Sentinel™ 5

Install Guide v5.1.1

- Linux
- Solaris
- Windows

Volume I of V

March 2006
www.esecurity.net

Preface

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

e-Security Technical documentation is broken down into five different volumes. They are:

- Volume I – Sentinel™ 5 Install Guide
- Volume II – Sentinel™ 5 User's Guide
- Volume III – Sentinel™ 5 Wizard User's Guide
- Volume IV – Sentinel™ 5 User's Reference Guide
- Volume V – Sentinel™ 3rd Party Integration

Volume I – Sentinel Install Guide

This guide explains how to install:

- Sentinel Server
- Sentinel Console
- Sentinel Correlation Engine
- Sentinel Crystal Reports
- Wizard Agent Builder
- Wizard Agent Manager
- Advisor

Volume II – Sentinel User's Guide

This guide discusses:

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

Volume III – Wizard User's Guide

This guide discusses:

- Wizard Agent Builder Operation
- Wizard Agent Manager
- Agents
- Wizard Host Management
- Building and maintaining agents

Volume IV - Sentinel User's Reference Guide

This guide discusses:

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

Volume V - Sentinel 3rd Party Integration Guide

- Remedy
- HP OpenView Operations
- HP Service Desk

Chapter 1 - Introduction

This guide will walk you through a basic installation. The Sentinel™ 5 User's Guide has more detailed architecture, operation and administrative procedures.

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

Conventions Used

Notes and Cautions

NOTE: Notes provide additional information that may be useful.

CAUTION: Cautions provide additional information that may keep you from performing damage or loss of data to your system.

Commands

Commands appear in courier font. For example:

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

Sentinel 5 Overview

Sentinel 5 raises the bar on what you should demand from a security information management solution. Sentinel 5 includes standard security information management capabilities such as collect, aggregate, correlate, and display event data. It also enables you to make decisive, appropriate responses to incidents by automating and enforcing incident identification and resolution processes.

The Sentinel 5 key features are iTRAC™, Active Views™ and iSCALE™. These enable you to manage, measure, and comply more effectively. With Sentinel 5, you can:

- Gain visibility and control required to manage your security environment more cost-effectively
- Detect and resolve incidents faster, while reducing operational costs
- Deliver appropriate reports and metrics to continually assess your security and compliance posture

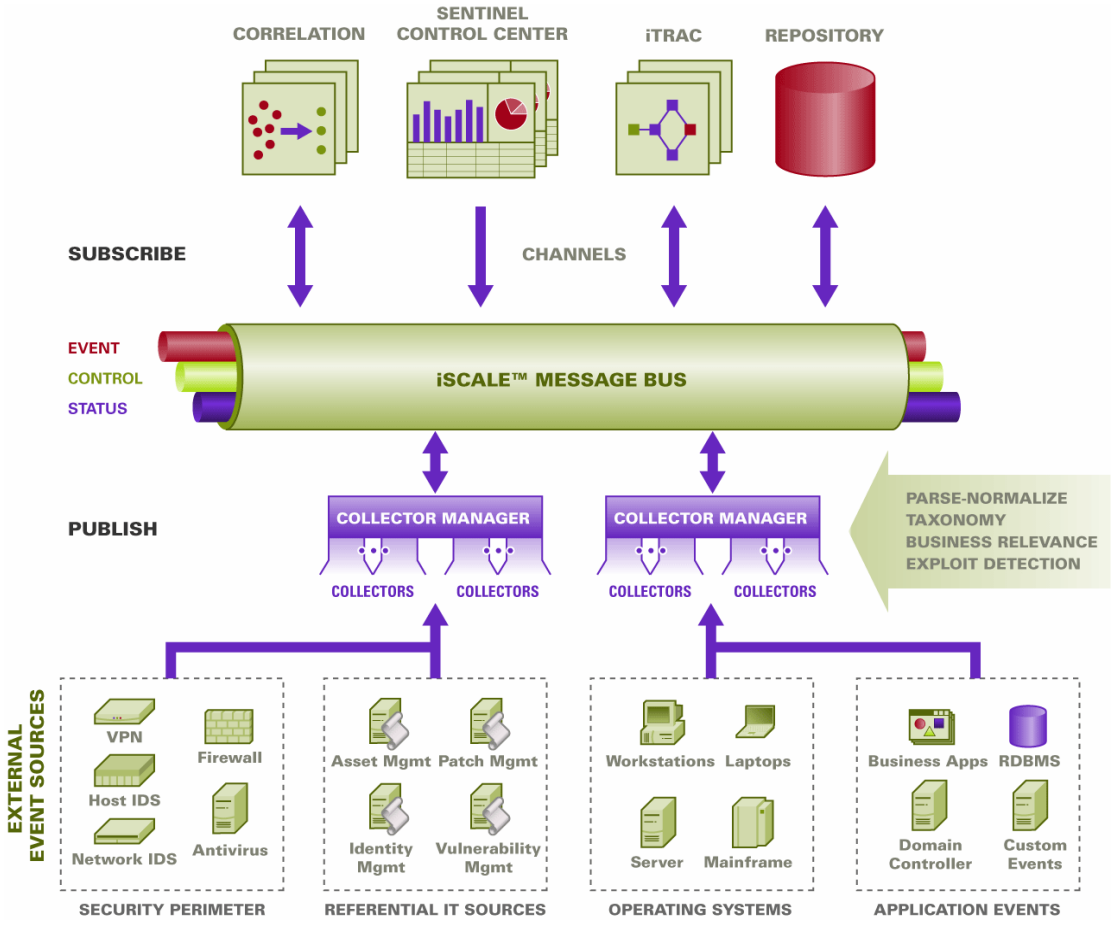
- Achieve and monitor Compliance with internal policies and government regulations.

Get more done with current resources by eliminating manual processes

Sentinel 5 is composed of multiple components that work together to comprise the leading solution on the market:

- Sentinel Control Center
- Sentinel Server
- Sentinel Advisor
- Sentinel Data Manager
- Sentinel Wizard
  - Wizard Agent Builder
  - Wizard Agent Manager
  - Wizard Engine

The following is a **conceptual architecture** of the Sentinel 5 product and it illustrates the components of Sentinel involved in performing Security Management.



Sentinel Product Modules

Sentinel 5 is composed of three primary modules – Sentinel Control Center, Sentinel Wizard (Agent Builder and Agent Manager) and Sentinel Advisor.

Sentinel Control Center

The Sentinel Control Center provides an integrated security management dashboard that enable 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
- Admin – Correlation rules definition and management
- iTRAC – Process management for documenting, enforcing and tracking incident resolution processes.
- Reporting – Historical reports and metrics

Sentinel Wizard

Sentinel Wizard 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. In any configuration, there may be one or more Wizards deployed, providing customers with the ability to deploy product components into their infrastructure based on their network topology.

Wizard enables you to efficiently develop and customize agents. This allows Sentinel to collect data from numerous different devices in an enterprise. These devices consist of (but not limited to):

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

Key components of the Sentinel Wizard include:

- Agent – a receptor that collects and normalizes unprocessed (raw) events from security devices and systems.
- Agent Engine – component that processes the template logic for each port.
- Agent Manager – the back-end component that manages agents and system status messages and performs global filtering of events.
- Agent Builder – a standalone application that enables you to build and configure agents.

Sentinel Advisor

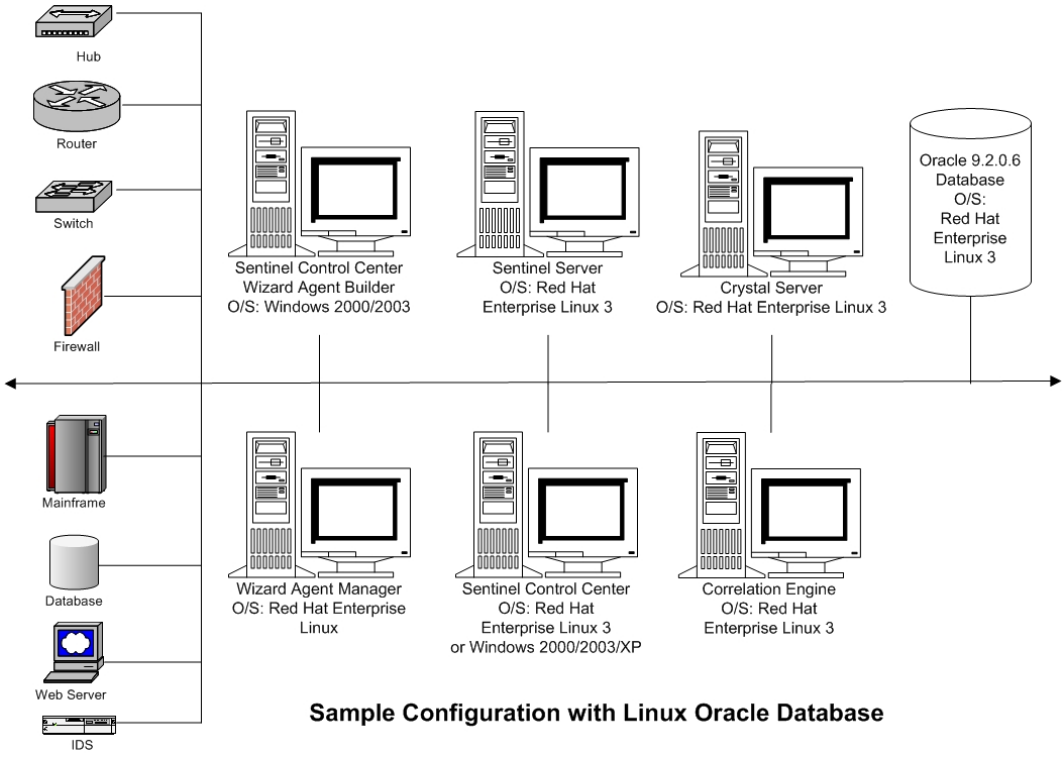
Sentinel Advisor is an optional add-on module that cross-references Sentinel's real-time alert data with known vulnerabilities and remediation information.

Typical Configuration

The following are typical configurations of the Sentinel 5 product and illustrates how Security Management is done. Your implementation may be different depending on where and how you do your installation.

NOTE: For more specific information regarding EPS (Events per Second), Platforms, RAM, HDD space requirements and CPU, see Chapter 2 – Best Practices.

Supported Platforms for Sentinel Server on Linux



Sample Configuration with Linux Oracle Database

Sentinel Server		
OS	**Version**	**Patch Level**
Red Hat Enterprise Linux	3	Update 5 ES (x86)

Database		
Database	**Version**	**Patch Level**
Oracle 64-bit Enterprise Edition	9i	9.2.0.6 2617419

NOTE: For more information regarding Critical Patch 2617419, see the Oracle website and the e-Security Customer Portal.

Sentinel Control Center (User Interface)		
OS	**Version**	**Patch Level**
Red Hat Enterprise Linux	3	3 Update 5 ES (x86)
Windows	XP	SP1
Windows	2000	SP4
Windows	2003	SP1

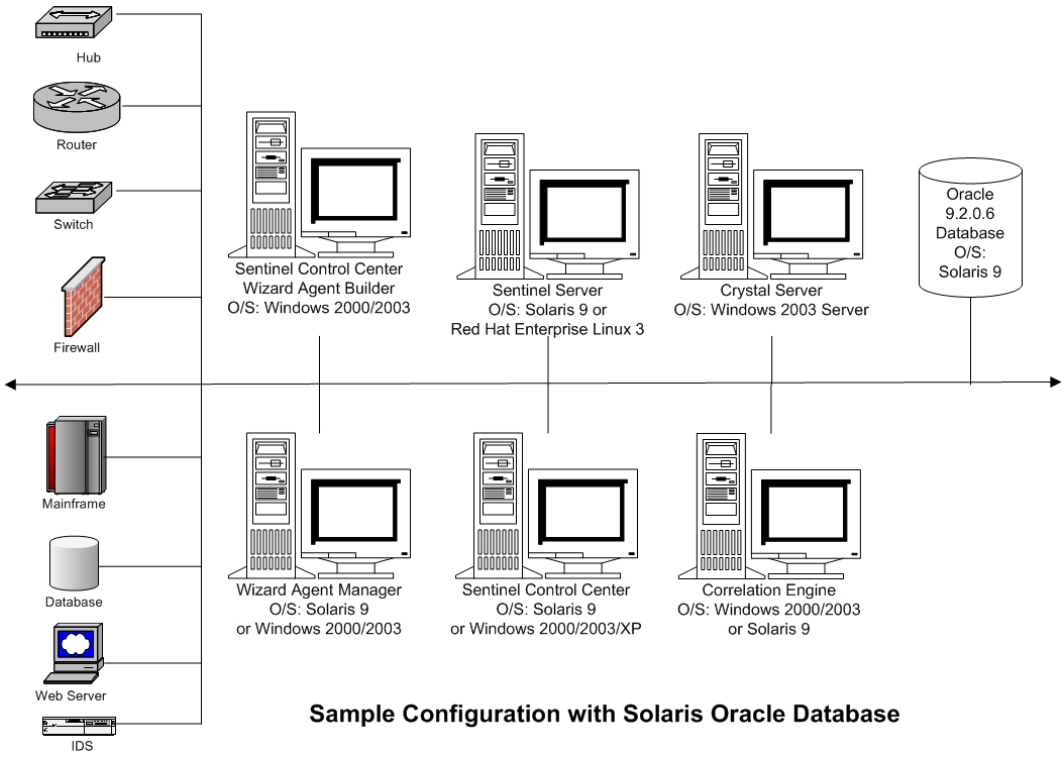
Agent Builder		
OS	**Version**	**Patch Level**
Windows	2000	SP4
Windows	2003	SP1

Agent Manager		
OS	**Version**	**Patch Level**
Red Hat Enterprise Linux	3	3 Update 5 ES (x86)

Crystal Server (Choice of two versions)			
Crystal Version	**OS**	**OS Version**	**OS Patch Level**
Crystal BusinessObjects Enterprise™ 11	Red Hat Enterprise Linux	3	3 Update 5 ES (x86)
Crystal BusinessObjects Enterprise™ 11	Windows	2003	SP1

NOTE: Sentinel 5 does not support Crystal XI on Windows® 2000 Server.

Supported Platforms for Sentinel Server on Solaris



Sample Configuration with Solaris Oracle Database

Sentinel Server		
OS	**Version**	**Patch Level**
Solaris 64-bit Enterprise Edition	9	Solaris 9 Recommended Patch Cluster DATE: May/03/05

Database		
Database	**Version**	**Patch Level**
Oracle 64-bit	9i	▪ 9.2.0.6 ▪ 2617419

NOTE: For more information regarding Critical Patch 2617419, see the Oracle website and the e-Security Customer Portal.

Sentinel Control Center (User Interface)		
OS	**Version**	**Patch Level**
Solaris 64-bit	9	Solaris 9 Recommended Patch Cluster DATE: May/03/05
Windows	XP	SP1
Windows	2000	SP4
Windows	2003	SP1

Agent Builder		
OS	**Version**	**Patch Level**
Windows	2000	SP4
Windows	2003	SP1

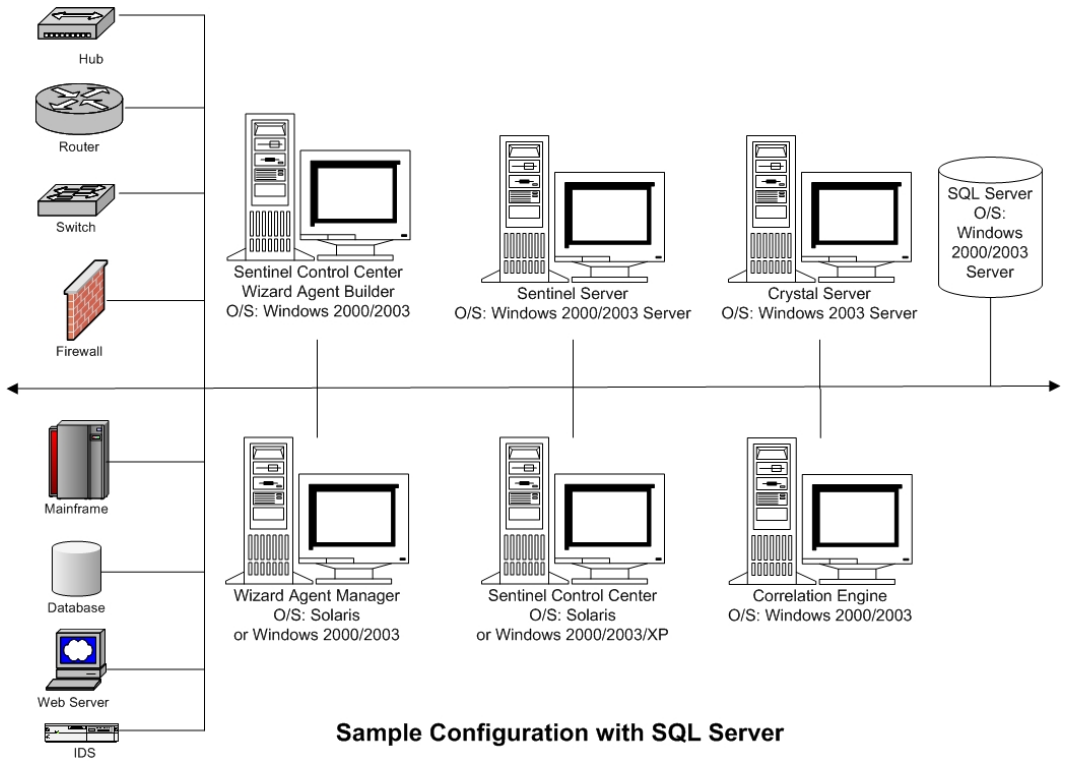
Agent Manager		
OS	**Version**	**Patch Level**
Solaris 64-bit	9	Solaris 9 Recommended Patch Cluster DATE: May/03/05
Windows	2000	SP4
Windows	2003	SP1
Red Hat Enterprise Linux	3	3 Update 5 ES (x86)

Crystal Server			
Crystal Version	**OS**	**OS Version**	**OS Patch Level**
Crystal BusinessObjects Enterprise™ 11	Windows	2003	SP1

NOTE: Crystal Reports v9 is supported on Sentinel v5.1 and earlier as well as Sentinel v5.1.1 SP1 and later. It is not supported on Sentinel v5.1.1 without SP1. If you are using Crystal Reports v9 and Sentinel v5.1.1, you must apply Sentinel v5.1.1 Service Pack 1.

NOTE: Sentinel 5 does not support Crystal XI on Windows® 2000 Server.

Supported Platforms for Sentinel Server on Windows



Sample Configuration with SQL Server

Sentinel Server		
OS	**Version**	**Patch Level**
Windows	2000 Server - Enterprise Edition	SP4
Windows	2003 Server - Enterprise Edition	SP1

Database		
Database	**Version**	**Patch Level**
SQL Server	2000	SP3a
SQL Server	2005 (Sentinel v5.1.1 SP1 and later)	

Sentinel Control Center (User Interface)		
OS	**Version**	**Patch Level**
Windows	XP	SP1
Windows	2000	SP4
Windows	2003	SP1

Agent Builder		
OS	**Version**	**Patch Level**
Windows	2000	SP4
Windows	2003	SP1

Agent Manager		
OS	**Version**	**Patch Level**
Solaris 64-bit	9	Solaris 9 Recommended Patch Cluster DATE: May/03/05
Windows	2000	SP4
Windows	2003	SP1
Red Hat Enterprise Linux	3	3 Update 5 ES (x86)

Crystal Server			
Crystal Version	**OS**	**OS Version**	**OS Patch Level**
Crystal BusinessObjects Enterprise™ 11	Windows	2003	SP1

NOTE: Crystal Reports v9 is supported on Sentinel v5.1 and earlier as well as Sentinel v5.1.1 SP1 and later. It is not supported on Sentinel v5.1.1 without SP1. If you are using Crystal Reports v9 and Sentinel v5.1.1, you must apply Sentinel v5.1.1 Service Pack 1.

NOTE: Sentinel 5 does not support Crystal XI on Windows® 2000 Server.

Other e-Security References

The following manuals are available with the e-Security install CDs.

- Sentinel™ Installation Guide
- Sentinel™ User's Guide
- Sentinel™ Wizard User's Guide
- Sentinel™ User's Reference Guide
- Sentinel™ 3rd Party Integration Guide
- Release Notes

Contacting e-Security

- For Technical Support, email at support@esecurity.net
- For information, email at info@esecurity.net
- Website: http://www.esecurity.net
- For 24x7 support, call Technical Support directly at 800-474-3131

Chapter 2 – Best Practices

This chapter discusses best practices and recommendations to best utilize Sentinel. Topics include:

Installation Best Practices

The following are the performance ratings for specific attributes of Sentinel.

Attribute	Rating	Comments
▪ EPS for event DB insertion	1250	Insert is affected by correlation rules and the mapping service.
▪ EPS for each Agent Manager	350	
▪ EPS per agent (Checkpoint, Win2K, etc...)	300	
▪ Maximum number of Agents supported per Agent Manager	10	
▪ Maximum number of Agent Managers per sentinel	20	
▪ How many rules deployed per correlation Engine	20-80	Low EPS (150 EPS) = 80 High EPS (1250 EPS) = 20
▪ How many Active Views™ per Sentinel	35 - 50	
▪ Maximum number of simultaneous users	20	
▪ Maximum number of views per Sentinel Control Center	10	
▪ Maximum number of maps per Sentinel	10	

Attribute	Rating	Comments
▪ Maximum size of each Map	10 MB	
▪ Maximum number of rows per map	350k	

CPU reference specification is based on:

- Windows - 3.2 GHz Xeon
- Solaris - 1.1 GHz Sparc-3
- Linux - 3.2 GHz Xeon

Configuration is for the following operating systems:

- Windows 2000 Server with SP4
- Windows 2003 Server with SP1
- Solaris 9 with patches with Generic_112233-11 version of recommended patch cluster
- Red Hat Enterprise Linux 3 Update 5 ES (x86)

Database is one of the following:

- MSSQL 2000 with SP3a
- Oracle 9i Enterprise Edition 9.2.0.6 with partitioning

Simple – Standalone (demo use) Configuration

This installation installs all components (including the database) on a single platform. This is primarily for demonstration purposes. This is not recommended for actual use. The hardware requirements are:

Components	Minimum		Recommended	
	RAM (GB)	CPU	RAM (GB)	CPU
Machine 1 ▪ All Sentinel components ▪ Agent Manager ▪ Agents ▪ Database ▪ Disk Array For Windows: ▪ Crystal Server ▪ Agent Builder For Linux: ▪ Crystal Server	2	2	4	2
Machine 2 (for UNIX installs only) For Solaris: ▪ Crystal Server ▪ Agent Builder For Linux: ▪ Agent Builder	1.0	1	2.0	2

Proof of Concept (POC) – Standalone Configuration

This installation installs all components, with the exception of the database, on a single platform. This configuration is typically used for proof of concepts in order to test the functionality under normal loads. In this case, the database is on a separate machine from the rest of Sentinel.

Components	Minimum		Recommended	
	RAM (GB)	CPU	RAM (GB)	CPU
Machine 1 ▪ All Sentinel components ▪ Agent Manager ▪ Agents For Windows: ▪ Crystal Server ▪ Agent Builder For Linux: ▪ Crystal Server	4.0	2	4	4
Machine 2 ▪ Database ▪ Disk Array	4	2	4	4
Machine 3 (for UNIX installs only) For Solaris: ▪ Crystal Server ▪ Agent Builder For Linux: ▪ Agent Builder	2.0	2	4.0	2

Production – Distributed Configuration

A Distributed Configuration is a custom installation that is intended for Standard and Enterprise Systems.

Due to Sentinel having 8 separate components in addition to Crystal Reports, there are numerous different configurations that can be built. The following addresses two different configurations.

Due to databases being IO dependent, it is recommended to have your database on a separate machine. The DB server will require a high speed storage array that will meet the IO requirement based on the event insertion rates.

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

Production – Distributed Configuration (Option 1)

4 Machine Configuration

Components	Minimum		Recommended	
	RAM (GB)	CPU	RAM (GB)	CPU
Machine 1 ▪ Base Components ▪ Correlation Engine ▪ DAS ▪ iSCALE (Message Bus) ▪ Advisor	4.0	4	8.0	8
Machine 2 ▪ Agent Manager ▪ Agents	1.0	2	2.0	2
Machine 3 ▪ Crystal Server	2.0	2	4.0	4
Machine 4 ▪ Database ▪ Disk Array	4	4	16	8

Production – Distributed Configuration (Option 2)

5 Machine Configuration

Components	Minimum		Recommended	
	RAM (GB)	CPU	RAM (GB)	CPU
Machine 1 ▪ Base Components ▪ DAS ▪ iSCALE (Message Bus) ▪ Advisor	4.0	4	8.0	8
Machine 2 ▪ Correlation Engine	1.0	2	2.0	2
Machine 3 ▪ Agent Manager ▪ Agents	1.0	2	2.0	2
Machine 4 ▪ Crystal Server	2.0	2	4.0	4
Machine 5 ▪ Database ▪ Disk Array	4	4	16	8

Patch Support Policy

e-Security will certify operating systems and database patches within 60 days of their release.

Hardware Recommendations

Sentinel Server Correlation Engine			
EPS	**RAM**	**Space**	**CPU**
250	2 GB	72 GB	Windows - 4 x 3.0 GHz Xeon Linux - 4 x 3.0 GHz Xeon Solaris - V280 2 x 1.1 GHz Ultra Sparc III
500	4 GB	72 GB	Windows - 4 x 3.0 GHz Xeon Linux - 4 x 3.0 GHz Xeon Solaris - V480 4 x 1.1 GHz Ultra Sparc III
1000+	8 GB	72 GB	Windows - 8 x 3.0 GHz Xeon Linux - 4 x 3.0 GHz Xeon Solaris - V880 8 x 1.1 GHz Ultra Sparc III

Agent Manager			
EPS	**RAM**	**Space**	**CPU**
250	2 GB	36 GB	Windows - 2 x 3.0 GHz Xeon Linux - 2 x 3.0 GHz Xeon Solaris - V280 2 x 1.1 GHz Ultra Sparc III
500	4 GB	36 GB	Windows - 4 x 3.0 GHz Xeon Linux - 4 x 3.0 GHz Xeon Solaris - V480 4 x 1.1 GHz Ultra Sparc III
1000+	8 GB	36 GB	Windows - 8 x 3.0 GHz Xeon Linux - 8 x 3.0 GHz Xeon Solaris - V880 8 x 1.1 GHz Ultra Sparc III

Sentinel Control Center Agent Builder (Windows only) Sentinel Data Manager		
RAM	**Space**	**CPU**
2 GB	15 GB	Windows 2000 or 2003 - 2 x 3.0 GHz Xeon Windows XP (Control Center only) - 2 x 3.0 GHz Xeon Linux - 2 x 3.0 GHz Xeon Sun Solaris 9 - V280 2 x 1.1 GHz Ultra Sparc III

Database			
EPS	**RAM**	**Space**	**CPU**
250	8 GB	500 GB	Windows - 4 x 3.0 GHz Xeon Linux - 4 x 3.0 GHz Xeon Solaris - V480 4 x 1.1 GHz Ultra Sparc III
500	12 GB	1.0 TB	Windows - 4 x 3.0 GHz Xeon Linux - 4 x 3.0 GHz Xeon Solaris - V880 6 x 1.1 GHz Ultra Sparc III
1000+	16 GB	2.0 TB	Windows - 8 x 3.0 GHz Xeon Linux - 8 x 3.0 GHz Xeon Solaris - V880 8 x 1.1 GHz Ultra Sparc III

Disk Array Configuration

The e-security Sentinel 5 server in a production setting requires a high speed disk array for the Database and sentinel hosts. This section will try to cover

typical disk (RAID) configuration recommendations. The following are the main components that are affected by the performance of the Disk hardware:

- Database component (MSSQL/Oracle): The Events per Second (EPS) rate and Query (Quick Query / Crystal performance) features are impacted.
- DAS-RT (Data Access Service Real Time Component): Active View feature is impacted.
- DAS-Aggregation: The number of summaries that can be activated are impacted.

Minimum Requirement for Enterprise Install (1000 EPS or more)

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

- RAID Group 1 – DB (Data, Indexes, transaction logs, etc)
- RAID Group 2 – Sentinel Server DAS (Data dir, Temp DIR*)
- Minimum disks: 13 per RAID Group
- Disk Type: 12k+ RPM, Fiber Channel or SCSI
- LUN 1 (RAID Group 1): 5GB – 144GB+ per disk
- LUN 2 (RAID Group 2): 5GB – 144GB+ per disk

Optimal configuration

For an optimal performance and redundancy configuration a RAID 1+0 can be utilized with the above same settings. However, it may be required to have additional RAID Groups and LUN's following the same guidelines as above to achieve more parallelism and IO for certain databases.

NOTE: See the section Installing Sentinel for instructions on how to point the DAS TEMP DIR to a different location.

Example Storage Configuration for a MS SQL Install

This example uses EMC^2 CLARiiON storage subsystem with:

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

RAID Groups

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

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

LUN Assignments

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

Storage Groups

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

Example Storage Configuration for a Oracle Configuration

volume 1	RAID 1	Oracle home
volume 2	RAID 1	redo log member a
volume 3	RAID 1	redo log member b
volume 4	RAID 0+1 or RAID 5	undo and temp tablespaces
volume 5	RAID 0+1 or RAID 5	e-Security data tablespaces
volume 6	RAID 0+1 or RAID 5	e-Security index tablespaces
volume 7	RAID 0+1 or RAID 5	e-Security summary data tablespaces
volume 8	RAID 0+1 or RAID 5	e-Security summary index tablespaces
volume 9	RAID 1	archive log files

Network Configuration

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

Sentinel Control Center, Agent Builder and Agent Service (Agent Manager): These are required to be connected to Sentinel Server via at least 100Mbit-FULL DUPLEX switches.

Installation of Oracle and MS SQL Server

NOTE: Most database install parameters can be changed after database install via Enterprise Manager or command line.

1. For performance reasons, depending if you are installing in RAID and if your RAID environment allows, the following logs should be installed on the fastest write disk you have available.
   - Redo Log (Oracle)
   - Transaction Log (MS SQL)
2. To more accurately determine your database size, you may want to initially start with a small database and extend your database size after having the system up and running for a short period. This will allow you observe your database growth based on your event insertion rate to determine your system database space requirements.
3. For recovery purposes, it is recommended to perform regularly scheduled backups of your database.
4. For Oracle installations, the Sentinel installer by default, turns off Archive Logging. For database recovery purposes, it is highly recommended that after you 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 will stop accepting events when the archive log destination reaches full capacity.
5. For performance reasons, the storage locations should point to different locations to avoid IO contentions.
   - Data directory
   - Index directory
   - Summary Data directory
   - Summary Index directory
   - Log Directory (MS SQL Only)
   - Temporary and Undo Tablespace directory (Oracle Only)
   - Redo Log Member A directory (Oracle Only)
   - Redo Log Member B directory (Oracle Only)

e-Security Database Patches

For MS SQL only, when Sentinel Database patches are applied, the installer will only add new indexes to *_P_MAX only. Already existing partitions will not be updated. You will have to manually add indexes to already existing partitions if

you want the new indexes to improve performance for queries running against existing partitions.

Recommended UNIX Kernel Settings

The following are suggested minimum values. For more information see your system and Oracle documentation.

Minimum Kernel Parameter Values for Linux

For more information on how to view and set kernel parameters on Linux, see Chapter 3 – Installing Sentinel 5 for Oracle – Oracle Pre-install on Linux.

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

Minimum Kernel Parameter Values for Solaris

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

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

Configuration Parameters When Creating Your Own Database Instance

The following is the recommended settings when creating your own database instance. Your settings may vary depending on your system configuration and requirements.

In the Oracle instance you will need to create:

- Oracle initialization parameters (these values are dependant on your system size and configuration)
- e-Security required tablespaces

Configuration Parameters for Solaris and Linux

Minimum Recommended Configuration Parameters	
Parameters	**Size (bytes or otherwise specified)**
db_cache_size	1 GB
java_pool_size	33,554,432
large_pool_size	8,388,608

Minimum Recommended Configuration Parameters	
Parameters	**Size (bytes or otherwise specified)**
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

Minimum Recommended Tablespace Size		
Tablespace	**Example Size**	**Notes**
REDO	3 x 100M	▪ This is a minimum value. You should create larger redo logs if you have a high EPS.
SYSTEM	500M	▪ Minimum value
TEMP	1G	▪ Minimum value
UNDO	1G	▪ Minimum value
ESENTD	5G	▪ Minimum value ▪ This for event data
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
ESENTX2	500M	▪ Minimum value ▪ Index for configuration, assets, vulnerability and associations (autoextend enabled)
SENT_ADVISORD	200M	▪ Minimum value ▪ For Advisor data (autoextend enabled)
SENT_ADVISORX	100M	▪ Minimum value ▪ For Advisor index (autoextend enabled)
SENT_LOBS	100M	▪ Minimum value ▪ For database large objects (autoextend enabled)
SENT_SMRYD	3G	▪ Minimum value ▪ For Aggregation, summary data
SENT_SMRYX	2G	▪ Minimum value ▪ For Aggregation, summary index

Installing Sentinel

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

1. When performing a clean installation of e-Security after having a previous version of e-Security installed, it is HIGHLY recommended that you remove certain files and system settings from the previous installation. Not removing these files could cause a new, clean installation to fail. This should be done on every machine you are performing a clean installation. For more information about which files to remove, see Appendix E.
2. The performance of Active Views and Mapping can improve dramatically by pointing the temp directory of the DAS_RT and DAS_Query processes to a fast disk (e.g. – a disk array). To point the temp directory of these processes to a fast disk, do the following on the machine where DAS is installed:
   a. Create a directory on the fast disk to place the temp files. If on UNIX, this directory must owned and writable by the user esecadm and the group esec.
   b. Make a backup copy of the file %ESEC_HOME%\configuration.xml.
   c. Open the file %ESEC_HOME%\configuration.xml in a text editor.
   d. For the DAS_RT and DAS_Query processes, add the JVM argument java.io.tmpdir, setting it to the directory you just created.
   e. To make this change to the DAS_RT process, look for the line containing the text

      ```
      -Dsrv_name=DAS_RT
      ```

      and add the argument

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

      right after it. An example of what the line should like (your –Xmx, -Xms, and –XX args may look different) is:

      ```
      <process component="DAS"
         image="&quot;$(ESEC_JAVA_HOME)/java&quot; -server
         -Dsrv_name=DAS_RT -Djava.io.tmpdir=D:\Temp2 -
         Xmx310m -Xms103m -XX:+UseParallelGC -Xss128k -Xrs
         -
         Desecurity.dataobjects.config.file=/xml/BaseMetaD
         ata.xml -
         Djava.util.logging.config.file=../config/das_rt_l
         og.prop -
         Dcom.esecurity.configurationfile=../../configurat
         ion.xml -
         Djava.security.auth.login.config=../config/auth.l
         ogin -
         Djava.security.krb5.conf=../../lib/krb5.conf -jar
         ../../lib/ccsbase.jar ..//config//das_rt.xml"
      ```

```
min_instances="1" post_startup_delay="5"
shutdown_command="cmd //C
&amp;quot;$(ESEC_HOME)/sentinel/scripts/stop_containe
r.bat&amp;quot; localhost DAS_RT"
working_directory="$(ESEC_HOME)/sentinel/bin"/>
```

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

`-Dsrv_name=DAS_Query`

and add the argument

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

right after it. An example of what the line should like (your –Xmx, -Xms, and –XX args may look different) is:

```
<process component="DAS"
   image="&amp;quot;$(ESEC_JAVA_HOME)/java&amp;quot; -server
   -Dsrv_name=DAS_Query -Djava.io.tmpdir=D:\Temp2 -
   Xmx256m -Xms85m -XX:+UseParallelGC -Xss128k -Xrs
   -
   Desecurity.dataobjects.config.file=/xml/BaseMetaD
   ata.xml,/xml/WorkflowMetaData.xml -
   Djava.util.logging.config.file=../config/das_quer
   y_log.prop -
   Djava.security.auth.login.config=../config/auth.l
   ogin -
   Djava.security.krb5.conf=../../lib/krb5.conf -
   Desecurity.execution.config.file=../config/execut
   ion.properties -
   Dcom.esecurity.configurationfile=../../configurat
   ion.xml -jar ../../lib/ccsbase.jar
   ..//config//das_query.xml" min_instances="1"
   post_startup_delay="5" shutdown_command="cmd //C
   &amp;quot;$(ESEC_HOME)/sentinel/scripts/stop_containe
   r.bat&amp;quot; localhost DAS_Query"
   working_directory="$(ESEC_HOME)/sentinel/bin"/>
```

Maximizing Event Reporting for Crystal Reporting

Depending on the number of events that Crystal is querying, you may get an error on maximum processing time or maximum record limit. To set your server to process a higher number or an unlimited number or reports you will need to reconfigure the Crystal Page Server.

Reconfiguring the Crystal Page Server (Windows Crystal Server only)

1. Click Start > All Programs > BusinessObjects 11 > Crystal Reports Server > Central Configuration Manager.
2. Right-click on Crystal Page Server and select Stop.
3. Right-click on Crystal 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.

Reconfiguring the Crystal Page Server (Linux or Windows Crystal Servers)

6. Open a web browser and enter the following url:

   For Linux Crystal Servers:

   ```
   http://<DNS or IP of Crystal
      Server>:8080/businessobjects/enterprise11/adminla
      unch
   ```

   For Window Crystal Servers:

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

7. Click Central Management Console.
8. The System Name should be your host computer name. Authentication Type should be Enterprise. If not, choose Enterprise.
9. Enter your user name, password and click Log On.
10. Click Servers.
11. Click <server name>.pageserver
12. Under ‘Database Records to Read When Previewing Or Refreshing a report’, click the ‘Unlimited records’ radio button.
13. Click Apply.
14. A prompt to restart the page server will appear, click OK.
15. You may be prompted for a logon name and password to access the operating system service manager.

e-Security Provided Reports

1. For v5.1.1 SP1 and later, the Top 10 reports queries aggregate tables instead of detailed events table. Ensure that EventFileRedirectService and Aggregation services (summaries) are turned on.

   EventFileRedirectService is located on your DAS machine can be enabled by editing das_binary.xml.

   The three summaries that need to be activated are:

   - EventDestSummary
   - EventSevSummary
   - EventSrcSummary

NOTE: For information about EventFileRedirectService and the three aggregation summaries, see the SDM Chapter in the Sentinel User's Guide or the Crystal Install chapters in the Sentinel Installation Guide.

2. Reports that query a large date range may run slow. They should be scheduled instead of running interactively.

NOTE: For information about scheduling Crystal Reports see the Crystal BusinessObjects Enterprise™ 11 documentation.

Tips When Developing Custom Crystal Reports

For custom developed reports, it is recommended to:

1. Utilize aggregate tables as much as possible.
2. If the reports can utilize pre-defined aggregate tables, choose the aggregate table that result in the processing of the least amount of data.
3. Try to push most of the data processing to the database engine.
4. To reduce processing overhead in Crystal Server, minimize the amount of data to retrieve to the Crystal Server.

Maintenance Best Practices

Database Analyze for Oracle

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

NOTE: This utility tool including a required SQL script may be periodically updated. It is recommended to periodically check the e-Security Customer Portal for any updates.

The following two shell scripts that should be run regularly via cron or other scheduler:

- AnalyzePartitions.sh

This script is located in $ESEC_HOME/utilities/db. This should run locally on the server where Sentinel database is installed. The UNIX user account that runs the script must be able to connect to the database as sysdba (e.g. – oracle).

Analyze Partitions

The AnalyzePartitions.sh script analyzes partitions that are recently populated. This script should be scheduled daily to update database statistics on partitions that are populated from the previous day. It is recommended to run this script two hours after midnight when events for the previous days have been inserted into the database.

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

Installing sp_esec_dba_utl.sql

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

   ```
   @sp_esec_dba_utl.sql
   ```

4. Exit SQL*Plus.

Running AnalyzePartitions.sh

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

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

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

   For Solaris:

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

   For Linux:

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

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

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

Database Health Check for Oracle

dbHealthCheck.sh is a script that gathers information about your Sentinel Oracle Database. The script checks for:

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

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

NOTE: This utility tool including a required SQL script may be periodically updated. It is recommended to periodically check the e-Security Customer Portal for any updates.

Installing and Running dbHealthCheck.sh

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

Installing sp_esec_dba_utl.sql

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

   ```
   @sp_esec_dba_utl.sql
   ```

5. Exit SQL*Plus.

Running dbHealthCheck.sh

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

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

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

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

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

   For Solaris:

   ```
   ./dbHealthCheck.sh
   ```

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

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

   For Linux:

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

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

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

Automatically Archiving Data and Adding Partitions (Windows Only)

NOTE: If your machine does not have access to DAS_Binary and DAS_Query, the SDM Command Line Option can be used in place of the SDM GUI.

This procedure is only applicable to Windows. Ensure that while performing your pre-configuration and configuration that the following is done:

- Make sure sdm.connect is initialized either by using SDM GUI or command line.
- Make sure the archive directory exists.
- Make sure the archiveConfig & dropPartitions days are equal.
- Make sure the batch file runs correctly from command prompt at least once before scheduling it to run automatically.

NOTE: If the scheduled task fails, it will not send a notification. It will log it in SDM_*.log

Pre-Configuration

Prior to automatically setting Archive Data and Add Partitions, you must:

- Save connection properties
- Establish archival parameters

Saving Connection Properties to Sentinel Data Manager

This must be performed prior to using the Sentinel Data Manager Command Line Options. To save your connection (saveConnection) to the Sentinel Data Manager, you must run the SDM Command Line with the saveConnection action.

If you have run the SDM GUI, you can use the sdm.connect file that was created from the GUI. It is located at %ESEC_HOME%\sdm.

The saveConnection action saves the connection details to the connectFile. The keystore referenced in the configuration.xml file is used to encrypt the password before saving it to the connectFile.

The following command line options for the saveConnection action are available to set the connection details:

-action	saveConnection
-server	Mssql
-host	<database host IP Address or host name to connect to>
-port	<database port number to connect to [SQL Server default: 1433]>
-database	<database name/SID to connect to>
-user	<database username>
-password	<database password>
-winAuth	Used for Windows authentication. When using this option, do not use -user and –password.
-connectFile	<filename to save the connection details [file name of your choosing]>

The application saves all the above connection details along with the encrypted password to the file specified. The application uses the saved connection details to execute the other SDM command line actions. This step should be completed the first time you start the application and every time you want to change the connection details.

Running saveConnection

1. Execute the command as follows:

```
sdm -action saveConnection -server <oracle/mssql> -
   host <hostIp/hostName> -port <portnum> -database
   <databaseName/SID> [-driverProps
   <propertiesFile>] {-user <dbUser> -password
   <dbPass> | -winAuth} -connectFile
   <filenameToSaveConnection>
```

The following example will save connection details to the file sdm.connect for a database named esec on a host with an IP address of 172.16.0.36 and port 1433 authenticating as the esecdba user.

```
sdm -action saveConnection -server mssql -host
   172.16.0.36 -port 1433 -database esec -user
   esecdba -password XXXXXX -connectFile
   sdm.connect
```

The following Windows Authentication example will save connection details to the file sdm.connect for a database named esec_51 on a host with an IP address of 172.16.1.3 and port 1433 authenticating using Windows Authentication.

```
sdm -action saveConnection -server mssql -host
   172.16.1.3 -port 1433 -database esec_51 –winAuth
   -connectFile  sdm.connect
```

This will save the connection details to the sdm.connect file. All the rest of the command line actions will take this filename as input in order to connect to the designated database to perform their actions.

NOTE: If you created a connect file to a different location or name than specified in the example, you will have edit the manage_data.bat file.

Establishing Archival Parameters

This can be done using the SDM Command Line.

This action (archiveConfig) is used to configure archiving. This configuration drives how the data is archived from the e-Security Database tables.

This action uses the following flags:

-action	archiveConfig
-dirPath	<valid directory path to write the archived files to>
-keepDays	<number of days to keep>
-connectFile	<path to the filename saved by “saveConnection”>

Establishing Archival Parameters via the Command Line

1. Create an archive output directory at the root called SDM_archive (c:\SDM_archive).

NOTE: If you create a different output directory or location, you will have to edit the manage_data.bat file.

2. Execute this command as follows:

```
sdm -action archiveConfig  -dirPath <directory path
   to write the archived files to> -keepDays <number
   of days to keep> -connectFile <path to the
   filename saved by “saveConnection”>
```

The following example archives all data older than 30 days to c:\SDM_archive directory.

```
sdm -action archiveConfig –dirpath c:\SDM_archive -
   keepDays 30 -connectFile sdm.connect
```

Establishing Archival Parameters via the GUI

1. Create an archive output directory at the root called SDM_archive (c:\SDM_archive).

NOTE: If you create a different output directory or location, you will have to edit the manage_data.bat file.

2. The SDM GUI does not require archival parameters. The GUI can directly archive data without having to establish archival parameters.

Delete Data (Drop Partitions)

This action (deleteData) deletes the data older than "keepDays" from the following tables:

- EVENTS
- CORRELATED_EVENTS

By default, this action does not drop any partitions that are not archived. If you want to delete unarchived partitions, the optional flag "forceDelete" has to be specified with a value of true. If forceDelete is used:

false or not specified	drops only the archived partitions older than keepDays. Does not delete unarchived partitions even if they are older than keepDays.
true	drops all the partitions older than keepDays including unarchived partitions

This command uses the following flags:

-action	deleteData
-keepDays	<number of days to keep>
[-forceDelete]	<either true or false>
-connectFile	<path to the filename saved by "saveConnection">

Running deleteData

1. Execute this command as follows:

```
sdm -action deleteData -keepDays <number of days to
   keep> -connectFile <path to the filename saved by
   "saveConnection">
```

   The following example drops the partitions from the EVENTS and CORRELATED_EVENTS table older than 30 days making sure all dropped partitions are archived. In the end, it lists any partitions that were not deleted if they have not been archived.

```
sdm -action deleteData -keepDays 30 -connectFile
   sdm.connect
```

Scheduling Archiving Data and Adding Partitions

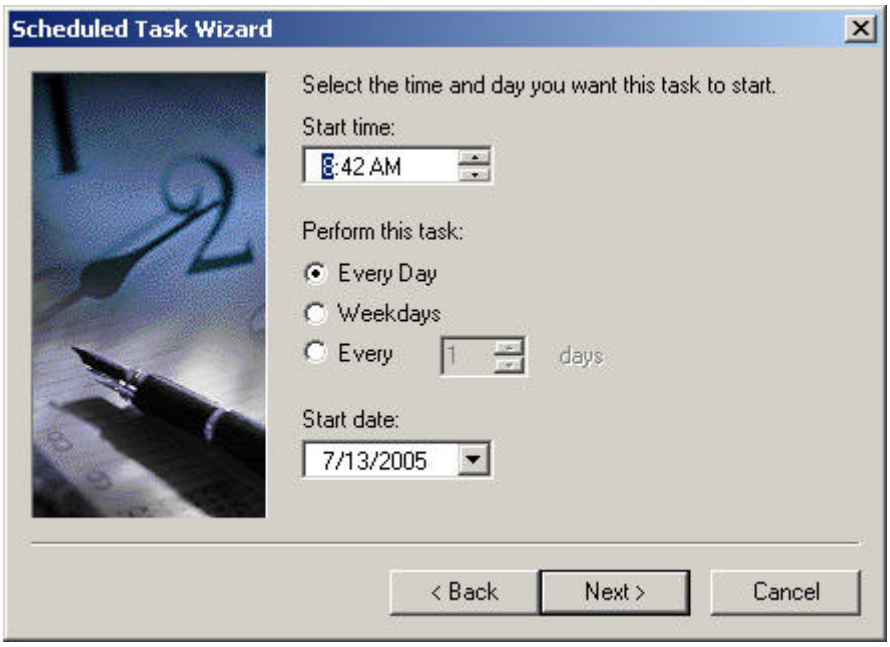
NOTE: The manage_data.bat file is set to a keepDay value of 30, archive output to c:\SDM_archive and connect file to %ESEC_HOME%\SDM\sdm.connect. If your values are different, you will need to edit the manage_data.bat file.

If you have set your connection properties and archival parameters, run the manage_data.bat from the command prompt to ensure that it works.

To Automatically Archive Data and Add Partitions

NOTE: The following steps are for Windows 2000 Professional. Steps for Windows 2000 Server, XP, and 2003 Server may be different, but similar.

1. In Windows, click Start > Setting > Control Panel.
2. Double-click 'Scheduled Tasks'.
3. Double-click 'Add Scheduled Task'. Click Next.
4. Click the Browse button and navigate to the manage_data.bat file (%ESEC_HOME%\sdm).
5. Enter a name for the scheduled task such as SDM_Archive. Select Daily under 'Perform this task:'. Click Next.
6. Select a time a day to run this task. Click Next.
7. Enter a time and date of choice. Click Next.



8. Enter a user that this task will run under. The user cannot be the local system account. It must be run as a specific user. If using Windows Authentication to connect to the database, you must use the e-Security Database Administrator Windows User. Click Next.
9. Click Finish to complete as scheduled task.

Correlation Engine

NOTE: For the Sentinel Correlation Engine to work properly, the machine system time needs to be synchronized within ± 30 seconds of all Agent Manager machines. It is recommended that all Correlation Engine and Agent Manager machines be connected to an NTP (Network Time Protocol) Server or other type of Time Server.

Understanding Advanced Correlation Rules

The advanced correlation rule is used to detect relationships between events, such as when a particular event happens (event B) after event A with a relationship between the two events. In this case event B is the current event and should be identified with a filter you enter in the Event Filter Criteria wizard pane. Event A is the past event and should be identified with a filter you enter in the Past Event Filter Criteria wizard pane. The relationship between the two events (e.g. - they have the same source and destination IP address) should be entered in the Event versus Past Events Criteria wizard pane. In this pane you also specify the maximum amount of time between the two events that you want to detect, this is the time window. If an event passes all those criteria it can then be grouped and counted up to a threshold value indicated in the Threshold and Grouping Criteria wizard pane.

Controlling Time

Window and Trigger operations both have a time window associated with them. The larger the time window the more events (actually pieces of event information) may be stored in memory for that time window. For the Window operation, what is stored is dependent on the filter that is specified for the past events. The more specific this filter can be, the less events are stored in the time window, allowing for a greater time period to be used (if necessary). For the Trigger operation, the total maximum storage space that can be used is dependent on the cardinality of the discriminator (i.e. - the more possible groupings there can be the more events may be stored over time) up to the threshold amount for every group. Many times scaling down the threshold and time period for the Trigger operation will yield equivalent results.

Understanding Trigger Update

Suppose you have received a correlated event for a rule, but you expect to see more correlated events. This can be due to the update behavior of the Trigger operation. In the Trigger operation, you can specify that when you see a set of 'n' events over 't' time to trigger a correlated event. Every time the correlation engine sees that set of 'n' events over 't' time it triggers. If upon triggering it is determined that it had triggered previously (for the same grouping) and there is at least one set member in common, those members are added to the original correlated event instead of creating a new correlated event.

Boolean Expressions Support Short-circuit Analysis

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

Don’t Be Afraid of Free-Form

If you cannot express a correlation rule using the wizard’s three predefined templates (Watchlist, Basic or Advanced) don’t be afraid to construct a free-form rule. All of the templates eventually form a free-form rule for the user. You can see the free-form representation by editing a rule and changing its type to free-form. This may be an easy way to extend a rule you couldn’t quite express using one of the three other options.

Transaction Log

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

Sentinel Log File Locations

There are certain logs in Sentinel that are helpful in troubleshooting your system. These logs can be extremely useful when working with e-Security Technical Support when attempting to resolve issues.

Sentinel Data Manager

Logs activities executed using Sentinel Data Manager for the specific client running on that machine.

For Windows:

```
%ESEC_HOME%\sdm\SDM_*.0.log
```

For UNIX:

```
$ESEC_HOME/sdm/SDM_*.0.log
```

iTRAC

Logs activities related to iTRAC.

For Windows:

```
%ESEC_HOME%\sentinel\log\activity_container_0.*.log
%ESEC_HOME%\sentinel\log\workflow_server_0.*.log
```

For Solaris:

```
$ESEC_HOME/sentinel/log/activity_container_0.*.log
$ESEC_HOME/sentinel/log/workflow_server_0.*.log
```

For Linux:

```
$ESEC_HOME/sentinel/log/das_itrac_0.*.log
```

Advisor

Logs activities related to advisor data download and process.

For Windows:

```
%ESEC_HOME%\sentinel\log\advisor.log
%ESEC_HOME%\sentinel\log\Advisor_0.*.log
```

For UNIX:

```
$ESEC_HOME/sentinel/log/advisor.log
$ESEC_HOME/sentinel/log/Advisor_0.*.log
```

Event Insertion

Logs activities related to event insertion into the database.

For Windows:

```
%ESEC_HOME%\sentinel\log\das_binary0.*.log
```

For UNIX:

```
$ESEC_HOME/sentinel/log/das_binary0.*.log
```

Database Queries

Logs activities related to database queries, agent, agent manager health, and all other DAS activities not performed by other DAS components.

For Windows:

```
%ESEC_HOME%\sentinel\log\das_query0.*.log
```

For UNIX:

```
$ESEC_HOME/sentinel/log/das_query0.*.log
```

Active Views

Logs activities related to Active Views.

For Windows:

```
%ESEC_HOME%\sentinel\log\das_rt0.*.log
```

For UNIX:

```
$ESEC_HOME/sentinel/log/das_rt0.*.log
```

Aggregation (v5.1.1.1 and later)

Logs activities related to aggregation.

For Linux:

```
$ESEC_HOME/sentinel/log/das_aggregation0.*.log
```

Sentinel Watchdog (v5.1.1.1 and later)

Logs activities related to Sentinel Watchdog.

NOTE: sentinel_wrapper.log is for service wrapper.

For Linux:

```
$ESEC_HOME/sentinel/log/sentinel0.*.log
$ESEC_HOME/sentinel/log/sentinel_wrapper.log
```

Agent Manager

Logs activities related to Agent Manager.

NOTE: agent-manager.log is for service wrapper.

For Windows:

```
%ESEC_HOME%\wizard\logs\agent-manager.log
%ESEC_HOME%\wizard\logs\am0.*.log
```

For UNIX:

```
$ESEC_HOME/wizard/logs/agent-manager.log
$ESEC_HOME/wizard/logs/am0.*.log
```

Chapter 3 – Installing Sentinel 5 for Oracle on Solaris

This chapter describes how to install e-Security Enterprise Security Management Sentinel 5 for Oracle on Solaris.

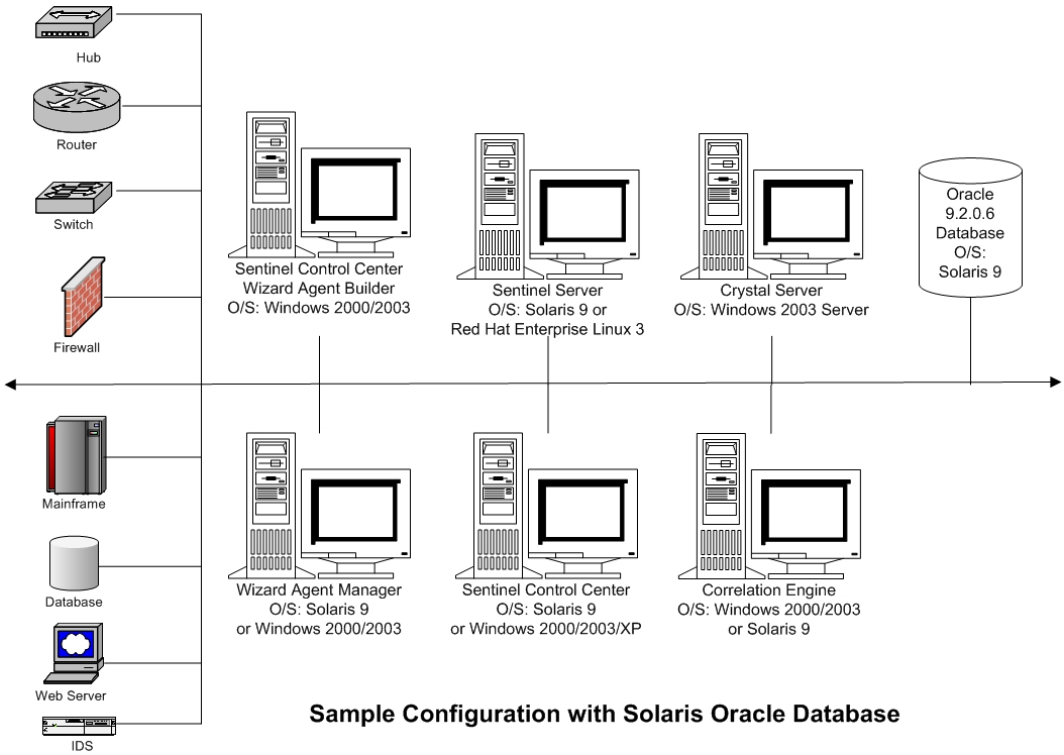
Pre-Installation of Sentinel 5 for Oracle on Solaris

NOTE: Before installation, ensure that your machines meet the minimum systems requirements and that the operating system has been "hardened" using current best security practices.

NOTE: Install Oracle Enterprise with partitioning. The Sentinel Data Manager requires this feature in order to manage the Sentinel Database.

NOTE: When performing a clean installation of e-Security after having a previous version of e-Security installed, you must remove certain files and system settings that may be left over from a previous installation. Not removing these files or settings could cause a new clean installation to fail. This should be done on every machine you are performing a clean installation. For more information, see Appendix E.

The following are typical configurations for Solaris for e-Security Sentinel. Your configuration may be different depending on your environment. Regardless of the configuration you choose, you need to install your database first.



Sample Configuration with Solaris Oracle Database

Obtaining a License Key

The Sentinel Server Database Access Service (DAS) requires that you have a valid license key in order to install and run the service. This license key is locked to the machine where you are going to install DAS. A license key issued for one machine will not work on another machine.

To obtain your license key, you must determine your host ID number and provide this information to e-Security who will assign you a license key.

To determine your host ID (Solaris)

1. Enter the following command:

   ```
   hostid
   ```

2. Submit this host ID number to e-Security customer support. They will provide you with a license key.

Sentinel Database

Before installing Sentinel Database, you will need:

- For hardware requirements, see Chapter 1 and 2.
- Sun SPARC Solaris Server running Solaris 9 with recommended Patch Cluster DATE: May/03/05
- Oracle 9i Enterprise Edition 9.2.0.6 with partitioning
- For Solaris, a copy of Oracle Note: 148673.1 SOLARIS: Quick Start Guide
- Oracle operating system user (default: oracle)
- Ensure the following environment variables are set for the Oracle operating system user:
  - ORACLE_HOME
  - ORACLE_BASE
  - PATH (must have $ORACLE_HOME/bin)
  - Although it is not recommended, if you manually create the Oracle database instance, see Creating an Oracle Instance for the Sentinel Database for instructions on creating your Oracle instance. If you choose this option, you must still use the installer to add the database objects to the manually created Oracle database instance (see Custom Installation on how do this).

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

- If using the installer to create the Oracle database instance (recommended), you will need the directory paths to place the database files. These directories must exist before running the installer as the installer will not create these directories. These directories must also be writable by the Oracle operating system user (e.g. – oracle).

  NOTE: For performance reasons, depending if you are installing in RAID and if your RAID environment allows, the Redo Log should point to the fastest write disk you have available.

NOTE: By default, the installer sets the following tablespaces to NOT autogrow: ESENTD, ESENTX, SENT_SMRYD and SENT_SMRYX. All other tablespaces are set to autogrow. The reason for not allowing autogrow for ESENTD, ESENTX, SENT_SMRYD and SENT_SMRYX is that they contain events and summary events data. Space utilization for events and summaries can be highly dynamic. These events tablespaces should be monitored and extended in a controlled manner based on your file system configuration and in consideration of IO balancing and database backup and recovery.

SDM partition management (archiving, dropping and adding partitions) should be scheduled to keep events data in a controlled size.

Sentinel Server

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

Before installing the Sentinel Server, you will need:

- For hardware requirements, see Chapter 1 and 2.
- Sun SPARC Solaris Server running Solaris 9 with recommended Patch Cluster DATE: May/03/05
- e-Security Sentinel 5 Serial Number and License key (For DAS). For more information, see Obtaining a License Key.
- SMTP Server – This is required to send email from Sentinel.

Sentinel Control Center and Wizard

Before installing the Sentinel Server, you will need:

- For hardware requirements, see Chapter 1 and 2
- One of the following operating systems:
  - Sun SPARC Solaris Server running Solaris 9 with recommended Solaris 9 Recommended Patch Cluster DATE: May/03/05patches
  - (Agent Builder only) – Windows 2000 or 2003

Advisor

To install Advisor, you will need to obtain an Advisor ID and password from e-Security. Direct Internet Download uses port 443.

NOTE: If you intend use Advisor for Exploit Detection only, you do not need to install Crystal Enterprise software. This is only required if you intend to run Crystal Reports for Sentinel. See Chapter 10, Advisor Configuration for more information.

Verifying Solaris Layout (Operating System Patch Requirements)

Verifying Solaris Layout

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

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

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

Oracle Pre-Install on Solaris

Installing Oracle on Solaris for Sentinel, requires that the following be done:

- Setting of kernel values
- Creation of a group and user account for Oracle
- Setting of environmental variables
- Installation of Oracle 9.2.0.6
- Patching of Oracle 9.2.0.6

Setting the Kernel values for Oracle on Solaris

For Oracle on Solaris, the following kernel values have to be set in /etc/system.

DISCLAIMER: The following are suggested minimum values. Consult your system administrator and Oracle documentation for more information.

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

NOTE: If your kernel values are equal to or higher than the above requirements, you do not need to change the settings.

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

Oracle Pre-Install on Solaris

DISCLAIMER: The following instructions 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 **/export/home/oracle** and that Oracle will be installed into **/opt/oracle**. Your exact configuration may vary. Consult your operating system and Oracle documentation for more information.

NOTE: When installing the Oracle software, recommend choosing a "typical" install. If not, ensure that when you are installing as a custom install, that you choose to install Oracle JDBC/OCI Interface. For more information see the Oracle documentation.

1. Login as root.
2. Create a UNIX group and UNIX user accounts for the Oracle database owner.

   Add a dba group (as root):

   ```
   groupadd –g 400 dba
   ```

   Add the oracle user (as root):

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

3. To set the necessary environment variables for Oracle, it is suggested to add the following information to the local.cshrc file:

   ```
   umask 022
   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
   ```

4. Follow the steps outlined in Oracle Note: 148673.1 SOLARIS: Quick Start Guide.
5. Install Oracle 9i Release 2 as the oracle user. You will be prompted for two additional CD-ROMs. You will need to navigate to different directories for each of the additional CD-ROMs.
6. Patch your system to release 9.2.0.6.0. Refer to Oracle documentation for patch procedures.
7. To verify the patch level, as the Oracle UNIX user, enter:

   ```
   sqlplus '/as sysdba'
   ```

   The results should indicate a release of 9.2.0.6.0. Exit by entering quit.
8. Remove the directory you created for the patch.
9. After installing patches, remove the patch directories and files.
10. Reboot.

Installation of Sentinel 5 for Oracle on Solaris

Sentinel 5 supports two installation types. They are:

- Simple – The all-in-one installation option. Sentinel Services, Agent Service, and Applications with Oracle on the same machine. This installation type is only for demonstration purposes.
- Custom – Allows for a fully distributed installation.

Simple Installation on Solaris

This installation installs the most common components (does not include Agent Builder or 3rdParty Integration features) on a single machine. This is primarily for demonstration purposes. This is not a recommended for use in a testing or production environment.

> **NOTE**: Simple install does not support Agent Manager password authentication.

How to perform a Simple install

1. Verify you have the collected the information, performed the tasks, and satisfied the requirements specified in the section Pre-Installation of Sentinel 5 for Oracle for the components you are installing.
2. Verify your Solaris Oracle setup.
3. Login as the root user.
4. Insert and mount the Sentinel Install CD.
5. Start the install program by going the install directory on the CD-ROM and enter:

   For GUI mode:

   ```
   ./setup.sh
   ```

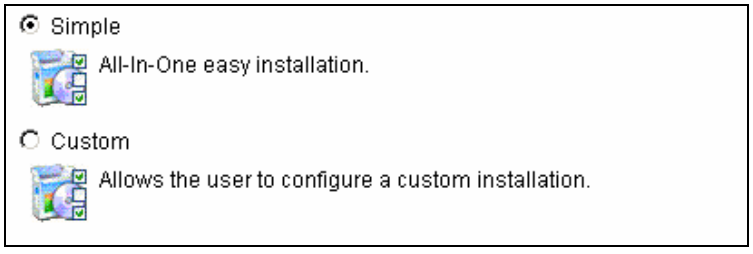
   or

   For textual (“headless”) mode:

   ```
   ./setup.sh –console
   ```

6. Follow the installer prompts.
7. After reading the Welcome screen, Click Next.
8. Accept End User License Agreement, Click Next.
9. Accept the default install directory or click Browse to specify your installation location. Click Next.

10. Select Simple. Click Next.



11. Enter your configuration information
    - Serial Number and License Key
    - SMTP Server (either the DNS name or IP address) – this is if you want Sentinel to have the ability to send emails
    - Email – enter a valid email address where Advisor notification emails should be sent (e.g. - Sent_Server@myserver.com).
    - Global System Password – enter a password and matching confirm password. This will become the password for all default users. This includes both the esecadm operating system user and the database users. Please see Sentinel Database, within the section Post-Installation of Sentinel 5 for Oracle, for the list of default database users created during installation.
    - Data Directory – the location for all of your Database and Advisor download (if installing Advisor) data files. To change the default location, click the ... button and select a location. Default is $ESEC_HOME/data

    NOTE: The Data Directory must be accessible (for reading, writing, and executing) by both the oracle and esecadm user. Since this installation is for demo purposes only, it is recommended that you achieve this accessibility by making the Data Directory readable, writable, and executable by everyone. This can be done by executing the following command:

    chmod 777 <directory_path>

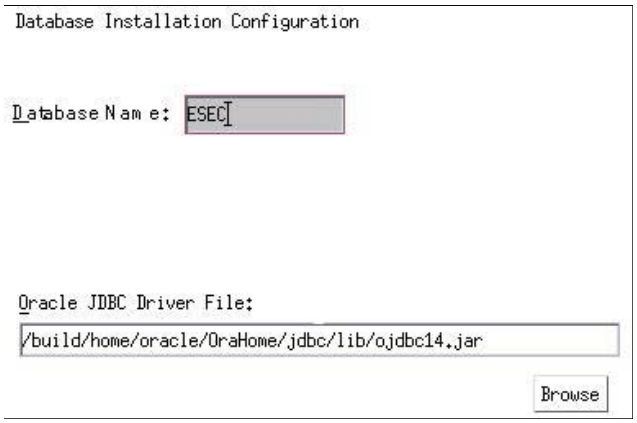
    NOTE: If installing Advisor, Simple install will configure Advisor to use Direct Internet Download with an update interval of 12 hours and all email notifications enabled.

    - To install Advisor, click the Install Advisor check box. Enter a username and password. If your username or password cannot be verified, after clicking Next you will be asked if you would like to continue (not recommended). If you choose to continue, enter your Advisor password again in the password confirmation window. Otherwise correct your Advisor password.

    Click Next.

12. Enter your database configuration information:
    - Database Name – The name of the Oracle database instance to create and install Sentinel Database objects. A database with this name must not already exist.

- Oracle JDBC Driver File. This is the fully qualified path to the jar file, typically $ORACLE_HOME/jdbc/lib/ojdbc14.jar (cannot use environment variables in this field).



13. Click Ok on the default oracle username.

14. Read the information on the screens that follow and click Next when done. Upon completion of installation, you will need to reboot your system.

> **NOTE**: If you wish to install any 3rd Party Integration software (HP Service Desk or Remedy Integration), after you machine reboots, run the installer again and select which 3rd Party Integration software you wish to install. For more information, see the 3rd Party Integration Guide.

15. 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 will stop accepting events.

Custom Installation on Solaris

How to perform a Custom install

1. Verify you have the collected the information, performed the tasks, and satisfied the requirements specified in the section Pre-Installation of Sentinel 5 for Oracle for the components you are installing.
2. Verify your Solaris Oracle setup.
3. Login as the root user.
4. Insert and mount the Sentinel Install CD.
5. Start the install program by going to the install directory on the CD-ROM and enter:

   For GUI mode:

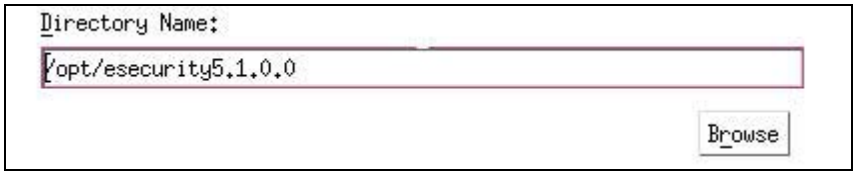
   ```
   ./setup.sh
   ```

   or

For textual (“headless”) mode:

```
./setup.sh –console
```

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



9. Select Custom (default). Click Next.
10. Select which features to install.

NOTE: For more information on which component can be installed where for different configurations, see Chapter 1, System Requirements.

The following options are available:

- Database– installs Sentinel Database
- Communication Server– installs message bus (iSCALE)
- Advisor
- Base Sentinel Services
- Correlation Engine
- DAS
- Agent Service
- Sentinel Control Center
- Sentinel Data Manager
- HP OpenView Service Desk*
- Remedy Integration*

NOTE: *For information regarding installation of HP OpenView Service Desk or Remedy Integration, see the 3rd Party Integration Guide.

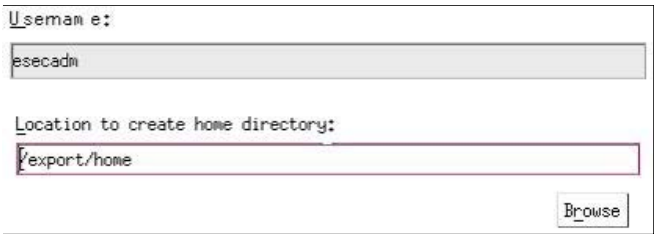
NOTE: If none of the child features of “Sentinel Services” are selected, make sure you de-select the “Sentinel Services” feature as well. It will appear grayed-out with a white check mark in it if it is still selected but all of its child features were de-selected.

NOTE: As part of the installation of the Sentinel Database component, the installer will place files in the $ESEC_HOME/utilities/db folder.

11. If you selected to install DAS, you will be prompted for:
    - Serial Number

- License Key

12. If you selected to install any 3rd party integration components, you will be prompted for a password to unlock the 3rd party integration component(s) you selected. For more information, see the 3rd Party Integration Guide.
13. Specify the operating system e-Security Administrator username and the location of its home directory. This is the username that will own the installed e-Security product. If the user does not already exist, one will be created along with a home directory in the specified directory.
    - OS Administrator username – Default is esecadm
    - OS Administrator user home directory – Default is "/export/home". If esecadm is the username, then the user's home directory will be /export/home/esecadm.



NOTE: If a new user is created, its password will need to be set manually, separately from this installer. e-Security recommends this be done directly by logging into the system following the installation of the product.

In order to meet stringent security configurations required by Common Criteria Certification, e-Security requires a strong password with the following characteristics:

1. Choose passwords of at least 8 with characters in length that includes at least one UPPER CASE, one lower case, one special symbol (#$_) and one numeric (0-9). Do not use blanks.

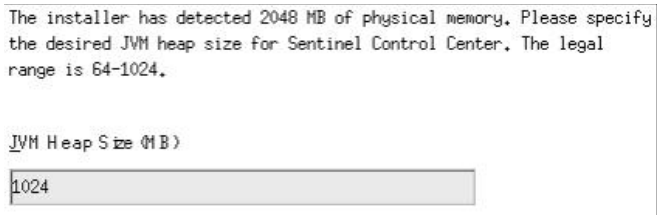
2. Your password may not contain your e-mail name or any part of your full name.

3. Your password should not be a "common" word (for example, it should not be a word in the dictionary or slang in common use).

4. Your password should not contain words from any language, because numerous password-cracking programs exist that can run through millions of possible word combinations in seconds.

5. You should choose a password you can remember and yet is complex. For example, Msi5#YOld (My Son is 5 years old) OR IhliCf5#yN (I have lived in California for 5 years now).

14. If you chose to install Sentinel Control Center, a JVM (Java Virtual Machine) heap size prompt will appear:
    - JVM heap size (MB) - By default, this set to half the size of the physical memory detected on the machine, with a maximum of 1024 MB. This will be the maximum JVM heap size used only by Sentinel Control Center.

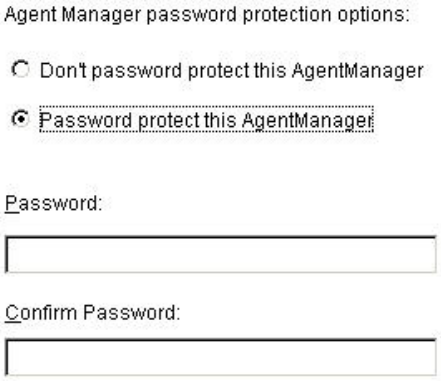


15. If you chose to install Agent Service, select to either protect or not protect the Wizard Agent Manager with a password. If you chose to protect the Wizard Agent Manager, you will be prompted to create a Wizard Agent Manager password.

NOTE: Protecting a Wizard Agent with a password will require you to enter this password when uploading, downloading, or debugging Agents on this Wizard Agent Manager. This password is in addition to the Sentinel username and password needed to login to Wizard Agent Builder.

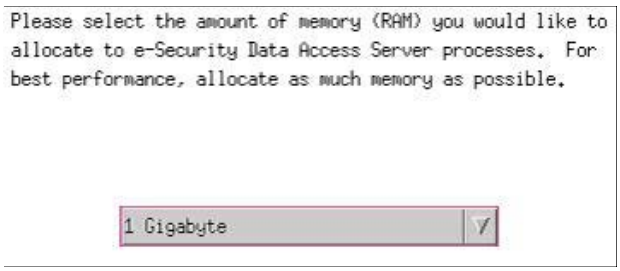
NOTE: In order to meet stringent security configurations required by Common Criteria Certification, e-Security requires a strong password with the following characteristics:

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

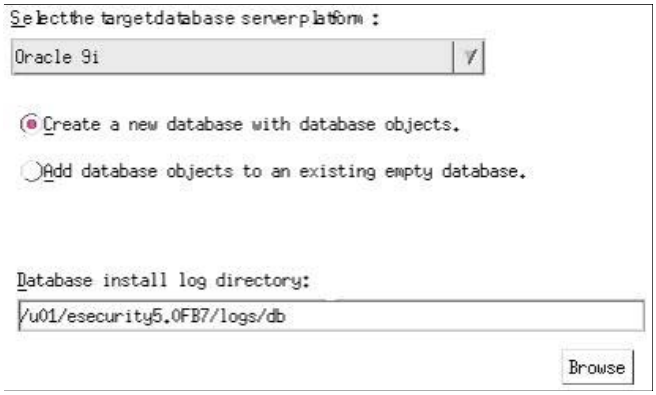


16. If you chose to install DAS, select the amount of RAM on your system you wish to allocate for the Data Access Service. For distributed environments, it recommended to select the maximum memory (4 GB).

For Standalone environments, it is recommended to select half of your RAM memory.

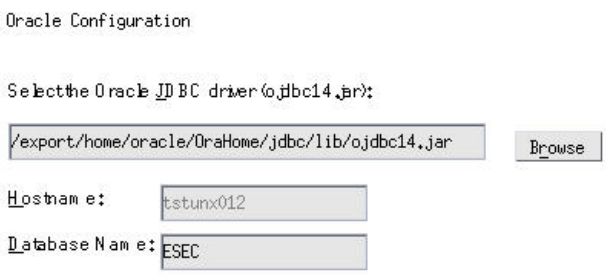


17. For database install, you will have the following prompts
    a. Select target database server platform as Oracle 9i and select one of the following:
        - Create a new database with database objects – creates a new Oracle database instance as well as populates the new instance with database objects.
        - Add database objects to an existing empty database – only adds database to an existing Oracle database instance. The existing database instance must be empty, except for the presence of the esecdba user.
    b. Enter the database install log directory (default: $ESEC_HOME/logs/db). Accept the default 'Database install log directory' or click Browse to specify a different location.



    c. Click Ok on the default oracle username.

    d. If you chose to create a new database , enter the following:
        - The path for Oracle JDBC driver file (typical name of the jar file is ojdbc14.jar). This is the fully qualified path to the jar file, typically $ORACLE_HOME/jdbc/lib/ojdbc14.jar (cannot use environment variables in this field).
        - Hostname – The hostname of the machine to install the database. This field is not configurable if creating new database instance.
        - Database Name – The name of the database instance to install.

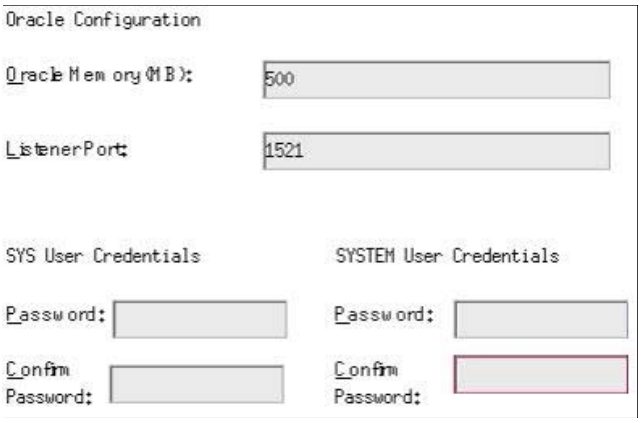


e. If you chose to add database objects to an existing empty Oracle database, you will be prompted for the following information.
   - The path for Oracle JDBC driver file (typical name of the jar file is ojdbc14.jar). This is the fully qualified path to the jar file, typically $ORACLE_HOME/jdbc/lib/ojdbc14.jar (cannot use environment variables in this field).
   - Database hostname or IP address – The name or IP address of the host where the Oracle database is you wish to add database objects to. This can be the local hostname or a remote hostname.
   - Database name – The name of the existing empty Oracle database instance you wish to add database objects to (default is ESEC). This database name must appear 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.

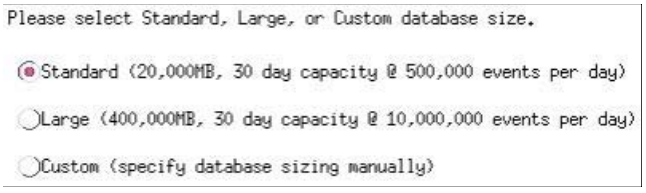
NOTE: If the database name is not in the tnsnames.ora, the installer will not give you an error at this point in the installation (because it verifies the connection using a direct JDBC connection), but the Database installation will fail when the Database installer tries to connect to the database via sqlplus. If the Database installation fails at that point, you can go backward to this prompt and fix the database name.

   - Database port (default is 1521)
   - For e-Security Database Administrator User (DBA), specify the password for the “esecdba” user. The username field in this prompt is not editable.

f. If you chose to create a new database, you will see the following prompt:
   - Oracle Memory (MB) – The amount of RAM to be allocated to this Oracle database instance.
   - Listener Port – the port on which to create an Oracle listener (default is 1521).
   - SYS user password and password confirmation – SYS is a default Oracle user. This user's password will be set to the value specified here.
   - SYSTEM user password and password confirmation - SYSTEM is a default Oracle user. This user's password will be set to the value specified here.



g. If you chose to create a new database, you be prompted to enter your database size. You have the following options:
   - Standard (20 GB)
   - Large (400 GB)
   - Custom (specify your size manually). If you choose this option you will be prompted for:
     - initial size of each database file in MB (100 – 10,000)
     - maximum size of each database file in MB (2,000 – 100,000)
     - size of all database files MB (7,000 – 2,000,000)
     - size of each log file in MB (100 – 100,000)



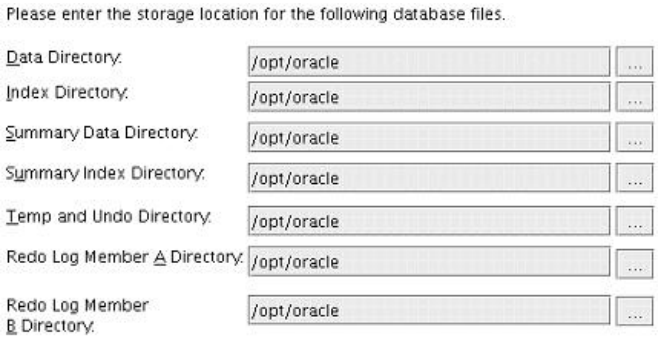
h. If you chose to create a new database, you will be prompted to enter the storage location for the following database files:

NOTE: For recovery and performance purposes, we recommend that these locations be on different I/O devices.

The installer will not create these directories, so they must be created externally before continuing beyond this step.

These directories must be writable by the oracle user.

- Data directory
- Index directory
- Summary Data directory
- Summary Index directory
- Temporary and Undo Tablespace directory
- Redo Log Member A directory
- Redo Log Member B directory



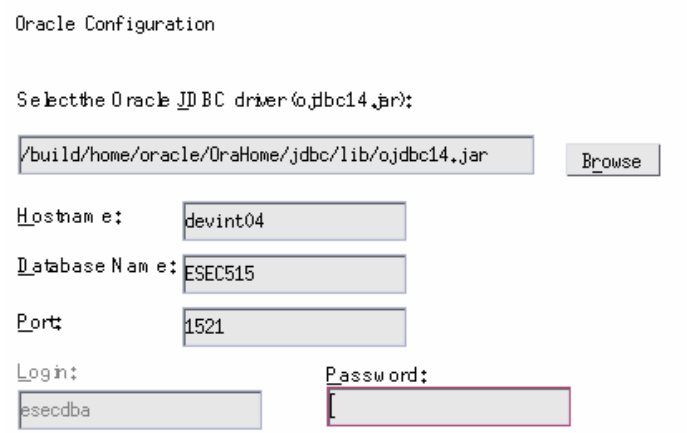
i. If you chose to create a new database, enter authentication information for the e-Security Database Administrator (DBA). This is esecdba, the owner of the database objects.

j. Enter authentication information for the e-Security Application Database user. This is esecapp, the e-Security application username that Sentinel processes use to connect to the database.

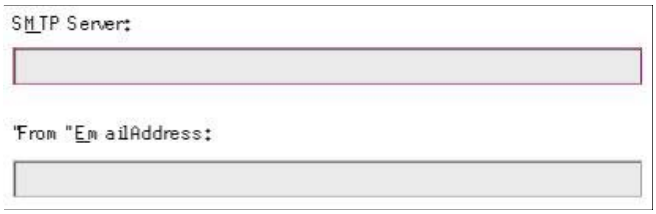
k. Enter authentication information for the e-Security Administrator Database user. This is esecadm, the Sentinel Administrator user.

l. Click Next on the database installation summary window.

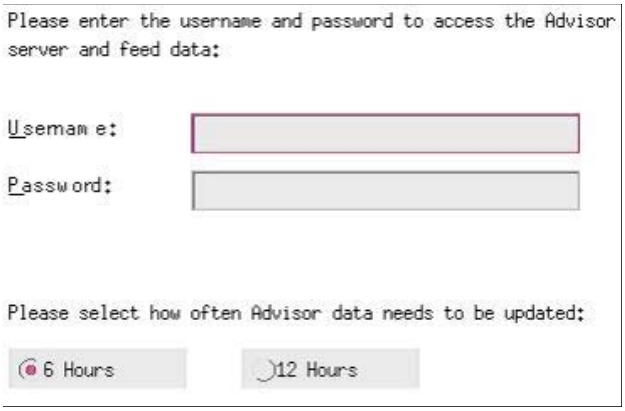
18. If you chose to install DAS, but did not choose to install Sentinel Database, you will be prompted for the following Oracle Sentinel Database information. This information will be used to configure DAS to point to the Sentinel Database.
    - Database hostname or IP address – The name or IP of the existing Oracle Sentinel Database you wish to configure the DAS component to connect to.
    - Database name – The name of the existing empty Oracle database instance you wish to configure the DAS component to connect to (default is ESEC).
    - Database port (default is 1521)
    - For e-Security Application Database User, specify the login “esecapp” and enter the password given for this user during Sentinel Database installation.



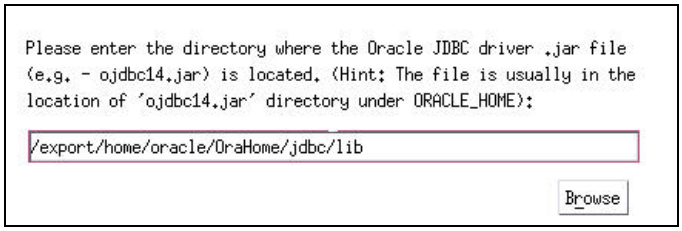
19. If you chose to install DAS, configure Sentinel email support. Specify the SMTP server and the from email address the Execution Service should use to send messages (optional – you may manually edit this after install [$ESEC_HOME\sentinel\config\execution.properties]):



20. If you chose to install Advisor, select the type of Advisor installation (if the Advisor option was chosen a username and password)
    - Direct Internet Download - Advisor machine is directly connected to the Internet. In this configuration, updates from e-Security are automatically downloaded from e-Security over the Internet on a regular schedule.
    - Standalone - Advisor is configured as an isolated system that requires manual intervention to receive an update from e-Security.
21. If you chose to install Advisor and selected to use Direct Internet Download, enter your Advisor username, password and how often Advisor data is to be updated. If your username or password cannot be verified, after clicking Next you will be asked if you would like to continue (not recommended). If you choose to continue, enter your Advisor password again in the password confirmation window. Otherwise correct your Advisor password.



22. If you chose to install Advisor, enter the path to the directory containing the Oracle JDBC driver (typical name of the driver file is ojdbc14.jar). This is the fully qualified path to the directory containing the driver jar file, typically $ORACLE_HOME/jdbc/lib (cannot use environment variables in this field).



23. If you chose to install Advisor, enter:
    - The directory where the Advisor data feed files will to be stored. This is the location the attack and alert feed files will be saved when they are downloaded.

NOTE: The Advisor data feed files directory must have the following ownership settings:

User – esecadm

Group – esec

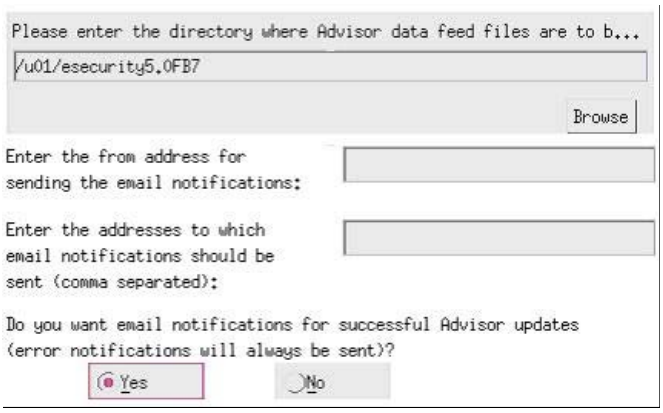
If the directory does not have these ownership settings, run the following command as root to set the ownership of the directory:

chown esecadm:esec <directory_path>

    - From address, which will appear in email notifications
    - To address for sending email notifications

NOTE: After installation, you can change the Advisor email addresses by editing the attackcontainer.xml and alertcontainer.xml files in the $ESEC_HOME/sentinel/config directory. For more information, see Chapter 7 – Advisor Tab of the Sentinel User's Guide.

    - Select either Yes or No for if you wish to receive emails for successful Advisor updates. Error notifications will always be sent.



24. If you chose to install HP Service Desk or Remedy Integration, you will be prompted for further information. For more information, see the Sentinel 3rd Party Integration Guide.
25. Read the information on the screens that follow and click Next when done. Upon completion of installation, you will be prompted to reboot. Click Finish to reboot your system.
26. 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 will stop accepting events.
27. If you expect a high event rate (greater than 500 events per sec), you must follow the additional configuration instructions in the section Setting Up The Oracle Call Interface (OCI) Event Insertion Strategy.

Post-Installation of Sentinel 5 for Oracle

Updating Sentinel email for SMTP Authentication

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

To configure execution.properties file

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

   ```
   $ESEC_HOME/sentinel/config
   ```

2. Execute mailconfig as follows:

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

   Example:

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

After entering this command you will be prompted for a new password.

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

NOTE: When using the password option, it must be the last argument.

To test your execution.properties configuration

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

   ```
   $ESEC_HOME/sentinel/config
   ```

2. Execute mailconfigtest as follows:

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

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

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

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

   ```
   Subject: Testing e-Security mail property
   This is a test for e-Security mail property set up. If
      you see this message, your e-Security mail property
      has been configured correctly to send emails
   ```

Sentinel Database

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

- esecdba - Database schema owner. DBA privilege is not granted to esecdba due to security concerns. To use Enterprise Manager, create a user with DBA privileges.
- esecapp – Database application user. This is the application user used to connect to the database.
- esecadm – Database user that is the e-Security Sentinel Administrator. This is not the same user account as the esecadm operating system user.
- esecrpt - Database report user
- SYS – SYS database user
- SYSTEM – SYSTEM database user

Agent Service

During the installation of the Agent Service, the following Agents will be installed and each will have an Agent port setup to run them.

Product	Agent Name
Demo Agents	
Testing for asset upload, works with DemoEvents Agent	DemoAssetUpload

Testing for demo events, works with DemoAssetUpload and DemoVulnerabilityUpload Agent	DemoEvents
Testing for vulnerability upload, works with DemoEvents Agent	DemoVulnerabilityUpload
Test for sending an event	SendOneEvent
Test for sending multiple events	SendMultipleEvents

NOTE: For more information regarding configuration of the Demo Agents, see Chapter 11, Testing the Installation.

NOTE: For additional agents, go to the e-Security Customer Portal. For more information (including configuration) go to the documentation provided with each Agent in:

$WORKBENCH_HOME/Elements/<agent name>/Docs/

To install additional agents, run the Service Pack script on the Service Pack CD. The script will install the agents locally.

On Windows:

```
.\service_pack.bat
```

On UNIX:

```
./service_pack.sh
```

For Service Pack installation instructions and listing of agents, see the Service Pack Release notes.

Updating Your License Key

How to update your license key (Solaris)

1. Login as user esecadm.
2. Go to $ESEC_HOME/utilities.
3. Enter the following command:

   ```
   /softwarekey
   ```

4. Enter the number 1 for entering your primary key. Press enter.

Creating an Oracle Instance for the Sentinel Database

NOTE: This procedure is provided as an example if you want to create your own tablespaces versus using the tablespace creation feature with the install CD. Your size values may vary depending on your system configuration and requirements. The tablespaces must be named exactly as specified below, however.

In the Oracle instance you will need to configure:

- parameters

- tablespaces

Creating an Oracle Instance

1. Login as an Oracle user.
2. Using the Oracle Database Assistant GUI, create the following:

NOTE: Your values may vary depending on your system configuration and requirements.

Minimum Recommended Solaris 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

Minimum Recommended Solaris Tablespace Size		
Tablespace	**Example Size**	**Notes**
REDO	3 x 100M	▪ This is a minimum value. You should create larger redo logs if you have a high EPS.
SYSTEM	500M	▪ Minimum value
TEMP	1G	▪ Minimum value
UNDO	1G	▪ Minimum value
ESENTD	5G	▪ Minimum value ▪ This for event data
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
ESENTX2	500M	▪ Minimum value ▪ Index for configuration, assets, vulnerability and associations (autoextend enabled)
SENT_ADVISORD	200M	▪ Minimum value ▪ For Advisor data (autoextend enabled)

Minimum Recommended Solaris Tablespace Size		
Tablespace	**Example Size**	**Notes**
SENT_ADVISORX	100M	▪ Minimum value ▪ For Advisor index (autoextend enabled)
SENT_LOBS	100M	▪ Minimum value ▪ For database large objects (autoextend enabled)
SENT_SMRYD	3G	▪ Minimum value ▪ For Aggregation, summary data
SENT_SMRYX	2G	▪ Minimum value ▪ For Aggregation, summary index

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.

Setting Up the Oracle Call Interface (OCI) Event Insertion Strategy

Sentinel 5.1 provides a framework for plugging in different strategies to insert events into the database. Sentinel 5.1 provides two strategies to insert events into the Oracle database

- JDBCLoadStrategy
- OCILoadStrategy

The strategy to be used for inserting events is governed by the insert.strategy property of the EventStoreService component in das_binary.xml.

The JDBC strategy is the default strategy configured out of the box.

The OCI strategy is a native insert strategy for faster event insertion. This strategy requires the Oracle OCI libraries be installed on the machine running the DAS component. The OCI strategy must be used in configurations where a high event rate is expected.

The number of events to be grouped together for insertion into the database is governed by the insert.batchsize property. This insert.batchsize property is used by all the event insert strategies.

To change Sentinel's Event Insertion strategy from the default JDBC Insertion Strategy to the OCI Insertion Strategy, there are a few steps that need to be performed.

Changing Event Insertion strategy from JDBC to OCI Insertion Strategy

1. Ensure the Oracle OCI libraries are installed on the machine running the e-Security DAS component. You will need to know the path to ORACLE_HOME in the following steps.
2. Log into the machine from step 1 as the esecadm user.

3. Create a ".profile" file in the esecadm user's home dir. Put the following text in that file (modify the path to ORACLE_HOME to match your installation):

   ```
   ORACLE_HOME=/build/home/oracle/OraHome
   export ORACLE_HOME
   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib
   export LD_LIBRARY_PATH
   ```

4. Open the $ESEC_HOME/sentinel/config/das_binary.xml file for editing in any text editor.
5. Do a search on the following text:

   ```
   JDBCLoadStrategy
   ```

6. Change that text to:

   ```
   OCILoadStrategy
   ```

7. Save this change to the das_binary.xml file.
8. Restart the DAS Binary application. (Restarting DAS Binary can most easily be done by performing a "ps –ef | grep DAS_Binary" to get the process ID, killing that process, and then letting the Sentinel Watchdog automatically restart the process.)

   Once DAS Binary has been restarted, the $ESEC_HOME/sentinel/lib/libocievent.so library will be loaded and used to perform the Event insertions into the database via OCI.

Additional OCI Event Insertion Options

In addition to specifying the "OCILoadStrategy" in the das_binary.xml file, there are several other OCI-related options that can also be configured.

- insert.batchsize – This setting allows you to configure the maximum number of Events to insert into the database at a time.
- insert.oci.workerCount – This setting allows you to configure the number of threads being used to insert Event data into the database.
- insert.oci.queueWaitTime – This setting specifies the max time in seconds to wait before inserting the data from the inbound queue into the database. Whenever a full "batchsize" of events is received, the entire batch is inserted. But if the inbound flow of events is slow, the queue wait time is used to determine when to do the database insertion (even if a full batch of events has not yet been received).
- insert.oci.highWatermark – The inbound Event queue's high water mark.
- insert.oci.lowWatermark – The inbound Event queue's low watermark.
- insert.oci.optimizationFlag – Optimization flag. "on" or "off".

OCI Debugging Tips

The OCI interface will log messages to the $ESEC_HOME/sentinel/log/ocievent.log file. Initial messages written to the log file should include success (or fail) database connection messages… This is a good place to check to verify that the OCI library was loaded and configured correctly.

The OCI interface will also log errors to the das_binary log file located in the $ESEC_HOME/sentinel/log directory. Errors logged to the das_binary log file include failures to locate/load the libocievent.so library, failures to connect to the database, and failures to insert Events/Event Associations.

If error messages indicate that the “libocievent.so” file is not being located or loaded, then there are three things to check:

1. Make sure the Oracle OCI libraries are installed.
2. Make sure that the “libocievent.so” file is located in the $ESEC_HOME/sentinel/lib directory.
3. Make sure that the $ESEC_HOME/sentinel/lib directory is in the “esecadm” user’s “LD_LIBRARY_PATH”. If not, you can update the LD_LIBRARY_PATH in the “esecadm” user’s .profile
4. Make sure that the environment variables ORACLE_HOME and LD_LIBRARY_PATH are updated properly in esecadm’s user environment variables as described in the section “Changing Event Insertion strategy from JDBC to OCI Insertion Strategy”.

Chapter 4 – Installing Sentinel 5 for Oracle on Linux

This chapter describes how to install e-Security Enterprise Security Management Sentinel 5 for Oracle on Linux.

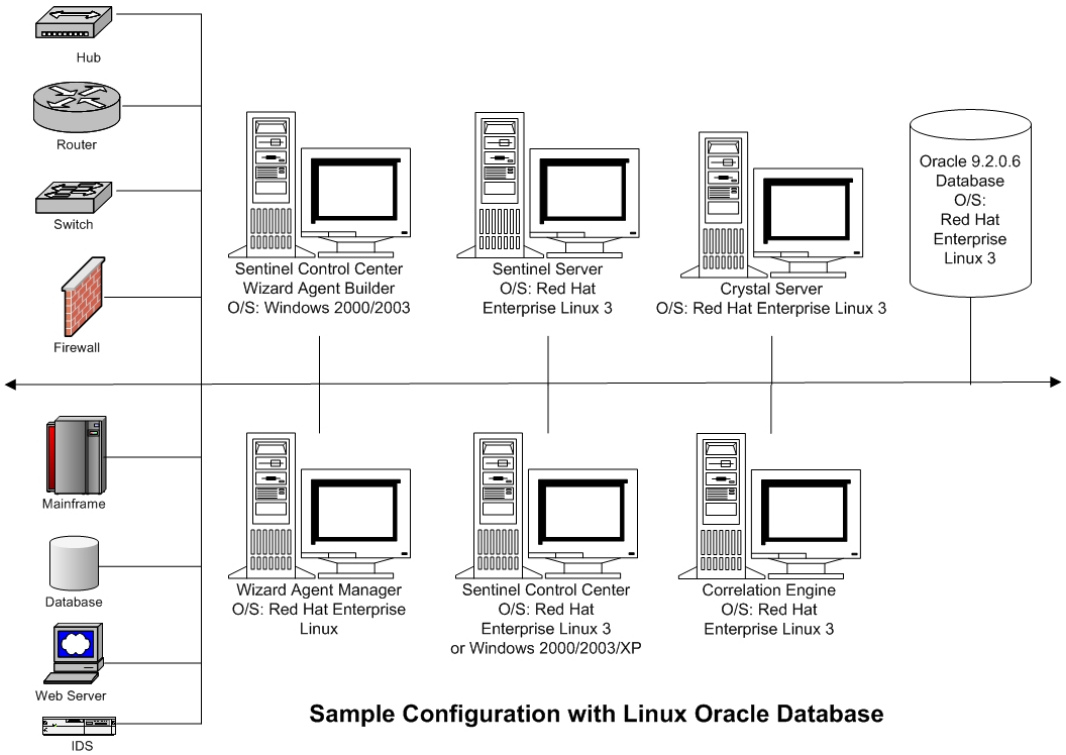
Pre-Installation of Sentinel 5 for Oracle on Linux

NOTE: Before installation, ensure that your machines meet the minimum systems requirements and that the operating system has been "hardened" using current best security practices.

NOTE: Install Oracle Enterprise with partitioning. The Sentinel Data Manager requires this feature in order to manage the Sentinel Database.

NOTE: When performing a clean installation of e-Security after having a previous version of e-Security installed, you must remove certain files and system settings that may be left over from a previous installation. Not removing these files or settings could cause a new clean installation to fail. This should be done on every machine you are performing a clean installation. For more information, see Appendix E.

The following are typical configurations for Linux for e-Security Sentinel. Your configuration may be different depending on your environment. Regardless of the configuration you choose, you need to install your database first.



Sample Configuration with Linux Oracle Database

Obtaining a License Key

The Sentinel Server Database Access Service (DAS) requires that you have a valid license key in order to install and run the service. This license key is locked to the machine where you are going to install DAS. A license key issued for one machine will not work on another machine.

To obtain your license key, you must determine your host ID number and provide this information to e-Security who will assign you a license key.

To determine your host ID (Linux)

1. Login as the root user.
2. Insert and mount the Sentinel Install CD.
3. cd to utilities/linux and enter:

```
./esechostid
```

4. Submit this host ID number to e-Security customer support. They will provide you with a license key.

Sentinel Database

Before installing Sentinel Database, you will need:

- For hardware requirements, see Chapter 1 and 2.
- Red Hat Enterprise Linux 3 Update 5 ES (x86)
- Oracle 9i Enterprise Edition 9.2.0.6 with partitioning
- Oracle operating system user (default: oracle)
- Ensure the following environment variables are set for the Oracle operating system user:
  - ORACLE_HOME
  - ORACLE_BASE
  - PATH (must have $ORACLE_HOME/bin)
  - Although it is not recommended, if you manually create the Oracle database instance, see Creating an Oracle Instance for the Sentinel Database for instructions on creating your Oracle instance. If you choose this option, you must still use the installer to add the database objects to the manually created Oracle database instance (see Custom Installation on how do this).

NOTE: If using an existing or manually created Oracle database instance, it must be empty except for the presence of the esecdba user. The section Creating an Oracle Instance for the Sentinel Database includes instructions for creating this user if it does not already exist.

- If using the installer to create the Oracle database instance (recommended), you will need the directory paths to place the database files. These directories must exist before running the installer as the installer will not create these directories. These directories must also be writable by the Oracle operating system user (e.g. – oracle).

NOTE: For performance reasons, depending if you are installing in RAID and if your RAID environment allows, the Redo Log should point to the fastest write disk you have available.

NOTE: By default, the installer sets the following tablespaces to NOT autogrow: ESENTD, ESENTX, SENT_SMRYD and SENT_SMRYX. All other tablespaces are set to autogrow. The reason for not allowing autogrow for ESENTD, ESENTX, SENT_SMRYD and SENT_SMRYX is that they contain events and summary events data. Space utilization for events and summaries can be highly dynamic. These tablespaces should be monitored and extended in a controlled manner based on your file system configuration and in consideration of IO balancing and database backup and recovery.

SDM partition management (archiving, dropping and adding partitions) should be scheduled to keep events data within a controlled size.

Sentinel Server

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

Before installing the Sentinel Server, you will need:

- For hardware requirements, see Chapter 1 and 2.
- Red Hat Enterprise Linux 3 Update 5 ES (x86)
- e-Security Sentinel 5 Serial Number and License key (For DAS). For more information, see Obtaining a License Key.
- SMTP Server – This is required to send email from Sentinel.

Sentinel Control Center and Wizard

Before installing the Sentinel Server, you will need:

- For hardware requirements, see Chapter 1 and 2
- Red Hat Enterprise Linux 3 Update 5 ES (x86)
- (Agent Builder and Sentinel Control Center) – Windows 2000 or 2003

Advisor

To install Advisor, you will need to obtain an Advisor ID and password from e-Security. Direct Internet Download uses port 443.

NOTE: If you intend to use Advisor for Exploit Detection only, you do not need to install Crystal Enterprise software. This is only required if you intend to run Crystal Reports for Sentinel. See Chapter 10, Advisor Configuration for more information.

Oracle Pre-Install on Linux

Installing Oracle on Linux for Sentinel, requires that the following be done:

- Setting of kernel values
- Creation of a group and user account for Oracle
- Setting of environmental variables for Oracle user
- Linking of gcc
- Patching Linux OS for Oracle 9.2.0.4 Install (obtain the patch p3006854_9204_LINUX from Oracle directly)
- Installation of Oracle 9.2.0.4 (obtain this software from Oracle directly)

- Patching Oracle 9.2.0.4 to Oracle 9.2.0.6 (obtain the Oracle 9.2.0.6 patch from Oracle directly)

Setting the Kernel values for Oracle on Linux

For Oracle on Linux, the following kernel values have to be set.

> **DISCLAIMER**: The following are suggested minimum values. If your current settings exceed these figures, then do not alter them. Consult your system administrator and Oracle documentation for more information.

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

1. Log in as root.
2. Set kernel parameters by adding the following text to the end of the "/etc/sysctl.conf" file:

> **NOTE:** The settings below are the suggested minimum values. If your settings exceed these figures, then do not alter them. 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`

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

3. Execute the following command to load the modifications to the "/etc/sysctl.conf" file:

```
sysctl -p
```

4. 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". If your Oracle userid is something else, replace "oracle" in the following text with your Oracle userid.

```
# Settings added for Oracle
oracle          soft    nproc   16384
oracle          hard    nproc   16384
```

```
oracle          soft    nofile  65536
oracle          hard    nofile  65536
```

Oracle Pre-Install on Linux

DISCLAIMER: The following instructions 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 **/export/home/oracle** and that Oracle will be installed into **/opt/oracle**. Your exact configuration may vary. Consult your operating system and Oracle documentation for more information.

1. Log in as root.
2. Create a UNIX group and UNIX user account for the Oracle database owner.

   Add a dba group (as root):

   ```
   groupadd dba
   ```

3. Add the Oracle user (as root):

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

4. Create directory for ORACLE_HOME and ORACLE_BASE:

   ```
   mkdir –p /opt/oracle/
   ```

5. Change the ownership of the ORACLE_BASE dir and deeper to oracle/dba:

   ```
   chown -R oracle:dba /opt/oracle
   ```

6. Change to the oracle user:

   ```
   su - oracle
   ```

7. Open the '.bash_profile' file (in oracle user's home directory) for editing and add the following to the end of the file:

   NOTE: This set of environment variables must only be used for the oracle user. Specifically, they should not be set in the system environment or in the esecadm user's environment.

   ```
   # Set the LD_ASSUME_KERNEL environment variable only
      for Red Hat 9,
   # RHEL AS 3, and RHEL AS 4 !!
   # Use the "Linuxthreads with floating stacks"
      implementation instead of NPTL:
   # for RH 9 and RHEL AS 3
   export LD_ASSUME_KERNEL=2.4.1
   # for RHEL AS 4
   # export LD_ASSUME_KERNEL=2.4.19
   # Oracle Environment
   ```

```
export ORACLE_BASE=/opt/oracle
export ORACLE_HOME=$ORACLE_BASE/
export ORACLE_SID=test
export ORACLE_TERM=xterm
# export TNS_ADMIN= Set if sqlnet.ora, tnsnames.ora,
   etc. are not in $ORACLE_HOME/network/admin
export NLS_LANG=AMERICAN;
export ORA_NLS33=$ORACLE_HOME/ocommon/nls/admin/data
LD_LIBRARY_PATH=$ORACLE_HOME/lib:/lib:/usr/lib
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/lib
export LD_LIBRARY_PATH
# Set shell search paths
export PATH=$PATH:$ORACLE_HOME/bin
```

8. Re-login as oracle user to load environment variable changes from last step:

```
exit
su - oracle
```

9. Link gcc to version 2.9.6

> **NOTE**: If /usr/bin/gcc296 or /usr/bin/g++296 does not exist, then gcc or g++ was not installed. If this is the case, install these components, then return to this step.

```
su - root
ln -s /usr/bin/gcc296 /usr/bin/gcc
ln -s /usr/bin/g++296 /usr/bin/g++
```

10. Exit to return to oracle user prompt.

```
exit
```

11. Run the Oracle patch p3006854_9204_LINUX.zip, which patches the Linux operating system for the Oracle installation. This patch can be obtained from Oracle.

```
su - root
unzip p3006854_9204_LINUX.zip
cd 3006854
sh rhel3_pre_install.sh
```

12. Exit to return to oracle user prompt.

```
exit
```

13. To install Oracle 9.2.0.4, from within Disk1, run the script:

```
./runInstaller
```

14. When progressing through the installer, leave all prompts at their default values unless other wise specified below.
    - At prompt for UNIX Group Name, enter: dba
    - At prompt for Installation Type, choose Custom.

    Select the following components to be installed:
    - Oracle 9i 9.2.0.4.0
    - Enterprise Edition Options 9.2.0.1.0
        - Oracle Partitioning 9i 9.2.0.4.0
    - Oracle Net Services 9.2.0.1.0
        - Oracle Net Listener 9.2.0.4.0
    - Oracle Enterprise Manager Products 9.2.0.1.0 (All)
    - Oracle 9i Development Kit 9.2.0.1.0 (All)
    - Oracle 9i for UNIX Documentation 9.2.0.1.0
    - Oracle HTTP Server 9.2.0.1.0 (All)
    - iSQL*Plus 9.2.0.4.0 (All)
    - Oracle JDBC/OCI Interfaces 9.2.0.1.0
15. At prompt for Create Database, choose NO.
16. Optional, cancel all the configuration assistants that the installer launches
17. Modify the file '/opt/oracle/network/admin/sqlnet.ora' (or create the file if it does not exist) to contain the following (remove any existing uncommented information in the file):

    ```
    NAMES.DIRECTORY_PATH = (TNSNAMES, HOSTNAME)
    ```

18. To apply the Oracle 9.2.0.6 Patch to the Oracle Installer, from within Disk1 of the Oracle 9.2.0.6 Patch distribution, run the script:

    NOTE: The Oracle 9.2.0.6 Patch will NOT apply unless the Oracle Installer is patched first.

    ```
    ./runInstaller
    ```

19. When progressing through the installer, leave all prompts at their default values unless other wise specified below.
    - At Welcome screen, click next.
    - At the Specify File Locations screen, for Destination Name choose "OUIHome" from the drop-down (or whatever you put as the Destination Name during the install of Oracle 9.2.0.4). Then, click next.
    - At the Select Product to Install screen, choose "Oracle Universal Installer 10.1.0.3.0". Then, click next.
    - At the Summary screen, review the install summary then click install.
    - At the End of Installation screen, click exit.
20. To apply the Oracle 9.2.0.6 Patch to Oracle, from within Disk1 of the Oracle 9.2.0.6 Patch distribution, run the script:

    ```
    ./runInstaller
    ```

21. When progressing through the installer, leave all prompts at their default values unless other wise specified below.
    - At Welcome screen, click next.
    - At the Specify File Locations screen, for Destination Name choose “OUIHome” from the drop-down (or whatever you put as the Destination Name during the install of Oracle 9.2.0.4). Then, click next.
    - At the Select Product to Install screen, choose “Oracle 9iR2 Patchset 9.2.0.6.0”. Then, click next.
    - At the Summary screen, review the install summary then click install.
    - At the End of Installation screen, click exit.
22. Unlink gcc:

```
su – root
rm /usr/bin/gcc
rm /usr/bin/g++
```

23. Exit to return to oracle user prompt.

```
exit
```

Installation of Sentinel 5 for Oracle on Linux

Sentinel 5 supports two installation types. They are:

- Simple – The all-in-one installation option. Sentinel Services, Agent Service, and Applications with Oracle on the same machine. This installation type is only for demonstration purposes.
- Custom – Allows for a fully distributed installation.

Simple Installation on Linux

This installation installs the most common components (does not include Agent Builder or 3rdParty Integration features) on a single machine. This is primarily for demonstration purposes. This is not a recommended for use in a testing or production environment.

> **NOTE**: Simple install does not support Agent Manager password authentication.

How to perform a Simple install

1. Verify you have the collected the information, performed the tasks, and satisfied the requirements specified in the section Pre-Installation of Sentinel 5 for Oracle for the components you are installing.
2. Verify your Linux Oracle setup.
3. Login as the root user.
4. Insert and mount the Sentinel Install CD.
5. Start the install program by going the install directory on the CD-ROM and enter:

   For GUI mode:

```
./setup.sh
```

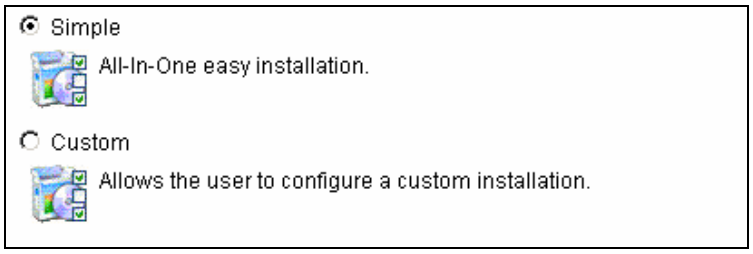
or

For textual (“headless”) mode:

```
./setup.sh –console
```

6. Follow the installer prompts.
7. After reading the Welcome screen, Click Next.
8. Accept End User License Agreement, Click Next.
9. Accept the default install directory or click Browse to specify your installation location. Click Next.

10. Select Simple. Click Next.



11. Enter your configuration information
    - Serial Number and License Key
    - SMTP Server (either the DNS name or IP address) – this is if you want Sentinel to have the ability to send emails
    - Email – enter a valid email address where Advisor notification emails should be sent (e.g. - Sent_Server@myserver.com).
    - Global System Password – enter a password and matching confirm password. This will become the password for all default users. This includes both the esecadm operating system user and the database users. Please see Sentinel Database, within the section Post-Installation of Sentinel 5 for Oracle, for the list of default database users created during installation.
    - Data Directory – the location for your Database data files. To change the default location, click the ... button and select a location. Default is $ESEC_HOME/data

NOTE: The Data Directory must be writable by the oracle user. This can be done by executing the following commands as the root user:

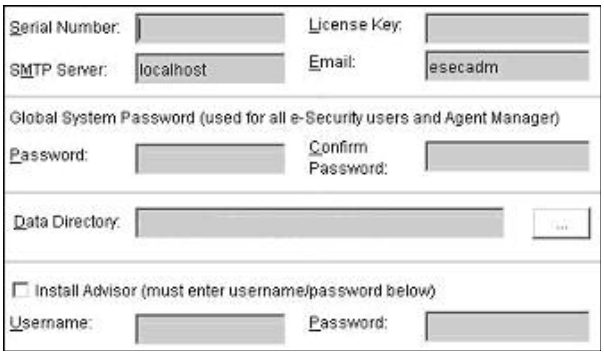
```
chown –R oracle:dba <directory_path>
chmod –R 770 <directory_path>
```

assuming “oracle” is your oracle username and “dba” is your oracle group name.

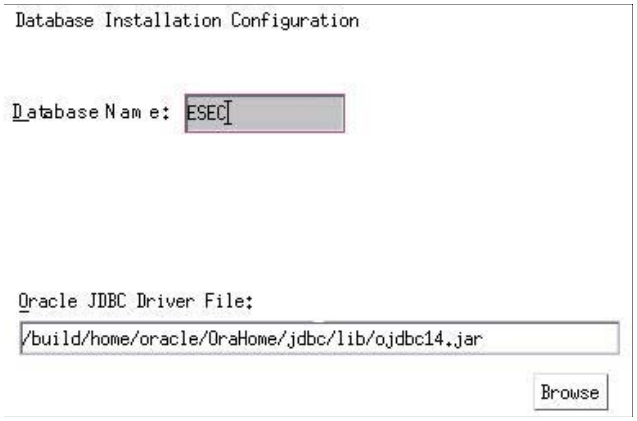
NOTE: If installing Advisor, Simple install will configure Advisor to use Direct Internet Download with an update interval of 12 hours and all email notifications enabled.

- To install Advisor, click the Install Advisor check box. Enter a username and password. If your username or password cannot be verified, after clicking Next you will be asked if you would like to continue (not recommended). If you choose to continue, enter your Advisor password again in the password confirmation window. Otherwise correct your Advisor password.

Click Next.



12. Enter your database configuration information:
    - Database Name – The name of the Oracle database instance to create and install Sentinel Database objects. A database with this name must not already exist.
    - Oracle JDBC Driver File. This is the fully qualified path to the jar file, typically $ORACLE_HOME/jdbc/lib/ojdbc14.jar (cannot use environment variables in this field).



13. Click Ok on the default oracle username.

14. Read the information on the screens that follow and click Next when done. Upon completion of installation, you will need to reboot your system.

> **NOTE**: If you wish to install any 3rd Party Integration software (HP Service Desk or Remedy Integration), after you machine reboots, run the installer again and select which 3rd Party Integration software you wish to install. For more information, see the 3rd Party Integration Guide.

15. 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 will stop accepting events.

Custom Installation on Linux

How to perform a Custom install

1. Verify you have the collected the information, performed the tasks, and satisfied the requirements specified in the section Pre-Installation of Sentinel 5 for Oracle for the components you are installing.
2. Verify your Linux Oracle setup.
3. Login as the root user.
4. Insert and mount the Sentinel Install CD.
5. Start the install program by going to the install directory on the CD-ROM and enter:

   For GUI mode:

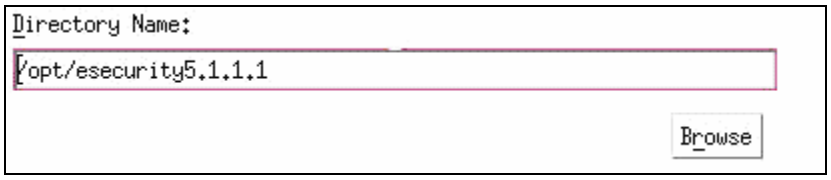
   ```
   ./setup.sh
   ```

   or

   For textual (“headless”) mode:

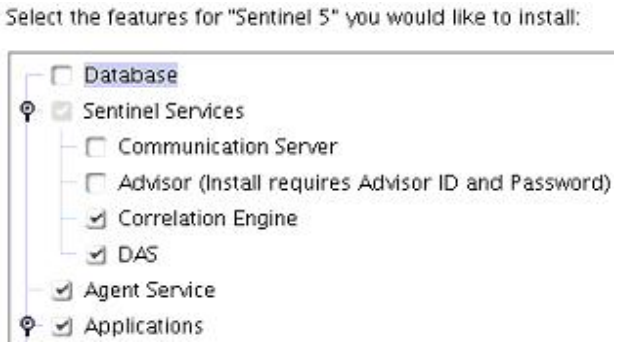
   ```
   ./setup.sh –console
   ```

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



9. Select Custom (default). Click Next.
10. Select which features to install.

> **NOTE**: For more information on which component can be installed where for different configurations, see Chapter 1, System Requirements.



The following options are available:

- Database– installs Sentinel Database
- Communication Server– installs message bus (iSCALE)
- Advisor
- Correlation Engine
- DAS
- Agent Service
- Sentinel Control Center
- Sentinel Data Manager
- HP OpenView Service Desk**
- Remedy Integration**

NOTE: For 5.1.1 Linux, the Base Sentinel Services feature present in 5.1.1 for Windows and Solaris has been folded into the DAS install feature. Allowing this feature to be installed separately provided no known performance benefit.

NOTE: **For information regarding installation of HP OpenView Service Desk or Remedy Integration, see the 3rd Party Integration Guide.

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 appear grayed-out 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/utilities/db folder.

NOTE: For the Linux release (v5.1.1.1), the Windows supported components are Agent Builder and Sentinel Control Center.

11. If you selected to install DAS, you will be prompted for:
    - Serial Number
    - License Key
12. If you selected to install any 3rd party integration components, you will be prompted for a password to unlock the 3rd party integration component(s) you selected. For more information, see the 3rd Party Integration Guide.
13. Specify the operating system e-Security Administrator username and the location of its home directory. This is the username that will own the installed e-Security product. If the user does not already exist, one will be created along with a home directory in the specified directory.
    - OS Administrator username – Default is esecadm
    - OS Administrator user home directory – Default is "/export/home". If esecadm is the username, then the user's home directory will be /export/home/esecadm.

NOTE: If a new user is created, its password will need to be set manually, separately from this installer. e-Security recommends this be done directly by logging into the system following the installation of the product.

In order to meet stringent security configurations required by Common Criteria Certification, e-Security requires a strong password with the following characteristics:

1. Choose passwords of at least 8 with characters in length that includes at least one UPPER CASE, one lower case, one special symbol (#$_) and one numeric (0-9). Do not use blanks.

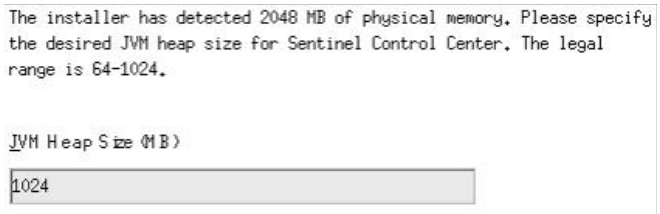
2. Your password may not contain your e-mail name or any part of your full name.

3. Your password should not be a "common" word (for example, it should not be a word in the dictionary or slang in common use).

4. Your password should not contain words from any language, because numerous password-cracking programs exist that can run through millions of possible word combinations in seconds.

5. You should choose a password you can remember and yet is complex. For example, Msi5#YOld (My Son is 5 years old) OR IhliCf5#yN (I have lived in California for 5 years now).

14. If you chose to install Sentinel Control Center, a JVM (Java Virtual Machine) heap size prompt will appear:
    - JVM heap size (MB) - By default, this set to half the size of the physical memory detected on the machine, with a maximum of 1024 MB. This will be the maximum JVM heap size used only by Sentinel Control Center.

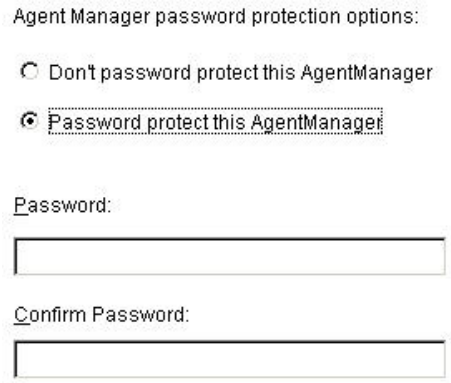


15. If you chose to install Agent Service, select to either protect or not protect the Wizard Agent Manager with a password. If you chose to protect the Wizard Agent Manager, you will be prompted to create a Wizard Agent Manager password.

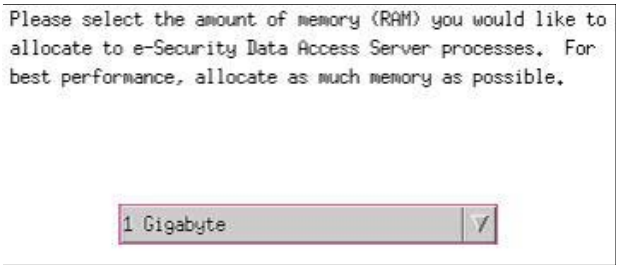
NOTE: Protecting a Wizard Agent with a password will require you to enter this password when uploading, downloading, or debugging Agents on this Wizard Agent Manager. This password is in addition to the Sentinel username and password needed to login to Wizard Agent Builder.

NOTE: In order to meet stringent security configurations required by Common Criteria Certification, e-Security requires a strong password with the following characteristics:

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



16. If you chose to install DAS, select the amount of RAM on your system you wish to allocate for the Data Access Service. For distributed environments, it recommended to select the maximum memory (4 GB). For Standalone environments, it is recommended to select half of your RAM memory.



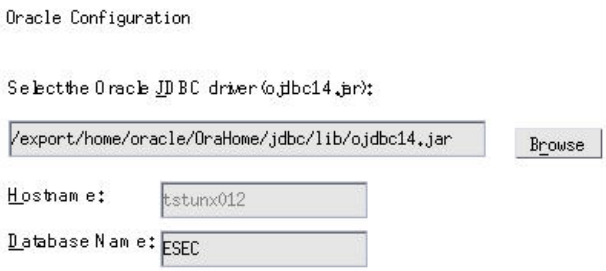
17. For database install, you will have the following prompts

a. Select target database server platform as Oracle 9i and select one of the following:
   - Create a new database with database objects – creates a new Oracle database instance as well as populates the new instance with database objects.
   - Add database objects to an existing empty database – only adds database to an existing Oracle database instance. The existing database instance must be empty, except for the presence of the esecdba user.

b. Enter the database install log directory (default: $ESEC_HOME/logs/db). Accept the default 'Database install log directory' or click Browse to specify a different location.

c. Click Ok on the default oracle username.

d. If you chose to create a new database , enter the following:
   - The path for Oracle JDBC driver file (typical name of the jar file is ojdbc14.jar). This is the fully qualified path to the jar file, typically $ORACLE_HOME/jdbc/lib/ojdbc14.jar (cannot use environment variables in this field).
   - Hostname – The hostname of the machine to install the database. This field is not configurable if creating new database instance.
   - Database Name – The name of the database instance to install.



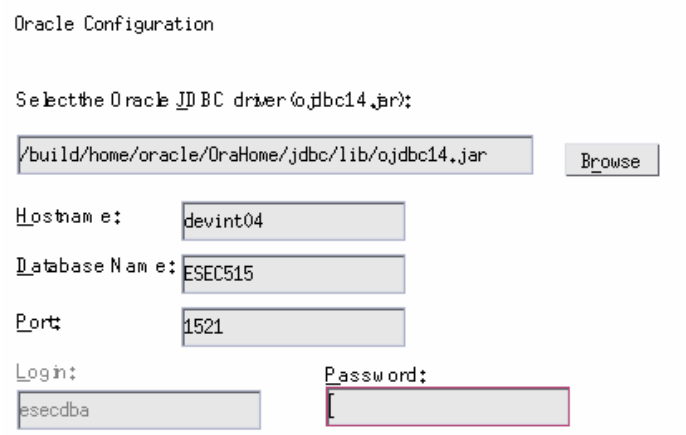
e. If you chose to add database objects to an existing empty Oracle database, you will be prompted for the following information.
   - The path for Oracle JDBC driver file (typical name of the jar file is ojdbc14.jar). This is the fully qualified path to the jar file, typically

$ORACLE_HOME/jdbc/lib/ojdbc14.jar (cannot use environment variables in this field).

- Database hostname or IP address – The name or IP address of the host where the Oracle database is you wish to add database objects to. This can be the local hostname or a remote hostname.
- Database name – The name of the existing empty Oracle database instance you wish to add database objects to (default is ESEC). This database name must appear 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.

NOTE: If the database name is not in the tnsnames.ora, 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 via 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 backwards in the installer one screen and then forward again. This will retry the Database installation with the new values in the tnsnames.ora file.

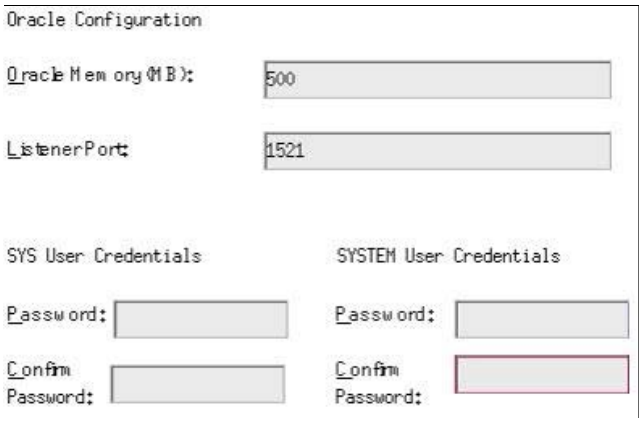
- Database port (default is 1521)
- For e-Security Database Administrator User (DBA), specify the password for the “esecdba” user. The username field in this prompt is not editable.



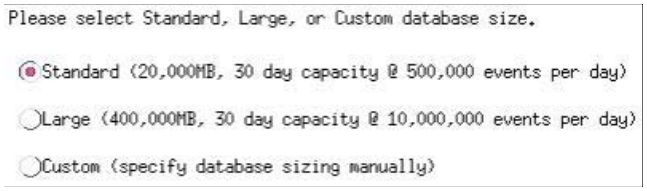
f. If you chose to create a new database, you will see the following prompt:

- Oracle Memory (MB) – The amount of RAM to be allocated to this Oracle database instance.
- Listener Port – the port on which to create an Oracle listener (default is 1521).
- SYS user password and password confirmation – SYS is a default Oracle user that will be created in the new database instance. This user’s password will be set to the value specified here.
- SYSTEM user password and password confirmation - SYSTEM is a default Oracle user that will be created in the new database

instance. This user's password will be set to the value specified here.



g. If you chose to create a new database, you be prompted to enter your database size. You have the following options:
   - Standard (20 GB)
   - Large (400 GB)
   - Custom (specify your size manually). If you choose this option you will be prompted for:
     - initial size of each database file in MB (100 – 10,000)
     - maximum size of each database file in MB (2,000 – 100,000)
     - size of all database files MB (7,000 – 2,000,000)
     - size of each log file in MB (100 – 100,000)



h. If you chose to create a new database, you will be prompted to enter the storage location for the following database files:

NOTE: For recovery and performance purposes, we recommend that these locations be on different I/O devices.

The installer will not create these directories, so they must be created externally before continuing beyond this step.

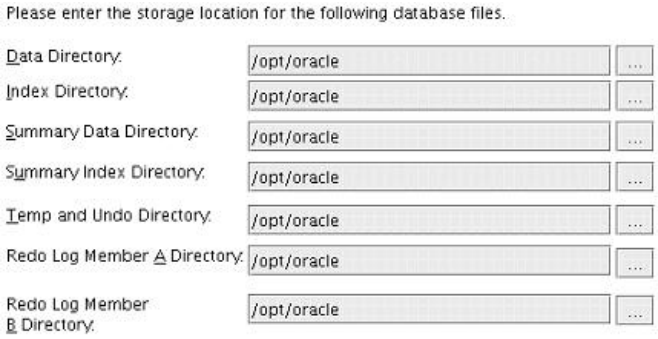
These directories must be writable by the oracle user. To make these directories writable by the oracle user, execute the following commands for each directory as the root user:

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

assuming "oracle" is your oracle username and "dba" is your oracle group name.

   - Data directory
   - Index directory
   - Summary Data directory

- Summary Index directory
- Temporary and Undo Tablespace directory
- Redo Log Member A directory
- Redo Log Member B directory



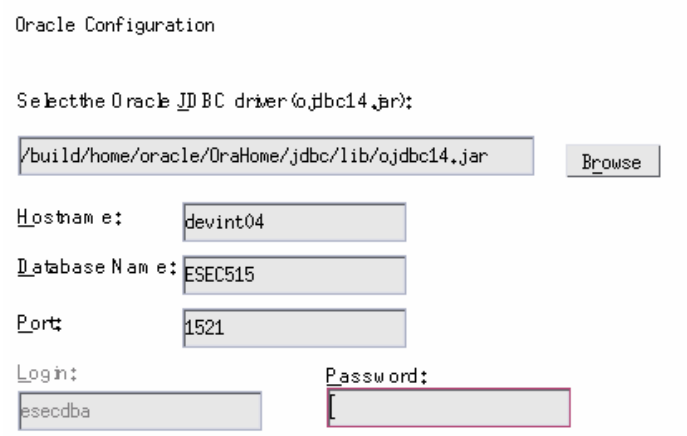
i. If you chose to create a new database, enter authentication information for the e-Security Database Administrator (DBA). This is esecdba, the owner of the database objects.

j. Enter authentication information for the e-Security Application Database user. This is esecapp, the e-Security application username that Sentinel processes use to connect to the database.

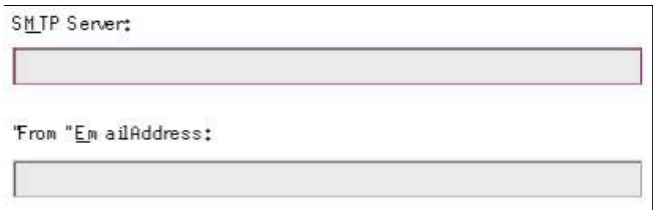
k. Enter authentication information for the e-Security Administrator Database user. This is esecadm, the Sentinel Administrator user.

l. Click Next on the database installation summary window.

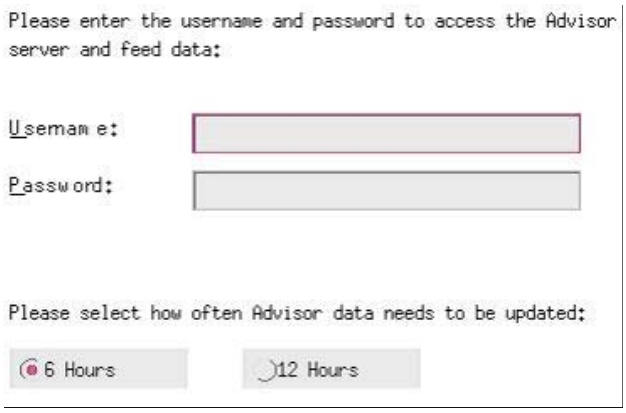
18. If you chose to install DAS, but did not choose to install Sentinel Database, you will be prompted for the following Oracle Sentinel Database information. This information will be used to configure DAS to point to the Sentinel Database.
    - Database hostname or IP address – The name or IP of the existing Oracle Sentinel Database you wish to configure the DAS component to connect to.
    - Database name – The name of the existing empty Oracle database instance you wish to configure the DAS component to connect to (default is ESEC).
    - Database port (default is 1521)
    - For e-Security Application Database User, specify the login “esecapp” and enter the password given for this user during Sentinel Database installation.



19. If you chose to install DAS, configure Sentinel email support. Specify the SMTP server and the from email address the Execution Service should use to send messages (optional – you may manually edit this after install [$ESEC_HOME\sentinel\config\execution.properties]):



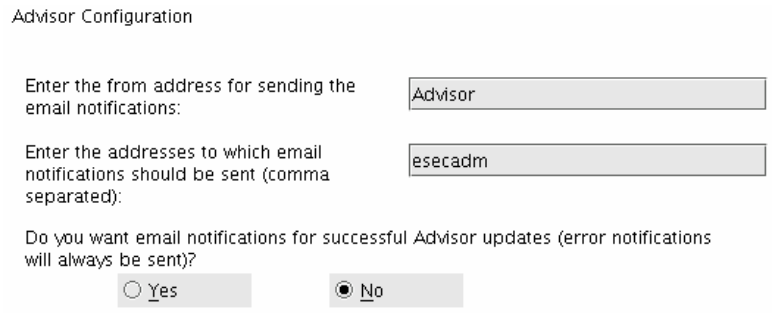
20. If you chose to install Advisor, select the type of Advisor installation (if the Advisor option was chosen a username and password)
    - Direct Internet Download - Advisor machine is directly connected to the Internet. In this configuration, updates from e-Security are automatically downloaded from e-Security over the Internet on a regular schedule.
    - Standalone - Advisor is configured as an isolated system that requires manual intervention to receive an update from e-Security.
21. If you chose to install Advisor and selected to use Direct Internet Download, enter your Advisor username, password and how often Advisor data is to be updated. If your username or password cannot be verified, after clicking Next you will be asked if you would like to continue (not recommended). If you choose to continue, enter your Advisor password again in the password confirmation window. Otherwise correct your Advisor password.



22. If you chose to install Advisor, enter:
    - From address, which will appear in email notifications
    - To address for sending email notifications

> **NOTE**: After installation, you can change the Advisor email addresses by editing the attackcontainer.xml and alertcontainer.xml files in the $ESEC_HOME/sentinel/config directory. For more information, see Chapter 7 – Advisor Tab of the Sentinel User's Guide.

    - Select either Yes or No for if you wish to receive emails for successful Advisor updates. Error notifications will always be sent.



23. If you chose to install HP Service Desk or Remedy Integration, you will be prompted for further information. For more information, see the Sentinel 3rd Party Integration Guide.
24. Read the information on the screens that follow and click Next when done. Upon completion of installation, you will be prompted to reboot. Click Finish to reboot your system.
25. 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 will stop accepting events.
26. If you expect a high event rate (greater than 500 events per sec), you must follow the additional configuration instructions in the section Setting Up The Oracle Call Interface (OCI) Event Insertion Strategy.

Installing Sentinel Control Center and Agent Builder on Windows

NOTE: The only components that can be installed on Windows from the 5.1.1 Linux release are Agent Builder and Sentinel Control Center.

Installing Sentinel Control Center and Agent Builder on Windows

1. Insert the Sentinel installation CD into the CD-ROM drive.
2. Browse to the CD and double-click on setup.bat.

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

3. After reading the Welcome screen, Click Next.
4. Accept the End User License Agreement, click Next.
5. Accept the default install directory or click Browse to specify your installation location. Click Next.

6. Select which features to install.

7. Enter the host address and port where the Communication Server is installed.

8. If you selected to install Sentinel Control Center, a JVM (Java Virtual Machine) prompt will appear:
   - JVM heap size (MB) - By default, this set to half the size of the physical memory detected on the machine, with a maximum of 1024 MB. This will be the maximum JVM heap size used only by Sentinel Control Center.

   Click Next.
9. Click Install.
10. Read the information on the screens that follow and click Next when done. Click Finish.

Post-Installation of Sentinel 5 for Oracle

Updating Sentinel email for SMTP Authentication

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

To configure execution.properties file

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

   ```
   $ESEC_HOME/sentinel/config
   ```

2. Execute mailconfig as follows:

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

   Example:

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

   After entering this command you will be prompted for a new password.

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

NOTE: When using the password option, it must be the last argument.

To test your execution.properties configuration

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

   ```
   $ESEC_HOME/sentinel/config
   ```

2. Execute mailconfigtest as follows:

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

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

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

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

   ```
   Subject: Testing e-Security mail property
   This is a test for e-Security mail property set up. If
      you see this message, your e-Security mail property
      has been configured correctly to send emails
   ```

Sentinel Database

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

- esecdba - Database schema owner. DBA privilege is not granted to esecdba due to security concerns. To use Enterprise Manager, create a user with DBA privileges.
- esecapp – Database application user. This is the application user used to connect to the database.
- esecadm – Database user that is the e-Security Sentinel Administrator. This is not the same user account as the esecadm operating system user.
- esecrpt - Database report user
- SYS – SYS database user
- SYSTEM – SYSTEM database user

Agent Service

During the installation of the Agent Service, the following Agents will be installed and each will have an Agent port setup to run them.

Product	Agent Name
Demo Agents	
Testing for asset upload, works with DemoEvents Agent	DemoAssetUpload
Testing for demo events, works with DemoAssetUpload and DemoVulnerabilityUpload Agent	DemoEvents
Testing for vulnerability upload, works with DemoEvents Agent	DemoVulnerabilityUpload
Test for sending an event	SendOneEvent
Test for sending multiple events	SendMultipleEvents

NOTE: For more information regarding configuration of the Demo Agents, see Chapter 10, Testing the Installation.

NOTE: For additional agents, go to the e-Security Customer Portal to obtain the latest Service Pack for the version you installed. The latest Service Pack for the release you are using will contain the full set of the latest agents available for the version of Sentinel you are using.

For more information (including configuration) go to the documentation provided with each Agent in:

$WORKBENCH_HOME/Elements/<agent name>/Docs/

To install additional agents, run the Service Pack script on the Service Pack CD. The script will install the agents locally.

On Windows:

```
.\service_pack.bat
```

On UNIX:

```
./service_pack.sh
```

For Service Pack installation instructions and listing of agents, see the Service Pack Release notes.

Updating Your License Key

How to update your license key (Linux)

1. Login as user esecadm.
2. Insert and mount the Sentinel Install CD.
3. cd to disk1/utilities/linux.
4. Enter the following command:

   ```
   ./softwarekey
   ```

5. Enter the number 1 for entering your primary key. Press enter.

Creating an Oracle Instance for the Sentinel Database

> **NOTE**: This procedure is provided as an example if you want to create your own tablespaces versus using the tablespace creation feature with the install CD. Your size values may vary depending on your system configuration and requirements. The tablespaces must be named exactly as specified below, however.

In the Oracle instance you will need to configure:

- parameters
- tablespaces

Creating an Oracle Instance

1. Login as an Oracle user.
2. Using the Oracle Database Assistant GUI, create the following:

> **NOTE**: Your values may vary depending on your system configuration and requirements.

Minimum Recommended 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

Minimum Recommended Linux Tablespace Size		
Tablespace	**Example Size**	**Notes**
REDO	3 x 100M	▪ This is a minimum value. You should create larger redo logs if you have a high EPS.
SYSTEM	500M	▪ Minimum value
TEMP	1G	▪ Minimum value
UNDO	1G	▪ Minimum value
ESENTD	5G	▪ Minimum value ▪ This for event data
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
ESENTX2	500M	▪ Minimum value ▪ Index for configuration, assets, vulnerability and associations (autoextend enabled)
SENT_ADVISORD	200M	▪ Minimum value ▪ For Advisor data (autoextend enabled)
SENT_ADVISORX	100M	▪ Minimum value ▪ For Advisor index (autoextend enabled)
SENT_LOBS	100M	▪ Minimum value ▪ For database large objects (autoextend enabled)
SENT_SMRYD	3G	▪ Minimum value ▪ For Aggregation, summary data
SENT_SMRYX	2G	▪ Minimum value ▪ For Aggregation, summary index

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.

Setting Up the Oracle Call Interface (OCI) Event Insertion Strategy

Sentinel 5.1 provides a framework for plugging in different strategies to insert events into the database. Sentinel 5.1 provides two strategies to insert events into the Oracle database

- JDBCLoadStrategy

- OCILoadStrategy

The strategy to be used for inserting events is governed by the insert.strategy property of the EventStoreService component in das_binary.xml.

The JDBC strategy is the default strategy configured out of the box.

The OCI strategy is a native insert strategy for faster event insertion. This strategy requires the Oracle OCI libraries be installed on the machine running the DAS component. The OCI strategy must be used in configurations where a high event rate is expected.

The number of events to be grouped together for insertion into the database is governed by the insert.batchsize property. This insert.batchsize property is used by all the event insert strategies.

To change Sentinel's Event Insertion strategy from the default JDBC Insertion Strategy to the OCI Insertion Strategy, there are a few steps that need to be performed.

Changing Event Insertion strategy from JDBC to OCI Insertion Strategy

1. Ensure the Oracle OCI libraries are installed on the machine running the e-Security DAS component. You will need to know the path to ORACLE_HOME in the following steps.
2. Log into the machine from step 1 as the esecadm user.
3. Create a ".bash_profile" in the esecadm user's home dir. Put the following text in that file (modify the path to ORACLE_HOME to match your installation):

   ```
   ORACLE_HOME=/build/home/oracle/OraHome
   export ORACLE_HOME
   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib
   export LD_LIBRARY_PATH
   ```

4. Open the $ESEC_HOME/sentinel/config/das_binary.xml file for editing in any text editor.
5. Do a search on the following text:

   ```
   JDBCLoadStrategy
   ```

6. Change that text to:

   ```
   OCILoadStrategy
   ```

7. Save this change to the das_binary.xml file.
8. Restart the DAS Binary application. (Restarting DAS Binary can most easily be done by performing a "ps –ef | grep DAS_Binary" to get the process ID, killing that process, and then letting the Sentinel Watchdog automatically restart the process.)

   Once DAS Binary has been restarted, the $ESEC_HOME/sentinel/lib/libocievent.so library will be loaded and used to perform the Event insertions into the database via OCI.

Additional OCI Event Insertion Options

In addition to specifying the “OCILoadStrategy” in the das_binary.xml file, there are several other OCI-related options that can also be configured.

- insert.batchsize – This setting allows you to configure the maximum number of Events to insert into the database at a time.
- insert.oci.workerCount – This setting allows you to configure the number of threads being used to insert Event data into the database.
- insert.oci.queueWaitTime – This setting specifies the max time in seconds to wait before inserting the data from the inbound queue into the database. Whenever a full “batchsize” of events is received, the entire batch is inserted. But if the inbound flow of events is slow, the queue wait time is used to determine when to do the database insertion (even if a full batch of events has not yet been received).
- insert.oci.highWatermark – The inbound Event queue’s high water mark.
- insert.oci.lowWatermark – The inbound Event queue’s low watermark.
- insert.oci.optimizationFlag – Optimization flag. “on” or “off”.

OCI Debugging Tips

The OCI interface will log messages to the $ESEC_HOME/sentinel/log/ocievent.log file. Initial messages written to the log file should include success (or fail) database connection messages… This is a good place to check to verify that the OCI library was loaded and configured correctly.

The OCI interface will also log errors to the das_binary log file located in the $ESEC_HOME/sentinel/log directory. Errors logged to the das_binary log file include failures to locate/load the libocievent.so library, failures to connect to the database, and failures to insert Events/Event Associations.

If error messages indicate that the “libocievent.so” file is not being located or loaded, then there are three things to check:

1. Make sure the Oracle OCI libraries are installed.
2. Make sure that the “libocievent.so” file is located in the $ESEC_HOME/sentinel/lib directory.
3. Make sure that the $ESEC_HOME/sentinel/lib directory is in the “esecadm” user’s “LD_LIBRARY_PATH”. If not, you can update the LD_LIBRARY_PATH in the “esecadm” user’s .profile
4. Make sure that the environment variables ORACLE_HOME and LD_LIBRARY_PATH are updated properly in esecadm’s user environment variables as described in the section “Changing Event Insertion strategy from JDBC to OCI Insertion Strategy”.

Chapter 5 – Installing Sentinel 5 for MS SQL

This chapter describes how to install e-Security Enterprise Security Management Sentinel 5 for MS SQL.

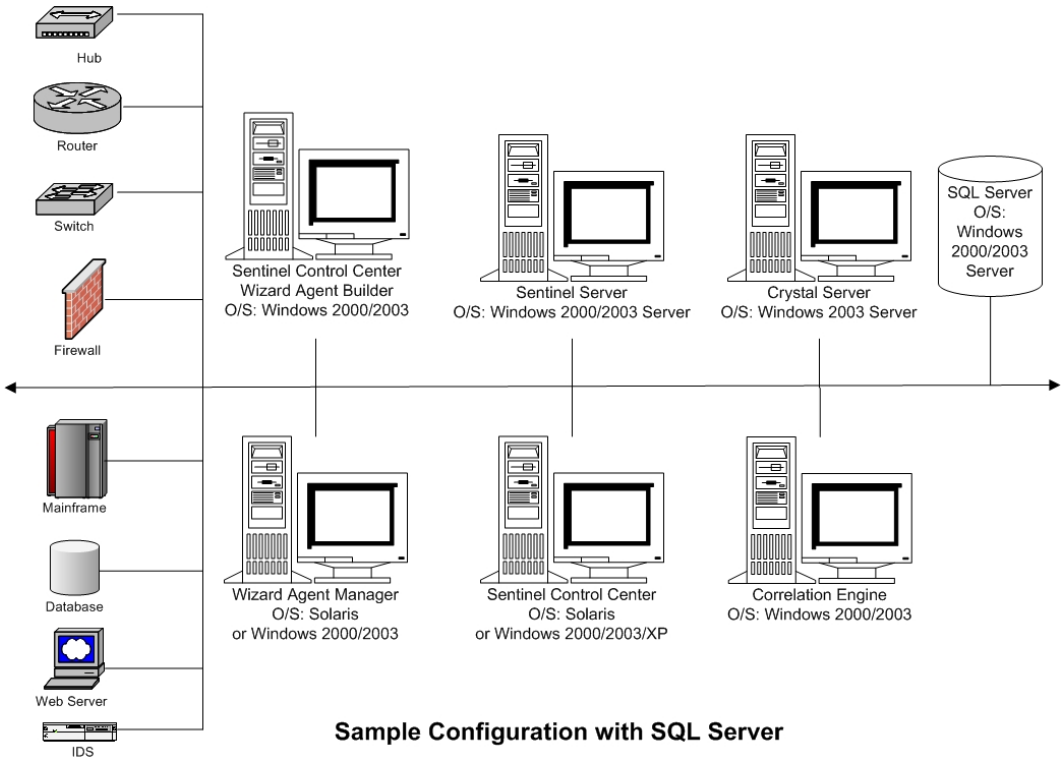
Pre-Installation of Sentinel 5 for MSSQL

NOTE: Before installation, ensure that your machines meet the minimum systems requirements and that the operating system has been "hardened" using current best security practices.

NOTE: e-Security does not support MS clustering or High Availability for Windows.

NOTE: When performing a clean installation of e-Security after having a previous version of e-Security installed, you must remove certain files and system settings that may be left over from a previous installation. Not removing these files or settings could cause a new clean installation to fail. This should be done on every machine you are performing a clean installation. For more information, see Appendix E.

The following is a typical configuration for e-Security Sentinel. Your configuration may be different depending on your environment. Regardless of the configuration you choose, you need to install your database first.



Sample Configuration with SQL Server

Obtaining a License Key

The Sentinel Server Database Access Service (DAS) requires that you have a valid license key in order to install and run the service. This license key is locked to the machine where you are going to install DAS. A license key issued for one machine will not work on another machine.

To obtain your license key, you must determine your host ID number and provide this information to e-Security who will then assign you a license key.

To determine your host ID

1. Insert the Sentinel installation CD into the CD-ROM drive.
2. Browse to the utilities directory on the CD.
3. Run the executable:

   ```
   hostid.exe
   ```

4. Submit this host ID number to e-Security customer support. They will provide you with a license key.

Sentinel Database

Before installing the Sentinel Server, you will need:

- For hardware requirements, see Chapter 1 and 2
- Windows 2000 Server with Service Patch 4 or Windows 2003 Server with Service Patch1
- SQL Server 2000 Enterprise Edition Service Pack 3a installed and running.

> **NOTE**: For performance reasons, it is HIGHLY recommended that depending if you are installing in RAID and if your RAID environment allows, the Transaction Log should point to the fastest write disk you have available.

> **NOTE**: If you installed SQL Server with mixed mode authentication you can login using your Windows login or using SQL Server Authentication. For non-mix mode, you must login using Window Authentication.
>
> To modify your authentication mode settings, in SQL Enterprise Manager, right-click on the server whose settings you'd like to modify (default: (local)(Windows NT)), select properties, click on the Security tab and select 'SQL Server and Windows' or 'Windows Only' for Authentication. The Startup Service Account should be set to 'System account'.

- Target SQL Server Instance Name – (default recommended).

> **NOTE:** If you named your instance during SQL Server install, use this name when prompted for the SQL Server instance name when installing the Database and/or DAS components. If you did not name your instance during SQL Server install, leave the instance name blank during installation (i.e.- if typing in the hostname, do not add "\<instance_name>" to the database hostname).

- Target SQL Server Instance port number (the default is 1433).
- If you are going to use Windows Authentication for one or more of the e-Security users, the corresponding Windows Domain user must exist before

installing the Sentinel Database. The following e-Security users can be assigned to a Windows Domain User:

- e-Security Database Administrator - Database schema owner (e.g. – esecdba)
- e-Security Application User - Used by e-Security applications to connect to the database (e.g. – esecapp)
- e-Security Sentinel Administrator – Administrator for logging into Sentinel Control Center (e.g. - esecadm)
- e-Security Report User – Used for creating reports (e.g. - esecrpt)

Sentinel Server

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

Before installing the Sentinel Server, you will need:

- For hardware requirements, see Chapter 1 and 2
- Windows 2000 Server with Service Patch 4 or Windows 2003 Server with Service Patch 1
- e-Security Sentinel 5 Serial Number and License key (For DAS). For more information, see Obtaining a License Key.
- If installing DAS and using a Windows Domain user account for the e-Security Application user, you must give that user the privilege to 'Log on as a service'. This can be done by opening the 'Local Security Policy' control panel on the machine you are going to install DAS (Start > Settings > Control Panel > Administrative Tools > Local Security Policy). In the Local Security Policy window, go to 'Local Policies > User Rights Assignment'. Open the 'Log on as a service' policy and add the user.

- SMTP Server – This is required to send email from Sentinel.

Sentinel Control Center and Wizard

Before installing the Sentinel Server, you will need:

- For hardware requirements, see Chapter 1 and 2
- Windows 2000 Server with Service Patch 4 or Windows 2003 Server with Service Patch 1.

Advisor

To install Advisor, you will need to obtain an Advisor ID and password from e-Security. Direct Internet Download uses port 443.

> **NOTE:** If you intend use Advisor for Exploit Detection only, you do not need to install Crystal Enterprise software. This is only required if you intend to run Crystal Reports for Sentinel. See Chapter 10, Advisor Configuration for more information.

Installation of Sentinel 5 for MS SQL

Sentinel 5 supports two installation types. They are:

- Simple – The all-in-one installation option. Windows Sentinel Services, Agent Service, and Applications with MS SQL Server all on the same machine. Supports SQL Server authentication only. This installation type is only for demonstration purposes.
- Custom – Allows for a fully distributed installation.

> **NOTE**: By default, the installer sets the following filegroups to NOT autogrow: ESENTD, ESENTX, SENT_SMRYD and SENT_SMRYX. All other filegroups are set to autogrow. The reason for not allowing autogrow for ESENTD, ESENTX, SENT_SMRYD and SENT_SMRYX is that they contain events and summary events data. Space utilization for events and summaries can be highly dynamic. These events filegroups should be monitored and extended in a controlled manner based on your file system configuration and in consideration of IO balancing and database backup and recovery.
>
> SDM partition management (archiving, dropping and adding partitions) should be scheduled to keep events data in a controlled size.

Simple Installation

This installation installs all components (including the database) on a single platform and only supports SQL Server authentication. This is primarily for demonstration purposes. This is not recommended for testing or production use.

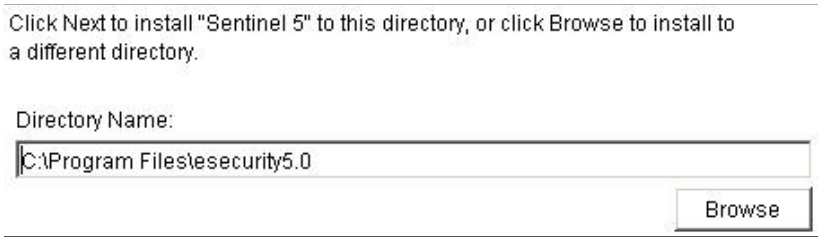
> **NOTE**: Simple install does not support Agent Manager password authentication.

Sentinel Simple Installation

1. Verify you have the collected the information, performed the tasks, and satisfied the requirements specified in the section Pre-Installation of Sentinel 5 for MSSQL for the components you are installing.
2. Insert the Sentinel installation CD into the CD-ROM drive.
3. Browse to the CD and double-click on setup.bat.

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

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



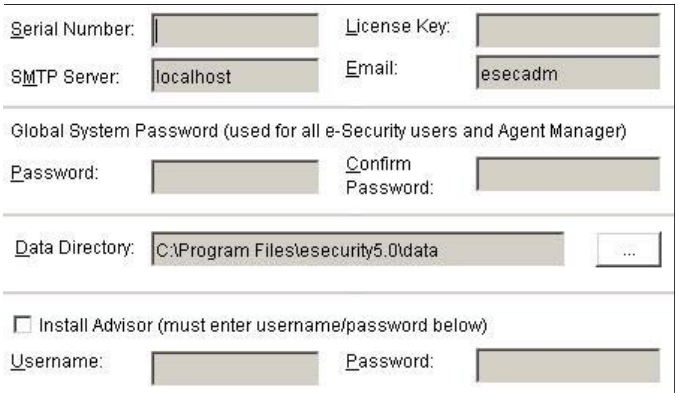
7. Select Simple. Click Next.

8. Enter you configuration information
   - Serial Number and License Key
   - SMTP Server (either the DNS name or IP address) – this is if you want Sentinel to have the ability to send emails
   - Email – enter a valid email address where Advisor notification emails should be sent (e.g. - Sent_Server@myserver.com).
   - Global System Password – enter a password and matching confirm password. This will become the password for all default users. This includes both the esecadm operating system user and the database users. See Sentinel Database, within the section Pre-Installation of Sentinel 5 for MSSQL, for the list of default database users created during installation.
   - Data Directory – the location for all of your Database and Advisor Database data files. To change the default location, click the ... button and select a location. Default is %ESEC_HOME%\data.

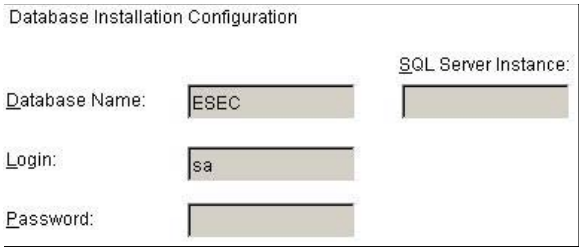
NOTE: If installing Advisor, Simple install will configure Advisor to use Direct Internet Download with an update interval of 12 hours and all email notifications enabled.

   - To install Advisor, click the Install Advisor check box. Enter a username and password. If your username or password cannot be verified, after clicking Next you will be asked if you would like to continue (not recommended). If you choose to continue, enter your Advisor password again in the password confirmation window. Otherwise correct your Advisor password.

   Click Next.



9. For Database installation configuration, enter:
   - sa username and password
   - If you named the SQL Server instance, enter that name



10. Read the information on the screens that follow and click Next when done. Upon completion of installation, you will need to reboot your system.

> **NOTE**: If you wish to install any 3rd Party Integration software (HP Service Desk or Remedy Integration), after your machine reboots, run the installer again and select which 3rd Party Integration software you wish to install. For more information, see the 3rd Party Integration Guide.

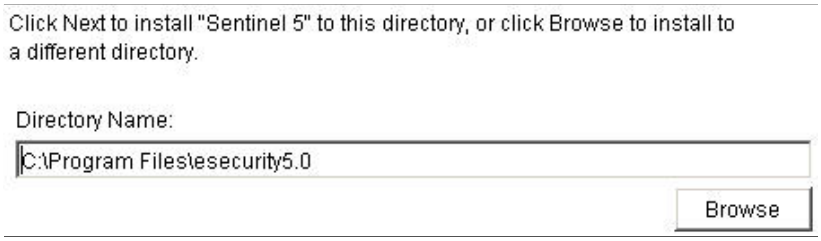
Custom Installation

Sentinel Custom Installation

1. Verify you have the collected the information, performed the tasks, and satisfied the requirements specified in the section Pre-Installation of Sentinel 5 for MSSQL for the components you are installing.
2. Insert the Sentinel installation CD into the CD-ROM drive.
3. Browse to the CD and double-click on setup.bat.

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

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



7. Select Custom (default). Click Next.
8. Select which features to install.

NOTE: For more information on which component can be installed where for different configurations, see Chapter 1, System Requirements.

The follow components can be installed:

- Database – installs Sentinel Database
- Communication Server – installs message bus (iSCALE)
- Advisor
- Base Sentinel Services
- Correlation Engine
- DAS
- Agent Service
- Agent Builder
- Sentinel Control Center
- Sentinel Data Manager
- HP OpenView Service Desk
- Remedy Integration

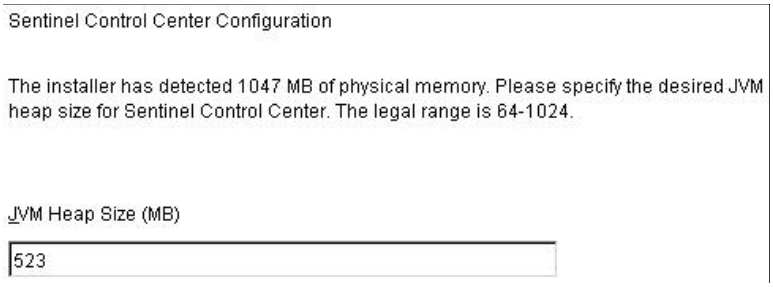
NOTE: For information regarding installation of HP OpenView Service Desk or Remedy Integration, see the 3rd Party Integration Guide.

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 appear grayed-out with a white check mark in it if it is still selected but all of its’ the 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%\utilities\db folder.

9. If you selected to install DAS, you will be prompted for:
   - Serial Number
   - License Key

10. If you selected to install any 3rd party integration components, you will be prompted for a password to unlock the 3rd party integration component(s) you selected. For more information, see the 3rd Party Integration Guide.
11. If you selected to install Sentinel Control Center, a JVM (Java Virtual Machine) prompt will appear:
    - JVM heap size (MB) - By default, this set to half the size of the physical memory detected on the machine, with a maximum of 1024 MB. This will be the maximum JVM heap size used only by Sentinel Control Center.



12. If you chose to install Agent Service, select to either protect or not protect the Wizard Agent Manager with a password. If you chose to protect the Wizard Agent Manager, you will be prompted to create a Wizard Agent Manager password.

NOTE: Protecting a Wizard Agent with a password will require you to enter this password when uploading, downloading, or debugging Agents on this Wizard Agent Manager. This password is in addition to the Sentinel username and password needed to login to Wizard Agent Builder.

NOTE: In order to meet stringent security configurations required by Common Criteria Certification, e-Security requires a strong password with the following characteristics:

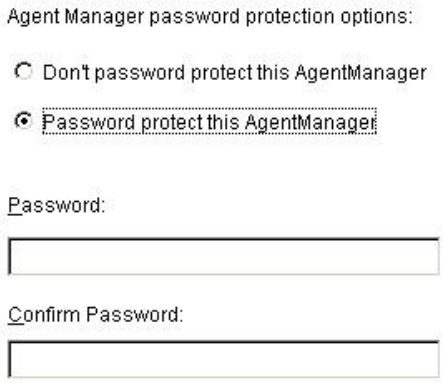
1. Choose passwords of at least 8 with characters in length that includes at least one UPPER CASE, one lower case, one special symbol (!@#$%^&*()_+), and one numeric (0-9).

2. Your password may not contain your e-mail name or any part of your full name.

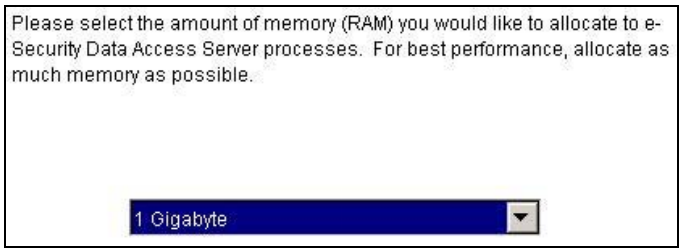
3. Your password should not be a "common" word (for example, it should not be a word in the dictionary or slang in common use).

4. Your password should not contain words from any language, because numerous password-cracking programs exist that can run through millions of possible word combinations in seconds.

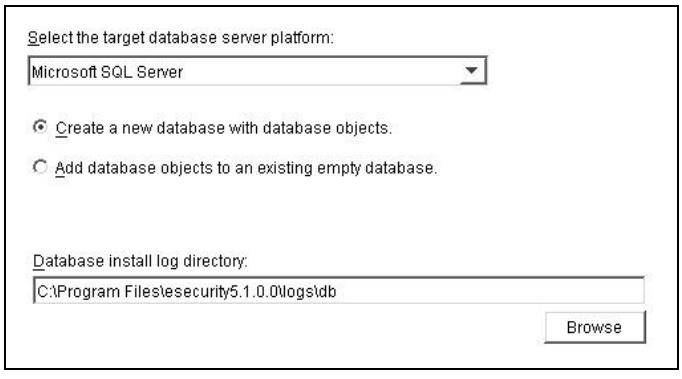
5. You should choose a password you can remember and yet is complex. For example, Msi5!YOld (My Son is 5 years old) OR IhliCf5#yN (I have lived in California for 5 years now).



13. If you chose to install DAS, select the amount of RAM on your system you wish to allocate for the Data Access Service. For distributed environments, it recommended to select the maximum memory (4 GB). For Standalone environments, it is recommended to select half of your RAM memory.

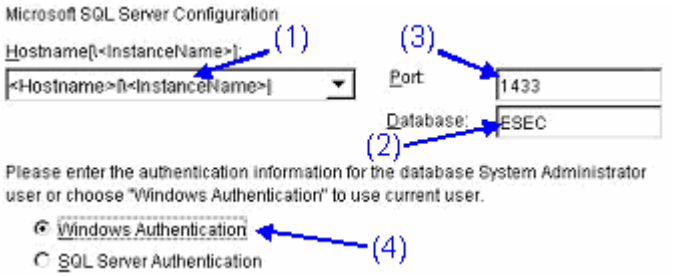


14. For database install, you will have the following prompts
    a. Select target database server platform as Microsoft SQL Server and select one of the following:
        - Create a new database with database objects – creates a new MS SQL database as well as populates the new database with database objects
        - Add database objects to an existing empty database – only adds database to an existing MS SQL database. The existing database must be empty.
    b. Enter the database install log directory (default: %ESEC_HOME%\logs\db). Accept the default 'Database install log directory' or click Browse to specify a different location.

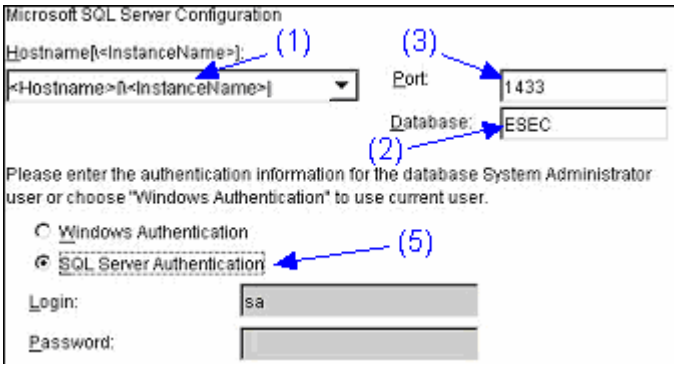


    c. Enter your SQL Server configuration information as follows:

- (1) Database hostname or IP address – by default, your local host machine will appear, if SQL Server is installed locally. If the SQL Server you wish to install does not appear in the drop-down list, select 'Other' in the list. A text box will appear allowing you to type in the hostname. The hostname you type must be fully qualified (e.g. - 'sqlserver.esecurity.net' instead of just 'sqlserver'). If you specified an instance name during SQL Server installation, you will need to add '\<instance_name>' to end of the hostname, where <instance_name> is the name you gave to the instance during SQL Server installation.
- (2) Database name (New Database) – The name to give the new SQL Server database. In addition to the database you name here, another database with the name <your_db_name>_WF will also be created to be used by iTRAC.
- (2) Database name (Existing Database) – The name of the existing empty SQL Server database you wish to add database objects to. Use the database name that does not contain the "_WF" suffix.
- (3) Database port (default is 1433)
- For system database administrator, select either:
  - (4) Windows Authentication - will use the username you are running the installer as.
  - (5) SQL Server Authentication - enter the sa user password



Windows Authentication

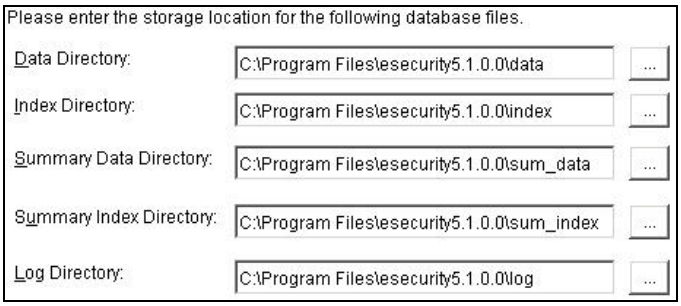


SQL Server Authentication

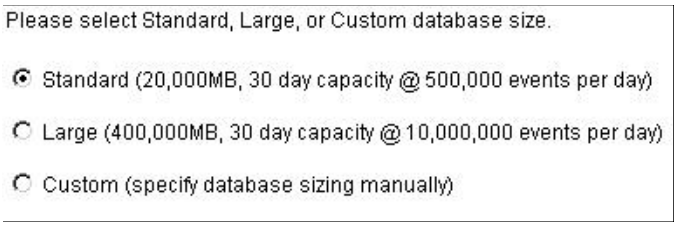
d. If you chose to install a new database, enter the location for the following database files:

NOTE: For recovery and performance purposes, we recommend that these locations be on different I/O devices.

- Data files
- Index files
- Summary Data files
- Summary Index files
- Log files

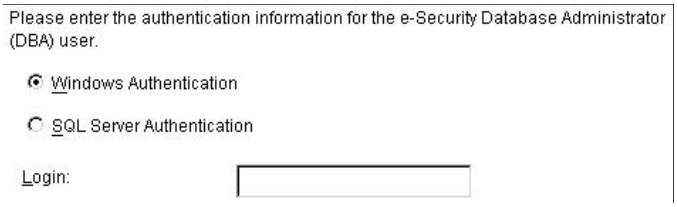


e. If you chose to install a new database, enter your database size:
   - Standard (20,000MB) – 30 day capacity at 500,000 events per day
   - Large (400,000MB) – 30 day capacity at 10,000,000 events per day
   - Custom (specify your size manually). If you choose this option you will also be prompted for:
     (1) size of your database in MB (10,000 – 2,000,000)
     (2) size of each log file in MB (100 – 100,000)
     (3) max size of each database file in MB (2,000 – 100,000)

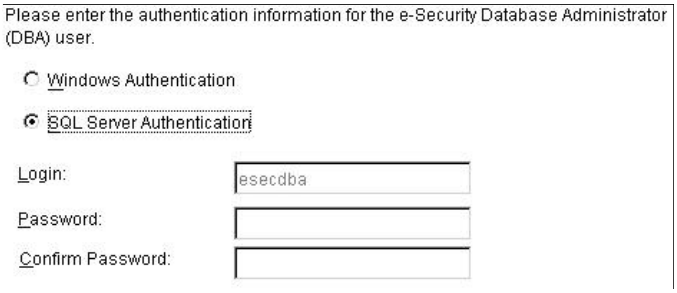


f. For the e-Security Database Administrator (DBA), select either:
   - Windows Authentication, enter <domain name>\<username>
   - SQL Server Authentication (esecdba), password and password confirmation

NOTE: If you select "SQL Server Authentication", you will not be able to modify the default login name.



Windows Authentication



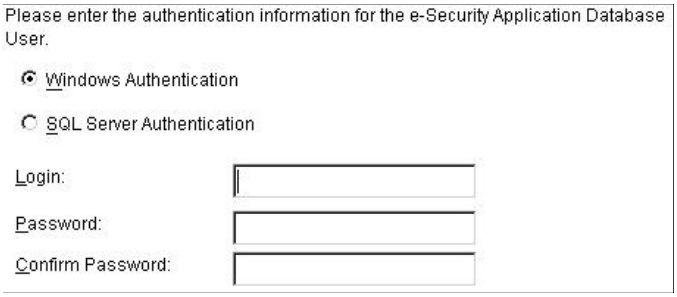
SQL Server Authentication

g. For the e-Security Application Database user, select either:

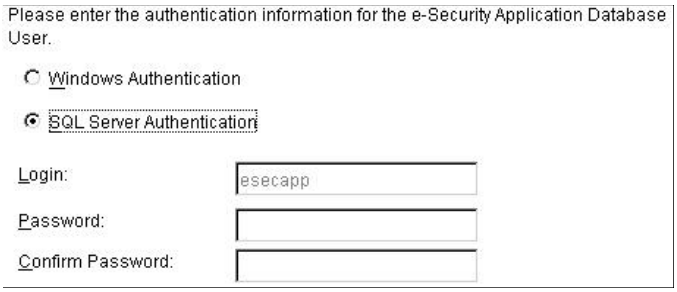
NOTE: If using a Windows Domain login for the e-Security Application Database User, you must give this user the "Log on as Service" privilege on this machine as specified in the section Sentinel Server, within the section Pre-Installation of Sentinel 5 for MSSQL.

- Windows Authentication, enter <domain name>\<username>, password and password confirmation
- SQL Server Authentication (esecapp), enter password and password confirmation

NOTE: If you select "SQL Server Authentication", you will not be able to modify the default login name.



Windows Authentication

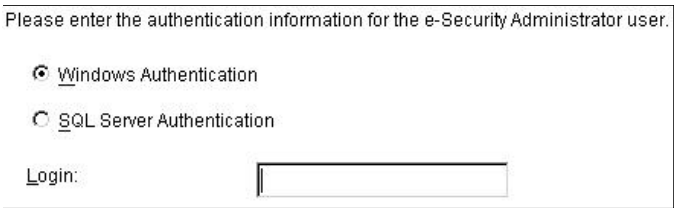


SQL Server Authentication

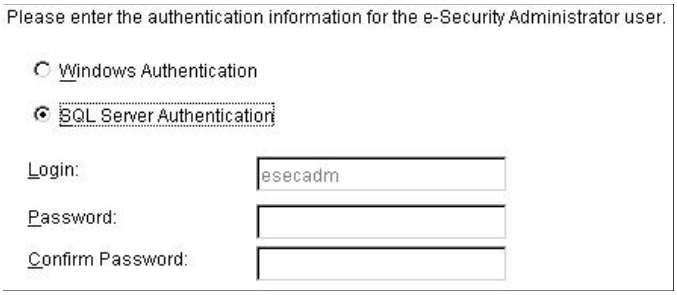
h. For the e-Security Administrator user, select either:

- Windows authentication, enter <domain name>\<username>
- SQL Authentication, enter username for the Sentinel Administrator (default: esecadm), password and password confirmation

NOTE: If you select "SQL Server Authentication", you will not be able to modify the default login name.



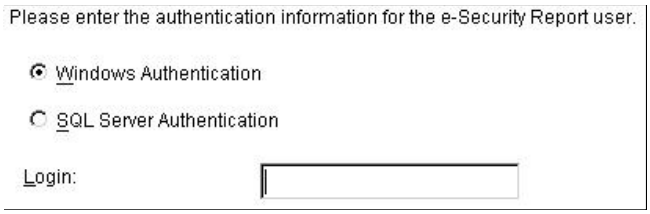
Windows Authentication



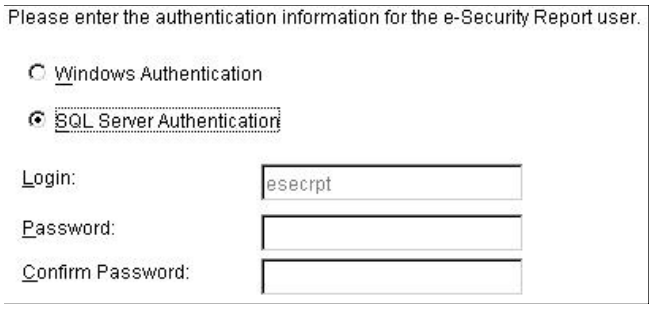
SQL Server Authentication

i. For the e-Security Reporting user, select either:
   - Windows Authentication, enter <domain name>\<username>
   - SQL Authentication (esecrpt), enter password and password confirmation

NOTE: If you select "SQL Server Authentication", you will not be able to modify the default login name.



Windows Authentication



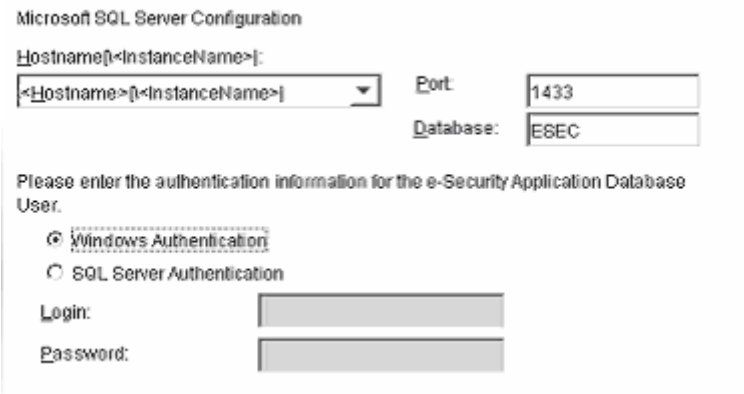
SQL Server Authentication

j. Click Next on the database installation summary window.

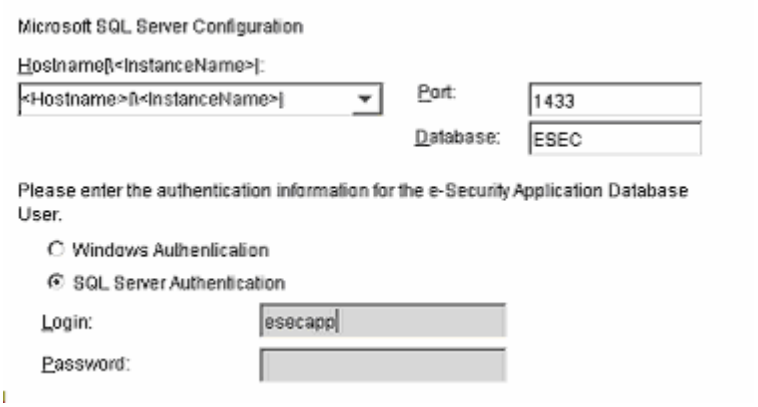
15. If you chose to install DAS, but did not choose to install Sentinel Database, you will be prompted for the following SQL Server Sentinel Database information. This information will be used to configure DAS to point to the Sentinel Database.
    - Database hostname or IP address – by default, your local host machine will appear, if SQL Server Sentinel Database is installed locally. If the SQL Server Sentinel Database you wish to configure DAS to connect to does not appear in the drop-down list, select 'Other' in the list. A text box will appear allowing you to type in the hostname. The hostname you type must be fully qualified (e.g. - 'sqlserver.esecurity.net' instead of just 'sqlserver'). If you specified an instance name during SQL Server installation, you will need to add '\<instance_name>' to end of the hostname, where <instance_name> is the name you gave to the instance during SQL Server installation.
    - Database name – The name of the existing SQL Server Sentinel Database you wish to configure DAS to connect to. Use the database name that does not contain the "_WF" suffix.
    - Database port (default is 1433)
    - For e-Security Application Database User, select either:

NOTE: If using a Windows Domain login for the e-Security Application Database User, you must give this user the "Log on as Service" privilege on this machine as specified in the section Sentinel Server, within the section Pre-Installation of Sentinel 5 for MSSQL.

    - Windows Authentication – Specify the Windows Domain login given for this user during Sentinel Database installation and enter the password for this user. The password is needed here to configure the e-Security Windows Service to "Log on as Service" as this Windows Domain login.
    - SQL Server Authentication – Specify the login "esecapp" and enter the password given for this user during Sentinel Database installation.

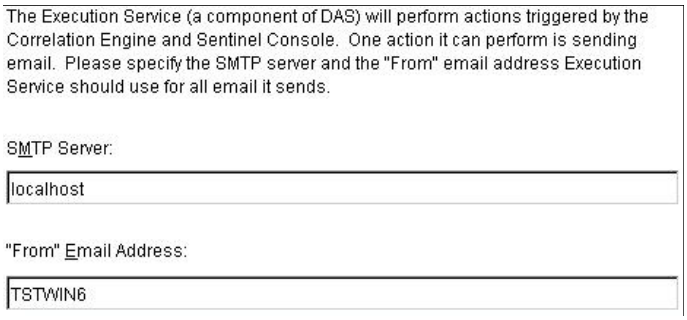


Windows Authentication

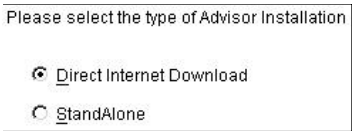


SQL Authentication

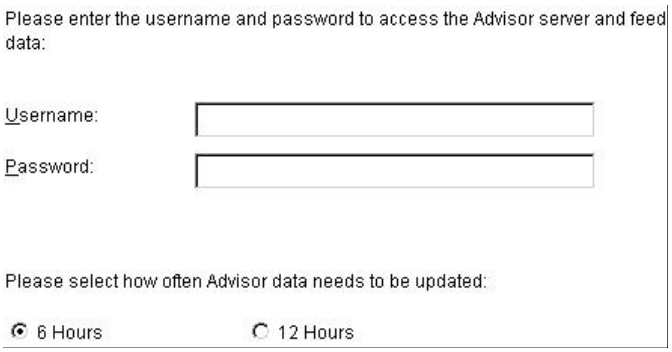
16. If you chose to install DAS, configure Sentinel email support. Specify the SMTP server and the from email address the Execution Service should use to send messages (optional – you may manually edit this after install [%ESEC_HOME%\sentinel\config\execution.properties]):



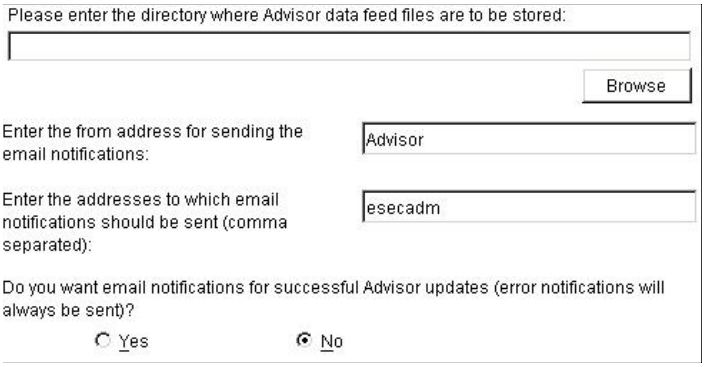
17. If you chose to install Advisor, the following prompt for the type of installation will appear:
    - Direct Internet Download - Advisor machine is directly connected to the Internet. In this configuration, updates from e-Security are automatically downloaded from e-Security over the Internet on a regular schedule.
    - Standalone - Advisor is configured as an isolated system that requires manual intervention to receive an update from e-Security.



18. If you chose to install Advisor and selected to use Direct Internet Download, enter your Advisor username, password and how often Advisor data is to be updated. If your username or password cannot be verified, after clicking Next you will be asked if you would like to continue (not recommended). If you choose to continue, enter your Advisor password again in the password confirmation window. Otherwise correct your Advisor password.



19. If you chose to install Advisor, enter:
    - The directory where the Advisor data feed files will to be stored. This is the location the attack and alert feed files will be saved when they are downloaded
    - To address for sending email notifications
    - Select either Yes or No for if you wish to receive emails for successful Advisor updates. Error notifications will always be sent.



NOTE: After installation, you can change the Advisor email addresses by editing the attackcontainer.xml and alertcontainer.xml. For more information, see Chapter 7 – Advisor Tab of the Sentinel User's Guide.

20. If you chose to install HP Service Desk or Remedy Integration, you will be prompted for further information. For more information, see the Sentinel 3rd Party Integration Guide.
21. Read the information on the screens that follow and click Next when done. Upon completion of installation, you will be prompted to reboot.
22. Click Finish to reboot your system.
23. If you expect a high event rate (greater than 800 events per sec), you must follow the additional configuration instructions in the section Setting Up the Active Data Objects (ADO) Event Insertion Strategy.

Post-Installation of Sentinel 5 for MS SQL

Updating Sentinel email for SMTP Authentication

If your system requires SMTP authentication, you will need to update your execution.properties file. This file is on the machine that has DAS installed. It is located at %ESEC_HOME%\sentinel\config. To configure this file, run mailconfig.bat to change the file and mailconfigtest.bat to test your changes.

To Configure execution.properties file

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

   ```
   %ESEC_HOME%\sentinel\config
   ```

2. Execute mailconfig as follows:

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

   Example:

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

   After entering this command you will be prompted for a new password.

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

NOTE: When using the password option, it must be the last argument.

To test your execution.properties configuration

1. On the machine where you have DAS installed, cd to:

   ```
   %ESEC_HOME%\sentinel\config
   ```

2. Execute mailconfigtest as follows:

   ```
   mailconfigtest.bat -to <destination email address>
   ```

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

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

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

   ```
   Subject: Testing e-Security mail property
   This is a test for e-Security mail property set up. If
      you see this message, your e-Security mail property
      has been configured correctly to send emails
   ```

Sentinel Database

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

- esecdba - Schema owner (if using Windows Domain user, configurable at install time)
- esecapp – User name used by e-Security applications to connect to the database (if using Windows Domain user, configurable at install time)
- esecadm - Sentinel administrator (if using Windows Domain user, configurable at install time)
- esecrpt - Reporter user (if using Windows Domain user, configurable at install time)

Agent Service

During the installation of the Agent Service, the following Agents will be installed and each will have an Agent port setup to run them.

Product	Agent Name
Demo Agents	
Testing for asset upload, works with DemoEvents Agent	DemoAssetUpload
Testing for demo events, works with DemoAssetUpload and DemoVulnerabilityUpload Agent	DemoEvents
Testing for vulnerability upload, works with DemoEvents Agent	DemoVulnerabilityUpload
Test for sending an event	SendOneEvent
Test for sending multiple events	SendMultipleEvents

NOTE: For more information regarding configuration of the Demo Agents, see Chapter 11, Testing the Installation.

NOTE: For additional agents, go to the e-Security Customer Portal. For more information (including configuration) go to the documentation provided with each Agent in:

%WORKBENCH_HOME%\Elements\<agent name>\Docs\

To install additional agents, run the Service Pack script on the Service Pack CD. The script will install the agents locally.

On Windows:

```
.\service_pack.bat
```

On UNIX:

```
./service_pack.sh
```

For Service Pack installation instructions and listing of agents, see the Service Pack Release notes.

Updating Your License Key

If your e-Security license key has expired and e-Security has issued you a new one, run the software key program to update your license key.

How to update your license key

1. Login as a use with administrative rights.
2. Go to %ESEC_HOME%\utilities.
3. Enter the following command:

   ```
   softwarekey.exe
   ```

4. Enter the number 1 for entering your primary key. Press enter.

Configuration Instructions for Using SQL Server Windows Authentication with DataDirect JDBC Driver

> **NOTE**: The following is taken from DataDirect Connect© for JDBC© Installation Guide. e-Security recommends that the following be done by your system administrator.

After installation of Connect for JDBC, some configuration is required on the following components to use Windows authentication on SQL Server:

- SQL Server database server
- Domain Controller
- Client Workstation

For more information about Windows authentication and the Connect for JDBC SQL Server driver, refer to the DataDirect Connect for JDBC User's Guide and Reference.

SQL Server Database Server

This section describes the configuration that is required on the SQL Server database server to use Windows authentication with the Connect for JDBC SQL Server driver.

Service Principle Name

To use the Kerberos authentication protocol, one Service Principle Name (SPN) for each SQL Server instance must be registered. A SPN is a unique name that maps the SQL Server service for a particular machine and port to an account name used to start the service (Service Startup Account). A SPN is composed of the following elements:

- Service class name is always MSSQLSvc for SQL Server
- Host name is the fully qualified DNS name of the machine running SQL Server
- Port is the port number on which the SQL Server instance is listening

For example: MSSQLSvc/DBServer.test:1433 is a SPN for a SQL Server instance running on a machine named DBServer in the test domain and listening on port 1433.

Listing SPNs

Check with your database or domain administrator to make sure that the appropriate SPNs have been registered for each SQL Server instance. Your database or domain administrator can use the Windows command ldifde to list registered SPNs.

Registering SPNs

If necessary, your database or domain administrator can register SPNs using the Setspn tool available with the Windows Resource Kit. For example:

```
setspn -A MSSQLSvc/DBServer.test:1433 sqlsvc
```

registers a SPN that maps the Service Startup Account named sqlsvc to a SQL Server instance running on a machine named DBServer in the test domain and listening on port 1433.

The Setspn tool is available from the following Web site: http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/setspn-o.asp.

Refer to the Microsoft documentation accompanying the Setspn tool for instructions on using it.

> **NOTE**: If the SQL Server Startup account is changed, SPNs for SQL Server must be deleted and re-registered.

Authentication Mode

To use Windows authentication, the SQL Server authentication mode can be set to one of the following modes:

- Windows Only authentication
- Mixed authentication

If SQL Server authentication will be used in addition to Windows authentication, the authentication mode must be set to use Mixed authentication.

Domain Controller

The SQL Server driver supports Windows authentication when the Kerberos Key Distribution Center (KDC) is running on a Windows 2000 domain controller. When communicating with the KDC, the messages passed between the KDC and SQL Server is encrypted.

Because SQL Server can only use the DES-CBC-MD5 encryption algorithm, the SQL Server Service Startup Account on the domain controller must contain the Active Directory property "Use DES encryption types for this account." Check with your domain administrator to verify that this property is set for the SQL Server Service Startup Account. The SQL Server Service Startup Account cannot be used as the Client login account.

Client Machine

This section describes the configuration that is required on the client machine to use Windows authentication with the Connect for JDBC SQL Server driver.

Kerberos Configuration File

The Kerberos login module requires the Kerberos realm name (Windows domain name) and the KDC name (Windows domain controller name) for that Kerberos realm. When you install Connect for JDBC, a configuration file is installed that specifies a generic Kerberos realm and KDC name. This file is named krb5.conf and is installed in the /lib directory of the Connect for JDBC installation directory.

You must modify the krb5.conf file to specify the Kerberos realm name and KDC name for your environment. If this file is not modified to include a valid Kerberos realm and KDC name, the following error is generated:

```
Message:[DataDirect][SQLServer JDBC Driver]Could not
     establish a connection using integrated security:
     No valid credentials provided
```

The Connect for JDBC SQL Server driver automatically configures the Kerberos login module to load the krb5.conf Kerberos configuration file unless the

java.security.krb5.conf system property is already set to point to another configuration file. You can override the Kerberos realm name and KDC name specified in the krb5.conf file by specifying the following system properties: java.security.krb5.realm and java.security.krb5.kdc.

Setting Up the Active Data Objects (ADO) Event Insertion Strategy

Sentinel 5.1 provides a framework for plugging in different strategies to insert events into the database. Sentinel 5.1 provides two strategies to insert events into the MS SQL database:

- JDBCLoadStrategy
- ADOLoadStrategy

The strategy to be used for inserting events is governed by the insert.strategy property of the EventStoreService component in das_binary.xml.

The JDBC strategy is the default strategy configured out of the box.

The ADO strategy is a native insert strategy for faster event insertion. This strategy requires the additional Windows packages be installed on the machine running the DAS component. See the section below for information on what packages must be installed. The ADO strategy must be used in configurations where a high event rate is expected.

The number of events to be grouped together for insertion into the database is governed by the insert.batchsize property. This insert.batchsize property is used by all the event insert strategies.

The sections below describe how to switch to ADO load strategies.

Prerequisites for ADOLoadStrategy

The ADO native connector needs the .net framework and the J# redistributable package to be installed on the machine running DAS Binary.

> **NOTE:** You will need to uninstall any older versions of the .net framework and the J# redistributable package and install the versions listed in the following order.

- net framework 2.0 Beta 2 available at http://www.microsoft.com/downloads/details.aspx?FamilyID=7ABD8C8F-287E-4C7E-9A4A-A4ECFF40FC8E&displaylang=en
- visual J# version 2.0 Beta 2 available at http://www.microsoft.com/downloads/details.aspx?FamilyId=A2788A92-76AB-4BF4-893A-FA9FD5031F14&displaylang=en

Setting up ADO Load Event Insertion Strategy

To change Sentinel's Event Insertion strategy from the default JDBC Insertion Strategy to the ADO Insertion Strategy, there are a few steps that need to be performed.

Changing from JDB Insertion Strategy to ADO Insertion Strategy

1. Using a text editor, open %ESEC_HOME%\sentinel\config\das_binary.xml.

2. Do a search on the following text:

   ```
   JDBCLoadStrategy
   ```

3. Change that text to:

   ```
   ADOLoadStrategy
   ```

4. Save this change to the das_binary.xml file.
5. Restart the DAS Binary application.

Once DAS Binary has been restarted, the %ESEC_HOME%\Sun-1.4.2\bin\ EventInsert.dll and EventJNICLIBridge.dll will be loaded and used to perform the Event insertions into the database via ADO.

ADO Debugging Tips

The ADO interface will only log error messages to the %ESEC_HOME%\sentinel\log\ADOEventStoreError.log file. Initial error messages written to the log file may include database connection failed messages. This file will also log exceptions that occur while inserting events into the database. Please note: only Errors are logged to this file,

To verify ADO connected and loaded properly please check the das_binary log file located in the %ESEC_HOME%\sentinel\log directory.

The ADO interface also logs errors to the das_binary log file located in the %ESEC_HOME%\sentinel\log directory. Errors logged to the das_binary log file include failures to locate/load the EventJNICLIBridge.dll, failures to connect to the database and failures to insert Events/Event Associations.

If error messages indicate that the native connectors have not been loaded properly, check the following:

- Make sure that the machine has the right version of .net framework and J# redistributable package installed.
- Make sure that the “EventJNICLIBridge.dll” and the “EventInsert.dll” files are located in the %ESEC_HOME%\Sun-1.4.2\bin\ directory.

Chapter 6 - Data Migration and Patch for Oracle on Solaris

This chapter discusses:

- Data Migration and Upgrade from v4.2.1 to v5.1

  NOTE: For upgrading, you cannot go directly from v4.2.1 to v5.1.1. You must data migrate to v5.1 and then patch to v5.1.1.

- Patch from v5.0.0 or v5.0.1 to v5.1
- Patch from v5.1 to v5.1.1

  NOTE: You cannot go directly from v5 to v5.1.1. Patch paths are v5 or v5.0.1 to v5.1 and v5.1 to v5.1.1. If you are patching from v5 or v5.0.1 to v5.1.1, you must first patch to v5.1 before patching to v5.1.1.

Data Migration and Upgrade from v4.2 to v5.1

Sentinel Server Components

Sentinel 5 requires that the previous version of the software be uninstalled before adding the sentinel 5 server components. Do not uninstall the previous version (v4.2) Database. This is required for data migration. Backup the Sentinel server machine ($ESEC_HOME install directory and Root Drive). This will allow you to restore v4.2 in case there are any unexpected failures.

The details of the migration and installation pre and post steps can be found below.

Agent Manager

Backup the v4.2 Agent Manager machine. v4.2 Agent Managers must be completely uninstalled before installing the v5 Agent Manager software.

For each machine running v4.2 Agent Manager with at least one port configured, save a copy of the contents of the following directories in an easy to access location. The contents of these directories will be used during post-migration to quickly reconfigure the Agents ports setup in your v4.2 install:

- $WORKBENCH_HOME/Agents - Contains the port configuration files.
- $WORKBENCH_HOME/Elements – Contains the Agent scripts.

If you do not make a copy of the contents of the above directories, you will need to reconfigure all Agent scripts and ports from scratch.

NOTE: v4.2 Agent Manager and Agent Builder is not compatible with v5 components.

Crystal Reporting Server

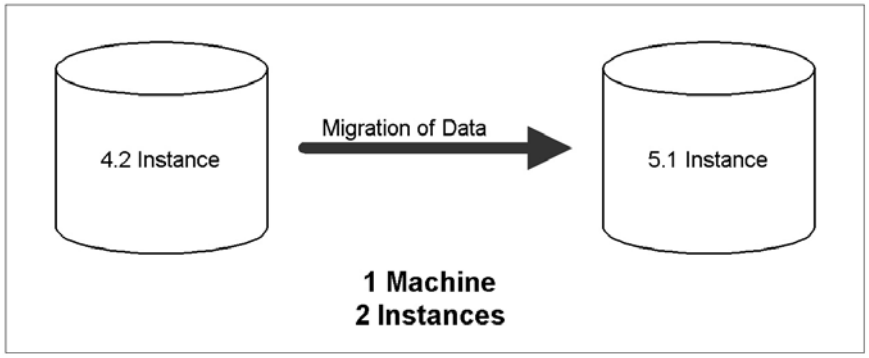
If you are only upgrading to v5.1, you must use the new reports provided with the v5 CD. The new reports are written to work with the new DB schema. If you are patching to v5.1.1, you must upgrade your Crystal Server from Crystal Enterprise 9 Standard® to Crystal BusinessObjects Enterprise™ 11. In addition, Sentinel 5 does not support Crystal XI on Windows® 2000 Server.

NOTE: Sentinel 5 does not support Crystal XI on Windows® 2000 Server.

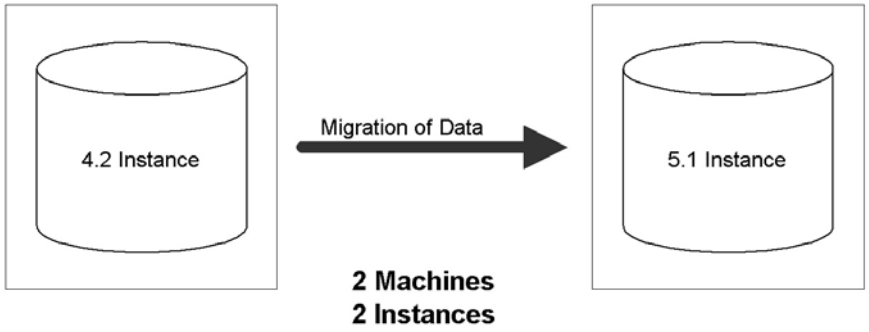
Database Server

Sentinel 5 data migration is provided to migrate data from Sentinel v4.2 on Solaris 8/9 to Sentinel 5.1 on Solaris 9. The data migration utility supports migration on:

- 1 machine with 2 instances



- 2 machines with 2 instances



The following is migrated:

- Users and assigned privileges created in v4.2 will migrate to Sentinel 5.
- Filters
- Right-click menu configuration options.
- Any renamed CV tags
- Partition and archive configurations
- Cases from v4.2 migrate over as incidents
- Incidents and incident-related events get migrated.

NOTE: Migration of data will NOT migrate event data. Only data associated with incidents.

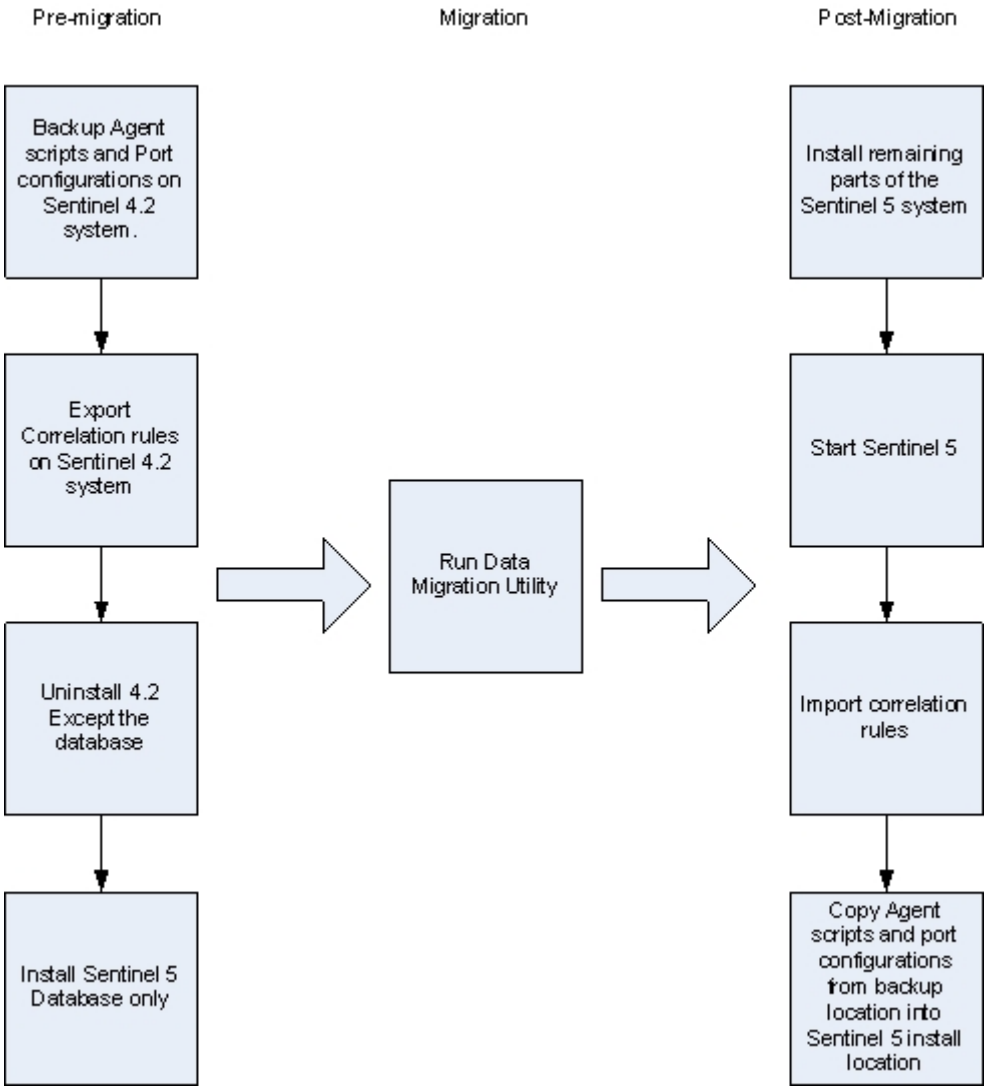
NOTE: Incident event data is not viewable through the Sentinel Console. Incident event data can be seen through SQL or Crystal Reporting.

Data migration and Sentinel 5 upgrade comprises of:

- Pre-migration
  - Backup Sentinel server Database Instance: This will allow you to restore v4.2 database in case there are any unexpected failures.

- Copy or save and right click system commands or scripts that may be under the $ESEC_HOME directory
- Copy Agents scripts and port configurations to backup location.
- Export Sentinel v4.2 correlation rules (if any)
- Except for the database, uninstall Sentinel v4.2
- Install Sentinel 5 database only

- Migration
  - Run the data migration utility
- Post migration
  - Install remaining component of Sentinel 5
  - Start Sentinel 5
  - Import correlation rules (if any)
  - Copy Agent scripts and port configurations from backup location into Sentinel 5 install location.
  - Reconfigure Crystal Reporting (Oracle 9i Client) and import Sentinel 5 Crystal Report Templates



NOTE: On Solaris, the Data Migration Utility uses Oracle*Net to connect to the Sentinel 5 database and between Sentinel 5 and 4.2 databases. Ensure that the tnsnames.ora file contains entries for both Sentinel 4.2 and 5 database so that Oracle*Net connections can be established.

Pre-migration – Exporting of Correlation Rules

Exporting a Correlation Rule Set

1. In the v4.2 Sentinel Console, under the Admin tab open the Correlation Rules window.
2. Select a Rule Set.
3. Click Export. A file browser will open, browse to the target device to write the rule to and click OK. The rule set will be exported as an xml file.

Pre-migration – Backup of Agent scripts and port configuration

Backing up Agent scripts and port configuration

1. On all Sentinel v4.2 machines running Agent Manager, create a directory to store all Agents scripts and port configurations for that machine.
2. In the directory you just created, created a text file that lists the name of all the Agents that are being used by a port configuration on this Agent Manager. Use an Agent Builder to determine the Agents being used by this Agent Manager. If this Agent Manager is on Solaris, you will need to use an Agent Builder on a Windows machine (Agent Builder is not supported on Solaris).
3. Copy the following directories into the directory you just created:
   - $WORKBENCH_HOME/Agents
   - $WORKBENCH_HOME/Elements

Pre-Migration – Uninstalling v4.2

Uninstalling v4.2

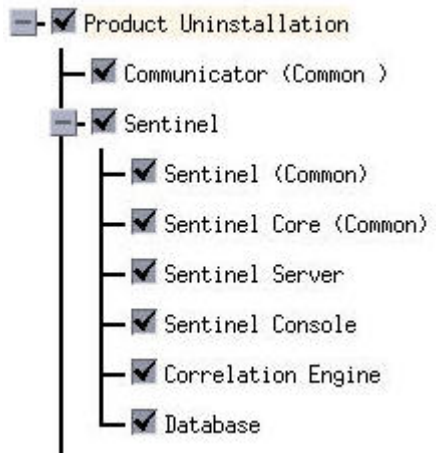
1. On your Sentinel v4.2 machine and any client machines, close all Sentinel Consoles and Agent Builders.
2. Login as user root.
3. Stop the Sentinel Server.
4. cd to:

   ```
   $ESEC_HOME/_uninst
   ```

5. Enter:

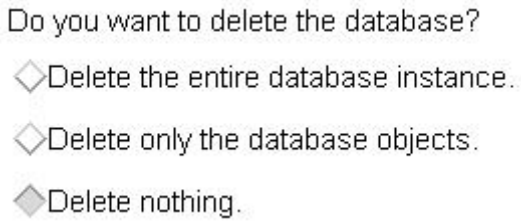
   ```
   ./uninstall.bin
   ```

6. Follow the screen prompts. Select which applications to uninstall. Select all of the features.



NOTE: If you have any 3rd party software, select to uninstall.

7. Click through the screen prompts to the Database Uninstall window.
8. In the Database Uninstall window, select 'Delete nothing'.



9. Click through the remaining uninstall windows.
10. Reboot your system

Pre-Migration – Installing Sentinel 5 Database

Sentinel 5 Database Installation

1. Verify you have the collected the information, performed the tasks, and satisfied the requirements specified in the section Sentinel Database in Chapter 3: Installing Sentinel 5 for Oracle > Pre-Installation of Sentinel 5 for Oracle.
2. Verify your Oracle Setup by reviewing the section Oracle Setup in Chapter 3: Installing Sentinel 5 for Oracle > Pre-Installation of Sentinel 5 for Oracle.
3. Login as the root user.
4. Insert and mount the Sentinel Install CD.
5. On the CD, browse to the full directory.
6. Start the install program by going to the install directory on the CD-ROM and enter:

   For GUI mode:

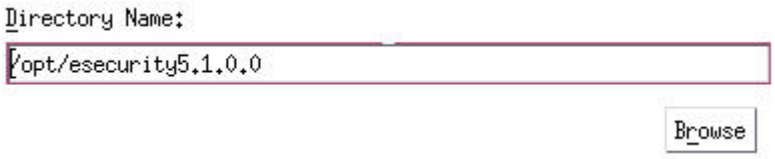
   ```
   ./setup.sh
   ```

   or

   For textual ("headless") mode:

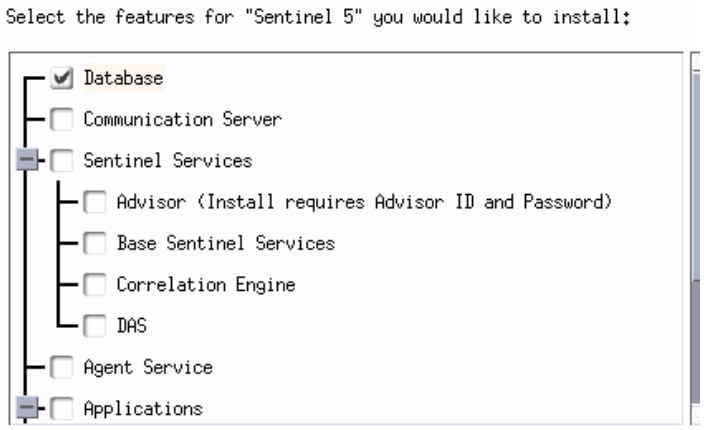
```
./setup.sh –console
```

7. After reading the Welcome screen, Click Next.
8. Accept End User License Agreement, Click Next.
9. Accept the default install directory or click Browse to specify your installation location. Click Next.

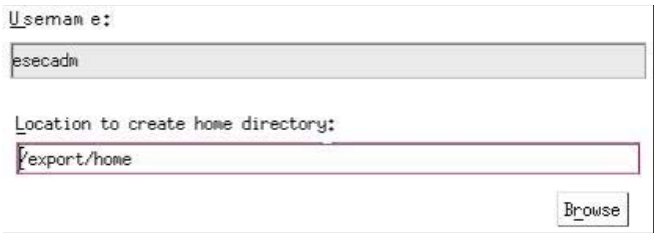


10. Select Custom (default). Click Next.
11. For which features to install, de-select all features and select Database only. Click Next.

NOTE: Make sure you de-select the parent “Sentinel Services” feature. It will appear grayed-out with a white check mark in it if it is still selected but all of its child features were de-selected.



12. Specify the operating system e-Security Administrator username and the location of its home directory. This is the username that will own the installed e-Security product. If the user does not already exist, one will be created along with a home directory in the specified directory.
    - OS Administrator username – Default is esecadm
    - OS Administrator user home directory – Default is “/export/home”. If esecadm is the username, then the user’s home directory will be /export/home/esecadm.

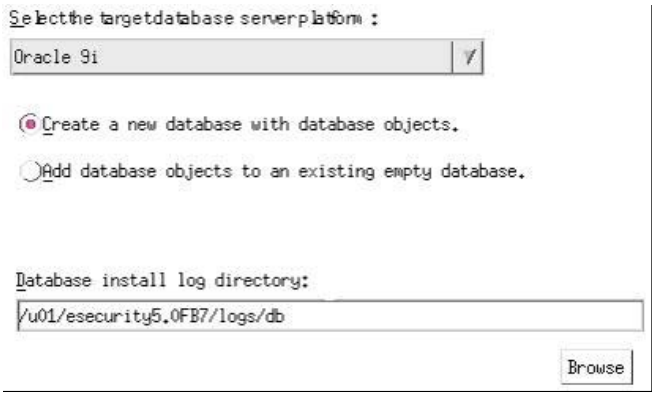


NOTE: If a new user is created, its password will need to be set manually, separately from this installer. e-Security recommends this be done directly by logging into the system following the installation of the product.

NOTE: In order to meet stringent security configurations required by Common Criteria Certification, e-Security requires a strong password with the following characteristics:

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

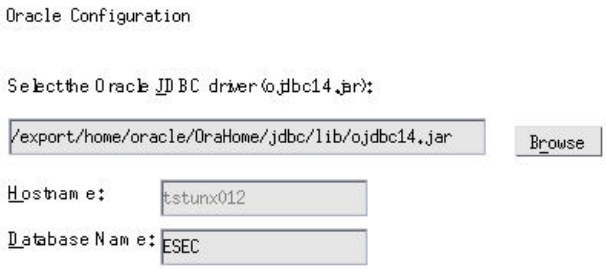
13. Enter hostname (or IP) and port number (default: 10012) for the Communication Server. Click Next.
14. Select target database server platform as Oracle and select one of the following:
    - Create a new database with database objects – creates a new Oracle database instance as well as populates the new instance with database objects.
    - Add database objects to an existing empty database – only adds database to an existing Oracle database instance. The existing database instance must be empty, except for the presence of the esecdba user
15. Enter the database install log directory (default: $ESEC_HOME/logs/db). Accept the default 'Database install log directory' or click Browse to specify a different location.



16. Click Ok on the default oracle username.

17. If you chose to create a new database, enter the following:
    - The path for Oracle JDBC driver file (typical name of the jar file is ojdbc14.jar). This is the fully qualified path to the jar file, typically $ORACLE_HOME/jdbc/lib/ojdbc14.jar (cannot use environment variables in this field).
    - Hostname – The hostname of the machine to install the database. This field is not configurable if creating new database instance.
    - Database Name – The name of the database instance to install.

NOTE: You will need to name your database to a different name than the name specified in your 4.2 installation.

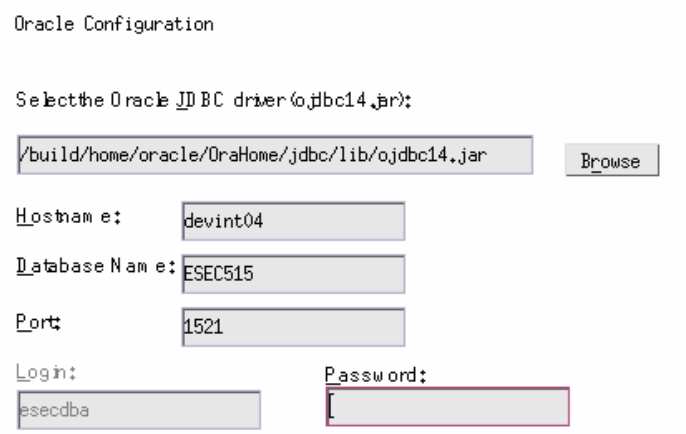


18. If you chose to add database objects to an existing empty Oracle database, you will be prompted for the following information.
    - The path for Oracle JDBC driver file (typical name of the jar file is ojdbc14.jar). This is the fully qualified path to the jar file, typically $ORACLE_HOME/jdbc/lib/ojdbc14.jar (cannot use environment variables in this field).
    - Database hostname or IP address – The name or IP address of the host where the Oracle database is you wish to add database objects to. This can be the local hostname or a remote hostname.
    - Database name – The name of the existing empty Oracle database instance you wish to add database objects to (default is ESEC. You will need to name your database to a different name than the name specified in your 4.2 installation). This database name must appear 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.

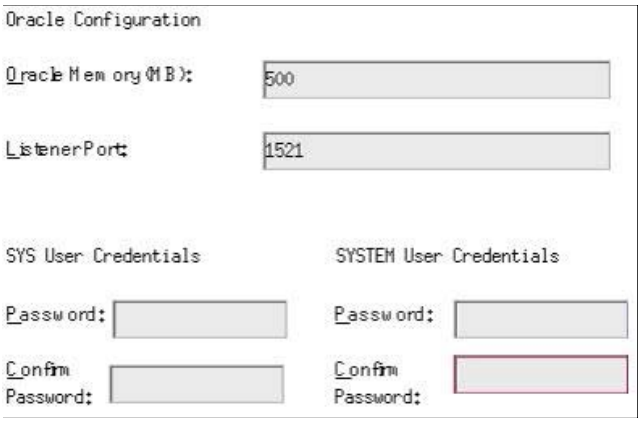
NOTE: If the database name is not in the tnsnames.ora, the installer will not give you an error at this point in the installation (because it verifies the connection using a direct JDBC connection), but the Database installation will fail when the Database installer tries to connect to the database via sqlplus. If the Database installation fails at that point, you can go backward to this prompt and fix the database name.

    - Database port (default is 1521)
    - For e-Security Database Administrator User (DBA), specify the password for the “esecdba” user. The esecdba password must match

the esecdba password of your v4.2 installation. The username field in this prompt is not editable.

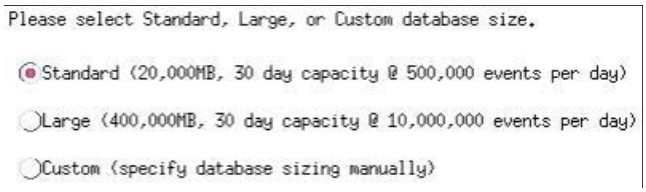


19. If you chose to create a new database, you will see the following prompt:
    - Oracle Memory (MB) – The amount of RAM to be allocated to this Oracle database instance.
    - Listener Port – the port on which to create an Oracle listener (default is 1521).
    - SYS user password and password confirmation – SYS is a default Oracle user. This user's password will be set to the value specified here.
    - SYSTEM user password and password confirmation - SYSTEM is a default Oracle user. This user's password will be set to the value specified here.



20. If you chose to create a new database, you be prompted to enter your database size. You have the following options:
    - Standard (20 GB)
    - Large (400 GB)
    - Custom (specify your size manually). If you choose this option you will be prompted for:
        - initial size of each database file in MB (100 – 10,000)
        - maximum size of each database file in MB (2,000 – 100,000)
        - size of all database files MB (7,000 – 2,000,000)

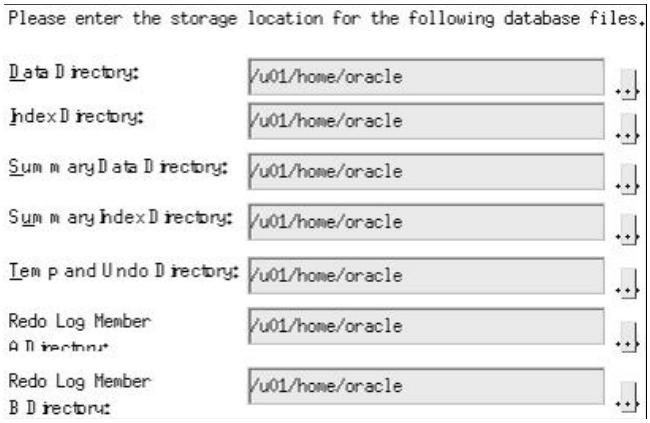
- size of each log file in MB (100 – 100,000)



21. If you chose to create a new database, you will be prompted to enter the storage location for the following database files:

NOTE: For recovery and performance purposes, we recommend that these locations be on different I/O devices.

- Data directory
- Index directory
- Summary Data directory
- Summary Index directory
- Temporary and Undo Tablespace directory
- Redo Log Member A directory
- Redo Log Member B directory



22. If you chose to create a new database, enter authentication information for the e-Security Database Administrator (DBA). This is esecdba, the owner of the database objects.
23. Enter authentication information for the e-Security Application Database user. This is esecapp, the e-Security application username that Sentinel processes use to connect to the database.
24. Enter authentication information for the e-Security Administrator Database user. This is esecadm, the Sentinel Administrator user.
25. Click Next on the database installation summary window.
26. Upon completion of installation, you will be prompted to reboot. Click Finish to reboot your system.

Migration for Solaris

Migration will only migrate the following:

- Users and assigned privileges created in v4.2 will migrate to Sentinel 5. New Sentinel users must be created after Sentinel 5 installation.

- Filters
- Right-click menu configuration options.
- Any renamed CV tags
- Partition and archive configurations
- Cases from v4.2 migrate over as incidents
- Incidents and incident-related events get migrated.

> **NOTE**: Migration of data will NOT migrate event data. Only data associated with incidents.

For Sentinel 4.2 databases not using esecdba as the e-Security Database Schema Owner

> **NOTE**: This procedure will add esecdba id to v4.2 database to allow data migration from v4.2 to v5.

1. For Solaris, login as the Oracle software owner.
2. Using SQL*Plus, connect to the v4.2 database as SYSDBA.
3. cd to:

   ```
   $ESEC_HOME/utilities/db/scripts/ddl/oracle/Migration
   ```

4. At the SQL prompt (SQL>), enter:

   ```
   @import_add_esecdba.sql
   ```

5. Exit SQL*Plus.

> **NOTE**: After performing data migration, you can use Oracle Enterprise Manager to delete the esecdba user from the Sentinel 4.2 database.

Data Migration

1. Ensure that java is in your path.
2. For Solaris, login as the root user.
3. Mount the Sentinel 5 software installation CD on the database server where Sentinel 5 database resides.
4. cd to:

   ```
   sentinel/dbsetup/bin
   ```

5. Enter:

   ```
   ./MigrateDb.sh
   ```

6. You will prompted for the following:
   - database host name
   - destination database name (the v5.1 database you are migrating to)
   - esecdba password (source and destination database)
   - source database name (v4.2 database name)
   - log directory
   - migration option:
     - (1) System settings
     - (2) Incidents/cases
     - (3) both

- (4) done

NOTE: System settings should be first migrated successfully before proceeding to migrate incidents and cases.

NOTE: If system migration fails, on your v5.1 database, uninstall and then reinstall the database object. Run Sentinel 5 uninstall, select database and delete database objects only.

NOTE: If incident migration fails, rerun incident migration. The migration utility will restart from the point of failure. No additional clean up tasks are required.

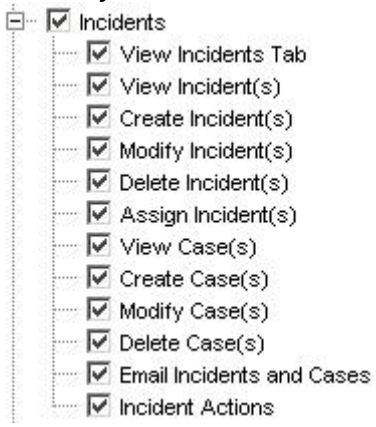
NOTE: After performing data migration, you can use Oracle Enterprise Manager to delete the esecdba user from the Sentinel 4.2 database.

Post-Migration – Installing Sentinel 5

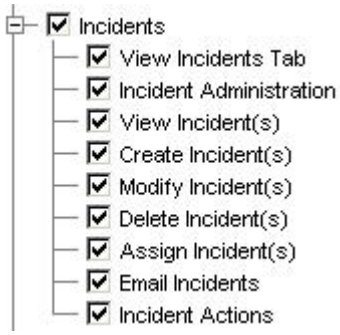
In v5.1, the following is new, different or removed.

- iTRAC – This is a new functionality.

- Incidents – added Incident Administration. Removed all case related functionality.

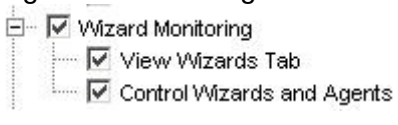


Sentinel v4.2 Incidents



Sentinel v5.1 Incidents

- Agent Management – in v4.2 this is Wizard Monitoring. 'View Wizards Tab' has changed to 'View Agents'. 'Control Wizards and Agent' has been changed to 'Control Agents' and 'Agent Administration'.



Sentinel v4.2 Wizard Monitoring

Sentinel v5.1 Agent Management

- Administration – added DAS Statistics, User Session Management and iTRAC Role Management. 'Correlation Rules' has been renamed to 'Correlation'. The Event Configuration feature has been moved to the Sentinel Data Manager. 'User Configuration' has been renamed to 'User Management'.

Sentinel v4.2 Administration

Sentinel v5.1 Administration

- ActiveViews™ - in v4.2 this is Real Time. 'Summary Displays' has been renamed to Active Views.

Sentinel v4.2 Real Time

Sentinel v5.1 Active Views™

- System Overview functionality is not available in Sentinel 5.

Installing Sentinel 5

1. Install Sentinel 5, see 'Installing Sentinel for Oracle' installation chapter. After install, refer to the following steps if you wish to add any new functionality to any of the existing users from v4.2.
2. Log into Sentinel Control Center as a user with Administration/User Management permission.
3. In Sentinel Control Center, click Admin tab. Expand User Configuration in the Navigation pane or from the navigation bar click Admin > User Configuration.
4. Right click on an Admin user or applicable (i.e. esecadm or other admin user) > User Details. Click the Permissions tab.
5. Expand iTRAC and assign permissions as needed.
6. Expand Incidents and assign 'Incident Administration' if needed.
7. Expand Agent Management and assign 'Agent Administration' if needed.
8. Expand Administration and assign 'DAS Statistics', 'User Session Management' or 'iTRAC Role Management' if needed.

9. Click the Roles tab and assign either Admin or Analyst Workflow Role. Click Ok.
10. If applicable, import any correlation rules. Rule Sets will be Rule Folders.
11. Copy from backup Agent scripts and port configurations by following the instructions in the section Post-Migration – Reconfiguring Agent Scripts and Port Configurations

Post-Migration – Reconfiguring Agent Scripts and Port Configurations

On each machine where the Sentinel 5 Agent Service (Agent Manager) is installed, perform the following steps to re-establish the Agent scripts and port configurations that were being used in the Sentinel v4.2 installation.

To re-establish the Agent scripts and port configurations

1. Stop Agent Manager by executing the following command as the esecadm user:

   ```
   $ESEC_HOME/wizard/agent-manager.sh stop
   ```

2. From the location you placed a backup of the $WORKBENCH_HOME/Agents directory of the Sentinel v4.2 installation, copy the following files to the directory $WORKBENCH_HOME/Agents of the current Sentinel 5 installation (overwrite files, if necessary):
   - localhost_portcfg.dat
   - localhost_snmpcfg.dat
3. Read the text file you created during Pre-Migration that lists all of the Agents being used by the Sentinel v4.2 Agent Manager installation on this machine. You will need to know the Agent names for the next step.
4. From the location you placed a backup of the $WORKBENCH_HOME/Elements directory of the Sentinel v4.2 installation, copy the directories whose names match Agent names in the text file into the directory $WORKBENCH_HOME/Elements of the current Sentinel 5 installation (overwrite directories/files, if necessary).
5. Mount the Sentinel v5.1 installation CD-ROM if it is not already mounted.
6. From within the 'utilities' directory in the CD-ROM, execute the command:

   ```
   ./UpgradePortCfgFile.sh
   ```

7. Execute the following command as the root user to ensure the ownership of the files just copied are properly set:

   ```
   chown –R esecadm:esec $ESEC_HOME/wizard
   ```

8. Start Agent Manager by executing the following command as the esecadm user:

   ```
   $ESEC_HOME/wizard/agent-manager.sh start
   ```

Post-Migration – Configuring Sentinel 5 for Crystal Reporting

If you were running Crystal Reporting for v4.2 and want run Crystal Reporting in Sentinel, you will have to:

- Upgrade to Crystal BusinessObjects Enterprise™ 11 (if you are running v5.1.1.)

- Change your settings in your Oracle 9i client
- Import the Sentinel 5 Crystal Report templates including the Data Migration templates

See the 'Crystal Reports' installation chapter for more information.

Patch from v5 to v5.1

The v5.1 installer supports upgrade from v5.0 or v5.0.1 to v5.1. After upgrading to v5.1, User Management Permissions and Menu Configuration options created in v5 must be updated.

Perform this procedure on any machine that has any Sentinel components installed.

> **NOTE**: You cannot go directly from v5 to v5.1.1. Patching paths are v5 or v5.0.1 to v5.1 and v5.1 to v5.1.1. If you are patching from v5 or v5.0.1 to v5.1.1, you must first upgrade to v5.1 before patching to v5.1.1.

If you are running the patch installer from the machine where you originally installed the Database component, you will need to know the password of the e-Security Database Administrator (esecdba) user.

> **NOTE**: Procedure for upgrade from v5 to v5.1 is identical to the procedure for upgrading from v5.1 to v5.1.1. Go to section Patch from v5.1 to v5.1.1.

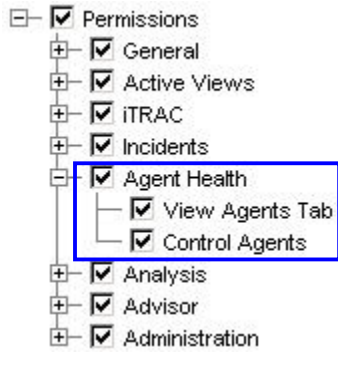
Updating User Management Permissions

When upgrading from v5 to v5.1, Agent Health is changed to Agent Management with an additional Agent Administration functionality added.

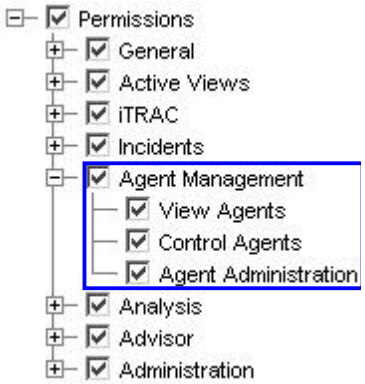
Updating User Management Permissions

1. Log into Sentinel Control Center as a user with Administration/User Management permission.

   In v5.1, Agent Health under Permissions has been changed from 'Agent Health' to 'Agent Management' with an additional permission added.



Sentinel v5.0 User Permission



Sentinel v5.1 User Permission

2. In Sentinel Control Center, click the Admin tab. Expand User Configuration in the Navigation pane or from the navigation bar click Admin > User Configuration.

3. Right click on an Admin user (i.e. esecadm or other admin user) > User Details. Click the Permissions tab.
4. Expand Agent Management and assign 'Agent Administration'. Click Ok.

Updating Menu Configuration Options

If additional entries in the Menu Configuration were created prior to upgrading to v5.1, the paths to the commands will need to be updated. As of 5.1.0.0, on Solaris, the command to be executed in the Menu Configuration must exist under the $ESEC_HOME/sentinel/exec directory. Additionally, all paths to the commands executed in the Menu Configuration are always relative to the $ESEC_HOME/sentinel/exec directory. If you need to execute a command elsewhere on the filesystem, create a symbolic link from a location under $ESEC_HOME/sentinel/exec to the command that is be executed.

The Menu Configuration for traceroute must be manually changed from 'tracert' to 'traceroute' in order to function properly.

To add an option to the Menu Configuration menu

1. Log into Sentinel Control Center as a user with Administration/User Management permission.
2. Click the Admin tab.
3. In the Admin Navigator, click Admin > Menu Configuration.
4. In the Menu Configuration window, click Modify and highlight a menu item that is to be updated. Click Details
5. In the Menu Configuration dialog box, make the necessary in:
   - Command line/URL
   - Parameters – must be enclosed by the percent sign (e.g., %EventName%)

   NOTE: For a list of available tags you can use when specifying parameters, click Help on the Menu Configuration dialog box or go to the Meta-tag chapter in the e-Security User's Reference Guide.
6. Click OK.
7. Click Save.

Patch from v5.1 to v5.1.1

Perform this procedure on any machine that has any Sentinel components installed.

NOTE: You cannot go directly from v5 to v5.1.1. Upgrade paths are v5 or v5.0.1 to v5.1 and v5.1 to v5.1.1. If you are patching from v5 or v5.0.1 to v5.1.1, you must first upgrade to v5.1 before patching to v5.1.1.

If you are running the patch installer from the machine where you originally installed the Database component, you will need to know the password of the e-Security Database Administrator (esecdba) user.

Upgrading from v5 to v5.1 for Solaris

1. Login as the root user.

2. Insert and mount the Sentinel Install CD.
3. Start the install program by going to the patch install directory on the CD-ROM and enter:

   For GUI mode:

   ```
   ./setup.sh
   ```

   or

   For textual (“headless”) mode:

   ```
   ./setup.sh –console
   ```

4. Click Next on the Welcome screen.
5. Accept the End User License Agreement and click Next.
6. Click Next until the database information window.
7. Ensure the database type is correct. Select the location of the database install log directory. Click Next.
8. Ensure the information for the Oracle server is correct. Enter esecdba password. Follow the remaining installer prompts.

Crystal Reporting Server

After patching to v5.1.1, you must upgrade your Crystal Server from Crystal Enterprise 9 Standard® to Crystal BusinessObjects Enterprise™ 11. See the Crystal Reports and Advisor Configuration Chapters. In addition, Sentinel 5 does not support Crystal XI on Windows® 2000 Server.

NOTE: Sentinel 5 does not support Crystal XI on Windows® 2000 Server.

Updating Sentinel email for SMTP Authentication

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

To Configure execution.properties file

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

   ```
   $ESEC_HOME/sentinel/config
   ```

2. Execute mailconfig as follows:

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

   Example:

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

   After entering this command you will be prompted for a new password.

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

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

NOTE: When using the password option, it must be the last argument.

To test your execution.properties configuration

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

   ```
   $ESEC_HOME/sentinel/config
   ```

2. Execute mailconfigtest as follows:

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

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

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

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

   ```
   Subject: Testing e-Security mail property

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

Chapter 7 – Data Migration and Patch for MS SQL

This chapter discusses data migration and upgrade for:

- Data Migration and Upgrade from v4.2.1 to v5.1

  NOTE: For upgrading, you cannot go directly from v4.2.1 to v5.1.1. You must data migrate to v5.1 and then upgrade to v5.1.1.

- Patch from v5.0.0 or v5.0.1 to v5.1
- Patch from v5.1 to v5.1.1

  NOTE: For upgrading, you cannot go directly from v5 to v5.1.1. Patching paths are v5 or v5.0.1 to v5.1 and v5.1 to v5.1.1. If you are patching from v5 or v5.0.1 to v5.1.1, you must first upgrade to v5.1 before patching to v5.1.1.

Data Migration and Upgrade from v4.2 to v5.1

Sentinel Server Components

Sentinel 5 requires that the previous version of the software be uninstalled before adding the sentinel 5 server components. Do not uninstall the previous version (v4.2) Database which is required for data migration. Backup the Sentinel server machine (%ESEC_HOME% install directory and Root Drive). This will allow you to restore v4.2 in case there are any unexpected failures.

The details of the migration and installation pre and post steps can be found below.

Agent Manager

Backup the v4.2 Agent Manager machine. v4.2 Agent Managers must be completely uninstalled before installing the v5 Agent Manager software.

For each machine running v4.2 Agent Manager with at least one port configured, save a copy of the contents of the following directories in an easy to access location. The contents of these directories will be used during post-migration to quickly reconfigure the Agents ports setup in your v4.2 install:

- %WORKBENCH_HOME%\Agents - Contains the port configuration files.
- %WORKBENCH_HOME%\Elements – Contains the Agent scripts.

If you do not make a copy of the contents of the above directories, you will need to reconfigure all Agent scripts and ports from scratch.

NOTE: v4.2 Agent Manager and Agent Builder is not compatible with v5 components.

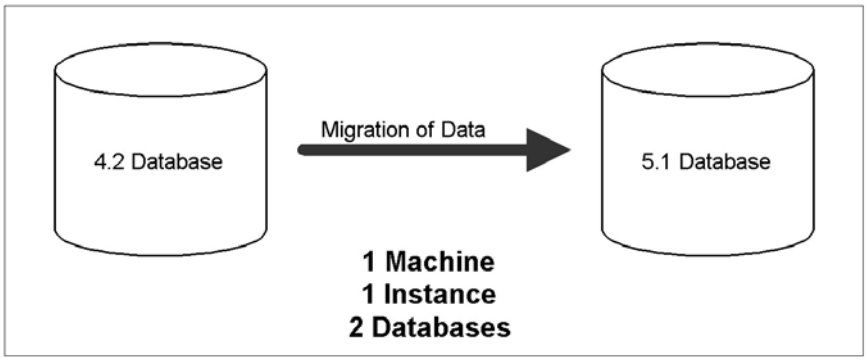
Crystal Reporting Server

If you are only upgrading to v5.1, you must use the new reports provided with the v5 CD. The new reports are written to work with the new DB schema. If you are upgrading to v5.1.1, you must upgrade your Crystal Server from Crystal Enterprise 9 Standard® to Crystal BusinessObjects Enterprise™ 11. In addition, Sentinel 5 does not support Crystal XI on Windows® 2000 Server.

NOTE: Sentinel 5 does not support Crystal XI on Windows® 2000 Server.

Database Server

Sentinel 5 data migration is provided to migrate data from Sentinel v4.2 to Sentinel 5. The data migration utility supports migration on 1 machine, 1 instance with 2 databases.



The following is migrated:

- Users and assigned privileges created in v4.2 will migrate to Sentinel 5.
- Filters
- Right-click menu configuration options.
- Any renamed CV tags
- Partition and archive configurations
- Cases from v4.2 migrate over as incidents
- Incidents and incident-related events get migrated.

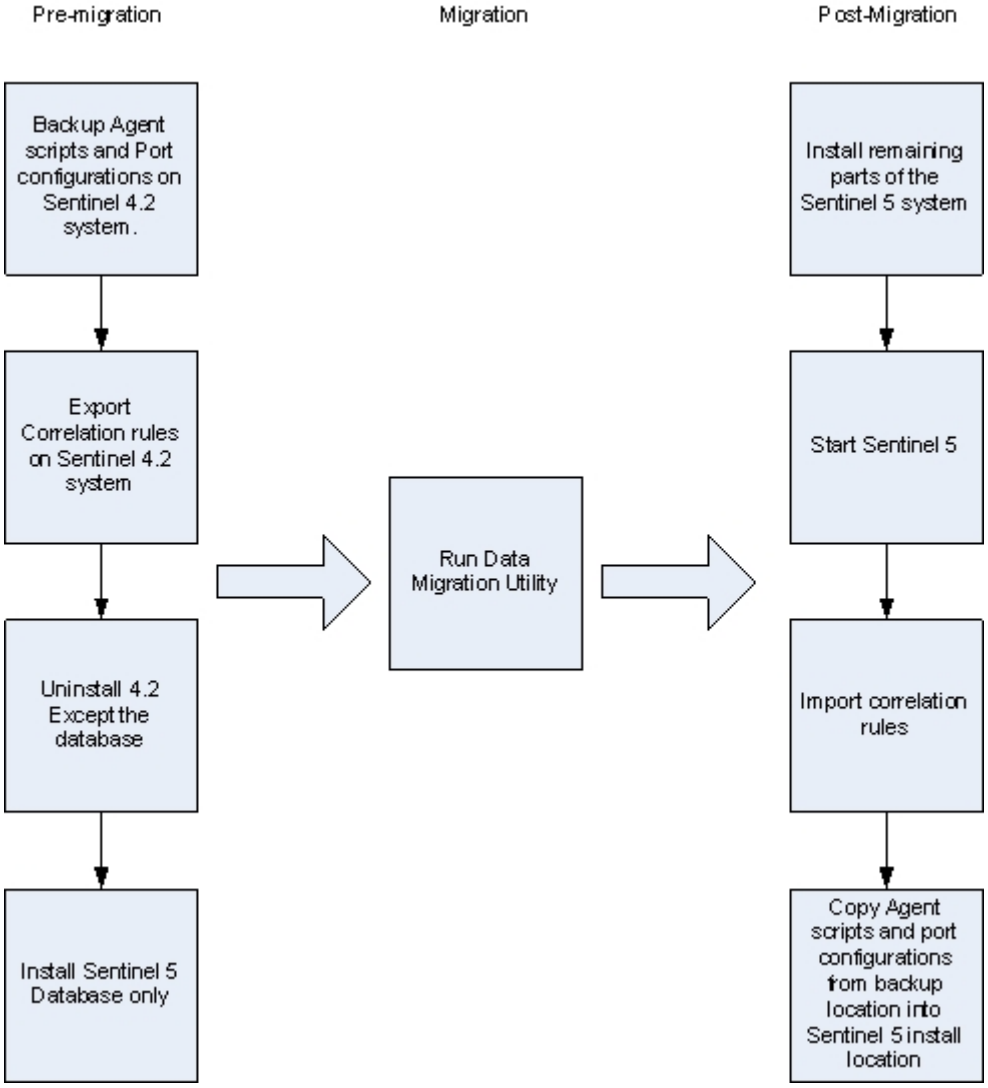
NOTE: Data Migration will NOT migrate event data. Only event data associated with incidents will migrate.

NOTE: Incident event data is not viewable through the Sentinel Console. Incident event data can be seen through SQL or Crystal Reporting.

Data migration and Sentinel 5 upgrade comprises of:

- Pre-migration
  - Backup Sentinel server Database Instance: This will allow you to restore v4.2 database in case there are any unexpected failures.
  - Copy or save and right click system commands or scripts that may be under the %ESEC_HOME% directory
  - Copy Agents scripts and port configurations to backup location.
  - Export Sentinel v4.2 correlation rules (if any)
  - Except for the database, uninstall Sentinel v4.2
  - Install Sentinel 5 database only
- Migration
  - Run the data migration utility
- Post migration
  - Install remaining component of Sentinel 5
  - Start Sentinel 5
  - Import correlation rules (if any)
  - Copy Agent scripts and port configurations from backup location into Sentinel 5 install location.

- If you are running Crystal Server with Sentinel, import Sentinel 5 Crystal Report Templates



Pre-migration – Exporting of Correlation Rules

Importing or Exporting a Correlation Rule Set

1. In the v4.2 Sentinel Console, under the Admin tab open the Correlation Rules window.
2. Select a Rule Set.
3. Click Export. A file browser will open, browse to the target device to write the rule to and click OK. The rule set will be exported as an xml file.

Pre-migration – Backup of Agent scripts and port configuration

Backing up Agent scripts and port configuration

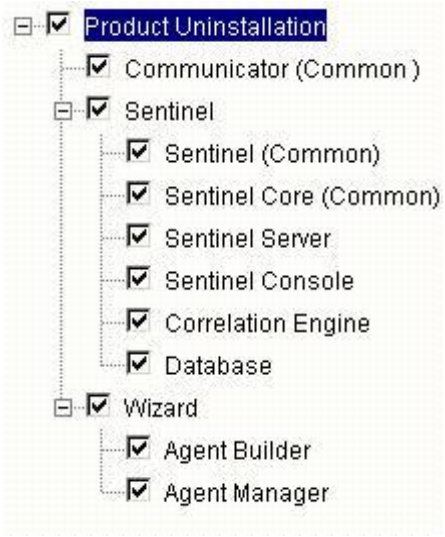
1. On all Sentinel v4.2 machines running Agent Manager, create a directory to store all Agents scripts and port configurations for that machine.

2. In the directory you just created, created a text file that lists the name of all the Agents that are being used by a port configuration on this Agent Manager. Use an Agent Builder to determine the Agents being used by this Agent Manager. If this Agent Manager is on Solaris, you will need to use an Agent Builder on a Windows machine (Agent Builder is not supported on Solaris).
3. Copy the following directories into the directory you just created:
   - %WORKBENCH_HOME%\Agents
   - %WORKBENCH_HOME%\Elements

Pre-Migration – Uninstalling v4.2 (Windows)

Uninstalling v4.2

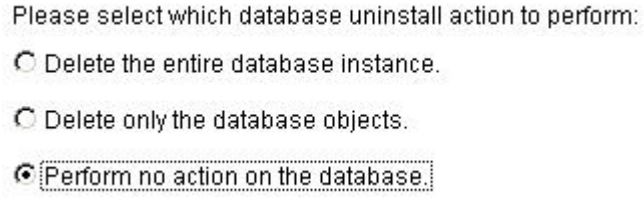
1. On your Sentinel v4.2 machine:
   - Close all Sentinel Consoles and Agent Builders
   - Click Start > Programs > e-Security > Uninstall e-Security 4.2.1.x
2. Click through the screen prompts until the uninstall feature window appears. Select all of the features.



NOTE: In the above example, 3rd party integration software is not shown. If you have any 3rd party software, select to uninstall.

Click through the screen prompts to the Database Uninstall window.

3. In the Database Uninstall window, select 'Perform no action on the database'.



4. Click through the remaining uninstall windows.

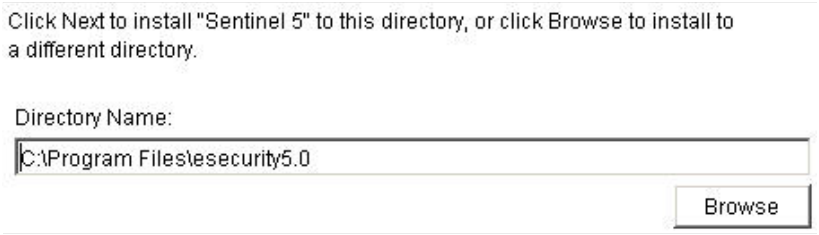
Pre-Migration – Installing Sentinel 5 Database

Sentinel 5 Database Installation

1. Verify that your environmental variable do not reference 4.2. If so, delete them. The following environmental variables should not be present:
   - ESEC_HOME
   - ESEC_VERSION
   - ESEC_JAVA_HOME
   - ESEC_CONF_FILE
   - WORKBENCH_HOME
2. Verify you have the collected the information, performed the tasks, and satisfied the requirements specified in the section Sentinel Database in Chapter 5: Installing Sentinel 5 for MS SQL > Pre-Installation of Sentinel 5 for MS SQL.
3. Insert the Sentinel installation CD into the CD-ROM drive.
4. Browse to the CD and double-click on setup.bat.

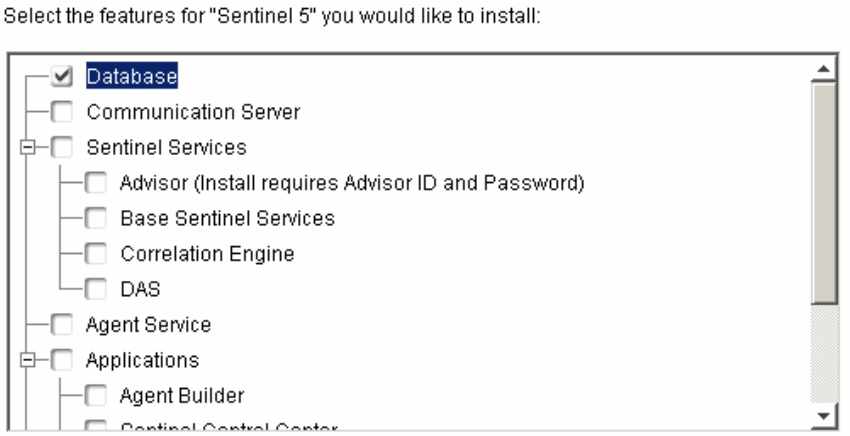
NOTE: Installing in console mode is not supported on Windows.

5. After reading the Welcome screen, Click Next
6. Accept the End User License Agreement, click Next
7. Accept the default install directory or click Browse to specify a different location. Click Next.

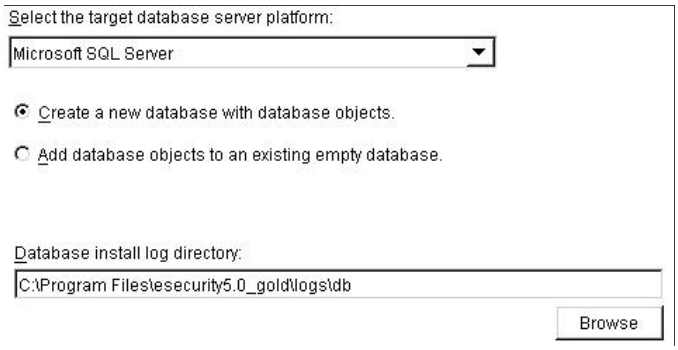


8. For type of installation, select Custom (default). Click Next.
9. For which features to install, de-select all features and select Database only. Click Next.

NOTE: Make sure you de-select the parent “Sentinel Services” feature. It will appear grayed-out with a white check mark in it if it is still selected but all of its child features were de-selected.



10. Enter hostname (or IP) and port number (default: 10012) for the Communication Server. Click Next.
11. Select Microsoft SQL Server as the target database platform and select 'Create a new database with database objects'. Also, enter the database install log directory (default: %ESEC_HOME%\logs\db). Accept the default 'Database install log directory' or click Browse to specify a different location. Click Next.

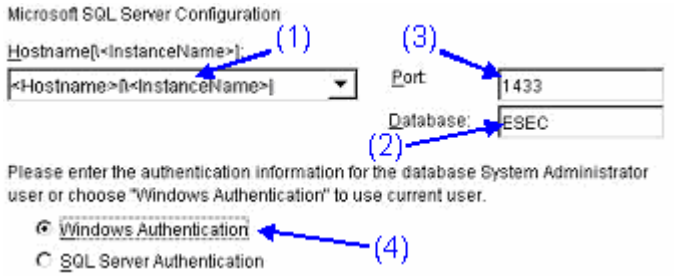


12. Enter your SQL Server configuration information:
    - (1) Database hostname or IP address – by default, your local host machine will appear, if SQL Server is installed locally. If the SQL Server you wish to install does not appear in the drop-down list, select 'Other' in the list. A text box will appear allowing you to type in the hostname. The hostname you type must be fully qualified (e.g. - 'sqlserver.esecurity.net' instead of just 'sqlserver'). If you specified an instance name during SQL Server installation, you will need to add '\<instance_name>' to end of the hostname, where <instance_name> is the name you gave to the instance during SQL Server installation.
    - (2) The name to give the new SQL Server database. In addition to the database you name here, another database with the name <your_db_name>_WF will also be created to be used by iTRAC.

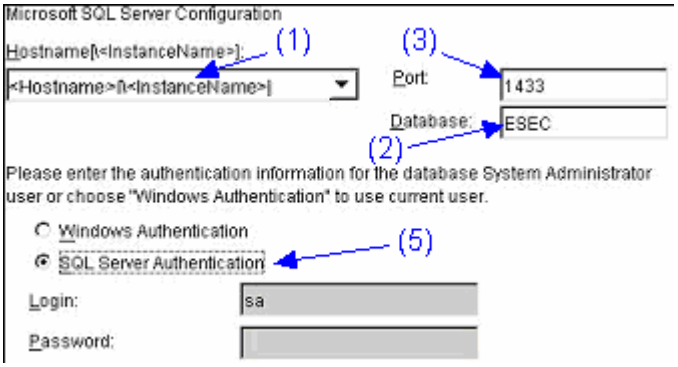
NOTE: You will need to name you database to a different name than the name specified in your 4.2 installation.

    - (3) Database port (default is 1433)
    - For system database administrator, select either:

- (4) Windows Authentication (will use the username your are running the installer as)
- (5) SQL Server Authentication and enter the sa user password



Windows Authentication

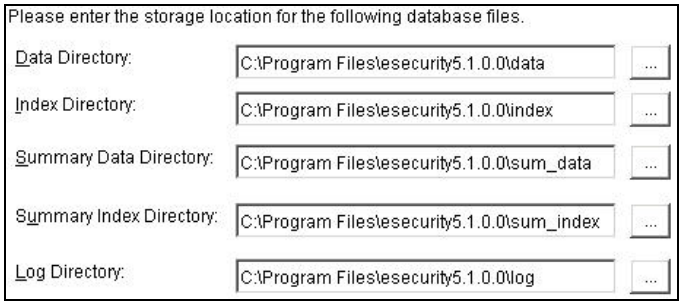


SQL Server Authentication

13. Enter the location for the following database files:

> **NOTE:** For recovery and performance purposes, we recommend that these locations be on different I/O devices.

- Data files
- Index files
- Summary Data files
- Summary Index files
- Log files

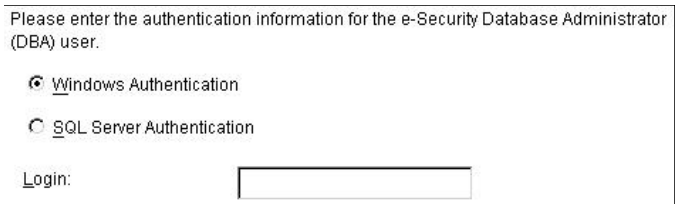


14. Enter your database size:
    - Standard (20,000MB) – 30 day capacity at 500,000 events per day
    - Large (400,000MB) – 30 day capacity at 10,000,000 events per day
    - Custom (specify your size manually). If you choose this option you will be prompted for:
      (1) size of your database in MB (10,000 – 2,000,000)

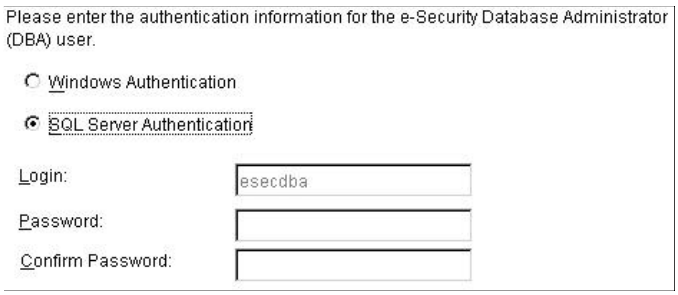
(2) size of each log file in MB (100 – 100,000)
(3) max size of each database file in MB (2,000 – 100,000)

15. For e-Security Database Administrator (DBA), select either:
    - SQL Server Authentication (esecdba), password and password confirmation
    - Windows Authentication, enter <domain name>\<username>

NOTE: If you select "SQL Server Authentication", you will not be able to modify the default login name.



Windows Authentication

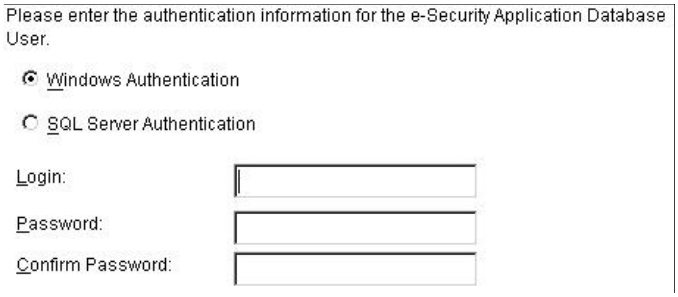


SQL Server Authentication

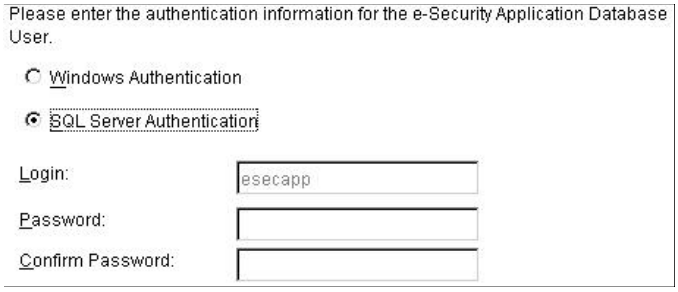
NOTE: For SQL authentication, installer will not proceed unless the esecdba password matches the v4.2 esecdba password.

16. For e-Security Application Database user. Select either:
    - SQL Server Authentication (esecapp), enter password and password confirmation
    - Windows Authentication, enter <domain name>\<username>, password and password confirmation

NOTE: If you select "SQL Server Authentication", you will not be able to modify the default login name.



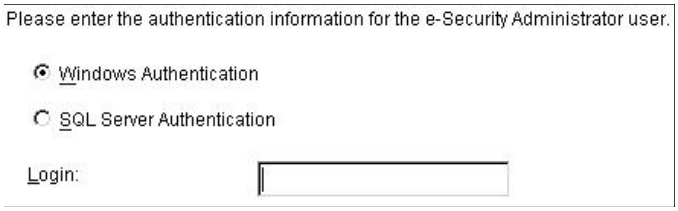
Windows Authentication



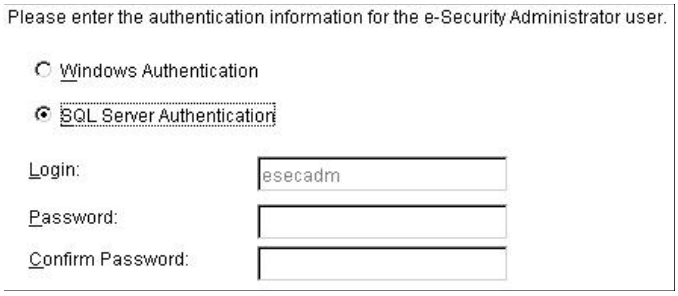
SQL Server Authentication

17. For e-Security Administrator user. Select either:
    - SQL Authentication, enter username for the Sentinel Administrator (default: esecadm), password and password confirmation
    - Windows authentication, enter <domain name>\<username>

NOTE: If you select "SQL Server Authentication", you will not be able to modify the default login name.



Windows Authentication



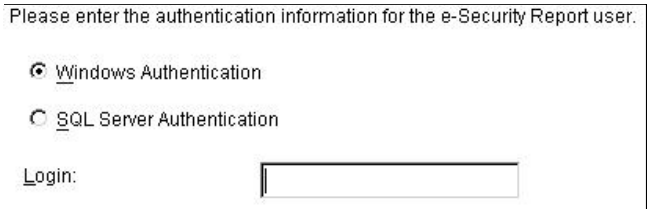
SQL Server Authentication

18. For the e-Security Reporting user. Select either:

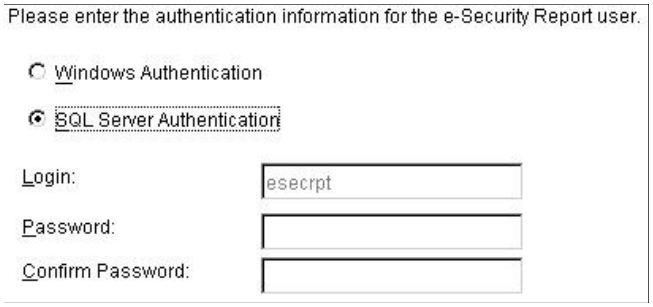
NOTE: For e-Security Reporting, Windows Authentication requires you to be running Crystal Enterprise Professional. Professional allows you to create different accounts and maps as needed. If you are using Standard, select SQL Authentication.

- SQL Authentication (esecrpt), enter password and password confirmation
- Windows Authentication, enter <domain name>\<username>

NOTE: If you select "SQL Server Authentication", you will not be able to modify the default login name.



Windows Authentication



SQL Server Authentication

19. Click Next on the database installation summary window.
20. Upon completion of installation, you will be prompted to reboot. Click Finish to reboot your system.

Data Migration for Windows

Migration will only migrate the following:

- Users and assigned privileges created in v4.2 will migrate to Sentinel 5. New Sentinel users must be created after Sentinel 5 installation.
- Filters
- Right-click menu configuration options.
- Any renamed CV tags
- Partition and archive configurations
- Cases from v4.2 migrate over as incidents
- Incidents and incident-related events get migrated.

> **NOTE**: Migration of data will NOT migrate event data. Only data associated with incidents.

For Sentinel 5 Windows e-Security Database Administrator Authentication Users.

> **NOTE**: This procedure is for Sentinel 5 window authentication installations for the e-Security Database Administrator (equivalent to esecdba). This procedure adds the esecdba user to the Sentinel 5 database so that data from v4.2 can be migrated to v5.

1. Login as a user with administrative rights.
2. Start MS SQL Server Query Analyzer. Login as the sa or Windows Authentication user.
3. Click File > Open. Navigate to:

   ```
   %ESEC_HOME%\utilities\db\scripts\ddl\mssql
   ```

4. Select import_add_esecdba.sql.

5. Click Open.
6. Click Query > Execute.
7. After the script has finished, exit Query Analyzer.

> **NOTE**: After performing data migration, you can use MS SQL Server Enterprise Manager to delete the esecdba user from the Sentinel 5 database.

Data Migration

1. Check your environmental variables to ensure that JAVA is in your path.
2. Login as a user with administrative rights.
3. On the install CD-ROM, at the command prompt, cd to:

   ```
   D:\sentinel\dbsetup\bin
   ```

4. Run MigrateDb.bat.
5. You will prompted for the following:
   - database host name
   - destination database name (the v5.1 database you are migrating to)
   - esecdba password (source and destination database)
   - source database name (v4.2 database name)
   - log directory
   - migration option:
     - (1) System settings
     - (2) Incidents/cases
     - (3) both
     - (4) done

> **NOTE**: System settings should be first migrated successfully before proceeding to migrate incidents and cases.

> **NOTE**: If system migration fails, on your v5.1 database uninstall and then reinstall the database object. Run Sentinel 5 uninstall, select database and delete database objects only.

> **NOTE**: If incident migration fails, rerun incident migration. The migration utility will restart from the point of failure. No additional clean up tasks are required.

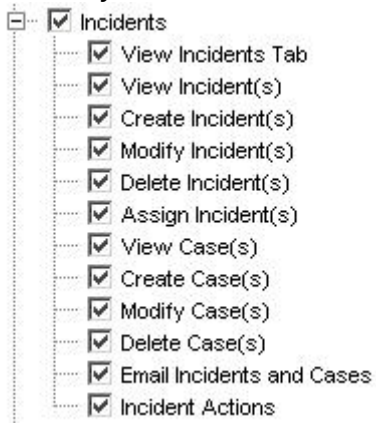
> **NOTE**: After performing data migration, you can use MS SQL Server Enterprise Manager to delete the esecdba user from the Sentinel 5 database.

Post-Migration – Installing Sentinel 5

In v5.1, the following is new, different or removed.

- iTRAC – This is a new functionality.

- Incidents – added Incident Administration. Removed all Case related functionality.



Sentinel v4.2 Incidents

Sentinel v5.1 Incidents

- Agent Management – in v4.2 this is Wizard Monitoring. 'View Wizards Tab' has changed to 'View Agents'. 'Control Wizards and Agent' has been changed to 'Control Agents' and 'Agent Administration'.

Sentinel v4.2 Wizard Monitoring

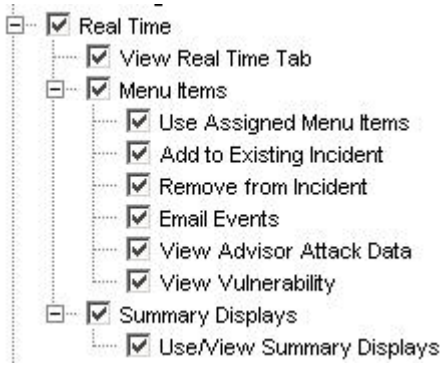
Sentinel v5.1 Agent Management

- Administration – added DAS Statistics, User Session Management and iTRAC Role Management. 'Correlation Rules' has been renamed to 'Correlation'. The Event Configuration feature has been moved to the Sentinel Data Manager. 'User Configuration' has been renamed to 'User Management'.

Sentinel v4.2 Administration

Sentinel v5.1 Administration

- ActiveViews™ - in v4.2 this is Real Time. 'Summary Displays' has been renamed to Active Views.



Sentinel v4.2 Real Time

Sentinel v5.1 Active Views™

- System Overview functionality is not available in Sentinel 5.

Installing Sentinel 5

1. Install Sentinel 5, see 'Installing Sentinel for Windows' installation chapter. After install, refer to the following steps if you wish to add any new functionality to any of the existing users from v4.2.
2. Log into Sentinel Control Center as a user with Administration/User Management permission.
3. In Sentinel Control Center, click Admin tab. Expand User Configuration in the Navigation pane or from the navigation bar click Admin > User Configuration.
4. Right click on an Admin user or applicable (i.e. esecadm or other admin user) > User Details. Click the Permissions tab.
5. Expand iTRAC and assign permissions as needed.
6. Expand Incidents and assign 'Incident Administration' if needed.
7. Expand Agent Management and assign 'Agent Administration' if needed.
8. Expand Administration and assign 'DAS Statistics', 'User Session Management' or 'iTRAC Role Management' if needed.
9. Click the Roles tab and assign either Admin or Analyst Workflow Role. Click Ok.
10. If applicable, import any correlation rules. Rule Sets will be Rule Folders.
11. Copy from backup Agent scripts and port configurations by following the instructions in the section Post-Migration – Reconfiguring Agent Scripts and Port Configurations

Post-Migration – Reconfiguring Agent Scripts and Port Configurations

On each machine where the Sentinel 5 Agent Service (Agent Manager) is installed, perform the following steps to re-establish the Agent scripts and port configurations that were being used in the Sentinel v4.2 installation.

To re-establish the Agent scripts and port configurations

1. Stop the Agent Manager Windows service.
2. From the location you placed a backup of the %WORKBENCH_HOME%\Agents directory of the Sentinel v4.2

installation, copy the following files to the directory %WORKBENCH_HOME%\Agents of the current Sentinel 5 installation (overwrite files, if necessary):

- localhost_portcfg.dat
- localhost_snmpcfg.dat

3. Read the text file you created during Pre-Migration that lists all of the Agents being used by the Sentinel v4.2 Agent Manager installation on this machine. You will need to know the Agent names for the next step.
4. From the location you placed a backup of the %WORKBENCH_HOME%\Elements directory of the Sentinel v4.2 installation, copy the directories whose names match Agent names in the text file into the directory %WORKBENCH_HOME%\Elements of the current Sentinel 5 installation (overwrite directories/files, if necessary).
5. Insert the Sentinel v5.1 installation CD-ROM if it is not already inserted.
6. Open a command prompt. From within the 'utilities' directory in the CD-ROM, execute the command:

```
.\UpgradePortCfgFile.bat
```

7. Start Agent Manager Windows service.

Post-Migration – Configuring Sentinel 5 for Crystal Reporting

If you were running Crystal Reporting for v4.2 and want run Crystal Reporting in Sentinel, you will have to:

- Upgrade to Crystal BusinessObjects Enterprise™ 11 (if you are running v5.1.1)
- Change your ODBC settings
- Import all the Crystal Report templates including the Data Migration templates

See the 'Crystal Reports' installation chapter for more information.

Patch from v5 to v5.1

The v5.1 installer supports upgrade from v5.0 or v5.0.1 to v5.1. Perform this procedure on any machine that has any Sentinel components installed.

> **NOTE**: You cannot go directly from v5 to v5.1.1. Patch paths are v5 or v5.0.1 to v5.1 and v5.1 to v5.1.1. If you are patching from v5 or v5.0.1 to v5.1.1, you must first patch to v5.1 before patching to v5.1.1.

Sentinel v5 to v5.1 Patch when e-Security Database Administrator (esecdba) is a SQL Server Authentication Login

> **NOTE**: Procedure for patching from v5 to v5.1 is identical to the procedure for patching from v5.1 to v5.1.1. Go to section Sentinel v5.1 to v5.1.1 Upgrade when e-Security Database Administrator (esecdba) is a SQL Server Authentication Login.

Sentinel v5 to v5.1 Patch for Windows Authentication

For Windows Authentication, the patch InstallShield will not apply the database patch. The database patch installer must be run as the ‘esecdba’ Windows Domain user for the Sentinel Database.

During the patch process, you will get a popup message stating that the database patch must be done via the command line.

> **NOTE**: Procedure for patching from v5 to v5.1 is identical to the procedure for patching from v5.1 to v5.1.1. When running the patch installer on the database machine you can find the name of the ‘esecdba’ user in SQL Server Enterprise Manager. Go to section Patch from v5.1 to v5.1.1 for Windows Authentication for determining the ‘esecdba” username and patch procedures.

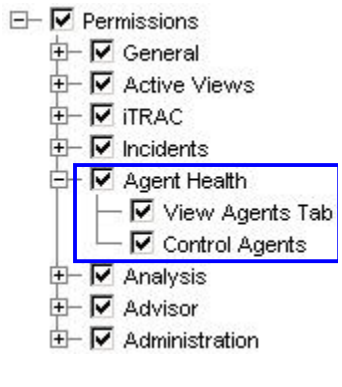
Updating User Management Permissions for v5 or v5.0.1 to v5.1

When upgrading from v5 or v5.0.1 to v5.1, Agent Health is changed to Agent Management with an additional Agent Administration functionality added.

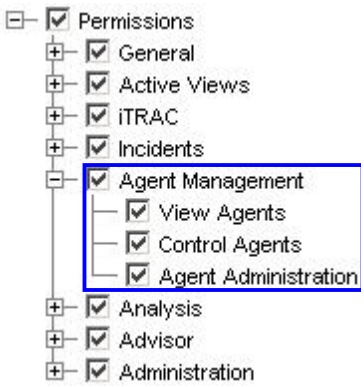
Updating User Management Permissions

1. Log into Sentinel Control Center as a user with Administration/User Management permission.

   In v5.1, Agent Health under Permissions has been changed from 'Agent Health' to 'Agent Management' with an additional permission added.



Sentinel v5.0 User Permission



Sentinel v5.1 User Permission

2. In Sentinel Control Center, click the Admin tab. Expand User Configuration in the Navigation pane or from the navigation bar click Admin > User Configuration.
3. Right click on an Admin user (i.e. esecadm or other admin user) > User Details. Click the Permissions tab.
4. Expand Agent Management and assign 'Agent Administration'. Click Ok.

Patch from v5.1 to v5.1.1

Perform this procedure on any machine that has any Sentinel components installed.

NOTE: You cannot go directly from v5 to v5.1.1. Patch paths are v5 or v5.0.1 to v5.1 and v5.1 to v5.1.1. If you are patching from v5 or v5.0.1 to v5.1.1, you must first patch to v5.1 before patching to v5.1.1.

Sentinel v5.1 to v5.1.1 Patch when e-Security Database Administrator (esecdba) is a SQL Server Authentication Login

Upgrading from v5.1 to v5.1.1 for SQL Server Authentication

1. Insert the Sentinel installation CD into the CD-ROM drive.
2. Browse to the CD and double-click setup.bat.

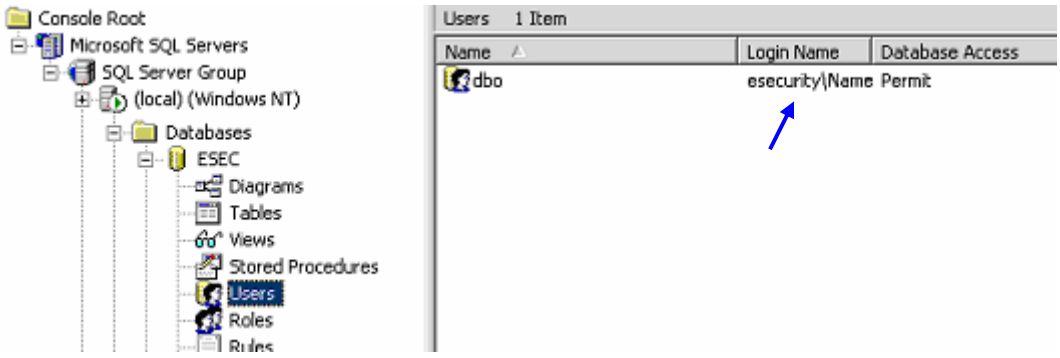
   NOTE: Installing in console mode is not currently supported on Windows.
3. Click Next on the Welcome screen.
4. Accept the End User License Agreement and click Next.
5. Click Next until the database information window.
6. Ensure the database type is correct. Select the location of the database install log directory. Click Next.
7. Ensure the information for the MS SQL server is correct. Select SQL Server Authentication. Enter your user name password.

   NOTE: For SQL Server authentication, use the esecdba user, not the sa user.
8. Click Next until the end of the install. You may be prompted to reboot your machine.

Sentinel v5.1 to v5.1.1 Upgrade for Windows Authentication

For Windows Authentication, the patch InstallShield will not apply the database patch. The database patch installer must be run as the 'esecdba' Windows Domain user for the Sentinel Database.

When running the patch installer on the machine where you originally installed the Database component, you will need to know the username and password of the e-Security Database Administrator (esecdba) user. You can determine what the esecdba user is by finding the Login Name for the dbo user of the e-Security database using SQL Server Enterprise Manager, as shown below.



During the patch process, you will get a popup message stating that the database patch must be done via the command line as explained below.

Patching from v5.1 to v5.1.1 for Windows Authentication

1. Insert the Sentinel installation CD into the CD-ROM drive.
2. Browse to the CD and double-click setup.bat.

   NOTE: Installing in console mode is not currently supported on Windows.
3. Click Next on the Welcome screen.
4. Accept the End User License Agreement and click Next.
5. Click Next until the database information window.
6. Ensure the database type is correct. Select the location of the database install log directory. Click Next.
7. Ensure the information for the MS SQL server is correct. Select Windows Authentication. Enter your user name password.
8. Click Next until the end of the install. During the patch install, at the database machine, you will get the following popup message. Click OK and continue.

   CAUTION: For the database machine, DO NOT REBOOT AT THE END OF THE INSTALL.
9. At the database machine, without rebooting, exit InstallShield.
10. If not already, at the database machine, login as the 'esecdba' Windows Domain user.
11. Open a command prompt.
12. Browse to the Sentinel installation CD and browse to:

    ```
    PATCH_INSTALLER\sentinel\dbsetup\bin
    ```
13. Enter the command:

    ```
    PatchDb.bat
    ```
14. At the prompt, enter the hostname or static IP address of the SQL Server of the Sentinel Database that you want to patch.
15. At the prompt, enter the name of the SQL Server Sentinel Database to patch.
16. At the prompt, enter option 1 for Windows Authentication. The script will verify the entered information and begin the database patch.
17. After the script is done applying the patch, reboot your machine.

Crystal Reporting Server

After upgrading to v5.1.1, you must upgrade your Crystal Server from Crystal Enterprise 9 Standard® to Crystal BusinessObjects Enterprise™ 11. See the

Crystal Reports and Advisor Configuration Chapters. In addition, Sentinel 5 does not support Crystal XI on Windows® 2000 Server.

NOTE: Sentinel 5 does not support Crystal XI on Windows® 2000 Server.

Updating Sentinel email for SMTP Authentication

If your system requires SMTP authentication, you will need to update your execution.properties file. This file is on the machine that has DAS installed. It is located at %ESEC_HOME%\sentinel\config. To configure this file, run mailconfig.bat to change the file and mailconfigtest.bat to test your changes.

To Configure execution.properties file

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

   ```
   %ESEC_HOME%\sentinel\config
   ```

2. Execute mailconfig as follows:

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

   Example:

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

   After entering this command you will be prompted for a new password.

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

NOTE: When using the password option, it must be the last argument.

To test your execution.properties configuration

1. On the machine where you have DAS installed, cd to:

   ```
   %ESEC_HOME%\sentinel\config
   ```

2. Execute mailconfigtest as follows:

   ```
   mailconfigtest.bat -to <destination email address>
   ```

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

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

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

   ```
   Subject: Testing e-Security mail property
   This is a test for e-Security mail property set up.
      If you see this message, your e-Security mail
      property has been configured correctly to send
      emails
   ```

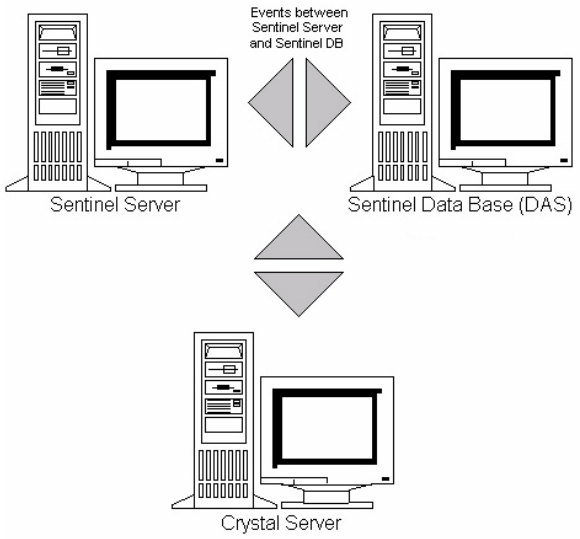
Chapter 8 – Crystal Reports for Windows and Solaris

Crystal BusinessObjects Enterprise™ 11 is a reporting tool.

This chapter discusses the installation configuration of Crystal Reports Server for Sentinel. The installation should be done in the order presented.

- Install Microsoft IIS and ASP.NET
- Install MS SQL (depending on configuration as Windows authentication or SQL Server authentication)
- Install Crystal Server
  - Configuring Open Database Connectivity (ODBC) for SQL Authentication

  or
  - Installing and Configuring Oracle 9i Client Software
- Configure inetmgr
- Patch Crystal reports
- Publishing (Importing) Crystal reports
- Setting a 'Named User' account
- Testing connectivity to the web server
- Enabling Top 10 reports (optional)
- Maximizing Event Reporting (recommended)
- Configuring Sentinel to the Crystal Enterprise Server



Overview

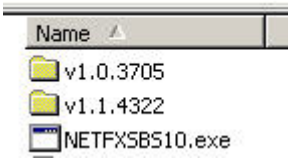
Crystal Reports Server requires a database to store information about the system and its users. This database is known as the Central Management Server (CMS) database. The CMS is a server that stores information about the Crystal Reports Server system. Other components of Crystal Reports Server can access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

It is required to set up a CMS database on top of a Local MS SQL 2000 Server database. Crystal Reports Server installer allows you to setup the CMS database

on top of MSDE database if a local MS SQL 2000 Server is not installed. Sentinel 5 does not support a MSDE configuration.

System Requirements

- Windows® 2003 Server with SP1 with an NTFS-formatted partition with IIS (Microsoft Internet Information Server) and NET.ASP installed. Sentinel 5 does not support Crystal XI on Windows® 2000 Server.
- .NET Framework 1.1 (Installed by default on Windows 2003. BusinessObjects Enterprise™ 11 does not support .NET Framework 2.0). 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:

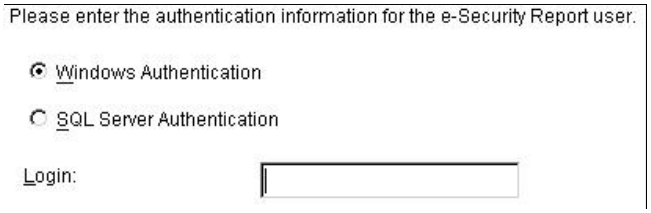


Configuration Requirements

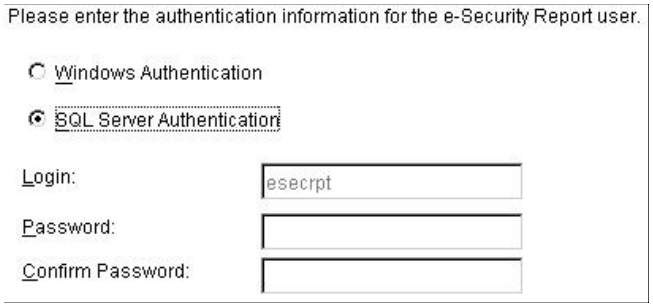
1. Make sure the account used to install Crystal Reports Server has local administrators right.
2. Disable Data Execution Prevention (DEP). This is particularly helpful to avoid “Error 1920. Service ‘Crystal Report Cache Server’ on Windows 2003”. Go to the following BusinessObjects website for procedures. http://support.businessobjects.com/library/kbase/articles/c2018187.asp

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

   DEP is accessed through Control Panel > System > Advanced > Performance Settings > Data Execution Prevention.
3. If you are planning to run e-Security reports using Windows NT authentication, make sure windows domain account for e-Security Report user already exists on e-Security database. This is done during Sentinel install by selecting Windows Authentication when setting the “Authentication Method for the e-Security Report user” as per the illustration below.



4. If you are planning to run e-Security reports using SQL Server authentication (also required for Sentinel Oracle installations), make sure the SQL Server login (esecrpt) already exists on e-Security database.
   - For Sentinel MS SQL database - this is done during Sentinel install for MS SQL by selecting SQL Server Authentication when setting the “Authentication Method for the e-Security Report user” as per the illustration below.



- For Sentinel Oracle database – this is done during Sentinel install for Oracle. esecrpt assumes the same password as esecadm.

5. For Oracle - Oracle 9i Client Release 2 (9.2.0.1.0), install this before installing Crystal BusinessObjects Enterprise™ 11.
6. For MS SQL Server - Install MS SQL 2000 sp3a prior to installing Crystal Reports Server 11.
7. Video resolution of 1024 x 768 or higher
8. Install Microsoft Internet Information Server (IIS) and NET.ASP

NOTE: Sentinel 5 does not support MSDE. Install MS SQL 2000 sp3a prior to installing Crystal Reports Server 11.

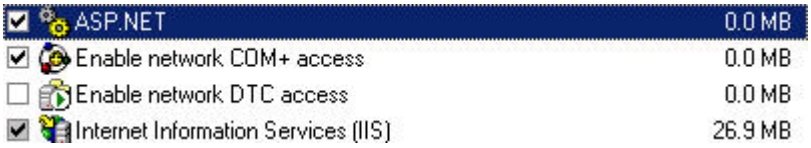
Installing Microsoft Internet Information Server (IIS) and ASP.NET

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

Installing IIS and ASP.NET

1. Go to Windows 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 may be prompted for the Windows installation CD.
8. Click Finish.

Known Issues

1. Installing Crystal Reports - You are issued with two keys, one for Crystal Reports Server and the other for Crystal Reports Developer. Make sure to use the Crystal Reports Server key when installing Crystal Reports Server.
2. Uninstalling Crystal Reports - In the event that you have to uninstall Crystal Reports Server, there is a manual uninstall procedure available

that cleans out the registry keys. This is particularly useful if your installation gets corrupted. Go to the following BusinessObjects website for procedures in manually uninstalling BusinessObjects Enterprise XI, http://support.businessobjects.com/library/kbase/articles/c2017905.asp.

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

3. During configuring .NET Administration Launchpad, when changing the access level from '(Inherited Rights)' to 'View on Demand' the update process will hang. Wait approximately thirty seconds. The Access Level will update.

Using Crystal Reports

For information about using Crystal Reports for Sentinel Reporting, see the *Crystal Reports Documentation* and *Sentinel User's Guide*.

Installation Overview

Installation Overview for MS SQL 2000 Server with Windows Authentication

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

1. Install Crystal Reports Server 11 – When installing the Sentinel 5 application, if you selected Windows Authentication for the e-Security Report user, follow the link for Installing Crystal Server for MS SQL 2000 Server with Windows Authentication.
2. Configure Open Database Connectivity (ODBC)
3. Mapping Crystal Reports for use with Sentinel
4. Import Crystal Report Templates
5. Create a Crystal Web Page (Configuring .NET Administration Launchpad)
6. Configure Sentinel to the Crystal Enterprise Server

Installation Overview for MS SQL 2000 Server with SQL Server Authentication

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

1. Install Crystal Reports Server 11 – When installing the Sentinel 5 application, if you selected SQL Server Authentication for the e-Security Report user, follow the link for Installing Crystal Server for MS SQL 2000 Server with SQL Authentication or for Oracle.
2. Configure Open Database Connectivity (ODBC)
3. Mapping Crystal Reports for use with Sentinel
4. Import Crystal Report Templates
5. Create a Crystal Web Page (Configuring .NET Administration Launchpad)
6. Configure Sentinel to the Crystal Enterprise Server

Installation Overview for Oracle

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

1. Install Oracle 9i Client
2. Install Crystal Reports Server 11 – follow the link for Installing Crystal Installing Crystal Server for MS SQL 2000 Server with SQL Authentication or for Oracle.
3. Configure Oracle native driver
4. Mapping Crystal Reports for use with Sentinel
5. Import Crystal Report Templates
6. Create a Crystal Web Page (Configuring .NET Administration Launchpad)
7. Configure Sentinel to the Crystal Enterprise Server

Installation

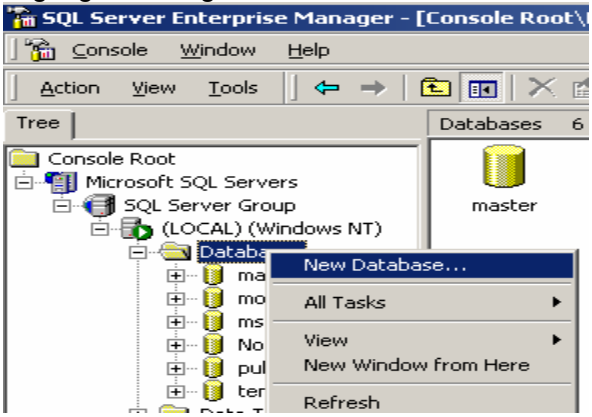
This section covers how to install Crystal Server for:

- MS SQL 2000 Server Sentinel database with Windows Authentication
- MS SQL 2000 Server Sentinel database with SQL Server Authentication
- Oracle Sentinel database

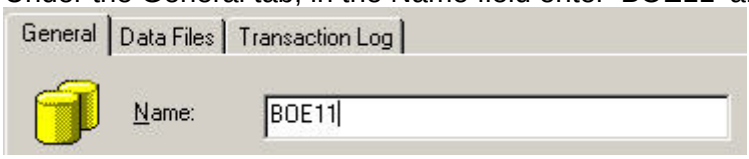
Installing Crystal Server for MS SQL 2000 Server with Windows Authentication

BOE XI Crystal Server Window Authentication Installation

1. Install MS SQL 2000 sp3a in mixed mode.
2. Launch MS SQL Enterprise Manager.
3. In the navigation pane, expand (local)(Windows NT).
4. Highlight and right-click on Database and select ‘New Database…’

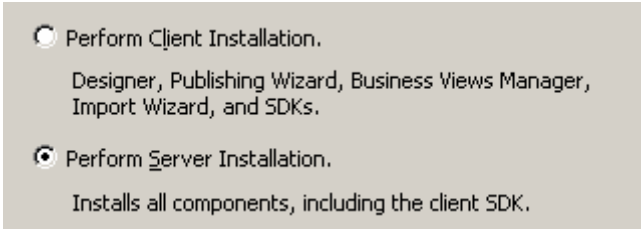


5. Under the General tab, in the Name field enter ‘BOE11’ and click OK.

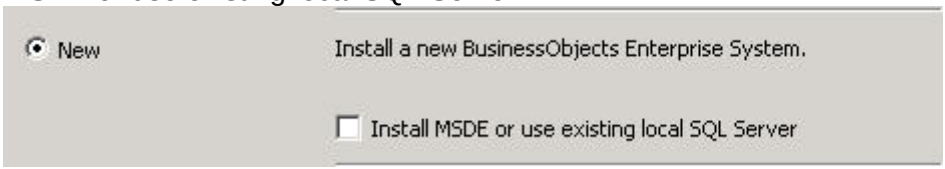


6. Exit MS SQL Enterprise Manager.

7. Insert the BOE XI Crystal Server CD into the CD-ROM.
8. If Autoplay is disabled on your machine, run setup.exe.
9. In the Select Client or Server Installation window, select Perform Server Installation.

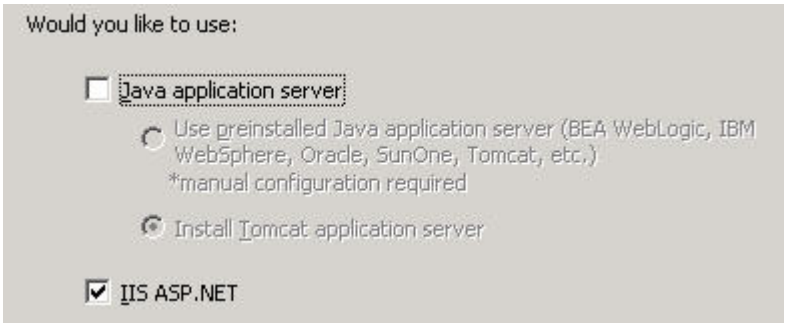


10. For install type, select the New radio button and do not select 'Install MSDE or use existing local SQL Server'.

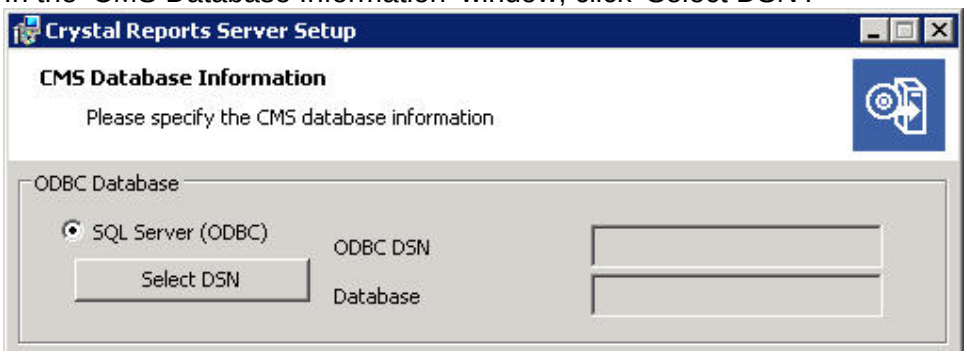


11. In the Web Component Adapter Type window, select IIS ASP.NET.

> **NOTE**: If you have not installed IIS and ASP.NET through Control Panel > Add Remove Program > Add/Remove Windows Components, IIS ASP.NET will be grayed out.

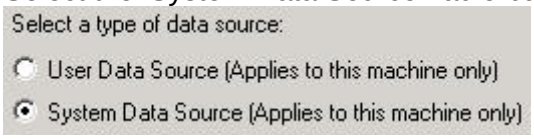


12. In the 'CMS Database Information' window, click 'Select DSN'.



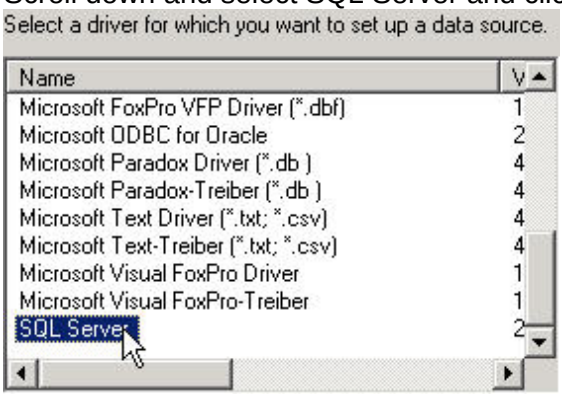
13. Click the 'Machine Data Source' tab.
14. Click the 'New…' button.

15. Select the ‘System Data Source’ radio button.

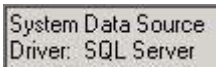


Click Next.

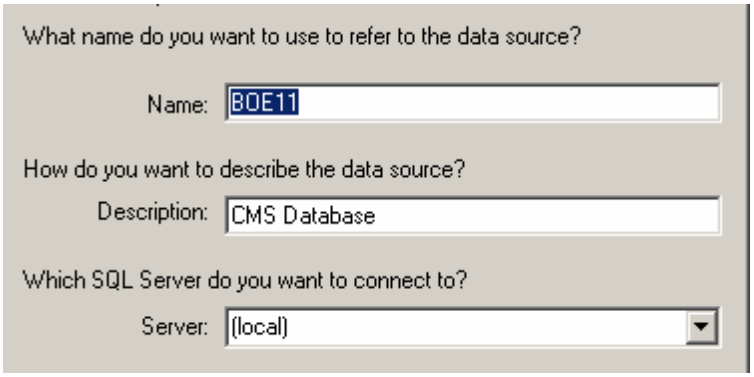
16. Scroll down and select SQL Server and click Next.



17. A new source will appear, click Finish.

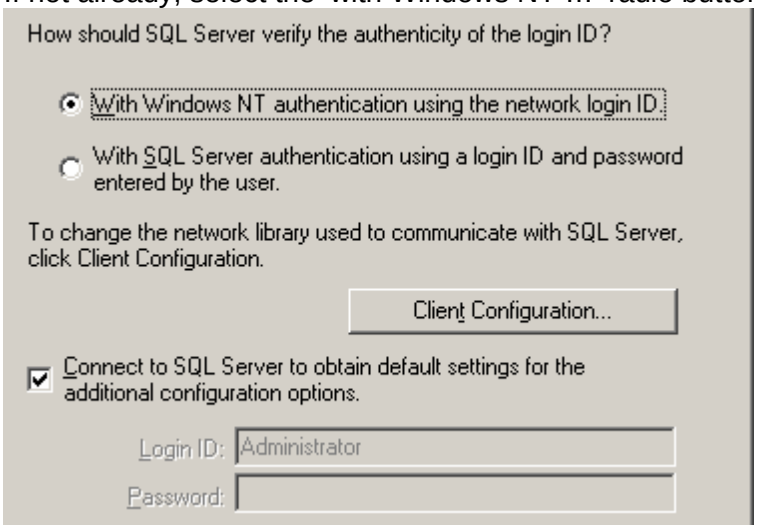


18. In the ‘…New Data Source to SQL Server’ window, enter:
    - Name of your data source (ex: i.e. BOE_XI)
    - Description (optional)
    - For Server, click the down arrow and select ‘(local)’



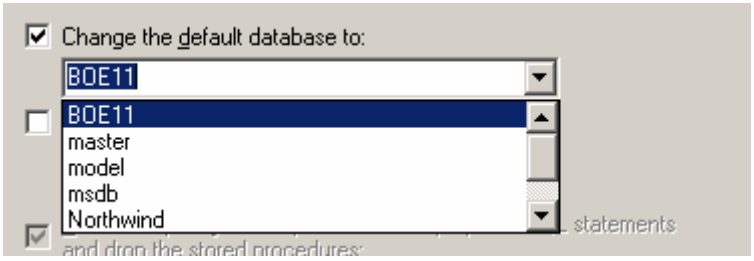
Click Next.

19. If not already, select the 'with Windows NT …' radio button. Click Next.

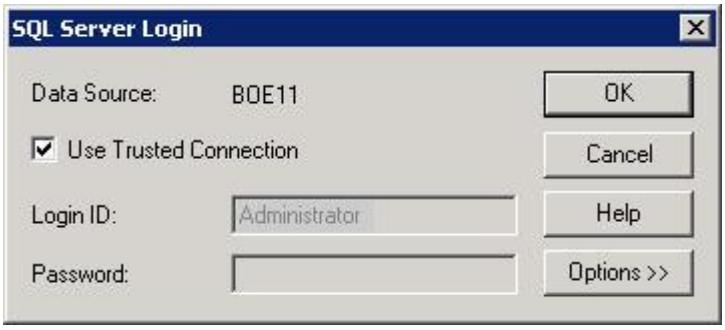


NOTE: The Login ID (grayed out) is your Windows login name.

20. Check the 'Change the default database to:' check box. Change your default database to 'BOE11'. Click Next.



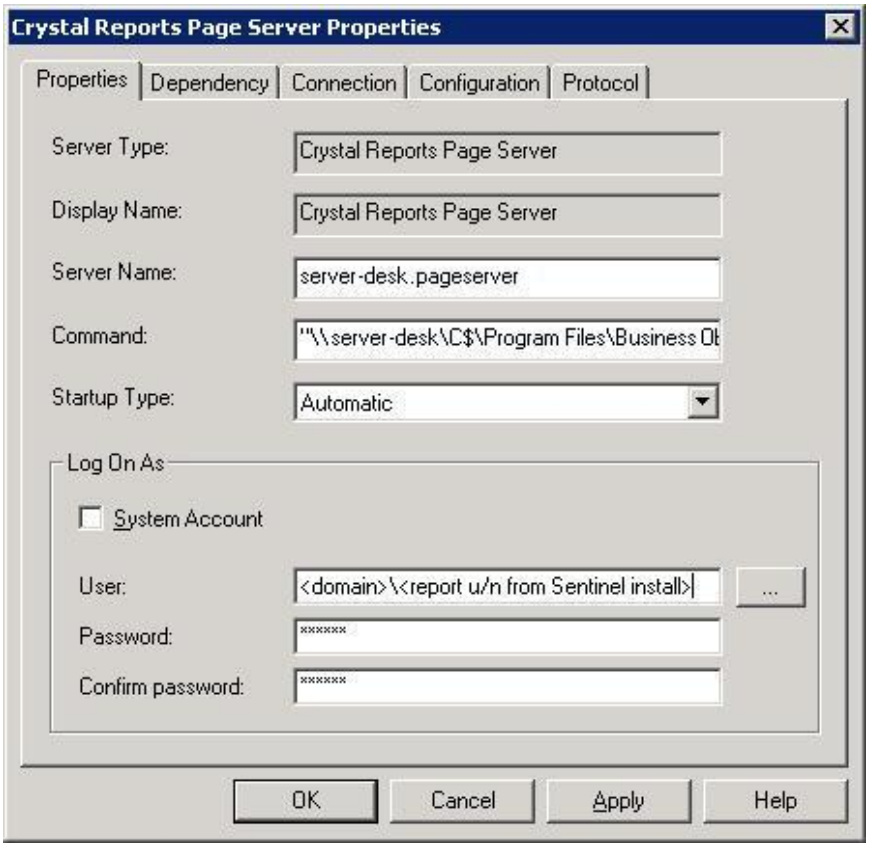
21. In the 'Create a New Data Source to SQL Server' window, click Finish.
22. Click the 'Test Data Source…' button. Should be successful. Click OK.
23. In the Select Data Source window, high light BOE11 and continue to click OK until you get to the 'SQL Server Login'. Ensure that 'Use Trusted Connection' is selected. Click OK.



NOTE: The Login ID (grayed out) is your Windows login name.

24. At the Warning Window, click OK.
25. At the 'CMS Database Information Window', click Next.
26. Click Next to continue installation.
27. After installation, you will need to change the log on account for Crystal Reports Page Server and Crystal Reports Job Server to e-Security Report User domain account.

a. Click Start > Programs > BusinessObjects 11 > Crystal Reports Server > Central Configuration Manager.
b. Right click on 'Crystal Reports Page Server' and select stop.
c. Right click on 'Crystal Reports Page Server' again and select Properties.
d. Uncheck "Log On As System Account" and enter the e-Security Report User domain account username and password that was used for the e-Security Report User during your Sentinel 5 install. Click OK.



e. High light Crystal Reports Page Server, right click to start the Crystal Reports Page Server.

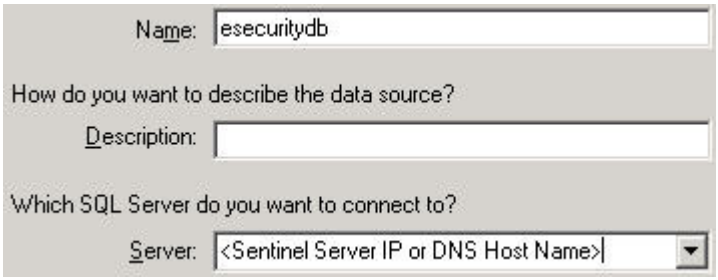
Configuring Open Database Connectivity (ODBC) for Windows Authenticaton

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

Setting up an ODBC data source for Windows Authentication

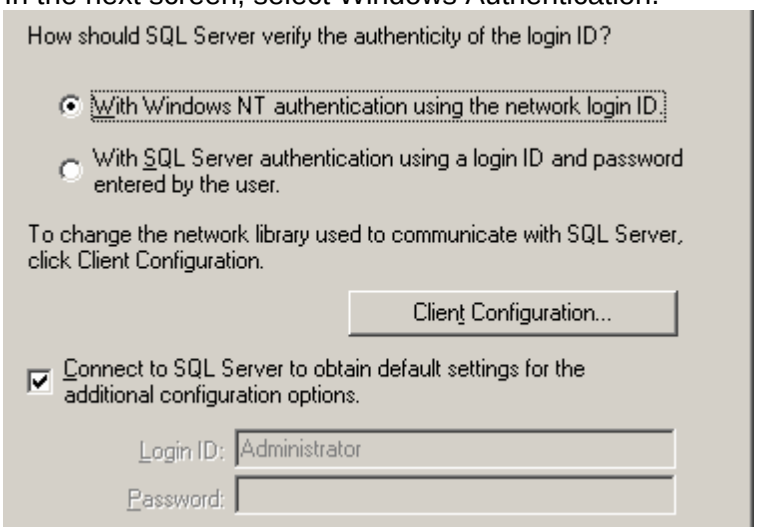
1. Go to Windows Control Panel > Administrative Tools > Data Sources (ODBC).
2. Click on System DSN tab and click the Add button.
3. Select SQL Server. Click Finish.
4. A screen will appear prompting for driver configuration information:
   - Data Source name, enter esecuritydb

- Description field (optional), enter a description
- Server field, enter your host name or IP address of your Sentinel Server



Click Next.

5. In the next screen, select Windows Authentication.



NOTE: The Login ID (grayed out) is your Windows login name.

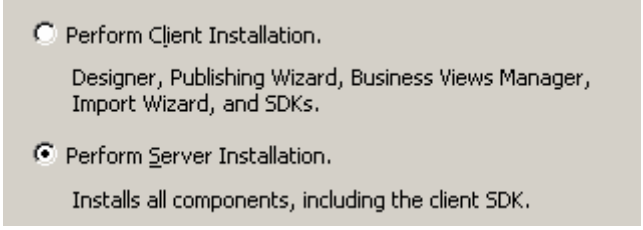
6. In the next screen select:
   - Change the e-Security database (Default name is ESEC)
   - Leave all the default settings

   Click Next.
7. Click Finish.
8. Click Test Data Source… You should get a successful connection. Click OK until you exit.

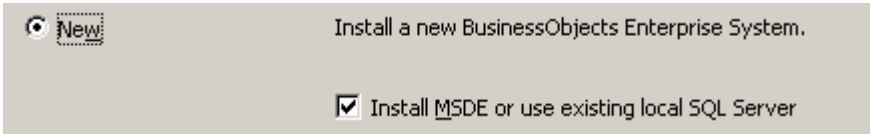
Installing Crystal Server for MS SQL 2000 Server with SQL Authentication

Install Crystal Reports Server 11 with the following options selected.

- Perform Server Installation



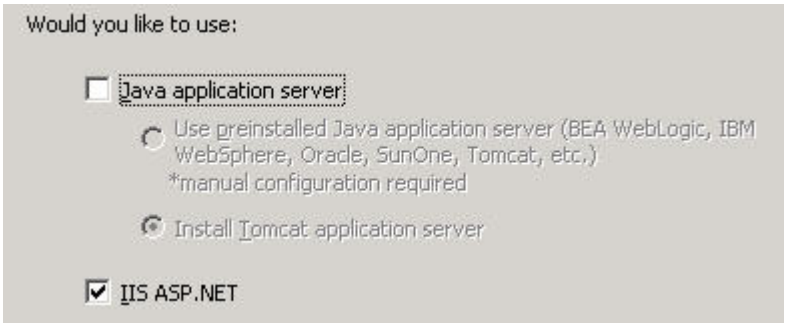
- Install a new BusinessObjects Enterprise System with the 'Install MSDE or use existing local SQL Server'.



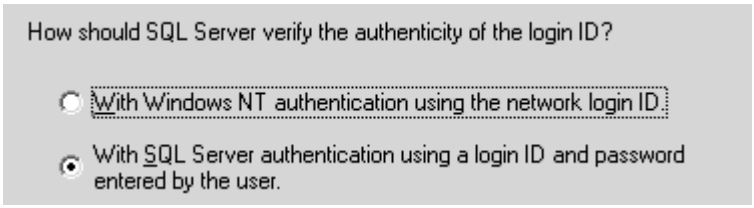
NOTE: Crystal Server and MS SQL Server 2000 must reside on the same machine.

- IIS ASP.NET.

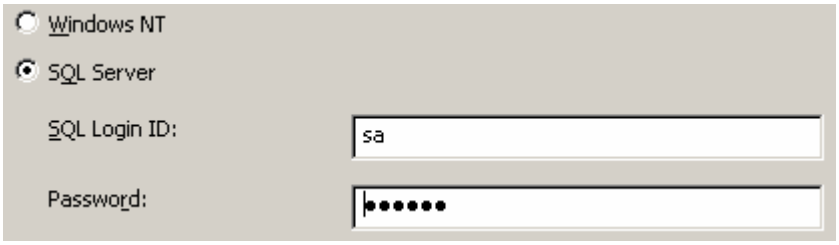
NOTE: If you have not installed IIS and ASP.NET through Control Panel > Add Remove Program > Add/Remove Windows Components, IIS ASP.NET will be grayed out.



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



- Select SQL Server Authentication. Enter sa and sa password.



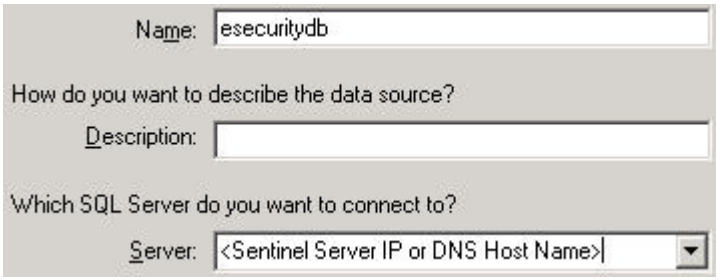
Configuring Open Database Connectivity (ODBC) for SQL Authentication

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

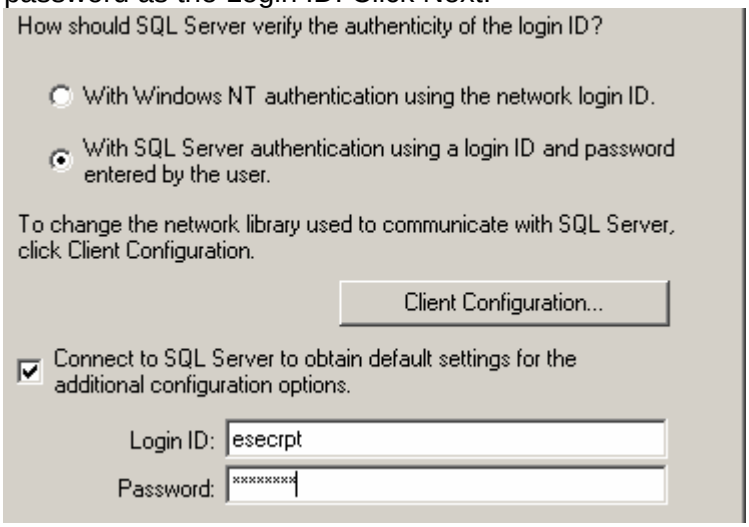
Setting up an ODBC data source for Windows

1. Go to Windows Control Panel > Administrative Tools > Data Sources (ODBC).
2. Click on System DSN tab and click the Add button.

3. Select SQL Server. Click Finish.
4. A screen will appear prompting for driver configuration information:
   - Data Source name, enter esecuritydb
   - Description field (optional), enter a description
   - Server field, enter your host name or IP address of your Sentinel Server



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



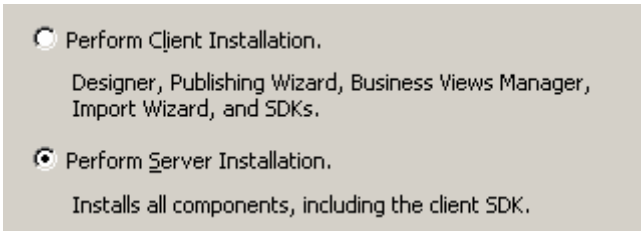
6. In the next screen select:
   - Change the e-Security database (Default name is ESEC)
   - Leave all the default settings

   Click Next.
7. Click Finish.
8. Click Test Data Source… You should get a successful connection. Click OK until you exit.

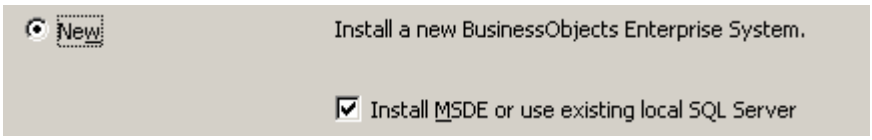
Installing Crystal Server for Oracle

Install Crystal Reports Server 11 with the following options selected.

- Perform Server Installation



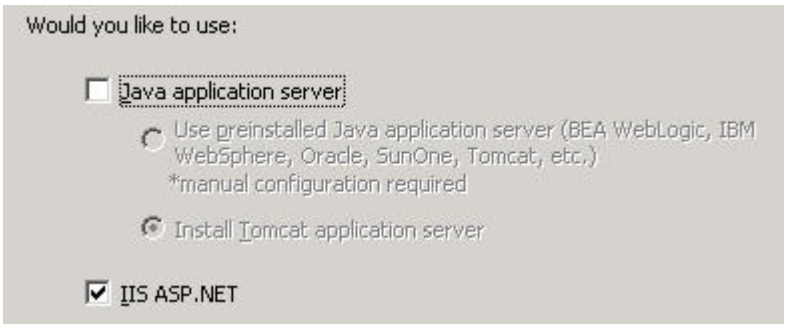
- Install a new BusinessObjects Enterprise System with the 'Install MSDE or use existing local SQL Server'.



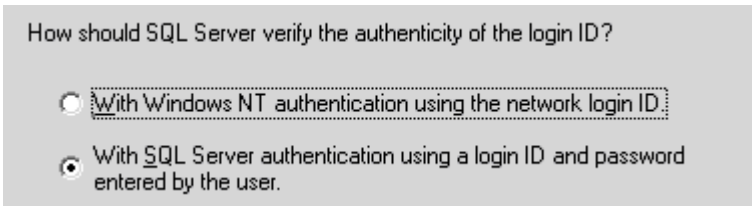
NOTE: Crystal Server and MS SQL Server 2000 must reside on the same machine.

- IIS ASP.NET.

NOTE: If you have not installed IIS and ASP.NET through Control Panel > Add Remove Program > Add/Remove Windows Components, IIS ASP.NET will be grayed out.



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



Crystal Reports supports direct access to Oracle 9 databases. This accessibility is provided by the crdb_oracle.dll translation file. This file communicates with the Oracle 9 database driver, which works directly with Oracle databases and clients, retrieving the data you need for your report.

NOTE: In order for Crystal Reports to use Oracle 9 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 9i Client Software

When installing Oracle 9i 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 install, create a local Net Service Name configuration.

Creating 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, enter a Net Service Name.
   - Enter 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:
   - Enter the hostname or IP address of the machine the database resides on
   - Select the Oracle Port (default 1521 on install)

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

   Click Next.
8. In the Test window, click the ‘Test…’ button. Click Next. Test may fail because the test uses a DB ID and password.
9. If test fails perform the following:
   - In the Connecting window, click Change Login.
   - Enter the Sentinel Oracle ID (use esecrpt) and password. Click OK.

   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 Finish.

Configuration for all Authentications and Configurations

Mapping Crystal Reports for use with Sentinel

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

Configuring inetmgr

inetmgr

1. Copy the web.config file from:

   ```
   C:\Program Files\Business Objects\BusinessObjects
      Enterprise 11\Web Content
   ```

   to c:\Inetpub\wwwroot.
2. Launch Internet Service Manager by clicking Start > Run. Enter inetmgr and click Ok.
3. Expand (local computer) > 'Web Sites' > 'Default Web Site' > businessobjects.
4. On businessobjects, right-click > properties.
5. Under the Virtual Directory tab, click the Configuration... button.
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	C:\Program Files\Business Objects\BusinessObjects Enterprise 11\win32_x86\cdzISAPI.dll

   Click OK to close the window.
7. Restart IIS by, expand (local computer) > 'Web Sites' > 'Default Web Site', high-light 'Default Web Site' and right-click > Start.

Patching Crystal Reports for use with Sentinel

In order to view Crystal Reports from the Sentinel Control Center's Analysis tab, several Crystal Enterprise files need to be updated to make them compatible with the browser that is embedded in Sentinel.

The following table lists those files and describes what each file is used for.

File Name	***Description***

`calendar.js`
 	
`calendar.html`
	Displays a popup calendar when you are selecting a date as a parameter to a report.

File Name	*Description*
`grouptree.html`	Displays the Loading... message while reports are loading.
`exportframe.html`	Displays the window that allows you to export a report for saving or for printing.
`exportIce.html`	File used by Sentinel when exporting a report for saving or for printing.
`GetInfoStore.asp`	File used to query the Crystal Server
`GetReports.asp`	File used by Sentinel Control Center to establish a connection with Crystal Server and display the report list.
`helper_js.asp`	A call file used by GetInfoStore.asp.

Patching Crystal Reports

1. On the Sentinel Service Pack CD-ROM, go to \content\reports\patch and copy all *.html and *.js files to the viewer file location, default is:

   ```
   C:\Program Files\Business Objects\BusinessObjects
      Enterprise 11\Web Content\Enterprise11\viewer\en
   ```

2. On the Sentinel Service Pack CD-ROM, go to \content\reports\patch and copy all *.asp and *.js files to:

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

> **NOTE:** Your web folder may be on a different drive or in a different location than specified above.

Crystal Report Templates

Crystal Report Templates are published using the Crystal Publishing Wizard.

Latest set of report templates can be downloaded from the customer portal at http://esecurity.custhelp.com/.

> **NOTE**: List of Attacks by CVE Report is an intersection of attack signatures from the Advisor feed and scanned vulnerabilities.

> **NOTE**: 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 Sentinel User's Guide, Chapter 10 – Sentinel Data Manager, section Reporting Data Tab or go to section Enabling Sentinel Top 10 Reports.

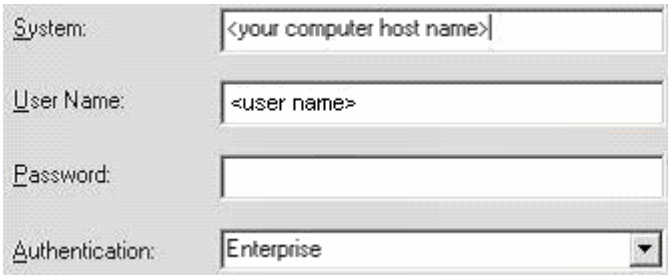
Publishing Report Templates Using Crystal Publishing Wizard

Publishing Crystal Report Templates

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

1. Click Start > All Programs > BusinessObjects 11 > Crystal Reports Server > Publishing Wizard.
2. Click Next.
3. 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. Enter your password and click Next.

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



4. Click the 'Add Folder' button.
5. Click the 'Include Subfolder' check box. Go to the Sentinel Service Pack CD-ROM and navigate to:

   For Crystal Reports (Oracle users):

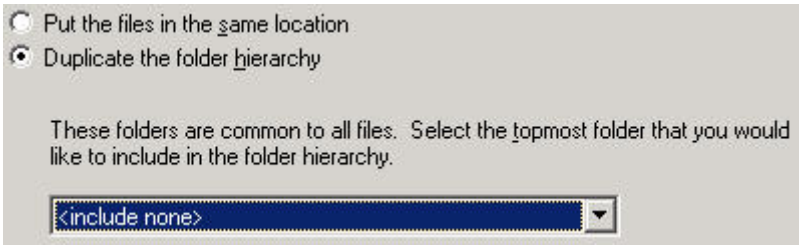
   ```
   \content\reports\Crystal_v11\SQL-Server
   ```

   For Crystal Reports (MSSQL users):

   ```
   \content\reports\Crystal_v11\Oracle
   ```

   Click OK.
6. Click Next.
7. In the Specify Location window, click the New Folder button (upper right corner) and create a folder called eSecurity_Reports. Click Next.

8. Select:
   - 'Duplicate the folder hierarchy' radio button.
   - Click the down arrow and select '<include none>'



Click Next.

9. In the Confirm Location window, click Next.
10. In the Specify Categories window:
    - a category name of choice (such as esecurity)
    - high-light the name and click the + button

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

    - click Next.
11. In the Specify Schedule window, click 'Let users update the object' (this should be default) radio button. Click Next.
12. In the Specify Repository Refresh window, click Enable All to enable repository refresh. Click Next.
13. In the Specify Keep Saved Data window, click Enable All to keep saved data when publishing reports. Click Next.
14. In the Change Defaults Values window, click 'Publish reports without modifying properties' radio button (this should be default). Click Next.
15. Click Next to add your objects.
16. Click Next.
17. A published list will appear, click Finish.

When the e-Security templates for Crystal Reports are published to the Crystal Enterprise server, the templates must reside within the eSecurity_Reports directory.

Setting a 'Named User' Account

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

Setting the Guest Account as 'Named User'

1. Click Start > All Programs > BusinessObjects 11 > Crystal Reports Server > .NET Administration Launchpad.
2. Click Central Management Console.
3. The System Name should be your host computer name. Authentication Type should be Enterprise. If not, choose Enterprise.
4. In the Organize pane, click Users.

5. Click Guest.
6. Change connection type from ‘Concurrent User’ to ‘Named User’.
7. Click Update.
8. Logoff and close window or proceed to section ‘Configuring .NET Administration Launchpad’.

Configuring .NET Administration Launchpad

This procedure discusses how to configure .NET Administration Launchpad to allow you to view and modify reports.

Configuring .NET Administration Launchpad

1. If not already, start .NET Administration Launchpad (Click Start > All Programs > BusinessObjects 11 > Crystal Reports Server > .NET Administration Launchpad).
2. Click Central Management Console.

   The System Name should be your host computer name. Authentication Type should be Enterprise. If not, choose Enterprise.
3. Enter your user name, password and click Log On.
4. In the Organize pane, click on Folders.
5. Single-click eSecurity_Reports.
6. Select All.
7. Click the Rights tab.
8. For Everyone, in the drop-down menu to the right under Access Level select ‘View on Demand’. Click Update.

   NOTE: When changing the access level from ‘(Inherited Rights)’ to ‘View on Demand’ the update process will hang. Wait approximately thirty seconds. The Access Level will update.
9. Logoff and close the window.

Testing for Web Server Connection to the Database

Testing for web server connection to the database

1. If not already, start .net Administration Launchpad (Start > All Programs > BusinessObjects 11 > Crystal Reports Server > .NET Administration Launchpad).
2. Enter Administrator as the User Name. Enter your password (by default, this will be blank). Click Log On.
3. Click Central Management Console.
4. Navigate to Public Folders > eSecurity_Reports > Internal Events Management.
5. Select ‘Column Display Details’.
6. Under the sort field drop-down menu, select Tag.
7. Click OK. A report should appear.

Testing Connectivity to the Web Server

Testing connectivity to the web server

1. Go to another machine that is on the same network as your webserver.
2. Enter

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

3. You should get a Crystal BusinessObjects Web page.

Enabling Sentinel Top 10 Reports

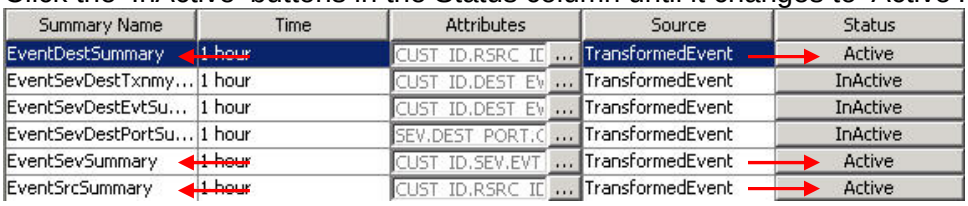
To enable Sentinel Top 10 Reports, you have to:

- Turn on Aggregation
- Enable EventFileRedirectService

Turning on Aggregation (aggregation)

1. Start Sentinel Data Manager.
2. Login.
3. Click the Reporting Data tab.
4. Enable the following summaries
   - EventDestSummary
   - EventSevSummary
   - EventSrcSummary

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



Enabling EventFileRedirectService (EventFileRedirestService)

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

   For UNIX:

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

   For Windows:

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

2. For EventFileRedirectService, change the status to on.

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

3. For Windows, restart the eSecurity service. For UNIX, reboot the DAS machine.

Maximizing Your Event Reporting

Depending on the number of events that Crystal is querying, you may get an error on maximum processing time or maximum record limit. To set your server to process a higher number or an unlimited number or reports you will need to reconfigure the Crystal Page Server. There are two methods of doing this, using the Central Configuration Manager or using the Crystal Web Page.

Reconfiguring the Crystal Page Server via the Central Configuration Manager

1. Click Start > All Programs > BusinessObjects 11 > Crystal Reports Server > Central Configuration Manager.
2. Right-click on ‘Crystal Reports Page Server’ and select Stop.
3. Right-click on ‘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.

Reconfiguring the Crystal Page Server via the Crystal Web Page

1. Open a web browser and enter the following url:

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

2. Click Central Management Console.
3. The System Name should be your host computer name. Authentication Type should be Enterprise. If not, choose Enterprise.
4. Enter your user name, password and click Log On.
5. Click Servers.
6. Click <server name>.pageserver
7. Under ‘Database Records to Read When Previewing Or Refreshing a report’, click the ‘Unlimited records’ radio button.
8. Click Apply.
9. A prompt to restart the page server will appear, click OK.
10. You may be prompted for a logon name and password to access the operating system service manager.

Configuring Sentinel to the Crystal Enterprise Server

After Crystal Enterprise is installed, the Sentinel Control Center needs to have the URLs for the Analysis reports.

Configuring Sentinel to the Crystal Enterprise Server

1. At the Sentinel Control Center, login as user esecadm.
2. Click the Admin tab.
3. Click on General Options in the navigator tree.
4. Click Modify.

5. In the Analysis URL field, enter the following (<IP> is the Crystal Enterprise Server IP):

   ```
   http://<IP>/GetReports.asp?APS=<IP>&user=Guest&pass
      word=&tab=Analysis
   ```

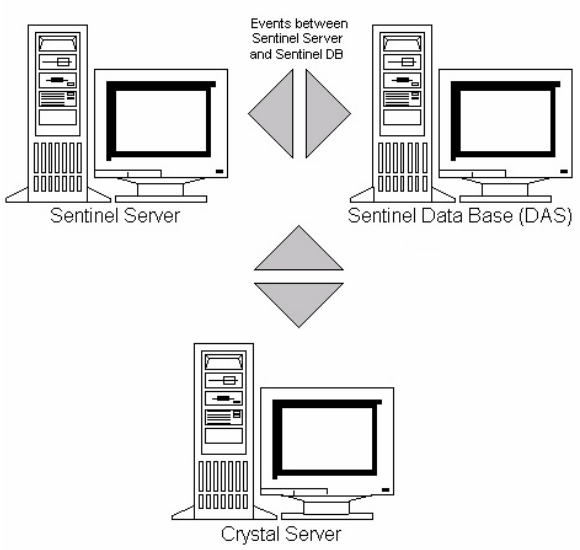
6. Click the refresh button next to the Analysis field.
7. Click the refresh button next to the Advisor field.
8. Click Save.
9. Logout and log back in to view the reports on the Analysis tabs.

Chapter 9 – Crystal Reports for Linux

Crystal BusinessObjects Enterprise™ 11 is one of the reporting tools with Sentinel.

This chapter discusses the installation configuration of Crystal Reports Server for Sentinel on Linux. The installation should be done in the order presented.

- Pre-install and install of Crystal BusinessObjects Enterprise™ 11
- Patch Crystal reports
- Publishing (Importing) Crystal reports
- Setting a 'Named User' account
- Testing connectivity to the web server
- Enabling Top 10 reports (optional)
- Maximizing Event Reporting (recommended)
- Configuring Sentinel to the Crystal Enterprise Server



Using Crystal Reports

For information about using Crystal Reports for Sentinel Reporting, see the *Crystal Reports Documentation* and *Sentinel User's Guide*.

Configuration

- Red Hat Enterprise Linux 3 Update 5 ES (x86)
- BusinessObjects Enterprise XI Server installed
- For Oracle - Oracle 9i Client Release 2 (9.2.0.1.0)

Installation

Pre-Install of Crystal BusinessObjects Enterprise™ 11

Pre-Install of Crystal BusinessObjects Enterprise

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

   ```
   groupadd bobje
   ```

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

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

5. Create directory for Crystal Software:

   ```
   mkdir –p /opt/crystal_xi
   ```

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

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

7. Change to the crystal user:

   ```
   su - crystal
   ```

8. The ORACLE_HOME environment variable must be set in the crystal user's environment. To do this, modify the crystal user's login script to set the ORACLE_HOME environment variable to the base of the Oracle software. For example, if the crystal user's shell is bash and the Oracle software is installed in the directory /opt/oracle/product/9.2, then open the file ~crystal/.bash_profile and add the following line to the end of the file:

   ```
   export ORACLE_HOME=/opt/oracle/product/9.2
   ```

9. The LD_LIRBARY_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_LIRBARY_PATH environment variable to include the Oracle software libraries. For example, if the crystal user's shell is bash, then open the file ~crystal/.bash_profile and add the following line to the end of the file (below where the ORACLE_HOME environment variable is set):

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

10. An entry must be added to the Oracle tnsnames.ora file with the Service Name “esecuritydb” that points to the Sentinel Database. To do this on the Crystal Server machine:
    a. Log in as the oracle user.
    b. Change directories to $ORACLE_HOME/network/admin
    c. Make a backup of the file tnsnames.ora.
    d. Open the file tnsnames.ora for editing.
    e. If the Sentinel Database is on the Crystal Server machine, then there should already be an entry in the tnsnames.ora file to the Sentinel Database. For example, if the Sentinel Database is named ESEC, then an entry similar to the following will exist:

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

    f. If the Sentinel Database is not on the Crystal Server machine, open the tnsnames.ora file on the Sentinel Database machine to find the entry described above.
    g. Make a copy of that entire entry and paste it at the bottom of the tnsnames.ora file on the Crystal Server machine. The Service Name part of the entry must be renamed to “esecuritydb”. For example, when the entry above is copied and renamed properly, it will look like:

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

h. Make sure the HOST part of the entry is correct (e.g. – make sure it is not set to localhost if the Crystal Server and Sentinel Database are on different machines).
i. Save the changes to the tnsnames.ora file.
j. Execute the following command to check that the esecuritydb Service Name is configured properly:

```
tnsping esecuritydb
```

k. If the command executed successfully, you should get a message saying the connection is OK.

Installing Crystal BusinessObjects Enterprise™ 11

Installing Crystal BusinessObjects Enterprise

1. Log in as crystal user.
2. Change directories into DISK_1 of the Crystal installer.
3. Execute:

```
./winstall
```

4. Select Language: English
5. Select New Installation
6. Accept License Agreement
7. Enter Product Keycode
8. Enter install directory:

```
/opt/crystal_xi
```

9. Select: User install
10. Select: New Install
11. Select: Install MySQL
12. Enter configuration information for MySQL:
    a. Use default port 3306
    b. Admin password
13. Enter more configuration information for MySQL:
    a. Default DB Name: BOE11
    b. User id: mysqladm
    c. Password
14. Enter more configuration information for MySQL:
    a. Local Name Server: <local machine's hostname>
    b. Default CMS Port Number: 6400
15. Select: Install Tomcat
16. Enter Tomcat configuration information:
    a. Default Receive HTTP requests port: 8080
    b. Default Redirect jsp requests port: 8443
    c. Default Shutdown Hook port: 8005
17. Press Enter to start installation

Patching Crystal Reports for use with Sentinel

In order to view Crystal Reports from the Sentinel Control Center's Analysis tab, several Crystal Enterprise files need to be updated to make them compatible with the browser that is embedded in Sentinel.

The following table lists those files and describes what each file is used for.

File Name	***Description***

`calendar.js`
 	
`calendar.html`
	Displays a popup calendar when you are selecting a date as a parameter to a report.

`grouptree.html`	Displays the Loading... message while reports are loading.
`exportframe.html`	Displays the window that allows you to export a report for saving or for printing.
`exportIce.html`	File used by Sentinel when exporting a report for saving or for printing.
`GetReports.jsp`	File used by Sentinel Control Center to establish a connection with Crystal Server and display the report list.

Patching Crystal Reports

1. THIS IS NOW ONLY AVAILABLE FROM SERVICE PACK. On the Sentinel Service Pack CD-ROM, go to \content\reports\patch and copy all *.html and *.js files to the viewer file location, default is:

   ```
   /opt/crystal_xi/bobje/webcontent/enterprise11/viewe
      r/en/
   ```

2. On the Sentinel Service Pack CD-ROM, go to \content\reports\patch and copy all *.jsp files to:

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

   NOTE: create a folder called **esec-script**

3. `Copy all *.jar files`

   From:
   `/opt/crystal_xi/bobje/tomcat/webapps/jsfadmin/WEB-INF/lib/`

   To:
   `/opt/crystal_xi/bobje/tomcat/webapps/esec-script/WEB-INF/lib`

   NOTE: create a folder structure **WEB-INF/lib**

Publishing Crystal Report Templates

These report templates are created by e-Security for use in the Sentinel Control Center Analysis and Advisor tab.

There are two methods of publishing reports.

- Crystal Publishing Wizard
- Crystal Reports Central Management Console

Also provided are example reports in pdf format.

> **NOTE**: List of Attacks by CVE Report is an intersection of attack signatures from the Advisor feed and scanned vulnerabilities.

> **NOTE**: 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 Sentinel User's Guide, Chapter 10 – Sentinel Data Manager, section Reporting Data Tab or go to section Enabling Sentinel Top 10 Reports.

Publishing Report Templates – Crystal Publishing Wizard

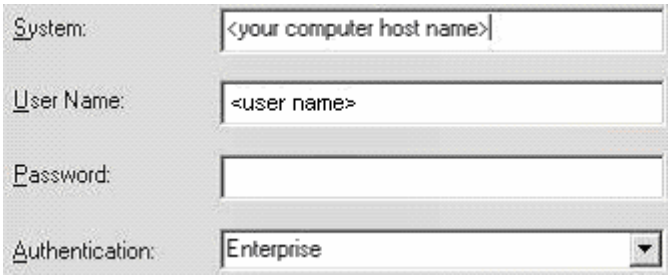
> **NOTE**: A Windows platform is required to run Crystal Publishing Wizard.

Importing Crystal Report Templates

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

1. Click Start > All Programs > BusinessObjects 11 > Crystal Reports Server > Publishing Wizard.
2. Click Next.
3. 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. Enter your password and click Next.

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

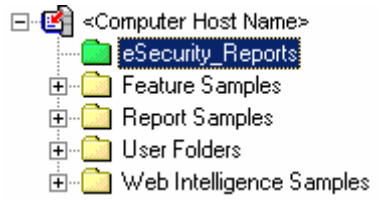


4. Click the 'Add Folder' button.
5. Click the 'Include Subfolder' check box. Go to the Sentinel Service Pack CD-ROM and navigate to:

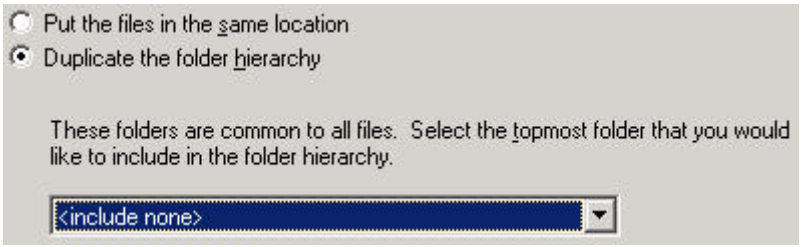
   `content\reports\Crystal_v11\Oracle`

Click OK.

6. Click Next.
7. In the Specify Location window, click the New Folder button (upper right corner) and create a folder called eSecurity_Reports. Click Next.



8. Select:
   - 'Duplicate the folder hierarchy' radio button.
   - Click the down arrow and select '<include none>'



Click Next.

9. In the Confirm Location window, click Next.
10. In the Specify Categories window:
    - a category name of choice (such as esecurity)
    - high-light the name and click the + button

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

    - click Next.

11. In the Specify Schedule window, click 'Let users update the object' (this should be default) radio button. Click Next.
12. In the Specify Repository Refresh window, click Enable All to enable repository refresh. Click Next.
13. In the Specify Keep Saved Data window, click Enable All to keep saved data when publishing reports. Click Next.
14. In the Change Defaults Values window, click 'Publish reports without modifying properties' radio button (this should be default). Click Next.
15. Click Next to add your objects.
16. Click Next.
17. Click Finish.

When the e-Security templates for Crystal Reports are published to the Crystal Enterprise server, the templates must reside within the e-Security directory.

Publishing Report Templates – Central Management Console

When publishing reports using the Central Management Console, the report cannot be batch published such as when using the Windows driven Publishing Wizard.

Importing Crystal Report Templates

1. Open a web browser and enter the following url:

   ```
   http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/businessobjects/enterprise11/adminlaunch
   ```

2. Click Central Management Console
3. Login to your Crystal Server.
4. Under the Organize pane, click Folders.
5. In the upper right-hand corner, click on ‘new Folder…’.
6. Create a folder called eSecurity_Reports. Click OK.
7. Click on eSecurity_Reports.
8. Click the Subfolders tab and create the following subfolders.
   - Advisor_Vulnerability
   - Incident Management
   - Internal Events
   - Security Events
   - Top 10
9. Click Home.
10. Click ‘Objects’.
11. Click ‘New Object’.
12. On left side of the page, high light Report.
13. Click the Browse button and browse to the Sentinel Service Pack CD:

    ```
    content\reports\Crystal_v11\Oracle
    ```

    Pick a folder and select a report.
14. High light eSecurity_Reports, click ‘Show Subfolders’.
15. Select the appropriate folder for the report, click ‘Show Subfolders’.
16. Click OK.
17. Click Update.
18. Click the Reports tab, and continue adding Reports.
19. To add the remaining reports to another folder, click Folders (upper left hand corner) and repeat steps 14 to 17.

Using the Crystal XI Web Server

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

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

```
http://<hostname_or_IP_of_web_server>:<web_server_p
   ort_default_8080>/businessobjects/enterprise11/ad
   minlaunch
```

The non-administrative (general use) portal is accessed through your browser at the following URL:

```
http://<hostname_or_IP_of_web_server>:<web_server_p
   ort_default_8080>/businessobjects/enterprise11
```

Testing connectivity to the web server

Testing connectivity to the web server

1. Go to another machine that is on the same network as your webserver.
2. Enter

```
http://<hostname_or_IP_of_web_server>:<web_server_p
   ort_default_8080>/businessobjects/enterprise11/ad
   minlaunch
```

3. You should get a Crystal BusinessObjects Web page.

Setting a ‘Named User’ Account

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

Setting the Guest Account as ‘Named User’

1. Open a web browser and enter the following url:

```
http://<hostname_or_IP_of_web_server>:<web_server_p
   ort_default_8080>/businessobjects/enterprise11/ad
   minlaunch
```

2. Click Central Management Console.
3. The System Name should be your host computer name. Authentication Type should be Enterprise. If not, choose Enterprise.
4. In the Organize pane, click Users.
5. Click Guest.
6. Change connection type from ‘Concurrent User’ to ‘Named User’.
7. Click Update.
8. Logoff and close window.

Configuring Reports

This procedure discusses how to configure Administration Launchpad to allow you to view and modify reports.

Configuring Administration Launchpad

1. Open a web browser and enter the following url:

```
http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/businessobjects/enterprise11/adminlaunch
```

2. Click Central Management Console.
3. The System Name should be your host computer name. Authentication Type should be Enterprise. If not, choose Enterprise.
4. Enter your user name, password and click Log On.
5. In the Organize pane, click on Folders.
6. Single-click eSecurity_Reports.
7. Select All.
8. Click the Rights tab.
9. For Everyone, in the drop-down menu to the right select View on Demand. Click Update.
10. Logoff and close the window.

Enabling Sentinel Top 10 Reports

To enable Sentinel Top 10 Reports, you have to:

- Turn on Aggregation
- Enable EventFileRedirectService

Turning on Aggregation (aggregation)

1. Start Sentinel Data Manager.
2. Login.
3. Click the Reporting Data tab.
4. Enable the following summaries
   - EventDestSummary
   - EventSevSummary
   - EventSrcSummary

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

Enabling EventFileRedirectService (EventFileRedirestService)

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

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

2. For EventFileRedirectService, change the status to on.

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

3. Restart the DAS_Binary process. This can be done by using Sentinel Control Center or by rebooting the machine.

Using Sentinel Control Center:

- Log into Sentinel Control Center as a user with administrator rights. This user must have the following “Server Views” permissions:
  - View Servers
  - Control Servers
- From the Admin tab, open a Server View to view all Sentinel Server Processes.
- Right click on the DAS_Binary process and select the Restart action.
- The “Starts” count for that process will increase by one if the process is restarted successfully.

Maximizing Event Reporting

Depending on the number of events that Crystal is querying, you may get an error on maximum processing time or maximum record limit. To set your server to process a higher number or an unlimited number or reports you will need to reconfigure the Crystal Page Server.

Reconfiguring the Crystal Page Server

1. Open a web browser and enter the following url:

   ```
   http://<hostname_or_IP_of_web_server>:<web_server_port_default_8080>/businessobjects/enterprise11/adminlaunch
   ```

2. Click Central Management Console.
3. The System Name should be your host computer name. Authentication Type should be Enterprise. If not, choose Enterprise.
4. Enter your user name, password and click Log On.
5. Click Servers.
6. Click <server name>.pageserver
7. Under ‘Database Records to Read When Previewing Or Refreshing a report’, click the ‘Unlimited records’ radio button.
8. Click Apply.
9. A prompt to restart the page server will appear, click OK.
10. You may be prompted for a logon name and password to access the operating system service manager.

Configuring Sentinel to the Crystal Enterprise Server

After Crystal Enterprise is installed, the Sentinel Control Center needs to have the URLs for the Analysis reports.

Configuring Sentinel to the Crystal Enterprise Server

1. At the Sentinel Control Center, login as user esecadm.
2. Click the Admin tab.
3. Click on General Options in the navigator tree.
4. Click Modify.

5. In the Analysis URL field, enter 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 Enterprise Server.
>
> **NOTE**: URL 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 the refresh button next to the Analysis field.
5. Click the refresh button next to the Advisor field.
6. Click Save.
7. Logout and log back in to view the reports on the Analysis tabs.

Utilities and Troubleshooting

Starting MySQL

To make sure MySQL is running:

1. Login as crystal user
2. cd /opt/crystal_xi/bobje
3. ./mysqlstartup.sh

Starting Tomcat

To make sure Tomcat is running:

1. Login as crystal user
2. cd /opt/crystal_xi/bobje
3. ./tomcatstartup.sh

Starting Crystal Servers

To make sure crystal servers are running:

1. Login as crystal user
2. cd /opt/crystal_xi/bobje
3. ./startservers

Crystal Host Name Error

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. Example:

```
172.16.9.46      dev-linux02
```

Cannot Connect to CMS

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

Troubleshooting CMS connection failure

1. If the command “netstat –an | grep 6400” does not return any results, try the following:
   - Re-enter MySQL connection information:

   a. Login as crystal user
   b. cd /opt/crystal_xi/bobje
   c. ./cmsdbsetup.sh
   d. Hit Enter when “[<hostname>.cms]” appears
   e. Choose “select” and re-enter all your MySQL DB info that was entered during install time (refer to install instructions).
   f. When done, quit cmsdbsetup.sh
   g. ./stopservers
   h. ./startservers

   - Re-initialize MySQL DB:

   a. Login as crystal user
   b. cd /opt/crystal_xi/bobje
   c. ./cmsdbsetup.sh
   d. Hit Enter when “[<hostname>.cms]” appears
   e. Choose “reinitialize” and follow instructions.
   f. When done, quit cmsdbsetup.sh
   g. ./stopservers
   h. ./startservers
2. Make sure all CCM servers are enabled:
   a. Login as crystal user
   b. cd /opt/crystal_xi/bobje
   c. ./ccm.sh -enable all

Chapter 10 – Advisor Configuration

e-Security Advisor, powered by SecurityNexus, provides real-time intelligence into enterprise vulnerabilities, expert advice and recommended steps toward remediation. Advisor provides a cross-reference between real-time IDS attack signatures and Advisor's knowledge base of vulnerabilities. Visit http://www.esecurity.net/Software/Products/Advisor.asp to find out more information.

Crystal BusinessObjects Enterprise™ 11 is one of the reporting tools that integrates with Sentinel. This chapter discusses how to configure Advisor to run Crystal Reports for Sentinel.

Installing Advisor is optional, however, it is a necessary component if you wish to use the exploit detection feature associated with Sentinel. If you are going to use Advisor for Exploit Detection only, you do not need to install a Crystal Server. A Crystal Server is only required if you intend to run reports.

These steps, under Windows 2003 Server, use the Crystal Publishing Wizard to import the standard set of Crystal Reports templates. These report templates are created by e-Security for use for reporting and analysis and appear in the Sentinel Control Center's Advisor tab.

For Crystal BusinessObjects Enterprise™ 11 installation information, see the 'Crystal Reports' chapter.

Installation of Advisor

Advisor can only be installed on the same machine where your Database Access Service (DAS) resides.

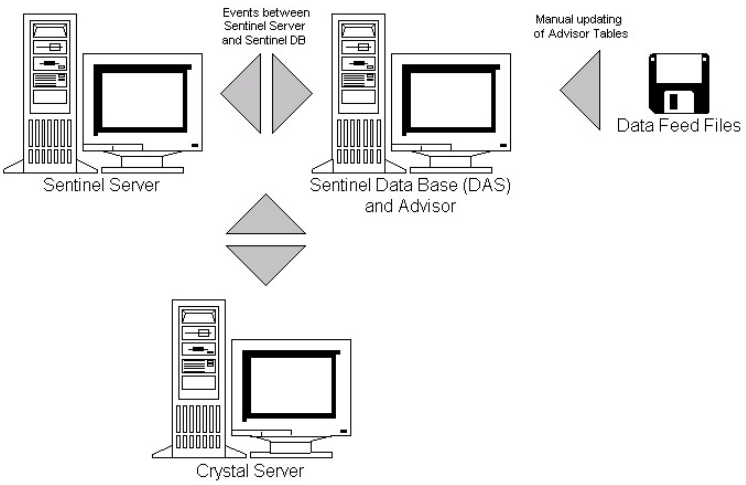
There are two different install options available. They are:

- Standalone
- Direct Internet Download

If you wish to run Advisor Crystal Reports, first see the Crystal Reports Chapter on installing and configuring your Crystal Server. Then, you must publish your Advisor Crystal Reports. See Crystal Report Templates for instructions on publishing your reports.

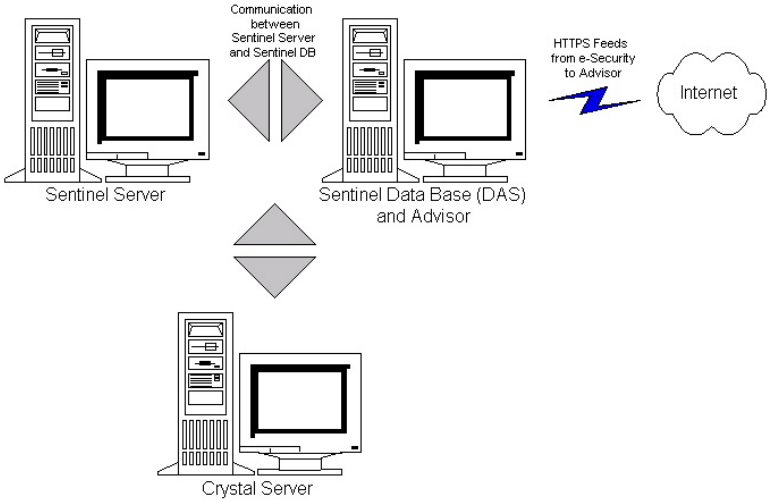
Standalone Configuration

Standalone installation is where Advisor is an isolated system that requires a manual intervention to receive an update from e-Security.



Direct Internet Download Configuration

Direct Internet Download is where the Advisor machine is directly connected to the Internet. In this configuration, updates from e-Security are automatically downloaded from e-Security over the Internet on a regular schedule.



Advisor Installation

NOTE: Prior to installing Advisor, ensure that you have the Advisor username and password given to you by e-Security. During install you will be prompted for the username and password.

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

- If not done already, perform the following (see Crystal Reports Chapter):
  - Install Microsoft Internet Information Server (IIS)
  - Install Crystal BusinessObjects Enterprise™ 11
  - **For Oracle (LINUX)** - Pre-Install of Crystal BusinessObjects Enterprise
  - **For Oracle (Solaris)** - Configure Oracle native driver (for Oracle installations)

  - **For MS SQL (Windows)** - Configure Open Database Connectivity (ODBC)
  - Patch Crystal Reports (patches) – See the 'Crystal Reports' chapter.
- Install Advisor – if Advisor is not already installed, see 'Adding Components to an Existing Installation' chapter.
- Import Crystal Report Templates
- Create a Crystal Web Page
- Configure Sentinel to the Crystal Enterprise Server

Importing Report Templates

Depending upon your operating system refer to:

- Chapter 8 – Crystal Reports for Windows and Solaris
- Chapter 9 - Crystal Reports for Linux

Configuring Administration Launchpad

Depending upon your operating system refer to:

- Chapter 8 – Crystal Reports for Windows and Solaris
- Chapter 9 - Crystal Reports for Linux

Setting Advisor Option in Sentinel

Advisor Configuration (configuring Sentinel to the Crystal Enterprise Server)

1. Log into Sentinel Control Center using your username and password. Only one admin user per Sentinel server will be able to do the following:
2. On the Admin tab, select General Options
3. Click Modify and enter the following the Advisor URL field:

   For Crystal XI on Linux):

   ```
   http://<hostname_or_IP_of_web_server>:<web_server_port_
      default_8080>/esec-
      script/GetReports.jsp?APS=<hostname_or_IP_of_web_serv
      er>&user=Guest&password=&tab=Advisor
   ```

   NOTE: <hostname_or_IP_of_web_server> must be replaced with the IP address or hostname of the Crystal Enterprise Server (appears twice in URL). <web_server_port_default_8080> must be replaced with the port the Crystal web server is listening on.
4. Click the Refresh button and wait until it turns green. Click Save.
5. Logout and log back in to the Sentinel Control Center and click on the Advisor tab. The report tree should appear on the Navigator window.

Updating Data in Advisor Tables

Unless you have a standalone configuration, the data in the advisor tables will automatically be updated during the next scheduled Advisor feed download. However, the data can also be manually updated. To update manually, see the e-Security Sentinel User's Guide.

Resetting Advisor password (Direct Download Only)

If you are running Advisor in Direct Download mode and you've obtained a new Advisor password or the Advisor password you set during installation was incorrect, you will need to reset your encrypted Advisor password stored in Advisor's configuration file.

Updating the encrypted Advisor password is not applicable if you are running Advisor in a Standalone configuration because, in this mode, a password is not stored in the Advisor configuration file.

To reset your encrypted Advisor password stored in Advisor's configuration file, perform the following steps:

1. For UNIX login as esecadm or for Windows login with administrative rights. Log into the machine where Advisor is installed.
2. Change directories to:

   For UNIX:

   ```
   $ESEC_HOME/sentinel/bin
   ```

   For Windows:

   ```
   %ESEC_HOME%\sentinel\bin
   ```

3. Enter the following commands:

   For UNIX:

   ```
   ./adv_change_passwd.sh <newpassword>
   ```

   For Windows:

   ```
   adv_change_passwd.bat <newpassword>
   ```

Chapter 11 – Testing the Installation

The following test Agents are installed with the Agent Service (Agent Manager) component to assist you with testing your installation. The name and description of each of these Agents is:

For testing the basic event flow:

- SendOneEvent – Sends one event through Sentinel and then stops.
- SendMultipleEvents – Sends 20 events through Sentinel and then stops.

For testing event asset mapping and exploit detection:

- DemoEvents – Sends 13 events through Sentinel and then stops.
- DemoAssetUpload – Loads demo asset data into Sentinel. When the DemoEvents Agent is run after running this Agent, then asset data from this Agent will appear in the events from the DemoEvents Agent as a result of event mapping. This agent does not generate any external events.
- DemoVulnerabilityUpload – Loads demo vulnerability data into Sentinel. When the DemoEvents Agent is run after running this Agent as well as after running the Advisor feed download, then a few of the events from the DemoEvents Agent will trigger an exploit detection (i.e. – the Vulnerability field of the event will be set to "1"). This agent does not generate any external events.

For more information (including configuration) on other Agents go to:

```
%ESEC_HOME%\wizard\Elements\<agent name>\docs\
```

Testing the Installation using the Test Agents

In Sentinel v5.1.1.1 and later, the test Agents are installed pre-configured on all Agent Managers. Therefore, if you are using this version of Sentinel, you can go right to running the test Agents to test your installation.

In Sentinel v5.1.1 and earlier, you must manually configure the Agents on an Agent Manager before they can be used. To configure the test Agents, follow the instructions in the section Configuring the Test Agents. Then, return to this section to test your installation using the test Agents.

Running the test Agents to test your installation

1. Open the Sentinel Control Center application.
2. Click on the Agents tab.
3. In the Agent View Manager dialog, double click on the ALL AGENTS view to open a view on all of the Agent ports.
4. The Agent View that appears displays all of the Agent ports that are currently configured, grouped by Agent Manager Name. If you do not see any Agent ports, then this means that none of your Agent Managers are currently connected to Sentinel. If you expect one or more Agent Managers to be connected to Sentinel, then check that your Agent Managers are running and if there are any errors in the Agent Manager or Sentinel Server log files.

5. Before running an Agent, open an Active View so that you can view the events that are generated by the test Agents. To do this:
   - Click on the Active Views tab
   - Select Active Views->Create Active View from the menu bar
   - Select the PUBLIC::External_Events filter
   - Click Finish.
6. To run an Agent to test basic event flow:
   - Go to the Agents tab
   - Right click on the SendMultipleEvents Agent port in the Agent View and select the Start action. Since the test agents only run for a short time and then stop, the Agent port status will turn to “on” briefly and then back to “off”.
   - To verify that events are flowing through your system, go back to the Active Views tab and monitor the Active View you created. Please note that it may take a minute for the event to appear in the Active View after you run the Agent.
7. To run an Agent to test event asset mapping
   - Go to the Agents tab
   - Right click on the DemoAssetUpload Agent port in the Agent View and select the Start action. Since the test agents only run for a short time and then stop, the Agent port status will turn to “on” briefly and then back to “off”.
   - Wait a minute or two for the asset data to load into Sentinel, generated into a map by the Mapping Service, and distributed to the Agent Managers. You’ll know when this has happened by watching for a RefreshingMapFromServer internal event with “Asset” in its event message. To see this internal event, you must use an Active View with a filter that allows internal events to pass (e.g. – PUBLIC::Internal_Events). The PUBLIC::External_Events filter does not allow internal events to pass.
   - Right click on the DemoEvents Agent port in the Agent View and select the Start action. Since the test agents only run for a short time and then stop, the Agent port status will turn to “on” briefly and then back to “off”.
   - To verify that event asset mappings occurred, double click on an event (in the events table at the bottom of the Active View) that was just generated by the DemoEvents Agent to view the event details. In the event details that appear to the left of the events table, expand the Asset group to view the event asset map data. Please note that it may take a minute for the event to appear in the Active View after you run the Agent.
8. To run an Agent to test exploit detection (requires that you have installed the Advisor component):
   - Run the Advisor feed download (this may take a while):

   On Windows:

   ```
   Log into the machine where Advisor is installed.
   ```

```
Run the Advisor Scheduled Task (Start -> Control Panel
   -> Scheduled Tasks -> {e-Security_Advisor | at1})
```

On UNIX:

```
Log into the machine where Advisor is installed as the
   esecadm user

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

- In the Sentinel Control Center, go to the Agents tab
- Right click on the DemoVulnerabilityUpload Agent port in the Agent View and select the Start action. Since the test agents only run for a short time and then stop, the Agent port status will turn to “on” briefly and then back to “off”.
- Wait until the updated exploit detection data has been uploaded to the Agent Manager. You’ll know when this has happened by watching for a RefreshingMapFromServer internal event with “IsExploitWatchlist” in its event message. To see this internal event, you must use an Active View with a filter that allows internal events to pass (e.g. – PUBLIC::Internal_Events). The PUBLIC::External_Events filter does not allow internal events to pass. It could take a little more than a half hour for the updated exploit detection data to be sent to the Agent Manager due to DAS, by default, updating the exploit detection data at most once in 30 minutes.
- Right click on the DemoEvents Agent port in the Agent View and select the Start action. Since the test agents only run for a short time and then stop, the Agent port status will turn to “on” briefly and then back to “off”.
- To verify that exploit detection occurred, double click on an event (in the events table at the bottom of the Active View) that was just generated by the DemoEvents Agent to view the event details. In the event details that appear to the left of the events table, expand the Exploit group to view the exploit detection data. Some of the events should show up with their Vulnerability field set to “1”. Please note that it may take a minute for the event to appear in the Active View after you run the Agent.

Configuring the Test Agents

In Sentinel v5.1.1 and earlier, the test Agents are not pre-configured at install time. Therefore, you must use the Agent Builder (on a Windows machine) to configure the Agents before they can be run.

In Sentinel v5.1.1.1 and later, these configuration steps are not needed unless the test Agent ports were deleted.

Configuring the SendOneEvent Agent

Configuring, uploading and running the Send One Event Agent

1. Open the Agent Builder application.
2. Click the Wizard Hosts tab.

3. Highlight the hostname of your computer. Your hostname will appear in the field below the menu at the top of the application.
4. Double-click new… under the Port Name header.
5. Enter a Wizard Port Name (e.g. - SendOneEvent).
6. For Rx/Tx Type, select None.
7. Leave Rx/Tx Value blank.
8. On the same row, click on the Agent column's drop-down menu and choose SendOneEvent.
9. Click the save button.
10. Click the Agents tab.
11. Expand the SendOneEvent Agent.
12. Right click on the template file SendOneEvent and click Build Scripts.
13. Right click on SendOneEvent Agent and click Upload Agent.
14. Under the Agents tab, you computer should be selected. Click Upload.
15. If prompted, enter the Agent Manager password.
16. Click OK.

Configuring the SendMultipleEvents Agent

Configuring, uploading and running the Send Multiple Events Agent

1. Open the Agent Builder application.
2. Click the Wizard Hosts tab.
3. Highlight the hostname for your computer. Your hostname will appear in the field below the menu at the top of the application.
4. Double-click new… under the Port Name header, enter a Wizard Port Name (e.g. - SendMultipleEvents).
5. On the same row, click on the Rx/Tx Type column's drop-down menu and choose File All.
6. On the same row, click on the Rx/Tx Value column's text box and enter the path to the input file:

   ```
   Elements\SendMultipleEvents\config\test_events.csv
   ```

7. On the same row, click on the Agent column's drop-menu and choose SendMultipleEvents.
8. Click the save button.
9. Click the Agents tab.
10. Expand the SendMultipleEvents Agent.
11. Right click on the template file SendMultipleEvents and click Build Scripts.
12. Right click on SendMultipleEvents Agent and click Upload Agent.
13. Under the Agents tab, you computer should be selected. Click Upload.
14. If prompted, enter the Agent Manager password.
15. Click OK.

Configuring the DemoEvents Agent

Configuring, uploading and running the DemoEvents Agent

1. Open the Agent Builder application.
2. Click the Wizard Hosts tab.
3. Highlight the hostname for your computer. Your hostname will appear in the field below the menu at the top of the application.
4. Double-click new… under the Port Name header, enter a Wizard Port Name (e.g. - DemoEvents).
5. On the same row, click on the Rx/Tx Type column's drop-menu and choose File All.
6. On the same row, click on the Rx/Tx Value column's text box and enter the path to the input file:

   ```
   Elements\DemoEvents\data\Generic_Events.csv
   ```

7. On the same row, click on the Agent column's drop-down menu and choose DemoEvents.
8. Click the Save button.
9. Click the Upload button.
10. Select the Agents tab.
11. Click the down-arrow and select the DemoEvents Agent.
12. Click the Upload button.
13. If prompted, enter the Agent Manager password.
14. Click OK.

Configuring the DemoAssetUpload Agent

Configuring, uploading and running the DemoAssetUpload Agent

1. Open the Agent Builder application.
2. Click the Wizard Hosts tab.
3. Highlight the hostname for your computer. Your hostname will appear in the field below the menu at the top of the application.
4. Double-click new… under the Port Name header, enter a Wizard Port Name (e.g. - DemoAssetUpload).
5. On the same row, click on the Rx/Tx Type column's drop-menu and choose File All.
6. On the same row, click on the Rx/Tx Value column's text box and enter the path to the input file:

   ```
   Elements\DemoAssetUpload\data\asset_info.csv
   ```

7. On the same row, click on the Agent column's drop-menu and choose DemoAssetUpload.
8. Click the Save button.
9. Click the Upload button.
10. Select the Agents tab.

11. Click the down-arrow and select DemoAssetUpload.
12. Click the Upload button.
13. If prompted, enter the Agent Manager password.
14. Click OK.

Configuring the DemoVulnerabiltyUpload Agent

Configuring, uploading and running the DemoVulnerabiltyUpload Agent

1. Open the Agent Builder application.
2. Click the Wizard Hosts tab.
3. Highlight the hostname for your computer. Your hostname will appear in the field below the menu at the top of the application.
4. Double-click new… under the Port Name header, enter a Wizard Port Name (e.g. - DemoVulnerabiltyUpload).
5. On the same row, click on the Rx/Tx Type column's drop-menu and choose File All.
6. On the same row, click on the Rx/Tx Value column's text box and enter the path to the input file:

   ```
   Elements\DemoVulnerabiltyUpload\data\vuln_info.csv
   ```

7. On the same row, click on the Agent column's drop-menu and choose DemoVulnerabiltyUpload.
8. Click the Save button.
9. Click the Upload button.
10. Select the Agents tab.
11. Click the down-arrow and select DemoVulnerabiltyUpload.
12. Click the Upload button.
13. Enter the Agent Manager password.
14. Click OK.

Chapter 12 – Making Changes to the Communication Layer (iSCALE)

The communication layer (iSCALE) connecting all components of the architecture is an encrypted TCP/IP based connection. By default this communication is encrypted using AES 256 bit. ARC4 is available for use.

The keymgr allows you to choose which encryption method to use and allows changing the key. The program generates a file in the lib directory of an e-Security installation ($ESEC_HOME/lib or %ESEC_HOME%\lib) called .keystore. This file must be copied to each machine that has an e-Security component installed.

e-Security recommends as a best practice that the default security key be changed to provide unique encryption and authentication parameters.

> **NOTE**: If you are using Advisor, DBConnector, or RDEP Agent connector, you must update the passwords stored in each of these component's configuration files. This is required because the encryption key used to encrypt the password before it is stored in these configuration files is based on the key in the .keystore file that is updated.

Making Encryption Key Changes

Making key changes or enable other encryption methods

1. For UNIX, login as esecadm. For Windows, login as a user with administrative rights.
2. cd to:

   For Windows:

   ```
   %ESEC_HOME%\lib
   ```

   For UNIX:

   ```
   $ESEC_HOME/lib
   ```

3. Run the following command:

   On Windows:

   ```
   "%ESEC_JAVA_HOME%\java" -jar keymgr.jar -–keyalgo
      <encryption [AES or ARC4]> --keysize 256
   ```

   On UNIX:

   ```
   $ESEC_JAVA_HOME/java -jar keymgr.jar -–keyalgo
      <encryption [AES or ARC4]> --keysize 256
   ```

   This will allow you to set your encryption method. A file called .keystore will be created in the lib directory.
4. Copy .keystore to each machine with an e-Security component installed. The file should be copied to:

   For Windows:

```
%ESEC_HOME%
```

For UNIX:

```
$ESEC_HOME
```

5. If you have the DBConnector or RDEP Agent connector configured on any Agent Manager machine, you must update the passwords in all instances of the connector's configuration file. This is required because the encryption key used to encrypt the password before it is stored in the connector's configuration file is based on the key in the .keystore file that was just updated. For instructions on setting the passwords in the connector configuration files, see the documentation for the DBConnector and RDEP Agent connector.
6. If you are running Advisor in Direct Download mode on your system, you will need to update your encrypted Advisor password stored in Advisor's configuration file. This is required because the encryption key used to encrypt the password before it is stored in Advisor's configuration file is based on the key in the .keystore file that was just updated. Updating the encrypted Advisor password is not applicable if you are running Advisor in a standalone configuration because, in this mode, a password is not stored in the Advisor configuration file. To update your encrypted Advisor password stored in Advisor's configuration file, perform the following steps in the order presented:
   - For UNIX login as esecadm or for Windows login with administrative rights. Log into the machine where Advisor is installed.
   - Change directories to:

   For UNIX:

   ```
   $ESEC_HOME/sentinel/bin
   ```

   For Windows:

   ```
   %ESEC_HOME%\sentinel\bin
   ```

   - Enter the following commands:

   For UNIX:

   ```
   ./adv_change_passwd.sh <newpassword>
   ```

   For Windows:

   ```
   adv_change_passwd.bat <newpassword>
   ```

Chapter 13 – Adding Components to an Existing Installation

Sentinel 5 e-Security Enterprise Security Management installer supports adding e-Security components to an existing installation. An example of adding a component would be if you installed only Wizard Agent Manager on a machine and at some later point you decided you would also like Sentinel Control Center on that machine. In this case, you would add the Sentinel Control Center component to the Wizard Agent Manager installation.

> **NOTE:** Before adding a component, ensure that you have the correct e-Security variables set.
>
> ESEC_HOME
> ESEC_JAVA_HOME
> WORKBENCH_HOME
> ESEC_CONF_FILE
> ESEC_VERSION
> ESEC_USER
> LD_LIBRARY_PATH

Adding Components on Solaris or Linux

Adding Components on Solaris

1. Login as the root user.
2. Insert and mount the Sentinel Install CD.
3. Start the install program by going the install directory on the CD-ROM and enter:

   ```
   ./setup.sh
   ```

   or

   ```
   ./setup.sh –console
   ```
   (if X Windows is not available)
4. A message will be displayed indicating the location of the previous install and which components are already installed. Click Next.
5. Choose which components you would like to add, click Next.
6. Follow the prompts, entering the appropriate information. For more information on a particular prompt, refer to the appropriate install chapter.

Adding Components on Windows

Adding Components on Windows

1. Insert the Sentinel installation CD into the CD-ROM drive.
2. Browse to the CD and double-click setup.bat.

   > **NOTE:** Installing in console mode is not supported on Windows.
3. Click Next on the Welcome screen.

4. Accept the End User License Agreement and click Next.
5. A message will be displayed indicating the location of the previous install and which components are already installed. Click Next.
6. Choose which components you would like to add, then click Next.

NOTE: For Linux, The only components that can be installed on Windows are Agent Builder and Sentinel Control Center.

7. Follow the prompts, entering the appropriate information. For more information on a particular prompt, refer to Chapter 3 (for Solaris) or Chapter 5 (for Windows).

Chapter 14 – Uninstalling the Software

Uninstalling Sentinel, Agent Manager and Advisor

Uninstall for Solaris and Linux

Starting the Sentinel uninstaller for Solaris

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

   ```
   $ESEC_HOME/_uninst
   ```

4. Enter:

   ```
   ./uninstall.bin
   ```

NOTE: On Solaris and Linux, after uninstalling Sentinel Server, you will need to manually remove the user esecadm from the OS, if desired.

Uninstall for Windows

Using the Sentinel Windows Uninstaller

1. Login as an Administrator.
2. Stop the Sentinel Server.
3. Select 'Start > Program Files > e-Security > Uninstall e-Security 5.x'

Follow the screen prompts. Select which applications to uninstall:

- Database
- Communication Server (message bus)
- Advisor
- Base Sentinel Services
- Correlation
- DAS
- Agent Service (Agent Manager)
- Sentinel Control Center
- Sentinel Database Manager (SDM)
- HP OpenView Service Desk
- Remedy Integration

Uninstalling Using Control Panel

To uninstall e-Security Windows applications

1. Click Start > Programs > Settings > Control Panel > Add/Remove Programs
2. Click e-Security 5.x.
3. Follow the prompts. It will prompt you select which application to uninstall. Select which applications you wish to uninstall.

Post-Uninstall

Uninstall leaves a few files on the machine, you will have to manually delete the files after uninstalling Sentinel 5. You may have to delete the $ESEC_HOME or %ESEC_HOME% directory and all sub-directories. For Advisor, you may want to delete your attack and alert folders used for your Advisor data files.

Some files that are left behind are:

- Sentinel log files
- Wizard log files
- DAS log files
- Agent Manager log files

Sometimes after un-installation, system settings remain. Go to Appendix E for procedures on how to manually remove remaining system settings.

Appendix A – Pre-installation Questionnaire

Pre-Install Questions

1. After determining which machine will be your DAS machine and that it meets the necessary OS and hardware requirements:
   a. Get the hostid number of your DAS machine
   b. Contact e-Security and get your license key
2. What is your goal or purpose with using e-Security Sentinel?
   a. Compliance
   b. SEM
   c. Other_____
3. What is the network architecture for the source devices with respect to the security segment where the Sentinel/Wizard hardware is to be located?

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

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

4. What reports do you want out of the system? This is important to ensure that your agents collect the correct data to be passed to the Sentinel database.
   a. _____
   b. _____
   c. _____
   d. _____
   e. _____
   f. _____

5. What source devices you do you want to collect data from (IDS, HIDS, Routers, Firewalls, etc…), 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 e-Security agents to collect and parse? This important to so that Sentinel will provide what you want.

6. 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 installs this is not applicable. However, e-security does not support NIS.
7. What hardware has been allocated for the installation of Sentinel? Is it in accordance with hardware specifications provided in Chapter 1 and 2 of the Installation Guide?
8. What is the required data retention in terms of days? Typically 30 days is good. MS SQL has difficulty over 60 days. Oracle is OK.
9. Based on the data retention information and EPS, what disk size will you be using? Use 500 to 800 bytes/event for sizing estimates.
10. Have you validated e-Security requirements for operation against your configuration as per chapter 1 and 2 of the Installation Guide?
    - OS patch levels
    - Service Patches
    - Hot Fixes, etc.

Appendix B – Pre-Install and Post Install Maintenance for Oracle Database on Solaris

Pre-install Check List

This Oracle Pre-Install Check-off list is intended primarily for distributed installations. However, it can be used for stand-alone installations. If your number of Agent Manager and Correlation Engine instances is above three, please make note of them. This check-off list allows for Agent Manager and Correlation Engine instances for three or less.

For more information, see Chapter 3 – Installing Sentinel 5 for Oracle.

	Configuration Variable			
1.	*Sentinel Version:*			*Today's Date:*
	Operating System			
	▪ Correct OS for DB	□: Yes | □: No	▪ Proper Patch	□: Yes | □: No
	▪ Correct Oracle DB w/ Partitioning	□: Yes | □: No	▪ Proper Patch	□: Yes | □: No
	▫ Version		▫ Patch level	
	▪ Copy of Oracle Note: 148673.1	□: Yes | □: No		
	▪ Correct environment variables set for Oracle OS user.	□: Yes | □: No		
	▪ Correct OS for Sentinel Components	□: Yes | □: No	▪ Proper Patch	□: Yes | □: No
2.	*DAS Machine*			
	▪ Host ID			
	▪ serial number			
	▪ license key			
3.	*DAS Install*			
	▪ DB hostname or IP			Default: ESEC
	▪ Database name			Default: 1521
	▪ Database port			
	▪ JDBC file location			
4.	*UNIX Kernel Values for Oracle. Below are min values.*			
	▪ shminfo_shmmax	4294967295	□: Yes | □: No	Value if higher:
	▪ shminfo_shmmin	1	□: Yes | □: No	Value if higher:
	▪ shminfo_shmseg	50	□: Yes | □: No	Value if higher:
	▪ shminfo_shmmni	400	□: Yes | □: No	Value if higher:
	▪ seminfo_semmns	14000	□: Yes | □: No	Value if higher:

	Configuration Variable		
	▪ seminfo_semmni	1024 □: Yes | □: No	Value if higher:
	▪ seminfo_semmsl	1024 □: Yes | □: No	Value if higher:
	▪ seminfo_shmopm	100 □: Yes | □: No	Value if higher:
	▪ seminfo_shmvmx	32767 □: Yes | □: No	Value if higher:
5.	*Database Instance (SID)*		
6.	*Database Name*		
7.	*Sentinel Components:*		
	▪ Sentinel Database (IP or DNS)		OS: Patch:
	▫ DB install log		
	▫ Oracle Memory(RAM)		
	▫ Instance Name		
	▫ Listener Port	Default: 1521	
	▫ SYS password		
	▫ SYSTEM password		
	▪ Communication Server (iSCALE) (IP or DNS)		OS: Patch:
	▪ Base Sentinel Services (IP or DNS)		OS: Patch:
	▪ DAS/Advisor (IP or DNS) (Advisor is optional)		OS: Patch:
	▫ DAS RAM		
	▪ Correlation Engine (IP and OS)		
		IP:	OS:
		IP:	OS:
		IP:	OS:
	▪ Crystal Server (IP or DNS)		
	▫ MS SQL (Optional, but recommended)	MS SQL Version: MS SQL Patch: sa password or holder or password:	
	▪ Agent Builder (IP or DNS) (recommend one install)		
	▪ Agent Manager (Agent Services)	**NOTE**: Agent Manager can be set without a password.	
	▫ IP: ▫ IP: ▫ IP:	PW: PW: PW:	OS: OS: OS:
8.	*Advisor (optional)*		
	▪ Data feed file location		

	Configuration Variable		
	▪ Advisor from address		
	▪ Advisor to address		
	▪ Username and password	u/n:	PW:
9.	*Database file locations:*		
	▪ Data files		
	▪ Index files		
	▪ Summary data files		
	▪ Summary index files		
	▪ Temporary and Undo Tablespace files		
	▪ Redo Log Member A directory		
	▪ Redo Log Member A directory		
10.	*Database size:*		
	▪ Standard (20GB)		
	▪ Large (400GB)		
	▪ Custom (size)		
11.	*SMTP Server (DNS or IP)*		
12.	*User passwords*		
	▪ esecadm	PW:	
	▫ Home directory		Default: /export/home
	▪ esecapp	PW:	
	▪ esecdba	PW:	
	▪ esecrpt	PW:	

Post Install Maintenance

There are some utilities available that you to periodically perform maintenance on your database. These utilities include:

- Analyze Partitions – gathers partition statistics for partitions that have recently been populated.
- Analyze Tables – gathers global table statistics for the events and correlated events tables.
- Database Health Check – gathers database information. It reports:
  - Checks if database instance is up
  - Checks if Oracle Listener is up
  - Displays space usage
  - Checks for unusable indexes
  - Checks for invalidate database objects
  - Checks for database analyze

For more information, see ***Chapter 2 – 'Best Practices'***, section 'Maintenance Best Practices'.

An application called Sentinel Data Manager is provided with Sentinel. Use this application to perform database management. For more information, see ***Sentinel User's Guide, Chapter 10 – 'Sentinel Data Manager'***.

Appendix C – Pre-Install and Post Install Maintenance for Oracle Database on Linux

Pre-install Check List

This Oracle Pre-Install Check-off list is intended primarily for distributed installations. However, it can be used for stand-alone installations. If your number of Agent Manager and Correlation Engine instances is above three, please make note of them. This check-off list allows for Agent Manager and Correlation Engine instances for three or less.

For more information, see Chapter 3 – Installing Sentinel 5 for Oracle.

	Configuration Variable			
1.	*Sentinel Version:*			*Today's Date:*
	Operating System			
	▪ Correct OS for DB	□: Yes | □: No	▪ Proper Patch	□: Yes | □: No
	▫ Version		▫ Patch Level	
	▪ Correct Oracle DB w/ Partitioning	□: Yes | □: No	▪ Proper Patch	□: Yes | □: No
	▫ Version		▫ Patch level	
	▪ Correct environment variables set for Oracle OS user.	□: Yes | □: No		
	▪ Startup Scripts (DB machine)	□: Yes | □: No		
	▪ Processes (DB machine)	□: Yes | □: No		
	▪ Sockets	□: Yes | □: No		
	▪ Correct OS for Sentinel Components	□: Yes | □: No	▪ Proper Patch	□: Yes | □: No
2.	*DAS Machine*			
	▪ Host ID			
	▪ serial number			
	▪ license key			
3.	*DAS Install*			
	▪ DB hostname or IP			
	▪ Database name			Default: ESEC
	▪ Database port			Default: 1521
	▪ JDBC file location			
4.	*UNIX Kernel Values for Oracle. Below are min values.*			
	▪ shmmax	2147483648	□: Yes | □: No	Value if higher:
	▪ shmmin	1	□: Yes | □: No	Value if higher:
	▪ shmseg	4096	□: Yes | □: No	Value if higher:

	Configuration Variable			
	▪ shmmni	400	□: Yes | □: No	Value if higher:
	▪ semmns	500	□: Yes | □: No	Value if higher:
	▪ semmni	1024	□: Yes | □: No	Value if higher:
	▪ semmsl	1024	□: Yes | □: No	Value if higher:
	▪ shmopm	100	□: Yes | □: No	Value if higher:
	▪ shmvmx	32767	□: Yes | □: No	Value if higher:
5.	*Database Instance (SID)*			
6.	*Database Name*			
7.	*Sentinel Components:*			
	▪ Sentinel Database (IP or DNS)			OS: Patch:
	▫ DB install log			
	▫ Oracle Memory(RAM)			
	▫ Instance Name			
	▫ Listener Port		Default: 1521	
	▫ SYS password			
	▫ SYSTEM password			
	▪ Communication Server (iSCALE) (IP or DNS)			OS: Patch:
	▪ Base Sentinel Services (IP or DNS)			OS: Patch:
	▪ DAS/Advisor (IP or DNS) (Advisor is optional)			OS: Patch:
	▫ DAS RAM			
	▪ Correlation Engine (IP and OS)			
		▫ IP:		OS:
		▫ IP:		OS:
		▫ IP:		OS:
	▪ Crystal Server (IP or DNS)			
	▫ MS SQL (Optional, but recommended)	MS SQL Version: MS SQL Patch: sa password or holder or password:		
	▪ Agent Builder (IP or DNS) (recommend one install)			
	▪ Agent Manager (Agent Services)	**NOTE**: Agent Manager can be set without a password.		
	▫ IP:	u/n:	PW:	OS:

	Configuration Variable			
	▫IP: ▫IP:	u/n: u/n:	PW: PW:	OS: OS:
8.	*Advisor (optional)*			
	▪ Data feed file location			
	▪ Advisor from address			
	▪ Advisor to address			
	▪ Username and password	u/n:		PW:
9.	*Database file locations:*			
	▪ Data files			
	▪ Index files			
	▪ Summary data files			
	▪ Summary index files			
	▪ Temporary and Undo Tablespace files			
	▪ Redo Log Member A directory			
	▪ Redo Log Member A directory			
10.	*Database size:*			
	▪ Standard (20GB)			
	▪ Large (400GB)			
	▪ Custom (size)			
11.	*SMTP Server (DNS or IP)*			
12.	*User passwords*			
	▪ esecadm	PW:		
	▫Home directory			Default: /export/home
	▪ esecapp	PW:		
	▪ esecdba	PW:		
	▪ esecrpt	PW:		

Post Install Maintenance

There are some utilities available that you to periodically perform maintenance on your database. These utilities include:

- Analyze Partitions – gathers partition statistics for partitions that have recently been populated.
- Analyze Tables – gathers global table statistics for the events and correlated events tables.
- Database Health Check – gathers database information. It reports:
  - Checks if database instance is up
  - Checks if Oracle Listener is up
  - Displays space usage
  - Checks for unusable indexes
  - Checks for invalidate database objects
  - Checks for database analyze

For more information, see ***Chapter 2 – 'Best Practices'***, section 'Maintenance Best Practices'.

An application called Sentinel Data Manager is provided with Sentinel. Use this application to perform database management. For more information, see ***Sentinel User's Guide, Chapter 10 – 'Sentinel Data Manager'***.

Appendix D – Pre-Install and Post Install Maintenance for MS SQL Database on Windows

Pre-install Check List

This MS SQL Pre-Install Check-off list is intended primarily for distributed installations. However, it can be used for stand-alone installations. If your number of Agent Manager and Correlation Engine instances is above three, please make note of them. This check-off list allows for Agent Manager and Correlation Engine instances for three or less.

For more information, see Chapter 4 – Installing Sentinel 5 for MS SQL.

	Configuration Variable			
1.	*Sentinel Version:*			*Today's Date:*
	Operating System			
	▪ Correct OS for DB	□: Yes | □: No	▪ Proper Patch	□: Yes | □: No
	▪ Correct SQL DB	□: Yes | □: No	▪ Proper Patch	□: Yes | □: No
	▫ Version		▫ Patch level	
	▪ Correct OS for Sentinel Components	□: Yes | □: No	▪ Proper Patch	□: Yes | □: No
2.	*For DAS installation under Windows Domain account, assign 'Log on as service'*	□: Yes | □: No		
3.	*DAS Machine*			
	▪ Host ID			
	▪ serial number			
	▪ license key			
4.	*Database Host name or IP:*	*<hostname>[\<Instance Name>]*		
5.	*Database Name:*			Default: ESEC
6.	*Port:*		Default: 1433	
7.	*SQL Install*	□: mixed □: non-mixed		
8.	*SQL server sa password or holder of password.*	PW:		
9.	*Sentinel Components:*			
	▪ Sentinel Database (IP or DNS)			OS: Patch:
	▪ Communication Server (iSCALE) (IP or DNS)			OS: Patch:
	▪ Base Sentinel Services (IP or DNS)			OS: Patch:
	▪ DAS/Advisor (IP or DNS) (Advisor is optional)			OS: Patch:

	Configuration Variable		
	▪ Correlation Engine (IP and OS)		
		IP:	OS:
		IP:	OS:
		IP:	OS:
	▪ Crystal Server (IP or DNS)		OS: Patch:
	▫ MS SQL (Optional, but recommended)	MS SQL Version: MS SQL Patch: sa password or holder of password:	
	▪ Agent Builder (IP or DNS) (recommend one install)		
	▪ Agent Manager (Agent Services passwords w/ IP or DNS and OS)	**NOTE**: Agent Manager can be set without a password.	
	▫IP: ▫IP: ▫IP:	PW: PW: PW:	OS: OS: OS:
10.	*Advisor (optional)*		
	▪ Data feed file location		
	▪ Advisor from address		
	▪ Advisor to address		
	▪ Username and password	u/n:	PW:
11.	*Database file locations:*		
	▪ Data files		
	▪ Index files		
	▪ Summary data files		
	▪ Summary index files		
	▪ Log files		
12.	*Database size:*		
	▪ Standard (20GB)		
	▪ Large (400GB)		
	▪ Custom (size)		
13.	*SMTP Server (DNS or IP)*		
14.	*For SQL Authentication (passwords)*		
	▪ esecadm	PW:	
	▪ esecapp	PW:	
	▪ esecdba	PW:	
	▪ esecrpt	PW:	
15.	*For Windows Authentication (passwords)*		

	Configuration Variable		
	▪ DBA (login)	u/n:	
	▪ Application user (login and password)	u/n:	PW:
	▪ e-Security Administrator (login)	u/n:	
	▪ e-Security Reporting user (login)	u/n:	

Post Install Maintenance

The Windows operating system allows you automatically archive data and add partitions. For more information, see Chapter 2 – 'Best Practices', section 'Automatically Archiving Data and Adding Partitions'.

Appendix E – Manual Cleanup of Previous Installations

When performing a clean installation of e-Security, it is HIGHLY recommended that you perform all of the following steps to make sure there are no files or system settings remaining from a previous installation of e-Security that could cause the new clean installation to fail. Perform the following steps for every machine you are performing a clean installation on BEFORE executing the installer.

> **CAUTION**: 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.

Solaris

Manual Cleanup of e-Security on Solaris

1. Login as root.
2. Make sure that all e-Security processes are not running.
3. Remove contents of /opt/esecurityXX (or wherever the e-Security software was installed)
4. Remove the following files in the /etc/rc3.d directory:
   - S98sentinel
   - S99wizard
   - S99esyslogserver (v5.1.1.1)
   - S99esdee (if SDEE connector is installed)
5. Remove the following files in the /etc/rc0.d directory:
   - K01wizard
   - K02sentinel
   - K01esdee (if SDEE connector is installed)
   - K01esyslogserver (v5.1.1.1)
6. Remove the following files in the /etc/init.d directory:
   - sentinel
   - wizard
   - esdee (if SDEE connector is installed)
   - esyslogserver (v5.1.1.1)
7. Remove the following files from /usr/local/bin:
   - restart_wizard.sh
   - stop_wizard.sh
   - start_wizard.sh
8. Clean up installshield references in /var/sadm/pkg. 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)

9. Remove the esecadm user (and home dir) and esec group (make sure no one is logged in as the esecadm user before performing this step)
   - Run: userdel -r esecadm
   - Run: groupdel esec
10. Remove Installshield section of /etc/profile, /etc/.login
11. Remove the /InstallShield directory, if one exists.
12. Remove the e-Security Oracle database by following the instructions in the section “Manual Cleanup of e-Security Oracle database on Solaris”.
13. Restart the operating system.

Manual Cleanup of e-Security Oracle database on Solaris

1. As oracle user, stop Oracle Listener:
   - Run: lsnrctl stop
2. Stop e-Security database:
   - Change to the Oracle user
   - Set the ORACLE_SID environment variable to the name of your e-Security database instance (usually ESEC).
   - Run: sqlplus '/ as sysdba'
   - At sqlplus prompt, run: shutdown immediate
3. Remove entry for e-Security database in the file /var/opt/oracle/oratab
4. Remove init<your_instance_name>.ora (usually initESEC.ora) file from the directory $ORACLE_HOME/dbs.
5. Remove entries for your e-Security database from the following files in the $ORACLE_HOME/network/admin directory:
   - tnsnames.ora
   - listener.ora
6. Delete the database data files from the location you chose to install them.

Linux

Manual Cleanup of e-Security on Linux

1. Login as root.
2. Make sure that all e-Security processes are not running.
3. Remove contents of /opt/esecurityXX (or wherever the e-Security software was installed)
4. Remove the following files in the /etc/rc5.d directory:
   - S98sentinel
   - S99wizard
   - S99esyslogserver (v5.1.1.1)
   - S99esdee (if SDEE connector is installed)
5. Remove the following files in the /etc/rc3.d directory:
   - S98sentinel
   - S99wizard

- S99esyslogserver (v5.1.1.1)
- S99esdee (if SDEE connector is installed)

6. Remove the following files in the /etc/rc0.d directory:
   - K01esyslogserver (v5.1.1.1)
   - K01wizard
   - K02sentinel
   - K01esdee (if SDEE connector is installed)
7. Remove the following files in the /etc/init.d directory:
   - sentinel
   - wizard
   - esyslogserver (v5.1.1.1)
   - esdee (if SDEE connector is installed)
8. Remove the following files from /usr/local/bin:
   - restart_wizard.sh
   - stop_wizard.sh
   - start_wizard.sh
9. Remove the directory /root/InstallShield
10. Remove the file /root/vpd.properties
11. Remove the esecadm user (and home dir) and esec group (make sure no one is logged in as the esecadm user before performing this step)
    - Run: userdel -r esecadm
    - Run: groupdel esec
12. Remove Installshield section of /etc/profile, /etc/.login
13. Remove the e-Security Oracle database by following the instructions in the section “Manual Cleanup of e-Security Oracle database on Linux”.
14. Restart the operating system.

Manual Cleanup of e-Security Oracle database on Linux

1. As oracle user, stop Oracle Listener:
   - Run: lsnrctl stop
2. Stop e-Security database:
   - Change to the Oracle user
   - Set the ORACLE_SID environment variable to the name of your e-Security database instance (usually ESEC).
   - Run: sqlplus '/ as sysdba'
   - At sqlplus prompt, run: shutdown immediate
3. Remove entry for e-Security database in the file /etc/oratab
4. Remove init<your_instance_name>.ora (usually initESEC.ora) file from the directory $ORACLE_HOME/dbs.
5. Remove entries for your e-Security database from the following files in the $ORACLE_HOME/network/admin directory:
   - tnsnames.ora

- listener.ora

6. Delete the database data files from the location you chose to install them.

Windows

Manual Cleanup of e-Security on Windows

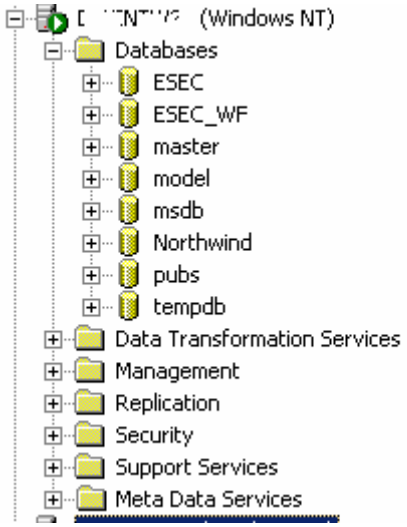
1. Delete the folder C:\Program Files\Common Files\InstallShield\Universal and all of its contents.
2. Delete the old e-Security installation folder (e.g.- C:\Program Files\esecurity5.0).
3. Delete the following environment variables (if they exist) by right-clicking on My Computer, selecting the Properties, clicking on the Advanced tab, then clicking on the Environment Variables button:
   - ESEC_HOME
   - ESEC_VERSION
   - ESEC_JAVA_HOME
   - ESEC_CONF_FILE
   - WORKBENCH_HOME
4. Remove any entries in the Path environment variable that point to a previous installation

   CAUTION: Be careful to only remove paths to old e-Security installations. Removing other entries in the Path can result in your system not functioning properly.

5. Delete all e-Security shortcuts from the Desktop.
6. Delete the shortcut folder Start > Programs > e-Security from the Start menu.
7. Remove the e-Security Microsoft SQL Server database by following the instructions in the section “Manual Cleanup of e-Security Microsoft SQL Server database on Windows”.
8. Restart the operating system.

Manual Cleanup of e-Security Microsoft SQL Server database on Windows

1. Open Microsoft SQL Server Enterprise Manager and connect to the SQL Server instance where you’ve installed your e-Security database.
2. Expand the Database tree and locate your e-Security database.



3. For each of the ESEC and ESEC_WF databases (or whatever name you gave your database during installation), right-click on the database and select “Delete”.
4. When prompted, select “Yes” to delete the database.

Appendix F – Sentinel Copyright Information

e-Security Sentinel™ 5

Sentinel 5 may contain the following third-party technologies:

- **Apache Axis** and **Apache Tomcat**, Copyright © 1999 to 2005, Apache Software Foundation. For more information, disclaimers and restrictions, see http://www.apache.org/licenses/
- **ANTLR.** For more information, disclaimers and restrictions, see http://www.antlr.org
- **Boost**, Copyright © 1999, Boost.org.
- **Bouncy Castle**, Copyright © 2000-2004, the Legion of Bouncy Castle. For more information, disclaimers and restrictions see http://www.bouncycastle.org.
- **Checkpoint.** Copyright © Check Point Software Technologies Ltd.
- **Concurrent**, utility package. Copyright © Doug Lea. Used without CopyOnWriteArrayList and ConcurrentReaderHashMap classes.
- **Crypto++ Compilation**. Copyright © 1995-2003, Wei Dai, incorporating the following copyrighted work: **mars.cpp** by Brian Gladman and Sean Woods. For more information, disclaimers and restrictions see http://www.eskimo.com/~weidai/License.txt.
- **Crystal Reports Developer and Crystal Reports Server**. Copyright © 2004 Business Objects Software Limited.
- **DataDirect Technologies Corp**. Copyright © 1991-2003.
- **edpFTPj**, licensed under the Lesser GNU Public License. For more information, disclaimers and restrictions see http://www.enterprisedt.com/products/edtftpj/purchase.html.
- **Enhydra Shark**, licensed under the Lesser General Public License available at: http://shark.objectweb.org/license.html.
- **ICEsoft ICEbrowser**. ICEsoft Technologies, Inc. Copyright © 2003-2004.
- **ILOG, Inc**. Copyright © 1999-2004.
- **Installshield Universal**. Copyright © 1996–2005, Macrovision Corporation and/or Macrovision Europe Ltd.
- **Java 2 Platform, Standard Edition**. Copyright © Sun Microsystems, Inc. For more information, disclaimers and restrictions see http://java.sun.com/j2se/1.4.2/j2re-1_4_2_10-license.txt.

The Java 2 Platform may also contain the following third-party products:

- CoolServlets © 1999
- DES and 3xDES © 2000 by Jef Poskanzer
- Crimson © 1999-2000 The Apache Software Foundation
- Xalan J2 © 1999-2000 The Apache Software Foundation
- NSIS 1.0j © 1999-2000 Nullsoft, Inc.
- Eastman Kodak Company © 1992
- Lucinda, a registered trademark or trademark of Bigelow and Holmes

  - Taligent, Inc.
  - IBM, some portions available at: http://oss.software.ibm.com/icu4j/

  For more information regarding these third-party technologies and their associated disclaimers and restrictions, see: http://java.sun.com/j2se/1.4.2/j2se-1_4_2-thirdpartylicensereadme.txt.

- **JavaBeans Activation Framework (JAF)**. Copyright © Sun Microsystems, Inc. For more information, disclaimers and restrictions see http://www.java.sun.com/products/javabeans/glasgow/jaf.html and click download > license.
- **JavaMail**. Copyright © Sun Microsystems, Inc. For more information, disclaimers and restrictions see http://www.java.sun.com/products/javamail/downloads/index.html and click download > license.
- **Java Ace**, by Douglas C. Schmidt and his research group at Washington University and **Tao (with ACE wrappers)** by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine and Vanderbilt University. Copyright © 1993-2005. For more information, disclaimers and restrictions see http://www.cs.wustl.edu/~schmidt/ACE-copying.html and http://www.cs.wustl.edu/~pjain/java/ace/JACE-copying.html
- **Java Authentication and Authorization Service Modules**, licensed under the Lesser General Public License. For more information, disclaimers and restrictions see http://free.tagish.net/jaas/index.jsp.
- **Java Network Launching Protocol (JNLP).** Copyright © Sun Microsystems, Inc. For more information, disclaimers and restrictions, please see http://www.java.sun.com/products/javawebstart/download-jnlp.html and click download > license.
- **Java Service Wrapper**. Portions copyrighted as follows: Copyright © 1999, 2004 Tanuki Software and Copyright © 2001 Silver Egg Technology. For more information, disclaimers and restrictions, see http://wrapper.tanukisoftware.org/doc/english/license.html.
- **JIDE**. Copyright © 2002 to 2005, JIDE Software, Inc.
- **jTDS** is licensed under the Lesser GNU Public License. For more information, disclaimers and restrictions see http://jtds.sourceforge.net/.
- **MDateSelector**. Copyright © 2005, Martin Newstead, licensed under the Lesser General Public License. For more information, disclaimers and restrictions see http://web.ukonline.co.uk/mseries.
- **Monarch Charts**. Copyright © 2005, Singleton Labs.
- **Net-SNMP**. Portions of the code are copyrighted by various entities, which reserve all rights. Copyright © 1989, 1991, 1992 by Carnegie Mellon University; Copyright © 1996, 1998 to 2000, the Regents of the University of California; Copyright © 2001 to 2003 Networks Associates Technology, Inc.; Copyright © 2001 to 2003, Cambridge Broadband, Ltd.; Copyright © 2003 Sun Microsystems, Inc. and Copyright © 2003 to 2004, Sparta, Inc. For more information, disclaimers and restrictions, see http://net-snmp.sourceforge.net.
- **The OpenSSL Project**. Copyright © 1998-2004. the Open SSL Project. For more information, disclaimers and restrictions, see http://www.openssl.org.
- **Oracle Help for Java**. Copyright © 1994-2006, Oracle Corporation.
- **RoboHELP Office.** Copyright © Adobe Systems Incorporated, formerly Macromedia.

- **Skin Look and Feel (SkinLF)**. Copyright © 2000-2006 L2FProd.com. Licensed under the Apache Software License. For more information, disclaimers and restrictions see https://skinlf.dev.java.net/.
- **Sonic Software Corporation**. Copyright © 2003-2004. The SSC software contains security software licensed from RSA Security, Inc.
- **Tinyxml**. For more information, disclaimers and restrictions see http://grinninglizard.com/tinyxmldocs/index.html.
- **SecurityNexus**. Copyright © 2003 to 2006. SecurityNexus, LLC. All rights reserved.
- **Xalan** and **Xerces**, both of which are licensed by the Apache Software Foundation Copyright © 1999-2004. For more information, disclaimers and restrictions see http://xml.apache.org/dist/LICENSE.txt.
- **yWorks.** Copyright © 2003 to 2006, yWorks.

NOTE: As of the publication of this documentation, the above links were active. In the event you find that any of the above links are broken or the linked webpages are inactive, please contact e-Security's Office of the Counsel at 1921 Gallows Road, Vienna, VA 22182. 703-852-8000.