AUTHORIZED DOCUMENTATION

Installation Guide

Novell® Sentinel™

6.1

July, 2008

www.novell.com

Legal Notices

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

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

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.

Contents

Preface

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

Audience

This documentation is intended for Information Security Professionals.

Feedback

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

Additional Documentation

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

- Sentinel 6.1 Install Guide (http://www.novell.com/documentation/sentinel61/pdfdoc/sentinel_61_installation_guide.pdf)
- Sentinel 6.1 User Guide (http://www.novell.com/documentation/sentinel61/pdfdoc/sentinel_61_user_guide.pdf)
- Sentinel 6.1 Reference Guide (http://www.novell.com/documentation/sentinel61/pdfdoc/sentinel_61_reference_guide.pdf)
- Sentinel SDK (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel)

  This site gives you details about developing collectors (proprietary or JavaScript) and JavaScript correlation actions.

Sentinel Install Guide

This guide explains how to install the following Sentinel components:

- Sentinel Communication Server
- Data Access Service (DAS)
- Sentinel Control Center
- Sentinel Correlation Engine
- Collector Manager
- Crystal Reports Server
- Advisor
- Collector Builder
- Sentinel Data Manager
- Sentinel Solution Designer

Sentinel User Guide

This guide discusses how to use the Sentinel components and features:

- Sentinel Console Operation
- Sentinel Features
- Sentinel Architecture
- Sentinel Communication
- Shutdown/Startup of Sentinel
- Vulnerability Assessment
- Event Monitoring
- Event Filtering
- Event Correlation
- Sentinel Data Manager
- Identity Integration
- Event Configuration for Business Relevance
- Mapping Service
- Historical Reporting
- Collector Host Management
- Incidents
- Cases
- User Management
- Workflow
- Solution Packs
- Actions and Integrators

Sentinel User Reference Guide

This guide discusses the following advanced topics:

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

Collector Builder User Guide

This guide discusses how to use the Collector Builder. This guide is located in the Novell Developer Community web site.

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

Sentinel Patch Installation Guide

This guide discusses how to upgrade from one version of Sentinel to another.

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

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

  ![Cannot put links here because there is no specific target ~ Mary]

  - For more information, see “Section Name” (if in the same Chapter).
  - For more information, see “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).

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, TM, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux or UNIX, should use forward slashes as required by your software.

Contacting Novell

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

Introduction

1

The following sections will walk you through the product basics. The rest of the *Sentinel User Guide*![xrefext to User Guide here ~ Mary] has more detailed architecture, operation and administrative procedures.

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

1.1 Sentinel Overview

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

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

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

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

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

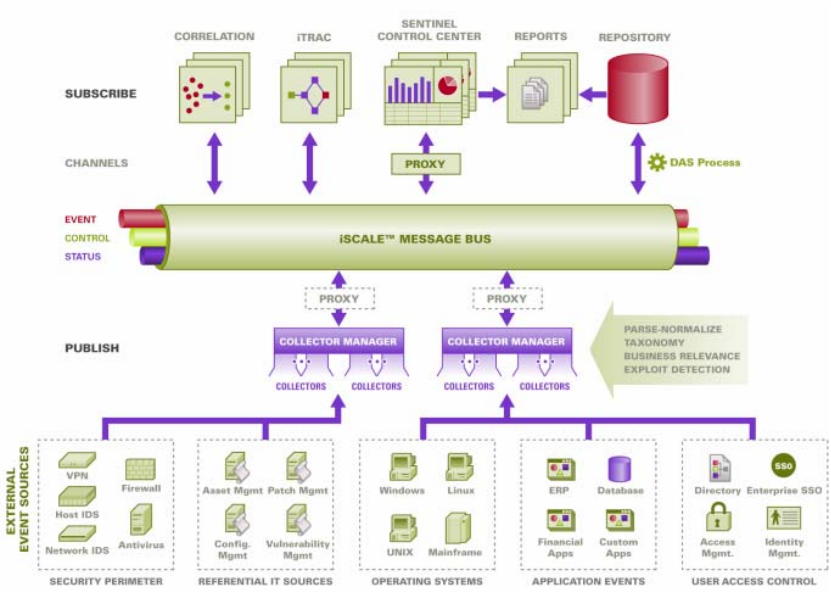
With Sentinel, you get:

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

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

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

Figure 1-1 *Conceptual Architecture of Sentinel*



1.2 Sentinel User Interfaces

Sentinel includes several easy-to-use user interfaces:

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

1.2.1 Sentinel Control Center

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

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

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

1.2.2 Sentinel Data Manager

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

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

1.2.3 Sentinel Solution Designer

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

1.2.4 Sentinel Collector Builder

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

1.3 Sentinel Server Components

Sentinel is made up of several components:

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

1.3.1 Sentinel Server

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

1.3.2 Sentinel Communication Server

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

1.3.3 Sentinel Database

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

1.3.4 Sentinel Collector Manager

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

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

1.3.5 Correlation Engine

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

1.3.6 iTRAC

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

1.3.7 Crystal Reports Server

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

1.3.8 Sentinel Advisor and Exploit Detection

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

1.4 Sentinel Plugins

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

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

1.4.1 Collectors

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

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

- Intrusion Detection Systems (host)
- 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

JavaScript Collectors can be written and run on Sentinel 6.0 SP1 and above using standard JavaScript development tools and the Collector SDK. Proprietary Collectors can be built or modified using Section 1.2.4, “Sentinel Collector Builder,” on page 15, a standalone application included with the Sentinel system.

1.4.2 Connectors and Integrators

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

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

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

1.4.3 Correlation Rules and Actions

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

1.4.4 Reports

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

1.4.5 iTRAC Workflows

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

1.4.6 Solution Packs

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

1.5 Language Support

Sentinel components are localized for the following languages:

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

There are several exceptions:

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

System Requirements

2

2.1 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 on the minimum requirements, look for updates at the Novell Documentation site (http://www.novell.com/documentation/sentinel61).

The table below lists the specific patch levels that were used to perform Sentinel testing. For convenience in this document, these platforms will be referred to by the short name in the left column. In situations in which the bit-length does not matter in this document, the bit-length may be truncated from the short name.

Table 2-1 *Patch Level Information*

Short Name	Full Name and Patch Level
SLES 10 (32-bit)	SUSE® Linux Enterprise Server 10 SP1 (32-bit)
SLES 10 (64-bit)	SUSE Linux Enterprise Server 10 SP1 (64-bit)
RHEL 4 (32-bit)	Red Hat Enterprise Linux 4 Nahant Update-4 (32-bit)
RHEL 4 (64-bit)	Red Hat Enterprise Linux 4 Nahant Update-4 (64-bit)
Solaris 10 (64-bit)	Sun Solaris 10 6/06 s10s_u2wos_09a (64-bit SPARC)
Windows 2003 (32-bit)	Windows 2003 SP2, Standard or Enterprise Edition (32-bit)
Windows 2003 (64-bit)	Windows 2003 SP1, Standard or Enterprise Edition (64-bit)
Windows 2008 (64-bit)	Windows 2008 SP1, Standard Edition (64-bit)
SLED 10 (32-bit)	SUSE® Linux Enterprise Desktop 10 SP1 (32-bit)
Windows XP (32-bit)	Windows XP SP2 (32-bit)
Windows Vista (32-bit)	Windows Vista SP1 (32-bit)
Oracle 10 (32-bit)	Oracle* 10g Enterprise Edition with partitioning (v 10.2.0.3 - 5901891 include critical patch #5881721, security patch 6864068) (32-bit), running on SuSE Linux Enterprise Server 9 (32-bit)
Oracle 10 (64-bit)	Oracle 10g Enterprise Edition with partitioning (v 10.2.0.3 - 5901891 include critical patch #5881721, security patch 6864068), running on (64-bit)
SQL Server 2005 (32-bit)	Microsoft SQL Server 2005 SP2, Standard or Enterprise Edition (32-bit)

Short Name	Full Name and Patch Level
SQL Server 2005 (64-bit)	Microsoft SQL Server 2005 SP2, Standard or Enterprise Edition (64-bit)
SQL Server 2008 (64-bit)	Microsoft SQL Server 2008 (Version 10.0.1300.13)
SLES 9 (32-bit)	SuSE Linux Enterprise Server 9 SP2 (32-bit)

You should check with the respective vendors for security updates and patches. These hotfixes and security patches typically have no impact on Sentinel operations and are therefores supported. Since major or minor releases of a database or operating system typically involve more substantial changes, only the versions above are supported for this release.

2.1.1 Database Supported Platforms

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

Table 2-2 *Database Supported Platforms*

	Oracle 10 (32)	Oracle 10 (64)	SQL Server 2005 (32)	SQL Server 2005 (64)	MS SQL 2008 (64)
SLES 10 (32)	Supported	Not Supported	Not Supported	Not Supported	Not Supported
SLES 10 (64)	Not Supported	Certified	Not Supported	Not Supported	Not Supported
RHEL 4 (32)	Supported	Not Supported	Not Supported	Not Supported	Not Supported
RHEL 4 (64)	Not Supported	Supported	Not Supported	Not Supported	Not Supported
Solaris 10 (32)	Supported	Not Supported	Not Supported	Not Supported	Not Supported
Solaris 10 (64)	Not Supported	Supported	Not Supported	Not Supported	Not Supported
Windows 2003 (32)	Not Supported	Not Supported	Supported	Not Supported	Not Supported
Windows 2003 (64)	Not Supported	Not Supported	Not Supported	Certified	Not Supported
Windows 2008 (64)	Not Supported	Not Supported	Not Supported	Not Supported	Supported

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

NOTE: All databases should be installed on an operating system that is certified by the database vendor and also by Novell for use with Sentinel components. Oracle must run on Linux* or Solaris (not Windows).

2.1.2 Sentinel Components

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

The Sentinel User Applications in the table below include Sentinel Control Center, Sentinel Data Manager, and Sentinel Solution Designer.

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

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

Table 2-3 *Software and Operating System Combinations*

	Sentinel Server Components	Sentinel User Applications	Collector Manager	Collector Builder	Crystal Reports Server
SLES 10 (32)	Supported	Supported	Certified	Not Supported	Not Supported
SLES 10 (64)	Certified	Supported	Supported	Not Supported	Not Supported
RHEL 4 (32)	Supported	Supported	Supported	Not Supported	Certified
RHEL 4 (64)	Supported	Supported	Supported	Not Supported	Not Supported
Solaris 10 (32)	Supported	Supported	Certified	Not Supported	Not Supported
Solaris 10 (64)	Certified	Supported	Supported	Not Supported	Not Supported
Windows 2003 (32)	Supported	Supported	Certified	Supported	Certified
Windows 2003 (64)	Certified	Supported	Supported	Supported	Not Supported
Windows 2008 (64)	Supported	Supported	Supported	Supported	Not Supported
SLED 10	Not Supported	Certified	Not Supported	Not Supported	Not Supported
Windows XP	Not Supported	Certified	Not Supported	Supported	Not Supported
Windows Vista	Not Supported	Supported	Not Supported	Supported	Not Supported
SLES 9 (32)	Not Supported	Not Supported	Not Supported	Not Supported	Certified

The supported reporting server is Crystal Reports Server XI R2. Crystal requires a web server and a Central Management Server (CMS) database for operation, in addition to the Sentinel database. The Crystal Reports Server can be run on the following platforms in the Sentinel environment:

- Red Hat Enterprise Linux 4 (32-bit)
  - Crystal CMS database on MySQL

- Web server on Apache Tomcat
- Sentinel database on Oracle recommended; other configurations untested

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

Novell has tested publishing and running reports from the Sentinel interface using the following versions of Crystal:

- **On Linux:** Crystal Reports Server XI R2 SP2
- **On Windows:** Crystal Reports Server XI R2 SP3

These service packs can be downloaded from the Download section of the SAP web site at

https://www.sdn.sap.com/irj/sdn/businessobjects-downloads (https://www.sdn.sap.com/irj/sdn/businessobjects-downloads)

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

2.1.3 Platform Support Exceptions and Cautions

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

- Crystal Reports Server XI R2's vendor does not currently support Crystal on Solaris or SUSE Linux Enterprise Server 10; therefore Novell will not support these combinations either.
- Oracle does not currently support Oracle 10 (32-bit) on 32-bit Solaris 10

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

- Sentinel on SUSE Linux Enterprise Server 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

Although Novell recommends running the Sentinel database and reporting engine on platforms that have been fully quality assured by Novell, both the Oracle database and Crystal Reports Server are supported on additional platforms by their respective vendors. If a customer wants to use one of these additional platforms, Novell will provide some support, with caveats.

- 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 may 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.

2.2 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.

WARNING: Because of high performance nature of Sentinel, Novell recommends that Sentinel run on dedicated hardware in production environments instead of Virtual Machines, or VMs.

2.2.1 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 Reports Server. Therefore, Novell makes the following recommendations:

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

In low event-rate environments (for example, eps < 25), 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 Reports Server be installed on its own dedicated machine, particularly if the database is large or reporting usage is heavy. Crystal can be installed on the same machine as the database if the database is small, the reporting usage is light, and the database is installed on either Windows or Linux (not Solaris). The suggested configurations below represent small, medium, and large implementations but are based on Sentinel 5.1.3. Updated recommendations will be posted on the Novell Documentation Site at http://www.novell.com/documentation/sentinel61 (http://www.novell.com/documentation/sentinel61) when testing is completed.

Table 2-4 *Two Machine Configuration, used for 1-500 EPS*

1-500 EPS: Two Machine Configuration			
Components	**RAM**	**Space**	**CPU**
Machine 1: Sentinel Server / Collector Manager ◆ Correlation Engine ◆ DAS ◆ Communication Server ◆ Advisor ◆ Collector Manager / Collectors ◆ Database ◆ Crystal Reports 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 Reports Server	2 GB	20 GB	Windows or Linux - 1 x Dual Core Intel® Xeon® 5150 (2.66 GHz)

Table 2-5 *Three Machine Configuration, used for 500-1500 EPS*

500 – 1500 EPS: Three Machine Configuration			
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 Reports 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 Reports Server	2 GB	20 GB	Windows or Linux - 1 x Dual Core Intel® Xeon® 5150 (2.66 GHz)

Table 2-6 *4-5 Machine Configuration, used for 1500-3000 EPS)*

1500 - 3000 EPS: 4-5 Machine Configuration			
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 ◆ Database ◆ Crystal Reports Server (optional for Windows/Linux)	8 GB+	3 TB+	Windows or Linux - 2 x Dual Core Intel® Xeon® 5160 (3.0 GHz) or Sun Solaris - 2 x 1.8 GHz UltraSPARC IV+

1500 - 3000 EPS: 4-5 Machine Configuration

Components	RAM	Space	CPU
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 Reports 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 Chapter 6, “Adding Sentinel Components,” on page 79.	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+

Installing Sentinel 6.1

3

3.1 Installer Overview

This section helps you install the major components of the Sentinel system. The Sentinel installer offers the option of a Simple installation or 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:

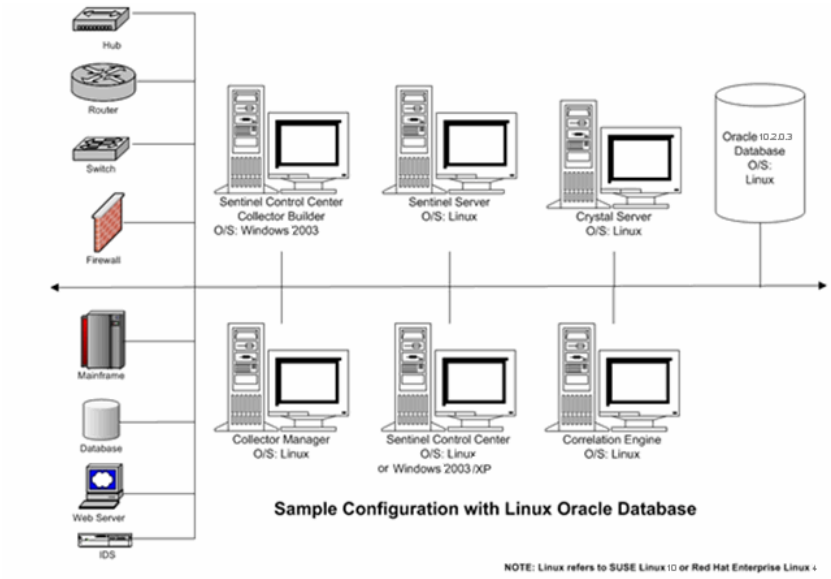
- **Database:** The database, which stores the events, correlated events, and configuration information, is an essential part of the Sentinel system. The database should be installed according to best practices recommended by Oracle and Microsoft for database installation, directory structure, and so on.
- **Crystal Reports 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 Chapter 8, “Crystal Reports for Windows,” on page 95 and Chapter 9, “Crystal Reports for Linux,” on page 123.
- **Crystal Reports Developer:** This application is used to create and modify reports.
- **Advisor:** Advisor provides real-time intelligence about attacks and vulnerabilities, including real-time exploit detection to determine which threats are taking place against vulnerable systems. This is an optional module. For more information about Advisor and information about the installer for the Advisor core data snapshot, see Chapter 4, “Advisor Configuration,” on page 59.
- **Third-Party Integration:** Sentinel integrates with HP OpenView Service Desk.

NOTE: Remedy Service Desk integration was previously available as an installer option. With the Sentinel 6.1 release, Remedy integration is achieved through an Integrator plugin and is no longer included in the Sentinel installer. With the proper license, the Remedy Integrator and associated Action can be downloaded from the content web site at http://support.novell.com/products/sentinel/sentinel61.html (http://support.novell.com/products/sentinel/sentinel61.html).

3.2 Sentinel Configurations

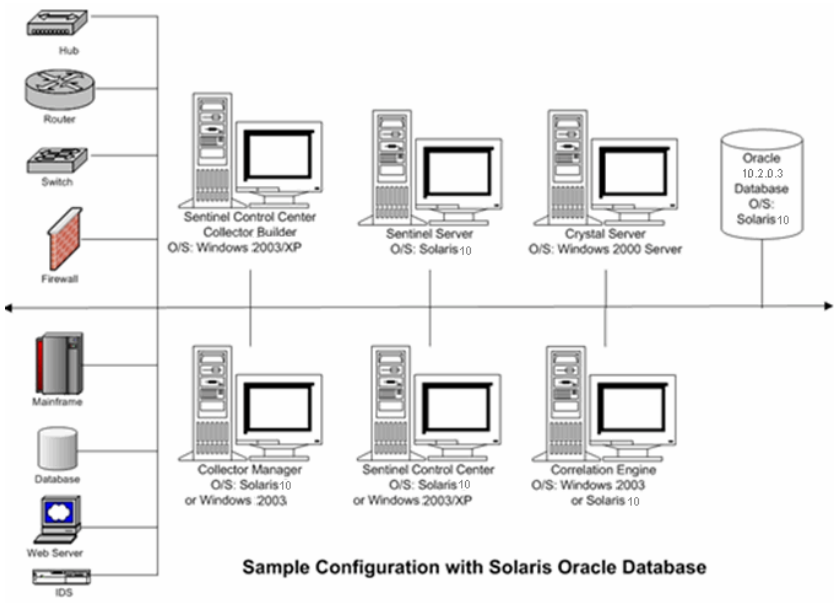
The following are some typical configurations for Sentinel. On Linux

Figure 3-1 *Sentinel Configuration on Linux*



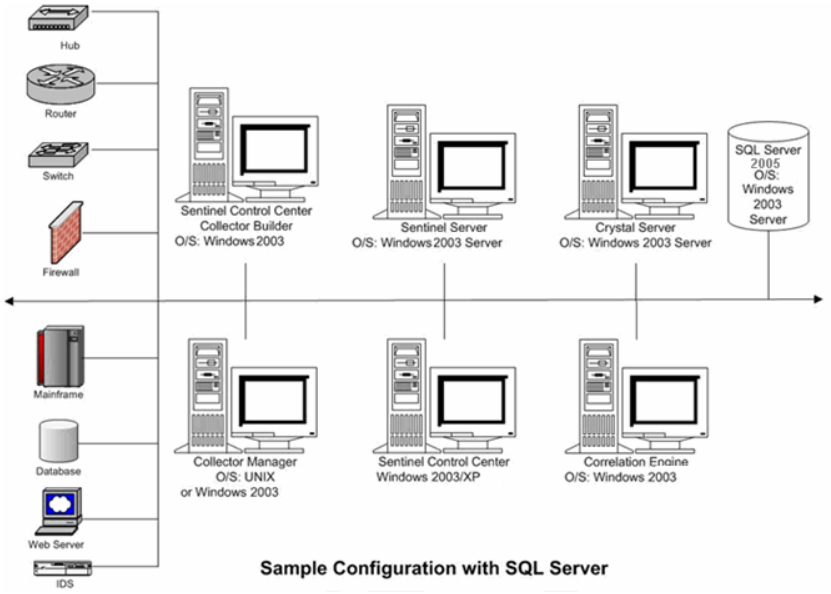
3.2.1 On Solaris

Figure 3-2 *Sentinel Configuration on Solaris*



3.2.2 On Windows

Figure 3-3 *Sentinel Configuration on Windows*



3.3 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 Chapter 2, "System Requirements," on page 19.

- 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 10, ensure that SLES is using the ext3 file system.
- If installing the Collector Manager on a 64-bit machine, ensure that 32-bit libraries are available. The 32-bit libraries are required when running a Collector that is written in the proprietary collector language (which includes almost all Collectors written before June 2008) as well as when running certain Connectors (such as the LEA Connector). JavaScript-based Collectors and the remainder of Sentinel are 64-bit enabled. Verifying that these libraries are available is particularly important on Linux platforms, which may not include them by default.
- You must install SUNWxcu4 package on your Solaris machine before installing Sentinel 6.1.
- Ensure that a Sentinel-certified database is installed. (If using Oracle, Enterprise Edition with partitioning is required in order for data archive to work. For more information on certified versions, see Chapter 2, "System Requirements," on page 19.
- Get the Sentinel, Crystal Reports Server, and Crystal Reports Developer serial numbers and license keys from the Novell Customer Center (https://secure-www.novell.com/center/regadmin). 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”.

Sentinel installations using the full installer should always 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 Chapter 10, “Uninstalling Sentinel,” on page 139. For information on uninstalling previous versions of Sentinel, see the relevant Installation guides on the Novell Documentation Website (http://www.novell.com/documentation/).

NOTE: Instructions for upgrading from a previous version of Sentinel 6 to Sentinel 6.1 are included with the patch installer.

3.3.1 Providing Power User privileges to “Domain Users”

IMPORTANT: If you install Sentinel as a domain user, where the user is not a part of administrator group in the active directory machine and the local machine, then the domain user should be a power user to start the Sentinel Services.

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.

3.3.2 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 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 by the database installer. If you run the Sentinel installer on another machine, the database instance must be manually created and the compatible JDBC client must be manually installed on the machine with the installer. Although newer Oracle drivers 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 Section 3.8.7, "Modifying Oracle dbstart and dbshut scripts," on page 57.

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 Section B.2, "Manual Oracle Instance Creation (Optional)," on page 153. 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 Section 3.6, "Custom Installation," on page 43.

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>
```

- After installing the Sentinel Database on Oracle, the database will contain the following users:

Table 3-1 *Database users*

USER	DESCRIPTION	SERVER ROLES	NEED FOR ROLE
Esecdba	Database schema owner. DBA privilege is not granted to Sentinel Database User because of security concerns, so to use Enterprise Manager, you must create a user with DBA privileges	Serveradmin and Sysadmin	esecdba needs serveradmin and sysadmin because Sentinel Data Manager need the privilege to use a build-in SQL Server stored procedure to write to the file system.
Esecapp	Database application user. This is the application user used to connect to the database.	securityadmin	esecapp needs securityadmin role because Sentinel runs under esecapp and it need this role to create new users in Sentinel and the database.
Esecadm	Database user that is the Sentinel Administrator. This is not the same user account as the Sentinel Administrator operating system user	Not required	
Esecrpt	Database report user	Not required	
SYS	SYS database user	Not required	
SYSTEM	SYSTEM database user	Not required	

Windows 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 Section 3.3.1, "Providing Power User privileges to "Domain Users"," on page 32 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

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

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

- **esecdba:** Database schema owner. DBA privilege is not granted to Sentinel Database User because of security concerns, so to use Enterprise Manager, you must create a user with DBA privileges.
- **esecapp:** Database application user. This is the application user used to connect to the database.

- **esecadm:** Database user that is the Sentinel Administrator. This is not the same user account as the Sentinel Administrator operating system user.
- **esecrpt:** Database report user
- **sa:** system administrator database user

3.3.3 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 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.

3.3.4 Sentinel Server Installation Prerequisites

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

3.3.5 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 Reports Server 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 Reports Server software. For more information about installation procedures, see Chapter 4, “Advisor Configuration,” on page 59.

3.4 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 and RHEL 4:
  - Creating a Group and User Account for Oracle
  - Setting the environment variables
  - Verifying Solaris Layout

- Installing Oracle
- Patching to Oracle (if required)

3.4.1 Setting Kernel Values

WARNING: 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.

   To determine your current setting for a particular kernel parameter, execute the command:

   `sysctl <kernel_parameter>`

   For example, to check the current value of the kernel parameter "kernel.sem", execute the command: `sysctl kernel.sem`

   On SUSE LINUX 10 SP2 only:

   ```
   # Oracle requires MLOCK privilege for hugetlb memory.
   vm.disable_cap_mlock=1
   ```

   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 10:

For Oracle 10g:

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

1. By default, Oracle instances are run as the oracle user of the dba group. A project with the `group.dba` name is created to serve as the default project for the oracle user. Run the id command to verify the default project for the oracle user.

   ```
   # su - oracle
   $ id -p
   uid=100(oracle) gid=100(dba) projid=100(group.dba)
   $ exit
   ```

2. To set the maximum shared memory size to 2 GB, run the projmod command

   ```
   # projmod -sK "project.max-shm-memory=(privileged,2G,deny)" group.dba
   ```

   Alternatively, add the project.max - `shm-memory=(privileged,2147483648,deny)` resource control to the last field of the project entries for the oracle project.

3. After these steps are complete, the /etc/project file should contain the following:

   ```
   # cat /etc/project
   ```

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.

3.4.2 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) for csh shell:

     ```
     useradd -g dba -d /export/home/oracle -m -s /bin/csh oracle
     ```
   - Add the oracle user (as root) for bash shell:

     ```
     useradd -g dba -d /export/home/oracle -m -s /bin/bash oracle
     ```

3.4.3 Setting Environment Variables for Oracle (Solaris Only)

To set environment variables:

1. Login as root.
2. To set the necessary environment variables for Oracle in csh shell, 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
   ```
3. To set the necessary environment variables for Oracle in bash shell, it is suggested to add the following information to the `.profile` file in $ORACLE_HOME directory:

   ```
   setenv ORACLE_HOME /opt/oracle
   setenv ORACLE_SID ESEC
   setenv LD_LIBRARY_PATH ${ORACLE_HOME}/lib
   setenv DISPLAY :0.0
   set path=(/bin /bin/java /usr/bin /usr/sbin ${ORACLE_HOME}/bin /usr/ucb/etc.)
   if ( $?prompt ) then
   set history=32
   endif
   ```

3.4.4 Install Oracle

To perform Oracle installation, see Appendix B, “Oracle Setup,” on page 149. This section describes installation settings recommended for Sentinel operations. It also describes the procedures for creating the Oracle instance. (Novell recommends creating the instance using the Sentinel installer but provides instructions in case corporate policy requires that the DBA create the instance manually.)

3.5 Simple Installation

The Simple Installation option is an all-in-one installation option that installs Sentinel Services, Collector Manager, and Sentinel Applications with the database on the same machine. This installation 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	Italian
French	Portuguese (Brazil)
German	Spanish
Simplified Chinese	Japanese
Traditional Chinese	

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 6.1on 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 Section 3.8.2, “Sentinel Database,” on page 55.
- 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.

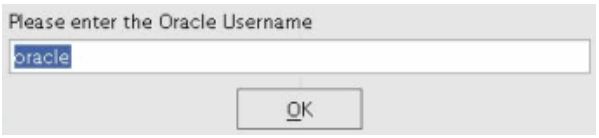
  NOTE: Usernames and passwords that were provided for Advisor prior to Sentinel 6.0 SP2 are no longer valid. You must use the Novell eLogin and password associated with the Advisor license. Some organizations have more than one individual with a Novell eLogin; the one used for Advisor downloads must be the one associated with the Advisor purchase.

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.

Figure 3-4 *Specify Oracle Username field*



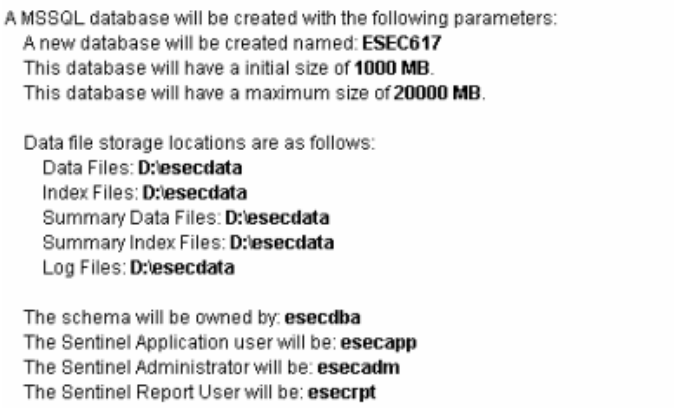
Provide Database Name

- 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.

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.).

3.6 Custom Installation

The Custom Installation option allows for a fully distributed installation, with more control over memory and other installation settings. The Custom Installation option can 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 Control Center
  - Sentinel Data Manager
  - Sentinel Solution Designer
- 3rd Party Integration
  - HP OpenView Service Desk

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.

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

5 After reading the Welcome screen, click Next.

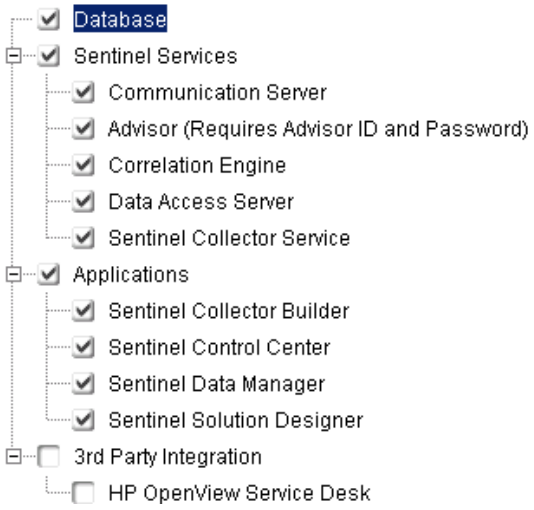
6 Read and accept End User License Agreement. Click Next.

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:

Component	Description
Database	Installs Sentinel database objects (tables, views, stored procedures and so on) into a database instance. Optionally creates the database instance first.
Communication Server	Installs message bus (iSCALE) and DAS Proxy
Correlation Engine	Installs correlation engine.

Component	Description
Advisor	Installs components related to the Advisor data subscription service. Requires an Advisor license and must reside on the same machine as DAS.
Data Access Server (DAS)	Installs components that communicate with the Sentinel database. Requires a Sentinel license key and serial number. (Required if installing Advisor.)
Sentinel Collector Service	Installs the Collector Manager, which handles connections to event sources, data parsing, mapping, and so on.
Sentinel Control Center	Installs the main console for security or compliance analysts.
Sentinel Data Manager (SDM)	Installs SDM, which is used for manual database management activities.
Solution Designer	Installs Solution Designer
HP OpenView Service Desk	Installs integration with HP OpenView Service Desk. Requires a license.

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 Section 3.6.1, “Console Installation on Linux/Solaris,” on page 52.

NOTE: In case of MS SQL (MS SQL 2000/2005/2008) databases, maximum number of online partitions allowed is 255. So you must schedule the offline delete/archive operations in such a way that the online partitions should not exceed 255.

![Bug #488374, Last updated: 05/06/09]

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.

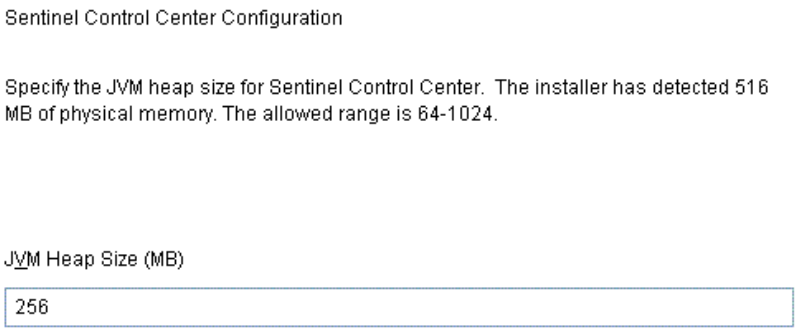
- OS Sentinel Administrator username – Default is esecadm
- OS Sentinel Administrator user home directory – Default is “/export/home”. If esecadm is the username, then the user’s home directory will be /export/home/esecadm.

NOTE: To meet stringent security configurations required by Common Criteria Certification.

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.

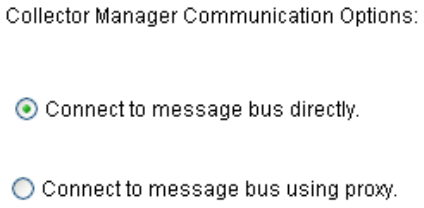
- **JVM heap size (MB):** By default this is 256.and a maximum can be 1024 MB.



13 If Collector Manager is selected to be installed and Data Access Server (DAS) is not, 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 Chapter 7, "Communication Layer (iSCALE)," on page 89.

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 26 on page 52.



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 on which the communication server is listening. Components connecting directly to the communication server will use this port.

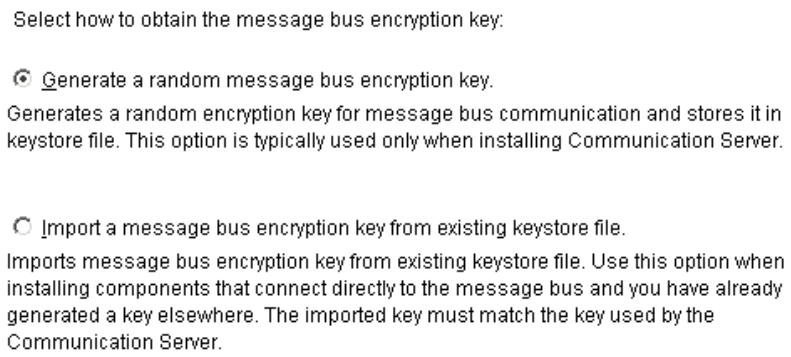
- **Sentinel Control Center Proxy Port:** the port on which the SSL proxy server (DAS Proxy) is listening to accept username and password based authenticated connections. Because Sentinel Control Center prompts for a username and password, it uses this port to connect to Sentinel Server.
- **Collector Manager Certificate Authentication Proxy Port:** the port on which 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.

NOTE: The port numbers must be identical on every machine in the Sentinel system to enable communications. 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.



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 Select the target Database Server platform. Click Next. 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.

Click Next.

17 If you chose to install the database, configure database for installation:

On Windows:

- Select Microsoft SQL Server 2005 or Microsoft SQL Server 2008 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 Section 3.3.2, "Sentinel Database Installation Prerequisites," on page 32.

18 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.

19 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.

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

21 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 only be available if there is sufficient memory on the machine.

22 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.

23 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.

24 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 AdvisorService section of the `advisor_client.xml` file in the $ESEC_HOME/config directory. For more information, see "Advisor Tab" in *Sentinel 6.1 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 you are prompted for further information.

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

26 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.

27 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.

3.6.1 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:

```
Sentinel 6.1 - InstallShield Wizard

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

   Sentinel 6.1

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

     1.  [ ] Database
     2. +[x] Sentinel Services
     3. +[x] Applications
     4. +[ ] 3rd Party Integration
```

```
   Other options:

     0. Continue installing

   Enter command [0] 1

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

   Sentinel 6.1

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

     1.  [x] Database
     2. +[x] Sentinel Services
     3. +[x] Applications
     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 6.1" you would like to install:

   Sentinel 6.1
    - Sentinel Services

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

        1.  [ ] Communication Server
        2.  [ ] Advisor (Requires Advisor ID and Password)
        3.  [x] Correlation Engine
        4.  [x] Data Access Server
        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 6.1" you would like to install:

   Sentinel 6.1
    - Sentinel Services

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

        1.  [x] Communication Server
        2.  [ ] Advisor (Requires Advisor ID and Password)
        3.  [x] Correlation Engine
        4.  [x] Data Access Server
```

```
        5.  [x] Sentinel Collector Service

      Other options:

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

      Enter command [0] 2

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

   Sentinel 6.1
    - Sentinel Services

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

        1.  [x] Communication Server
        2.  [x] Advisor (Requires Advisor ID and Password)
        3.  [x] Correlation Engine
        4.  [x] Data Access Server
        5.  [x] Sentinel Collector Service

       Other options:

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

3.7 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 Section 3.3.1, “Providing Power User privileges to “Domain Users”,” on page 32 to provide power user privileges.
3. Install Sentinel 6.0 as an administrator user. See Section 3.6, “Custom Installation,” on page 43 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.

3.8 Post-Installation Configuration

3.8.1 Configuring SMTP Integrator to Send Sentinel Notifications

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

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

- When a Correlation rule that is deployed with a Send Email action is triggered. The Send Email action referred here is the action indicated by the gear icon, which is only valid for correlation (as opposed to the JavaScript `SendEmail` Action, which is indicated by the JS JavaScript icon).
- Workflow includes a Mail Step or Activity that is configured to send email.
- User opens an incident and selects to execute an Activity that is configured to send email.
- User right-clicks an event and selects Email.
- User opens an incident and selects Email Incident.
- Advisor download sends a notification.

No configuration is necessary to the `SendEmail` Action, but the SMTP Integrator must be configured with valid connection information before it will work..

3.8.2 Sentinel Database

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

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

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

To enable writing to archive directory by Oracle:

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]
5. Save the file and exit.

3.8.3 Collector Service

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

3.8.4 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.

3.8.5 Starting Collector Manager Service

To start Collector Manager service:

1. Start Sentinel 6.1
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

4. Start Sentinel 6.1
5. Click Event Source Management > Live View.
6. In Event Source Management (Live View) window, right-click the Collector Manager you must start; select Start.

3.8.6 Managing Time

Novell strongly recommends that all Sentinel components, particularly the Correlation Engine and Collector Manager Machines, be connected to an NTP (Network Time Protocol) Server or other type of Time Server. If the system time across machines is not synchronized, the Sentinel

Correlation Engine and Active Views will not work properly. The events from the Collector Managers will not be considered to be real-time and will therefore be sent directly to the Sentinel database, bypassing the Sentinel Control Centers and Correlation Engines.

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

3.8.7 Modifying Oracle dbstart and dbshut scripts

Sentinel cannot start the Oracle 10 database because of errors in the Oracle `dbstart` and `dbshut` scripts. For details on the script errors, see https://metalink.oracle.com (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, you need to modify the `dbstart` and `dbshut` scripts for Sentinel to start an 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. Ensure "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.
6. To modify dbshut script on Solaris 10:
7. Open dbshut script for edit from the path $ORACLE_HOME/bin/dbshut.
8. Ensure "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.
9. 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. Ensure "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.
4. To modify dbshut script on RedHat Linux ES4:

5 Open `dbshut` script for edit from the path $ORACLE_HOME/bin/dbshut.

6 Ensure “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.

7 Click Save and exit.

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

NOTE: DAS and the Sentinel database are typically located in a secure portion of your network. However, you may want to add another security layer to protect the data being transmitted from DAS to the database. For Oracle, the DBA can use the "Advanced Security" feature. For SQL Server, the DBA can enable the SSL functionality in the jTDS driver. For more information, see http://jtds.sourceforge.net/faq.html and search for "ssl".

Advisor Configuration

4

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.

4.1 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)

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

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 PC Protection	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

Supported Systems	Device Type	RV31 Value
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

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

- In the IDS collector, RV39 (MSSPCustomerName) must be set to the MSSP Customer Name.
- 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

Collectors provided by Novell set these variables by default.

4.2 About Installing Advisor

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

To load the initial data, Novell strongly recommends using the Advisor Core Data ISO, available through the Novell Customer Care portal to customers who have purchased the Advisor data subscription. This installer will load approximately 10GB of data that would otherwise have to be transmitted over the network using the regular update service.

By default, the scripts that initiate the automatic downloads are disabled. They should be enabled after the Advisor Core Data has been loaded.

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

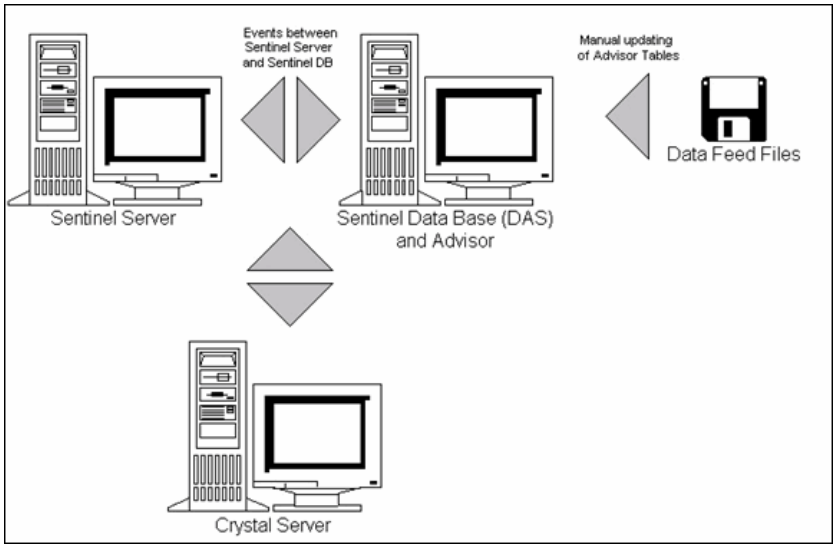
NOTE: The Advisor data feed for Sentinel 6.0 SP2 and above has been augmented with additional signatures. The changes in SP2 affect both the storage space required and the installation procedures.

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

4.2.1 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/ (https://advisor.novell.com/advisordata/)

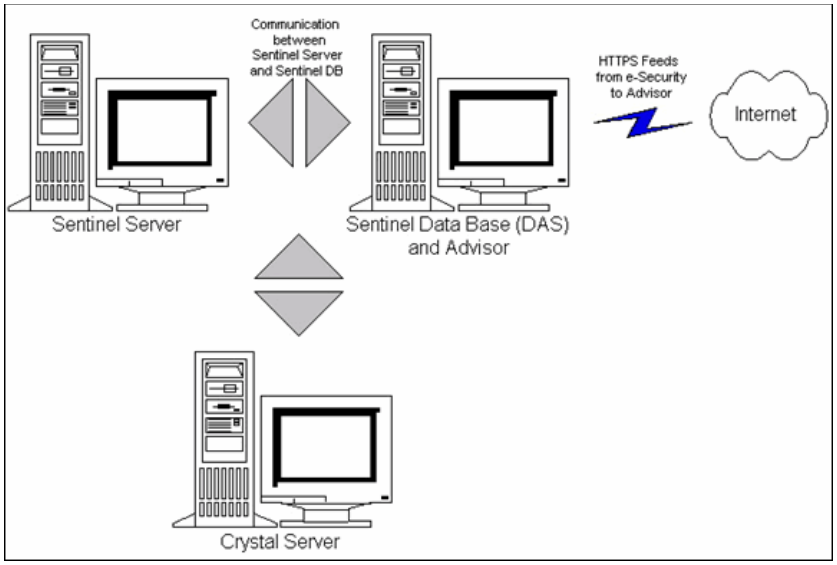
- Sentinel 6.0 SP2 and above:

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

4.2.2 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, seeChapter 3, “Installing Sentinel 6.1,” on page 29.

Figure 4-2 *Direct Internet Download*



4.3 Installing Advisor

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

NOTE: Advisor configuration 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/sentinel61 (http://www.novell.com/documentation/sentinel61).

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.

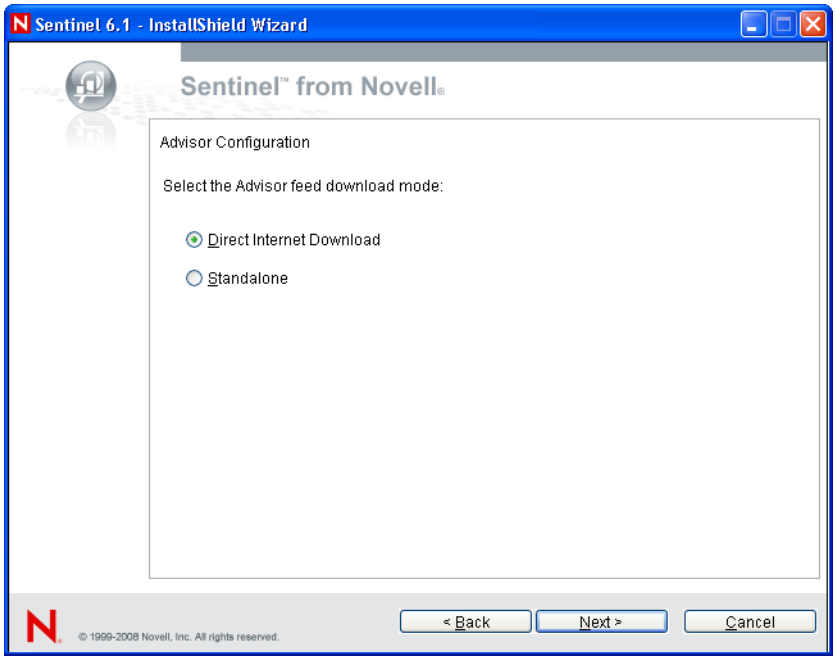
7 Accept the default install directory or click Browse to specify your installation location. Click Next.

8 Select Custom. Click Next.

9 In this window, provide the configuration information and click Next.

- Serial Number
- License Key
- 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 Section 3.8.2, "Sentinel Database," on page 55.

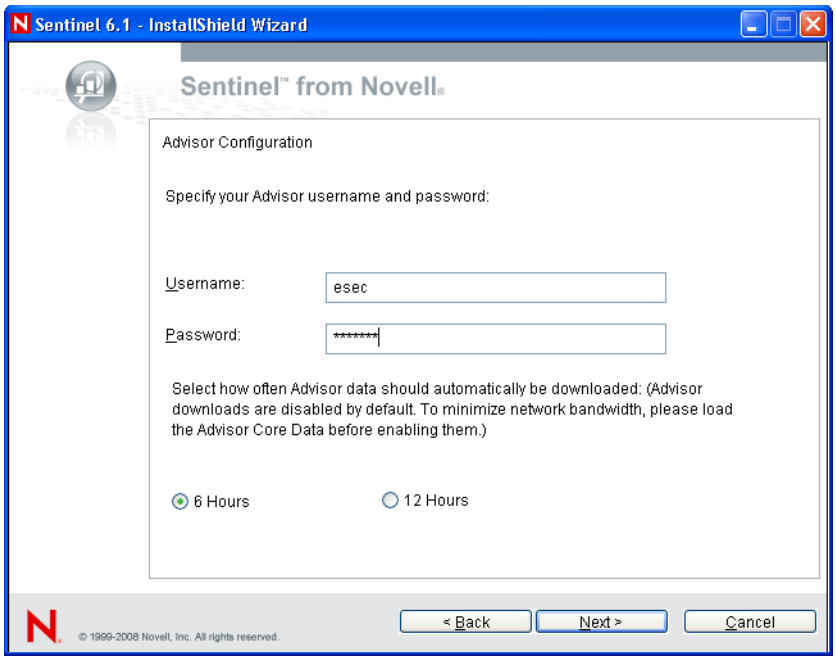
10 Select from the two options available: Direct Internet Download or Standalone.



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. This login may or may not be the same as the Novell eLogin associated with the purchase of Sentinel. For more information, see "Advisor Tab " section in *Sentinel User Guide*.*Sentinel 6.1 User Guide*



12 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 later, the login and password must be the Novell login and password that is associated with the entitlement to Advisor. A common source of error is using the wrong Novell login and password, one which may be a valid Novell login but is not associated with the entitlement or the Advisor license.

13 Click Install.

14 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.

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 ” section in *Sentinel 6.1 User Guide*.

4.3.1 Loading Data

Although the initial Advisor data load can be performed using the scheduled service (Direct Internet Download) or manually using the Standalone option, this approach is not recommended due to network load. Therefore, the `advisor.sh` and `advisor.bat` scripts are initially disabled by default. They should be enabled after loading the data using the Sentinel 6 Exploit Detection and Advisor Core Data (Advisor Core Data) disk contains a snapshot of the Advisor data. Loading this data significantly decreases the amount of time and network bandwidth required to make the database current.

The Advisor Core Data is available through the Novell Customer Care Portal to customers who have purchased an annual subscription to Advisor. The ISO is less than 900MB but loads approximately 10GB of data into the Advisor tables.

The initial data load may take up to one day, 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. 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`
4. 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.
5. Specify the time to pause in seconds between processing each file. The default is 0 seconds, but this can be increased if database load is high to introduce a pause between processing data files.
6. 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
   ```

7. The Advisor script starts and the bulk data is fed into the appropriate table. The snapshot of the data is stored in the database.
8. 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
   ```

9. On completion of bulk feed, the system displays successful completion message.
10. Enable the incremental Advisor data updates.

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

4.3.2 Enabling Advisor Updates

To prevent excessive network load, the incremental Advisor downloads are disabled by default. They should be enabled after the Advisor Core Data is loaded.

To enable Advisor downloads:

1. Open the `advisor.sh` or `advisor.bat` file for editing.

   On Linux: $ESEC_HOME/bin/advisor.sh

   On Windows: %ESEC_HOME%\bin\advisor.bat

2. **For Linux:**

   Place a pound sign (#) in front of the exit command at the beginning of the file to comment it out.

   # exit

   For Windows:

   Type rem in front of the exit command at the beginning of the file to comment it out.

   rem exit

3. Save the file.

The next scheduled or manual download should now load data as expected.

4.3.3 Connecting to Advisor Server through a 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 `container.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%\sentinel\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.

4.4 Advisor Reports

Crystal Reports Server™ is the reporting tool that integrates with Sentinel.

To run Crystal reports on Advisor:

- Install and configure Crystal Server. For more information on Crystal Reports Server installation, see Chapter 8, “Crystal Reports for Windows,” on page 95 andChapter 9, “Crystal Reports for Linux,” on page 123.
- Publish Advisor Crystal Reports to the Crystal Server.

4.4.1 Advisor Report Configuration

To run Advisor reports, you must follow the Crystal Reports Server configuration steps for either Windows or Linux and configure the Advisor URL for reports. For more information on importing report templates and configuring the Sentinel Control Center to show the Advisor reports, see Chapter 8, “Crystal Reports for Windows,” on page 95 and Chapter 9, “Crystal Reports for Linux,” on page 123.

4.5 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. If these updates are not scheduled using Direct Internet Download, they must be performed manually.
- Changing the password Advisor uses for automatic data updates, if needed
- 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 6.1 User Guide*.

Testing the Installation

5

5.1 Testing the Installation

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

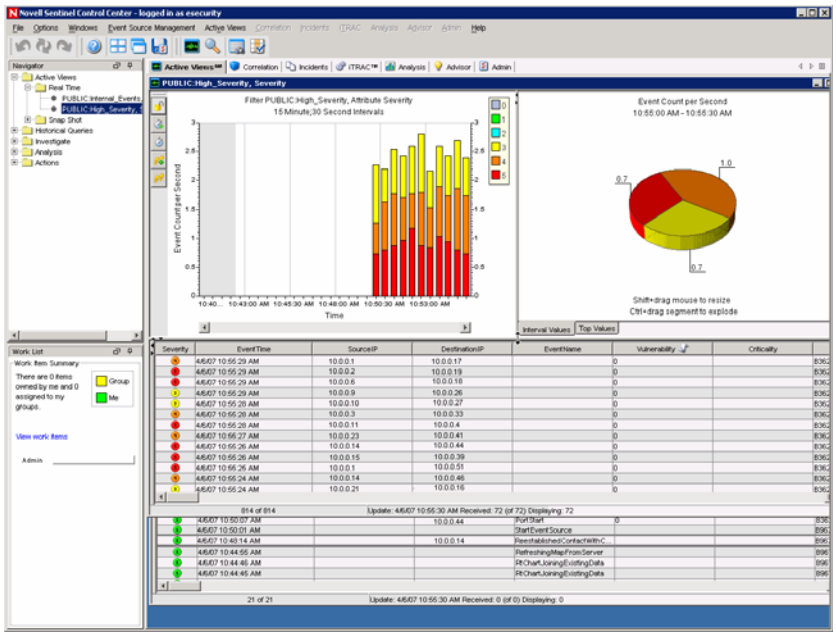
At a basic level, these tests allow you to confirm the following:

- 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”.



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.

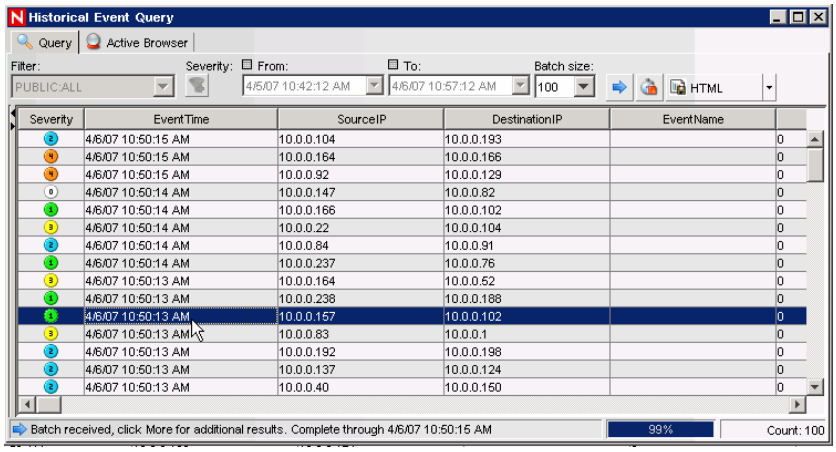
7 Click Event Query button in the toolbar. The Historical Event Query window displays.

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.

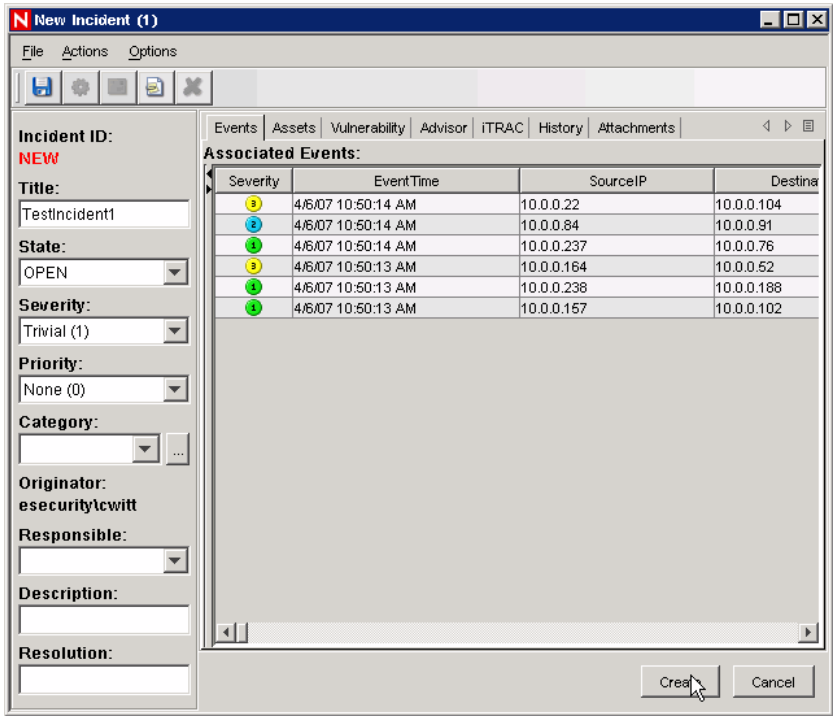
10 Select a batch size from the Batch size drop down.

11 Click the Magnifying Glass icon to run the query.



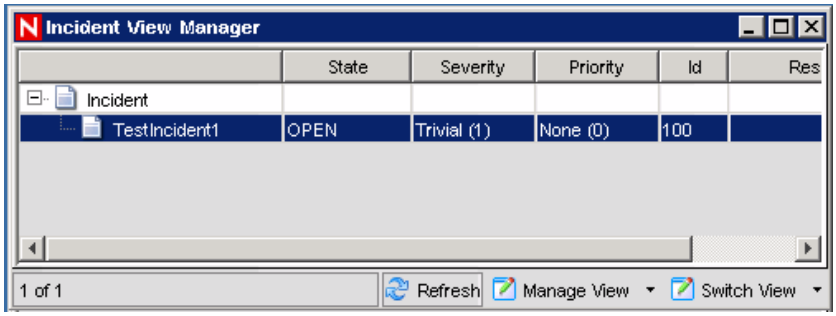
12 Hold down the Ctrl or Shift key and select multiple events from the Historical Event Query window.

13 Right-click and select Create Incident.

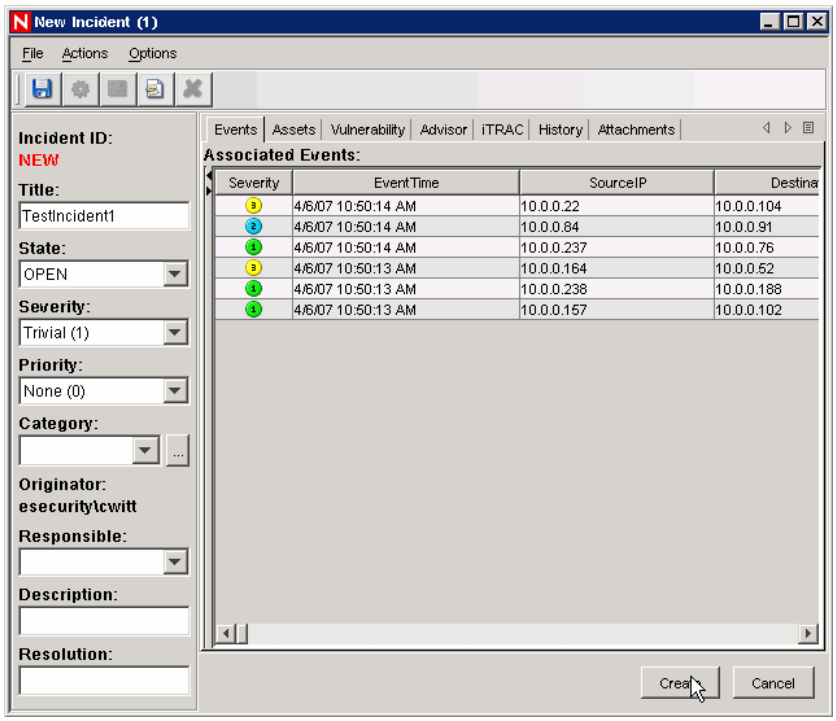


14 Name the incident TestIncident1 and click Create. A success notification displays. Click OK.

15 Go to the Incident Tab. Incident View Manager displays. In the Incident View Manager you will see the incident you just created.



16 Double-click the incident to display.



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)

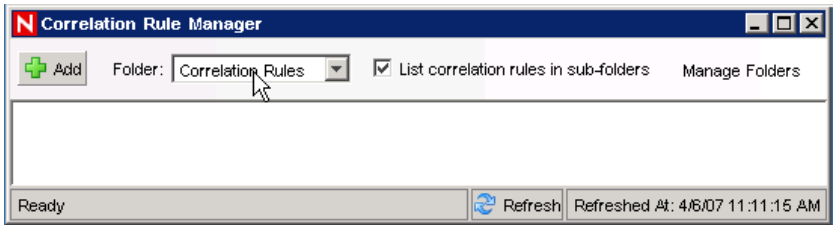
21 Click Begin Searching icon.

22 To view the next batch of events, click More.

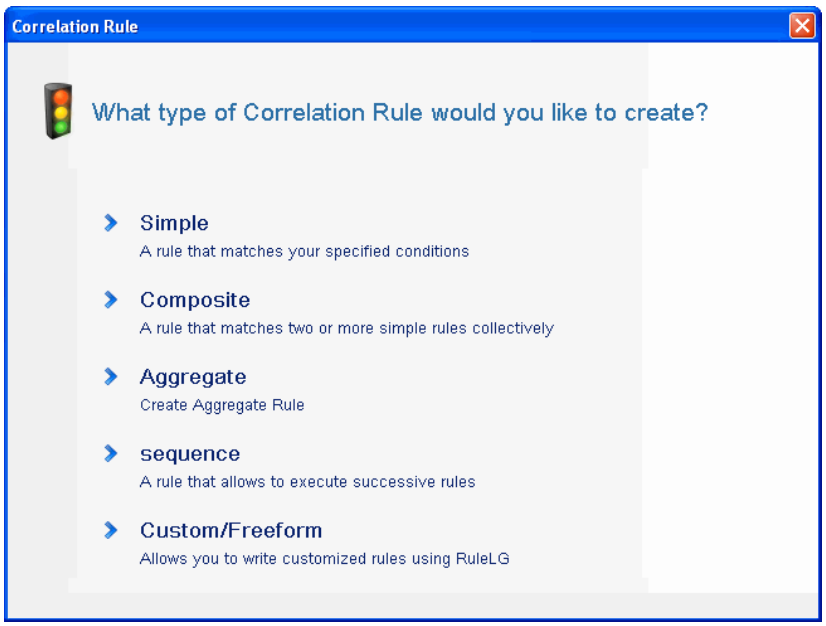
23 Rearrange the columns by dragging and dropping them and arrange the sort order by clicking in the column heading.

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

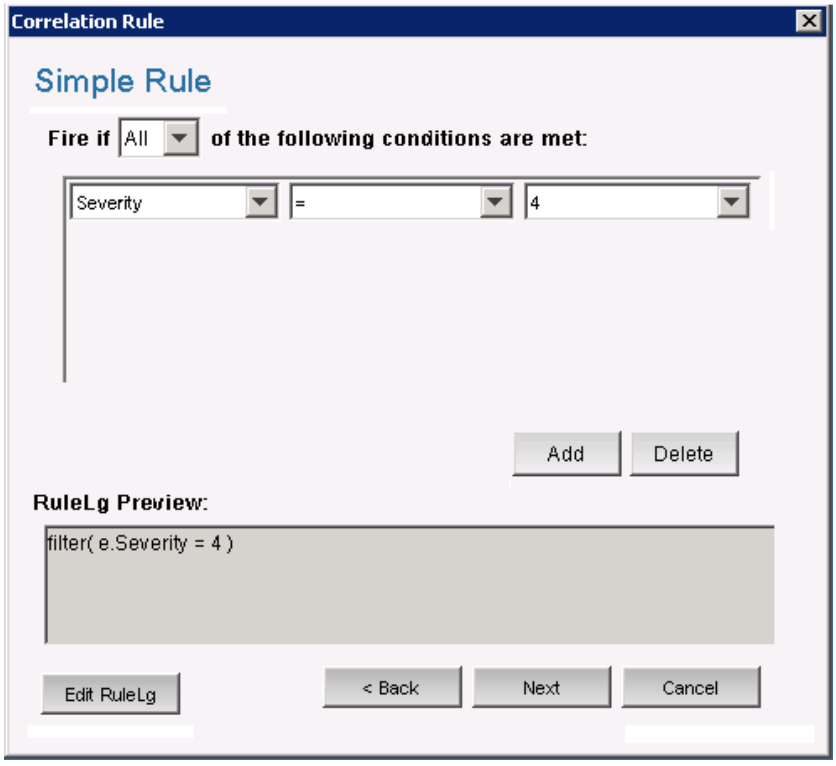
25 Go to Correlation tab. The Correlation Rule Manager displays.



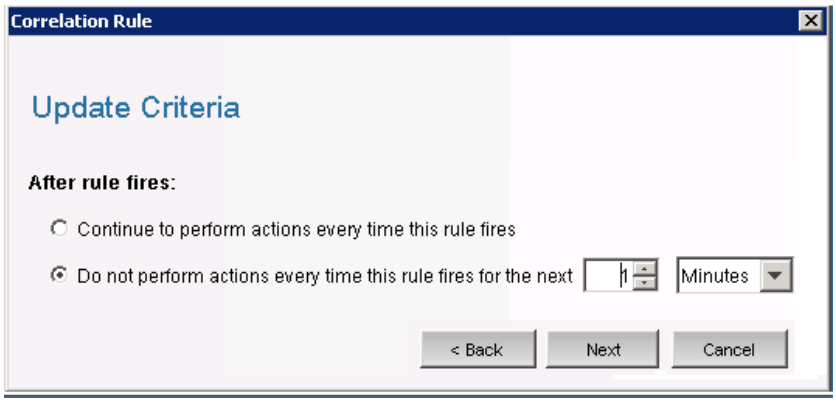
26 Click Add. The Correlation Rule wizard displays.



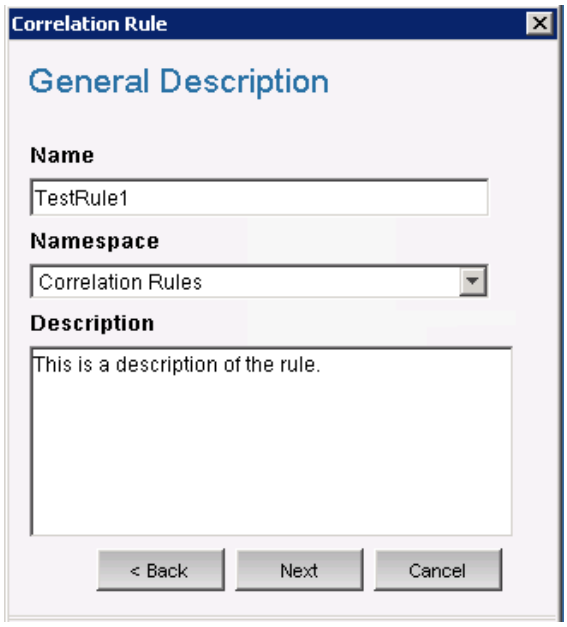
27 Click Simple. Simple Rule window displays.



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



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.

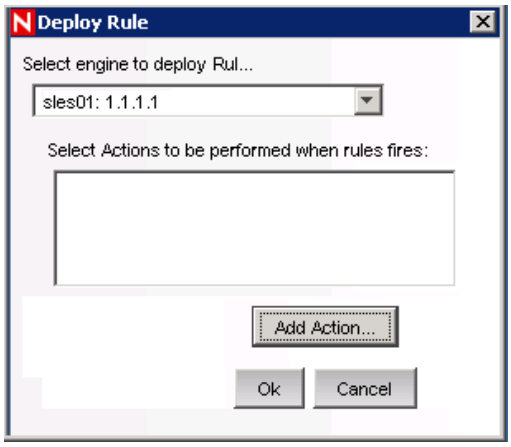


30 Name the rule as “Correlation Rule”, provide description, and click Next.

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

32 Open the Correlation Rule Manager window.

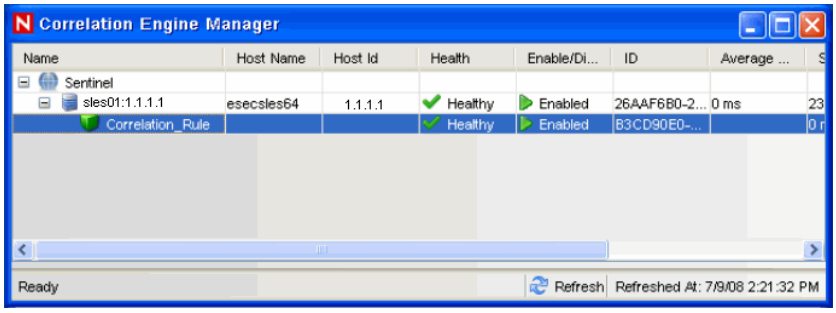
33 Highlight a rule and click Deploy rules link. The Deploy Rule window displays.



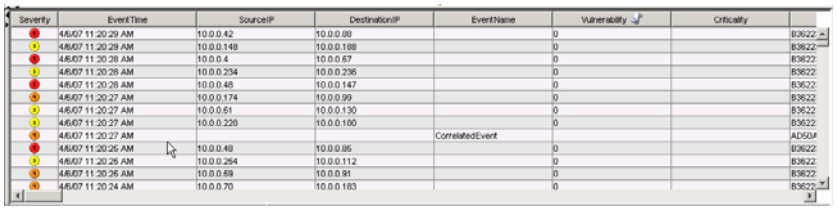
34 In the Deploy rule window, select the Engine to deploy the rule from the drop-down list.

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.



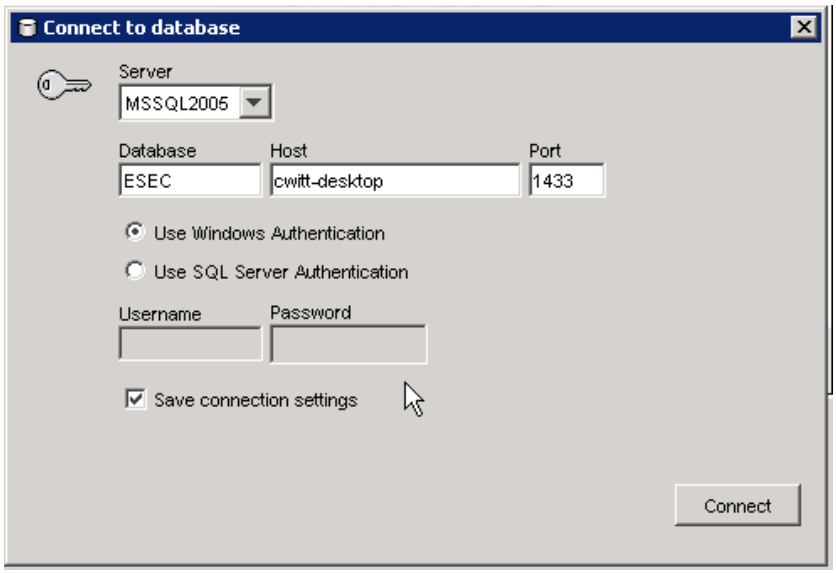
37 Go to Active Views tab and verify that the Correlated Event has generated.



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).



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.

5.2 Testing the Advisor Installation

Follow the instructions given below to verify the Advisor installation.

1 Upload the Advisor data to the Sentinel database.

- For Windows: Go to the location `%ESEC_HOME%\bin` and run `advisor.bat` to download the Advisor data from the Advisor server and upload it to the Sentinel database.
- For non-Windows: Go to the location `$ESEC_HOME/bin` and run `advisor.sh` to download the Advisor data from the Advisor server and upload it to the Sentinel database.

2 Configure a Vulnerability Collector (`Tenable_Nessus_3_LOG_600.zip`) with File Connector and sample log file (ES).

NOTE: The sample log data will be shipped along with the Collectors. The Collectors can be downloaded from the Sentinel 6 Content Web site (http://support.novell.com/products/sentinel/secure/sentinel6.html).

---

3 Start the Event Source.

4 Make sure that the exploitDetection.csv file is created with attack data in the following location:

- For Windows: `%ESEC_HOME%\data\map_data`
- For non-Windows: `$ESEC_HOME/data/map_data`

5 Configure an IDS Collector (`Sourcefire_Snort_2_LOG_600.zip`) with File Connector and sample log file (ES).

NOTE: Ensure that the *Connection Mode* of the Event Source is set to Syslog Format and the *MSSP Customer Name* of the Collector is set to `default`.

6 Start the Event Source so that events with Vulnerability meta-tag set to 1 will be generated.

NOTE: Ensure that the meta-tags, `DestinationIP`, `DeviceName`, and `DeviceAttackName` populated in the Active View matches with those in exploitDetection.csv.

7 In the Active View, right-click on one of the events where Vulnerability meta-tag is set to 1 and navigate to *Analyze* > *Advisor Data*.

This provides you the "Advisor Attack Result" which contains *Advisor Summary* and *Advisor Report*.

5.3 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).

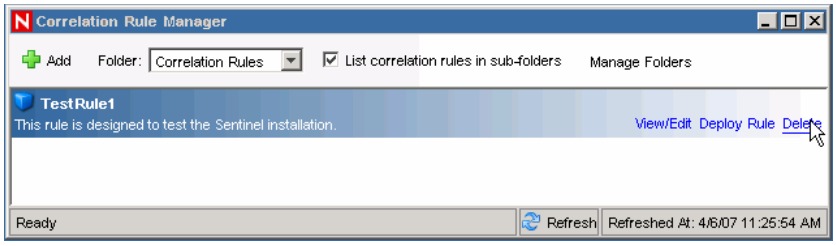
2 Go to the Correlation tab.

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.



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.

5.4 Getting Started

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

Adding Sentinel Components

6

6.1 Adding Sentinel Components to an Existing Installation

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

The Sentinel installer makes it simple to perform this kind of installation. First make sure you’ve satisfied the prerequisites of the additional component being installed as specified in the Chapter 3, “Installing Sentinel 6.1,” on page 29 The requirements on the machine are likely to increase when installing additional components. Then run the Sentinel installer on the target machine just as if you were installing on a “clean” machine. When running in add component mode, the installer slightly changes its behavior in the following ways:

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

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

6.2 Installing Additional Load Balancing Nodes

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

To do this, simply run the installer on the new machine as described in theChapter 3, “Installing Sentinel 6.1,” on page 29 As you step through the installer, select only the components you want to add additional load balancing nodes for. The following components can be load balanced:

- Correlation Engine
- Collector Manager
- DAS_Binary process

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

6.2.1 Multiple DAS_Binary Processes

Although not true load-balancing, it is possible to configure multiple DAS_Binary instances in a Sentinel system to improve performance. 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 Novell Documentation site (http://www.novell.com/documentation/sentinel61).

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

Distibuting Multiple DAS_binary Instances Across Different Machines

IMPORTANT: Before you proceed, ensure that you have installed the Sentinel Server includng the DAS. This installation is referred to as the Sentinel Server or the primary DAS_Binary.

1. Use the Sentinel installer to install the DAS component on each of the other machines that you want to 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 the DAS_Binary, including the primary DAS_Binary, make the following modifications:
   - **2a** Login as `esecadm` (on UNIX) or an `Administrator` (on Windows) to any one of the machines that run an instances of the DAS_Binary process and locate the `configuration.xml` file in the $ESEC_HOME/config (%ESEC_HOME%\config on Windows) directory.
   - **2b** Add the following information to services section of the `configuration.xml` file:

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

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

     ```
     min_instances="0"
     ```

for the following process entries:

- DAS_RT
- DAS_Aggregation
- DAS_Query
- DAS_ITRAC

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

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

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

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

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

NOTE: The `das_binary.xml` file will later be copied to other DAS_Binary installations.

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

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

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

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

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

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

4f Save the `das_binary.xml` file.

5 Copy the modified `das_binary.xml` file to all machines that run a DAS_Binary process, including the primary DAS_Binary.

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

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

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

```
<obj-component id="EventStoreService">
<class>esecurity.ccs.comp.event.EventStoreService</class>
<property name="handler">esecurity.event.create</property>
<property name="waitBlocked">true</property>
<property name="maxThreads">6</property>
<property name="minThreads">6</property>
<property name="maxThreadsQueued">10</property>
<property name="queueSize">1000000</property>
<obj-component-ref>
<name>ThreadPool</name>
<ref-id>EventStoreThreadPool</ref-id>
</obj-component-ref>
<obj-component-ref>
<name>DispatchManager</name>
<ref-id>EventStoreDispatchManager</ref-id>
</obj-component-ref>
<obj-component id="Persistor">
<class>esecurity.ccs.comp.event.jdbc.JDBCEventStore</class>
<property name="insert.batchsize">600</property>
<property
name="insert.strategy">esecurity.ccs.comp.event.jdbc.JDBCLoadStrategy</
property>
<property name="insert.oci.workerCount">5</property>
<property name="insert.oci.queueWaitTime">1</property>
<property name="insert.oci.highWatermark">10000000</property>
<property name="insert.oci.lowWatermark">9000000</property>
<property name="insert.oci.optimizationFlag">on</property>
<property name="insert.pmaxWarningTime">300</property>
<property name="insert.pminWarningTime">300</property>
```

```
</obj-component>
<obj-component-ref>
<name>EventRedirect</name>
<ref-id>EventFileRedirectService</ref-id>
</obj-component-ref>
</obj-component>
```

6 Delete the unneeded durable subscription.

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

6a Open the Sonic Management Console.

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

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

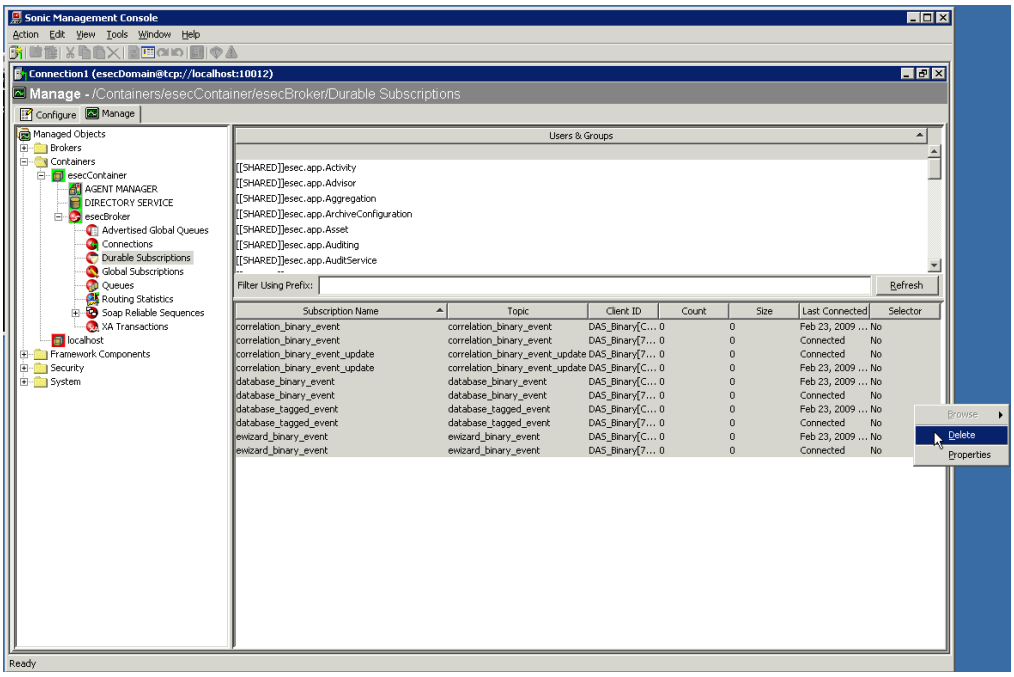
```
$ESEC_HOME/3rdparty/SonicMQ/MQ7.0/bin/startmc.sh
```

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

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

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

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



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

6f Select all durable subscriptions, right click, and then select *Delete*.

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

UNIX: Run the following command:

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

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

Configuring Multiple DAS_binary Instances on the Same Machine

1 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 Dsrv_name:** Change to match the DAS_Binary service names defined in step 4, such as DAS_Binary2.
- **DAS_Binary communication service name:** Insert the following text into the process entry's image attribute at the location shown in bold in the process entry example below. For each DAS_Binary process entry, replace the DAS_Binary part of the text below with the associated service name, such as DAS_Binary2.

  ```
  -Desecurity.communication.service=DAS_Binary
  ```

- **`das_binary.xml` file name:** Use any unique name(s), such as `das_binary_2.xml`. These names are used in a later step.
- **das_binary_log_prop file name:** Use any unique name(s), such as `das_binary_log_2.prop`. These names are used in a later step.
- **das_binary.cache directory name:** Use any unique name(s), such as `das_binary2.cache`. Each instance of DAS_Binary must use a different `das_binary.cache` directory.
- **DAS_Binary process name:** Change the value of the process entry's name attribute to match the DAS_Binary service names defined in step 4, such as DAS_Binary2.

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

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

6 Save the `configuration.xml` file.

7 Locate the `das_binary.xml` file in the $ESEC_HOME/config (%ESEC_HOME%\config on Windows) directory.

8 Create a copy of the `das_binary.xml` file for each instance of DAS_Binary you want to run. For example, to run two instances of DAS_Binary, create two copies of `das_binary.xml`.

9 Rename the copied `das_binary.xml` files to match the names selected in step 5.

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

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

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

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 Delete the unneeded durable subscription.

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

15a Open the Sonic Management Console.

15b **Windows:** Select *Start* > *Programs* > *Sentinel* >*SonicMQ* >*SonicMQ 7.0* >*Management Console*

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

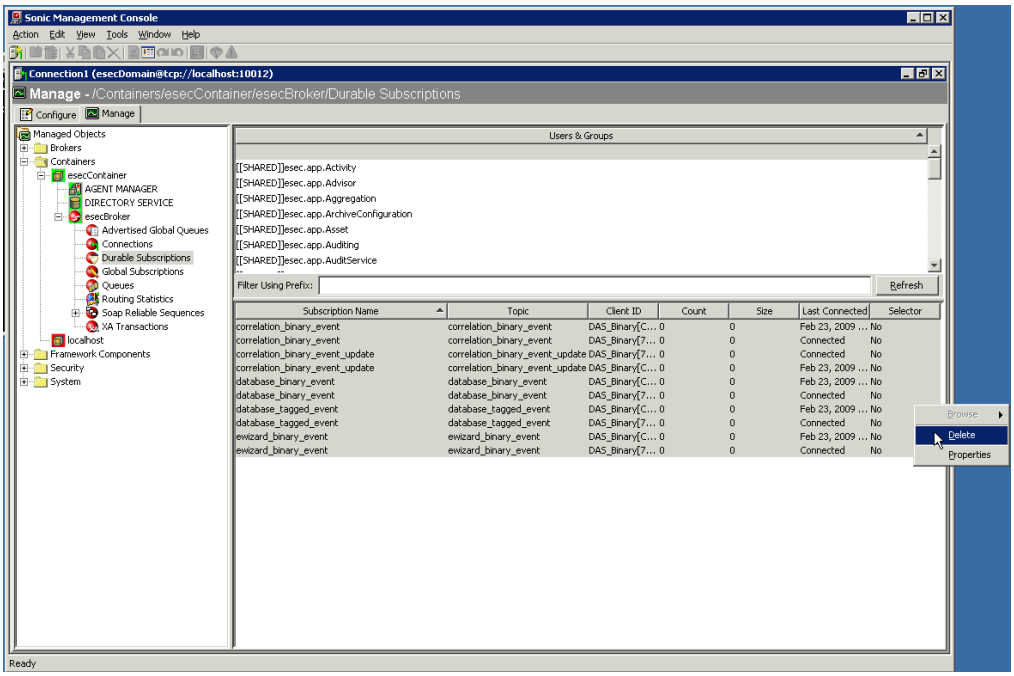
```
$ESEC_HOME/3rdparty/SonicMQ/MQ7.0/bin/startmc.sh
```

15c Specify the following to log in to the management console:

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

15d In the management console, select *Manage tab >Containers > esecContainer > esecBroker >Durable Subscriptions*.

15e Select the first empty row in the Users & Groups table on the right side of the GUI.



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

15f Select all durable subscriptions, right click, and then select *Delete*.

16 Restart the Sentinel service to activate your changes.

UNIX:

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

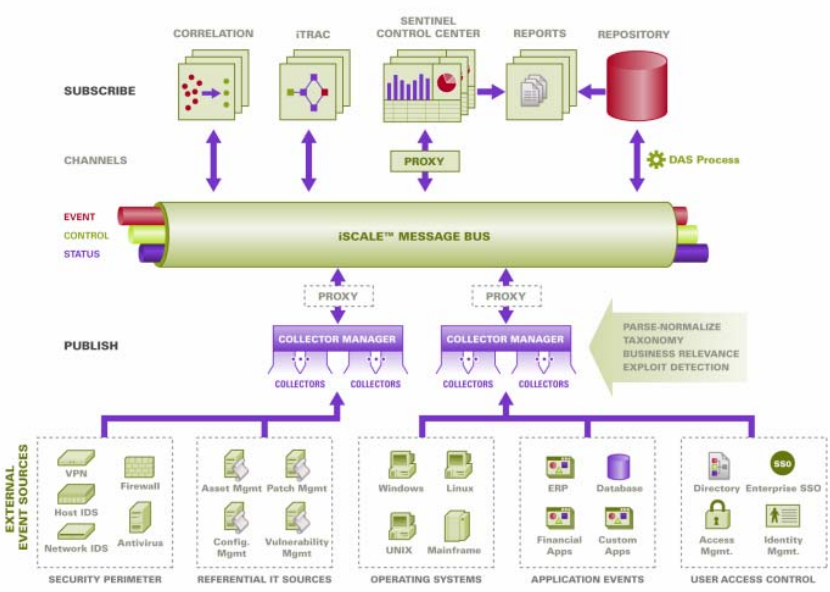
Windows: Restart the Sentinel service using the Windows Service Manager.

Communication Layer (iSCALE)

7

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 7-1 *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.

7.1 SSL Proxy and Direct Communication

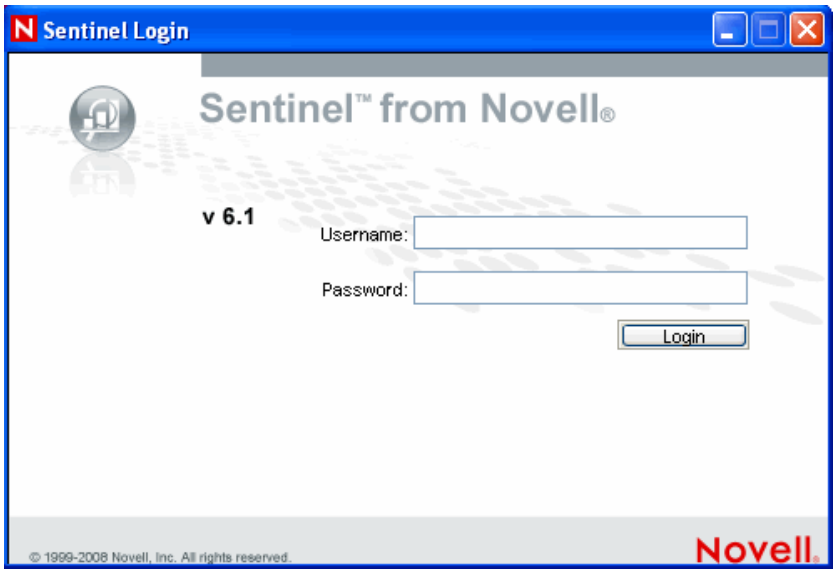
The Sentinel components that might use the SSL proxy are the Sentinel Control Center and the Collector Manager.

7.1.1 Sentinel Control Center

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

To Log into Sentinel Control Center for the First Time:

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



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

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

To Start the Sentinel Control Center on Linux and Solaris:

1 As the Sentinel Administrator User (esecadm), change directory to:

```
$ESEC_HOME/bin
```

2 Run the following command:

```
control_center.sh
```

3 Provide your username and password and click OK.

4 A Certificate window displays, click Accept.

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

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

7.1.2 Collector Manager

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

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

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

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

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

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

To Reset Trust Relationship for a Collector Manager:

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

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

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

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

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

7.2 Changing the Communication Encryption Key

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

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

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

To change the encryption key for Direct Communication:

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

   For UNIX:

   ```
   $ESEC_HOME/lib
   ```

   For Windows:

   ```
   %ESEC_HOME%\lib
   ```
3. Run the following command:

   On UNIX:

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

   On Windows:

   ```
   keymgr.bat --keyalgo AES --keysize 128 --keystore <output filename, usually
   .keystore>
   ```
4. Copy `.keystore` to each machine with a Sentinel Server component installed (unless it is using proxy communication). The file should be copied to:

   For UNIX:

   ```
   $ESEC_HOME/config
   ```

   For Windows:

   ```
   %ESEC_HOME%\config
   ```

NOTE: If you are using Advisor in Direct Download mode, you must update the Advisor password stored in Advisor's configuration files. This password is encrypted using the information in `.keystore` and must be recreated using the new `.keystore` value. To update the password, follow the instructions in Chapter 4, "Advisor Configuration," on page 59.

7.3 Increasing AES Key Strength

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

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

To configure AES 256-bit encryption:

1. Download Unlimited Encryption policies from Sun (http://java.sun.com/javase/downloads/index_jdk5.jsp). In the Other Downloads section, download "Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 5.0".
2. Apply the above mentioned policy file to all the JRE's that run processes that connect directly to Sonic (DAS, Correlation Engine, Communication Server, Collector Manager if used in Direct to Sonic mode). To understand how to apply policy files, go through the `Readme.txt` available in the policy you downloaded.
3. Use the keymgr utility to generate a 256-bit `AES .keystore` file by follow the instructions in Section 7.2, "Changing the Communication Encryption Key," on page 93.
4. Copy this `.keystore` file to all machines in step #2 and place in the $ESEC_HOME/config or %ESEC_HOME%\config directory.

NOTE: If you are using Advisor in Direct Download mode, you must update the Advisor password stored in Advisor's configuration files. This password is encrypted using the information in `.keystore` and must be recreated using the new `.keystore` value. For more information on updating a password, see "Certificate Management for DAS_Proxy" section in *Sentinel 6.1 Reference Guide*.

Crystal Reports for Windows

8

Crystal Reports Server™ (from Business Objects) 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 Chapter 2, “System Requirements,” on page 19 section.

On Windows, Sentinel has been tested with Crystal Reports Server XI R2 SP3. For more information on Crystal Reports Server XI Release 2 Service Packs, see https://www.sdn.sap.com/irj/sdn/businessobjects-downloads (https://www.sdn.sap.com/irj/sdn/businessobjects-downloads) and search for the correct version and platform.

This section discusses running Crystal Reports Server on Windows. For more information on running Crystal Reports Server on Linux/Solaris, see Chapter 9, “Crystal Reports for Linux,” on page 123.

To Install Crystal Reports Server:

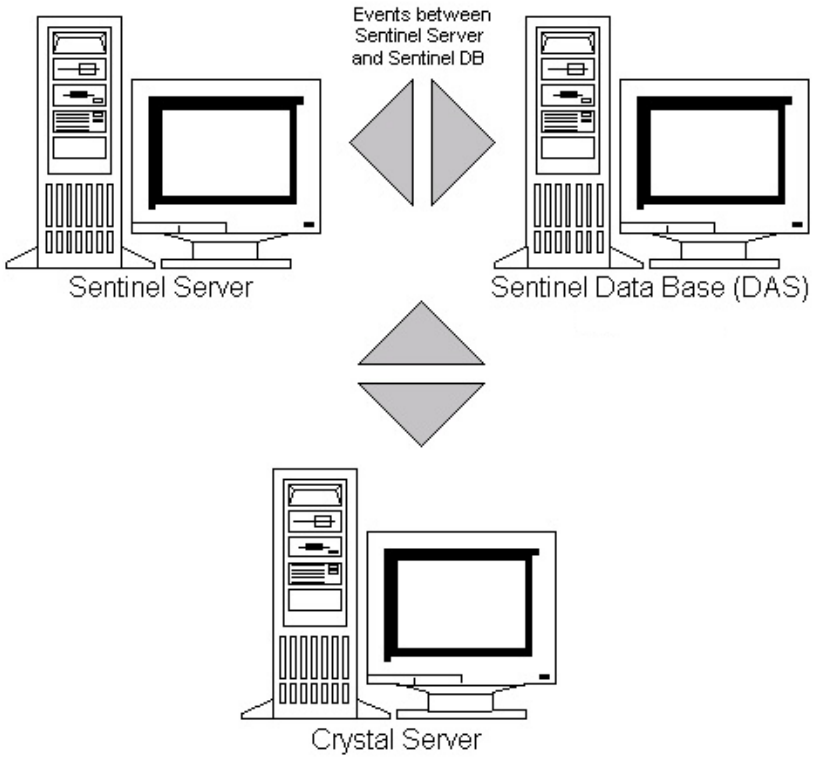
1. Install Microsoft IIS and ASP.NET
2. Install Microsoft SQL (depending on configuration as Windows authentication or SQL Server authentication)
3. For Chinese (Traditional & Simple) and Japanese users only: Install Asian Fonts (for example, Arial Unicode MS) to view reports in these languages.
4. Install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

     or
   - Installing and Configuring Oracle 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 Reports Server Report Refresh Record Limit (recommended)

11 Configure Sentinel Control Center to integrate with Crystal Reports Server.

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



8.1 Overview

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

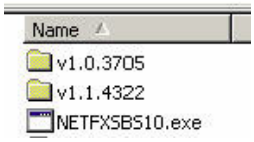
It is required to set up the CMS database on top of a local Microsoft SQL Server database for a Crystal installation on Windows. Although the Crystal Reports Server installer allows you to set up the CMS database on top of MSDE database, this configuration is not tested or supported for Sentinel.

8.2 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:

Figure 8-1 *Version of .NET Framework*



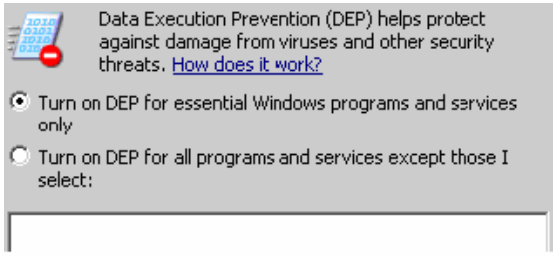
For more information on supported platforms for Crystal Reports Server in a Sentinel environment, Chapter 2, "System Requirements," on page 19 section.

8.3 Configuration Requirements

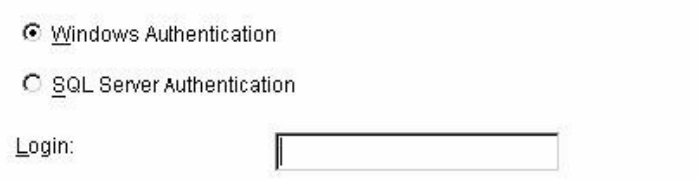
1. Make sure the account used to install Crystal Reports Server is a local administrator.
2. Set Data Execution Prevention (DEP) to run on essential Windows programs and services only. This is particularly helpful to avoid "Error 1920. Service Crystal Report Cache Server on Windows 2003".

   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.



3. The installation and configuration instructions for Crystal Reports Server assume that the Sentinel server and database have already been installed. You need to know which authentication mode was chosen for the Sentinel Report User. This user is called esecrpt, if you are using local database authentication. It could be called anything you choose if using Windows Authentication. The authentication mode was set on a screen similar to the one below during the Sentinel installation process.



NOTE: The esecrpt password can be explicitly set in case of Windows.

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

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

8.3.1 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.

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

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

8.4 Known Issues

- **Installing Crystal Reports:** Novell issues two Crystal keys, one for Crystal Reports Server and the other for Crystal Reports Developer (to modify or create new reports). 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 Business Objects Web site for procedures in manually uninstalling Crystal Reports Server:http://support.businessobjects.com/library/kbase/articles/c2017905.asp (http://support.businessobjects.com/library/kbase/articles/c2017905.asp).

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

8.5 Using Crystal Reports

For more information on using Crystal Reports Server for Sentinel Reporting, see Crystal Reports Server Documentation (http://support.businessobjects.com/documentation/product_guides/default.asp) and *Sentinel 6.1 User Guide*.

8.6 Installation Overview

Below is the overview of Installation.

8.6.1 Installation Overview for Crystal with SQL Server 2005

These are the high-level steps for installing Crystal Reports 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 Section 8.7.1, "Installing Crystal Reports Server for Microsoft SQL Server 2005 with Windows Authentication," on page 100.
   - If you selected SQL Authentication for the Sentinel Report user when installing Sentinel, see Section 8.7.2, "Installing Crystal Reports Server for Microsoft SQL Server 2005 with SQL Authentication," on page 104 or Section 8.7.3, "Installing Crystal Reports Server for Oracle," on page 109
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 (Section 8.9.5, "Configuring Reports Permissions," on page 117)
8. Configure Sentinel to the Crystal Reports Server

NOTE: These steps must be performed in order.

8.6.2 Installation Overview for Crystal with Oracle

These are the high-level steps for installing Crystal Reports 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 Section 8.7.2, "Installing Crystal Reports Server for Microsoft SQL Server 2005 with SQL Authentication," on page 104 or Section 8.7.3, "Installing Crystal Reports Server for Oracle," on page 109
4. Map Crystal Reports for use with Sentinel
5. Import Crystal Report Templates
6. Create a Crystal Web Page (Section 8.9.5, "Configuring Reports Permissions," on page 117)
7. Configure Sentinel to the Crystal Reports Server

NOTE: These steps must be performed in order.

8.7 Installation

This section covers how to install Crystal Reports Server for:

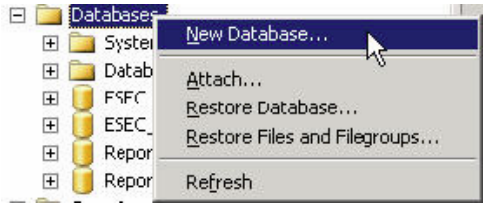
- Section 8.7.1, “Installing Crystal Reports Server for Microsoft SQL Server 2005 with Windows Authentication,” on page 100
- Section 8.7.2, “Installing Crystal Reports Server for Microsoft SQL Server 2005 with SQL Authentication,” on page 104
- Section 8.7.3, “Installing Crystal Reports Server for Oracle,” on page 109

8.7.1 Installing Crystal Reports Server for Microsoft SQL Server 2005 with Windows Authentication

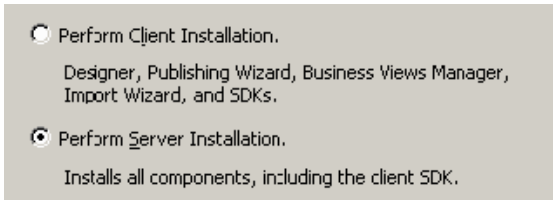
To install Crystal Reports Server with Windows Authentication:

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

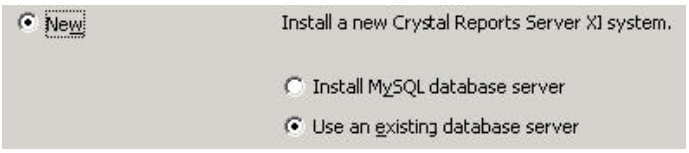
   Highlight and right-click Database and select New Database to create the Crystal CMS database.



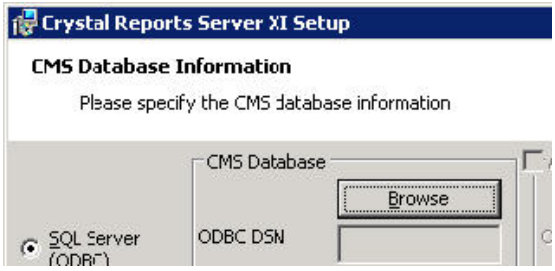
4. Under the Database name field, provide BOE115 and click OK.
5. Exit Microsoft SQL Server Management Studio.
6. Insert the Crystal Reports XI R2 Server CD into the CD-ROM.
7. If Autoplay is disabled on your machine, run `setup.exe`.
8. Select the Crystal Reports setup language.
9. In the Select Client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



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.

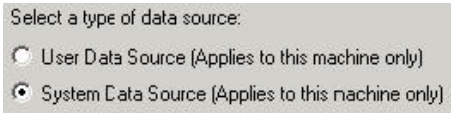


13 In the CMS Database Pane, click Browse.



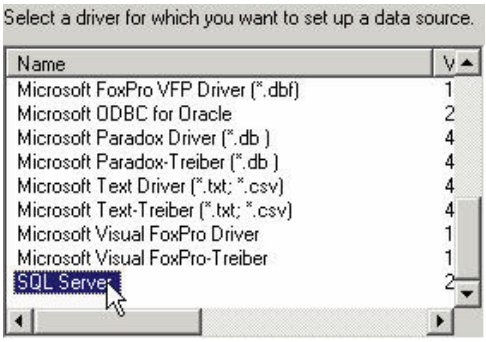
14 Click the Machine Data Source tab. Click New.

15 Select System Data Source.

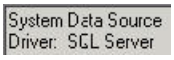


Click Next.

16 Scroll down and select SQL Server and click Next.



17 A new source displays, click Finish.

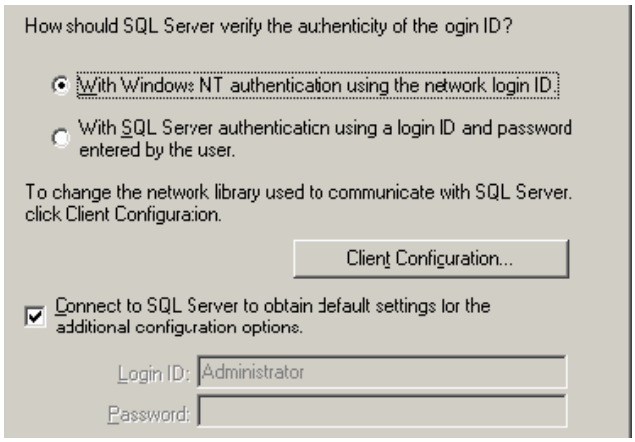


18 In the New Data Source to SQL Server window, specify:

- 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.



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.

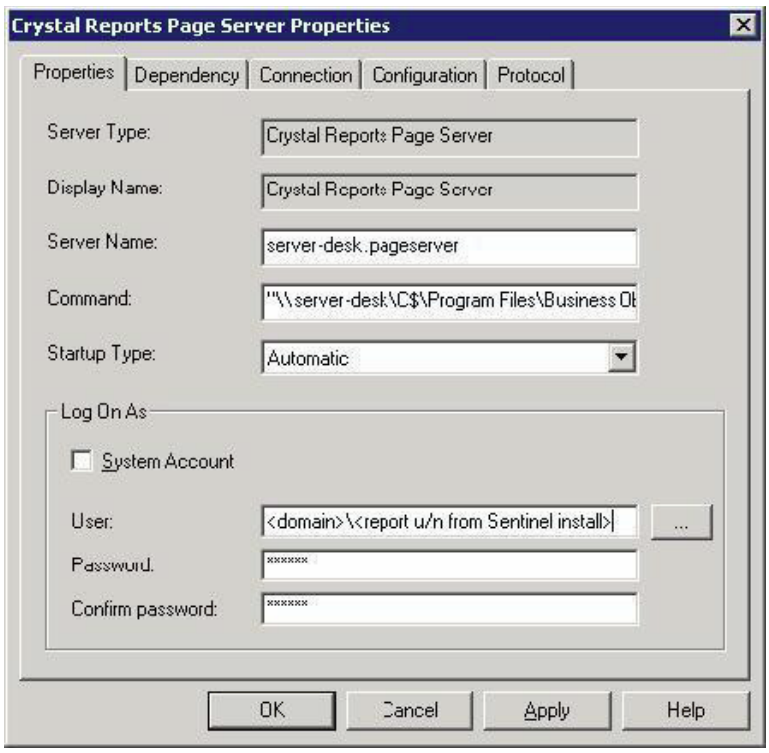
24 In the Web Component Adapter Type window, select IIS ASP.NET.

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).

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.



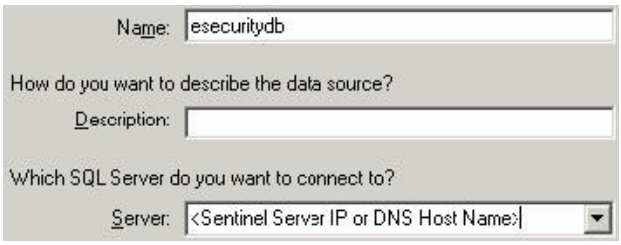
26 Highlight Crystal Reports Page Server and right-click to start.

Configuring Open Database Connectivity (ODBC) for Windows Authentication

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

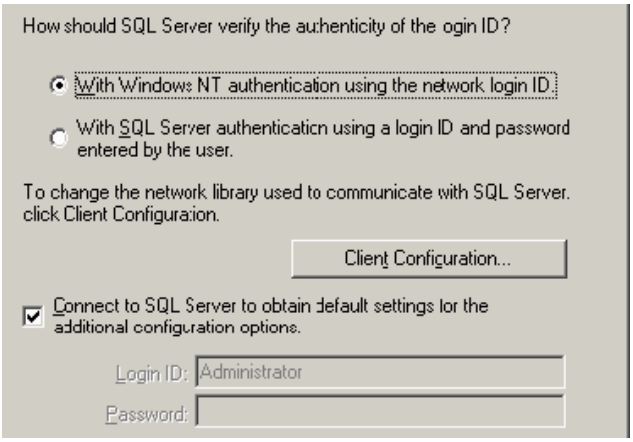
To Set up an ODBC data source for Windows Authentication:

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



5 Click Next.

In the next window, select Windows Authentication.



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

6 In the next window select:

- Change the Sentinel database (Default name is ESEC)
- Leave all the default settings

Click Next.

7 Click Finish.

8 Click Test Data Source. A connection is established. Click OK until you exit.

8.7.2 Installing Crystal Reports Server for Microsoft SQL Server 2005 with SQL Authentication

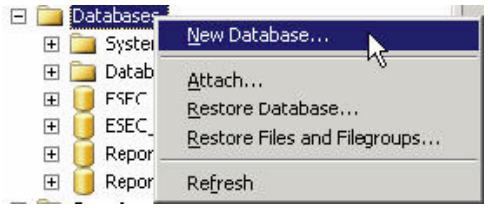
To Install Crystal Reports Server with SQL Authentication:

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 to create the Crystal CMS database.



4 Under the Database name field, provide BOE115 and click OK.

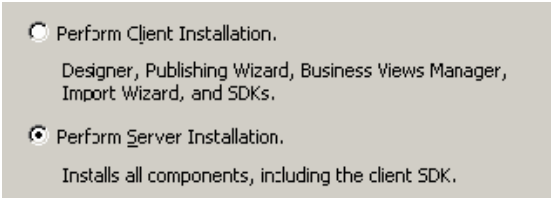
5 Exit Microsoft SQL Server Management Studio.

6 Insert the Crystal Reports Server XI R2 CD into the CD-ROM.

7 If Autoplay is disabled on your machine, run `setup.exe`.

8 Select the Crystal Reports setup language.

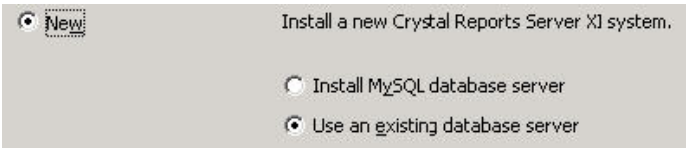
9 In the Select Client or Server Installation window, select Perform Server Installation.



10 Provide Crystal license key (obtained from Novell Customer Center (https://secure-www.novell.com/center/regadmin))

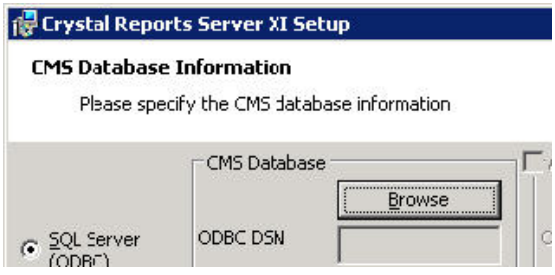
11 Specify a destination folder.

12 For install type, select Use an existing database server.



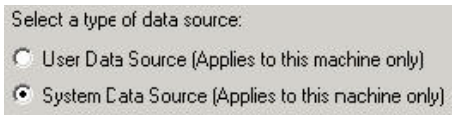
NOTE: Crystal Reports Server and Microsoft SQL Server must reside on the same machine.

13 In the CMS Database Pane, click Browse.



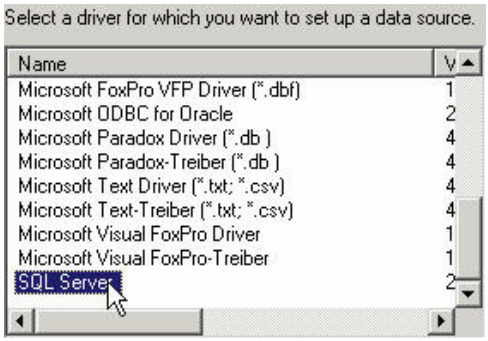
14 Click the Machine Data Source tab; click New.

Select System Data Source.

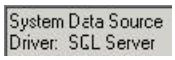


Click Next.

Scroll down and select SQL Server and click Next.



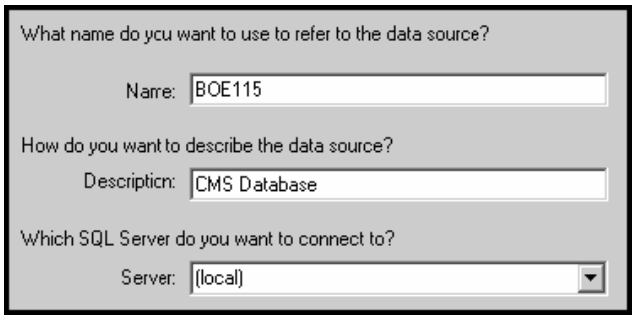
A new source displays, click Finish.



15 Right-click Databases and select Create New Database (BOE115).

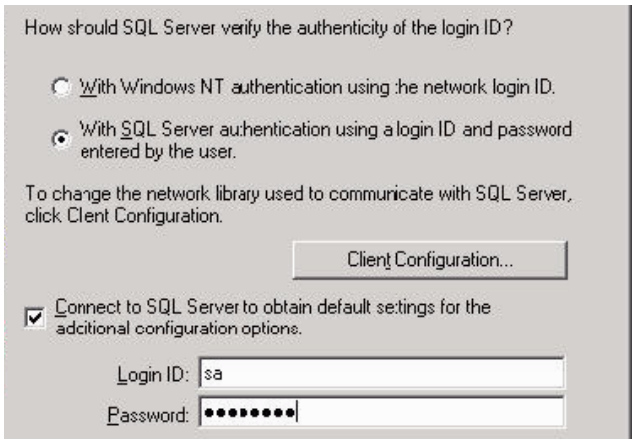
16 In New Data Source to SQL Server window, specify:

- Name of your data source (For example, BOE115)
- Description (optional)
- For Server, click the down arrow and select (local)



Click Next.

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

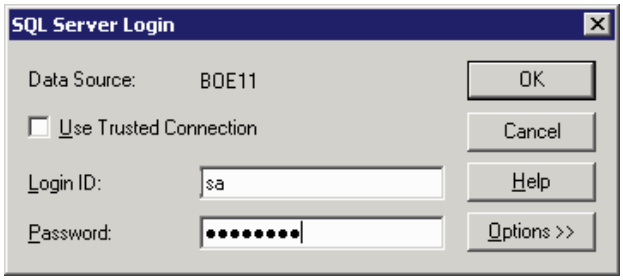


Check the Change the default database to: check box. Change your default database to BOE115. Click Next.

18 In the Create a New Data Source to SQL Server window, click Finish.

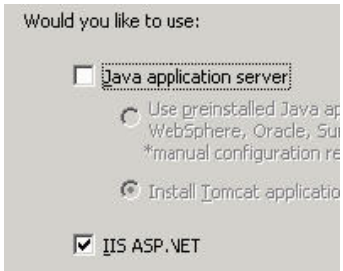
19 Click Test Data Source. Click OK.

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.



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).

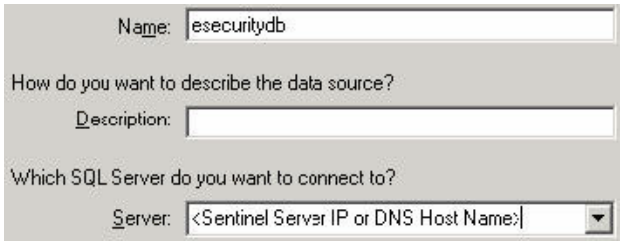


Configuring Open Database Connectivity (ODBC) for SQL Authentication

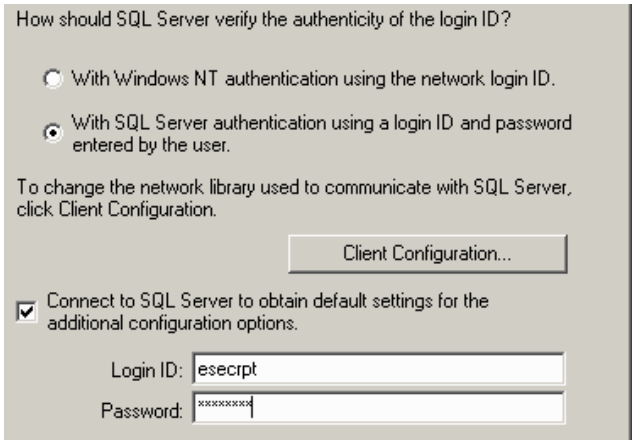
This procedure sets up an ODBC data source name to allow the Crystal Reports Server to connect to the Sentinel database on Windows and SQL Server using SQL authentication. These steps must be performed on the Crystal Reports Server machine.

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



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



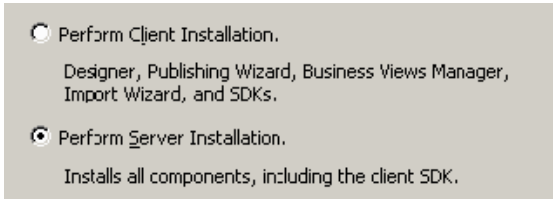
6. In the next window select:
   - Change the Sentinel database (Default name is ESEC)
   - Leave all the default settings

   Click Next; click Finish.
7. Click Test Data Source. After testing, click OK. Click OK until you exit.

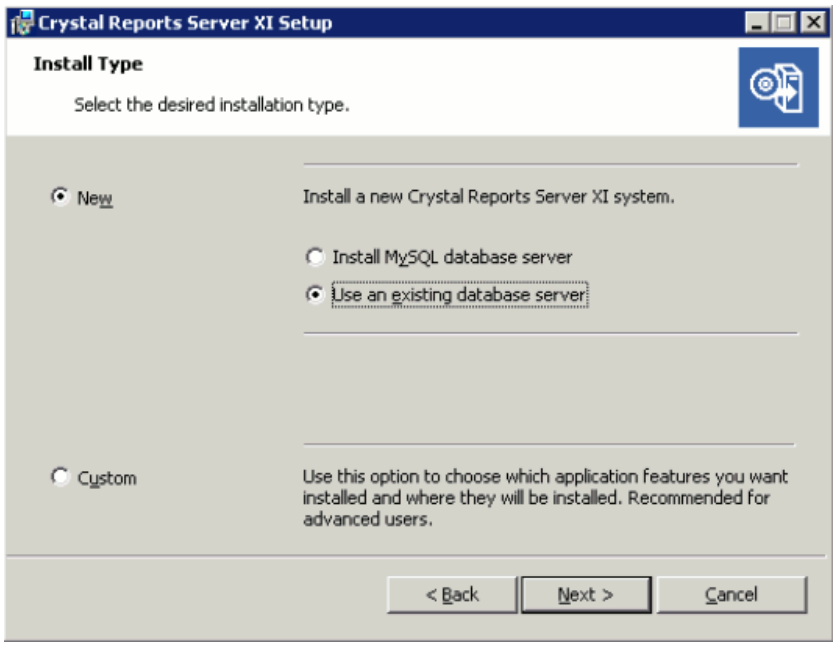
8.7.3 Installing Crystal Reports Server for Oracle

To Install Crystal Reports Server XI R2 for Oracle:

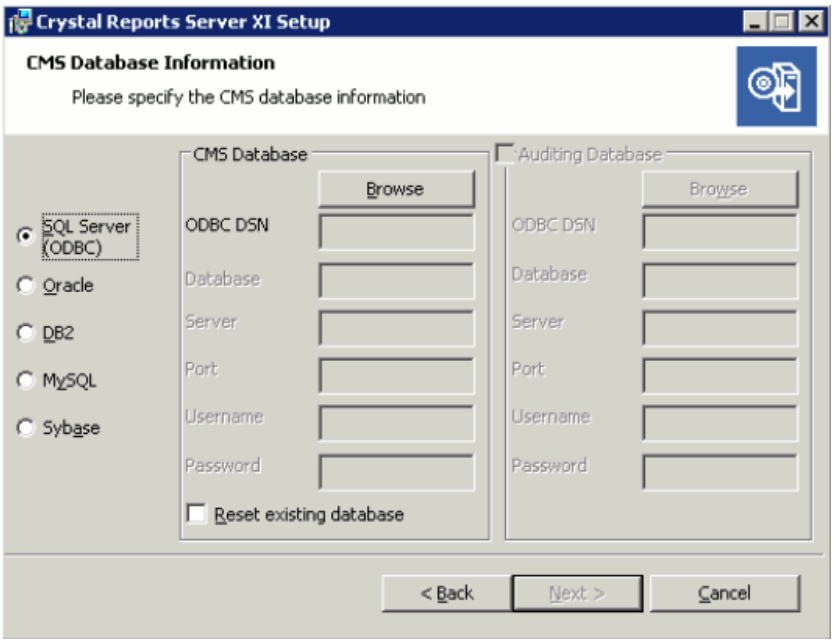
1. Insert the Crystal Reports XI R2 Server CD into the CD-ROM.
2. Select the Crystal Reports setup language.
3. In the Select Client or Server Installation window, select Perform Server Installation.



4. Select Use an existing database server.



The CMS Database Information window displays:



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.

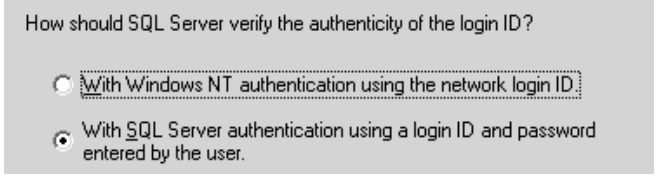
NOTE: Crystal Reports Server and Microsoft SQL Server 2005 must reside on the same machine.

---

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.

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



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

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

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

To Create Net Service Name Configuration (Configuring Oracle 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 Sentinel database resides on
   - Select the Oracle Port (default 1521 on install)

   Click Next.
7. To identify the Sentinel 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.

8.8 Configuration for all Authentications and Configurations

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

8.8.1 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

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.

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

8.9 Publishing Crystal Report Templates

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

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

There are four ways to add reports to the system:

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

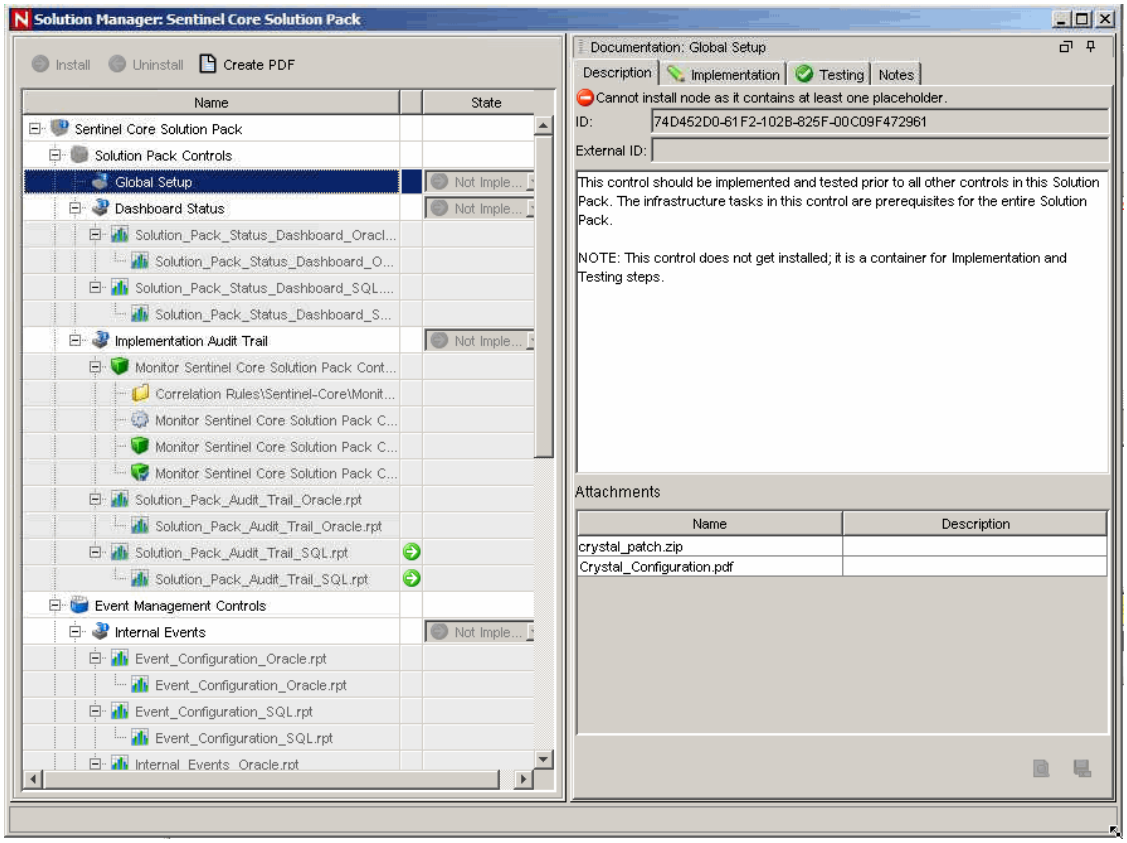
IMPORTANT: To run any Top 10 reports, aggregation must be enabled and EventFileRedirectService in `DAS_Binary.xml` must be set to “on”. This is already configured in a default Sentinel installation. For information on how to enable aggregation, see “Report Data Configuration” section of “Admin” in*Sentinel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

8.9.1 Publishing Report Templates using Solution Manager

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

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

Figure 8-2 *Core Solution Pack in Solution Manager Showing Crystal Auxiliary Files*



8.9.2 Publishing Report Templates - Crystal Publishing Wizard

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

To publish the Crystal Report Templates:

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

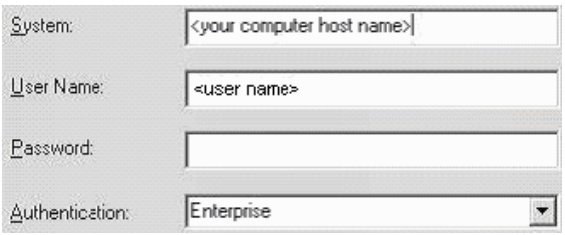
---

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.

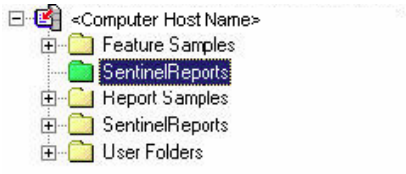
   NOTE: Publishing reports under user Administrator allows all users access to the reports.



3 Click Add Folder. [Optional] Select Include Subfolders.

4 Navigate to the location of the report template(s). Click OK. Click Next.

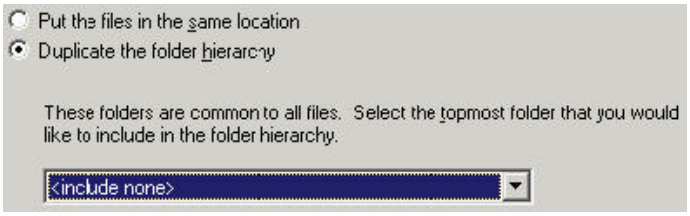
5 In the Specify Location window, click New Folder (upper right corner) and create a folder called SentinelReports (if it does not already exist). Click Next.



6 Select:

- Duplicate the folder hierarchy.

Click the down arrow and select <include none>



Click Next.

7 In the Confirm Location window, click Next.

8 In the Specify Categories window, provide a category name (such as sentinel), highlight the name, and click the + button.

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

Click Next.

9 In the Specify Schedule window, click Let users update the object (this should be default). Click Next.

10 In the Specify Repository Refresh window, click Enable All to enable repository refresh. Click Next.

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

12 In the Change Defaults Values window, click Publish reports without modifying properties (this should be default). Click Next.

13 Click Next to add your objects.

14 A published list displays, click Finish.

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

8.9.3 Publishing Report Templates – Central Management Console

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

To import Crystal Report Templates:

1 Open a Web browser and provide the following URL:

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

2 Click Central Management Console.

3 Login to your Crystal Reports Server.

4 Under the Organize pane, click Folders.

5 In the upper right-hand corner, click New Folder.

6 Create a folder SentinelReports (if it does not already exist). Click OK.

NOTE: You must exactly name the folder SentinelReports.

7 Click SentinelReports.

8 Click the Subfolders tab and create subfolders if desired. If adding the Sentinel core reports manually, create the following subfolders:

- Advisor_Vulnerability
- Dashboards
- Incident Management
- Internal Events
- Security Events
- Top 10

9 Click Home > Objects > New Object.

10 On left side of the page, highlight Report.

11 Click Browse and browse to the location of the report templates you want to add. Pick a folder and select a report.

12 Highlight SentinelReports, click Show Subfolders.

13 Select the appropriate folder for the report, click Show Subfolders.

14 Click Submit.

15 To add the remaining reports, repeat steps 9 to 17 until all reports have been added.

8.9.4 Setting a Named User Account

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

To Set the Guest Account as Named User:

1 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.

8.9.5 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 (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 Sentinel Database

To Test for Web Server connection to the database:

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

2 Click Central Management Console.

3 Provide Administrator as the User Name. Provide your password (by default, this will be blank). Click Log On.

4 Navigate to Folders > SentinelReports > Internal Events.

5 Select Column Display Details.

6 Click Preview.

7 Depending on your system, login as esecrpt or as the Sentinel Report User.

8 Under the Sort field drop-down menu, select Tag.

9 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>:<port number>/
businessobjects/enterprise115/adminlaunch/default.aspx
```

You should get a Crystal BusinessObjects Web page.

8.9.6 Disabling Sentinel Top 10 Reports

By default Sentinel Top 10 Reports are enabled. If you do not expect to use these reports, you can reduce database storage and CPU usage by disabling the Sentinel Top 10 Reports:

- Turn off Aggregation
- Disable EventFileRedirectService

To Turn off Aggregation:

1 Start Sentinel Control Center.

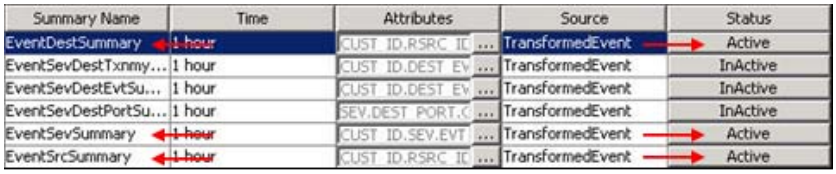
2 Login.

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.



To Disable 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
```

8.9.7 Configuring Sentinel Control Center to Integrate with Crystal Reports Server

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

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

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

To Configure Sentinel to integrate with Crystal Reports Server:

1 Log into Sentinel Control Center as a user that has privileges to the Admin tab.

2 On the Admin tab, select Crystal Report Configuration.

3 In the Analysis URL field, provide the following:

```
http://<hostname_or_IP_of_web_server>/
GetReports.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 Reports Server.

NOTE: The URL above will not work properly if the Automated Process Scheduler (APS) is set to the IP Address. It must be the host name of the Crystal Reports 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>/
GetReports.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 Reports Server.

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

6 Click Refresh next to the Advisor URL field.

7 Click Save.

8 Log out 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.

8.10 High-Performance Configurations for Crystal

8.10.1 Increasing Crystal Reports 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 must reconfigure the Crystal Page Server. This can be done by using either the Central Configuration Manager or the Crystal Web Page.

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

1 Click Start > All Programs > BusinessObjects 11 > Crystal Reports Server > Central Configuration Manager.

2 Right-click Crystal Reports Page Server and select Stop.

3 Right-click Crystal Reports Page Server and select properties.

4 In the Command field under the Properties tab, at the end of the command line add:

```
maxDBResultRecords <value greater than 20000 or 0 to disable the default limit>
```

5 Restart Crystal Page Server.

To Reconfigure the Crystal Page Server through the Central Management Console:

1 Click Start > All Programs > BusinessObjects 11 > Crystal Reports Server > .Net Administration Launchpad. Alternatively, open a Web browser and provide the following URL:

```
http://<DNS name or IP address of your web server>:<port number>/
businessobjects/enterprise11/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.

You might be prompted for a logon name and password to access the operating system service manager.

8.10.2 Reports Using Aggregation Service

To improve performance, the Top 10 reports included in the Sentinel Core Solution Pack query summary tables instead of the events table. The summary tables contain counts over time for combinations of fields in the event data. This provides a much smaller data set for certain types of queries and results in much faster queries and report run time.

The Aggregation service is responsible for populating the summary tables with summarizations of all of the events in the events table. The Aggregation service will only generate summarized data for summaries that are active. The following summaries are required by the Top 10 reports and are enabled by default:

- EventDestSummary
- EventSevSummary
- EventSrcSummary

Summaries can be activated or inactivated using the 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 “Report Data Configuration” in Admin in the *Sentinel 6.1 User Guide*.

NOTE: Reports that query a large date range might take sometime to run. They can be scheduled instead of running interactively. For information about scheduling Crystal Reports, see Crystal BusinessObjects Enterprise™ 11 documentation (http://support.businessobjects.com/documentation/product_guides/default.asp).

8.10.3 Report Development

The Crystal Reports Developer can be used to create or modify Crystal reports. For custom developed reports, the following is recommended:

- If the reports can utilize 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.

Crystal Reports for Linux

9

Crystal Reports Server™ (from Business Objects) 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 Chapter 2, “System Requirements,” on page 19.

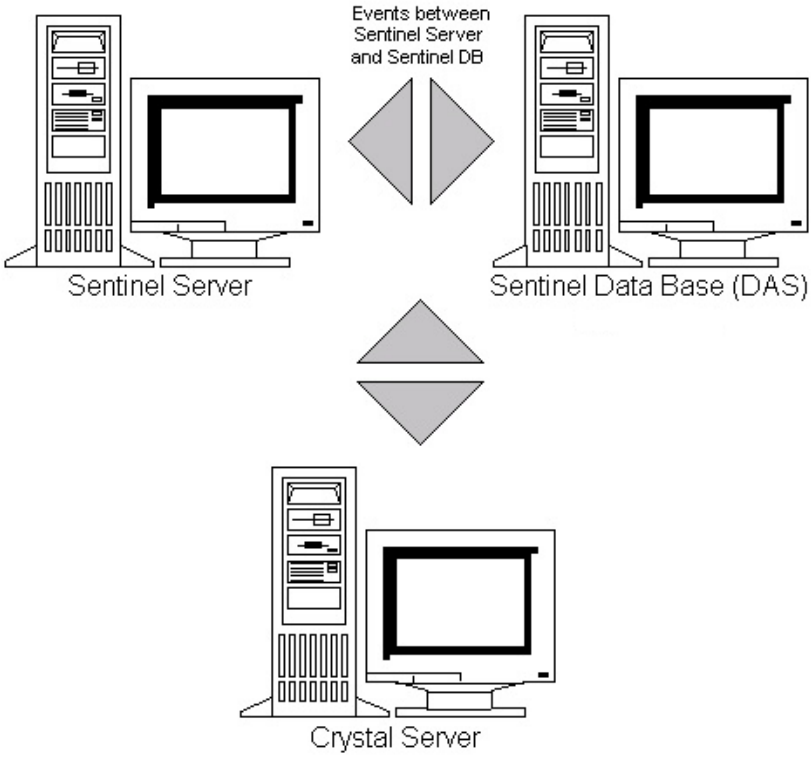
On Linux, Sentinel has been tested with Crystal Reports Server XI R2 SP2. For more information on Crystal Reports Server XI Release 2 Service Packs or to download them, see https://www.sdn.sap.com/irj/sdn/businessobjects-downloads (https://www.sdn.sap.com/irj/sdn/businessobjects-downloads) and search for the correct version and platform.

This section discusses running Crystal Reports Server on Linux. For more information on running Crystal Reports Server on Windows, see Chapter 8, “Crystal Reports for Windows,” on page 95.

IMPORTANT: The installation should be done in the order presented below.

To Install Crystal Reports Server:

1. Pre-install and install of Crystal Reports Server™ XI R2
2. Patch Crystal Reports Server
3. Publishing (importing) Crystal reports
4. Setting a “Named User” account
5. Testing connectivity to the Web Server
6. Enabling Top 10 reports (optional)
7. Increasing Crystal Reports Server Report Refresh Record Limit (recommended)
8. Configuring Sentinel Control Center to Integrate with Crystal Reports Server



9.1 Overview

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

9.2 Installation

9.2.1 Pre-Install of Crystal Reports Server™ XI R2

To Pre-Install Crystal Reports Server:

1. If the Sentinel Database is not on the same machine as the Crystal Reports Server, then you must install the Oracle Client software on the Crystal Reports Server machine. This additional step is not needed if the Sentinel Database is on the same machine as the Crystal Reports Server because in this case the required Oracle software is already installed during the Oracle database installation.
2. Login to the Crystal Reports Server machine as the root user
3. Create bobje group

```
groupadd bobje
```

4. Create Crystal user (the home directory in this example is /export/home/crystal, change if needed; the /export/home part of the path must already exist).

   ```
   useradd -g bobje -s /bin/bash -d /export/home/crystal -m crystal
   ```

5. Create directory for Crystal Software:

   ```
   mkdir -p /opt/crystal_xir2
   ```

6. Change the ownership of the Crystal Software directory (recursively) to crystal/bobje:

   ```
   chown -R crystal:bobje /opt/crystal_xir2
   ```

7. You must grant permissions to the crystal user on the $ORACLE_HOME directory using an Access Control List (ACL). Assuming the crystal user is “crystal” and $ORACLE_HOME is `/opt/oracle/product/10.2/db_1`, the command to perform this is:

   ```
   setfacl -m u:crystal:rx -R  /opt/oracle/product/10.2/db_1
   ```

   To verify that the ACL was set correctly, run the following command and check for “crystal” in the output:

   ```
   getfacl  /opt/oracle/product/10.2/db_1
   ```

8. Add the crystal user to the oracle group using the following command:

   ```
   groupmod -A crystal oinstall
   ```

   This enables the crystal user to communicate with the Oracle database and execute Oracle utilities like sqlplus and tnsping.

9. Change to the crystal user:

   su - crystal

10. The ORACLE_HOME environment variable must be set in the crystal user’s environment. To do this, modify the crystal user’s login script to set the ORACLE_HOME environment variable to the base of the Oracle software. For example, if the crystal user’s shell is bash and the Oracle software is installed in the directory `/opt/oracle/product/10.2/db_1`, then open the file `~crystal/.bash_profile` (`.profile` on SLES) and add the following line to the end of the file:

    ```
    export ORACLE_HOME=/opt/oracle/product/10.2/db_1
    ```

11. The LD_LIBRARY_PATH environment variable in the crystal user’s environment must contain the path to the Oracle software libraries. To do this, modify the crystal user’s login script to set the LD_LIBRARY_PATH environment variable to include the Oracle software libraries. For example, if the crystal user’s shell is bash, then open the file `~crystal/.bash_profile` and add the following line to the end of the file (below where the ORACLE_HOME environment variable is set):

    ```
    export LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH
    ```

12. The PATH environment variable in the crystal user’s environment must contain the path to the Oracle software executables. To do this modify the crystal user's script to set the PATH environment variable to include the Oracle software executables. For example if the crystal user's shell is bash, then open the file `~crystal/.bash_profile` and add the following line to the end of the file.

```
export PATH=$PATH:$ORACLE_HOME/bin
```

13 An entry must be added to the Oracle `tnsnames.ora` file with the Service Name esecuritydb that points to the Sentinel Database. To do this on the Crystal Reports Server machine:

13a Log in as the oracle user.

13b Change directories to $ORACLE_HOME/network/admin

13c Make a backup of the file `tnsnames.ora`.

13d Open the file `tnsnames.ora` for editing.

13e If the Sentinel Database is on the Crystal Reports Server machine, then there should already be an entry in the `tnsnames.ora` file to the Sentinel Database. For example, if the Sentinel Database is named ESEC, then an entry similar to the following will exist:

```
ESEC =
(DESCRIPTION =
 (ADDRESS_LIST =
  (ADDRESS = (PROTOCOL = TCP)(HOST = dev-linux02)(PORT = 1521))
  )
  (CONNECT_DATA =
  (SID = ESEC)
  )
)
```

13f If the Sentinel Database is not on the Crystal Reports Server machine, open the `tnsnames.ora` file on the Sentinel Database machine to find the entry described above.

13g Make a copy of that entire entry and paste it at the bottom of the `tnsnames.ora` file on the Crystal Reports Server machine. The Service Name part of the entry must be renamed to `esecuritydb`. For example, when the entry above is copied and renamed properly, it will look like:

```
esecuritydb =
(DESCRIPTION =
 (ADDRESS_LIST =
  (ADDRESS = (PROTOCOL = TCP)(HOST = dev-linux02)(PORT = 1521))
  )
  (CONNECT_DATA =
  (SID = ESEC)
  )
)
```

13h Make sure the HOST part of the entry is correct (for example, make sure it is not set to localhost if the Crystal Reports Server and Sentinel Database are on different machines).

13i Save the changes to the `tnsnames.ora` file.

13j Execute the following command to check that the `esecuritydb` Service Name is configured properly:

```
tnsping esecuritydb
```

13k After the command is executed, you will get a message saying the connection is OK.

9.2.2 Installing Crystal Reports Server XIR2

The Crystal Reports Server installer consists of two `.iso` files. During the installation, you will be prompted for the location of the second disk.

To Install Crystal Reports Server:

1. Log in as crystal user.
2. Change directories into disk1 of the Crystal installer.
3. Execute:

   ```
   ./install.sh
   ```
4. Select Language: English
5. Select New Installation.
6. Read and accept License Agreement.
7. Provide Product Keycode.
8. Provide install directory:

   ```
   /opt/crystal_xir2
   ```
9. Select: User install.
10. Select: New Install.
11. Select: Install MySQL unless you plan to install the Crystal CMS database into an existing database.
12. Specify configuration information for MySQL:
    - **12a** Use default port 3306
    - **12b** Admin password
13. Specify more configuration information for MySQL:
    - **13a** Default DB Name: BOE115
    - **13b** User id: mysqladm
    - **13c** Password
14. Specify more configuration information for MySQL:
    - **14a** Local Name Server: <local machine's hostname>
    - **14b** Default CMS Port Number: 6400
15. Select: Install Tomcat
16. Specify Tomcat configuration information:
    - **16a** Default Receive HTTP requests port: 8080
    - **16b** Default Redirect jsp requests port: 8443
    - **16c** Default Shutdown Hook port: 8005
17. Press Enter to confirm the default directory.
18. Press Enter to start installation.
19. Note the link to the CMS server, which will probably be something similar to this:

    http://<hostname>:8080/businessobjects/enterprise115/adminlaunch/launchpad.html

---

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

9.3 Publishing Crystal Reports Templates

NOTE: It is strongly encouraged that the Sentinel Reports Release Notes be reviewed before performing this task. There can be updated files, scripts and additional steps.

Many report templates are created by Novell for use in the Sentinel Control Center Analysis tab and Advisor tab. The most recent reports can be downloaded from the Sentinel 6.1 Content Web site (http://support.novell.com/products/sentinel/sentinel61.html).

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

There are four ways to add reports to the system:

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

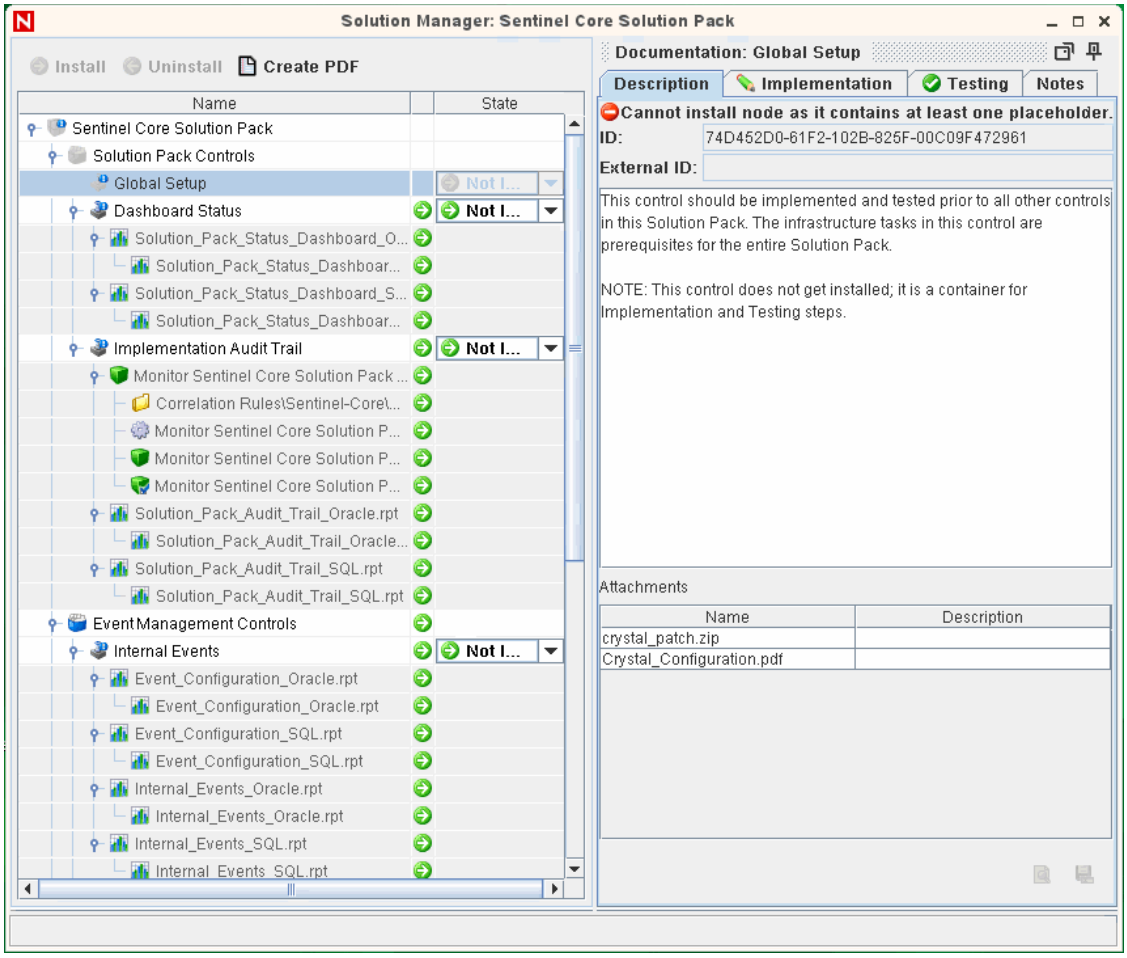
IMPORTANT: To run any Top 10 reports, aggregation must be enabled and EventFileRedirectService in `DAS_Binary.xml` must be set to on. For information on how to enable aggregation, see "Report Data Configuration" section of "Admin" in *Sentinel 6.1 User Guide*.

9.3.1 Publishing Report Templates using Solution Manager

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

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

Figure 9-1 *Core Solution Pack in Solution Manager Showing Crystal Auxiliary Files*



9.3.2 Publishing Report Templates – Crystal Publishing Wizard

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

NOTE: A Windows platform is required to run Crystal Publishing Wizard.

To import Crystal Reports templates:

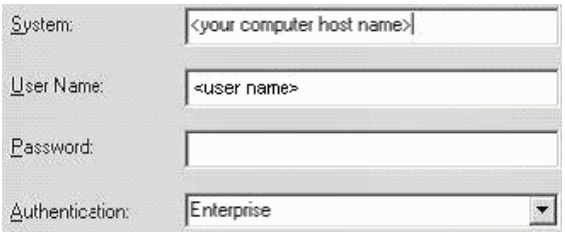
NOTE: If you import (publish) your Reports Templates again, delete your previous import of Report Templates.

---

1. Click Start > All Programs > BusinessObjects 115 > Crystal Reports Server > Publishing Wizard.
2. Click Next.

   Login. System should be your host computer name and Authentication should be Enterprise. User Name can be Administrator. For security reasons, you should use another user other than Administrator. Provide your password and click Next.

NOTE: Publishing reports under user Administrator allows all users access to the reports.



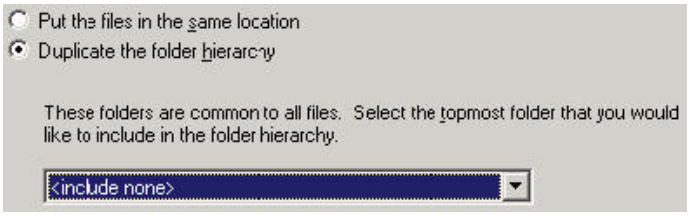
3 Click Add Folder. [Optional] Click Include Subfolders.

4 Navigate to the location of the report template(s). Click OK. Click Next.

5 In the Specify Location window, click New Folder (upper right corner) and create a folder called SentinelReports (if it does not already exist). Click Next.

6 Select:

- Duplicate the folder hierarchy.
- Click the down arrow and select <include none>



Click Next.

7 In the Confirm Location window, click Next.

8 In the Specify Categories window, provide a category name (such as sentinel), highlight the name, and click the + button.

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

Click Next.

9 In the Specify Schedule window, click Let users update the object (this should be default). Click Next.

10 In the Specify Repository Refresh window, click Enable All to enable repository refresh. Click Next.

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

12 In the Change Defaults Values window, click Publish reports without modifying properties (this should be default). Click Next.

13 Click Next to add your objects.

14 Click Next. Click Finish.

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

9.3.3 Publishing Report Templates – Central Management Console

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

To import Crystal Reports Templates:

1 Open a Web browser and provide the following URL:

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise115/adminlaunch
```

2 Click Central Management Console

3 Login to your Crystal Reports Server.

4 Under the Organize pane, click Folders.

5 In the upper right-hand corner, click New Folder.

6 Create a folder SentinelReports (if it does not already exist). Click OK.

NOTE: You must exactly name the folder SentinelReports.

---

7 Click SentinelReports.

8 Click the Subfolders tab and create subfolders if desired. If adding the Sentinel core reports manually, create the following subfolders:

- Advisor_Vulnerability
- Dashboards
- Incident Management
- Internal Events
- Security Events
- Top 10

9 Click Home > Objects > New Object.

10 On left side of the page, highlight Report.

11 Click Browse and browse to the location of the report templates you want to add. Pick a folder and select a report.

12 Highlight SentinelReports, click Show Subfolders.

13 Select the appropriate folder for the report, click Show Subfolders.

14 Click Submit.

15 To add the remaining reports, repeat steps 9 to 17 until all reports have been added.

9.4 Using the Crystal XI R2 Web Server

Crystal Reports Server XI on Linux installs a Web Server through which you can perform administrative tasks as well publish and view reports.

The administrative portal is accessed through your browser at the following URL:

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise115/adminlaunch
```

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
```

9.4.1 Testing connectivity to the Web Server

To test connectivity to the Web Server:

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

2 Provide

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise115/adminlaunch
```

You should get a Crystal BusinessObjects Web page.

9.4.2 Setting a “Named User” Account

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

To set the Guest Account as Named User:

1 Open a Web browser and provide the following url:

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise115/adminlaunch
```

2 Click Central Management Console.

3 The System Name should be your host computer name. Authentication Type should be Enterprise. If not, select Enterprise.

4 In the Organize pane, click Users > Guest.

5 Change connection type from Concurrent User to Named User; Click Update.

Logoff and close window.

9.4.3 Configuring Reports Permissions

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

To Configure Reports Permissions:

1 Open a Web browser and provide the following URL:

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise115/adminlaunch
```

2 Click Central Management Console.

The System Name should be your host computer name. Authentication Type should be Enterprise. If not, select Enterprise.

3 Provide your user name, password and click Log On.

4 In the Organize pane, click Folders.

5 Single-click SentinelReports; Select All.

6 Click the Rights tab.

7 For Everyone, in the drop-down menu to the right select View on Demand.

8 Click Update; Logoff and close the window.

9.5 Increasing Crystal Reports Server Report Refresh Record Limit

If Crystal attempts to process an extremely large number of events, it might give an error about maximum processing time or maximum record limit. To set your server to process a higher number or an unlimited number of records you will need to reconfigure the Crystal Page Server.

To Reconfigure the Crystal Page Server:

1 Open a Web browser and provide the following URL:

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/
businessobjects/enterprise115/adminlaunch
```

2 Click Central Management Console.

3 The System Name should be your host computer name. Authentication Type should be Enterprise. If not, select Enterprise.

4 Provide your user name, password and click Log On.

5 Click Servers; Click <server name>.pageserver.

6 Under Database Records to Read When Previewing Or Refreshing a report, click Unlimited records; Click Apply.

7 A prompt to restart the page server displays, click OK.

8 You might be prompted for a logon name and password to access the operating system service manager.

9.6 Configuring Sentinel Control Center to Integrate with Crystal Reports Server

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

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

NOTE: This configuration must be performed only after the Crystal Reports Server has been installed and Crystal Reports have been published to it. For more information on supported platforms for Crystal Reports Server in a Sentinel environment, Chapter 2, "System Requirements," on page 19.

To Configure Sentinel to Integrate with Crystal Reports Server:

1 Log into Sentinel Control Center as a user that has privileges to the Admin tab.

2 On the Admin tab, select Crystal Report Configuration.

3 In the Analysis URL field, provide the following:

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/esec-script/GetReports.jsp?APS=<hostname>&user=Guest&password=&tab=Analysis
```

NOTE: <hostname_or_IP_of_web_server> must be replaced with the IP address or hostname of the Crystal Reports Server.

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

NOTE: <web_server_port_default_8080> must be replaced with the port the Crystal Web Server is listening on.

---

4 Click Refresh next to the Analysis URL field.

5 If you have Advisor installed, provide the following in the Advisor URL field:

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/esec-script/GetReports.jsp?APS=<hostname>&user=Guest&password=&tab=Advisor
```

NOTE: <hostname_or_IP_of_web_server> must be replaced with the IP address or hostname of the Crystal Reports Server.

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

NOTE: <web_server_port_default_8080> must be replaced with the port the Crystal Web Server is listening on.

---

6 Click Refresh next to the Advisor URL field;

Click Save.

7 Logout and log back in to the Sentinel Control Center.

The Crystal Reports trees in the Analysis and Advisor (if Advisor is installed) tabs should now display in the Navigator window.

9.7 Utilities and Troubleshooting

9.7.1 Starting MySQL

To make sure MySQL is running:

1 Login as crystal user.

2 cd /opt/crystal_xir2/bobje

3 `./mysqlstartup.sh`

9.7.2 Starting Tomcat

To make sure Tomcat is running:

1 Login as crystal user

2 cd /opt/crystal_xir2/bobje

3 `./tomcatstartup.sh`

9.7.3 Starting Crystal Reports Servers

To make sure Crystal Reports Servers are running:

1 Login as crystal user

2 cd /opt/crystal_xir2/bobje

3 `./startservers`

9.7.4 Crystal Host Name Error

To resolve Host Name error

1 If you get the following error:

```
Warning: ORB::BOA_init: hostname lookup returned `localhost' (127.0.0.1)
Use the -OAhost option to select some other hostname
```

Make sure your IP and hostname are in the /etc/hosts file. For example,

```
10.0.0.1   linuxCE02
```

9.7.5 Cannot Connect to CMS

If the system reports that it cannot connect to the CMS, try executing the following commands.

To Troubleshoot CMS connection failure:

1 If the command netstat –an | grep 6400 does not return any results, try the following:

- Provide MySQL connection information again:
  1. Login as crystal user
  2. cd /opt/crystal_xir2/bobje
  3. `./cmsdbsetup.sh`
  4. Press Enter when `[<hostname>.cms]` displays.
  5. Select select and provide all your MySQL DB info that was entered during install time. For more information, see install instructions in Chapter 3, “Installing Sentinel 6.1,” on page 29.
  6. When done, quit `cmsdbsetup.sh`
  7. `./stopservers`
  8. `./startservers`
- Re-initialize MySQL DB:
  1. Login as crystal user
  2. cd /opt/crystal_xir2/bobje
  3. `./cmsdbsetup.sh`
  4. Press Enter when `[<hostname>.cms]` displays.
  5. Select reinitialize and follow instructions.
  6. When done, quit `cmsdbsetup.sh`
  7. `./stopservers`
  8. `./startservers`

2 Make sure all CCM servers are enabled:

2a Login as crystal user

2b cd /opt/crystal_xir2/bobje

2c `./ccm.sh` -enable all

9.8 High-Performance Configurations for Crystal

Depending on the number of events that Crystal is querying, you might get an error on maximum processing time or maximum record limit. To set your server to process a higher number or an unlimited number of records you must reconfigure the Crystal Page Server. This can be done by using either the Central Configuration Manager or the Crystal Web Page.

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

1 Click Start > All Programs > BusinessObjects 11 > Crystal Reports Server > Central Configuration Manager.

2 Right-click Crystal Reports Page Server and select Stop.

3 Right-click Crystal Reports Page Server and select properties.

4 In the Command field under the Properties tab, at the end of the command line add:

```
maxDBResultRecords <value greater than 20000 or 0 to disable the default limit>
```

5 Restart Crystal Page Server.

To Reconfigure the Crystal Page Server through the Central Management Console:

1 Click Start > All Programs > BusinessObjects 11 > Crystal Reports Server > .Net Administration Launchpad. Alternatively, open a Web browser and provide the following URL:

```
http://<DNS name or IP address of your web server>:<port number>/
businessobjects/enterprise11/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, 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.

9.8.1 Reports Using Aggregation Service

To improve performance, the Top 10 reports included in the Sentinel Core Solution Pack query summary tables instead of the events table. The summary tables contain counts over time for combinations of fields in the event data. This provides a much smaller data set for certain types of queries and results in much faster queries and report run time.

The Aggregation service is responsible for populating the summary tables with summarizations of all of the events in the events table. The Aggregation service will only generate summarized data for summaries that are active. The following summaries are required by the Top 10 reports and are enabled by default:

- EventDestSummary
- EventSevSummary
- EventSrcSummary

Summaries can be activated or inactivated using the Report Data Configuration window under the Admin tab of Sentinel Control Center.

The Aggregation service also depends on the `EventFileRedirectService` component in DAS Binary to feed it the event data that it will summarize. Therefore, this component must be enabled in order for the Aggregation service to run properly. This component is enabled or disabled by modifying the "status" attribute of the `EventFileRedirectService` component in the `das_binary.xml` file to “on” or “off”. By default, this component is “on”.

NOTE: For information about EventFileRedirectService and the three aggregation summaries, see "Report Data Configuration" in Admin in the *Sentinel 6.1 User Guide*.

NOTE: Reports that query a large date range might take sometime to run. They can be scheduled instead of running interactively. For information about scheduling Crystal Reports, see Crystal Reports Server XI R2 documentation (http://support.businessobjects.com/documentation/product_guides/default.asp).

9.8.2 Report Development

The Crystal Reports Developer can be used to create or modify Crystal reports. For custom developed reports, the following is recommended:

- If the reports can utilize pre-defined aggregate tables, select the aggregate table that result in the processing of the least amount of data.
- Try to push most of the data processing to the database engine.
- To reduce processing overhead in Crystal Server, minimize the amount of data to retrieve to the Crystal Server.
- Always write reports against the database views provided by Novell instead of writing reports against the base tables.

Uninstalling Sentinel

10

To remove a Sentinel installation, uninstallers are provided for Linux, Solaris, and Windows. Several files, including log files, are preserved and can be manually removed if desired. Before performing a new installation, it is highly recommended that you perform all of the following steps to ensure there are no files or system settings remaining from a previous installation.

WARNING: These instructions involve modifying operating system settings and files. If you are not familiar with modifying these system setting and/or files, please contact your System Administrator.

10.1 Uninstalling Sentinel

10.1.1 Uninstall for Solaris and Linux

To use the Sentinel Uninstaller for Solaris and Linux:

1. Login as user root.
2. Stop the Sentinel Server.
3. Go to:

   ```
   $ESEC_HOME/_uninst
   ```

4. Provide:

   For GUI mode:

   ```
   ./uninstall.bin
   ```

   Or

   For text-based (“serial console”) mode:

   ```
   ./uninstall.bin -console
   ```

5. Select a language and click OK.
6. The Sentinel Install Shield Wizard displays. Click Next.
7. Select the components you want to uninstall and click Next.
8. Ensure any running Sentinel applications are stopped and click Next.

9 If you have selected to uninstall the Database component, you are prompted to select one of the following options:

- **Delete the entire database instance:** Removes the database instance and frees up disk space used by the database.
- **Delete only the database objects:** Removes the contents of the database except for the esecdba user. The database instance can then be repopulated using the Sentinel installer. This option does not free up disk space.

10 If you selected to Delete only the database objects, you will be prompted to provide the esecdba password. Click Next.

11 A summary of the features selected for uninstall will be displayed. Click Uninstall.

12 Click Finish.

10.1.2 Uninstall for Windows

To use the Sentinel Windows Uninstaller:

1 Login as an Administrator.

2 Stop the Sentinel Server.

3 Select Start > All Programs (Win XP) or Programs (WIN 2000)> Sentinel > Uninstall Sentinel. You can also type %Esec_home%_uninst in Start > Run, and double-click `uninstall.exe`.

4 Select a language and click OK.

5 The Sentinel 6.1 - InstallShield Wizard displays. Click Next.

6 Select the components you want to uninstall and click Next.

7 Ensure any running Sentinel applications are stopped and click Next.

8 If you have selected to uninstall the Database component, you are prompted to select one of the following options:

- **Delete the entire database:** Removes the database and frees up disk space used by the database.
- **Delete only the database objects:** Removes the contents of the database except for the esecdba user. The database can then be repopulated using the Sentinel installer. This option does not free up disk space.

9 If you have selected to uninstall the Database component, you are also prompted to select one of the following:

- **Windows Authentication:** To use Windows Authentication, you must be logged into Windows as a user that is a MS SQL Server instance System Administrator.
- **SQL Authentication:** Provide the sa (or equivalent) user's username and password.

Click Next.

10 A summary of the features selected for uninstall will be displayed. Click Uninstall.

11 Select to Reboot the system and click Finish.

10.2 Post-Uninstall

- Section 10.2.1, "Sentinel Settings," on page 141

10.2.1 Sentinel Settings

After uninstalling Sentinel, certain systems settings remain, which can be manually removed. These settings should be removed before performing a "clean" installation of Sentinel, particularly if the Sentinel uninstallation encountered errors.

NOTE: On Solaris and Linux, uninstalling Sentinel Server will not remove the Sentinel Administrator User from the operating system. You will need to manually remove that user, if desired.

Remove Sentinel System Settings on Linux

To Manually Cleanup Sentinel on Linux:

1. Login as root.
2. Ensure that all Sentinel processes are stopped.
3. Remove contents of /opt/novell/sentinel6 (or wherever the Sentinel software was installed).
4. Remove Sentinel Service startup files:

   On SLES:

   ```
   chkconfig --del sentinel
   ```

   On RedHat:

   ```
   rm /etc/rc.d/rc0.d/K02sentinel
   rm /etc/rc.d/rc3.d/S98sentinel
   rm /etc/rc.d/rc5.d/S98sentinel
   ```

5. Remove the following files in the `/etc/rc.d/rc0.d` directory, if they exist:
   - K01wizard
   - K01esdee
   - K01esyslogserver
6. Remove the following files in the `/etc/rc.d/rc3.d` directory, if they exist:
   - S99wizard
   - S99esyslogserver
   - S99esdee
7. Remove the following files in the `/etc/rc.d/rc5.d` directory, if they exist:
   - S99wizard
   - S99esyslogserver
   - S99esdee
8. Remove the following files in the `/etc/init.d` directory, if they exist:
   - sentinel
   - wizard
   - esdee
   - esyslogserver

9 Make sure nobody is logged in as the Sentinel Administrator operating system user (esecadm by default), then remove the user (and home dir) and esec group.
   - Run: `userdel -r esecadm`
   - Run: `groupdel esec`
10 Remove the directory /root/InstallShield
11 Remove the file /root/vpd.properties
12 Remove InstallShield section of `/etc/profile and /etc/.login`
13 Remove the Sentinel Oracle database. For more information, see "Remove Sentinel Oracle Database on Linux and Solaris" on page 143.
14 Restart the operating system.

Remove Sentinel System Settings on Solaris

To Manually Cleanup Sentinel on Solaris:

1 Login as root.
2 Ensure that no Sentinel processes are running.
3 Remove contents of `/opt/novell/sentinel6` (or wherever the Sentinel software was installed).
4 Remove the following files in the `/etc/rc0.d` directory, if they exist:
   - K01wizard
   - K02sentinel
   - K01esdee
   - K01esyslogserver
5 Remove the following files in the `/etc/rc3.d` directory, if they exist:
   - S98sentinel
   - S99wizard
   - S99esyslogserver
   - S99esdee
6 Remove the following files in the `/etc/init.d` directory, if they exist:
   - sentinel
   - wizard
   - esdee
   - esyslogserver
7 Remove the following files from `/usr/local/bin`, if they exist:
   - `stop_wizard.sh`
   - `restart_wizard.sh`
   - `start_wizard.sh`

8 Make sure nobody is logged in as Sentinel Administrator operating system user, then remove the user (and home dir) and esec group.
   - Run: `userdel -r esecadm`
   - Run: `groupdel esec`
9 Remove Installshield section of `/etc/profile and /etc/.login`
10 Remove the /InstallShield directory, if one exists.
11 Clean up InstallShield references in `/var/sadm/pkg.` If the following files exist. remove the following files from the `/var/sadm/pkg` directory:
   - All files that begin with IS (IS* on the command line)
   - All files that begin with ES (ES* on the command line)
   - All files that begin with MISCwp (MISCwp* on the command line)
12 Remove the Sentinel Oracle database. For more information, see "Remove Sentinel Oracle Database on Linux and Solaris" on page 143.
13 Restart the operating system.

Remove Sentinel Oracle Database on Linux and Solaris

To Manually Cleanup Sentinel Oracle Database on Linux and Solaris:

NOTE: Make sure no other applications are using this database before removing it.

1 Log in as oracle.
2 Stop Oracle Listener:
   - Run: `lsnrctl stop`
3 Stop Sentinel database:
   - Set the ORACLE_SID environment variable to the name of your Sentinel database instance (default ESEC).
   - Run: `sqlplus "/ as sysdba"`
   - At sqlplus prompt, run: `shutdown immediate`
4 Remove entry for Sentinel database in the oratab file located at:

   On Linux:

   `/etc/oratab`

   On Solaris:

   `/var/opt/oracle/oratab`
5 Remove init<your_instance_name>.ora (default `initESEC.ora`) file from the directory $ORACLE_HOME/dbs.
6 Remove entries for your Sentinel database from the following files in the $ORACLE_HOME/network/admin directory:
   - `tnsnames.ora`
   - `listener.ora`

7 Delete the database data files from the location you have selected to install them.

8 Delete the database archive files from the location you have selected to create them.

Remove Sentinel System Settings on Windows with MS SQL Server

To Manually Cleanup Sentinel on Windows:

1 Delete the folder %CommonProgramFiles%\InstallShield\Universal and all of its contents.

2 Delete the %ESEC_HOME% folder (by default: C:\Program Files\Novell\Sentinel6).

3 Right-click My Computer > Properties > Advanced tab.

4 Click the Environment Variables button.

5 If they exist, delete the following variables:

- ESEC_HOME
- ESEC_VERSION
- ESEC_JAVA_HOME
- ESEC_CONF_FILE
- WORKBENCH_HOME

6 Remove any entries in the PATH environment variable that point to the Sentinel installation.

WARNING: Do not remove paths to anything other than the old Sentinel installation. This could result in your system not functioning properly.

7 Delete all Sentinel shortcuts from the Desktop.

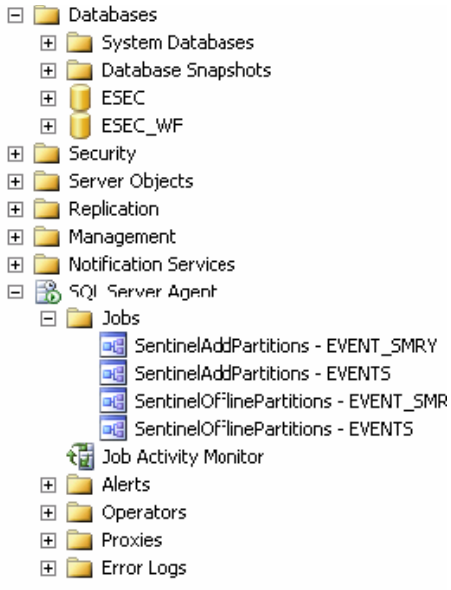
8 Delete the shortcut folder Start >Programs > Sentinel from the Start menu.

9 Restart the operating system.

To Manually Cleanup Sentinel Microsoft SQL Server database on Windows:

NOTE: Make sure no other applications are using this database before removing it.

1 Open Microsoft SQL Server Management Studio and connect to the SQL Server instance where you've installed your Sentinel database.



2 Expand the SQL Server Agent > Jobs tree and remove the Sentinel jobs.

3 Expand the Databases tree and locate your Sentinel database. There should be a Sentinel database (by default called ESEC) and an iTRAC database (by default called ESEC_WF). Right-click each and select Delete.

4 When prompted, select Yes to delete the database.

5 Expand the Security > Login tree and remove the Sentinel database users, if they exist.

- esecdba
- esecapp
- esecadm
- esecrpt

6 Delete the database archive files from the location you have selected to create them.

Pre-installation Questionnaire

A

Answering these questions can be helpful in planning your own installation or preparing for consultants to install your Sentinel system.

Pre-Install Questions

1 What is your goal or purpose of using Novell Sentinel?

1a Compliance

1b Security Event Management

1c Other_____

2 What hardware has been allocated for the installation of Sentinel? Is it in accordance with hardware specifications provided in the Sentinel Installation Guide?

3 Have you validated Sentinel hardware and operating system requirements described in the Sentinel Installation Guide against your configuration?

- OS patch levels
- Service Patches
- Hot Fixes and so on.

4 Does your DAS machine meet the necessary OS and hardware requirements?

5 What is the network architecture for the source devices with respect to the security segment where the Sentinel and Collector hardware is to be located?

NOTE: This is important to understand the hierarchy of Collector data collection and to identify any firewalls that must be penetrated to enable Collector to Sentinel communication or Sentinel to DB communication or Crystal Server to DB communication.

Provide information below (text and/or drawing) or link to information.

6 What reports do you want out of the system? This is important to ensure that your Collectors collect the correct data to be passed to the Sentinel database.

6a _____

6b _____

6c _____

6d _____

6e _____

6f _____

7 What source devices do you want to collect data from (IDS, HIDS, Routers, Firewalls and so on), event rate (EPS – events per second), versions, connection methods, platforms and patches?

Device (mfr/ model)	Event Rate (EPS)	Version	Connection Method	Platform	Patches

Can you provide sample data of what you want the Sentinel Collectors to collect and parse? Sentinel can be configured to provide the desired output based on the information provided here.

8 What security model/standards exist at your site?

- What is your stance on local accounts versus domain authentication?
  - For Windows with domain authentication, proper domain account settings must be created to ensure that Sentinel can be installed.
  - For Solaris install, this is not applicable. However, Sentinel does not support NIS.

9 What is the required data retention in terms of days?

10 Based on the data retention information and EPS, what disk size will you be using? Use 500 to 800 bytes/event for sizing estimates.

11 What event patterns do you want to identify in your data?

12 Does the current data available from your event sources support the event patterns you want to detect, or will event enrichment using the mapping service be needed?

13 If the mapping service is needed, what is the source of the enrichment data, and what key will be used to perform the mapping? How will the maps be kept up to date?

14 When a security or compliance violation is detected, what processes will be used to remediate?

Oracle Setup

B

B.1 Installing Oracle

IMPORTANT: 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.

For more information on Oracle installations and for the exact patch level that is certified or supported for Sentinel, see Chapter 2, “System Requirements,” on page 19 .

B.1.1 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.

B.1.2 Oracle 10g Installation on Red Hat Linux 4

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
```

![Bug https://bugzilla.novell.com/show_bug.cgi?id=457520]

9 Save the `.bash_profile` 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 10.2.0.1. 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.

B.1.3 Oracle 10g Installation on Solaris 10

NOTE: For more information on the procedures of setting kernel parameter settings in Solaris 10, see Section 3.4.1, “Setting Kernel Values,” on page 37.

To install Oracle 10g on Solaris 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.

B.2 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. Consult your DBA.

Table B-1 *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 B-2 *Minimum Recommended Solaris / Linux Tablespace Size*

Tablespace	Example Size	Notes
REDO	3x100M	Minimum value. This should be increased if the event rate is high.
SYSTEM	500M	Minimum value (autoextend enabled)
TEMP	1G	Minimum value (autoextend enabled)
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	15G	Minimum value if Advisor is purchased.
		For Advisor data (autoextend enabled).
SENT_ADVISORX	15G	Minimum value if Advisor is purchased.
		For Advisor index (autoextend enabled)
SENT_AUDITD	250M	Minimum value
		For Sentinel audit data (autoextend enabled)
SENT_AUDITX	250M	Minimum value
		For Sentinel audit index (autoextend enabled)
SENT_LOBS	100M	Minimum value in basic installation
		For database large objects (autoextend enabled)
	2G	Minimum value in installation if integration with identity management system is enabled.
		For database large objects (autoextend enabled)
SENT_SMRYD	3G	Minimum value
		For Aggregation, summary data (autoextend enabled)

Tablespace	Example Size	Notes
SENT_SMRYX	2G	Minimum value
		For Aggregation, summary index (autoextend enabled)
SYSAUX	100M	Minimum value
		For Oracle 10g auditing (not Sentinel-specific)
		Required for Oracle 10g only

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.

For more information on database installation for installing into an existing database, see Chapter 3, "Installing Sentinel 6.1," on page 29.

Sentinel with Oracle Real Application Clusters

C

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.

C.1 Configuring the Oracle RAC database

To configure the Oracle RAC database:

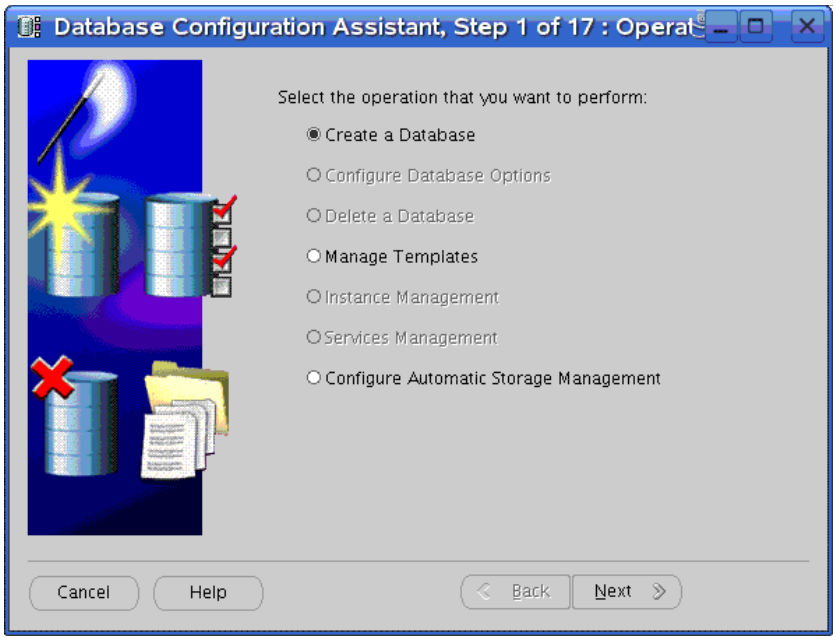
- Create the RAC database using Oracle Database Configuration Assistant utility
- Create the required Sentinel tablespaces to contain Sentinel data
- Create the Sentinel schema owner ESECDBA
- Install Sentinel database
- Install remaining Sentinel components
- Configure the connection properties file

C.1.1 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.

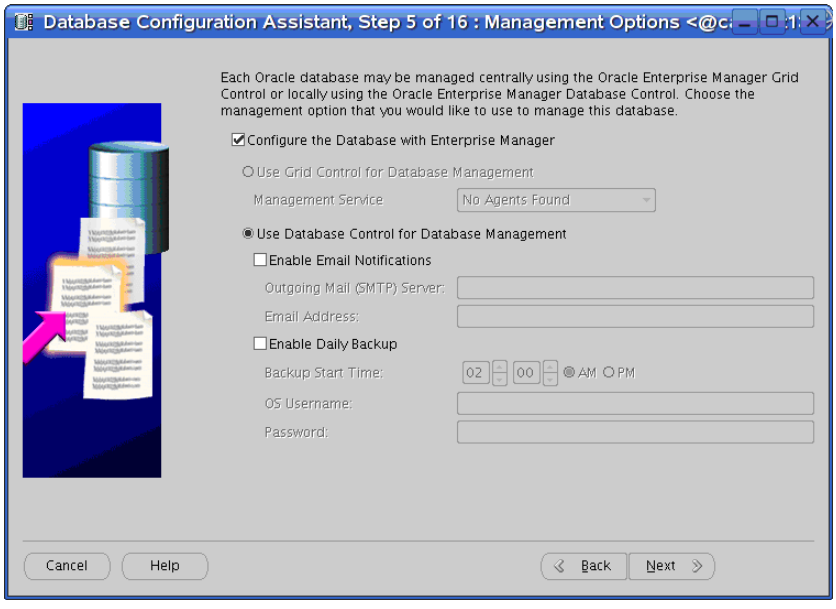


3 To select all nodes to create cluster database, click Select All. Click Next.

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.

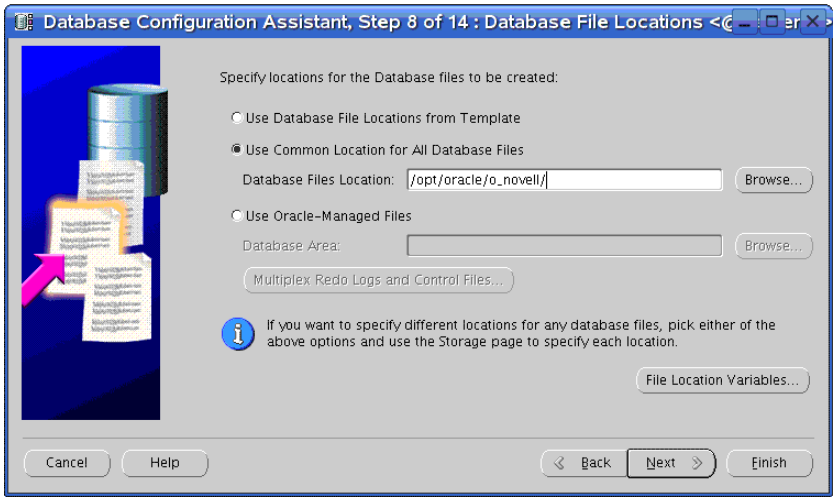
6 The default management option selected to manage this database is Configure the Database with Enterprise Manager. Click Next.



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.



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.

C.1.2 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.

Table C-1 *Minimum Recommended Tablespace size*

Tablespace	Example Size	Notes
REDO	3 x 100M	This is a minimum value. You should create larger redo logs if the event rate is high.
SYSTEM	500M	Minimum value (autoextend enabled)
TEMP	1G	Minimum value (autoextend enabled)
UNDO	1G	Minimum value (autoextend enabled)
ESENTD	5G	Minimum value
		This for event data (autoextend enabled)

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	15G	Minimum value if Advisor is purchased
		For Advisor data (autoextend enabled)
SENT_ADVISORX	15G	Minimum value if Advisor is purchased
		For Advisor index (autoextend enabled)
SENT_AUDITD	250M	Minimum value
		For Sentinel audit data (autoextend enabled)
SENT_AUDITX	250M	Minimum value
		For Sentinel audit index (autoextend enabled)
SENT_LOBS	100M	Minimum value in basic installation
		For database large objects (autoextend enabled)
	2G	Minimum value in installation if integration with identity management system is enabled.
		For database large objects (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)

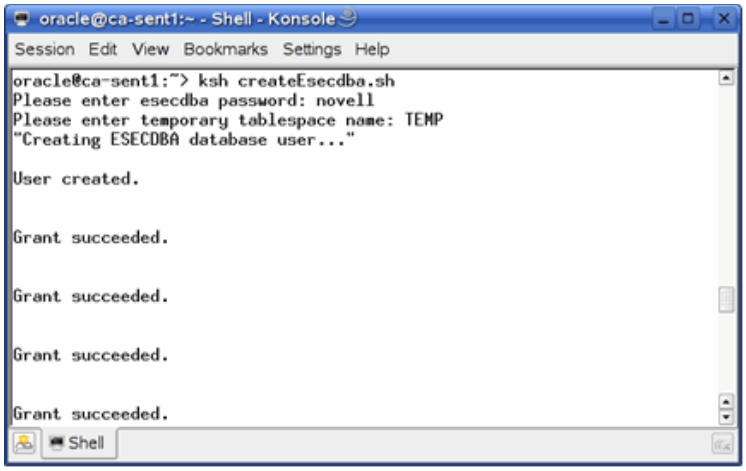
C.1.3 Creating ESECDBA

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.



C.2 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 Chapter 3, “Installing Sentinel 6.1,” on page 29.

C.3 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=28,600,1012,1014,1033,1034,1035,1089,1090,1092,1094,2396,31
06,3111,3113,3114
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.properties
```

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=""$(ESEC_JAVA_HOME)/java" -server -
Dsrv_name=DAS_Query
-Xmx256m -Xms85m -XX:+UseParallelGC -Xss136k -Xrs
-Duser.language=en -Dfile.encoding=UTF8
-Desecurity.dataobjects.config.file=/xml/BaseMetaData.xml,
/xml/WorkflowMetaData.xml
-Djava.util.logging.config.file=../config/das_query_log.prop
-Djava.security.auth.login.config=../config/auth.login
-Djava.security.krb5.conf=../config/krb5.conf
-Desecurity.execution.config.file=../config/execution.properties -
Dcom.esecurity.configurationfile=../config/configuration.xml
-Desecurity.connect.config.file=../config/RACconnect.properties
-jar ../lib/ccsbase.jar ..//config//das_query.xml" min_instances="1"
name="DAS_Query" post_startup_delay="20" type="container"
working_directory="$(ESEC_HOME)/data" />
```

5 Restart the Sentinel services so the database connection changes will take effect.

C.4 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**

C.5 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)
     )
   )
)
```

Documentation Updates

D

This section contains information about documentation content changes made to the *Installation Guide for Novell Sentinel 6.1*. If you are an existing user, review the change entries to readily identify modified content. If you are a new user, simply read the guide in its current state.

Refer to the publication date that appears on title page to determine the release date of this guide. For the most recent version of the *Novell Sentinel Installation Guide*, see the Novell Sentinel 6.1 documentation Web site (http://www.novell.com/documentation/sentinel61/).

In this section, content changes appear in reverse chronological order, according to the publication date. Within a dated entry, changes are grouped and sequenced, according to where they appear in the document itself. Each change entry provides a link to the related topic and a brief description of the change.

This document was updated on the following dates:

- Section D.1, "March 2009," on page 165
- Section D.2, "May 2009," on page 166

D.1 March 2009

Updates were made to the following section. The changes are explained below:

Table D-1 *Updates*

Location	Changes
Section 2.1, "Supported Software," on page 19	Updated Table 2-1 on page 19 with Microsoft SQL Server 2008 version information. Fixed Bug#455532 (https://bugzilla.novell.com/show_bug.cgi?id=455532).
Section 2.1, "Supported Software," on page 19	Updated Table 2-1 on page 19 to include that Oracle 10g can be installed only on SLES 9. Fixed Bug#455530 (https://bugzilla.novell.com/show_bug.cgi?id=455530).
Chapter 5, "Testing the Installation," on page 69	Added Section 5.2, "Testing the Advisor Installation," on page 76.
Chapter 6, "Adding Sentinel Components," on page 79	Incorporated the edit comments for the entire chapter.
Section 6.2, "Installing Additional Load Balancing Nodes," on page 79	Updated the section to add instructions for creating a Second DAS_Binary Server. Fixed Bug#474575 (https://bugzilla.novell.com/show_bug.cgi?id=474575).

Location	Changes
◆ Section 8.9.3, “Publishing Report Templates – Central Management Console,” on page 116 ◆ Section 8.9.5, “Configuring Reports Permissions,” on page 117 ◆ Section 8.10.1, “Increasing Crystal Reports Server Report Refresh Record Limit,” on page 120 ◆ Section 9.8, “High-Performance Configurations for Crystal,” on page 136	Updated the guide to add the correct Crystal URL.. Fixed Bug#468138 (https://bugzilla.novell.com/show_bug.cgi?id=468138).
◆ Section 9.3.1, “Publishing Report Templates using Solution Manager,” on page 128 ◆ Section 8.9.1, “Publishing Report Templates using Solution Manager,” on page 113	Updated the section to include the details about supporting files and documentation to publish Solution Pack or Collector Pack in the Crystal Reports server. Added a screenshot of the Solution Manager with the Core Solution Pack open. Fixed Bugs#479676 (https://bugzilla.novell.com/show_bug.cgi?id=479676).
Section B.1.2, “Oracle 10g Installation on Red Hat Linux 4,” on page 150	Updated Step 8 on page 151 to add the correct path. Fixed Bug#457520 (https://bugzilla.novell.com/show_bug.cgi?id=457520).
Section B.1.2, “Oracle 10g Installation on Red Hat Linux 4,” on page 150	Updated the list of packages. Fixed Bug#457522 (https://bugzilla.novell.com/show_bug.cgi?id=457522)
Entire Book	Removed all occurrences of Oracle 9 in the guide. Fixed Bug#451627 (https://bugzilla.novell.com/show_bug.cgi?id=451627).

D.2 May 2009

Updates were made to the following section. The changes are explained below:

Table D-2 *Updates*

Location	Changes
Section 3.6, “Custom Installation,” on page 43	Added a note to fix Bug#488374 (https://bugzilla.novell.com/show_bug.cgi?id=488374)