP (Network Time Protocol) Server or other type of Time Server. For the Sentinel Correlation Engine to work properly, the machine system time needs to be synchronized within ± 30 seconds of all Collector Manager machines.

Memory Usage

In the correlation rule language, "Window" and "Trigger" operators both have a time window associated with them. The larger the time window, the more event information can be stored in memory for that time window. This impacts the amount of memory needed to do Sentinel's in-memory correlation. If the Correlation Engine is using too much memory, consider the following options:

- Install the Correlation Engine on a dedicated machine and redeploy all current rules to the new Correlation Engine.
- Install a new Correlation Engine and redeploy selected current rules to the new Correlation Engine.
- Tune the Window clause of your Correlation Rules.
  - Make the filter for past events more specific
  - Decrease the size of the time window.
- Tune the Trigger clause of your Correlation Rules.
  - Decrease the size of the time window.
  - Decrease the threshold for the number of events required to trigger the rule.
  - Choose discriminators with low cardinality (For example, Device Type).
  - If your discriminator has low cardinality (For example, Source IP Address), decrease the threshold for the number of events required to trigger the rule and simultaneously decrease the size of the time window to achieve an equivalent result.

Short-circuit Analysis

Number comparisons are faster than string comparisons and string comparisons are faster than regular expression comparisons. The Filter operation performs short-circuit analysis on the Boolean expressions. By carefully ordering your expression you might be able to increase the speed of evaluation.

Free-Form Rules

If you cannot express a correlation rule using the Correlation Rule Wizard, construct a free-form rule using the correlation rule language. For more information on creating a free-form rule, see Correlation Engine in *Sentinel User Reference Guide*.

Sentinel Log Files

It is a good practice to periodically review the log files generated by Sentinel for any errors. For more information on these files and their locations, see Sentinel Log Locations in *Sentinel User Reference Guide*.

3 Installing Sentinel 6

Installer Overview

This section helps you install the major components of the Sentinel system. There are three installers available (FULL, CM, and CLIENT), and the following chart shows which components might be installed by which installer.

Sentinel Component	FULL Installer	CM Installer	CLIENT Installer
Database	X		
Communication Server	X		
Advisor	X		
Correlation Engine	X		
Data Access Server (DAS)	X		
Sentinel Collector Service	X	X	
Sentinel Collector Builder	X		X
Sentinel Control Center	X		X
Sentinel Data Manager	X		X
HP OpenView Service Desk	X		
Remedy Integration	X		

Table 3-1: *Sentinel Components and Installers*

The FULL installer also offers the option of a Simple installation or a Custom installation. The Simple installation installs all components on one machine and is intended for demonstration or training systems. Many minimal default settings are used for a Simple installation, and therefore it is not intended for production use. 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, which stores the events, correlated events, and configuration information, is an essential part of the Sentinel system. The database should be installed according to best practices recommended by Oracle and Microsoft.

- **Crystal Enterprise Report Server:** Crystal (and its associated Web Server and database) is used to run reports from Novell's report library or custom-designed reports. There is a separate installer for Crystal components. For more information about installing Crystal, see "Crystal Reports for Windows" and "Crystal Reports for Linux" section.
- **Crystal Report 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. This is an optional module. For more information about Advisor and information about the installer for the Advisor core data snapshot, see "Advisor Configuration" section.
- **Third-Party Integration:** Sentinel integrates with HP OpenView Service Desk and BMC Remedy ticketing systems. For more information, see 3rd Party Integration Guide.

NOTE: Novell recommends that all third-party components that are part of the Sentinel system be installed on platforms that are certified by the third party vendors, and all internal testing is performed on certified platforms. For more information, see "Supported Platforms and Best Practices" section.

Sentinel Configurations

The following are some typical configurations for Sentinel. To determine the configuration that is best applicable for your environment, see "Supported Platforms and Best Practices" section and work with Novell Customer Center (https://secure-www.novell.com/center/regadmin).

On Linux

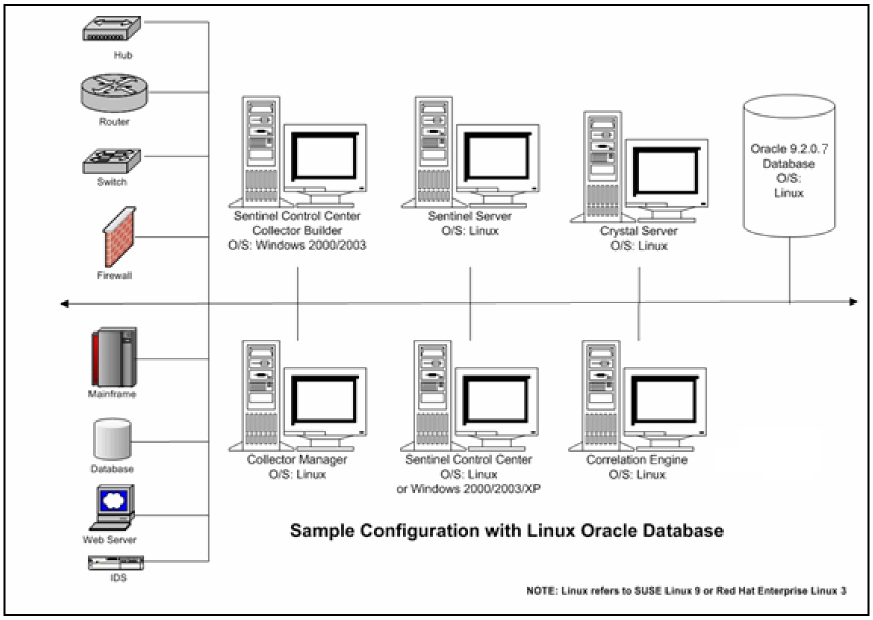


Figure 3-1: *Sentinel Configuration on Linux*

On Solaris

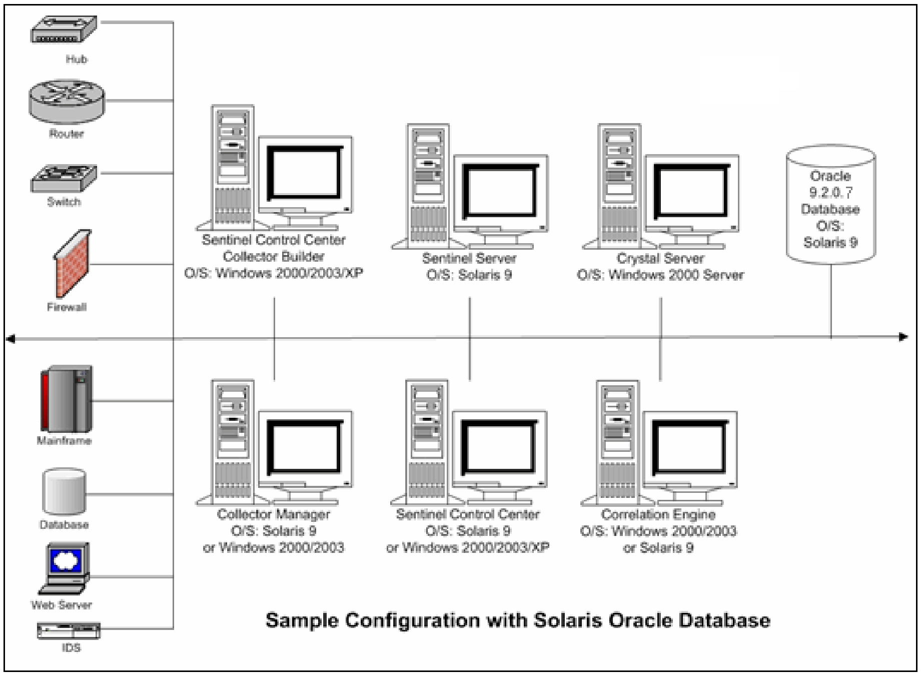


Figure 3-2: *Sentinel Configuration on Solaris*

On Windows

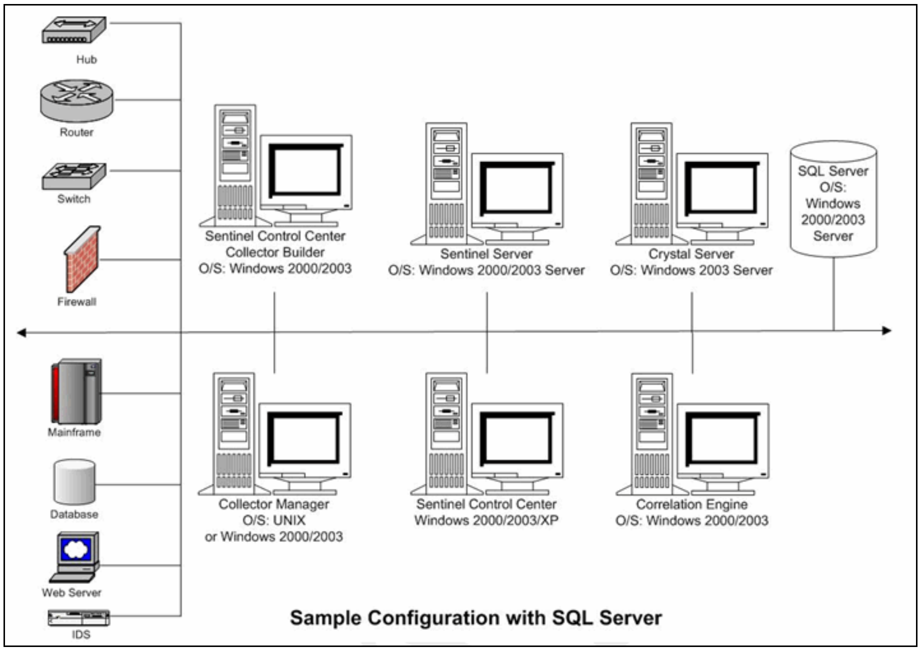


Figure 3-3: *Sentinel Configuration on Windows*

General Installation Prerequisites

The following are several steps that should be taken before installing Sentinel. For more information about many of these prerequisites (including the list of certified platforms), see "Supported Platforms and Best Practices" section.

- 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" using current best security practices.
- If installing on SUSE Linux Enterprise Server 9 or 10, ensure that SLES is using the ext3 file system.
- You must install SUNWxcu4 package on your Solaris machine before installing Sentinel 6.
- Ensure that a Sentinel-certified database is installed. (If using Oracle, Enterprise Edition with partitioning is required in order to data archive to work. For more information on certified versions, see "Supported Platforms and Best Practices" section.
- Get the Sentinel, Crystal Server, and Crystal Developer serial numbers and license keys from the Novell Customer Center (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 be able to send mail notifications from the Sentinel system.
- Create a directory with ASCII-only characters (and no special characters) from which to run the installer.
- Provide Power user privileges to "Domain User".

All Sentinel installations should take place on a "clean" system. If Sentinel 6 was previously installed on any of the machines, Novell recommends that you follow the uninstall procedures in "Uninstalling Sentinel" section. For information on uninstalling previous versions of Sentinel, see the relevant Installation guides on the Novell Documentation Website (http://www.novell.com/documentation/).

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.

To provide power user privileges to domain users:

1. 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 using this domain user.

Sentinel Database Installation Prerequisites

Before installing the Sentinel Database components, you must perform the following steps and gather the following information.

Linux/Solaris Database Installation Prerequisites for Sentinel

- If installing on SLES 9 or 10, the filesystem for the operating system must be ext3.

- On Linux/Solaris, the Oracle database must be installed and running.
- On Linux/Solaris, the Oracle JDBC client (`ojdbc14.jar`) must be installed on the machine from which you are running the installer. If you run the Sentinel installer on the database machine, a compatible JDBC client should already be installed. If you run the Sentinel installer on another machine, the compatible JDBC client must be manually installed. Although newer Oracle drivers should be backward-compatible, Sentinel testing was performed with the drivers that 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 Oracle 10 database because of 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 Appendix E, "Oracle Setup".

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

  - It is recommended to allow the Sentinel installer to create the Oracle database instance for Sentinel.
  - The database instance creation can be performed manually if desired. To ensure this instance is compatible with Sentinel, see *Manual Oracle Instance Creation in* Appendix E, "Oracle Setup". If you chose this option, you must run the Novell-provided script `createEsecDBA.sh` and use the Sentinel installer to add the database objects to the manually created Oracle database instance. For more information, see "Custom Installation".

NOTE: If using an existing or manually created Oracle database instance, it must be empty except for the presence of the Sentinel Database User.

- Get login credentials for the Oracle operating system user (default: oracle).
- Get login credentials for SYSTEM and SYS.
- Ensure 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 is 1521).
- On Linux/Solaris, 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: These directories must be writable by the oracle user. To make these directories writable by the oracle user, execute the following commands for each directory as the root user:

chown –R oracle:dba <directory_path>

chmod –R 770 <directory_path>

- On Solaris only, get a copy of Oracle Note: 148673.1 SOLARIS: Quick Start Guide

Windows Database Installation Prerequisites for Sentinel

- The SQL Server database must be installed and running.
- The sc command to start the SQL Server Agent Service must be available on your database operating system. (If it is not, the SQL Server Agent Service must be started manually in order for partitioning and data archiving to work properly. It must also be scheduled to restart after a reboot using another utility.)
- Get login credentials for the System Administrator database user
  - If the database allows SQL Authentication, the default database administrator user is sa.
  - If the database is in 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 login using the Local System Account.
- Determine the SQL Server Instance Name, if applicable.

NOTE: If you named your instance during SQL Server install, use this name when prompted for the SQL Server instance name when installing the Sentinel Database and/or DAS components. If you did not name your instance during SQL Server install, leave the instance name blank during installation (that is, if typing in 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 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 Sentinel Services. See "Providing Power User privileges to Domain Users" 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 into 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 Sentinel Database Administrator user, Sentinel Application User and Sentinel Administrator user by default

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

Authentication Mode Settings on Microsoft SQL

On Windows, you need to install SQL Server with mixed mode authentication to log into the Sentinel Control Center using either Windows or SQL Server Authentication. If you install SQL server with Windows NT Authentication, you will be able to login using Window Authentication only.

To modify your authentication mode settings:

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

Sentinel Server Installation Prerequisites

NOTE: If you are not going to install the Sentinel Database on the same machine as Sentinel Server, you must install the Sentinel Database first.

On Windows, if using Windows Authentication, you must provide the Sentinel Application User (esecapp) with “Log on as a Service” privilege on the machine on which the Data Access Service (DAS) will be installed.

To enable Log on as a Service privileges:

1. Log into the machine on which Sentinel Server and the Data Access Service (DAS) will be installed.
2. Go to *Start* > *Settings* > *Control Panel* > *Administrative Tools* > *Local Security Policy*.
3. In the *Local Security Policy* window, go to *Local Policies* > *User Rights Assignment*.
4. Double-click the *Log on as a service* policy and add the user.

Advisor Installation Prerequisites

To install Advisor, you must purchase the optional Sentinel Exploit Detection and Advisor Data Subscription. After this, your Novell eLogin is granted permission to download and update the Advisor data.

If you chose Direct Internet Download, outgoing port 443 should be open. You should plan to install Crystal Enterprise software on your system to run reports.

NOTE: If you intend to use Advisor for Exploit Detection only, you do not need to install Crystal Enterprise software. For more information about installation procedures, see "Advisor Configuration" section.

Database Installation

An experienced DBA should be involved in the installation of either Oracle or SQL Server. In addition to the recommendations from the DBA, Novell also makes some recommendations for installing Oracle. These recommendations are in the following areas:

- Setting Kernel values
- On Solaris:
  - Creating a Group and User Account for Oracle
  - Setting the environment variables
  - Verifying Solaris Layout
- Installing Oracle
- Patching to Oracle (if required)

Setting Kernel Values

DISCLAIMER: 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 with your system administrator and Oracle documentation.

To set the Kernel values on Linux:

1. Log in as root.
2. Make a backup copy of `/etc/sysctl.conf`.
3. Using a text editor, change the kernel parameters by adding the following text to the end of the "`/etc/sysctl.conf`" file:

NOTE: The kernel settings below are minimal recommended settings. These settings can be increased if the machine hardware can support it.

NOTE: 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 9 SP2 only:

```
# Oracle requires MLOCK privilege for hugetlb
memory.
```

```
vm.disable_cap_mlock=1
```

On REDHAT LINUX 3

```
# Kernel settings for Oracle
# kernel.sem = <SEMMSL> <SEMMNS> <SEMOPM>
<SEMMNI>
kernel.sem = 1024        32000   100      1024
kernel.shmmax = 2147483648
kernel.shmmni = 4096
fs.file-max = 65536
net.ipv4.ip_local_port_range = 1024 65000
```

On REDHAT 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 RedHat Linux4)
```

5. Set the file handles and process limits by adding the following text to the end of 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 text assumes 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
```

To set the Kernel values on Solaris 9:

On Solaris, the following kernel values must be set in /etc/system.

For Oracle 9i:

shmmax=4294967295
shmmin=1
shmseg=50
shmmni=400
semmns=14000
semmni=1024
semmsl=1024
shmopm=100
shmvmx=32767

For Oracle 10g:

noexec_user_stack=1
semsys:seminfo_semmni=100
semsys:seminfo_semmns=1024
semsys:seminfo_semmsl=256
semsys:seminfo_semvmx=32767
shmsys:shminfo_shmmax=4294967295
shmsys:shminfo_shmmni=100

NOTE: The kernel settings above are minimal recommended settings. These settings can be increased if the machine hardware can support it.

1. Log in as root.
2. Make a backup copy of `/etc/system`.
3. Using a text editor, change the kernel parameters in the `/etc/system` file as per the above table.
4. Reboot.

To set the Kernel values on Solaris 10:

For Oracle 10g:

noexec_user_stack=1
semsys:seminfo_semmni=100
semsys:seminfo_semmns=1024
semsys:seminfo_semmsl=256
semsys:seminfo_semvmx=32767
shmsys:shminfo_shmmax=4294967295
shmsys:shminfo_shmmni=100

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
```

4. 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
```

5. 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
```

NOTE: For additional information, see Oracle documentation for Solaris 10 installation.

Creating Group and User Account for Oracle (Solaris Only)

To create a group and user account and set environment variables:

1. Login 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):

     ```
     useradd –g dba –d /export/home/oracle –m –s
     /bin/csh oracle
     ```

Setting Environment Variables for Oracle (Solaris Only)

To set environment variables:

1. Login as root.
2. To set the necessary environment variables for Oracle, it is suggested to 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
```

Applying Patch Cluster for Solaris 9:

To apply Patch Cluster:

1. Go to Sun internet site and download the recommended patch set for Solaris 9:
   - Patch Cluster DATE: May/03/05

NOTE: Consult the README file and other included documentation. It is HIGHLY recommended that a complete system backup is made of the system before any patches are applied.

2. Login as the root user and install the applicable patch cluster and kernel patches.
3. Once the patches have been completed, delete the *_Recommended.zip file and the expanded files in the directories that were created by the patch and reboot your server.

Install Oracle

To perform Oracle installation, see Appendix E, "Oracle Setup". This section describes installation settings recommended for Sentinel operations. It also describes the procedures for creating the Oracle instance. (Novell recommends creating the instance using the Sentinel installer but provides instructions in case corporate policy requires that the DBA create the instance manually.)

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 type 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 the previous section, you can proceed with installing Sentinel. If the Simple Installation is chosen, some assumptions are made and several 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.
- Advisor is configured to use Direct Internet Download.
- Advisor is set to download new information every 12 hours.
- Advisor email notifications are enabled.
- The database size is 10GB.

To install Sentinel:

1. Login as root user on Solaris/Linux or administrator user on Windows.
2. Insert and mount the Sentinel Install CD.
3. Start the install program by going to the install directory on the CD-ROM and
   - On Windows, run `setup.bat`
   - On Solaris/Linux:

     For GUI mode:

     ```
     ./setup.sh
     ```

     Or for text-based ("serial console") mode:

     ```
     ./setup.sh –console
     ```

NOTE: You cannot run the installer on UNIX from a directory path that has a space in it.

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

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

5. After reading the *Welcome* screen, 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*.

NOTE: You cannot install into a directory with special characters or non-ASCII characters. For example, when installing Sentinel 6 on Windows x86-64, the default path will be C:\Program Files (x86). You must change the default path to avoid the special characters to continue installation.

8. Select *Simple*. Click *Next*.
9. In this window, provide the configuration information and click *Next*.
   - Serial Number
   - License Key
   - SMTP Server
     - Sentinel sends email through this server.
   - E-mail
     - Email sent by Sentinel displays as sent from this email address.
   - Global System Password
   - The password you entered 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 using installation, see "Sentinel Database".
   - Advisor Username and Password (optional)

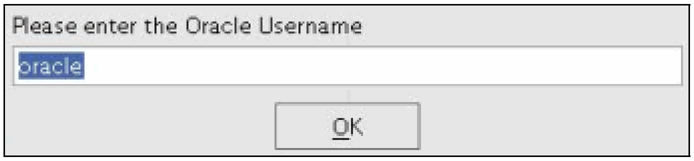
- To install Advisor, specify a Novell eLogin and password associated with the Advisor license. Provide your Advisor password again in the password confirmation window.

NOTE: Because of the changes in Advisor starting with Sentinel 6.0 SP2, the Sentinel 6.0 installer is not able to validate the Novell eLogin and password. If you entered your login and password correctly, you can ignore the error message and proceed.

10. For Database Configuration:

- Select the target Database platform.

  On Solaris/Linux, you are prompted to specify the Oracle username. Provide the username and click *OK*.



Please enter the Oracle Username

oracle

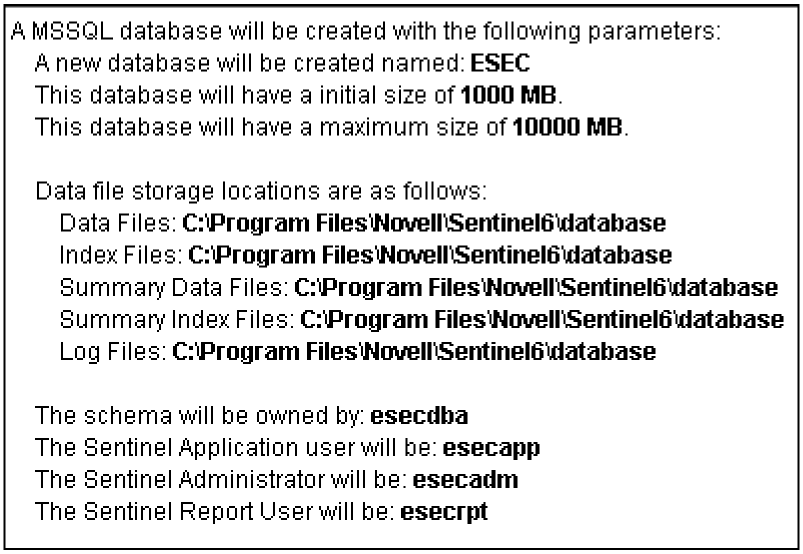
Figure 3-4: *Specify Oracle Username field*

Provide Database Name

- On Linux/Solaris, specify Oracle JDBC Driver File.
- On Windows, provide Database user credentials and SQL Server Instance name.

Click *Next*.

NOTE: On Linux/Solaris, the installer backs up any existing `tnsnames.ora` and listener.ora files to the $ORACLE_HOME/network/admin directory. It will overwrite the listener.ora file with Sentinel database connection information, and append 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.



```
A MSSQL database will be created with the following parameters:
  A new database will be created named: ESEC
  This database will have a initial size of 1000 MB.
  This database will have a maximum size of 10000 MB.

  Data file storage locations are as follows:
    Data Files: C:\Program Files\Novell\Sentinel6\database
    Index Files: C:\Program Files\Novell\Sentinel6\database
    Summary Data Files: C:\Program Files\Novell\Sentinel6\database
    Summary Index Files: C:\Program Files\Novell\Sentinel6\database
    Log Files: C:\Program Files\Novell\Sentinel6\database

  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
```

Figure 3-5: *Summary of the Database Parameters*

11. Summary of the database parameters selected displays. Click *Next*.
12. Summary of the Installation displays. Click *Install*.
13. After install, click *Finish*.
14. Reboot the system. (Scheduled services such as the Advisor download will only work after the reboot.).

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 be used to install one or more Sentinel components, including:

- Sentinel Database Components
- Sentinel Services
  - Communication Server
  - Advisor
  - Correlation Engine
  - Data Access Server (DAS)
  - Sentinel Collector Service (Collector Manager)
- Applications
  - Sentinel Collector Builder
  - Sentinel Control Center
  - Sentinel Data Manager
- 3rd Party Integration
  - HP OpenView Service Desk
  - Remedy Integration

After meeting the prerequisites mentioned in the previous section, you can 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 components on the same machine; a distributed installation will include a subset of the steps below.

NOTE: For installing 3rd Party Integration, see *3rd Party Integration Guide.*

To install Sentinel:

1. Login as root user on Solaris/Linux or administrator user on Windows.

NOTE: Installing the Sentinel Database component on Windows when the target MS SQL Server instance is in Windows Authentication only mode requires that you log into Windows as a System Administrator database user.

2. Insert and mount the Sentinel Install CD.
3. Start the install program by going to the install directory on the CD-ROM and
   - On Windows, run `setup.bat`
   - On Solaris/Linux:

     For GUI mode:

     ```
     ./setup.sh
     ```

     Or for textual ("headless") mode:

```
./setup.sh –console
```

NOTE: You cannot run the installer on UNIX from a directory path that has a space in it.

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

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

5. After reading the Welcome screen, 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*.

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

8. Select *Custom*. Click *Next*.
9. Select the components of Sentinel to install.

   The following options are available:

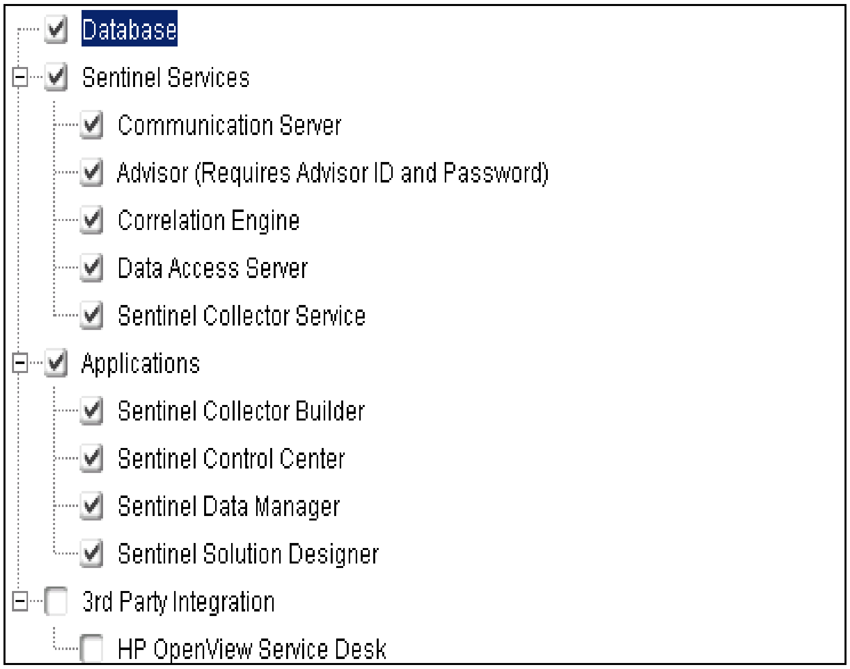
   Database – installs Sentinel Database
   Communication Server – installs message bus (iSCALE) and DAS Proxy
   Advisor
   Correlation Engine
   DAS (for database communication)
   Sentinel Collector Service
   Collector Builder
   Sentinel Control Center
   Sentinel Data Manager
   HP OpenView Service Desk
   Remedy Integration

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

NOTE: If none of the child features of *Sentinel Services* are selected, make sure you de-select the *Sentinel Services* feature as well. It will display dimmed (not available) with a white check mark in it if it is still selected but all of its child features were de-selected.

NOTE: As part of the installation of the Sentinel Database component, the installer will place files in the %ESEC_HOME%\ unist\db folder.

NOTE: If using "console" mode, the component selection page will not display all of the components together. Follow the on-screen instructions for viewing and editing the selected child components. Not all child components are selected by default. For information, see "Console Installation on Linux/Solaris".



- ☑ Database
- ☑ Sentinel Services
  - ☑ Communication Server
  - ☑ Advisor (Requires Advisor ID and Password)
  - ☑ Correlation Engine
  - ☑ Data Access Server
  - ☑ Sentinel Collector Service
- ☑ Applications
  - ☑ Sentinel Collector Builder
  - ☑ Sentinel Control Center
  - ☑ Sentinel Data Manager
  - ☑ Sentinel Solution Designer
- □ 3rd Party Integration
  - □ HP OpenView Service Desk

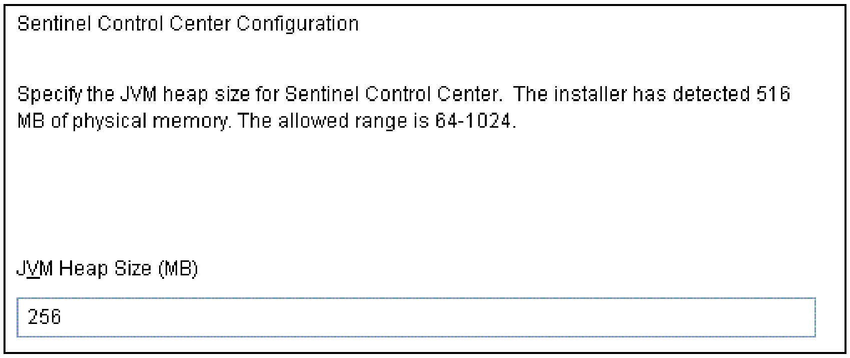
Figure 3-6: *Feature Selection window*

10. If you select to install DAS, you are prompted for:
    - Serial Number
    - License Key
11. On Linux/Solaris, specify the operating system Sentinel Administrator username and the location of its home directory. This is the username that will own the installed Sentinel product. If the user does not already exist, one will be created along with a home directory in the specified directory.
    - OS Administrator username – Default is esecadm
    - OS Administrator user home directory – Default is "/export/home". If esecadm is the username, then the user's home directory will be /export/home/esecadm.

NOTE: To meet stringent security configurations required by Common Criteria Certification, see Setting Passwords in "Supported Platforms and Best Practices" section.

NOTE: The esecadm user will be created without having a password set. In order to login in as this user, you will need to first set its password.

12. If you chose to install Sentinel Control Center, the installer will prompt for the maximum memory space to be allocated to Sentinel Control Center. Specify the maximum JVM heap size (MB) you want to be used only by Sentinel Control Center.
    - **JVM heap size (MB):** By default this is 256.and a maximum can be 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)

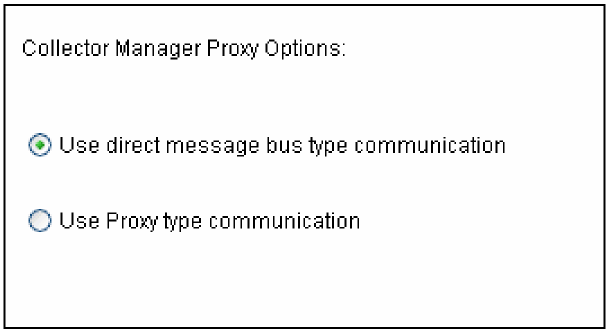
256

Figure 3-7: *Sentinel Control Center Configuration*

13. If Collector Manager is selected to be installed, you have two options to establish communication between the Sentinel Collector Managers and the Sentinel Server. You can select *Direct Message Bus type* communication or *Proxy type* communication. For more information on these two options, see "Communication Layer (iSCALE)" section. If DAS is also selected to be installed, the installer will automatically select *Direct Message Bus type* communication because the shared encryption key will be required for DAS and, therefore, *Proxy type* communication will provide no benefit.

NOTE: If *Proxy type* communication is selected, immediately after installation completes you are prompted for information required to register this Collector Manager as a trusted client. This requires that the Communication Server is running.

If the Communication Server will not be available, select *Direct Message Bus type* communication and later manually configure *Proxy type* communication by performing the step 28 "Configuring Proxy Type communication".



Collector Manager Proxy Options:

● Use direct message bus type communication

○ Use Proxy type communication

Figure 3-8: *Collector Manager Proxy Options*

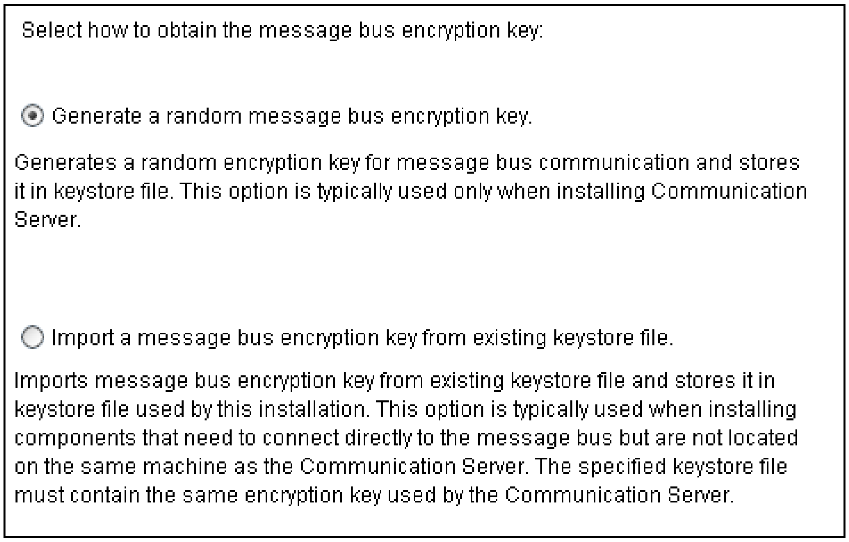
14. You are prompted to specify Communication Server port/host server name information. Provide the required information and click *Next*.

- **Message bus port:** The port the message bus is listening on. Components connecting directly to the message bus will use this port.
- **Sentinel Control Center Proxy Port:** The port the SSL proxy server (DAS Proxy) is listening to accept username and password based authenticated connections. Because Sentinel Control Center prompts for a username and password, it uses this port to connect to Sentinel Server.

- **Collector Manager Certificate Authentication Proxy Port:** The port the SSL proxy server (DAS Proxy) is listening to accept certificate based authenticated connections. Because 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.
- **Sentinel Communication Center Proxy Port:** The port used to communicate with the proxy server. This option will only display if you select Proxy type communication for the Collector Manager.
- **Communication Server hostname:** The hostname or IP of the machine where the Communication Server component is installed. If this component is currently being installed, the local hostname will be assumed and this field will not display.

NOTE: The port numbers must be identical on every machine in the Sentinel system to enable communications. Please make a note of these ports for future installations on other machines.

15. If installing a component that will make a direct connection to the message bus or if installing Communication Server, you are prompted for how to obtain the shared message bus encryption key:
    - Generate random encryption key
    - Import encryption key from keystore file. You are prompted to navigate to the location of an existing .keystore file.



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 and stores it in keystore file used by this installation. This option is typically used when installing components that need to connect directly to the message bus but are not located on the same machine as the Communication Server. The specified keystore file must contain the same encryption key used by the Communication Server.

***Figure 3-9:** Message Bus Encryption Key selection*

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

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

16. Click *Next.*

17. If you chose to install any of the Sentinel Server components, you are prompted to specify the amount of memory (RAM) to allocate to these components. The installer will factor in operating system and database overhead when determining what allocation options to display. There are two ways to specify memory allocation:

    - **Automatic Memory Configuration:** Select the total amount of memory to allocate to Sentinel Server. The installer will automatically determine the optimal distribution of memory across components taking into account estimated operating system and database overhead.

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 fine-tune memory allocations. This option will not be available if there is too little memory on the machine.

18. If you chose to install DAS and the Sentinel Database Components are already installed, you are prompted for the following Sentinel Database information. This information will be used to configure DAS to point to the Sentinel Database.

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

19. If you chose to install the database components, configure database for installation:

    On Windows:

    - Select Microsoft SQL Server 2005 as target database server platform.
        - **Create a new database with database objects:** Creates a new Microsoft SQL database as well as populate the new database with database objects
        - **Add database objects to an existing empty database:** Only adds database objects to an existing Microsoft SQL Server 2005 database. The existing database must be empty.
        - Specify the Database Install log directory.

      Click *Next*.

    - If creating a new database, specify existing directories to use as storage for:

  - Data Directory
  - Index Directory
  - Summary Data Directory
  - Summary Index Directory
  - Log Directory

  Click *Next*.

- If creating a new database, select the database character set support option, either Unicode or ASCII only database. 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, select a database format and click *OK*.

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

- If creating a new database, select a database size option. Click *Next*.
- If creating a new database and *Custom* database size was selected, specify custom database size settings:
  - **Maximum Database Size:** The maximum amount of disk space the database will occupy. The database will automatically grow up to this size as it accumulates data. Regardless of the value specified here, the database's initial size will be 1000 MB.
  - **Log File Size:** The size of the transaction log file.
  - **Maximum Database File Size:** No single database file will grow beyond this size.

  Click *Next*.

  On Linux/Solaris:

- Select the target Oracle database server version as well as the following:
  - **Create a new database with database objects:** Creates a new Oracle database instance as well as populates the new database with database objects
  - **Add database objects to an existing empty database:** Only adds database objects to an existing Oracle database instance. The existing database must be empty except for the presense of the esecdba user.
  - Specify the Database Install log directory.

  Click *Next*.

- Specify Oracle User Name or Accept default user name. Click *OK*.
- If you chose to create a new database , specify the following:
  - **The path for Oracle JDBC driver file:** Specify the fully qualified path to the jar file, typically `$ORACLE_HOME/jdbc/lib/ojdbc14.jar` (however, 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.

- If you chose to add database objects to an existing empty Oracle database, you are prompted for the following information.
  - **The path for Oracle JDBC driver file:** Specify the fully qualified path to the jar file, typically `$ORACLE_HOME/jdbc/lib/ojdbc14.jar` (however, 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 (default is ESEC). This database name must display as a service name in the `tnsnames.ora` file (in the directory $ORACLE_HOME/network/admin/) of the machine you are running the installer from.
  - **Database port:** The default 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.

NOTE: If the database name is not in the `tnsnames.ora` file, the installer will not give you an error at this point in the installation (because it verifies the connection using a direct JDBC connection), but the Database installation will fail when the Database installer tries to connect to the database through sqlplus. If the Database installation fails at that point, without exiting the installer you should 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 will retry the Database installation with the new values in the `tnsnames.ora` file.

NOTE: The installer will back up any existing `tnsnames.ora` and `listener.ora` files to the $ORACLE_HOME/network/admin directory. It will overwrite the `listener.ora` file with Sentinel database connection information, and append 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.

- If creating a new database instance, specify Oracle memory (RAM) allocation and listener port or accept the default values.
- If creating a new database instance, specify the passwords to set for the default SYS and SYSTEM database users. Click *Next*.
- If creating a new database instance, select a database size option. Click *Next*.
- If creating a new database instance and *Custom* database size was selected, specify custom database size settings:
  - **Maximum Database Size:** The maximum amount of disk space the database will occupy. The database will automatically grow

up to this size as it accumulates data. Regardless of the value specified here, the database's initial size will be 5000 MB.

  - **Log File Size:** The size of each redo log file
  - **Maximum Database File Size:** No single database file will grow beyond this size.

- If creating a new database instance, specify 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

  Click *Next*.

NOTE: 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 will 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 "Sentinel Database Installation Prerequisites".

20. If you chose to install the database component, configure database partitions.
    - Select *Enable automatic database partitions* to allow Sentinel Data Manager to handle database partitioning and archiving.
    - For data partitions, specify an existing directory for archive files.
    - Specify start time for adding partitions and archiving data. These operations should not overlap because they use shared resources.

      Click *Next*.
21. If you chose to install the database component, provide Authentication Information for:
    - 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 will be 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 using Windows Authentication.

Click *Next*.

22. If you chose to install the database component, summary of Database parameters specified displays. Click *Next*.

23. If you chose to install DAS, configure Sentinel email support. Specify the SMTP server and the *From* email that Sentinel should use to send email.

NOTE: These settings can be manually edited after install at the following locations: `$ESEC_HOME\sentinel\config\execution.properties` on Linux/Solaris or `%ESEC_HOME%\sentinel\config\execution.properties` on Windows.

If your SMTP server requires authentication, see "Updating Sentinel email for SMTP Authentication" after installation.

24. If you chose to install Advisor, the following prompt for the type of updates will display:
    - **Direct Internet Download:** In this configuration, updates from Novell are automatically downloaded from Novell over the Internet on a regular schedule (every 6 or 12 hours). Use this option if the machine has direct access to the Internet.
    - **Standalone:** In this configuration, updating Advisor will require manually downloading files from Novell. Use this option if the machine does not have direct access to the Internet.
25. If you chose to install Advisor and selected to use Direct Internet Download, provide a Novell eLogin and password associated with the Advisor license and how often Advisor data is to be updated (every 6 or 12 hours. Click *Next*.

NOTE: Because of the changes in Advisor starting with Sentinel 6.0 SP2, the Sentinel 6.0 installer is not able to validate the Novell eLogin and password. If you entered your login and password correctly, you can ignore the error message and proceed.

26. If you chose to install Advisor, provide:
    - *From* address, which will display in Advisor related email notifications
    - *To* address for sending Advisor related email notifications

NOTE: After installation, you can change the Advisor email addresses by editing the `attackcontainer.xml` and `alertcontainer.xml` files in the $ESEC_HOME/config directory. For more information, see Advisor Tab in *Sentinel User Guide*.

- Select either Yes or No for if you want to receive emails for successful Advisor updates.

NOTE: Error notifications will always be sent regardless of what is selected.

NOTE: If you chose to install HP Service Desk or Remedy Integration, you are prompted for further information. For more information, see 3rd Party Integration Guide.

27. Click *Next*. Summary screen with the features selected for installation displays. Click *Install*.

28. 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 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. Registering a trusted client involves accepting the Communication Server's SSL certificate and uploading the Collector Manager's SSL certificate to the Communication Server. When the connection with the Communication Server is initiated, you are prompted to accept the server's certificate. After reviewing the certificate's attributes, select "Accept Permanently". The installer will then automatically upload the Collector Manager's certificate to the Communication Server.

NOTE: If you chose to install HP Service Desk or Remedy Integration, you are prompted for further information. For more information, see *3rd Party Integration Guide*.

29. After installation, you are prompted to reboot or re-login and start Sentinel Services manually. Click *Finish* to reboot your system. (Scheduled services such as the Advisor download will only work after the reboot.)

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

Console Installation on Linux/Solaris

If using "console" mode, the installer's component selection page will not display all of the components together. Follow the on-screen instructions for viewing and editing the selected child components.

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

```
Select the features for "Sentinel 6" you would
like to install:
   Sentinel 6
   To select/deselect a feature or to view its
children, type its number:
     1.  [ ] Database
     2. +[x] Sentinel Services
     3. +[x] Applications
     4. +[ ] 3rd Party Integration
   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" you would
like to install:
   Sentinel 6
    - Sentinel Services
      To select/deselect a feature or to view
its children, type its number:
        1. [ ] Communication Server
        2. [ ] Advisor (Install requires
Advisor ID and Password)
        3. [x] Correlation Engine

        4. [x] Data Access Service

        5. [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" you would
like to install:
   Sentinel 6
    - Sentinel Services
      To select/deselect a feature or to view
its children, type its number:
        1. [x] Communication Server
        2. [ ] Advisor (Install requires
Advisor ID and Password)
        3. [x] Correlation
        4. [x] DAS
        5. [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" you would
like to install:
   Sentinel 6
   To select/deselect a feature or to view its
children, type its number:
     1. [ ] Database
     2. +[x] Sentinel Services
     3. +[x] Applications
     4. +[ ] 3rd Party Integration
   Other options:
     0. Continue installing
   Enter command [0]
```

Installing Sentinel as a Domain user

To install Sentinel as a domain user:

1. Map a domain user to any of the Sentinel users (esecdba, esecadm, esecrpt.

2. Perform the actions mentioned in "Providing Power User privileges to Domain Users" to provide power user privileges.
3. Install Sentinel 6.0 as an administrator user. See "Custom Installation" to install Sentinel.
4. When installer prompts for *esecdba*, *esecadm,* and *esecrpt* user credentials; specify the created domain user in "domain\domain user" format, provide password and continue installation.

Client Installation

The CLIENT installer can be used to install Sentinel Control Center, Collector Builder, and Sentinel Data Manager. This installer is smaller than the FULL installer` and is appropriate to provide to users that should not be installing Sentinel Server components.

NOTE: Because the client-only installer automatically includes Collector Builder in addition to Sentinel Control Center and Sentinel Data Manager, this installer can only be used on Windows operating systems. However, applications installed using the CLIENT installer can work with a Sentinel Server on Linux, Solaris, or Windows.

To Install Sentinel Control Center and Collector Builder using the Client-Only Installer:

1. Login as root user on Solaris/Linux or administrator user on Windows.
2. Insert and mount the Sentinel Install CD.
3. Start the install program by going to the install directory on the CD-ROM and
   - On Windows, run `setup.bat`
   - On Solaris/Linux:

     For GUI mode:

     ```
     ./setup.sh
     ```

     Or for textual ("headless") mode:

     ```
     ./setup.sh –console
     ```

NOTE: You cannot run the installer on UNIX from a directory path that has a space in it.

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

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

5. After reading the *Welcome* screen, 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*.

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

8. Select the components of Sentinel to install.

   The following options are available:

   - Collector Builder
   - Sentinel Control Center
   - Sentinel Data Manager

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

NOTE: If using "console" mode, the component selection page will not display all of the components together. Follow the on-screen instructions for viewing and editing the selected child components. For information, see "Console Installation on Linux/Solaris".

9. On Linux/Solaris, specify the operating system Sentinel Administrator username and the location of its home directory. This is the username that will own the installed Sentinel product. If the user does not already exist, one will be created along with a home directory in the specified directory.

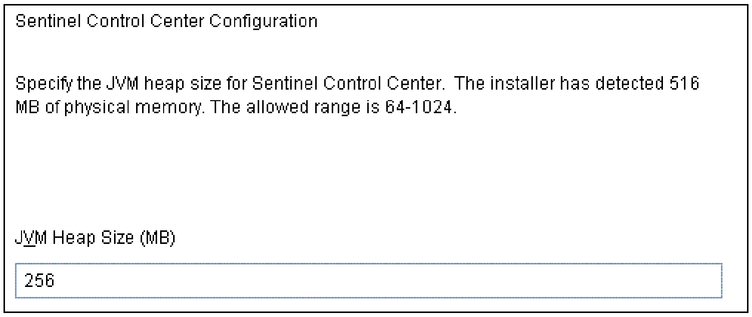
   - OS Administrator username – Default is esecadm
   - OS Administrator user home directory – Default is "/export/home". If esecadm is the username, then the user's home directory will be /export/home/esecadm.

NOTE: To meet stringent security configurations required by Common Criteria Certification, see Setting Passwords topic in "Supported Platforms and Best Practices" section.

NOTE: The esecadm user will be created without having a password set. In order to login in as this user, you will need to first set its password.

10. If you chose to install Sentinel Control Center, the installer will prompt for the maximum memory to be allocated to Sentinel Control Center. Specify the maximum JVM heap size (MB) you want to be used only by Sentinel Control Center.

    - **JVM heap size (MB):** By default, this is set to 256 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)

256

Figure 3-10: *Sentinel Control Center Configuration*

11. If Sentinel Control Center is selected to be installed, you are prompted to provide Communication Server port/host name information. Provide the required information and click *Next*.

- **Sentinel Control Center Proxy Port:** The port the SSL proxy server (DAS Proxy) is listening to accept username and password based authenticated connections. Because Sentinel Control Center prompts for a username and password, it uses this port to connect to Sentinel Server.
- **Communication Server hostname:** The hostname or IP of the machine where the Communication Server component is installed. If this component is currently being installed, the local hostname will be assumed and this field will not display.

12. Summary of the installation displays. Click *Install*.
13. After install, click *Finish*.

Collector Manager (CM) Installation

The CM Installer can be used to install the Collector Manager only. This installer is smaller than the FULL installer.

To Install Collector Manager using the CM Installer:

1. Login as root user on Solaris/Linux or administrator user on Windows.
2. Insert and mount the Sentinel Install CD.
3. Start the install program by going to the install directory on the CD-ROM and

- On Windows, run `setup.bat`
- On Solaris/Linux:

  For GUI mode:

  ```
  ./setup.sh
  ```

  or for textual (“headless”) mode:

  ```
  ./setup.sh –console
  ```

NOTE: You cannot run the installer on UNIX from a directory path that has a space in it.

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

English
French
German
Simplified Chinese
Traditional Chinese

Italian
Portuguese (Brazil)
Spanish
Japanese

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

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

8. On Linux/Solaris, specify the operating system Sentinel Administrator username and the location of its home directory. This is the username that will own the installed Sentinel product. If the user does not already

exist, one will be created along with a home directory in the specified directory.

- OS Administrator username – Default is esecadm
- OS Administrator user home directory – Default is "/export/home". If esecadm is the username, then the user's home directory will be /export/home/esecadm.

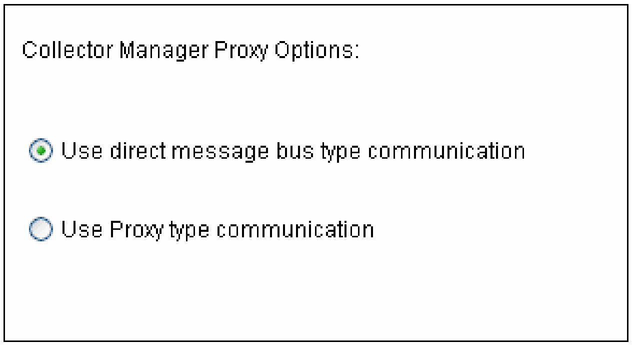
NOTE: To meet stringent security configurations required by Common Criteria Certification, see Setting Passwords topic in "Supported Platforms and Best Practices" section.

NOTE: The esecadm user will be created without having a password set. In order to login in as this user, you must first set its password.

9. You have two options to establish communication between the Sentinel Collector Managers and the Sentinel Server. You can select *Direct Message Bus type* communication or *Proxy type* communication. For more information on these two options, see "Communication Layer (iSCALE)" section.

NOTE: If *Proxy type* communication is selected, immediately after installation completes you are prompted for information required to register this Collector Manager as a trusted client. This requires that the Communication Server is running.

If the Communication Server will not be available, select *Direct Message Bus type* communication and later manually configure *Proxy type* communication by performing step 28.



Collector Manager Proxy Options:

● Use direct message bus type communication

○ Use Proxy type communication

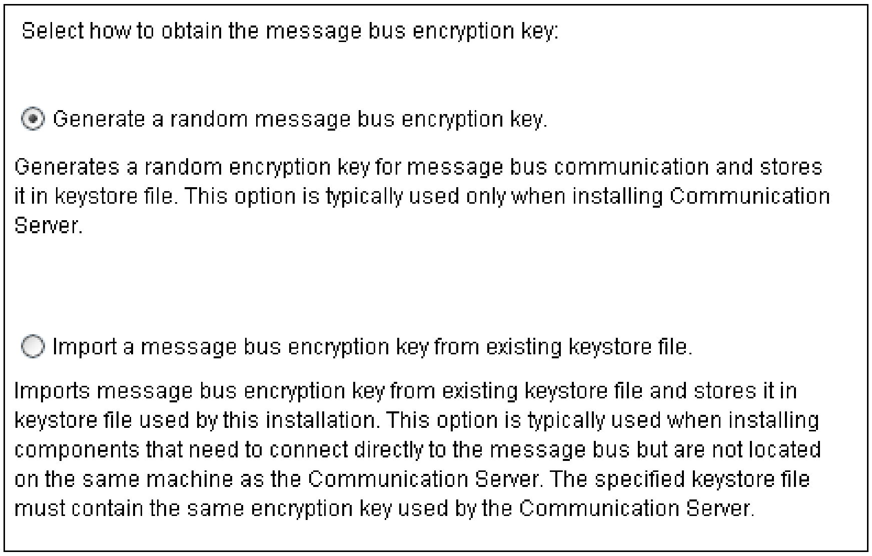
Figure 3-11: *Collector Manager Proxy options*

10. You are prompted to specify Communication Server port/host name information. Provide the required information and click *Next*.

- **Message bus port:** The port the message bus is listening on. This option is only displayed if *Direct Message Bus type* communication was selected.
- **Collector Manager Certificate Authentication Proxy Port:** The port the SSL proxy server (DAS Proxy) is listening to accept certificate based authenticated connections. Because Collector Manager cannot prompt for a username and password, it uses this port to connect to Sentinel Server if it is configured to connect through the proxy. This option is only displayed if *Proxy type* communication was selected.

- **Communication Server hostname:** The hostname or IP of the machine where the Communication Server component is installed

11. If *Direct Message Bus type* communication was selected, you are prompted for how to obtain the shared message bus encryption key:
    - Generate random encryption key
    - Import encryption key from `keystore` file. You are prompted to navigate to the location of an existing `.keystore` file.



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 and stores it in keystore file used by this installation. This option is typically used when installing components that need to connect directly to the message bus but are not located on the same machine as the Communication Server. The specified keystore file must contain the same encryption key used by the Communication Server.

***Figure 3-12:** Message Bus Encryption Key selection*

NOTE: All components connecting directly to the message bus must share the same encryption key. Novell recommends importing this key generated when installing the Communication Server component. If Collector Manager is configured to connect through the proxy, the shared message bus encryption key is not needed.

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

12. Click *Next.*
13. You are prompted to specify the amount of memory (RAM) to allocate to Collector Manager. The installer will factor in operating system 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 Collector Manager.

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 fine-tune memory allocations. This option will not be available if there is too little memory on the machine.

14. Click *Next*. Summary screen with the features selected for installation displays.

15. Click *Install*.
16. If *Proxy type* communication was selected, you are prompted to provide the username and password of a Sentinel user that has the permission to register 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. Registering a trusted client involves accepting the Communication Server's SSL certificate and uploading the Collector Manager's SSL certificate to the Communication Server. When the connection with the Communication Server is initiated, you are prompted to accept the server's certificate. After reviewing the certificate's attributes, select "Accept Permanently". The installer will then automatically upload the Collector Manager's certificate to the Communication Server.
17. After installation, you are prompted to select *Yes* or *No* to reboot your system. Select your option and click *Finish*.

Post-Installation Configuration

Updating Sentinel email for SMTP Authentication

If your system requires SMTP authentication, you will need to update the `execution.properties` file on the machine where DAS is installed. It is located at $ESEC_HOME/sentinel/config. To configure this file, run `mailconfig.sh` to change the file and `mailconfigtest.sh` to test your changes.

To configure execution.properties file:

NOTE: This example is on Linux/Solaris OS. Similar configuration has to be done for Windows OS.

1. On the machine where you have DAS installed, login as Sentinel Administrator User and cd to:

```
$ESEC_HOME/bin
```

2. Execute mailconfig as follows:

```
./mailconfig.sh -host <SMTP Server> -from
<source email address> -user <mail
authentication user> –password
```

Example:

```
./mailconfig.sh -host 10.0.1.14 -from
my_name@domain.com -user my_user_name –password
```

After entering this command you are prompted for a new password.

```
Enter your password:*********

Confirm your password:*********
```

NOTE: When using the password argument, it must be the last argument. The actual password should not be specified on the command line. The utility will prompt you for the password when the *–password* argument is specified.

To test your execution.properties configuration:

1. On the machine where you have DAS installed, login as Sentinel Administrator User and cd to:

   ```
   $ESEC_HOME/bin
   ```

2. Execute mailconfigtest as follows:

   ```
   ./mailconfigtest.sh -to <destination email
   address>
   ```

   After your mail is sent, you will get the following on screen output and e-mail received at the destination address:

   ```
   Email has been sent successfully!
   ```

   Check the destination e-mail mailbox to confirm receipt of email. The subject line and content should be:

   ```
   Subject: Testing Sentinel mail property
   ```

   ```
   This is a test for Sentinel mail property set
   up. If you see this message, your Sentinel mail
   property has been configured correctly to send
   emails
   ```

Sentinel 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 For example, 2000MB and so on.

Sentinel database automatic partition management (archiving, dropping and adding partitions) should have been selected to be enabled during installation to keep events data within a controlled size. Automatic partition management can also be configured post installation using Sentinel Data Manager (SDM).

To Edit init<OracleSID>.ora File (Oracle Only):

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 archived Sentinel data should be written. You should have one of the following:
   - UTL_FILE_DIR = *

     or
   - UTL_FILE_DIR = [specific directory path]

After installing the Sentinel Database, the database will contain the following default users:

- **esecdba:** Database schema owner. DBA privilege is not granted to Sentinel Database User because of security concerns. To use Enterprise Manager, 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
- **SYS:** SYS database user
- **SYSTEM:** SYSTEM database user

Collector Service

During the installation of the Collector Service, a Collector called General Collector will be configured. This Collector can be used to test the installation. Additional Collectors can be downloaded from the Novell Web site (http://support.novell.com/products/sentinel/collectors.html)

Updating License Key (from Evaluation to Production 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.

To update your license key (UNIX):

1. Log into the machine where the DAS component is installed as the Sentinel Administrator operating system user (default is *esecadm*).
2. In command prompt, change directory to $ESEC_HOME/bin
3. Specify the following command:

```
./softwarekey.sh
```

4. Specify number 1 to set your primary key. Press enter.

To update your license key (Windows):

1. Log into the machine where the DAS component is installed as a user with administrative rights.
2. In command prompt, change directory to %ESEC_HOME%\bin
3. Specify the following command:

```
.\softwarekey.bat
```

4. Specify number 1 to set your primary key. Press enter.

Starting Collector Manager Service

To start Collector Manager service:

1. Start Sentinel 6.0
2. Click the *Admin* tab > *Servers View*. You can also click *Servers View* in *Navigator* pane.
3. Expand the Servers view. List of processes displays.

Right-click *Collector Manager* you must start; select *Actions > Start.*

Or

1. Start Sentinel 6.0
2. Click *Event Source Management > Live View.*
3. In *Event Source Management (Live View)* window, right-click the *Collector Manager* you must start; select *Start.*

4 Advisor Configuration

This section discusses loading Advisor data, configuring regular updates to the Advisor data, and configuring Sentinel to run Advisor Reports (provided by Novell) from the *Advisor* tab of the Sentinel Control Center.

Advisor Overview

Advisor is an optional subscription service that provides device-level correlation between real-time events from intrusion detection and prevention systems and enterprise vulnerability scan results. By providing normalized attack information, Advisor acts as an early warning service to detect attacks against vulnerable systems (“exploit detection”). It also provides associated remediation information.

NOTE: Installing Advisor is optional. It is, however, a necessary component if you want to use the Sentinel Exploit Detection or Advisor Reporting features. Advisor is a subscription-based data service and requires an additional license from Novell.

The supported systems are listed below with their associated device type (IDS for intrusion detection system, VULN for vulnerability scanners, and FW for firewall).

Supported Systems	**Device Type**	**RV31 Value**
Cisco Secure IDS	IDS	Secure
Enterasys Dragon Host Sensor	IDS	Dragon
Enterasys Dragon Network Sensor	IDS	Dragon Network
Intrusion.com (SecureNet_Provider)	IDS	SecureNet_Provider
ISS BlackICE	IDS	BlackICE
ISS RealSecure Desktop	IDS	RealSecure Desktop
ISS RealSecure Network	IDS	RealSecure
ISS RealSecure Server	IDS	RealSecure Server
ISS RealSecure Guard	IDS	RealSecure Guard
Sourcefire Snort/Phalanx	IDS	Snort
Symantec Network Security 4.0 (ManHunt)	IDS	ManHunt
Symantec Intruder Alert	IDS	Intruder
McAfee IntruShield	IDS	IntruShield
eEYE Retina	VULN	Retina
Foundstone Foundscan	VULN	Foundstone
ISS Database Scanner	VULN	Database Scanner
ISS Internet Scanner	VULN	Internet Scanner
ISS System Scanner	VULN	System Scanner
ISS Wireless Scanner	VULN	Wireless Scanner
Nessus	VULN	Nessus
nCircle IP360	VULN	nCircle IP360
Qualys QualysGuard	VULN	QualysGuard
Cisco IOS Firewall	FW	Cisco IOS

Table 4-1: *Supported Systems and their Associated Device Type*

To fully enable exploit detection, the Sentinel Collectors must populate several variables correctly. Collectors built by Novell populate these variables by default.

- In IDS and vulnerability collectors, the RV31 (reserved value) variable must be set to the value in the RV31 column above. This string is case-sensitive.
- In the IDS collector, the DIP (Destination IP) must be populated with the IP address of the machine that is being attacked.
- In the IDS collector, RT1 (DeviceAttackName) must be set to the attack name or attack code for that IDS

Novell-provided collectors set these variables by default.

About Installing Advisor

The two primary components of an Advisor installation are loading the initial Advisor data and managing the regular updates that are included with the data subscription service.

Advisor must be installed on the same machine where the Database Access Service (DAS) is installed. The regular updates can be either manual or automatic, based on your choices in the Sentinel installer.

- Standalone – manual updates
- Direct Internet Download – scheduled, automatic updates

NOTE: The Advisor data feed for Sentinel 6.0 SP2 and above has been augmented with additional signatures. The changes in SP2 affect both the storage space required and the installation procedures.

Novell recommends approximately 50 GB disk space for the Advisor data, in addition to the disk space required for the Sentinel data itself.

Standalone Configuration

Standalone installation is where Advisor is an isolated system that requires a manual updates to the Advisor data. Advisor installations in a secure environment frequently do not have internet connections and therefore require the standalone configuration.

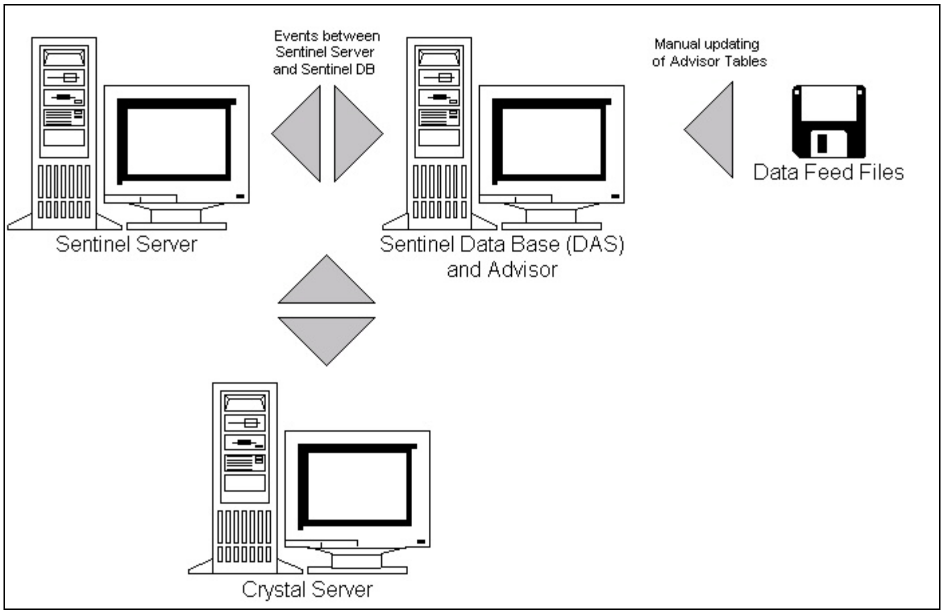


Figure 4-1: *Standalone Configuration*

For standalone configuration, the Advisor data can be manually downloaded from one of the following locations:

- Sentinel 6.0 SP1 and below:

  https://advisor.novell.com/advisordata/

- Sentinel 6.0 SP2 and above:

  https://secure-www.novell.com/sentinel/advisor/advisordata

Direct Internet Download Configuration

Direct Internet Download is where the Advisor machine is directly connected to the Internet. In this configuration, updates to the Advisor data are automatically downloaded from Novell over the Internet on a regular schedule (every 6 or 12 hours). For more information, see “Installing Sentinel 6” section.

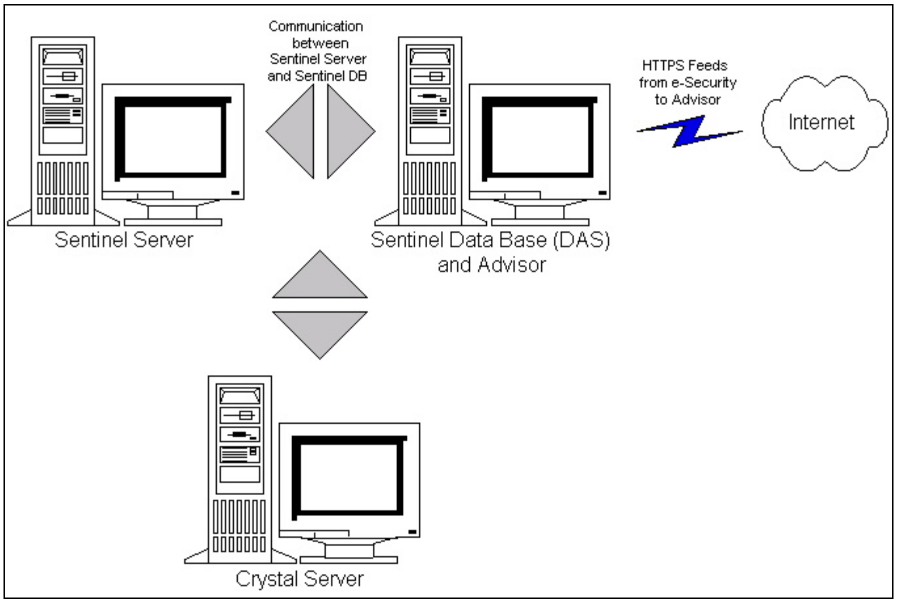

Communication between Sentinel Server and Sentinel DB
HTTPS Feeds from e-Security to Advisor
Internet
Sentinel Server
Sentinel Data Base (DAS) and Advisor
Crystal Server

Figure 4-2: *Direct Internet Download*

Installing Advisor

You can install *Advisor* when installing Sentinel or you can install it as an additional component.

> **NOTE:** Advisor changed significantly between Sentinel 6.0 SP1 and 6.0 SP2. If you are using 6.0 SP1 or below, see appropriate version of the documentation at http://www.novell.com/documentation/sentinel6.

To install Advisor:

1. Login as root user on Solaris/Linux or administrator user on Windows.
2. Insert and mount the Sentinel Install CD.
3. Start the install program by going to the install directory on the CD-ROM and
   - On Windows, run `setup.bat`
   - On Solaris/Linux:

   For GUI mode:

   ```
   ./setup.sh
   ```

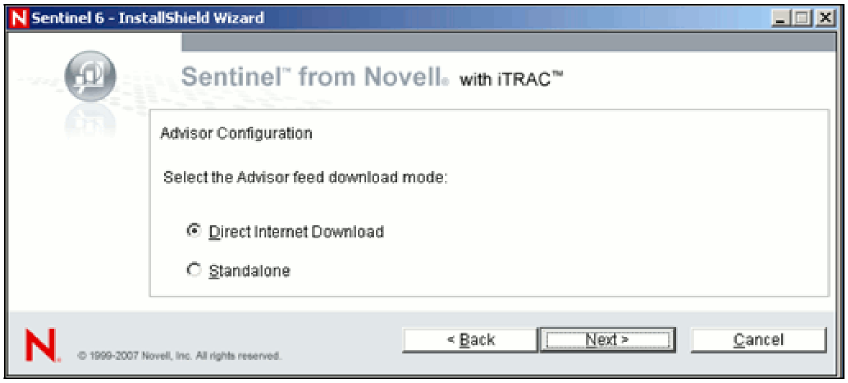
   Or for text-based (“serial console”) mode:

   ```
   ./setup.sh –console
   ```

4. Select the language and click *OK*
5. After reading the Welcome screen, click *Next*.
6. Read and accept End User License Agreement, then click *Next*.
7. Accept the default install directory or click *Browse* to specify your installation location. Click *Next*.
8. Select *Custom*. Click *Next*.
9. In this window, provide the configuration information and click *Next*.

- Serial Number
- License Key
- SMTP Server
    - Sentinel sends email through this server.
- E-mail
    - Email sent by Sentinel display as sent from this email address.
- Global System Password
- The password you entered 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 using installation, see “Sentinel Database”.

10. Select from the two options available: *Direct Internet Download* or *Standalone*.



Sentinel 6 - InstallShield Wizard

Advisor Configuration

Select the Advisor feed download mode:

● Direct Internet Download

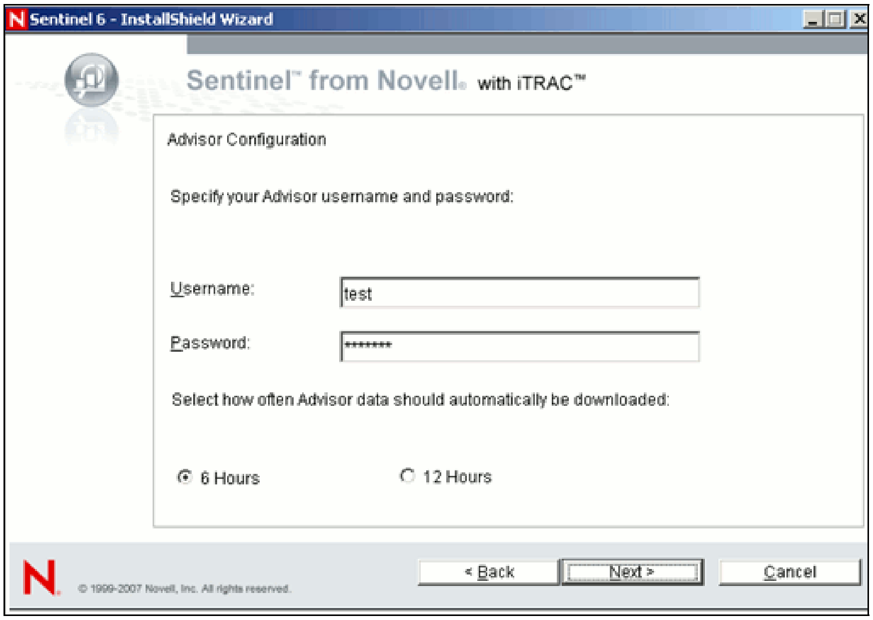
○ Standalone

Sentinel™ from Novell. with iTRAC™
© 1999-2007 Novell, Inc. All rights reserved.
< Back
Next >
Cancel

Figure 4-3: *Advisor Configuration- Advisor feed download mode selection*

11. If you have selected *Direct Internet Download*, specify the following:
    - Advisor Username
    - Advisor Password
    - How often Advisor data is to be updated

NOTE: For Sentinel 6.0 SP2 and above, the Advisor username and password are the Novell eLogin associated with the purchase of Advisor. For more information, see Advisor Tab section in *Sentinel User Guide*.


Sentinel 6 - InstallShield Wizard
Sentinel™ from Novell. with iTRAC™

Advisor Configuration

Specify your Advisor username and password:

Username: test

Password: *******

Select how often Advisor data should automatically be downloaded:

● 6 Hours ○ 12 Hours

© 1999-2007 Novell, Inc. All rights reserved.
< Back
Next >
Cancel

Figure 4-4: *Advisor Configuration-Specify Advisor Login Credentials*

Click *Next.*

IMPORTANT:

If your username and password cannot be verified, you are prompted if you want to continue.

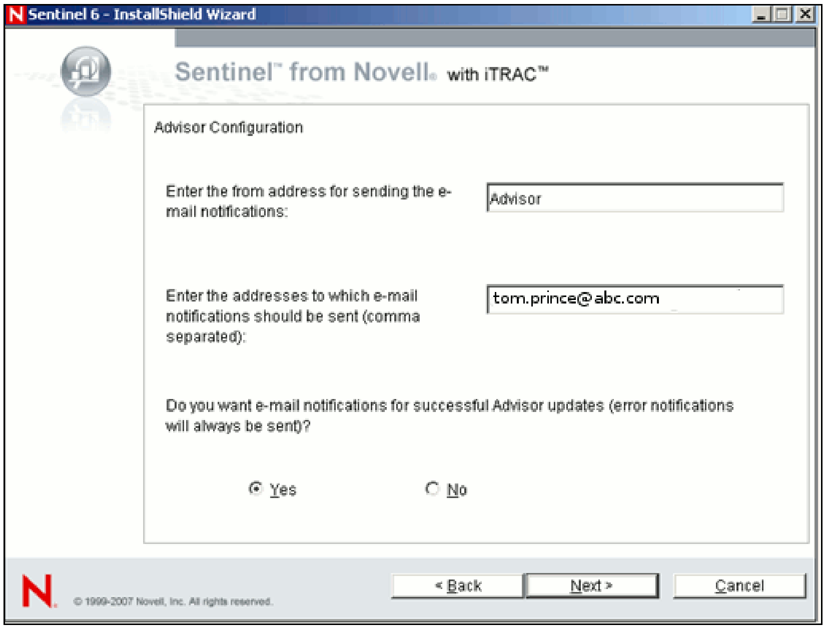
For Sentinel 6.0 SP2 and above, you should provide your Novell eLogin and password, but because of changes in authentication, these will not be recognized as a valid by the installer. You can proceed without this validation.

12. For both Direct Internet Download and Standalone installation, specify the following:

    - *From* address, as it should display in Advisor related email notifications
    - *To* address for sending Advisor related email notifications

    Select your option for receiving mails on successful Advisor updates.

NOTE: Error Notifications will always be sent regardless of what is selected.


Sentinel 6 - InstallShield Wizard
Sentinel™ from Novell® with iTRAC™

Advisor Configuration

Enter the from address for sending the e-mail notifications: Advisor

Enter the addresses to which e-mail notifications should be sent (comma separated): tom.prince@abc.com

Do you want e-mail notifications for successful Advisor updates (error notifications will always be sent)?

● Yes ○ No

© 1999-2007 Novell, Inc. All rights reserved.
< Back
Next >
Cancel

Figure 4-5: *Advisor Configuration-E-mail Notification Configuration*

Click *Next*.

TIP:

After installation, you can change the Advisor email addresses by editing the `advisor_client.xml` file in the $ESEC_HOME/config directory. For more information, see Advisor Tab in *Sentinel User Guide*.

Click *Install*.

13. After installation, you are prompted to reboot or re-login and start Sentinel Services manually. Click *Finish* to reboot your system.

IMPORTANT:

The scheduled Advisor download will only work after the reboot.

Loading Data

Although the initial Advisor data load can be performed using the scheduled service (Direct Internet Download) or even manually, with the additional signatures added to the data feed starting in Sentinel 6.0 SP2, this approach is no longer recommended.

The Sentinel 6 Exploit Detection and Advisor Core Data disk, which contains a snapshot of the Advisor data, significantly decreases the amount of time and network bandwidth required to perform the initial data load. This package is available as a download or a media kit through the Novell Customer Care Portal.

The initial data load can take as long as 24 hours, depending on the machines specifications and other loads on the database server.

After the initial data load, incremental updates can be loaded manually or using the Direct Internet Download feature.

IMPORTANT:

The data installer for Advisor works only with Sentinel 6.0 SP2 and above after the appropriate database patches have been applied as part of the patch installation process. The upgrade process and data installer replace all Advisor data that was downloaded prior to Sentinel 6.0 SP2.

To download data snapshot of Advisor:

1. Login as root user on Solaris/Linux or administrator user on Windows.
2. Insert and mount the Sentinel 6 Advisor Core Data installation disk.
3. The automated updates done by the Advisor service should be disabled before attempting to load the Advisor core data by adding "*exit*" to the beginning of the scripts(advisor.bat/.sh), or it will encounter errors with the bulk load process.
4. Start the installation program by going to the install directory on the CD-ROM and
   - On Solaris/Linux, run `advisor_bcp_in.sh`
   - On Windows, run `advisor_bcp_in.bat`
5. In the console, provide the appropriate DB credentials:
   - On Linux, provide the database user name (esecdba by default), password, and Oracle SID (instance name).
   - On Windows, provide the database host name, database name (ESEC by default), and authentication mode for the database. If using SQL Authentication, you must also provide the database user name (esecdba by default) and password.
6. Specify the time to pause in seconds between processing each file . The default is 0 seconds, but this can be paused if database load is high to introduce a pause between processing data files.
7. To increase the efficiency of the data loading process, the system disables indexes and constraints on the Advisor tables and truncates the Advisor tables. The following message is displayed:

```
Disabling indexes on the Advisor tables…

Successfully disabled indexes on the Advisor
   tables

Disabling constraints on the Advisor tables...

Successfully disabled constraints on the Advisor
   tables

Truncating Advisor tables...

Successfully truncated Advisor tables
```

8. The Advisor script starts and the bulk data is fed into the appropriate table. The snapshot of the data is stored in the database.
9. After all files in the snapshot have been loaded, it enables constraints, rebuilds indexes, and displays the following messages:

```
Successfully enabled constraints on the Advisor
   tables

Successfully rebuilt indexes on the Advisor tables
```

10. On completion of bulk feed, the system displays successful completion message.
11. The automated updates disabled before the bulk load should be enabled on completion of bulk feed by deleting "*exit*" from the beginning of the scripts(advisor.bat/.sh).

Regular incremental Advisor data updates should be planned (either scheduled using Direct Internet Download or manually) to bring and keep the Advisor database up to date.

Connecting to Advisor Server through Proxy

To connect to the Advisor server through a proxy server for feed downloads, you must update the Advisor configuration. This might require adding up to four new properties to each `advisor_client.xml` file used by Advisor. If the proxy server does not require authentication, you need to add only the proxy server's host and port information. If the proxy server requires authentication, you also need to add the username and password for the proxy server.

To configure Advisor:

1. Install Advisor in "Direct Connection" mode. Because the current installer does not support connection through a proxy server, the authentication check performed by the installer will fail. You must continue with the installation anyway.
2. Browse to `%ESEC_HOME%\config folder.`
3. Open `advisor_client.xml` and add the following lines to the DownloadComponent section.

   ```
   <property name="proxy_host">proxyHost</property>
   <property name="proxy_port">proxyPort</property>
   ```

   Also add the following properties, if the proxy server requires authentication.

   ```
   <property
      name="proxy_username">proxyUser</property>
   <property name="proxy_password" />
   ```

4. If the proxy server requires authentication, follow the following steps:
   - Copy the file `proxy_password_update.bat` to %ESEC_HOME%\sentinel\bin folder.
   - To update the Advisor container files with the proxy user password execute the following command:
     ```
     %ESEC_HOME%\sentinel\bin\proxy_password_update
     .bat   proxyPasswd
     ```
   - Verify that `advisor_client.xml` now contains the encrypted proxy password
5. Run `advisor.bat` to download and process Advisor data. You can verify that Advisor can connect through the proxy server by reviewing the following log files: `%ESEC_HOME%\sentinel\log\Advisor_0.0.log` and `%ESEC_HOME%\sentinel\log\advisor.log` files.

Advisor Reports

Crystal BusinessObjects Enterprise™ XI is the reporting tool that integrates with Sentinel.

NOTE: Crystal Server is required only if you intend to run reports. If you are going to use Advisor for Exploit Detection only, you do not need to install a Crystal Server.

To run Crystal reports on Advisor:

- Install and configure Crystal Server. For more information on Crystal BusinessObjects Enterprise™ XI installation, see "Crystal Reports for Windows" and "Crystal Reports for Linux" section.
- Publish Advisor Crystal Reports to the Crystal Server.

Advisor Report Configuration

If you intend to run Advisor reports (Crystal Reports), perform the following procedure in the order presented. You do not need to perform the following procedure if you just intend to utilize Advisor for Exploit Detection.

- If not done already, perform the following actions:
    - Install Microsoft Internet Information Server (IIS)
    - Install Crystal BusinessObjects Enterprise™ 11
    - **For Sentinel Database on Oracle (Solaris/Linux):** Configure Oracle native driver (for Oracle installations)
    - **For Sentinel Database on Microsoft SQL 2005 (Windows):** Configure Open Database Connectivity (ODBC)
    - Patch Crystal Reports.
- Install Advisor
- Import Crystal Report Templates
- Create a Crystal Web Page
- Configure Sentinel Control Center to integrate with Crystal Enterprise Server

NOTE: For more information on importing report templates and configuring the, Sentinel Control Center to show the Advisor reports, see "Crystal Reports for Windows" and "Crystal Reports for Linux" section..

Maintaining Advisor

Several maintenance tasks for Advisor that are described in the Sentinel user guide:

- Updating Advisor data manually: To be effective, the Advisor data must be updated on a regular basis as new attacks and vulnerabilities are added to the data feed.
- Changing the password Advisor uses for automatic data updates
- Changing the configuration for Advisor notification emails
- Changing the scheduled data update time

For more information on all of these maintenance tasks, see Maintaining Advisor in the *Sentinel User Guide.*

5 Testing the Installation

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 same exact events, but your results should be similar to the results below.

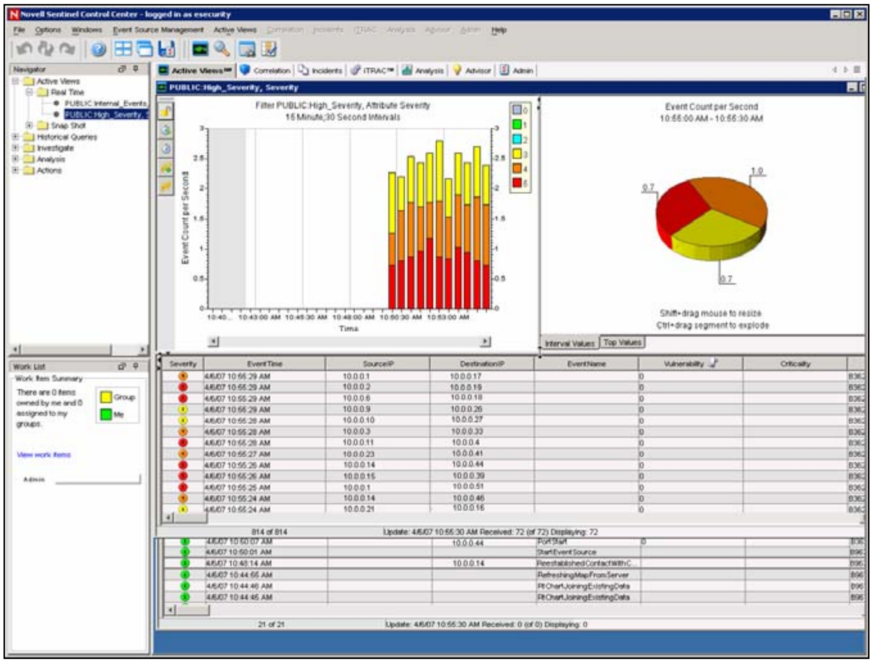
At a basic level, these tests allow you to confirm the following:

- 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), if necessary.

To test the installation:

1. Double-click the *Sentinel Control Center* icon on the desktop.
2. Log into the system using the Sentinel Administrative User specified during installation (esecadm by default). The *Sentinel Control Center* opens and you can see the *Active Views* tab with the events filtered by the public filters “Internal_Events” and “High_Severity”.


Novell Sentinel Control Center - logged in as esecurity
File Options Windows Event Source Management Active Views Correlation Incidents iTRAC Analysis Advisor Admin Help
Navigator
Active Views
Real Time
PUBLIC:Internal_Events
PUBLIC:High_Severity, S
Snap Shot
Historical Queries
Investigate
Analysis
Actions
Active Views Correlation Incidents iTRAC Analysis Advisor Admin
PUBLIC:High_Severity, Severity
Filter PUBLIC:High_Severity, Attribute Severity
15 Minute,30 Second Intervals
Event Count per Second
Time
10:40... 10:43:00 AM 10:45:30 AM 10:48:00 AM 10:50:30 AM 10:53:00 AM
Event Count per Second
10:55:00 AM - 10:55:30 AM
0.7
1.0
0.7
Shift+drag mouse to resize
Ctrl+drag segment to explode
Interval Values Top Values
Work List
Work Item Summary
There are 0 items owned by me and 0 assigned to my groups.
Group
Me
View work items
Admin

Severity	EventTime	SourceIP	DestinationIP	EventName	Vulnerability	Criticality	
	4/6/07 10:55:29 AM	10.0.0.1	10.0.0.17		0		B362
	4/6/07 10:55:29 AM	10.0.0.2	10.0.0.19		0		B362
	4/6/07 10:55:29 AM	10.0.0.6	10.0.0.18		0		B362
	4/6/07 10:55:29 AM	10.0.0.9	10.0.0.26		0		B362
	4/6/07 10:55:28 AM	10.0.0.10	10.0.0.27		0		B362
	4/6/07 10:55:28 AM	10.0.0.3	10.0.0.33		0		B362
	4/6/07 10:55:28 AM	10.0.0.11	10.0.0.4		0		B362
	4/6/07 10:55:27 AM	10.0.0.23	10.0.0.41		0		B362
	4/6/07 10:55:26 AM	10.0.0.14	10.0.0.44		0		B362
	4/6/07 10:55:26 AM	10.0.0.15	10.0.0.39		0		B362
	4/6/07 10:55:25 AM	10.0.0.1	10.0.0.51		0		B362
	4/6/07 10:55:24 AM	10.0.0.14	10.0.0.46		0		B362
	4/6/07 10:55:24 AM	10.0.0.21	10.0.0.16		0		B362

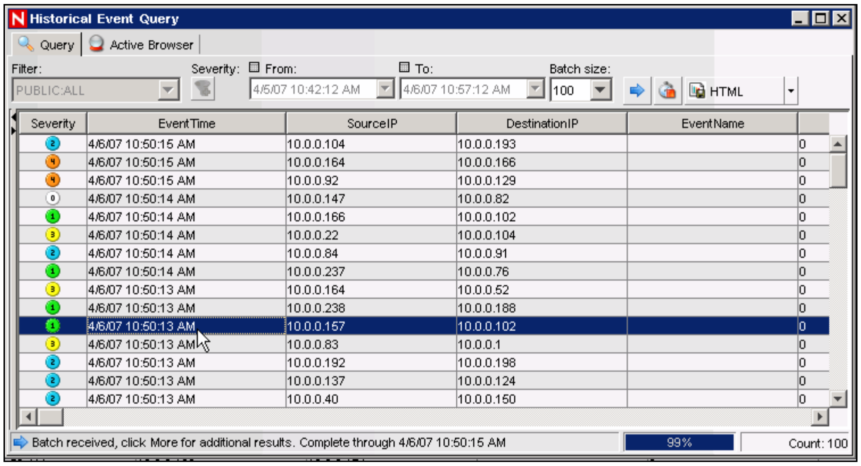
814 of 814 Update: 4/6/07 10:55:30 AM Received: 72 (of 72) Displaying: 72

Severity	EventTime	SourceIP	DestinationIP	EventName	Vulnerability	Criticality	
	4/6/07 10:50:07 AM		10.0.0.44	PortStart	0		B96
	4/6/07 10:50:01 AM			StartEventSource			B96
	4/6/07 10:48:14 AM		10.0.0.14	ReestablishedContactWithC...			B96
	4/6/07 10:44:55 AM			RefreshingMapFromServer			B96
	4/6/07 10:44:46 AM			RtChartJoiningExistingData			B96
	4/6/07 10:44:45 AM			RtChartJoiningExistingData			B96

21 of 21 Update: 4/6/07 10:55:30 AM Received: 0 (of 0) Displaying: 0

Figure 5-1: *Sentinel Control Center*

3. Go to 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. Go to the *Active Views* tab. There will be an *Active* window titled *PUBLIC: High_Severity, Severity*. It might take some time for the collector to start and the data to display in this window.
7. Click *Event Query* button in the toolbar. The *Historical Event Query* window displays.
8. In the *Historical Event Query* window, click the *Filter* 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 form *From* and *To* drop down arrow.
10. Select a batch size from the *Batch size* drop down.
11. Click the *Magnifying Glass* icon to run the query.



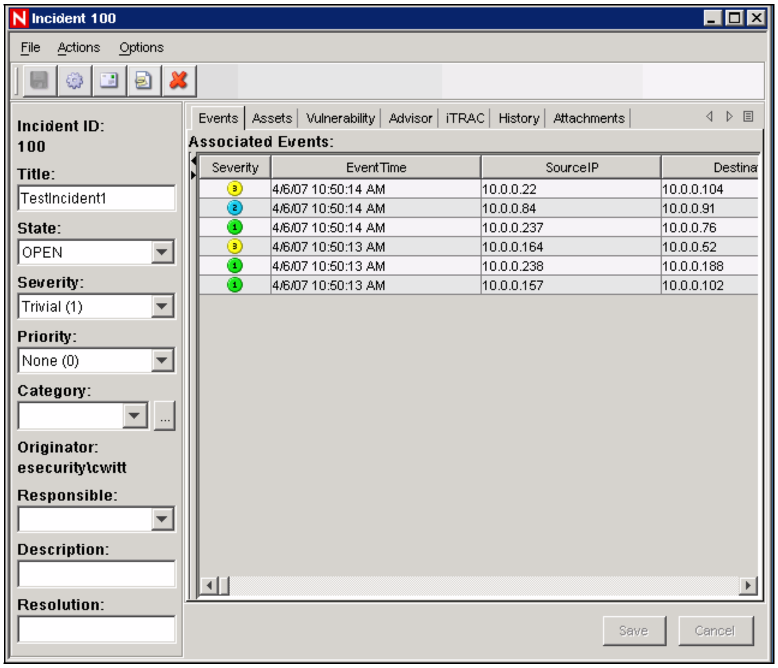
Filter: PUBLIC:ALL Severity: □ From: 4/5/07 10:42:12 AM □ To: 4/6/07 10:57:12 AM Batch size: 100

Severity	EventTime	SourceIP	DestinationIP	EventName	
2	4/6/07 10:50:15 AM	10.0.0.104	10.0.0.193		0
4	4/6/07 10:50:15 AM	10.0.0.164	10.0.0.166		0
4	4/6/07 10:50:15 AM	10.0.0.92	10.0.0.129		0
0	4/6/07 10:50:14 AM	10.0.0.147	10.0.0.82		0
1	4/6/07 10:50:14 AM	10.0.0.166	10.0.0.102		0
3	4/6/07 10:50:14 AM	10.0.0.22	10.0.0.104		0
2	4/6/07 10:50:14 AM	10.0.0.84	10.0.0.91		0
1	4/6/07 10:50:14 AM	10.0.0.237	10.0.0.76		0
3	4/6/07 10:50:13 AM	10.0.0.164	10.0.0.52		0
1	4/6/07 10:50:13 AM	10.0.0.238	10.0.0.188		0
1	4/6/07 10:50:13 AM	10.0.0.157	10.0.0.102		0
3	4/6/07 10:50:13 AM	10.0.0.83	10.0.0.1		0
2	4/6/07 10:50:13 AM	10.0.0.192	10.0.0.198		0
2	4/6/07 10:50:13 AM	10.0.0.137	10.0.0.124		0
2	4/6/07 10:50:13 AM	10.0.0.40	10.0.0.150		0

Batch received, click More for additional results. Complete through 4/6/07 10:50:15 AM 99% Count: 100

Figure 5-2: *Historical Event 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*.



Incident ID:
100

Title: TestIncident1

State: OPEN

Severity: Trivial (1)

Priority: None (0)

Category:

Originator:
esecurity\cwitt

Responsible:

Description:

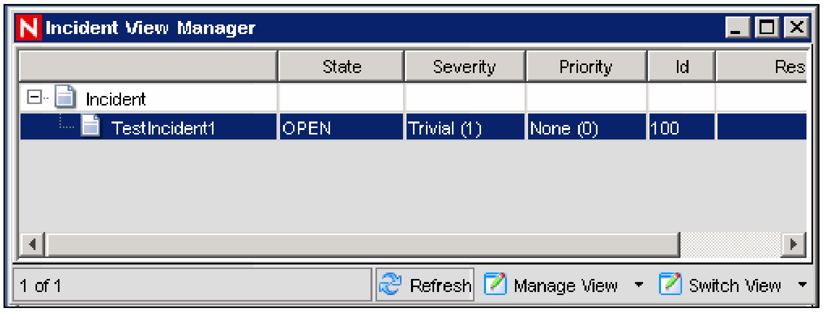
Resolution:

Associated Events:

Severity	EventTime	SourceIP	Destina
3	4/6/07 10:50:14 AM	10.0.0.22	10.0.0.104
2	4/6/07 10:50:14 AM	10.0.0.84	10.0.0.91
1	4/6/07 10:50:14 AM	10.0.0.237	10.0.0.76
3	4/6/07 10:50:13 AM	10.0.0.164	10.0.0.52
1	4/6/07 10:50:13 AM	10.0.0.238	10.0.0.188
1	4/6/07 10:50:13 AM	10.0.0.157	10.0.0.102

Figure 5-3: *Creating Incident*

14. Name the incident TestIncident1 and click *Create*. A success notification displays. Click *OK*.
15. Go to the *Incident* Tab. *Incident View Manager* displays. In the *Incident View Manager* you will see the incident you just created.

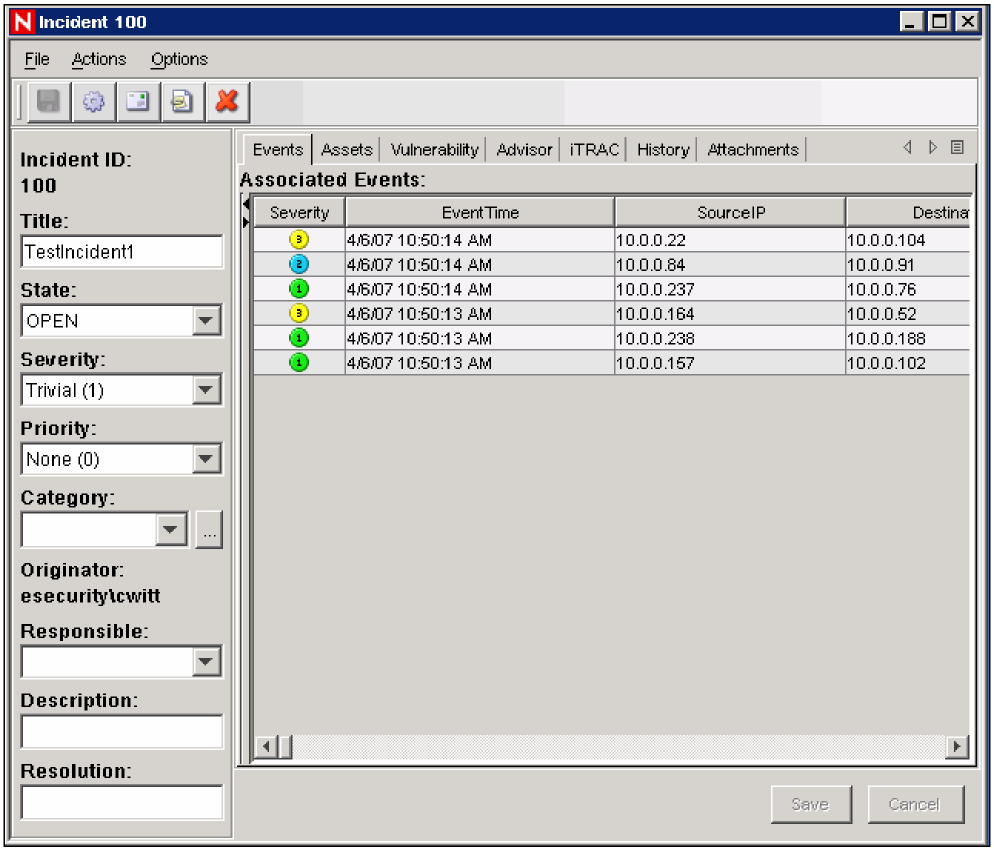


	State	Severity	Priority	Id	Res
Incident					
TestIncident1	OPEN	Trivial (1)	None (0)	100	

1 of 1

Figure 5-4: *Incident View Manager*

16. Double-click the incident to display.



Incident ID: 100

Title: TestIncident1

State: OPEN

Severity: Trivial (1)

Priority: None (0)

Category:

Originator: esecurity\cwitt

Responsible:

Description:

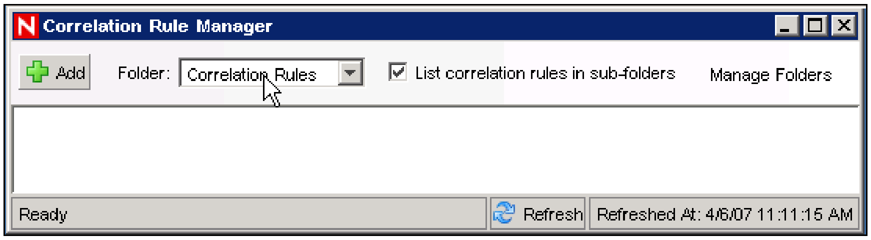
Resolution:

Associated Events:

Severity	EventTime	SourceIP	Destina
3	4/6/07 10:50:14 AM	10.0.0.22	10.0.0.104
2	4/6/07 10:50:14 AM	10.0.0.84	10.0.0.91
1	4/6/07 10:50:14 AM	10.0.0.237	10.0.0.76
3	4/6/07 10:50:13 AM	10.0.0.164	10.0.0.52
1	4/6/07 10:50:13 AM	10.0.0.238	10.0.0.188
1	4/6/07 10:50:13 AM	10.0.0.157	10.0.0.102

Figure 5-5: *Incident window*

17. Close the *Incident* window, go to *File* > *Exit* to close or by click “X” on the upper right corner of the window.
18. Click the *Analysis* tab. In the *Analysis* Navigator open the *Events* folder.
19. Click *Historical Event Queries*.
20. Click *Analysis* > *Create Report* or click *Create Report icon*. An *Event Query* window displays. 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)
21. Click *Begin Searching* icon.
22. To view the next batch of events, click *More*.
23. Rearrange the columns by dragging and dropping them and arrange the sort order by clicking in the column heading.
24. When your query is complete, it is added to the list of quick queries in the *Navigator*.
25. Go to *Correlation* tab. The *Correlation Rule Manager* displays.



Folder: Correlation Rules

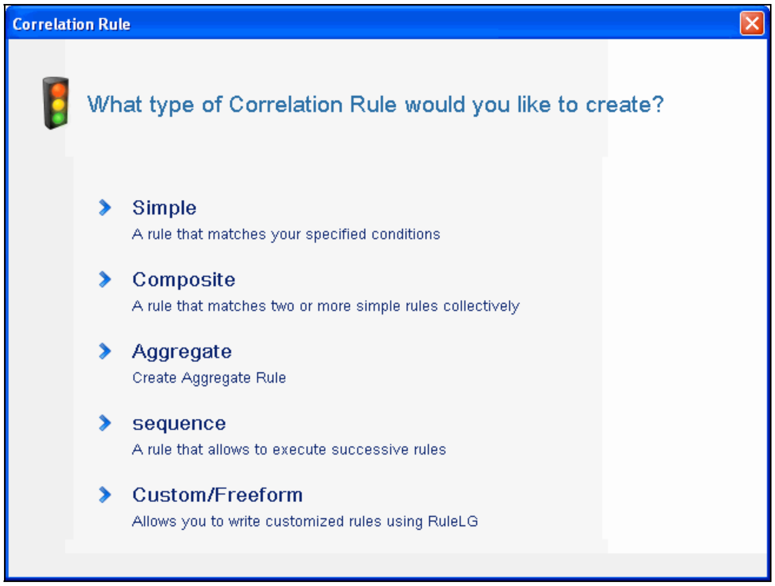
☑ List correlation rules in sub-folders

Ready

Refreshed At: 4/6/07 11:11:15 AM

Figure 5-6: *Correlation Rule Manager*

26. Click *Add*. The *Correlation Rule* wizard displays.

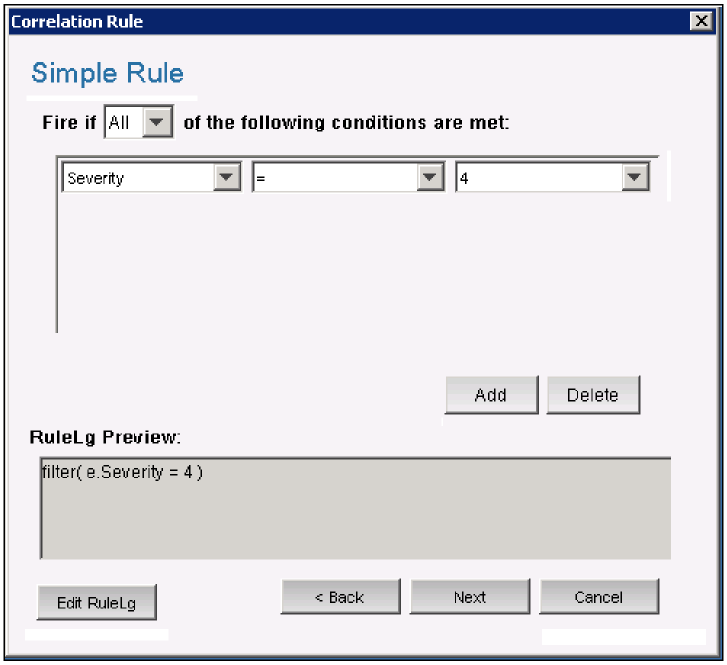


What type of Correlation Rule would you like to create?

- Simple
  A rule that matches your specified conditions
- Composite
  A rule that matches two or more simple rules collectively
- Aggregate
  Create Aggregate Rule
- sequence
  A rule that allows to execute successive rules
- Custom/Freeform
  Allows you to write customized rules using RuleLG

Figure 5-7: *Correlation Rule window*

27. Click *Simple*. *Simple Rule* window displays.



Fire if All of the following conditions are met:

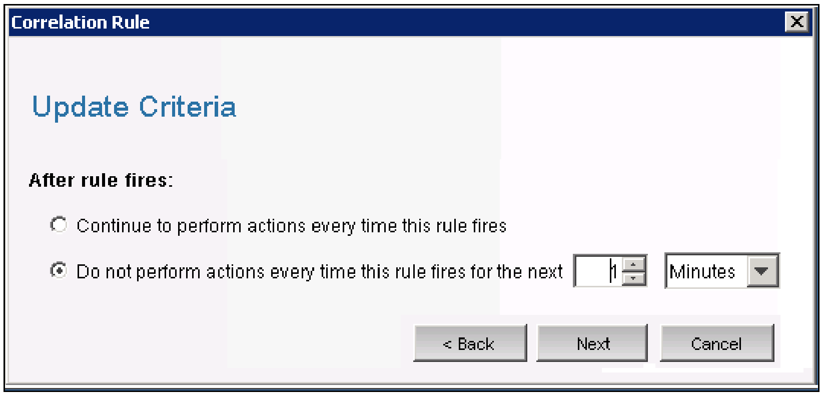
Severity = 4

RuleLg Preview:

```
filter( e.Severity = 4 )
```

Figure 5-8: *Correlation Rule-Simple Rule window*

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



Correlation Rule

Update Criteria

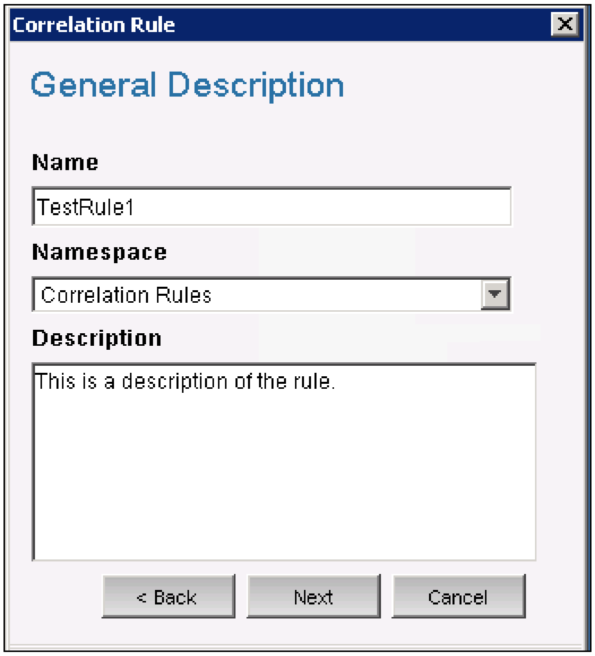
After rule fires:

○ Continue to perform actions every time this rule fires

● Do not perform actions every time this rule fires for the next 1 Minutes

Figure 5-9: *Correlation Rule-Update Criteria window*

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



Correlation Rule

General Description

Name

TestRule1

Namespace

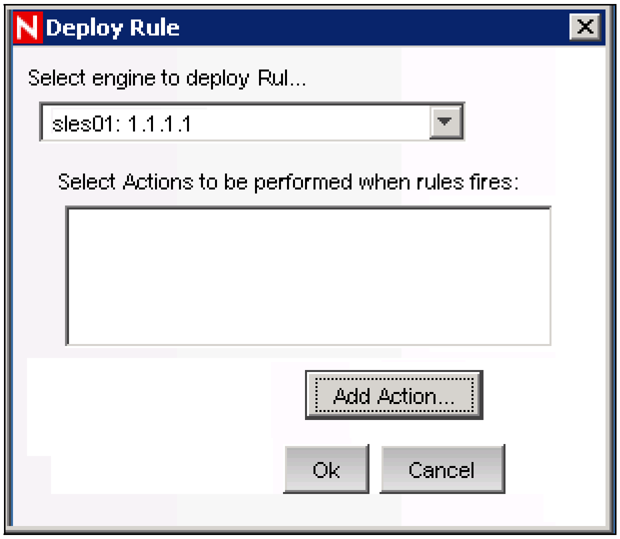
Correlation Rules

Description

This is a description of the rule.

Figure 5-10: *Correlation Rule-General Description window*

30. Name the rule as “TestRule1”, provide description, and click *Next*.
31. Select “*No, do not create another rule*” and click *Next.*
32. Open the *Correlation Rule Manager* window.
33. Highlight a rule and click *Deploy rules* link. The *Deploy Rule* window displays.



Deploy Rule

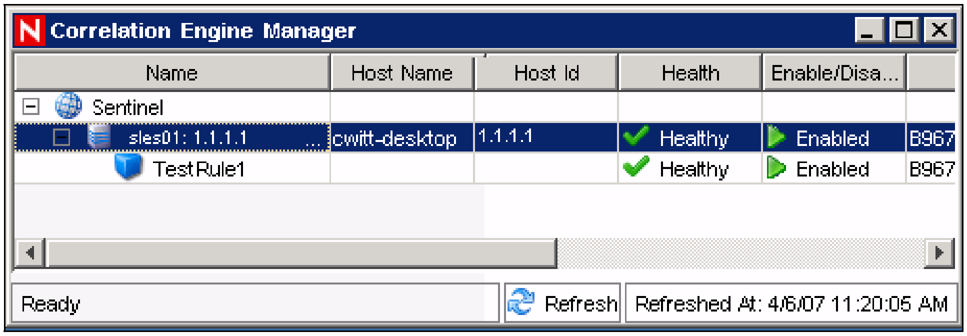
Select engine to deploy Rul...

sles01: 1.1.1.1

Select Actions to be performed when rules fires:

Figure 5-11: Deploy Rule window

34. In the *Deploy rule* window, select the Engine to deploy the rule from the drop-down list.
35. Select an action *Send email* to associate with the rule and click *OK*. Prior to associating an action, it should be created in Sentinel.
36. Select *Correlation Engine Manager*. Under the Correlation engine, you can see the rule is deployed/enabled.



Correlation Engine Manager

Name	Host Name	Host Id	Health	Enable/Disa...	
⊟ Sentinel					
⊟ sles01: 1.1.1.1 ...	cwitt-desktop	1.1.1.1	✓ Healthy	▶ Enabled	B967
TestRule1			✓ Healthy	▶ Enabled	B967

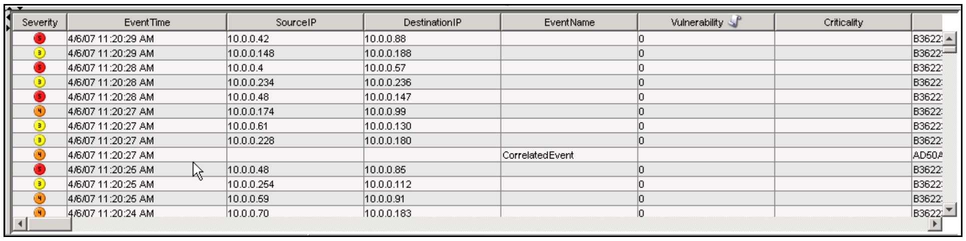
Ready

Refresh

Refreshed At: 4/6/07 11:20:05 AM

Figure 5-12: Correlation Engine Manager

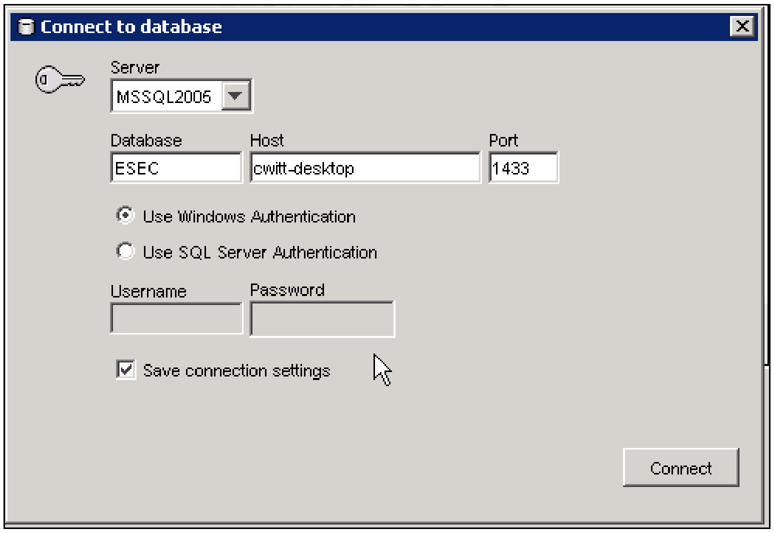
37. Go to *Active Views* tab and verify that the Correlated Event has generated.



Severity	EventTime	SourceIP	DestinationIP	EventName	Vulnerability	Criticality	
5	4/6/07 11:20:29 AM	10.0.0.42	10.0.0.88		0		B3622
3	4/6/07 11:20:29 AM	10.0.0.148	10.0.0.188		0		B3622
5	4/6/07 11:20:28 AM	10.0.0.4	10.0.0.57		0		B3622
3	4/6/07 11:20:28 AM	10.0.0.234	10.0.0.236		0		B3622
5	4/6/07 11:20:28 AM	10.0.0.48	10.0.0.147		0		B3622
4	4/6/07 11:20:27 AM	10.0.0.174	10.0.0.99		0		B3622
3	4/6/07 11:20:27 AM	10.0.0.61	10.0.0.130		0		B3622
3	4/6/07 11:20:27 AM	10.0.0.228	10.0.0.180		0		B3622
4	4/6/07 11:20:27 AM			CorrelatedEvent			AD50A
5	4/6/07 11:20:25 AM	10.0.0.48	10.0.0.85		0		B3622
3	4/6/07 11:20:25 AM	10.0.0.254	10.0.0.112		0		B3622
4	4/6/07 11:20:25 AM	10.0.0.59	10.0.0.91		0		B3622
4	4/6/07 11:20:24 AM	10.0.0.70	10.0.0.183		0		B3622

Figure 5-13: Active View

38. Close the *Sentinel Control Center*.
39. Double-click the *Sentinel Data Manager* (SDM) icon on the desktop.
40. Log into *SDM* using the Database Administrative User specified during installation (esecdba by default).



Connect to database

Server: MSSQL2005

Database: ESEC

Host: cwitt-desktop

Port: 1433

● Use Windows Authentication

○ Use SQL Server Authentication

Username:

Password:

☑ Save connection settings

Figure 5-14: *Connect to database window*

41. Click each tab to verify that you can access them.
42. Close *Sentinel Data Manager*.

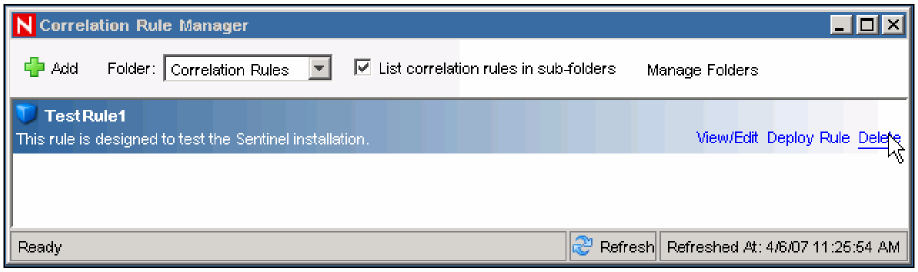
If you were able to proceed through all of these steps without errors, you have completed a basic verification of the Sentinel system installation.

Clean Up from Testing

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

To clean up after system testing:

1. Log into the system using the Sentinel Administrative User specified during installation (esecadm by default).
2. Go to the *Correlation* tab.
3. Open the *Correlation Engine Manager*.
4. Right-click TestRule1 in the *Correlation Engine Manager* and select *Undeploy*.
5. Open the *Correlation Rule Manager*.
6. Select *TestRule1* and click *Delete*.



Correlation Rule Manager

Folder: Correlation Rules

☑ List correlation rules in sub-folders

TestRule1

This rule is designed to test the Sentinel installation.

Ready

Refreshed At: 4/6/07 11:25:54 AM

Figure 5-15: *Correlation Rule Manager*

7. Go to 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. Go to the *Incidents* tab.
11. Open the *Incident View Manager*.
12. Select *TestIncident1*, right-click and select *Delete.*

Getting Started

You might now start using your system. For more information, see Quick Start in *Sentinel User Guide*.

6 Upgrade to Sentinel 6

This section provides a high-level overview on upgrading from the previous versions of Sentinel to Sentinel 6.0. The basic steps are backing up previous versions of Sentinel, installation/uninstallation of software, configuration changes and data migration.

NOTE: This document does not provide detailed procedures for performing the upgrade. Detailed information is provided in the Patch Installation documentation available at Novell Documentation Website (http://www.novell.com/documentation/sentinel6).

The patch installers available for patching to Sentinel 6.0 are:

- Sentinel 4.x to Sentinel 6.0
- Sentinel 5.x to Sentinel 6.0

There are several important changes between Sentinel 6.0 and previous versions that might affect your upgrade. More detail is provided in the Patch Installation documentation.

- There are minor database schema changes between Sentinel 5.x and 6.0 and major database schema changes between Sentinel 4.x and 6.0. Because of the schema changes, there is a new report library available with Sentinel 6.0, and custom reports might require modification
- The new Event Source Management framework might require some minor changes to Collectors to use new Connectors.
- There are new user permissions available for Sentinel Control Center users.
- System requirements have changed, including support for several new platforms.
- The directory structure has changed, so scripts that refer to directory paths might require updating.

Upgrade from Sentinel 5.x to Sentinel 6.0

Things to remember:

- Sentinel 5.x to Sentinel 6.0 is an in-place upgrade using Sentinel 6.0 Patch Installer.
- Data Migration from Microsoft SQL Server 2000 for Sentinel 5.x to Microsoft SQL Server 2005 for Sentinel 6.0 is supported. (SQL Server 2000 is no longer supported in Sentinel 6.)
- Data Migration from Oracle 9i for Sentinel 5.x to Oracle 10g for Sentinel 6.0 is supported.
- Data Migration from non-Unicode database to Unicode database is not supported.

- After Data Migration, correlation rules and iTRAC Workflow templates are not migrated. Correlation rules can be exported from 5.x and imported into 6.0. iTRAC workflow templates must be recreated in Sentinel 6.0.

To upgrade from Sentinel 5.x to Sentinel 6.0:

- Verify System Requirements; see "Supported Platforms and Best Practices" section.
  - Verify that the hardware specifications of the system meet the hardware requirements.
  - Verify that the operating system and database versions meet the system requirements.
- Perform back up of the required components
  - Sentinel Server
  - Sentinel Collector Manager
  - Crystal Reporting Server
  - Database Server
  - Collector Scripts
  - Export Correlation Rules
  - Back up iTRAC Workflows
- Perform Microsoft SQL Server or Oracle software upgrade, if needed.
- Run the Sentinel Patch Installer provided by Novell
- Perform manual configuration updates
  - Update user permissions
  - Update menu configurations
  - Reconfigure email settings
  - Redeploy Collectors (modifications might be needed for selected Collectors)
  - Redeploy reports

Upgrade from Sentinel 4.x to Sentinel 6.0

Things to remember:

- Data Migration from Microsoft SQL Server 2000 for Sentinel 4.x to Microsoft SQL Server 2005 for Sentinel 6.0 is supported. (SQL Server 2000 is no longer supported in Sentinel 6.)
- Data Migration from Oracle 9i for Sentinel 4.x to Oracle 10g for Sentinel 6.0 is supported.
- After Data Migration, the following objects are migrated from Sentinel 4.x to Sentinel 6.0:
  - Users and assigned permissions
  - Filters
  - Right-click menu configuration options
  - Renamed CV tags
  - Partition configurations
  - Cases from 4.x are migrated to 6.0 as incidents
  - Incidents and incident-related events
- After Data Migration, correlation rules and all events are not migrated.

Correlation rules can be exported from 4.x and imported into 6.0. Events that are part of an incident are migrated; other events are not.

To upgrade from Sentinel 4.x to Sentinel 6.0:

- Verify System Requirements; see "Supported Platforms and Best Practices" section.
  - Verify if the Hardware specifications of the system meet the Hardware requirements. You might need to update your Hardware as the hardware specifications for Sentinel 4.x and Sentinel 6.0 differ.
  - Verify that the operating system and database versions meet the system requirements.
- Perform back up of the required components
  - Sentinel Server
  - Sentinel Collector Manager
  - Crystal Reporting Server
  - Database Server
  - Collector Scripts
  - Export Correlation Rules
  - Back up iTRAC Workflows
- Install a clean Sentinel 6.0 Database
- Perform Data Migration from the Sentinel 4.x Database to the Sentinel 6.0 Database.
- Install a clean Sentinel 6.0 (excluding Database)
- Perform manual configuration updates
  - Update user permissions
  - Update menu configurations
  - Reconfigure email settings
  - Redeploy Collectors (modifications might be needed for selected Collectors)
  - Republish reports

7 Adding Sentinel Components

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, Sentinel Control Center is already installed on a machine where *Collector Builder* is also needed.

The Sentinel installer makes it simple to perform this kind of installation. First make sure you've satisfied the prerequisites of the additional component being installed as specified in the "Installing Sentinel 6" section. The requirements on the machine are likely to increase when installing additional components. Then run the Sentinel installer on the target machine just as 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: There can exist at most one instance of Advisor and the Communication Server in a distributed Sentinel installation.

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. 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 the "Installing Sentinel 6" section. 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

However, there can be more than one instance of the DAS_Binary process, which 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. Addtionally, the *Correlation Engine* and *Collector Manager* components can be load balanced by installing instances of these components on additional machines

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. 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 performance testing, see "Supported Platforms and Best Practices" section.

Multiple DAS_binary processes can be installed on the same machine or distributed across multiple machines.

To configure DAS_binary instances on different machines:

1. Use the Sentinel installer to install the DAS component on each of the other machines that will run a DAS_Binary process. All DAS_Binary's 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 DAS_Binary, make the following modifications:
   a. Login as *esecadm* (on UNIX) or an Administrator (on Windows) to any one of the machines that will 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.
   b. Add the following information to services section of the `configuration.xml` file:

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

   c. 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 one that is not running on the main Sentinel Server.
   a. 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.

b. 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

4. 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 (remove the # character from the beginning of the line):

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

```
and commenting the following line (insert the
# character at the beginning of the line):
```

```
#wrapper.app.parameter.1=../config/sentinel_pr
imary.xml
```

5. Make the following changes to the `das_binary.xml` file on one of the machines that will run a DAS_Binary process:

a. 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.

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

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

d. 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.

e. Add the following XML element to the *EventStoreService* component:

```
<obj-component-ref>

<name>DispatchManager</name>

<ref-id>EventStoreDispatchManager</ref-id>
```

```
</obj-component-ref>
```

f. Save the `das_binary.xml` file.

6. Copy the `das_binary.xml` file to all machines that will run a DAS_Binary process. Here 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,database_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.EventStoreServ
ice</class>

<property
name="handler">esecurity.event.create</propert
y>

<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.JDBCEvent
Store</class>

<property
name="insert.batchsize">600</property>

<property
name="insert.strategy">esecurity.ccs.comp.even
t.jdbc.JDBCLoadStrategy</property>

<property
name="insert.oci.workerCount">5</property>

<property
name="insert.oci.queueWaitTime">1</property>

<property
name="insert.oci.highWatermark">10000000</prop
erty>
```

```
<property
name="insert.oci.lowWatermark">9000000</proper
ty>

<property
name="insert.oci.optimizationFlag">on</propert
y>

<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>
```

7. To activate your changes, restart the Sentinel service on all machines where you modifications.

   On UNIX:

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

   On Windows:

   ```
   Restart the "Sentinel" service using the
   Windows Service Manager.
   ```

To configure multiple DAS_binary instances on the same machine:

1. Login as *esecadm* (on UNIX) or an Administrator (on 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 srv_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.cac
he -
Desecurity.dataobjects.config.file=/xml/BaseMetaD
ata.xml -
Djava.util.logging.config.file=../config/das_bina
ry_log.prop -
Dcom.esecurity.configurationfile=../config/config
uration.xml -
Djava.security.auth.login.config=../config/auth.l
ogin -
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>
  ```

11. Save the `das_binary.xml` files.
12. Locate the `das_binary_log.prop` file in the $ESEC_HOME/config (%ESEC_HOME%\config on Windows) directory.
13. 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`.
14. Rename the `das_binary_log.prop` files to match the names selected in step 5.
15. Restart the Sentinel service to activate your changes.

    On UNIX:

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

    On Windows:

    ```
    Restart the "Sentinel" service using the
    Windows Service Manager.
    ```

8 Communication Layer (iSCALE)

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.

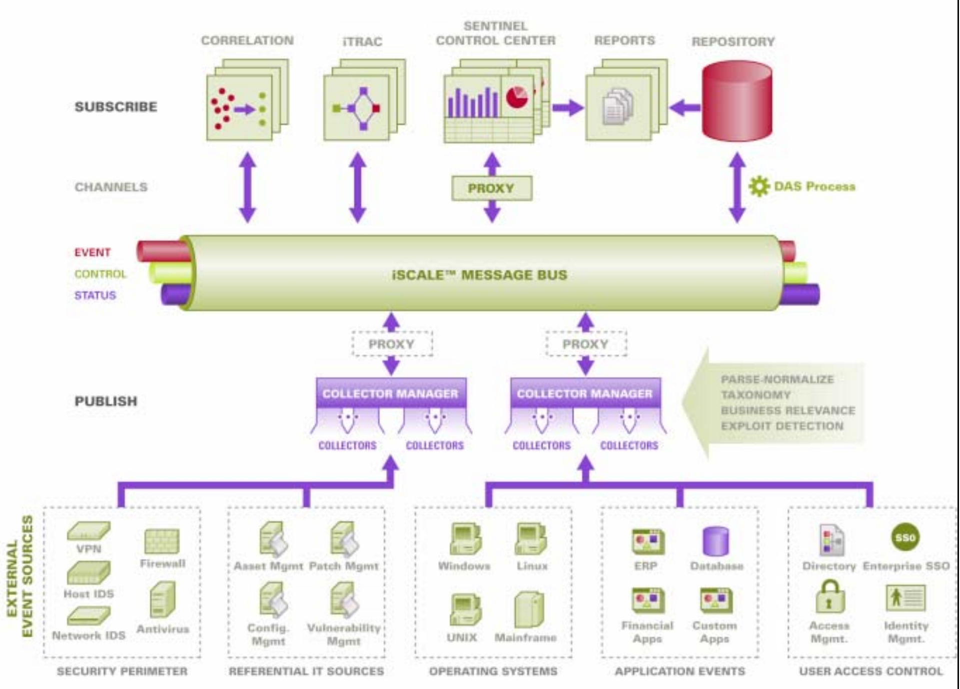


Figure 8-1: *Sentinel Architecture*

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.

SSL Proxy and Direct Communication

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

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.

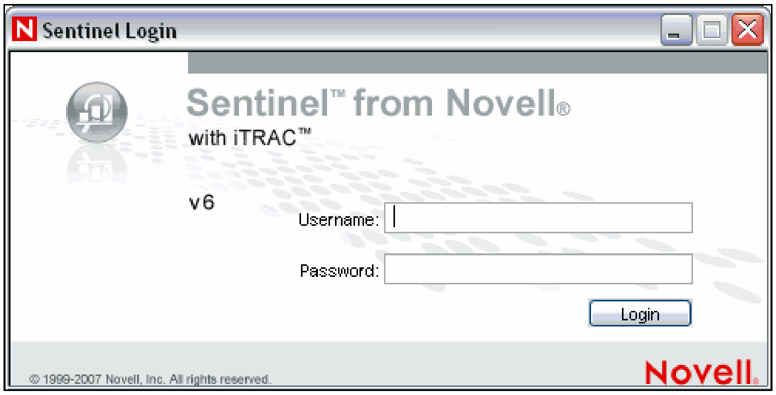
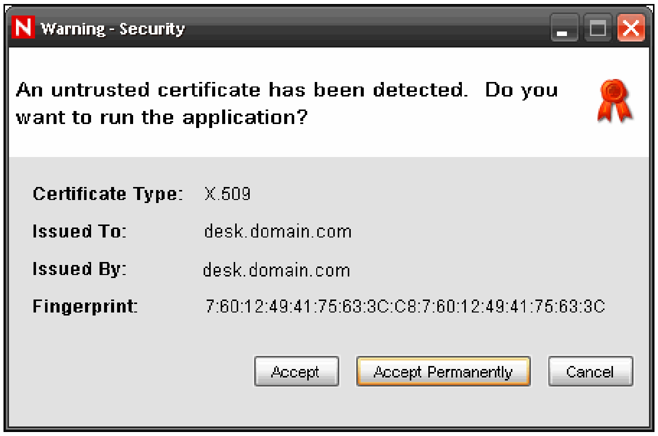


Figure 8-2: *Sentinel Login window*

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.



An untrusted certificate has been detected. Do you want to run the application?

Certificate Type: X.509

Issued To: desk.domain.com

Issued By: desk.domain.com

Fingerprint: 7:60:12:49:41:75:63:3C:C8:7:60:12:49:41:75:63:3C

Figure 8-3: *Warning-Security window*

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

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 under these circumstances:

- 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:B
      4: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\.proxyClientK
      eystore
```

6. Restart the Sentinel Service on the server hosting the Communication Server. Wait until DAS Proxy is done initializing.
7. Restart the Sentinel Service on the server hosting the *Collector Manager*.
8. Repeat these steps on all *Collector Managers* using the proxy communication.

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 machine that only has *Sentinel Control Center*, *Collector Builder*, *Sentinel Data Manager*, or *Collector Manager* (if connecting through the 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 the "Advisor Configuration" section.

Enabling Unlimited 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 at 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 the section "Changing the Communication Encryption Key".
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 "Advisor Configuration" section.

9 Crystal Reports for Windows

Crystal Business Objects Enterprise™ XI is the reporting tool used with Sentinel. This section discusses the installation and configuration of Crystal Reports Server for Sentinel. For more information on supported platforms for Crystal Reports Server in a Sentinel environment, see "Supported Platforms and Best Practices" section.

For more information on Crystal Reports Server XI Release 2 Service Packs, see http://support.businessobjects.com/downloads/service_packs/crystal_reports_server.asp

This section discusses running Crystal Reports Server on Windows. For more information on running Crystal Reports Server on Linux/Solaris, see "Crystal Reports for Linux/Solaris" section.

To Install Crystal Reports Server:

1. Install Microsoft IIS and ASP.NET
2. Install Microsoft SQL (depending on configuration as Windows authentication or SQL Server authentication)
3. For Chinese (Traditional & Simple) and Japanese users only: Install Asian Fonts (for example, Arial Unicode MS) to view reports in these languages.
4. Install Crystal Server
   - Configuring Open Database Connectivity (ODBC) for SQL Authentication

   or

   - Installing and Configuring Oracle 9i Client Software
5. Configure `inetmgr`
6. Patch Crystal reports
7. Publish (Importing) Crystal reports

8. Set a *Named User* account
9. Test connectivity to the Web Server
10. Increase Crystal Enterprise Server Report Refresh Record Limit (recommended)
11. Configure Sentinel Control Center to Integrate with Crystal Enterprise Server.

NOTE: You must install the components in the order given above.

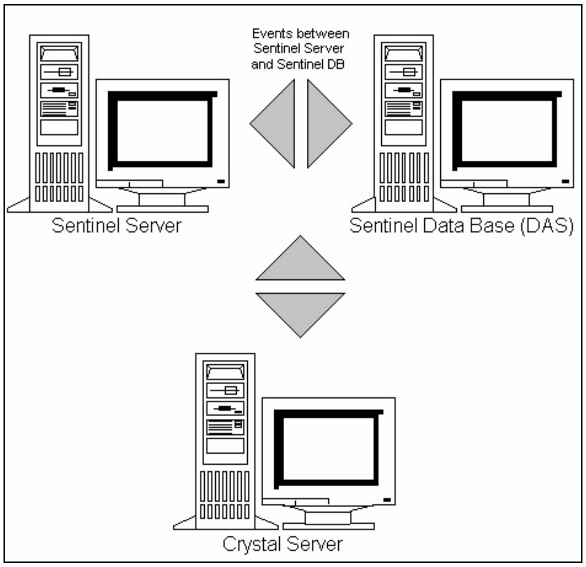


Figure 9-1: *Events between Sentinel Server, Crystal Server and Sentinel DB*

Overview

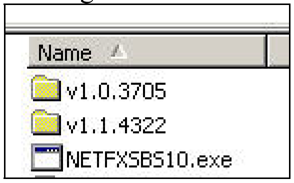
Crystal Reports Server requires a database to store information about the system and its users. This database is known as the Central Management Server (CMS) database. The CMS is a server that stores information about the Crystal Reports Server system. Other components of Crystal Reports Server can access this information as required.

It is required to set up a CMS database on top of a Local Microsoft SQL Server database. Although the Crystal Reports Server installer allows you to set up the CMS database on top of MSDE database, this configuration is not supported for Sentinel.

System Requirements

Windows® 2003 Server with 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® 2000 Server.

.NET Framework 1.1 or 2.0 (Installed by default on Windows 2003) To determine which version of .NET Framework is on your machine, go to %SystemRoot%\Microsoft.NET\Framework. The highest numerical folder should not be greater than v.1.1.xxxx. For example:



Name

v1.0.3705

v1.1.4322

NETFXSBS10.exe

__Figure 9-2:__ Version of .NET Framework

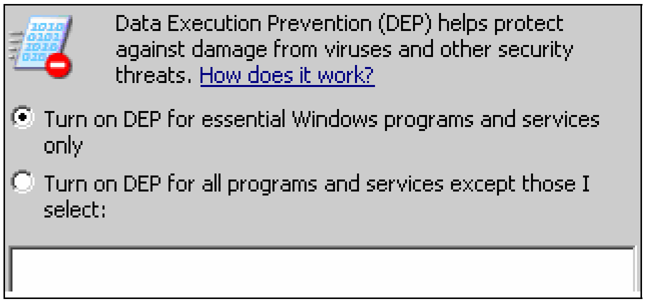
For more information on supported platforms for Crystal Reports Server in a Sentinel environment, see "Supported Platforms and Best Practices" section.

Configuration Requirements

1. Make sure the account used to install Crystal Reports Server is a local administrator.
2. Set Data Execution Prevention (DEP) to run on essential Windows programs and services only. This is particularly helpful to avoid "Error 1920. *Service Crystal Report Cache Server* on Windows 2003".

   DEP is accessed through *Control Panel > System > Advanced tab > Performance Settings > Data Execution Prevention.*

   Select *Turn on DEP for essential Windows programs and services only*.

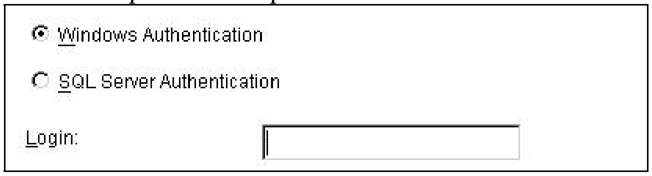
   Data Execution Prevention (DEP) helps protect against damage from viruses and other security threats. How does it work?

   ● Turn on DEP for essential Windows programs and services only

   ○ Turn on DEP for all programs and services except those I select:

   __Figure 9-3:__ Data Execution Prevention (DEP)

   If you are planning to run Sentinel reports using Windows NT authentication, make sure windows domain account for Sentinel Report user already exists on Sentinel database. This is done during Sentinel install by selecting *Windows Authentication* when setting the *Authentication Method for the Sentinel Report user* as per the illustration below.

   ● Windows Authentication

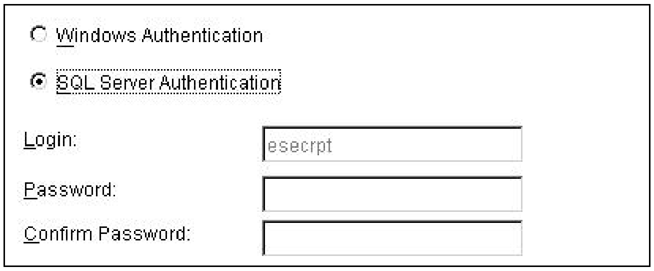
   ○ SQL Server Authentication

   Login:

   __Figure 9-4:__ Authentication Method

3. If you are planning to run Sentinel reports using SQL Server authentication (also required for Sentinel Oracle installations), make sure the SQL Server login (esecrpt) already exists on Sentinel database.

   - **For Sentinel Microsoft SQL database:** This is done during Sentinel install for Microsoft SQL by selecting *SQL Server Authentication* when setting the *Authentication Method for the Sentinel Report user* as per the illustration below.



○ Windows Authentication

● SQL Server Authentication

Login: esecrpt

Password:

Confirm Password:

Figure 9-5: Authentication Method-SQL Server Authentication

- **For Sentinel Oracle database:** This is done during Sentinel install for Oracle. esecrpt assumes the same password as esecadm.
- **For Oracle:** Oracle 9i Client Release 2 (9.2.0.1.0), install this before installing Crystal BusinessObjects Enterprise™ XI R2.
- **For Microsoft SQL Server 2005:** Install Microsoft SQL Server 2005 prior to installing Crystal Reports Server XI R2.

4. Video resolution of 1024 x 768 or higher
5. Install Microsoft Internet Information Server (IIS) and ASP.NET

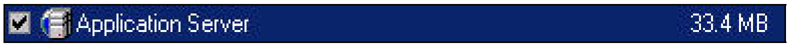
NOTE: Sentinel does not support MSDE. Install Microsoft SQL Server 2005 prior to installing Crystal Reports Server XI R2.

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

To add these Windows components you might need the *Windows 2003 Server* installation CD.

To Install IIS and ASP.NET:

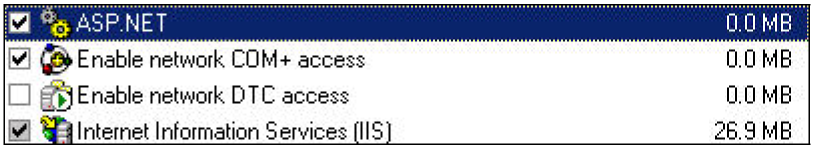
1. Go to *Control Panel > Add/Remove Programs*.
2. In the left vertical panel, click *Add/Remove Windows Components*.
3. Select *Application Server*.



☑ Application Server 33.4 MB

Figure 9-6: Application Server

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



☑	ASP.NET	0.0 MB
☑	Enable network COM+ access	0.0 MB
□	Enable network DTC access	0.0 MB
☑	Internet Information Services (IIS)	26.9 MB

Figure 9-7: ASP.NET and Internet Information Services (IIS) selection

6. Click *OK*.
7. Click *Next*. You might be prompted for the Windows installation CD.
8. Click *Finish*.

Known Issues

- **Installing Crystal Reports:** You are issued with two keys, one for Crystal Reports Server and the other for Crystal Reports Developer. Make sure to use the Crystal Reports Server key when installing Crystal Reports Server.

- **Uninstalling Crystal Reports:** In the event that you need to uninstall Crystal Reports Server, there is a manual uninstall procedure available that cleans out the registry keys. This is particularly useful if your installation gets corrupted. Go to the following BusinessObjects Web site for procedures in manually uninstalling BusinessObjects Enterprise XI R2, (http://support.businessobjects.com/library/kbase/articles/c2017905.asp).

  NOTE: The above URL was correct as of publication of this document.

Using Crystal Reports

For more information on using Crystal Reports for Sentinel Reporting, see Crystal Reports Documentation (http://support.businessobjects.com/documentation/product_guides/default.asp) and *Sentinel User Guide*.

Installation Overview

Installation Overview for Crystal with SQL Server 2005

These are the high-level steps for installing Crystal Server with a Microsoft SQL Server 2005 Sentinel database using Windows Authentication or SQL Authentication. Each step is described in more detail in the rest of this section.

1. Install Crystal Reports Server XI R2
   - If you selected *Windows Authentication* for the Sentinel Report user when installing Sentinel, see "Installing Crystal Server for Microsoft SQL Server 2005 with Windows Authentication".
   - If you selected *SQL Authentication* for the Sentinel Report user when installing Sentinel, see "Installing Crystal Server for Microsoft SQL Server 2005 with SQL Authentication or for Oracle"
2. "Configure Open Database Connectivity (ODBC)"
3. "Map Crystal Reports for use with Sentinel"
4. "Patch Crystal Reports"
5. "Publish Reports"
6. "Set the Named User Account"
7. Create a Crystal Web Page ("Configuring .NET Administration Launchpad")
8. "Configure Sentinel to the Crystal Enterprise Server"

NOTE: These steps must be performed in order.

Installation Overview for Crystal with Oracle

These are the high-level steps for installing Crystal Server with an Oracle Sentinel database. Each step is described in more detail in the rest of this section.

To properly install Crystal Reports, perform the following procedure in the order presented.

1. Install Oracle Client and "Configure Oracle native driver".
2. For Chinese (Traditional & Simple) and Japanese users only: Install Asian Fonts (for example, Arial Unicode MS) to view reports in these languages.

3. Install Crystal Reports Server XI R2. For more information, see "Installing Crystal Server for Microsoft SQL Server 2005 with SQL Authentication or for Oracle".
4. "Map Crystal Reports for use with Sentinel"
5. "Import Crystal Report Templates"
6. Create a Crystal Web Page ("Configuring .NET Administration Launchpad")
7. "Configure Sentinel to the Crystal Enterprise Server"

NOTE: These steps must be performed in order.

Installation

This section covers how to install Crystal Server for:

- "Microsoft SQL Server 2005 Sentinel database with Windows Authentication"
- "Microsoft SQL Server 2005 Sentinel database with SQL Server Authentication"
- "Oracle Sentinel database"

Installing Crystal Server for Microsoft SQL Server 2005 with Windows Authentication

To Install Crystal Server with Windows Authentication:

1. Install Microsoft SQL Server 2005 in mixed mode.
2. Launch *Microsoft SQL Server Management Studio*.
3. In the navigation pane, expand *Databases*.

   Highlight and right-click *Database* and select *New Database*

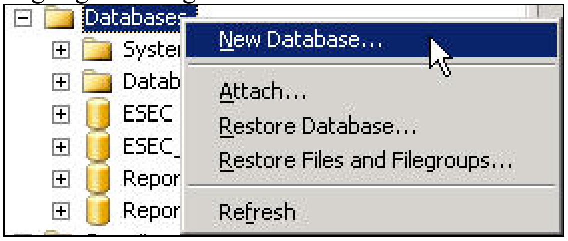
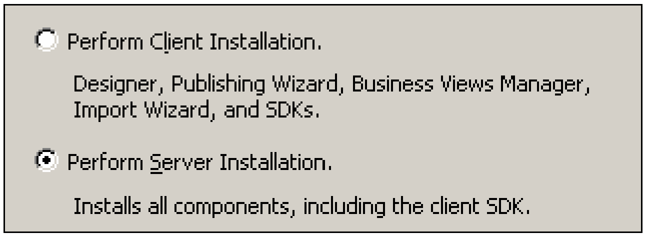


Figure 9-8: *Creating New Database*

4. Under the *Database name* field, provide *BOE115* and click *OK*.
5. Exit *Microsoft SQL Server Management Studio*.
6. Insert the *Crystal Reports XI R2 Server* CD into the CD-ROM.
7. If Autoplay is disabled on your machine, run `setup.exe`.
8. Select the Crystal Reports setup language.

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



○ Perform Client Installation.

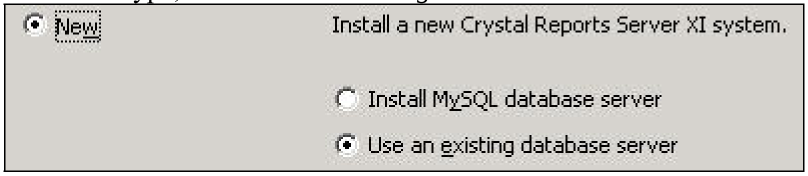
Designer, Publishing Wizard, Business Views Manager, Import Wizard, and SDKs.

● Perform Server Installation.

Installs all components, including the client SDK.

Figure 9-9: *Select Client or Server Installation window*

10. Provide Crystal license key (obtained from Novell Customer Center (https://secure-www.novell.com/center/regadmin)).
11. Specify a destination folder.
12. For install type, select *Use an existing database server*.



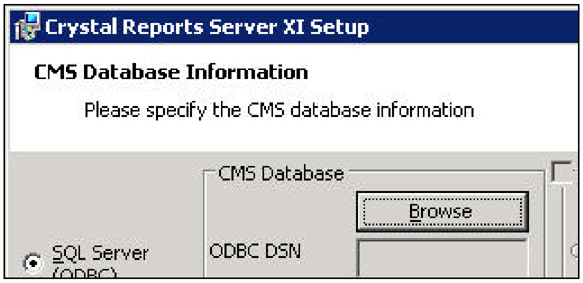
● New — Install a new Crystal Reports Server XI system.

○ Install MySQL database server

● Use an existing database server

Figure 9-10: *Install Type*

13. In the *CMS Database* Pane, click *Browse*.



Crystal Reports Server XI Setup

CMS Database Information

Please specify the CMS database information

CMS Database

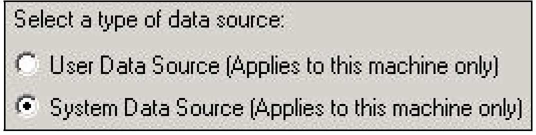
Browse

● SQL Server (ODBC)

ODBC DSN

Figure 9-11: *CMS Database Pane*

14. Click the *Machine Data Source* tab. Click *New*.
15. Select *System Data Source*.



Select a type of data source:

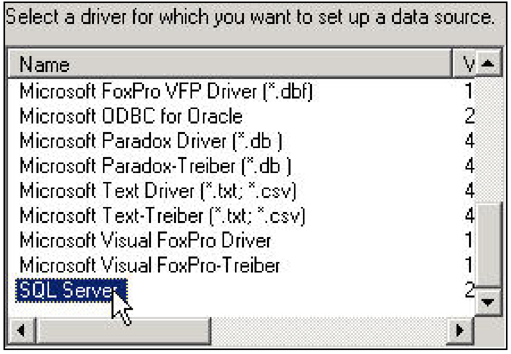
○ User Data Source (Applies to this machine only)

● System Data Source (Applies to this machine only)

Figure 9-12: *Data Source type selection*

Click *Next*.

16. Scroll down and select *SQL Server* and click *Next*.

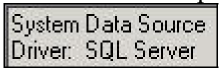


Select a driver for which you want to set up a data source.

Name	V
Microsoft FoxPro VFP Driver (*.dbf)	1
Microsoft ODBC for Oracle	2
Microsoft Paradox Driver (*.db)	4
Microsoft Paradox-Treiber (*.db)	4
Microsoft Text Driver (*.txt; *.csv)	4
Microsoft Text-Treiber (*.txt; *.csv)	4
Microsoft Visual FoxPro Driver	1
Microsoft Visual FoxPro-Treiber	1
SQL Server	2

Figure 9-13: *Data Source Driver*

17. A new source displays, click *Finish*.



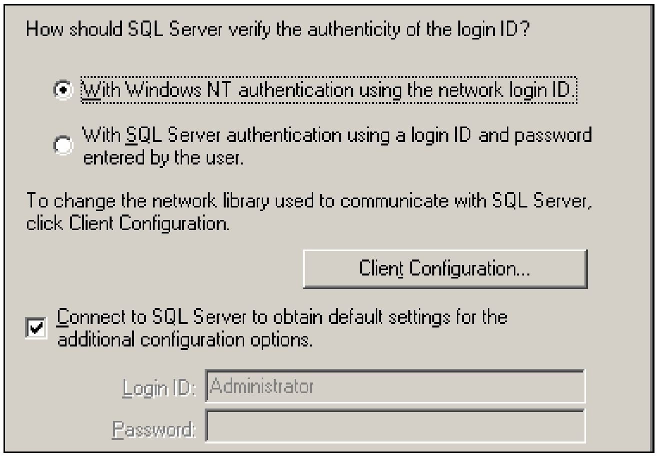
System Data Source
Driver: SQL Server

Figure 9-14: *Source display*

18. In the *New Data Source to SQL Server* window, specify:
    - Name of your data source (For example, BOE_XI)
    - Description (optional)
    - For Server, click the down arrow and select *(local)*

    Click *Next*.

19. If not already, select *With Windows NT,* Click *Next*.



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: Administrator

Password:

Figure 9-15: *SQL Server Verification*

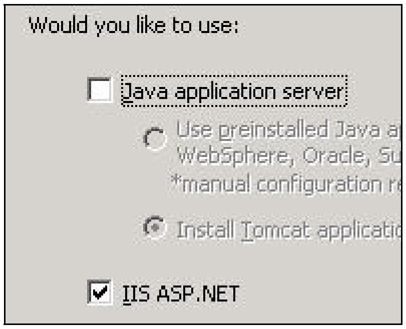
NOTE: The Login ID (dimmed -not available) is your Windows login name.

20. Check *Change the default database to* check box. Change your default database to *BOE115*. Click *Next*.
21. In the *Create a New Data Source to SQL Server* window, click *Finish*.
22. Click *Test Data Source* and test the data source. After testing of data source, click *OK*.
23. In the *Select Data Source* window, highlight *BOE115* and continue to click *OK* until you get to the *SQL Server Login*. Ensure that *Use Trusted Connection* is selected. Click *OK*.

NOTE: The Login ID (dimmed -not available) is your Windows login name.

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

NOTE: If you have not installed IIS and ASP.NET through *Control Panel > Add Remove Programs > Add/Remove Windows Components*, IIS ASP.NET will be dimmed (not available).



Would you like to use:

☐ Java application server

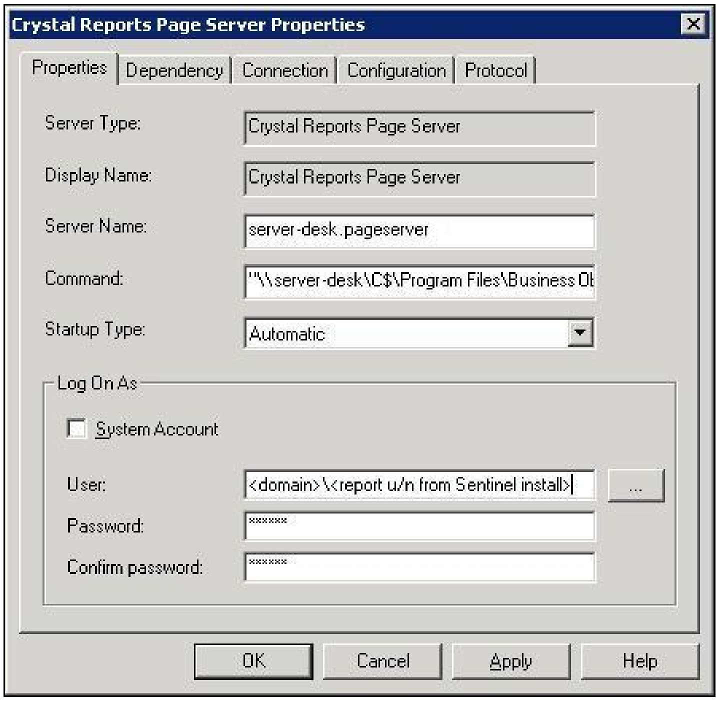
○ Use preinstalled Java a
WebSphere, Oracle, Su
*manual configuration r

● Install Tomcat applicati

☑ IIS ASP.NET

Figure 9-16: *Web Component Adapter Type window*

25. After installation, you will need to change the log on account for Crystal Reports Page Server and Crystal Reports Job Server to Sentinel Report User domain account.
    - Click *Start* > *Programs* > *BusinessObjects* > *Crystal Reports Server* > *Central Configuration Manager*.
    - Right-click *Crystal Reports Page Server* and select *stop*.
    - Right-click *Crystal Reports Page Server* again and select *Properties*.
    - Uncheck *Log On As System Account* and specify the Sentinel Report User domain account username and password that was used for the Sentinel Report User during your Sentinel install. Click *OK*.



Crystal Reports Page Server Properties

Server Type: Crystal Reports Page Server

Display Name: Crystal Reports Page Server

Server Name: server-desk.pageserver

Command: "\\server-desk\C$\Program Files\Business Ot

Startup Type: Automatic

Log On As

☐ System Account

User: <domain>\<report u/n from Sentinel install>

Password: ******

Confirm password: ******

Figure 9-17: *Crystal Reports Page Server Properties window*

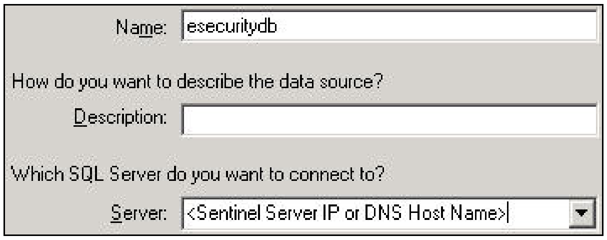
26. Highlight Crystal Reports Page Server and right-click to start.

Configuring Open Database Connectivity (ODBC) for Windows Authentication

This procedure sets up an ODBC data source between Crystal Reports on Windows and SQL Server. This has to be performed on the Crystal Server machine.

To Set up an ODBC data source for Windows Authentication:

1. Go to Windows *Control Panel>Administrative Tools>Data Sources (ODBC)*.
2. Click *System DSN* tab and click *Add*.
3. Select *SQL Server*. Click *Finish*.
4. A window displays prompting for driver configuration information:
   - *Data Source name*, specify esecuritydb
   - *Description* field (optional), provide a description
   - *Server* field, provide your host name or IP address of your Sentinel Server



Name: esecuritydb

How do you want to describe the data source?

Description:

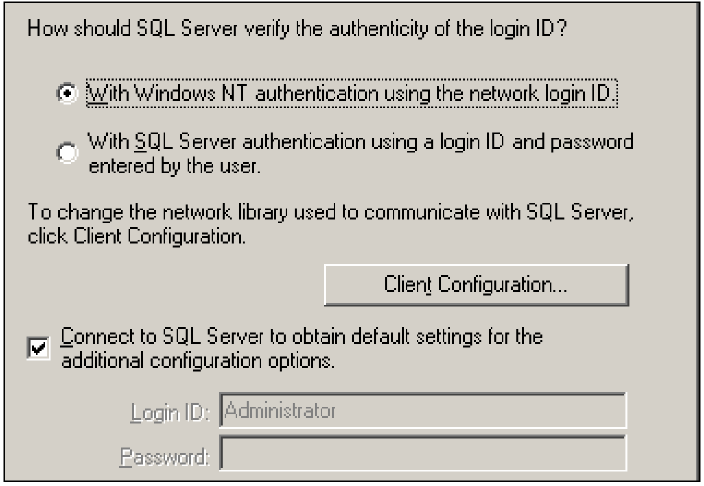
Which SQL Server do you want to connect to?

Server: <Sentinel Server IP or DNS Host Name>

Figure 9-18: Driver Configuration

Click *Next*.

In the next window, select *Windows Authentication*.



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: Administrator

Password:

Figure 9-19: *SQL Server Authenticity*

NOTE: The Login ID (dimmed -not available) is your Windows login name.

5. In the next window select:
   - Change the Sentinel database (Default name is ESEC)
   - Leave all the default settings

Click *Next*.

6. Click *Finish*.
7. Click *Test Data Source.* A connection is established. Click *OK* until you exit.

Installing Crystal Server for Microsoft SQL Server 2005 with SQL Authentication

To Install Crystal Server with SQL Authentication:

1. Install Microsoft SQL Server 2005.
2. Launch *Microsoft SQL Server Management Studio*.
3. In the navigation pane, expand *Databases*.

   Highlight and right-click *Database* and select *New Database*.

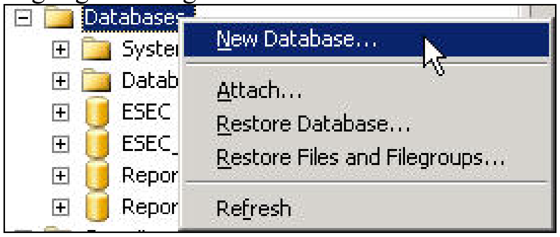
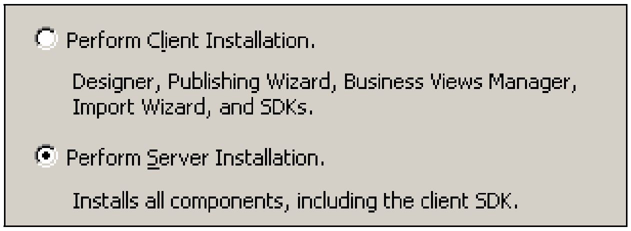


Figure 9-20: *Creating New Database*

4. Under the *Database name* field, provide *BOE115* and click *OK*.
5. Exit *Microsoft SQL Server Management Studio*.
6. Insert the *Crystal Reports XI R2 Server* CD into the CD-ROM.
7. If Autoplay is disabled on your machine, run `setup.exe`.
8. Select the Crystal Reports setup language.
9. In the *Select Client or Server Installation* window, select *Perform Server Installation*.



○ Perform Client Installation.

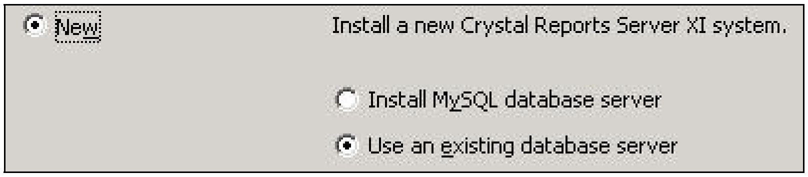
Designer, Publishing Wizard, Business Views Manager, Import Wizard, and SDKs.

● Perform Server Installation.

Installs all components, including the client SDK.

Figure 9-21: *Select Client or Server Installation window*

10. Provide Crystal license key (obtained from Novell Customer Center (https://secure-www.novell.com/center/regadmin))
11. Specify a destination folder.
12. For install type, select *Use an existing database server*.



● New — Install a new Crystal Reports Server XI system.

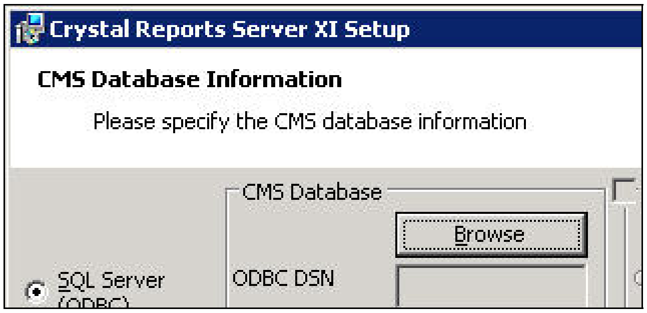
○ Install MySQL database server

● Use an existing database server

Figure 9-22: *Use an existing database server selection*

NOTE: Crystal Server and Microsoft SQL Server must reside on the same machine.

13. In the *CMS Database* Pane, click *Browse*.



Crystal Reports Server XI Setup

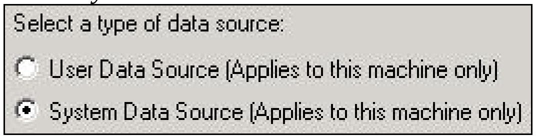
CMS Database Information

Please specify the CMS database information

Figure 9-23: *CMS Database Pane*

14. Click the *Machine Data Source* tab; click *New*.

    Select *System Data Source*.



Select a type of data source:

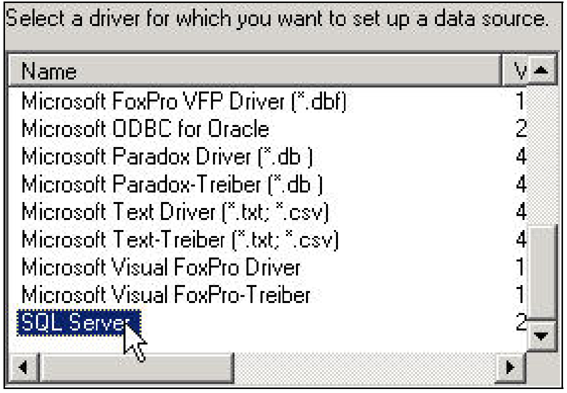
○ User Data Source (Applies to this machine only)

● System Data Source (Applies to this machine only)

Figure 9-24: *Data Source Type selection*

Click *Next*.

Scroll down and select *SQL Server* and click *Next*.

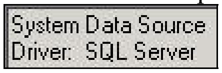


Select a driver for which you want to set up a data source.

Name	V
Microsoft FoxPro VFP Driver (*.dbf)	1
Microsoft ODBC for Oracle	2
Microsoft Paradox Driver (*.db)	4
Microsoft Paradox-Treiber (*.db)	4
Microsoft Text Driver (*.txt; *.csv)	4
Microsoft Text-Treiber (*.txt; *.csv)	4
Microsoft Visual FoxPro Driver	1
Microsoft Visual FoxPro-Treiber	1
SQL Server	2

Figure 9-25: *Data Source Driver selection*

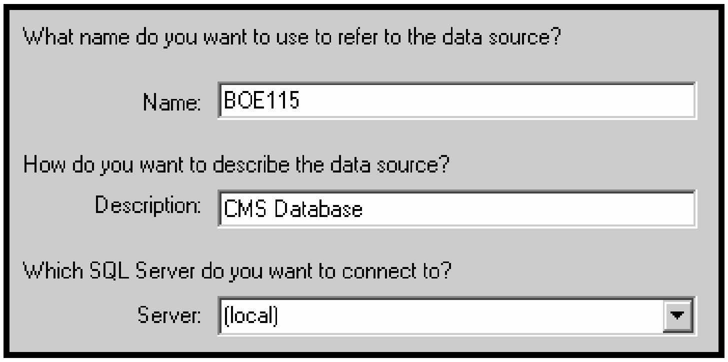
A new source displays, click *Finish*.



System Data Source
Driver: SQL Server

Figure 9-26: *Source Display*

15. Right-click *Databases* and select *Create New Database* (BOE115).
16. In *New Data Source to SQL Server* window, specify:
    - Name of your data source (For example, BOE115)
    - *Description* (optional)
    - For Server, click the down arrow and select *(local)*


What name do you want to use to refer to the data source?

Name: BOE115

How do you want to describe the data source?

Description: CMS Database

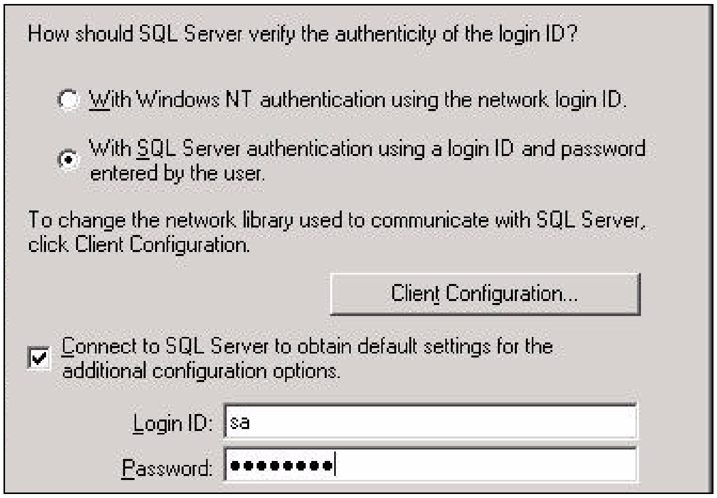
Which SQL Server do you want to connect to?

Server: (local)

Figure 9-27: *New Data Source to SQL Server window*

Click *Next*.

17. Select *With SQL Server authentication*, provide sa and the password for sa. Click *Next*.


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: sa

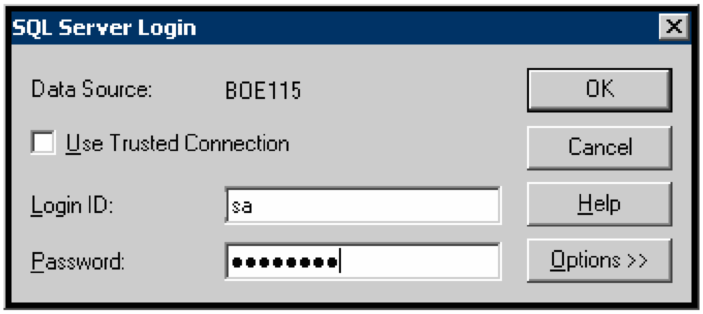
Password: ●●●●●●●●●

Figure 9-28: *SQL Server Authenticity verification*

Check the *Change the default database to:* check box. Change your default database to *BOE115*. Click *Next*.

18. In the *Create a New Data Source to SQL Server* window, click *Finish*.
19. Click *Test Data Source*. Click *OK*.

In the *Select Data Source* window, highlight *BOE115* and continue to click *OK* until you get to the *SQL Server Login*. Ensure that *Use Trusted Connection* is NOT selected. Click *OK*. Click *Next*.


SQL Server Login

Data Source: BOE115

□ Use Trusted Connection

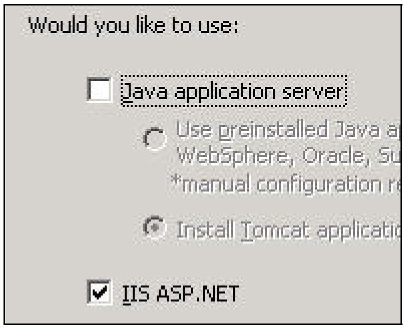
Login ID: sa

Password: ●●●●●●●●●

Figure 9-29: *SQL Server Login*

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

NOTE: If you have not installed IIS and ASP.NET through *Control Panel > Add Remove Programs > Add/Remove Windows Components*, IIS ASP.NET will be dimmed (not available).



Would you like to use:

□ Java application server

○ Use preinstalled Java a
WebSphere, Oracle, Su
*manual configuration r

● Install Tomcat applicati

☑ IIS ASP.NET

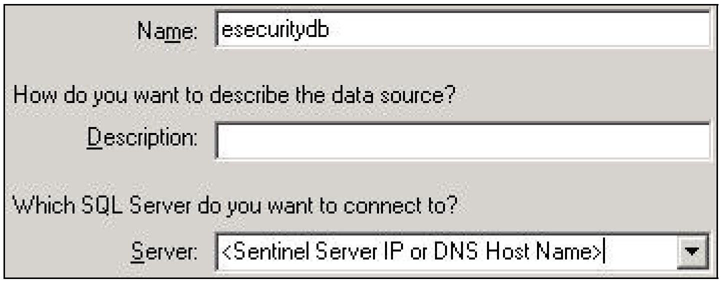
Figure 9-30: *Web Component Adapter Type window*

Configuring Open Database Connectivity (ODBC) for SQL Authentication

This procedure sets up an ODBC data source between Crystal Reports on Windows and SQL Server. This has to be performed on the Crystal Server machine.

To Set up an ODBC data source for Windows:

1. Go to Windows *Control Panel > Administrative Tools > Data Sources (ODBC)*.
2. Click *System DSN* tab and click *Add*.
3. Select *SQL Server*. Click *Finish*.
4. A window displays prompting for driver configuration information:
   - *Data Source name*, specify esecuritydb
   - *Description* field (optional), provide a description
   - *Server* field, specify your host name or IP address of your Sentinel Server



Name: esecuritydb

How do you want to describe the data source?

Description:

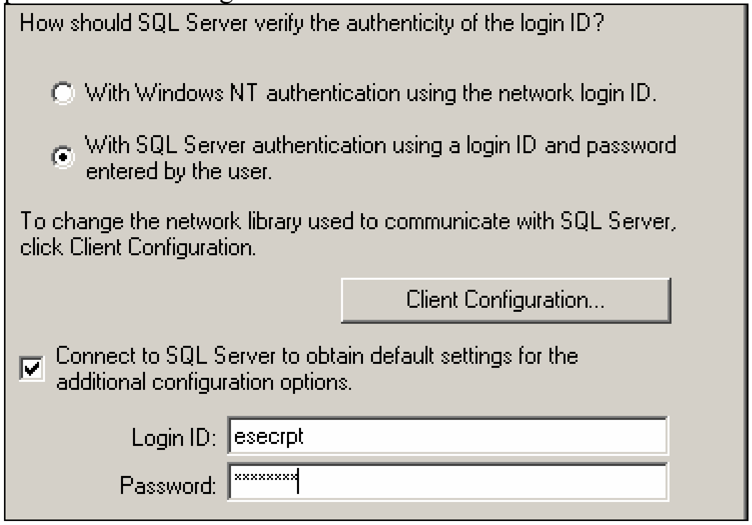
Which SQL Server do you want to connect to?

Server: <Sentinel Server IP or DNS Host Name>

Figure 9-31: *Driver Configuration*

Click *Next*.

5. In the next window, select *SQL Authentication*. Provide esecrpt and password as the Login ID. Click *Next*.



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: esecrpt

Password: ********

Figure 9-32: *SQL Server Authenticity verification*

6. In the next window select:
   - Change the Sentinel database (Default name is ESEC)
   - Leave all the default settings

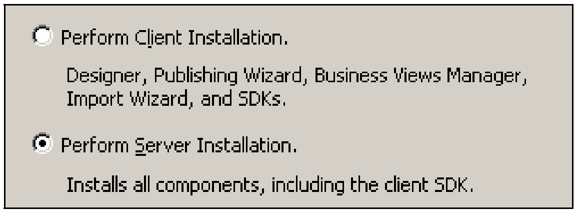
   Click *Next*; click *Finish*.

7. Click *Test Data Source*. After testing, click *OK*. Click *OK* until you exit.

Installing Crystal Server for Oracle

To Install Crystal Reports Server XI R2 for Oracle:

1. Insert the Crystal Reports XI R2 Server CD into the CD-ROM.
2. Select the Crystal Reports setup language.
3. In the *Select Client or Server Installation* window, select *Perform Server Installation*.



○ Perform Client Installation.

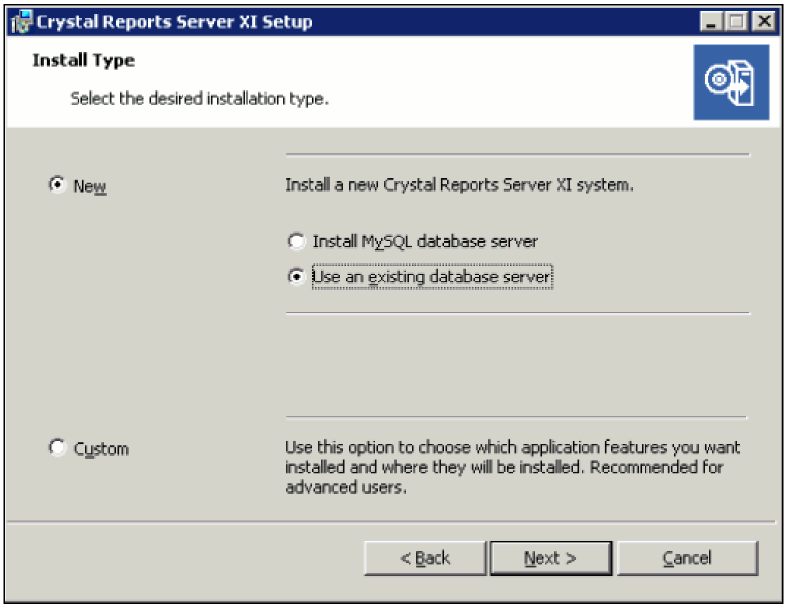
Designer, Publishing Wizard, Business Views Manager, Import Wizard, and SDKs.

● Perform Server Installation.

Installs all components, including the client SDK.

Figure 9-33: *Select Client or Server Installation window*

4. Select *Use an existing database server*.



Crystal Reports Server XI Setup

Install Type

Select the desired installation type.

● New — Install a new Crystal Reports Server XI system.

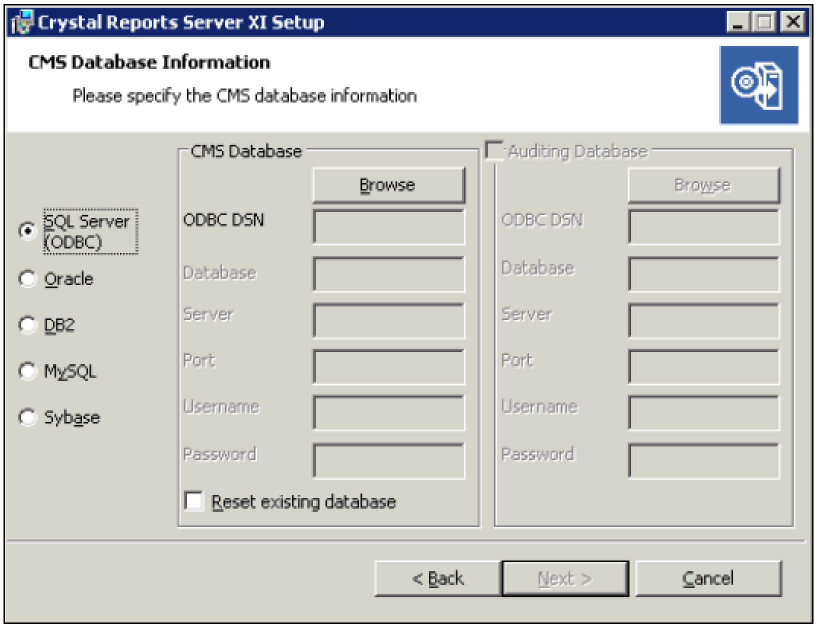
○ Install MySQL database server

● Use an existing database server

○ Custom — Use this option to choose which application features you want installed and where they will be installed. Recommended for advanced users.

Figure 9-34: *Crystal Reports Server XI Setup-Install Type*

The *CMS Database Information* window displays:



Crystal Reports Server XI Setup

CMS Database Information

Please specify the CMS database information

● SQL Server (ODBC)

○ Oracle

○ DB2

○ MySQL

○ Sybase

CMS Database

ODBC DSN	
Database	
Server	
Port	
Username	
Password	

□ Reset existing database

□ Auditing Database

ODBC DSN	
Database	
Server	
Port	
Username	
Password	

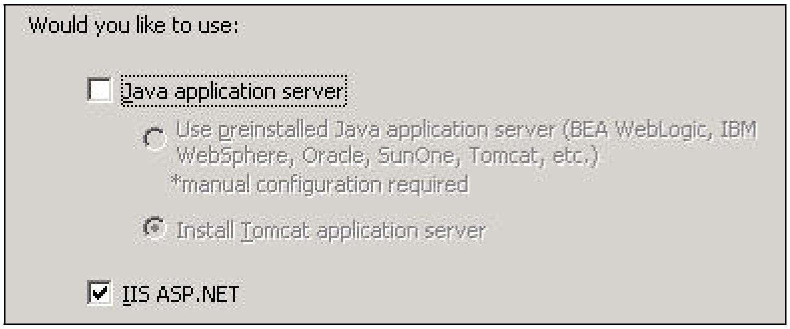
Figure 9-35: *Crystal Reports Server XI Setup-CMS Database Information*

Select *SQL Server (ODBC)* type and click *Browse* to select a DSN. After you select a DSN, you are prompted for Username and Password. Provide the required information and click *Next.*

NOTE: Crystal Server and Microsoft SQL Server 2005 must reside on the same machine.

5. Select *IIS ASP.NET*.

NOTE: If you have not installed IIS and ASP.NET through *Control Panel > Add Remove Programs > Add/Remove Windows Components*, IIS ASP.NET will be dimmed (not available). Installing IIS and ASP.NET is a prerequisite to this installation.



Would you like to use:

☐ Java application server

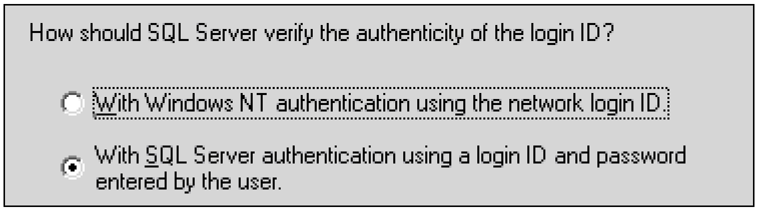
○ Use preinstalled Java application server (BEA WebLogic, IBM WebSphere, Oracle, SunOne, Tomcat, etc.)
*manual configuration required

● Install Tomcat application server

☑ IIS ASP.NET

Figure 9-36: *IIS ASP.NET selection*

6. You will be prompted to specify your Authentication Mode. Select *SQL Server authentication*.



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.

Figure 9-37: *Authentication Mode specification*

Crystal Reports supports direct access to Oracle databases. 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.

NOTE: In order for Crystal Reports 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.

Installing and Configuring Oracle Client Software

When installing Oracle Client:

- Accept the default install location
- No – for Perform Typical Configuration
- No – for Directory Service
- Select *Local*
- TNS Service Name: ESEC
- User (optional): esecrpt

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

The following procedure is for the Oracle 9 native driver, but the procedure should be similar for Oracle 10.

To Create Net Service Name Configuration (Configuring Oracle 9 native driver):

1. Select *Oracle-OraHome92* > *Configuration and Migration Tools* > *Net Manager*.
2. In the navigation pane, expand Local and highlight Service Naming.
3. Click the plus sign on the left to add a Service Name.
4. In the *Service Name* window, provide a Net Service Name.
    - Provide ESECURITYDB

Click *Next*.

5. In the *Select Protocols* window, select the default:
   - TCP/IP (Internet Protocol)

   Click *Next*.
6. For Host Name and Port Number:
   - Provide the hostname or IP address of the machine the database resides on
   - Select the Oracle Port (default 1521 on install)

   Click *Next*.
7. To identify the database or service:
   - Select *(Oracle8i or later)*, provide your Service Name (This is your Oracle instance name).
   - For connection type, select *Database Default*.

   Click *Next*.
8. In the *Test* window, click *Test.* Click *Next*. Test might fail because the test uses a DB ID and password.
9. If test fails perform the following:
   - In the *Connection Test* window, click *Change Login*.
   - Provide the Sentinel Oracle ID (use esecrpt) and password. Click *Test*.

   If the test fails:
   - Ping the Sentinel Server
   - Verify that the host name of the Sentinel Server is in the hosts file on the Crystal Reports Server. The hosts file is located under %SystemRoot%\system32\drivers\etc\.
10. Click *Close* and then click *Finish*.

Configuration for all Authentications and Configurations

The following procedures are required for Crystal Server to work with the Sentinel Control Center.

Configuring inetmgr

To configure 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 *Internet Service Manager* by clicking *Start* > *Run*. Provide *inetmgr* and click *OK.*
3. *Expand (local computer)* > *Web Sites* > *Default Web Site* > *businessobjects*.
4. On *businessobjects, right-click* > *properties.*

5. Under *Virtual Directory* tab, click *Configuration*.
6. You should have the following mappings. If not, add them. If you are going to add a mapping, do not click *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`

***Table 9-1:** Mapping Table*

Click *OK* to close the window.

7. Restart IIS by expanding (local computer) > *Web Sites* > *Default Web Site*, high-light *Default Web Site* and right-click > *Stop.*
8. Expand (local computer) > *Web Sites* > *Default Web Site*, high-light *Default Web Site* and right-click > *Start.*

Patching Crystal Reports for use with Sentinel

In order to view Crystal Reports from the Sentinel Control Center's *Analysis* tab, several Crystal Enterprise files need to be updated to make them compatible with the browser. The following table lists those files and describes what each file is used for. These files can be found on the Sentinel 6 content Web pages at the following URL: http://support.novell.com/products/sentinel/sentinel6.html

File Name	Description
`calendar.js` `calendar.html`	Displays a popup calendar when you are selecting a date as a parameter to a report.
`grouptree.html`	Displays the Loading... message when the reports are loading.
`exportframe.html`	Displays the 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 Sentinel Control Center to establish a connection with Crystal Server and display the report list.
`GetReportURL.asp`	File used to support hyperlinks between reports.
`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.

File Name	Description
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.

Table 9-2: *Crystal Enterprise files*

To patch Crystal Reports:

1. Download the Sentinel report patches.

   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.

2. From within the Sentinel Reports Distribution, go to the "patch" directory and copy all `*.html` and `*.js` files to the viewer file location, default is:

   ```
   C:\Program Files\Business
   Objects\BusinessObjects Enterprise 11.5\Web
   Content\Enterprise115\viewer\en
   ```

3. From within the Sentinel Reports Distribution, go to the "patch" directory and copy all `*.asp` and `*.js` files to:

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

   NOTE: Your Web folder might be on a different drive or in a different location than specified above.

4. Create a Sentinel subdirectory in the Crystal installation directory. In a default installation, the path will be:

   ```
   C:\Program Files\BusinessObjects Enterprise
   11.5\Web
   Content\Enterprise115\WebTools\Sentinel
   ```

5. Place the `publish_report.aspx` and `delete_report.aspx` in the Sentinel directory.

   NOTE: 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 at http://support.novell.com/products/sentinel/sentinel6.html.

6. Open the `web.config` file in the Crystal install directory for editing.

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.

Publishing Crystal Report 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.

These report templates are created by Novell for use in the Sentinel Control Center *Analysis* tab and *Advisor* tab. The latest set of reports can be downloaded from the Sentinel 6 content Web pages at the following URL:

http://support.novell.com/products/sentinel/sentinel6.html

There are three methods of publishing reports.

- Crystal Publishing Wizard
- Crystal Reports Central Management Console
- Solution Manager (for reports included in a Solution Pack)

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 Reporting Data Tab section of Sentinel Data Manager in *Sentinel User Guide* and "Enabling Sentinel Top 10 Reports".

Publishing Report Templates - Crystal Publishing Wizard

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.

Publishing Crystal Report Templates

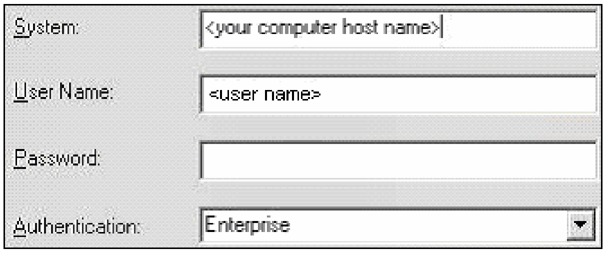
NOTE: If you want to publish your Reports Templates again, delete your previous import of Report Templates.

1. Click *Start>Programs > BusinessObjects > Crystal Reports Server > Publishing Wizard.*

   Click *Next*.

2. Login. System should be the hostname of the machine where Crystal is installed, and Authentication should be Enterprise. User Name can be Administrator. For security reasons, it is strongly encouraged to create a new user other than using 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

***Figure 9-38:** Publishing Wizard*

3. Click *Add Folder*; select *Include Subfolders*. From within the Sentinel Reports Distribution, navigate to:
   For Sentinel Database running on Microsoft SQL:

   ```
   Crystal_v115\SQL-Server
   ```

   For Sentinel Database running on Oracle:

   ```
   Crystal_v115\Oracle
   ```

   Click *OK*. Click *Next*.

4. In the *Specify Location* window, click *New Folder* (upper right corner) and create a folder called *SentinelReports*. Click *Next*.

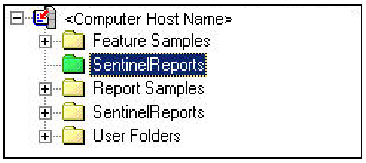
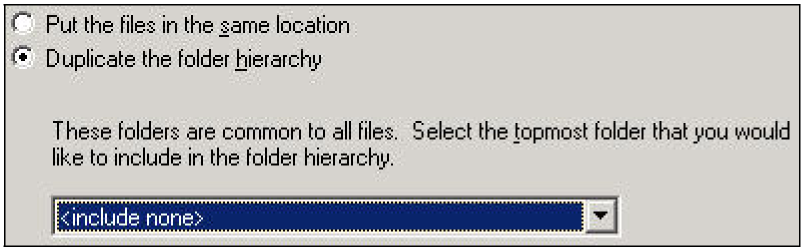


***Figure 9-39:** Specify Location window*

5. 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>

***Figure 9-40:** Duplicate the folder hierarchy selection*

Click *Next*.

6. In the *Confirm Location* window, click *Next*.
7. In the *Specify Categories* window, provide a category name of choice (such as sentinel)
   high-light the name and click the + button

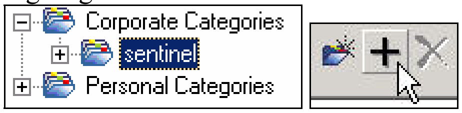


***Figure 9-41:** Specify Categories window*

NOTE: Only the first report displays under the category after clicking *Next*.

Click *Next*.

8. In the *Specify Repository Refresh* window, click *Enable All* to enable repository refresh. Click *Next*.
9. In the *Specify Keep Saved Data* window, click *Enable All* to keep saved data when publishing reports. Click *Next*.
10. In the *Change Defaults Values* window, click *Publish reports without modifying properties* (this should be default). Click *Next*.
11. Click *Next* to add your objects.
12. A published list displays, click *Finish*.

When the Sentinel templates for Crystal Reports are published to the Crystal Enterprise server, the templates must reside within the *SentinelReports* directory.

Publishing Report Templates – Central Management Console

To import Crystal Report Templates:

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

```
http://<hostname_or_IP_of_web_server>/business
objects/enterprise115/WebTools/adminlaunch
```

2. Click *Central Management Console*
3. Login to your *Crystal Server*.
4. Under the *Organize* pane, click *Folders*.
5. In the upper right-hand corner, click *New Folder*.
6. Create a folder *SentinelReports*. Click *OK*.

NOTE: You must exactly name the folder *SentinelReports*.

7. Click *SentinelReports*.
8. Click the *Subfolders* tab and 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 following folder with the Sentinel Reports Distribution:

    ```
    Crystal_v115\SQL-Server
    ```

    Pick a folder and select a report.
12. High light *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.

Publishing Report Templates from a Solution Pack

If the Web Server and Crystal Reports server are configured properly using the installation instructions, reports included in a Solution Pack can be published directly to the Crystal Reports Server using the Solution Manager.

To configure direct report publishing for Apache Tomcat:

1. The first step in this context is to create the following directory:

   ```
   /opt/crystal_xi/bobje/tomcat/webapps/esec-script/
   ```

2. Go to *reports_patch>Tomcat* in the *service pack top-level directory* and copy the files `publish_report.jsp` and `delete_report.jsp` to the `esec-script` directory.
3. Set the permissions and ownership for these two files to the following values:

   ```
   -rwxr-xr-x 1 crystal bobje
   ```

4. If Crystal was installed in a non-default location or was installed as a 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_xi"
   ```

5. If report publishing or deletion does not work immediately, you may need to restart the web server and Crystal Server.
   To configure direct report publishing for Microsoft IIS:

   I. Perform all other web configuration steps for Sentinel. For more information, see Crystal Reports for Windows in Sentinel Installation Guide. The steps in this section also incorporate the steps below.

   II. Create a Sentinel subdirectory in the Crystal installation directory, which is the following subdirectory of Business Objects by default:

`\BusinessObjects Enterprise 11.5\Web Content\Enterprise115\WebTools\`

III. Go to *reports_patch\IIS* in the *service pack top-level directory* and copy the files `publish_report.aspx` and `delete_report.aspx` to the *Sentinel subdirectory* in the *Crystal installation* directory.

IV. Open the `web.config file` in the *Crystal install directory* for editing.

V. Add two new entries to the `<assemblies>` section of the `web.config file` for `Enterprise.PluginManagerand Enterprise.Desktop.Report`. The following example shows a sample <assemblies> section:

```
      <assemblies>
<add
assembly="CrystalDecisions.CrystalReports.Engi
ne, 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.Framewor
k, Version=11.5.3300.0, Culture=neutral,
PublicKeyToken=123abcd1234a1234? />
<add
assembly="CrystalDecisions.Enterprise.InfoStor
e, 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.PluginMa
nager, 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.

NOTE: These steps are also described in the installation instructions for the Sentinel Core Solution Pack. For more current instructions see Solution Pack at Sentinel 6 content site.

Setting a Named User Account

The license key supplied with Crystal 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. Click *Start* > *Programs* > *BusinessObjects* > *Crystal Reports Server* > *.NET Administration Launchpad*.
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 Administrator as the User Name. Provide your password (by default, this will be blank). Click *Log On*. In the Organize pane, click *Users*.
5. Click *Guest*.
6. Change connection type from *Concurrent User* to *Named User*.

   IMPORTANT:

   You should use Named User License account so as to generate unlimited reports.
7. Click *Update*.
8. Logoff and close window or proceed to section *Configuring .NET Administration Launchpad*.

Configuring Reports Permissions

This procedure discusses how to use the *.NET Administration Launchpad* to configure the permissions on reports to allow you to view and modify reports on demand.

To Configure Reports Permissions:

1. If not already, start .NET Administration Launchpad (*Click Start* > *Programs* > *BusinessObjects* > *Crystal Reports Server* > *.NET Administration Launchpad*).

   NOTE: When launching *.NET Administration Launchpad*, if you find “HTTP 404 - File or Directory not found” error, see http://support.microsoft.com/kb/315122 for resolution.
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 Administrator as the User Name. Provide your password (by default, this will be blank). Click *Log On*. In the Organize pane, click *Folders*.
4. Single-click *SentinelReports*.

5. Select *All*.
6. Click the *Rights* tab.
7. For *Everyone*, in the drop-down menu to the right under Access Level select *View on Demand*.
8. Click *Update*.
9. Logoff and close the window.

Testing for Web Server Connection to the Database

To Test for Web Server connection to the database:

10. If not already, start *.net Administration Launchpad* (*Start* > *Programs* > *BusinessObjects* > *Crystal Reports Server* > *.NET Administration Launchpad*).
11. Click *Central Management Console*.
12. Provide Administrator as the User Name. Provide your password (by default, this will be blank). Click *Log On*.
13. Navigate to *Folders* > *SentinelReports* > *Internal Events*.
14. Select *Column Display Details*.
15. Click *Preview*.
16. Depending on your system, login as esecrpt or as the Sentinel Report User.
17. Under the *Sort* field drop-down menu, select *Tag*.
18. Click *OK*. A report displays.

Testing Connectivity to the Web Server

To Test the connectivity to the Web Server:

1. Go to another machine that is on the same network as your Web Server.
2. Specify

```
http://<DNS name or IP address of your web
server>/businessobjects/enterprise115/WebTools
/adminlaunch/default.aspx
```

You should get a Crystal BusinessObjects Web page.

Disabling Sentinel Top 10 Reports

By default Sentinel Top 10 Reports are enabled. To disable Sentinel Top 10 Reports, you must:

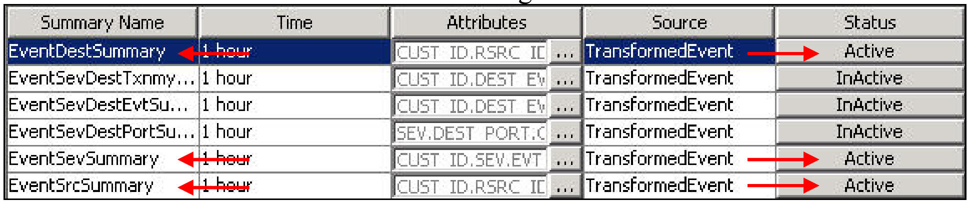
- Turn off Aggregation
- Disable EventFileRedirectService

To Turn off Aggregation (aggregation):

1. Start Sentinel Control Center.
2. Login.
3. Click the *Admin* tab and open the *Reporting Data* option.
4. Disable the following summaries
   - EventDestSummary
   - EventSevSummary

- EventSrcSummary

Click *Active* in the Status column until it changes to *InActive*.



Summary Name	Time	Attributes	Source	Status
EventDestSummary	1 hour	CUST ID.RSRC ID ...	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 ID ...	TransformedEvent	Active

Figure 9-42: *Changing Active state to InActive state*

To Disable EventFileRedirectService (EventFileRedirectService):

1. At your DAS machine, using text editor, open:

   For UNIX:

   ```
   $ESEC_HOME/config/das_binary.xml
   ```

   For Windows:

   ```
   %ESEC_HOME%\config\das_binary.xml
   ```

2. For EventFileRedirectService, change the status to off.

   ```
   <property name="status">off</property>
   ```

3. Restart the DAS component by doing the following:

   On Windows:

   ```
   Use Service Manager to stop and then start the
   “sentinel” service
   ```

Increasing Crystal Enterprise Server Report Refresh Record Limit

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 will need to reconfigure the Crystal Reports Page Server. This can be done by using either the Central Configuration Manager or the Crystal Web Page.

To Reconfigure the Crystal Reports Page Server through the Central Configuration Manager:

1. Click *Start* > *Programs* > *BusinessObjects* > *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 Reports Page Server.

To Reconfigure the Crystal Reports Page Server through the Crystal Web Page:

1. Click *Start > Programs > BusinessObjects > Crystal Reports Server > .Net Administration Launchpad.*
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.

Configuring Sentinel Control Center to Integrate with Crystal Enterprise Server

The Sentinel Control Center can be configured to integrate with the Crystal Enterprise Server, allowing you to view Crystal Reports from within Sentinel Control Center.

To enable Sentinel Control Center integration with Crystal Enterprise Server, follow the instructions below.

NOTE: This configuration must be performed only after the Crystal Enterprise Server has been installed and Crystal Reports have been published to it.

To Configure Sentinel to integrate with Crystal Enterprise Server:

1. Log into Sentinel Control Center as a user that has privileges to the *Admin* tab.
2. On the *Admin* tab, select *Reporting Configuration*.
3. In the *Analysis URL* field, provide the following:

```
http://<hostname_or_IP_of_web_server>/GetRepor
ts.asp?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 Enterprise Server.

NOTE: The URL above will not work properly if the APS is set to the IP Address. It must be the host name of the Crystal Server.

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>/GetRepor
ts.asp?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 Enterprise Server.

NOTE: The URL above will not work properly if the APS is set to the IP Address. It must be the host name of the Crystal Server.

6. Click *Refresh* next to the *Advisor URL* field.
7. Click *Save*.
8. Logout and log back in to the Sentinel Control Center. The Crystal Report trees in the *Analysis* tab and *Advisor* (if Advisor is installed) tab should now display in the *Navigator* window.

10 Crystal Reports for Linux

Crystal Business Objects Enterprise™ XI is the reporting tool used with Sentinel. This section discusses the installation and configuration of Crystal Reports Server for Sentinel. For more information on supported platforms for Crystal Reports Server in a Sentinel environment, see Supported Platforms and Best Practices section.

For more information on Crystal Reports Server XI Release 2 Service Packs, see http://support.businessobjects.com/downloads/service_packs/crystal_reports_server.asp

This section discusses running Crystal Reports Server on Linux. For more information on running Crystal Reports Server on Windows, see “Crystal Reports for Windows” section.

IMPORTANT:

The installation should be done in the order presented below.

- Pre-install and install of Crystal BusinessObjects Enterprise™ XI
- Patch Crystal reports
- Publishing (importing) Crystal reports
- Setting a “Named User” account
- Testing connectivity to the Web Server
- Enabling Top 10 reports (optional)
- Increasing Crystal Enterprise Server Report Refresh Record Limit (recommended)
- Configuring Sentinel Control Center to Integrate with Crystal Enterprise Server

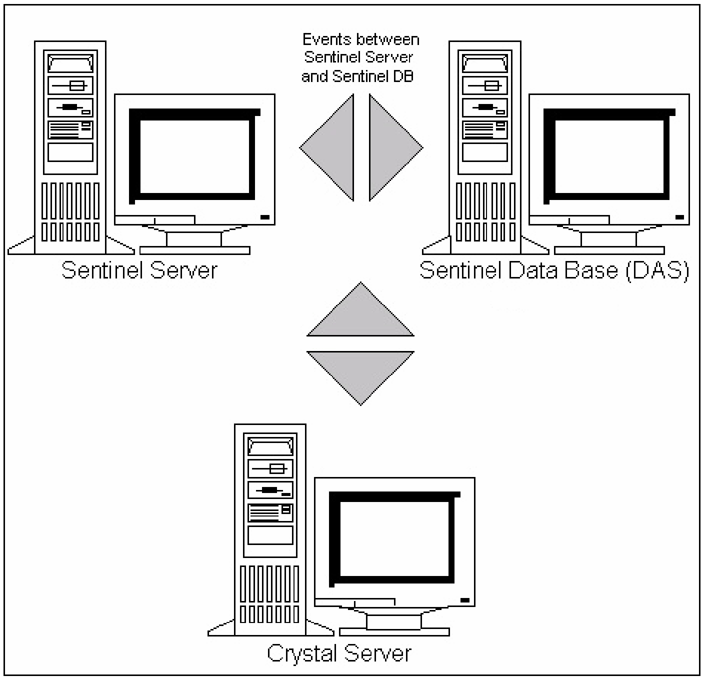


Figure 10-1: *Events between Sentinel Server, Crystal Server and Sentinel DB (DAS)*

Installation

Pre-Install of Crystal BusinessObjects Enterprise™ XI

To Pre-Install Crystal BusinessObjects Enterprise:

1. If the Sentinel Database is not on the same machine as the Crystal Server, then you must install the Oracle Client software on the Crystal Server machine. This additional step is not needed if the Sentinel Database is on the same machine as the Crystal Server because in this case the required Oracle software is already installed with the Oracle database software required by the Sentinel Database.
2. Login to the Crystal 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. Change to the crystal user:

   ```
   su - crystal
   ```

8. 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/9.2, 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/9.2
   ```

9. 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
   ```

10. 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 Server machine:

    a. Log in as the oracle user.
    b. Change directories to $ORACLE_HOME/network/admin
    c. Make a backup of the file `tnsnames.ora`.
    d. Open the file `tnsnames.ora` for editing.
    e. If the Sentinel Database is on the Crystal 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)
      )
    )
    ```

    f. If the Sentinel Database is not on the Crystal Server machine, open the `tnsnames.ora` file on the Sentinel Database machine to find the entry described above.
    g. Make a copy of that entire entry and paste it at the bottom of the `tnsnames.ora` file on the Crystal 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)
  )
)
```

h. Make sure the HOST part of the entry is correct (for example, make sure it is not set to localhost if the Crystal Server and Sentinel Database are on different machines).
i. Save the changes to the `tnsnames.ora` file.
j. Execute the following command to check that the `esecuritydb` Service Name is configured properly:

```
tnsping esecuritydb
```

k. After the command is executed, you will get a message saying the connection is OK.

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 BusinessObjects Enterprise:

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 into an existing database.
12. Specify configuration information for MySQL:
    a. Use default port 3306
    b. Admin password
13. Specify more configuration information for MySQL:

a. Default DB Name: BOE115
b. User id: mysqladm
c. Password

14. Specify more configuration information for MySQL:

    a. Local Name Server: <local machine's hostname>
    b. Default CMS Port Number: 6400

15. Select: *Install Tomcat*
16. Specify Tomcat configuration information:

    a. Default Receive HTTP requests port: 8080
    b. Default Redirect jsp requests port: 8443
    c. 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

Patching Crystal Reports for Use with Sentinel

In order to view Crystal Reports from the Sentinel Control Center's *Analysis* tab, several Crystal Enterprise files need to be updated to make them compatible with the browser.

The following table lists those files and describes what each file is used for. These files can be found on the Sentinel 6 content Web pages at the following URL:

http://support.novell.com/products/sentinel/sentinel6.html.

File Name	Description
`calendar.js`	Displays a popup calendar when you are selecting a date as a parameter to a report.
`calendar.html`	
`grouptree.html`	Displays the Loading... message when reports are loading.
`exportframe.html`	Displays the 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.
`GetReports.jsp`	File used by Sentinel Control Center to establish a connection with Crystal Server and display the report list.
`GetReportURL.jsp`	File used to support hyperlinks between reports.
`publish_report.jsp`	Used to publish reports directly from a Solution Pack to the Crystal server when a control is installed. This file is also available in the SP2 patch distribution.
`delete_report.jsp`	Used to remove reports directly from the Crystal server when a control is uninstalled. This file is also available in the SP2 patch distribution.

Table 10-1: *Crystal Enterprise files*

To patch Crystal Reports Server:

1. Download the Sentinel report patches. .

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.

2. Create the directory structure *esec-script/WEB-INF/lib* in the following location:

   ```
   /opt/crystal_xir2/bobje/tomcat/webapps/
   ```

3. From within the Sentinel Reports Distribution, go to the patch directory and copy all `*.html` and `*.js` files to the viewer file location, default is:

   ```
   /opt/crystal_xir2/bobje/webcontent/enterprise115/viewe
   r/en/
   ```

4. From within the Sentinel Reports Distribution, go to the patch directory and copy all `*.jsp` files to:

   ```
   /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 at http://support.novell.com/products/sentinel/sentinel6.html.

5. Set the permissions and ownership for the `publish_report.jsp` and `delete_report.jsp` files to the following values:

   ```
   -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 was installed as a 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 *Crystal Server*.

Publishing Crystal Report 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.

These report templates are created by Novell for use in the Sentinel Control Center *Analysis* and *Advisor* tab. The latest set of reports can be downloaded from the Sentinel 6 content Web pages at the following URL:

http://support.novell.com/products/sentinel/sentinel6.html

There are two methods of publishing reports.

- Crystal Publishing Wizard
- Crystal Reports Central Management Console
- Solution Manager (for reports included in a Solution Pack)

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 Reporting Data Tab section of Sentinel Data Manager in *Sentinel User Guide*.

Publishing Report Templates – Crystal Publishing Wizard

NOTE: A Windows platform is required to run *Crystal Publishing Wizard*.

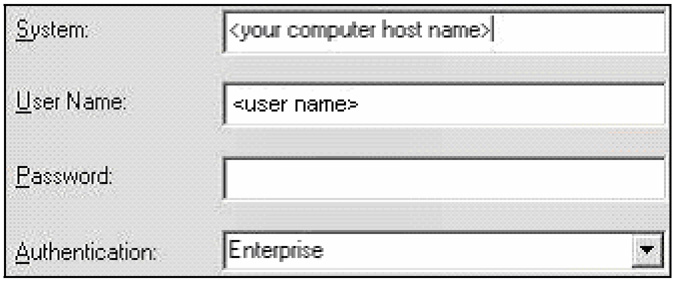
To import Crystal Report templates:

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

Figure 10-2: *Login Credentials*

   Click *Add Folder*.

3. Click *Include Subfolder*. From within the Sentinel Reports Distribution, navigate to: `Crystal_v115\Oracle`

   Click *OK*. Click *Next*.

4. In the, click *New Folder* (upper right corner) and create a folder called *SentinelReports*. Click *Next*.

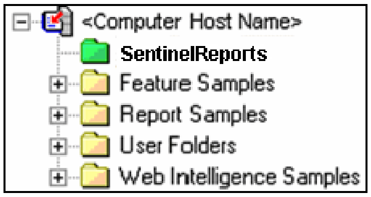
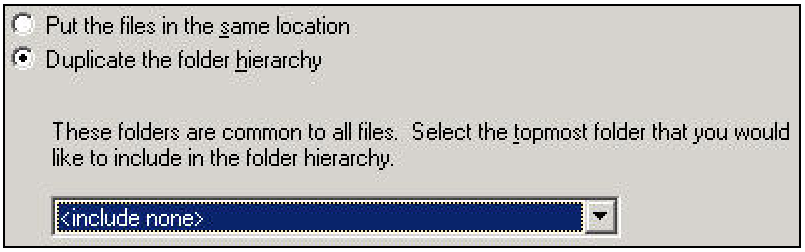


Figure 10-3: *Specify Location window*

5. Select:
   - *Duplicate the folder hierarchy*.
   - Click the down arrow and select <*include none*>



○ Put the files in the same location

● Duplicate the folder hierarchy

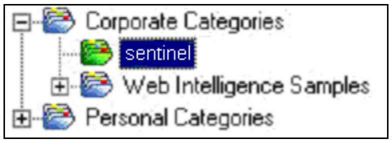
These folders are common to all files. Select the topmost folder that you would like to include in the folder hierarchy.

<include none>

Figure 10-4: *Duplicating the folder hierarchy*

Click *Next*.

6. In the *Confirm Location* window, click *Next*.
7. In the *Specify Categories* window:
   - a category name of choice (such as sentinel)



Corporate Categories
- sentinel
- Web Intelligence Samples

Personal Categories

Figure 10-5: *Specify Categories window*

   - high-light the name and click the + button

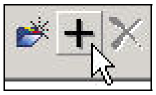


Figure 10-6: *Adding reports*

NOTE: Only the first report displays under the category after clicking *Next*.

   - Click *Next*.

8. In the *Specify Schedule* window, click *Let users update the object* (this should be default). Click *Next*.
9. In the *Specify Repository Refresh* window, click *Enable All* to enable repository refresh. Click *Next*.
10. In the *Specify Keep Saved Data* window, click *Enable All* to keep saved data when publishing reports. Click *Next*.
11. In the *Change Defaults Values* window, click *Publish reports without modifying properties* (this should be default). Click *Next*.
12. Click *Next* to add your objects.
13. Click *Next*. Click *Finish*.

When the Sentinel templates for Crystal Reports are published to the Crystal Enterprise server, the templates must reside within the *SentinelReports* directory.

Publishing Report Templates – Central Management Console

To import Crystal Report Templates:

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

```
http://<hostname_or_IP_of_web_server>:<web_server_port
_default_8080>/businessobjects/enterprise115/adminlaun
ch
```

2. Click *Central Management Console*
3. Login to your *Crystal Server*.
4. Under the *Organize* pane, click *Folders*.
5. In the upper right-hand corner, click *New Folder*.
6. Create a folder *SentinelReports*. Click *OK*.

   NOTE: You must exactly name the folder *SentinelReports*.

7. Click *SentinelReports*.
8. Click the *Subfolders* tab and 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 following folder with the Sentinel Reports Distribution:

    ```
    Crystal_v115\Oracle
    ```

    Pick a folder and select a report.
12. High light *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.

Publishing Report Templates from a Solution Pack

If the Web Server and Crystal Reports server are configured properly using the installation instructions, reports included in a Solution Pack can be published directly to the Crystal Reports Server using the Solution Manager.

To configure direct report publishing for Apache Tomcat:

16. The first step in this context is to create the following directory:

    ```
    /opt/crystal_xi/bobje/tomcat/webapps/esec-script/
    ```

17. Go to *reports_patch>Tomcat* in the *service pack top-level directory* and copy the files `publish_report.jsp` and `delete_report.jsp` to the `esec-script` directory.
18. Set the permissions and ownership for these two files to the following values:

    ```
    -rwxr-xr-x 1 crystal bobje
    ```

19. If Crystal was installed in a non-default location or was installed as a 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_xi"
    ```

20. If report publishing or deletion does not work immediately, you may need to restart the web server and Crystal Server.
    To configure direct report publishing for Microsoft IIS:

    I. Perform all other web configuration steps for Sentinel. For more information, see Crystal Reports for Windows in Sentinel Installation Guide. The steps in this section also incorporate the steps below.

    II. Create a Sentinel subdirectory in the Crystal installation directory, which is the following subdirectory of Business Objects by default: `\BusinessObjects Enterprise 11.5\Web Content\Enterprise115\WebTools\`

    III. Go to *reports_patch\IIS* in the *service pack top-level directory* and copy the files `publish_report.aspx` and `delete_report.aspx` to the *Sentinel subdirectory* in the *Crystal installation* directory.

    IV. Open the `web.config file` in the *Crystal install directory* for editing.

    V. Add two new entries to the `<assemblies>` section of the `web.config file` for En`terprise.PluginManagerand 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.

NOTE: These steps are also described in the installation instructions for the Sentinel Core Solution Pack. For more current instructions see Solution Pack at Sentinel 6 content site.

Using the Crystal XI R2 Web Server

Crystal 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>:<web_server_port
_default_8080>/businessobjects/enterprise115/adminlaun
ch
```

The non-administrative (general use) portal is accessed through your browser at the following URL:

```
http://<hostname_or_IP_of_web_server>:<web_server_port
_default_8080>/businessobjects/enterprise115
```

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>:<web_server_port
   _default_8080>/businessobjects/enterprise115/adminlaun
   ch
   ```

3. You should get a Crystal BusinessObjects Web page.

Setting a “Named User” Account

The license key supplied with Crystal 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>:<web_server_port
_default_8080>/businessobjects/enterprise115/adminlaun
ch
```

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.

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>:<web_server_port
   _default_8080>/businessobjects/enterprise115/adminlaun
   ch
   ```

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.

Increasing Crystal Enterprise 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>:<web_server_port
   _default_8080>/businessobjects/enterprise115/adminlaun
   ch
   ```

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.

Configuring Sentinel Control Center to Integrate with Crystal Enterprise Server

The Sentinel Control Center can be configured to integrate with the Crystal Enterprise Server, allowing you to view Crystal Reports from within Sentinel Control Center.

To enable Sentinel Control Center integration with Crystal Enterprise Server, follow the instructions below.

NOTE: This configuration must be performed only after the Crystal Enterprise 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, see "Supported Platforms and Best Practices" section.

To Configure Sentinel to Integrate with Crystal Enterprise Server:

1. Log into Sentinel Control Center as a user that has privileges to the Admin tab.
2. On the Admin tab, select *Reporting 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&passwo
rd=&tab=Analysis
```

NOTE: <hostname_or_IP_of_web_server> must be replaced with the IP address or hostname of the Crystal Enterprise 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&passwo
rd=&tab=Advisor
```

NOTE: `<hostname_or_IP_of_web_server>` must be replaced with the IP address or hostname of the Crystal Enterprise 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 Report trees in the *Analysis* and *Advisor* (if Advisor is installed) tabs should now display in the *Navigator* window.

Utilities and Troubleshooting

Starting MySQL

To make sure MySQL is running:

1. Login as crystal user.
2. cd /opt/crystal_xir2/bobje
3. `./mysqlstartup.sh`

Starting Tomcat

To make sure Tomcat is running:

1. Login as crystal user
2. cd /opt/crystal_xir2/bobje
3. `./tomcatstartup.sh`

Starting Crystal Servers

To make sure crystal servers are running:

1. Login as crystal user
2. cd /opt/crystal_xir2/bobje
3. `./startservers`

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
   ```

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:

a. Login as crystal user
b. cd /opt/crystal_xir2/bobje
c. `./cmsdbsetup.sh`
d. Press *Enter* when `[<hostname>.cms]` displays.
e. Select *select* and provide all your MySQL DB info that was entered during install time. For more information, see install instructions in, "Installing Sentinel 6" section.
f. When done, quit `cmsdbsetup.sh`
g. `./stopservers`
h. `./startservers`

- Re-initialize MySQL DB:

a. Login as crystal user
b. cd /opt/crystal_xir2/bobje
c. `./cmsdbsetup.sh`
d. Press *Enter* when `[<hostname>.cms]` displays.
e. Select *reinitialize* and follow instructions.
f. When done, quit `cmsdbsetup.sh`
g. `./stopservers`
h. `./startservers`

2. Make sure all CCM servers are enabled:

a. Login as crystal user
b. cd /opt/crystal_xir2/bobje
c. `./ccm.sh` -enable all

11 Uninstalling Sentinel

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. In addition, 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 that could interfere with a new 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.

Uninstalling Sentinel

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* and log out,

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 Install Shield 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.*

Post-Uninstall

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".
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".
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.

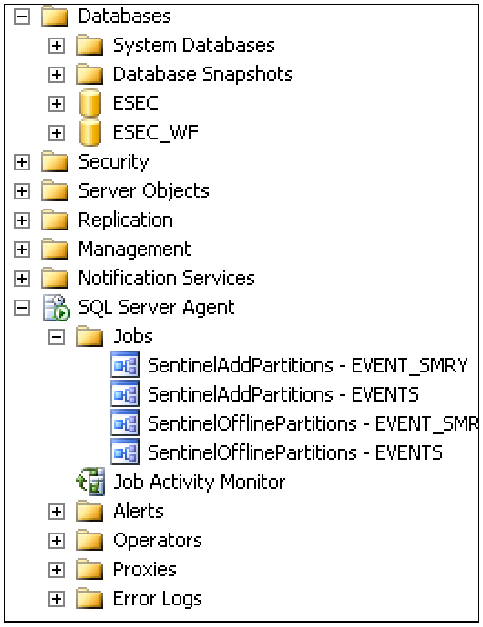
   WARNING:

   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.



```
⊟ Databases
    ⊞ System Databases
    ⊞ Database Snapshots
    ⊞ ESEC
    ⊞ ESEC_WF
⊞ Security
⊞ Server Objects
⊞ Replication
⊞ Management
⊞ Notification Services
⊟ SQL Server Agent
    ⊟ Jobs
          SentinelAddPartitions - EVENT_SMRY
          SentinelAddPartitions - EVENTS
          SentinelOfflinePartitions - EVENT_SMR
          SentinelOfflinePartitions - EVENTS
      Job Activity Monitor
    ⊞ Alerts
    ⊞ Operators
    ⊞ Proxies
    ⊞ Error Logs
```

Figure 11-1: *Connecting to the SQL Server Instance*

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.

A Pre-installation Questionnaire

Pre-Install Questions

1. What is your goal or purpose of using Novell Sentinel?

   a. Compliance

   b. SEM

   c. 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.

   a. ____

   b. ____

   c. ____

   d. ____

   e. ____

   f. ____

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.

B Installation Record for Sentinel on Linux with Oracle

This checklist works for distributed installations with up to three Collector Manager and Correlation Engine instances.

For more information on Hardware and OS requirements, see "Supported Platforms and Best Practices" section and for more information on installation procedure, see "Installing Sentinel 6" section

	Configuration Variable			
1.	*Sentinel Version:*		*Today's Date:*	
2.	*UNIX Kernel Values for Oracle.*	*In SLES and RHEL, you can set parameters in "etc/sysctl.conf".*		
	▪ shmmax		□: Yes | □: No	Value if higher:
	▪ shmmin		□: Yes | □: No	Value if higher:
	▪ shmseg		□: Yes | □: No	Value if higher:
	▪ shmmni		□: Yes | □: No	Value if higher:
	▪ semmns		□: Yes | □: No	Value if higher:
	▪ semmni		□: Yes | □: No	Value if higher:
	▪ semmsl		□: Yes | □: No	Value if higher:
	▪ shmopm		□: Yes | □: No	Value if higher:
	▪ shmvmx		□: Yes | □: No	Value if higher:
3.	*Database System*			
	▪ Correct OS for Sentinel Components	□: Yes | □: No	▪ Proper Patch	□: Yes | □: No
	▪ Correct OS for DB	□: Yes | □: No	▪ Proper Patch	□: Yes | □: No
	▫ Version		▫ Patch Level	
	▪ Correct Oracle DB w/ Partitioning	□: Yes | □: No	▪ Proper Patch	□: Yes | □: No
	▫ Version		▫ Patch level	
	▪ Correct environment variables set for Oracle OS user.	□: Yes | □: No		
	▪ `Init.ora` file configured	□: Yes | □: No		
4.	*DAS Machine*			

	Configuration Variable			
	▪ Correct OS for Sentinel Components	□: Yes | □: No	▪ Proper Patch	□: Yes | □: No
	▪ serial number			
	▪ license key			
5.	*DAS Install*			
	▪ DB hostname or IP			
	▪ Database name			Default: ESEC
	▪ Database port			Default: 1521
	▪ JDBC file location			
6.	*Database Instance (SID)*			
7.	*Database Name*			
8.	*Sentinel Components:*			
	▪ Sentinel Database (IP or DNS)			OS: Patch:
	▫ DB install log			
	▫ Oracle Memory(RAM)			
	▫ Instance Name			
	▫ Listener Port		Default: 1521	
	▫ SYS password			
	▫ SYSTEM password			
	▪ .keystore file imported when installing:			
	▫ Correlation	□: Yes | □: No		
	▫ DAS	□: Yes | □: No		
	▫ Collector Manager	□: Yes | □: No		
	▫ Communication Server	□: Yes | □: No		
	▫ Communication Server (iSCALE) (IP or DNS)	▫ IP/DNS:		OS: Patch:
	▫ DAS/Advisor (IP or DNS) (Advisor is optional)			OS: Patch:
	▫ DAS RAM			
	▪ Correlation Engine (IP and OS)			
		▫ IP:		OS:
		▫ IP:		OS:
		▫ IP:		OS:
	▪ Collector Builder (IP or DNS) (recommend one install)			
	▪ Collector Manager	Provide the details of each Collector Manager you deploy.		
	Collector Manager	□: Yes | □: No	□ Proxy | □ Direct Message Bus	
	▫ IP: ▫ OS:	▫ Message Bus Port: ▫ Sentinel Control Center Proxy Port: ▫ Communication Server Host Name: ▫ Collector Manager Certificate authentication Port:		

	Configuration Variable		
9.	*Advisor (optional)*		
	▪ Installed on same machines as DAS?	□: Yes | □: No	
	▪ Advisor download:	□: Standalone	□: Direct Internet Download
	▪ Data feed file location		
	▪ Advisor from address		
	▪ Advisor to address		
	▪ Username	u/n:	
10.	*Database file locations:*		
	▪ Data files		
	▪ Index files		
	▪ Summary data files		
	▪ Summary index files		
	▪ Temporary and Undo Tablespace files		
	▪ Redo Log Member A directory		
	▪ Redo Log Member A directory		
11.	*Database size:*		
	▪ Standard (20GB)		
	▪ Large (400GB)		
	▪ Custom (size)		
12.	*SMTP Server (DNS or IP)*		
13.	*User passwords*		
	▪ esecadm	PW:	
	▫ Home directory		Default: /export/home
	▪ esecapp	PW:	
	▪ esecdba	PW:	
	▪ esecrpt	PW:	
	Crystal Installation		
1.	*Crystal Version:*		
	▪ OS		
	▪ Crystal DB		
	▪ Crystal Server (IP or DNS)		
	▪ Web Server (IP or DNS)		
2.	*Crystal Reports*		
	▪ All reports published	□: Yes | □: No	
	▪ Configured reports on Sentinel Control Center	□: Yes | □: No	

C Installation Record for Sentinel on Solaris with Oracle

This checklist works for distributed installations with up to three Collector Manager and Correlation Engine instances.

For more information on Hardware and OS requirements, see "Supported Platforms and Best Practices" section and for more information on installation procedure, see "Installing Sentinel 6" section.

	Configuration Variable			
1.	*Sentinel Version:*			*Today's Date:*
2.	*UNIX Kernel Values for Oracle.*	*In SLES and RHEL, you can set parameters in "etc/sysctl.conf".*		
	shmmax		□: Yes | □: No	Value if higher:
	shmmin		□: Yes | □: No	Value if higher:
	shmseg		□: Yes | □: No	Value if higher:
	shmmni		□: Yes | □: No	Value if higher:
	semmns		□: Yes | □: No	Value if higher:
	semmni		□: Yes | □: No	Value if higher:
	semmsl		□: Yes | □: No	Value if higher:
	shmopm		□: Yes | □: No	Value if higher:
	shmvmx		□: Yes | □: No	Value if higher:
3.	*Database System*			
	Correct OS for Sentinel Components	□: Yes | □: No	Proper Patch	□: Yes | □: No
	▪ Correct OS for DB	□: Yes | □: No	▪ Proper Patch	□: Yes | □: No
	▪ Correct Oracle DB w/ Partitioning	□: Yes | □: No	▪ Proper Patch	□: Yes | □: No
	▫ Version		▫ Patch level	
	▪ Copy of Oracle Note: 148673.1	□: Yes | □: No		
	▪ Correct environment variables set for Oracle OS user.	□: Yes | □: No		
	▪ Init.ora file configured	□: Yes | □: No		

	Configuration Variable			
	▪ Correct OS for Sentinel Components	□: Yes | □: No	▪ Proper Patch	□: Yes | □: No
4.	*DAS Machine*			
	▪ serial number			
	▪ license key			
5.	*DAS Install*			
	▪ DB hostname or IP			
	▪ Database name			Default: ESEC
	▪ Database port			Default: 1521
	▪ JDBC file location			
6.	*Database Instance (SID)*			
7.	*Database Name*			
8.	*Sentinel Components:*			
	▪ Sentinel Database (IP or DNS)			OS: Patch:
	▫ DB install log			
	▫ Oracle Memory(RAM)			
	▫ Instance Name			
	▫ Listener Port		Default: 1521	
	▫ SYS password			
	▫ SYSTEM password			
	▪ .keystore file imported when installing:			
	▫ Correlation	□: Yes | □: No		
	▫ DAS	□: Yes | □: No		
	▫ Collector Manager	□: Yes | □: No		
	Collector Manager			
	Install Collector Manager:	□: Yes | □: No	□ Proxy | □ Direct Message Bus	
	▫ IP: ▫ OS:	▫ Message Bus Port: ▫ Sentinel Control Center Proxy Port: ▫ Communication Server Host Name: ▫ Collector Manager Certificate authentication Port:		
	▫ Communication Server	□: Yes | □: No		
	▫ Communication Server (iSCALE) (IP or DNS)	IP/DNS:		OS: Patch:
	▪ DAS/Advisor (IP or DNS) (Advisor is optional)			OS: Patch:
	▫ DAS RAM			

	Configuration Variable			
	▪ Correlation Engine (IP and OS)			
		IP:		OS:
		IP:		OS:
		IP:		OS:
	▪ Crystal Server (IP or DNS)			
	▫ MySQL for Crystal Server	MySQL Version: MySQL Patch: sa password or holder of password:		
	▫ IP:	u/n:	PW:	OS:
	▪ Collector Builder (IP or DNS) (recommend one install)			
	▪ Collector Manager			
	▪ Installing Collector Manager using:	□: Yes | □: No	□: Proxy |	□: Direct Message Bus
	▫ IP:	PW:		OS:
	▫ IP:	PW:		OS:
	▫ IP:	PW:		OS:
9.	*Advisor (optional)*			
	Installed on same machines as DAS?	□: Yes | □: No		
	▪ Advisor download:	□: Standalone	□: Direct Internet Download	
	▪ Data feed file location			
	▪ Advisor from address			
	▪ Advisor to address			
	▪ Username and password	u/n:		
10.	*Database file locations:*			
	▪ Data files			
	▪ Index files			
	▪ Summary data files			
	▪ Summary index files			
	▪ Temporary and Undo Tablespace files			
	▪ Redo Log Member A directory			
	▪ Redo Log Member A directory			
11.	*Database size:*			
	▪ Standard (20GB)			
	▪ Large (400GB)			
	▪ Custom (size)			
12.	*SMTP Server (DNS or IP)*			
13.	*User passwords*			
	▪ esecadm	PW:		

	Configuration Variable		
	▫ Home directory		Default: /export/home
	▪ esecapp	PW:	
	▪ esecdba	PW:	
	▪ esecrpt	PW:	
	Crystal Installation		
1.	Crystal Version:		
	▪ OS		
	▪ Crystal DB		
	▪ Crystal Server (IP or DNS)		
	▪ Web Server (IP or DNS)		
2.	*Crystal Reports*		
	▪ All reports published	□: Yes | □: No	
	▪ Configured reports on Sentinel Control Center	□: Yes | □: No	

D Installation Record for Sentinel on Windows with Microsoft SQL Server

This checklist works for distributed installations with up to three Collector Manager and Correlation Engine instances.

For more information on Hardware and OS requirements, see "Supported Platforms and Best Practices" section and for more information on installation procedure, see "Installing Sentinel 6" section.

	Configuration Variable				
1.	*Sentinel Version:*				*Today's Date:*
	Database System				
	▪ Correct OS for Sentinel Components	□: Yes | □: No	▪	Proper Patch	□: Yes | □: No
	▪ Correct OS for DB	□: Yes | □: No	▪	Proper Patch	□: Yes | □: No
	▪ Correct SQL DB	□: Yes | □: No	▪	Proper Patch	□: Yes | □: No
	▫ Version		▫	Patch level	
2.	*For DAS installation under Windows Domain account, assign 'Log on as service'*	□: Yes | □: No			
3.	*DAS Machine*				
	▪ serial number				
	▪ license key				
4.	*Database Host name or IP:*	*<hostname>[\<Instance Name>]*			
5.	*Database Name:*				Default: ESEC
6.	*Port:*				Default: 1433
7.	*Authentication Mode*	□: mixed □: non-mixed			
8.	*SQL server sa password or holder of password.*	PW:			
9.	*Sentinel Components:*				
	▪ Sentinel Database (IP or DNS)				OS: Patch:
	▪ `.keystore` file imported when installing:				
	▫ Correlation	□: Yes | □: No			
	▫ DAS	□: Yes | □: No			

	Configuration Variable		
	▫ Collector Manager Service	□: Yes | □: No	
	▫ Communication Server	□: Yes | □: No	
	▫ Communication Server (iSCALE) (IP or DNS)		OS: Patch:
	▪ DAS/Advisor (IP or DNS) (Advisor is optional)		OS: Patch:
	▪ Correlation Engine (IP and OS)		
		IP:	OS:
		IP:	OS:
		IP:	OS:
	▪ Crystal Server (IP or DNS)		OS: Patch:
	▫ Microsoft SQL Server for Crystal Server	Microsoft SQL Version: Microsoft SQL Patch: sa password or holder of password:	
	▪ Collector Builder (IP or DNS) (recommend one install)		
	▪ Collector Manager (passwords w/ IP or DNS and OS)		
	▪ Collector Manager	□: Yes | □: No □ Proxy | □ Direct Message Bus	
	▫ IP: ▫ OS:	▫ Message Bus Port: ▫ Sentinel Control Center Proxy Port: ▫ Communication Server Host Name: ▫ Collector Manager Certificate authentication Port:	
10.	*Advisor (optional)*		
	Installed on same machines as DAS?	□: Yes | □: No	
	▪ Advisor download:	□: Standalone | □: Direct Internet Download	
	▪ Data feed file location		
	▪ Advisor from address		
	▪ Advisor to address		
	▪ Username and password	u/n:	
11.	*Database file locations:*		
	▪ Data files		
	▪ Index files		
	▪ Summary data files		
	▪ Summary index files		
	▪ Log files		
12.	*Database size:*		
	▪ Standard (20GB)		
	▪ Large (400GB)		

	Configuration Variable			
	▪ Custom (size)			
13.	*SMTP Server (DNS or IP)*			
14.	*For SQL Authentication (passwords)*			
	▪ Esecadm	PW:		
	▪ Esecapp	PW:		
	▪ Esecdba	PW:		
	▪ Esecrpt	PW:		
15.	*For Windows Authentication (passwords)*			
	▪ DBA (login)	u/n:		
	▪ Application user (login and password)	u/n:		PW:
	▪ Sentinel Administrator (login)	u/n:		
	▪ Sentinel Reporting user (login)	u/n:		
	Crystal Installation			
1.	*Crystal Version:*			
	▪ OS			
	▪ DB			
	▪ Crystal Server (IP or DNS)			
	▫ Microsoft SQL (Optional, but recommended)	Microsoft SQL Version: Microsoft SQL Patch: sa password or holder or password:		
	▫ IP:	u/n:	PW:	OS:
2.	*Crystal Reports*			
	▪ Type of Report	□: SQL	□: Oracle	
	▪ All reports published	□: Yes | □: No		
	▪ Configured reports on Sentinel Control Center	□: Yes | □: No		

E Oracle Setup

Installing Oracle

DISCLAIMER: The instructions provided in this document are not intended to replace Oracle's documentation. This is only an example of one setup scenario. This documentation assumes that the Oracle users' home directory is **/home/oracle** and that Oracle will be installed into **/opt/oracle**. Your exact configuration might vary. Consult your operating system and Oracle documentation for more information.

Oracle 9i Installation on SLES 9

To install Oracle on SUSE Linux Enterprise Server 9:

1. Follow Installation instructions provided in SLES 9 install manual. Install SLES 9 with the ext3 filesystem and default packages along with *C/C++ Compiler and Tools* and SP2.

   NOTE: If you have already installed SUSE Linux, you can use YaST (Yet Another Setup Tool) in the SUSE Linux GUI to install *C/C++ Compiler and Tools*.

2. Login as root.
3. Install gcc_old using YaST.
4. Verify you are running SP3 by typing:

   ```
   SPident
   ```

   or

   ```
   cat /etc/SuSE-release
   ```

   You should get:

   ```
   CONCLUSION: System is up-to-date!
         Found     SLES-9-i386-SP3
   ```

   or

   ```
   SUSE LINUX Enterprise Server (i586)
   VERSION = 9
   PATCHLEVEL = 3
   ```

5. To automate most of the Oracle pre-install tasks and to create the oracle user, install `orarun.rpm` included with SLES 9.

   NOTE: See Oracle installation document for complete list of prerequisites.

   ```
   rpm -i <path>/orarun-1.8-109.15.i586.rpm
   ```

NOTE: `orarun` is also available from the [Novell Web site (http://www.novell.com).](http://www.novell.com)

6. The account for the oracle user is disabled. Enable it, by changing the shell for the oracle user from /bin/false to /bin/bash using YaST user administration or by editing the /etc/passwd.
7. Set a new password for the oracle user by using YaST or typing:

   ```
   /usr/bin/passwd oracle
   ```

8. To set the kernel parameters, run

   ```
   /usr/sbin/rcoracle start
   ```

   Ignore any errors.

   ```
   /sbin/chkconfig oracle on
   ```

9. Change to the oracle user:

   ```
   su - oracle
   ```

10. To install Oracle 9.2.0.4, from within Disk1, run the script:

    ```
    ./runinstaller
    ```

11. When progressing through the installer, leave all prompts at their default values unless other wise specified below.
    - At prompt for UNIX Group Name, provide: dba
    - At prompt for *Installation Type*, select *Custom*.

    Select the following components to be installed:
    - Oracle 9i 9.2.0.4.0
    - Enterprise Edition Options 9.2.0.1.0
      - Oracle Partitioning 9i 9.2.0.4.0
    - Oracle Net Services 9.2.0.1.0
      - Oracle Net Listener 9.2.0.4.0
    - Oracle JDBC/OCI Interfaces 9.2.0.1.0
12. At the prompt for *Create Database*, select *NO*.
13. Optional, cancel all configuration assistants that the installer launches.
14. Modify the file `/opt/oracle/network/admin/sqlnet.ora` (or create the file (and directories) if it does not exist) to contain the following (remove any existing uncommented information in the file):

    ```
    NAMES.DIRECTORY_PATH = (TNSNAMES, HOSTNAME)
    ```

15. To apply the Oracle 9.2.0.7 Patch to Oracle, from within Disk1 of the Oracle 9.2.0.7 Patch distribution, run the script:

    ```
    Disk1/install/runInstaller
    ```

16. When progressing through the installer, leave all prompts at their default values unless other wise specified below.
    - At *Welcome* window, click *Next*.
    - At the *Specify File Locations* window, for *Destination Name* select *OUIHome* from the drop-down (or whatever you put as the *Destination Name* during the install of Oracle 9.2.0.4). Click *Next*.

- Depending on your version, at the *Select Product to Install* window, select *Oracle 9iR2 Patchset 9.2.0.7.0*. Click *Next*.
- At the *Summary* window, review the install summary. Click *Install*.
- At the *End of Installation* window, click *Exit*.

Oracle 10g R2 Installation on SLES 9

To install Oracle on SUSE Linux Enterprise Server 9:

1. Follow Installation instructions provided in SLES 9 install manual. Install SLES 9 with default packages along with *C/C++ Compiler and Tools* and SP2.

   NOTE: If you have already installed SUSE Linux, you can use YaST (Yet Another Setup Tool) in the SUSE Linux GUI to install *C/C++ Compiler and Tools*.

2. Login as root.
3. Install gcc_old using YaST.
4. Verify you are running SP2 by typing:

   ```
   SPident
   ```

   or

   ```
   cat /etc/SuSE-release
   ```

   You should get:

   ```
   CONCLUSION: System is up-to-date!
         Found     SLES-9-i386-SP2
   ```

   or

   ```
   SUSE LINUX Enterprise Server (i586)
   VERSION = 9
   PATCHLEVEL = 2
   ```

5. To automate most of the Oracle pre-install tasks and to create the oracle user, install orarun.rpm included with SLES 9.

   NOTE: See Oracle installation document for complete list of prerequisites.

   ```
   rpm -i <path>/orarun-1.8-109.15.i586.rpm
   ```

   NOTE: Recent copy of orarun is also available at Novell Web site: (http://www.novell.com).

6. The account for the oracle user is disabled. Enable it, by changing the shell for the oracle user from /bin/false to /bin/bash using YaST user administration or by editing the /etc/passwd file.
7. Set a new password for the oracle user by using YaST or typing:

   ```
   /usr/bin/passwd oracle
   ```

8. To set the kernel parameters, run

   ```
   /usr/sbin/rcoracle start
   ```

   Ignore any errors.

```
/sbin/chkconfig oracle on
```

9. Change to the oracle user:

   ```
   su - oracle
   ```

10. To install Oracle 10g R2 from within Disk1, run the script:

    ```
    ./runinstaller
    ```

11. At the *Welcome* window, select *Basic Installation*. Click *Next*.
12. Select *Create Starter Database* option and provide Global Database credentials. Click *Next*.
13. Provide Inventory Directory path and credentials. Click *Next*.
14. At the *Product-Specific Prerequisite Checks* window, verify that all systems checks were successful. Click *Next.*
15. At the *Summary* window, review the install summary and click *Install.*
16. In the *Configuration Assistants* window, click *Next*. In the *Execute Configurations* window, click *OK*.
17. In the *End of Installation* window, click *Exit*.

Oracle 10g Installation on SLES 10

To install Oracle on SUSE Linux Enterprise Server 10:

1. Follow Installation instructions provided in SLES 10 install manual. Install SLES 10 with the ext3 filesystem and default packages along with Oracle Server Base, *C/C++ Compiler and Tools*.
2. Login as root.
3. Install SLES 10 Service pack. Verify the service pack information by typing:

   ```
   SPident
   ```

   or

   ```
   cat /etc/SuSE-release
   ```

   At the time of this documentation, SLES 10 service pack is not released. Use SPident or cat/etc/SUSE-release to verify.

   You should get:

   ```
   CONCLUSION: System is up-to-date!
          Found     SLES-10-x86_64-current
   ```

4. The account for the oracle user is disabled. Enable it, by changing the shell for the oracle user from /bin/false to /bin/bash using YaST user administration or by editing the /etc/passwd file.
5. Set a new password for the oracle user by using YaST or typing:

   ```
   /usr/bin/passwd oracle
   ```

6. Change the default Oracle environment set by orarun, if required:
   - Change Oracle home directory by editing ORACLE_HOME variable in `/etc/profile.d/oracle.sh` file.
   - Default ORACLE_SID set by orarun install is ‘orcl’. Change it to ESEC in `/etc/profile.d/oracle.sh` file.

7. To set the kernel parameters, run

   ```
   /usr/sbin/rcoracle start
   ```

8. Change to the oracle user:

   ```
   su - oracle
   ```

9. Change to database directory and run `./runinstaller` (Oracle Universal Installer). An error occurs as shown below:
10. Fix the error by doing one of the following:
    - Modify `database/install/oraparam.ini` file to add support for SUSE Linux 10. After modifying oraparam.ini file "[Certified Versions]" line looks like:

      ```
      [Certified Versions]
      
      Linux=redhat=3,SuSE-9,SuSE-10,redhat-
      4,UnitedLinux-1.0.asianux-1,asianux-2
      ```

    - Install with option -ignoreSysPrereqs

      ```
      that is ./runInstaller –ignoreSysPrereqs
      ```

11. Accept the default inventory directory or Browse and select a new directory. Click *Next*.
12. From the Installation types, select *Enterprise Edition*. Click *Next*.
13. For checking Network configuration requirements, select *User Verified*. Click *Next*.
14. From the *Configuration* options, select *Install Database Software* only. Click *Next*.
15. Installation summary displays. Review and click *Install*.
16. Execute specified scripts as root and click *OK* on completion.
17. After install, click *Exit*.

Oracle (9i and 10g) Installation on Red Hat Linux (RHEL3 Only)

To install Oracle on Red Hat Linux:

1. Log in as root.
2. Create a UNIX group and UNIX user account for the Oracle database owner.

   Add a dba group (as root):

   ```
   groupadd dba
   ```

3. Add the Oracle user (as root):

   ```
   useradd –g dba –s /bin/bash –d /home/oracle –m
   oracle
   ```

4. Create directory for ORACLE_HOME and ORACLE_BASE:

   ```
   mkdir –p /opt/oracle/
   ```

5. Change the ownership of the ORACLE_BASE dir and deeper to oracle/dba:

```
chown -R oracle:dba /opt/oracle
```

6. Change to the oracle user:

```
su - oracle
```

7. Open the `.bash_profile` file (in oracle user's home directory) for editing and add the following to the end of the file:

NOTE: This set of environment variables must only be used for the oracle user. Specifically, they should not be set in the system environment or in the Sentinel Administrator User's environment.

```
# Set the LD_ASSUME_KERNEL environment
variable only for Red Hat 9,

# RHEL AS 3, and RHEL AS 4 !!

# Use the "Linuxthreads with floating stacks"
implementation instead of NPTL:

# for RH 9 and RHEL AS 3

export LD_ASSUME_KERNEL=2.4.1

# for RHEL AS 4

# export LD_ASSUME_KERNEL=2.4.19

# Oracle Environment

export ORACLE_BASE=/opt/oracle

export ORACLE_HOME=$ORACLE_BASE/

export ORACLE_SID=test

export ORACLE_TERM=xterm

# export TNS_ADMIN= Set if sqlnet.ora,
tnsnames.ora, etc. are not in
$ORACLE_HOME/network/admin

export NLS_LANG=AMERICAN;

export
ORA_NLS33=$ORACLE_HOME/ocommon/nls/admin/data

LD_LIBRARY_PATH=$ORACLE_HOME/lib:/lib:/usr/lib

LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/li
b

export LD_LIBRARY_PATH

# Set shell search paths

export PATH=$PATH:$ORACLE_HOME/bin
```

8. Re-login as oracle user to load environment variable changes from last step:

```
exit

su - oracle
```

9. Link gcc to version 2.9.6

NOTE: If /usr/bin/gcc296 or /usr/bin/g++296 does not exist, then gcc or g++ was not installed. If this is the case, install these components, and then return to this step.

```
su - root
ln -s /usr/bin/gcc296 /usr/bin/gcc
ln -s /usr/bin/g++296 /usr/bin/g++
```

10. Exit to return to oracle user prompt.

```
exit
```

11. Run the Oracle patch p3006854_9204_LINUX.zip, which patches the Linux operating system for the Oracle installation. This patch can be obtained from Oracle.

```
su - root
unzip p3006854_9204_LINUX.zip
cd 3006854
sh rhel3_pre_install.sh
```

12. Exit to return to oracle user prompt.

```
exit
```

13. To install Oracle 9.2.0.4, from within Disk1, run the script:

```
./runInstaller
```

14. When progressing through the installer, leave all prompts at their default values unless other wise specified below.
    - At prompt for UNIX Group Name, provide: dba
    - At prompt for *Installation Type*, select *Custom*.

    Select the following components to be installed:
    - Oracle 9i 9.2.0.4.0
    - Enterprise Edition Options 9.2.0.1.0
        - Oracle Partitioning 9i 9.2.0.4.0
    - Oracle Net Services 9.2.0.1.0
        - Oracle Net Listener 9.2.0.4.0
    - Oracle JDBC/OCI Interfaces 9.2.0.1.0
15. At prompt for *Create Database*, select *NO*.
16. Optional, cancel all the configuration assistants that the installer launches
17. Modify the file `/opt/oracle/network/admin/sqlnet.ora` (or create the file if it does not exist) to contain the following (remove any existing uncommented information in the file):

```
NAMES.DIRECTORY_PATH = (TNSNAMES, HOSTNAME)
```

18. To apply the Oracle 9.2.0.7 Patch to Oracle, from within Disk1 of the Oracle 9.2.0.7 Patch distribution, run the script:

```
./runInstaller
```

19. When progressing through the installer, leave all prompts at their default values unless other wise specified below.

- At *Welcome* window, click *Next*.
- At the *Specify File Locations* window, for *Destination Name* select *OUIHome* from the drop-down (or whatever you put as the *Destination Name* during the install of Oracle 9.2.0.4). Click *Next*.
- Depending on your version, at the *Select Product to Install* window, select *Oracle 9iR2 Patchset 9.2.0.7.0*. Click *Next*.
- At the *Summary* window, review the install summary. Click *Install*.
- At the *End of Installation* window, click *Exit*.

20. Unlink gcc:

```
su – root
rm /usr/bin/gcc
rm /usr/bin/g++
```

21. Exit to return to oracle user prompt.

```
Exit
```

Oracle (9i and 10g) Installation on Red Hat Linux (RHEL4 Only)

To install Oracle on Red Hat Linux:

1. Log in as root.
2. Run the following command to ensure the required packages (listed below) are installed on your server.

```
rpm –q make
```

List of Packages:

```
compat –db
compat-gcc-32
compat-gcc-32-c++
compat-oracle-rhel4
compat-libcwait
compat-libgcc-296
compat-libstdc++-296
compat-libstdc++-33
gcc
gcc-c++
gnome-libs
gnome-libs-devel
libaio-devel
libaio
make
openmotif21
```

```
xorg-x11-deprecated-libs-devel

xorg-x11-deprecated-libs
```

3. Create a UNIX group and UNIX user account for the Oracle database owner.

   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 directory for ORACLE_HOME and ORACLE_BASE:

   ```
   mkdir –p /opt/oracle/product/<10.2.0.3>
   ```

6. Change the ownership of the ORACLE_BASE dir and deeper to oracle/oinstall:

   ```
   chown -R oracle:oinstall /opt/oracle
   ```

7. Change to the oracle user:

   ```
   su - oracle
   ```

8. Open the `.bash_profile` file (in oracle user's home directory) for editing and add the following to the end of the file:

   NOTE: This set of environment variables must only be used for the oracle user. Specifically, they should not be set in the system environment or in the Sentinel Administrator User's environment.

   ```
   # 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
```

9. Save the `.bash_prolie` and exit.
10. Re-login as oracle user to load environment variable changes from last step:

    ```
    exit
    su - oracle
    ```

11. Check if the `.bash_profile` ran as expected, using the following command:

    ```
    set | more
    ```

12. Login as Oracle user. If you are using X emulation, set the DISPLAY environmental variable:

    ```
    DISPLAY=<machine-name>:0.0; export DISPLAY
    ```

13. To install Oracle 10.2.0.1, from within Disk1, run the script:

    ```
    ./runInstaller
    ```

14. When progressing through the installer, leave all prompts at their default values unless other wise specified below.
    - At *Welcome* window, click *Next*.
    - In the *File Locations* window, for *Destination Name* select *OUIHome* from the drop-down. Click *Next*.
    - Depending on your version, in *Select Product to Install* window, select *Oracle 10g Database 10.2.0.3*. Click *Next*.
    - In the *Installation Types* window, select *Enterprise Edition*. Click *Next*.
    - In *Database Configuration* window, select *General Purpose*. Click *Next*.
    - At the *Summary* window, review the install summary then click *Install*.
    - At the *End of Installation* window, click *Exit*.
15. To apply the Oracle 10.2.0.3 Patch, from within Disk1 of the Oracle 10.2.0.3 Patch distribution, run the script:

    ```
    ./runInstaller
    ```

16. Follow the prompts in the *Installation* windows. At the *Summary* window, review the install summary and click *install.* At the *End of Installation* window, click *Exit.*

Oracle 9i Installation on Solaris 9

To install Oracle 9i on Solaris 9:

1. Log in as root.

2. Follow the steps outlined in Oracle Note: 148673.1 SOLARIS: Quick Start Guide.
3. Install Oracle 9i Release 2 (9.2.0.1) as the oracle user. You are prompted for two additional CD-ROMs. You need to navigate to different directories for each of the additional CD-ROMs.
4. Patch your system to Oracle 9.2.0.7. See Oracle documentation for patch procedures.
5. To verify the patch level, as the Oracle UNIX user, provide:

   ```
   sqlplus ‘/as sysdba’
   ```

   The results should indicate a release of 9.2.0.7. Exit by typing quit.
6. Remove the directory you created for the patch.
7. After installing patches, remove the patch directories and files.
8. Reboot.

Oracle 9i Installation on Solaris 10

To install Oracle 9i on Solaris 10:

1. Log in as root.
2. To start the installation,

   ```
   # su  - oracle
   ```

   ```
   # < Installation directory or CD mount>/
   .runInstaller
   ```

3. When progressing through the installer, leave all prompts at their default values unless other wise specified below.
   - At prompt for UNIX Group Name, provide: dba
   - At prompt for *Installation Type*, select *Custom*.

   Select the following components to be installed:
   - Oracle 9i 9.2.0.4.0
   - Enterprise Edition Options 9.2.0.1.0
     - Oracle Partitioning 9i 9.2.0.4.0
   - Oracle Net Services 9.2.0.1.0
     - Oracle Net Listener 9.2.0.4.0
   - Oracle JDBC/OCI Interfaces 9.2.0.1.0
4. At prompt for *Create Database*, select *NO*.
5. Optional: Cancel all the configuration assistants that the installer launches.
6. Modify the file `/opt/oracle/network/admin/sqlnet.ora` (or create the file if it does not exist) to contain the following (remove any existing uncommented information in the file):

   ```
   NAMES.DIRECTORY_PATH = (TNSNAMES, HOSTNAME)
   ```

7. To apply the Oracle 9.2.0.7 Patch to Oracle, from within Disk1 of the Oracle 9.2.0.7 Patch distribution, run the script:

   ```
   ./runInstaller
   ```

8. When progressing through the installer, leave all prompts at their default values unless other wise specified below.
   - Read *Welcome* window, click *Next*.
   - At the *Specify File Locations* window, for *Destination Name* select *OUIHome* from the drop-down (or whatever you put as the *Destination Name* during the install of Oracle 9.2.0.4). Click *Next*.
   - Depending on your version, in the *Select Product to Install* window, select *Oracle 9iR2 Patchset 9.2.0.7.0*. Click *Next*.
   - At the *Summary* window, review the install summary. Click *Install*.
   - At the *End of Installation* window, click *Exit*.

Oracle 10g Installation on Solaris 9 and Solaris 10

NOTE: Sentinel is currently are certified with Oracle 10.2.0.3, with Oracle critical patch #5881721. See the kernel settings section for the procedures of setting kernel parameter settings in Solaris 9 and Solaris 10 respectively.

To install Oracle 10g on Solaris 9 and 10:

1. Log in as root.
2. Start the installation

```
#  su - oracle

# < Installation directory or CD mount>/
.runInstaller
```

3. In the *Welcome* window:
   - Select *Basic Installation*.
   - Uncheck *Create Starter Database* option.
   - Specify the Oracle Home Location.
   - UNIX DBA group is usually dba. Click *Next*.
4. In the *Product-Specific Prerequisite* window:
   - Verify that all systems checks were successful. Click *Next*.
5. In the *Summary* window:
   - Review the install summary and click *Install*.
   - At the *End of Installation* window, click *Exit*.

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 https://metalink.oracle.com for the error numbers 336299.1 with subject “dbstart errors out when executing in 10.2.0.1.0”, 5183726 and 4665320.

After installation of Sentinel 6.0, you need to modify the `dbstart` and `dbshut` scripts for Sentinel to start Oracle 10 database.

To modify dbstart script on Solaris 10:

1. Open `dbstart` script for edit from the path $ORACLE_HOME/bin/dbstart.

2. Go to line 78 and replace the same with ORACLE_HOME_LISTNER=$ORACLE_HOME.
3. Add `#!/bin/bash` at the start to request the bash shell.
4. Make sure “ORATAB” pointing to ORATAB=/var/opt/oracle/oratab.

   NOTE: If ORATAB is not in the above specified location on your machine, modify the ORATAB path manually to exact location.
5. Click *Save* and exit.

To modify dbshut script on Solaris 10:

1. Open `dbshut` script for edit from the path $ORACLE_HOME/bin/dbshut.
2. Make sure “ORATAB” pointing to ORATAB=/var/opt/oracle/oratab.

   NOTE: If ORATAB is not in the above specified location on your machine, modify the ORATAB path manually to exact location.
3. Click *Save* and exit.

To modify dbstart script on RedHat Linux ES4:

1. Open `dbstart` script for edit from the path $ORACLE_HOME/bin/dbstart.
2. Make sure “ORATAB” pointing to ORATAB=/etc/oratab.

   NOTE: If ORATAB is not in the above specified location on your machine, modify the ORATAB path manually to exact location.
3. Click *Save* and exit.

To modify dbshut script on RedHat Linux ES4:

1. Open `dbshut` script for edit from the path $ORACLE_HOME/bin/dbshut.
2. Make sure “ORATAB” pointing to ORATAB=/etc/oratab.

   NOTE: If ORATAB is not in the above specified location on your machine, modify the ORATAB path manually to exact location.
3. Click *Save* and exit.

Manual Oracle Instance Creation (Optional)

For simplicity, Novell recommends using the Sentinel installer to create the Oracle instance during the Sentinel database components installation. However, this procedure is provided in case it is corporate policy that the DBA create the Oracle instance. The tablespaces must be named exactly as specified.

In the Oracle instance you need to configure:

- Parameters
- Tablespaces

To create an Oracle Instance:

1. Login as an Oracle user.
2. Using the Oracle Database Assistant GUI, create the following:

NOTE: Your values might vary depending on your system configuration and requirements.

Minimum Recommended Solaris / Linux Configuration Parameters	
Parameters	**Size (bytes or otherwise specified)**
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
hash_join_enabled	TRUE
optimizer_index_caching	50
optimizer_index_cost_adj	55

Table E-1: *Minimum Recommended Solaris / Linux Configuration Parameters*

Minimum Recommended Solaris / Linux Tablespace Size		
Tablespace	**Example Size**	**Notes**
SYSTEM	500M	Minimum value (autoextend enabled)
TEMP	1G	Minimum value
UNDO	1G	Minimum value (autoextend enabled)
ESENTD	5G	Minimum value This for event data (autoextend enabled)
ESENTD2	500M	Minimum value Data for configuration, assets, vulnerability and associations (autoextend enabled)
ESENTWFD	250M	For iTrac data (autoextend enabled)
ESENTWFX	250M	For iTrac index (autoextend enabled)
ESENTX	3G	Minimum value For event index (autoextend enabled)
ESENTX2	500M	Minimum value Index for configuration, assets, vulnerability and associations (autoextend enabled)
SENT_ADVISORD	50G	Minimum value For Advisor data (autoextend enabled)
SENT_ADVISORX	100M	Minimum value For Advisor index (autoextend enabled)
SENT_AUDITD	250M	Minimum value For Audit data (autoextend enabled)
SENT_AUDITX	250M	Minimum value For Audit index (autoextend enabled)
SENT_LOBS	100M	Minimum value For database large objects (autoextend enabled)
SENT_SMRYD	3G	Minimum value For Aggregation, summary data (autoextend enabled)
SENT_SMRYX	2G	Minimum value For Aggregation, summary index (autoextend enabled)

Minimum Recommended Solaris / Linux Tablespace Size		
Tablespace	**Example Size**	**Notes**
SYSAUX	100M	Minimum value For Oracle 10g auditing (not Sentinel-specific) Required for Oracle 10g only

Table E-2: *Minimum Recommended Solaris / Linux Tablespace Size*

NOTE: Novell also recommends allocating space for the redo log files. 3 x 100M is the minimum value, which should be increased if the event rate is high.

3. Run the script `createEsecdba.sh` found in the directory sentinel\dbsetup\bin in the Sentinel Installation CD. This script will create the user esecdba, which is required to add database objects using the Sentinel installer.
4. Back up the database.

F Sentinel with Oracle Real Application Clusters

Sentinel 6 is certified to run on an Oracle database with Real Application Clusters (RAC). The supported Oracle database version is Oracle 10g 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:

- Configure Oracle RAC database
- Install Sentinel Database schema on Oracle RAC
- Configure connection properties files for DAS components
- Configure connection for Sentinel Data Manager
- Configure connection for Crystal Enterprise Server

These steps are described in this document.

NOTE: Before installing Sentinel 6.0 software, please make sure your Oracle cluster is up and running using Oracle RAC tools.

Configuring the Oracle RAC database

To configure the Oracle RAC database:

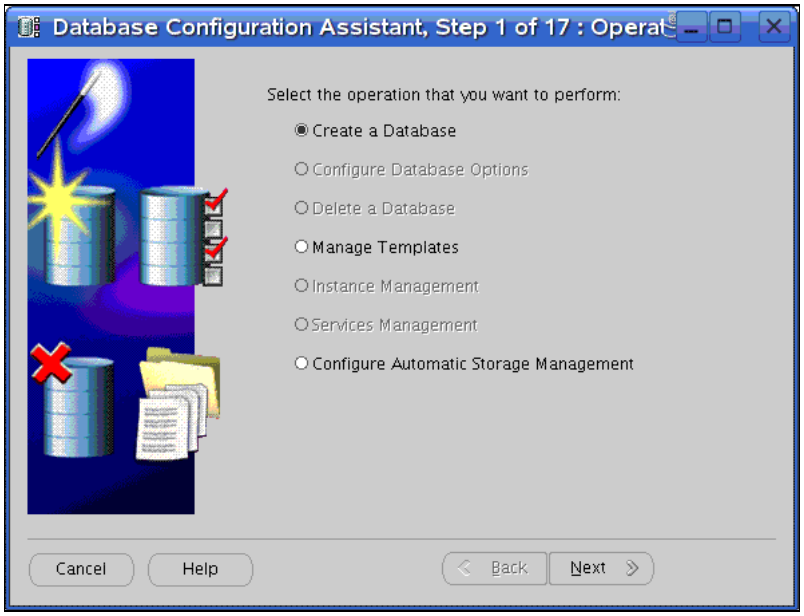
- Create the RAC database using Oracle Database Configuration Assistant utility
- Create the required Sentinel tablespaces to contain Sentinel data
- Create the Sentinel schema owner ESECDBA
- Install Sentinel database
- Install remaining Sentinel components
- Configure the connection properties file

Creating the RAC Database

This procedure will create an empty Oracle RAC database that is ready for the installation of Sentinel components. This procedure uses the Oracle Database Configuration Assistant (DBCA).

To create RAC database:

1. Select *Oracle Real Application Clusters database* in the Database Configuration Assistant. Click *Next*.
2. From the options in this screen, select *Create a database*. Click *Next*.



Database Configuration Assistant, Step 1 of 17 : Operat

Select the operation that you want to perform:

● Create a Database

○ Configure Database Options

○ Delete a Database

○ Manage Templates

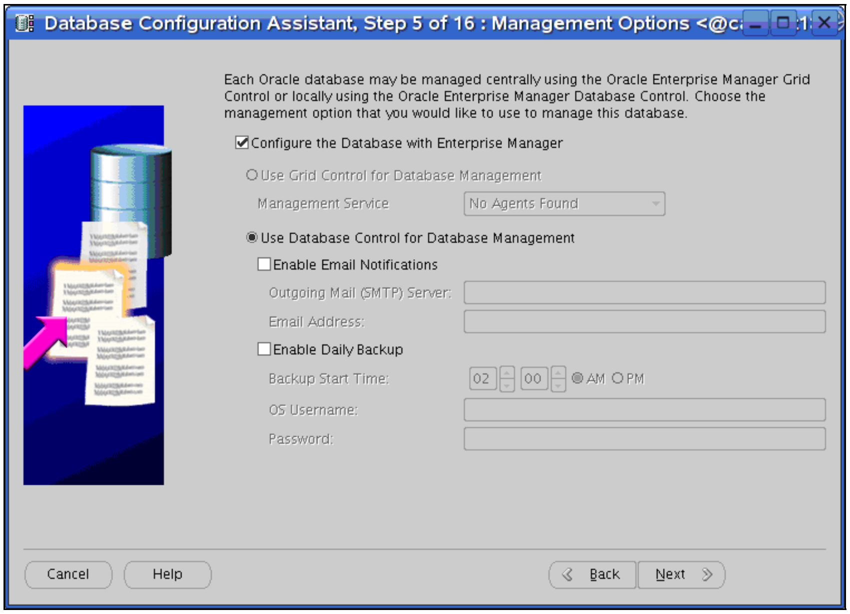
○ Instance Management

○ Services Management

○ Configure Automatic Storage Management

Figure F-1: *Database Configuration Assistant-Operation selection*

3. To select all nodes to create cluster database, click *Select All*. Click *Next*.
4. From the list of templates, select a template. By default, General Purpose is selected. Click *Next*.
5. Provide the *Database Name* and *SID* (Oracle System Identifier) prefix. Click *Next*.
6. The default management option selected to manage this database is *Configure the Database with Enterprise Manager*. Click *Next*.



Database Configuration Assistant, Step 5 of 16 : Management Options <@c

Each Oracle database may be managed centrally using the Oracle Enterprise Manager Grid Control or locally using the Oracle Enterprise Manager Database Control. Choose the management option that you would like to use to manage this database.

☑ Configure the Database with Enterprise Manager

○ Use Grid Control for Database Management

Management Service: No Agents Found

● Use Database Control for Database Management

□ Enable Email Notifications

Outgoing Mail (SMTP) Server:

Email Address:

□ Enable Daily Backup

Backup Start Time: 02 00 ● AM ○ PM

OS Username:

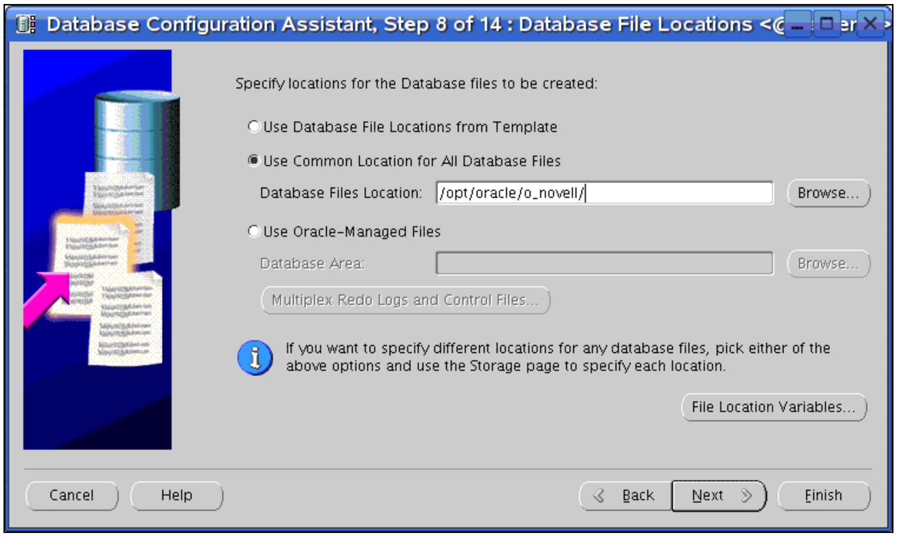
Password:

Figure F-2: *Database Configuration Assistant-Management option selection*

7. You can use same passwords for all user accounts or you can use different passwords. Select your option and provide the passwords. Click *Next*.

8. From the three storage mechanisms offered by the system, Cluster File System / Automatic Storage Management / Raw Devices, select your option. If you chose Raw Devices, specify the path of the Raw Devices mapping file. Click *Next*.

9. Specify a directory to place the database files on the Storage system. Click *Finish*.



Database Configuration Assistant, Step 8 of 14 : Database File Locations

Specify locations for the Database files to be created:

○ Use Database File Locations from Template

● Use Common Location for All Database Files

Database Files Location: /opt/oracle/o_novell/

○ Use Oracle-Managed Files

Database Area:

If you want to specify different locations for any database files, pick either of the above options and use the Storage page to specify each location.

Browse...
Browse...
Multiplex Redo Logs and Control Files...
File Location Variables...
Cancel
Help
Back
Next
Finish

Figure F-3: *Database Configuration Assistant-Specify Locations*

10. Retain the default selection in the *Recovery options and Sample Schemas* windows, click *Next*.

11. You can create a Database Service here or you can create later using DBCA.

12. In the *Database storage* window, retain the default selection. Click *Next*.

13. From the Database creation options, select *Create Database*. Click *Finish*.

Creating Sentinel Tablespaces

WARNING: The Sentinel installation will not be successful unless all of the tablespaces below are created.

NOTE: You can use Oracle Enterprise Manager or SQL query to verify the existence of these tablespaces.

Minimum Recommended Tablespace Size

Tablespace	Example Size	Notes
REDO	3 x 100M	This is a minimum value. You should create larger redo logs if you have a high EPS.
SYSTEM	500M	Minimum value (autoextend enabled)
TEMP	1G	Minimum value
UNDO	1G	Minimum value (autoextend enabled)
ESENTD	5G	Minimum value This for event data (autoextend enabled)

Minimum Recommended Tablespace Size

Tablespace	Example Size	Notes
ESENTD2	500M	Minimum value Data for configuration, assets, vulnerability and associations (autoextend enabled)
ESENTWFD	250M	For iTRAC data (autoextend enabled)
ESENTWFX	250M	For iTRAC index (autoextend enabled)
ESENTX	3G	Minimum value For event index (autoextend enabled)
ESENTX2	500M	Minimum value Index for configuration, assets, vulnerability and associations (autoextend enabled)
SENT_ADVISORD	200M	Minimum value For Advisor data (autoextend enabled)
SENT_ADVISORX	100M	Minimum value For Advisor index (autoextend enabled)
SENT_AUDITD	250M	Minimum value For Audit data (autoextend enabled)
SENT_AUDITX	250M	Minimum value For Audit index (autoextend enabled)
SENT_LOBS	100M	Minimum value For database large objects (autoextend enabled)
SENT_SMRYD	3G	Minimum value For Aggregation, summary data (autoextend enabled)
SENT_SMRYX	2G	Minimum value For Aggregation, summary index (autoextend enabled)
SYSAUX	100M	Minimum value For Oracle 10g auditing (not Sentinel-specific)

Table F-1: *Minimum Recommended Tablespace size*

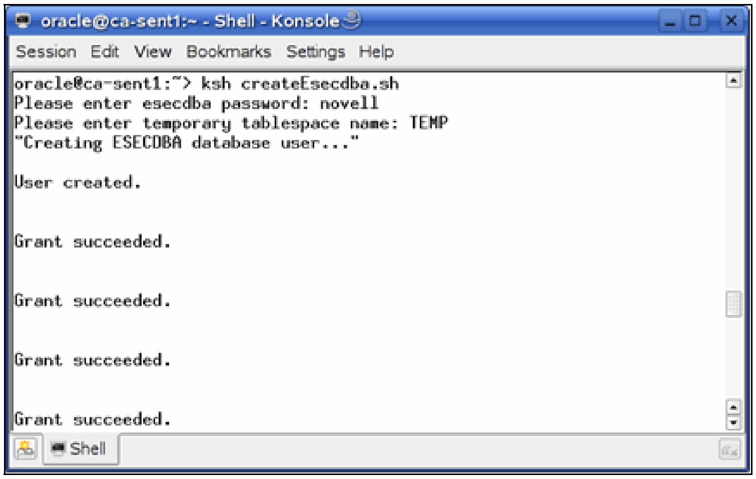
Creating ESECDBA

ESECDBA is the name of the Sentinel schema owner. Most objects created by the Sentinel installer will be owned by this user.

To create ESECDBA:

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 might need to edit the script to properly set Oracle environment variables and the “CONNECT AS” string (by default the script connects as “sysdba”).

   WARNING: Run this script only once.


oracle@ca-sent1:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
Shell

```
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.
```

Figure F-4: *Creating ESECDBA*

Installing Sentinel Database

After the database is configured, you must install the Sentinel database. This procedure will install to a single cluster node as if it were 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 that machine will also be the Sentinel Server, you can install those components at the same time (see sections above for prompts for core components).

To install the Sentinel database:

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 and double-click:

   For GUI mode:

   ```
   ./setup.sh
   ```

   For textual (“headless”) mode:

   ```
   ./setup.sh –console
   ```

4. Select the language and click *OK*.
5. After reading the Welcome screen, click *Next*.
6. Read and accept End User License Agreement, Click *Next*.
7. Accept the default install directory or click *Browse* to specify a different location. Click *Next*.
8. For type of installation, select Custom (default). Click *Next*.
9. In the *Feature Selection* window, de-select any unnecessary options and select *Database*. Click *Next*.
10. Select the target database server platform.
    - Select Oracle 10g from the drop-down list.
    - Select *Add database objects to an existing database*.

    Click *Next*.

11. Provide Authentication Information for creating:
    - Sentinel Application Database User
    - Sentinel Administrator User

    Click *Next*.
12. Summary of Database parameters specified will display. Click *Next*.
13. Installation Summary displays. Click *Install*.
14. After install, click *Finish*.
15. Install the rest of the Sentinel system (including Collector Services, DAS, Communication Server, and other Sentinel components) using the information in "Installing Sentinel 6" section.

Configuring Connection Properties File

You need to create a database connection property file manually 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 file $ORACLE_HOME/db/network/admin/tnsnames.ora on the cluster nodes.

To configure RACconnect.properties:

1. Log into the machine where the Sentinel Data Access Service (DAS) components are installed.
2. Change directory to $ESEC_HOME/config.
3. Create RACconnect.properties file. Here is a sample example configured 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
,1090,1092,1094,2396,3106,3111,3113,3114
advancedconnectionstring=(DESCRIPTION=
(ADDRESS= (PROTOCOL=TCP) (HOST=ca-sent1.novell.com)
(PORT=1521))
(ADDRESS= (PROTOCOL=TCP) (HOST=ca-sent2.novell.com)
(PORT=1521))
(ADDRESS= (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 and add following arguments to the process components listed below:

```
-
Desecurity.connect.config.file=../config/RACconnect.pr
operties
```

The process components which need this change include:

- DAS_Aggregation
- DAS_Binary
- DAS_iTRAC
- DAS_Query
- DAS_RT

For example:

```
<process component="DAS" depends="UNIX Communication
Server,Windows Communication Server"
image=""$(ESEC_JAVA_HOME)/java" -server -
Dsrv_name=DAS_Query
-Xmx256m -Xms85m -XX:+UseParallelGC -Xss136k -Xrs
-Duser.language=en -Dfile.encoding=UTF8
-
Desecurity.dataobjects.config.file=/xml/BaseMetaData.x
ml,
/xml/WorkflowMetaData.xml
-
Djava.util.logging.config.file=../config/das_query_log
.prop
-Djava.security.auth.login.config=../config/auth.login
-Djava.security.krb5.conf=../config/krb5.conf
-
Desecurity.execution.config.file=../config/execution.p
roperties -
Dcom.esecurity.configurationfile=../config/configurati
on.xml
-
Desecurity.connect.config.file=../config/RACconnect.pr
operties
-jar ../lib/ccsbase.jar ..//config//das_query.xml"
min_instances="1" name="DAS_Query"
post_startup_delay="20" type="container"
working_directory="$(ESEC_HOME)/data" />
```

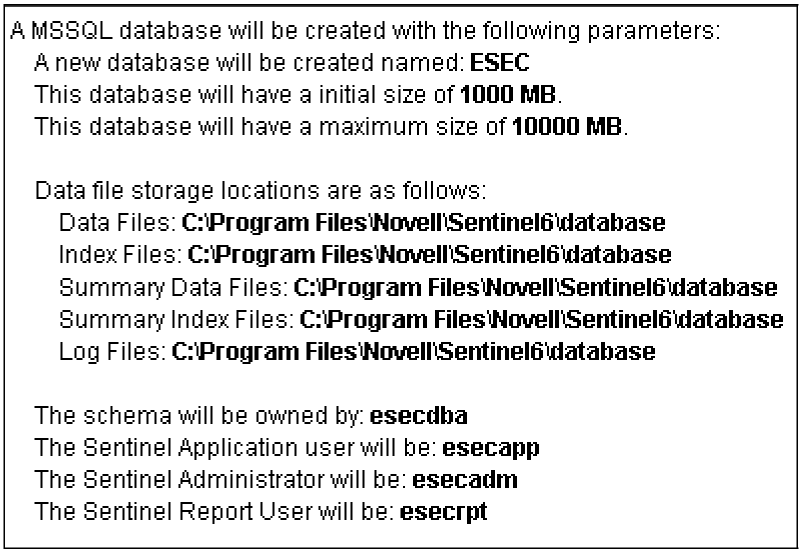
5. Restart the Sentinel services so the database connection changes will take effect.

Configuring Connection for Sentinel Data Manager

The advancedconnectionstring value from the RACconnect.properties file must be used to log into Sentinel Data Manager.

To log into Sentinel Data Manager:

1. Launch Sentinel Data Manager from $ESEC_HOME/bin/sdm.
2. Provide 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. Check *Save connection settings*.
6. Click *Connect*.



A MSSQL database will be created with the following parameters:
A new database will be created named: **ESEC**
This database will have a initial size of **1000 MB**.
This database will have a maximum size of **10000 MB**.

Data file storage locations are as follows:
Data Files: **C:\Program Files\Novell\Sentinel6\database**
Index Files: **C:\Program Files\Novell\Sentinel6\database**
Summary Data Files: **C:\Program Files\Novell\Sentinel6\database**
Summary Index Files: **C:\Program Files\Novell\Sentinel6\database**
Log Files: **C:\Program Files\Novell\Sentinel6\database**

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**

Figure F-5: *Summary Details*

Configuring Connection for Crystal

For Crystal Enterprise Server to use the Oracle RAC database, you must edit the tnsnames.ora file. The steps in the standard installation for Crystal Enterprise Server must be followed before performing this step.

To edit the tnsnames.ora file:

1. Log into the server with Crystal Enterprise Server installed and locate the tnsnames.ora file.
2. Modify the ESECURITYDB service to show 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)
     )
   )
)
```