AUTHORIZED DOCUMENTATION

Reference Guide

Novell® Sentinel™

6.1

March 2009

www.novell.com

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc., has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

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

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

Novell Trademarks

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

Third-Party Materials

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

Contents

Preface

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

Audience

This documentation is intended for Information Security Professionals.

Feedback

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

Additional Documentation

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

- *Sentinel 6.1 Installation Guide*
- *Sentinel 6.1 User Guide*
- *Sentinel 6.1 User Reference Guide*
- The documentation for this product is available at http://www.novell.com/documentation/sentinel61/index.html (http://www.novell.com/documentation/sentinel61/index.html)
- Additional documentation on developing collectors (proprietary or JavaScript) and JavaScript correlation actions is available at the Novell Developer Community web site: http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel)

Sentinel Install Guide

This guide explains how to install the following Sentinel components:

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

Sentinel User Guide

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

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

Sentinel User Reference Guide

This guide discusses the following advanced topics:

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

Collector Builder User Guide

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

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

Sentinel Patch Installation Guide

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

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

Documentation Conventions

The following are the conventions used in this manual:

- Notes and Warnings

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

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

- Commands appear in courier font. For example:

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

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

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

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

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

Contacting Novell

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

Sentinel™ User Reference Introduction

1

The Sentinel User Reference Guide is your reference for:

Collector administrator functions	Sentinel correlation engine
Collector and Sentinel meta tags	Sentinel command line options
Sentinel console user permissions	Sentinel server database views

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

This guide discusses about:

- Sentinel Meta tags
- Sentinel User Permissions
- Correlation Engine RuleLG Language
- Sentinel Data Access Service
- Sentinel Accounts and Password Changes
- Sentinel Database Views for Oracle
- Sentinel Database Views for Microsoft SQL Server

Sentinel Event Fields

2

Every Sentinel event or correlated event has certain fields that are automatically populated (such as Event Time and Event UUID) and other fields that may or may not be populated, depending on the type of event, the collector parsing, and the mapping service configuration. This event data is visible in Active Views, historical queries, and reports. They are stored in the database and can be accessed via the report views. They can also be used in actions available through the right-click event menu, correlation actions, and iTRAC workflow actions.

2.1 Event Field Labels and Tags

Each field can be referred to by a user-friendly label or a short tag. The user-friendly label is visible throughout the Sentinel Control Center interface, for example:

- Column headers for Active Views, historical event queries, and the Active Browser
- Correlation wizard drop-down menus
- Active View configuration drop-down menus

Each field has a default label, but that label is user-configurable using the Event Configuration option on the Admin tab. For more information, see "Admin Tab" section in *Sentinel 6.1 User Guide*. InitUserName is the default label to represent the account name of the user who initiated the event, but this can be changed by the administrator. When a user changes the default label, the changes are reflected in most areas of the interface, including any correlation rules, filters, and right-click menu options.

WARNING: Changing the default label for any variables other than Customer Variables may cause confusion when working with Novell Technical Services or other parties who are familiar with the default names. In addition, JavaScript Collectors built by Novell refer to the default labels described in this chapter and are not automatically updated to refer to new labels.

Each field also has a short tag name that is always used for internal references to the field and is not user-configurable. This short tag name may not correspond exactly to the default label; Sentinel labels have changed over the years, but the underlying short tags remain the same for backward compatibility. (For example, InitUserName is the default label for the account name of the user who initiated the event. The default label was previously SourceUserName, and the underlying short tag is "sun".)

NOTE: Many of the default labels were updated for clarity in the Sentinel 6.1 release. Because all filters, actions, and correlation rule definitions are defined using the short tags (even though the label may be visible in the interface), there is no change in functionality due to the label renaming.

Each field is associated with a specific data type, which corresponds to the data type in the database:

- **string:** limited to 255 characters (unless otherwise specified)
- **integer:** 32 bit signed integer
- **UUID:** 36 character (with hyphens) or 32 character (without hyphens) hexadecimal string in the format XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX (For example, -6A5349DA-7CBF-1028-9795-000BCDFFF482)

- **date:** Collector Variable must be set with date as number of milliseconds from January 1, 1970 00:00:00 GMT. When displayed in Sentinel Control Center, meta-tags of type date are displayed in a regular date format.
- **IPv4:** IP address in dotted decimal notation (that is – xxx.xxx.xxx.xxx)

2.1.1 Free-Form Filters and Correlation Rules

Users can use either the tag or the label when they write free-form language in the Sentinel Control Center. The Sentinel interface shows the user-friendly label.

Figure 2-1 *Correlation Wizard displaying labels in drop-down and free-form language*

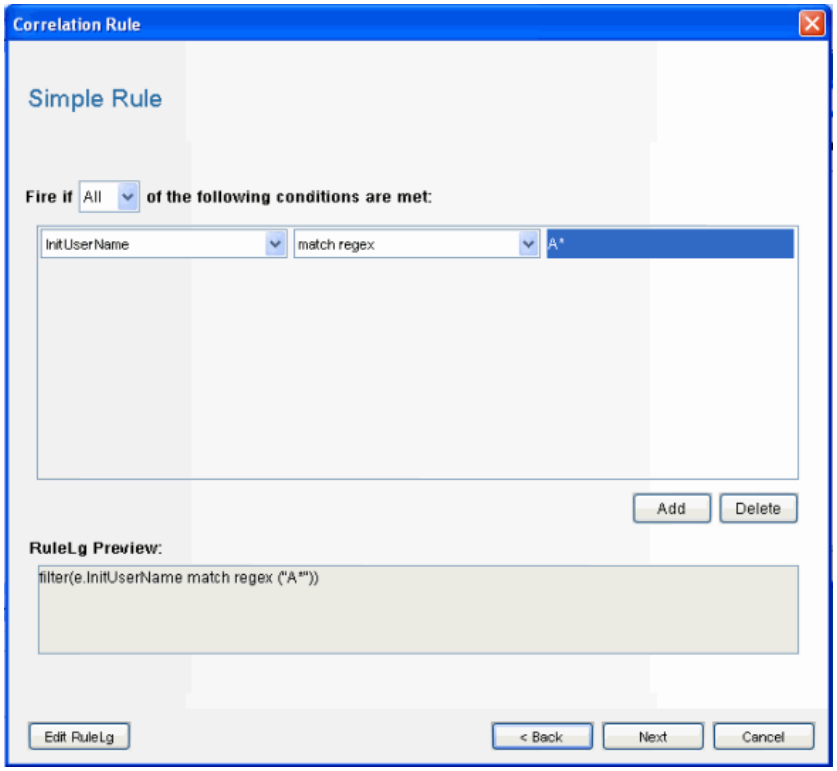
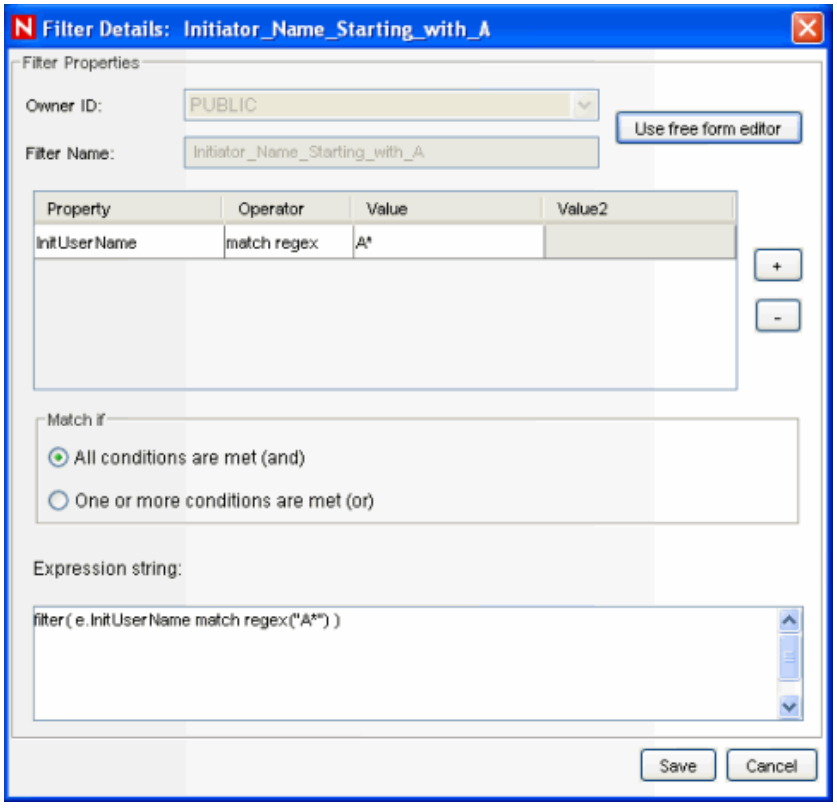


Figure 2-2 *Filter Wizard displaying labels in drop-down and free-form language*



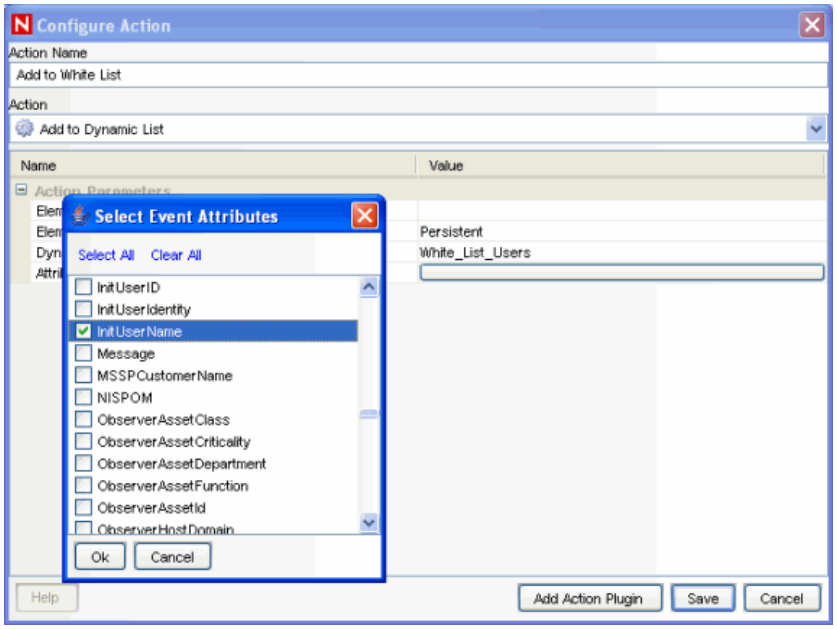
The representation of fields in the free-form RuleLG language is usually prefaced by “e.” for example, “e.InitUserName” or “e.sun” can refer to the Initiator User Name for the incoming or current event. In special cases, “w.” may be used to refer to a field in a past event (for example, “w.InitUserName”). For more information about the RuleLG language, see Chapter 4, “Sentinel Correlation Engine RuleLG Language,” on page 43.

2.1.2 Actions

Users can use either the tag or the label when they define parameters to be sent to right-click Event Menu actions, correlation actions, and iTRAC workflow actions.

To pass a field value to an action, you may use a checklist that shows the labels or type the parameter name directly into the configuration.

Figure 2-3 *Configuration Action - Select Event Attributes window*



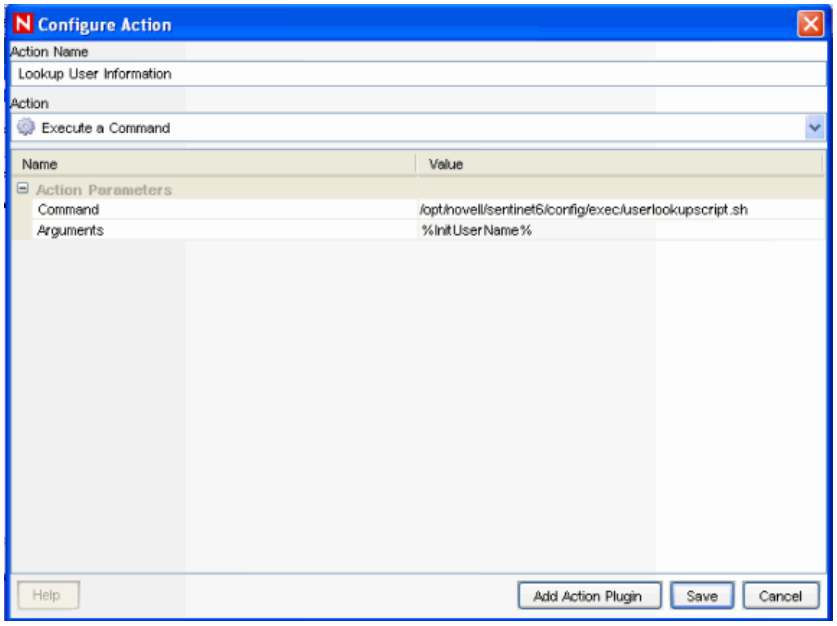
When you type the label or short tag for a field to be used in an action, the name can be enclosed in percent signs (%tag%) or dollar signs (tag). For example:

- %sun% in a correlation action refers to the value of InitUser in the correlated event
- sun in a correlation action refers to the value of InitUser in the current, “trigger” event (the final event that caused the correlation rule to fire)

NOTE: In a right-click menu event operating on a single event, there is no functional difference between %sun% and sun.

For example, to pass the Initiator User Name to a command line action to look up information from a database about that user, you could use %InitUserName% or %sun%. For more information about Actions, see “Actions and Integrators” section in *Sentinel 6.1 User Guide*.

Figure 2-4 *Configuration Action window*



2.1.3 Proprietary Collectors

Proprietary Collectors, written in Novell's own language, always use variables based on the short tag to refer to event fields. The short tag name must be prefaced by a letter and underscore, where the letter indicates the data type for the field (i_ for integer, s_ for string).

2.1.4 JavaScript Collectors

JavaScript Collectors usually refer to event fields using an "e." followed by the same user-friendly label set in Event Configuration in the Sentinel Control Center. For a Sentinel system with a default configuration, for example, the Initiator User Name would be referred to as "e.InitUserName" in the JavaScript Collector. There are some exceptions to this general rule. Refer to the Sentinel Collector SDK (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel) for more details.

2.2 List of Fields and Representations

The table on the following pages shows the default labels, descriptions and data types for the Sentinel event fields, along with the proper way to refer to the tags in filters, correlation rules, actions, and proprietary collector scripts. Fields that cannot or should not be manipulated in the Collector parsing do not have a Collector variable.

Table 2-1 *Labels and Meta-tags used in Sentinel Control Center and proprietary Collector language*

Default Label	Filters and Correlation Rules	Menu and Correlation Actions	Proprietary Collector Language	Data Type	Description
DeviceEventTimeString	e.et	%et%	s_ET	string	The normalized date and time of the event, as reported by the sensor.
DeviceEventTime	e.det	%det%		date	The normalized date and time of the event, as reported by the sensor.
SentinelProcessTime	e.spt	%spt%		date	The date and time Sentinel received the event.
BeginTime	e.bgnt	%bgnt%	s_BGNT	date	The date and time the event started occurring (for repeated events).
EndTime	e.endt	%endt%	s_ENDT	date	The date and time the event stopped occurring (for repeated events).
RepeatCount	e.rc	%rc%	s_RC	integer	The number of times the same event occurred if multiple occurrences were consolidated.
EventTime	e.dt	%dt%		date	The normalized date and time of the event, as given by the Collector.
SentinelServiceID	e.src	%src%		UUID	Unique identifier for the Sentinel service which generated this event.
Severity	e.sev	%sev%	i_Severity	integer	The normalized severity of the event (0-5).
Vulnerability	e.vul	%vul%	s_VULN	integer	The vulnerability of the asset identified in this event. Set to 1 if Sentinel detects an exploit against a vulnerable system. Requires Advisor.
Criticality	e.crt	%crt%	s_CRIT	integer	The criticality of the asset identified in this event.
InitIP	e.sip	%sip%	s_SIP	IPv4	IPv4 address of the initiating system.
TargetIP	e.dip	%dip%	s_DIP	IPv4	IPv4 address of the target system.
Collector	e.port	%port%		string	Name of the Collector that generated this event.

Default Label	Filters and Correlation Rules	Menu and Correlation Actions	Proprietary Collector Language	Data Type	Description
CollectorScript	e.agent	%agent%		string	The name of the Collector Script used by the Collector to generate this event.
Resource	e.res	%res%	s_Res	string	Compliance monitoring hierarchy level 1
SubResource	e.sres	%sres%	s_SubRes	string	Subresource name
ObserverHostName	e.sn	%sn%	s_SN	string	Unqualified hostname of the observer (sensor) of the event.
SensorType	e.st	%st%	s_ST	string	The single character designator for the sensor type (N, H, O, V, C, W, A, I).
Protocol	e.prot	%prot%	s_P	string	Protocol used between initiating and target services.
InitHostName	e.shn	%shn%	s_SHN	string	Unqualified hostname of the initiating system.
InitServicePort	e.spint	%spint%	s_SPINT	integer	Port used by service/ application that initiated the connection.
InitServicePortName	e.sp	%sp%	s_SP	string	Name of the initiating service that caused the event.
TargetHostName	e.dhn	%dhn%	s_DHN	string	Unqualified hostname of the target system.
TargetServicePort	e.dpint	%dpint%	s_DPINT	integer	Network port accessed on the target.
TargetServicePortName	e.dp	%dp%	s_DP	string	Name of the target service affected by this event.
InitUserName	e.sun	%sun%	s_SUN	string	Initiating user's account name. Example jdoe during an attempt to su.
TargetUserName	e.dun	%dun%	s_DUN	string	Target user's account name. Example root during a password reset.
FileName	e.fn	%fn%	s_FN	string	The name of the program executed or the file accessed, modified or affected.

Default Label	Filters and Correlation Rules	Menu and Correlation Actions	Proprietary Collector Language	Data Type	Description
ExtendedInformation	e.ei	%ei%	s_EI	string	Stores additional collector-processed information. Values within this variable are separated by semi-colons (;).
ReporterHostName	e.rn	%rn%	s_RN	string	Unqualified hostname of the reporter of the event.
ProductName	e.pn	%pn%	s_PN	string	Indicates the type, vendor and product code name of the sensor from which the event was generated.
Message	e.msg	%msg%	s_BM	string	Free-form message text for the event.
DeviceAttackName	e.rt1	%rt1%	s_RT1	string	Device specific attack name that matches attack name known by Advisor. Used in Exploit Detection.
Rt2	e.rt2	%rt2%	s_RT2	string	Reserved by Novell for expansion.
Ct1 thru Ct2	e.ct1 thru e.ct2	%ct1% thru %ct2%	s_CT1 and s_CT2	string	Reserved for use by customers for customer-specific data.
Rt3	e.rt3	%rt3%		integer	Reserved by Novell for expansion.
Ct3	e.ct3	%ct3%	s_CT3	integer	Reserved for use by customers for customer-specific data.
CorrelatedEventUuids	e.ceu	%ceu%	s_RT3	string	List of event UUIDs associated with th correlated event. Only relevant for correlated events.
CustomerHierarchyId	e.rv1	%rv1%	s_RV1	integer	Used for MSSPs.
ReservedVar2 thru ReservedVar10	e.rv2 thru e.rv10	%rv2% thru %rv10%	s_RV2 thru s_RV10	integer	Reserved by Novell for expansion.
ReservedVar11 thru ReservedVar20	e.rv11 thru e.rv20	%rv11% thru %rv20%	s_RV11 thru s_RV20	date	Reserved by Novell for expansion.

Default Label	Filters and Correlation Rules	Menu and Correlation Actions	Proprietary Collector Language	Data Type	Description
CollectorManagerId	e.rv21	%rv21%	s_RV21	UUID	Unique identifier for the Collector Manager which generated this event.
CollectorId	e.rv22	%rv22%	s_RV22	UUID	Unique identifier for the Collector which generated this event.
ConnectorId	e.rv23	%rv23%	S_RV23	UUID	Unique identifier for the Connector which generated this event.
EventSourceId	e.rv24	%rv24%	S_RV24	UUID	Unique identifier for the Event Source which generated this event.
RawDataRecordId	e.rv25	%rv25%	S_RV25	UUID	Unique identifier for the Raw Data Record associated with this event.
ControlPack	e.rv26	%rv26%	S_RV26	string	Sentinel control categorization level 1 (for Solution Packs).
EventMetricClass	e.rv28	%rv28%	s_RV28	string	Class of the event-dependent numeric value.
InitIPCountry	e.rv29	%rv29%	s_RV29	string	Country where the IPv4 address of the initiating system is located.
TargetIPCountry	e.rv30	%rv30%	s_RV30	string	Country where the IPv4 address of the target system is located.
DeviceName	e.rv31	%rv31%	s_RV31	string	Name of the device generating the event. If this device is supported by Advisor, the name should match the name known by Advisor. Used in Exploit Detection.
DeviceCategory	e.rv32	%rv32%	s_RV32	string	Device category (FW, IDS, AV, OS, DB).
EventContext	e.rv33	%rv33%	s_RV33	string	Event context (threat level).
InitThreatLevel	e.rv34	%rv34%	s_RV34	string	Initiator threat level.
InitUserDomain	e.rv35	%rv35%	s_RV35	string	Domain (namespace) in which the initiating account exists.
DataContext	e.rv36	%rv36%	s_RV36	string	Data context.
InitFunction	e.rv37	%rv37%	s_RV37	string	Initiator function.

Default Label	Filters and Correlation Rules	Menu and Correlation Actions	Proprietary Collector Language	Data Type	Description
InitOperationalContext	e.rv38	%rv38%	s_RV38	string	Initiator operational context.
MSSPCustomerName	e.rv39	%rv39%	s_RV39	string	MSSP customer name.
VendorEventCode	e.rv40	%rv40%	s_RV40	string	Event code reported by device vendor.
TargetHostDomain	e.rv41	%rv41%	s_RV41	string	Domain portion of the target system's fully-qualified hostname.
InitDomain	e.rv42	%rv42%	s_RV42	string	Domain portion of the initiating system's fully-qualified hostname.
ReservedVar43	e.rv43	%rv43%	s_RV43	string	Reserved by Novell for expansion.
TargetThreatLevel	e.rv44	%rv44%	s_RV44	string	Target threat level.
TargetUserDomain	e.rv45	%rv45%	s_RV45	string	Domain (namespace) in which the target account exists..
VirusStatus	e.rv46	%rv46%	s_RV46	string	Virus status.
TargetFunction	e.rv47	%rv47%	s_RV47	string	Target function.
TargetOperationalContext	e.rv48	%rv48%	s_RV48	string	Target operational context.
TaxonomyLevel4	e.rv53	%rv53%	s_RV53	string	Sentinel event code categorization - level 4.
CustomerHierarchyLevel2	e.rv54	%rv54%	s_RV54	string	Customer Hierarchy Level 2 (used by MSSPs).
VirusStatus	e.rv56	%rv56%	s_RV56	string	Virus Status.
InitMacAddress	e.rv57	%rv57%	s_RV57	string	Initiator Mac Address. Part of initiator host asset data.
InitNetworkIdentity	e.rv58	%rv58%	s_RV58	string	Initiator Network Identity. Part of initiator host asset data.
InitAssetFunction	e.rv60	%rv60%	s_RV60	string	Function of the initiating system (fileserver, webserver, etc.).
InitAssetValue	e.rv61	%rv61%	s_RV61	string	Initiator Asset Value. Part of initiator host asset data.
InitAssetCriticality	e.rv62	%rv62%	s_RV62	string	Criticality of the initiating system (0-5).

Default Label	Filters and Correlation Rules	Menu and Correlation Actions	Proprietary Collector Language	Data Type	Description
Variables reserved for future use by Novell	e.rv63 thru e.rv75	%rv63% thru %rv75%	s_RV63 thru s_rv75	string	Variables not currently in use
InitAssetDepartment	e.rv76	%rv76%	s_RV76	string	Department of the initiating system.
InitAssetId	e.rv77	%rv77%	s_RV77	string	Internal asset identifier of the initiator.
Variables reserved for future use by Novell	e.rv78 thru e.rv80	%rv78% thru %rv80%	s_RV78 thru s_rv80	string	Variables not currently in use
TargetAssetClass	e.rv81	%rv81%	s_RV81	string	Class of the target system (desktop, server, etc.).
TargetAssetFunction	e.rv82	%rv82%	s_RV82	string	Function of the target system (fileserver, webserver, etc.).
TargetAssetValue	e.rv83	%rv83%	s_RV83	string	Target Asset Value. Part of target host asset data.
Variables reserved for future use by Novell	e.rv84 thru e.rv97	%rv84% thru %rv97%	s_RV84 thru s_rv97	string	Variables not currently in use.
TargetDepartment	e.rv98	%rv98%	s_RV98	string	Target Department. Part of target host asset data.
TargetAssetId	e.rv99	%rv99%	s_RV99	string	Internal asset identifier of the target.
CustomerHierarchyLevel4	e.rv100	%rv100%	s_RV100	string	Customer Hierarchy Level 4 (used by MSSPs)
Variables reserved for future use by Novell	e.rv101 thru e.rv200	%rv101% thru %rv200%	s_rv101 thru s_rv200	various	Variables not currently in use
CustomerVar1 thru CustomerVar10	e.cv1 thru e.cv10	%cv1% thru %cv10%	s_CV1 thru s_CV10	integer	Number variable reserved for customer use. Stored in database.
CustomerVar11 thru CustomerVar20	e.cv11 thru e.cv20	%cv11% thru %cv20%	s_CV11 thru s_CV20	date	Date variable reserved for customer use. Stored in database.
CustomerVar21 thru CustomerVar89	e.cv21 thru e.cv89	%cv21% thru %cv89%	s_CV21 thru s_CV29	string	String variable reserved for customer use. Stored in database.

Default Label	Filters and Correlation Rules	Menu and Correlation Actions	Proprietary Collector Language	Data Type	Description
SARBOX	e.cv90	%cv90%	s_CV90	string	Set to 1 if the asset is governed by Sarbanes-Oxley.
HIPAA	e.cv91	%cv91%	s_CV91	string	Set to 1 if the asset is governed by the Health Insurance Portability and Accountability Act (HIPAA) regulation.
GLBA	e.cv92	%cv92%	s_CV92	string	Set to 1 if the asset is governed by the Gramm-Leach Bliley Act (GLBA) regulation.
FISMA	e.cv93	%cv93%	s_CV93	string	Set to 1 if the asset is governed by the Federal Information Security Management Act (FISMA) regulation.
NISPOM	e.cv94	%cv94%	s_CV94	string	Set to 1 via an asset map if the target asset is governed by the National Industrial Security Program Operating Manual (NISPOM)
CustomerVar95 thru CustomerVar100	e.cv95 thru e.cv100	%cv95% thru %cv100%	s_CV95 thru s_CV100	string	String variable reserved for customer use. Stored in database.
CustomerVar101 thru CustomerVar110	e.cv101 thru e.cv110	%cv101% thru %cv110%	s_CV101 thru s_CV110	string	Integer variable reserved for customer use. Stored in database.
CustomerVar111 thru CustomerVar120	e.cv111 thru e.cv120	%cv111% thru %cv120%	s_CV111 thru s_CV120	string	Date variable reserved for customer use. Stored in database.
CustomerVar121 thru CustomerVar130	e.cv121 thru e.cv130	%cv121% thru %cv130%	s_CV121 thru s_CV130	string	UUID variable reserved for customer use. Stored in database.
CustomerVar131 thru CustomerVar140	e.cv131 thru e.cv140	%cv131% thru %cv140%	s_CV131 thru s_CV140	string	IPv4 variable reserved for customer use. Stored in database.
CustomerVar141 thru CustomerVar150	e.cv141 thru e.cv150	%cv141% thru %cv150%	s_CV141 thru s_CV150	string	String variable reserved for customer use. Stored in database.
CustomerVar151 thru CustomerVar160	e.cv151 thru e.cv160	%cv151% thru %cv160%	s_CV151 thru s_CV160	string	Integer variable reserved for customer use. Not stored in database.

Default Label	Filters and Correlation Rules	Menu and Correlation Actions	Proprietary Collector Language	Data Type	Description
CustomerVar161 thru CustomerVar170	e.cv161 thru e.cv170	%cv161% thru %cv170%	s_CV161 thru s_CV170	string	Date variable reserved for customer use. Not stored in database.
CustomerVar171 thru CustomerVar180	e.cv171 thru e.cv180	%cv171% thru %cv180%	s_CV171 thru s_CV180	string	UUID variable reserved for customer use. Not stored in database.
CustomerVar181 thru CustomerVar190	e.cv181 thru e.cv190	%cv181% thru %cv190%	s_CV181 thru s_CV190	string	IPv4 variable reserved for customer use. Not stored in database.
CustomerVar191 thru CustomerVar200	e.cv191 thru e.cv200	%cv191% thru %cv200%	s_CV191 thru s_CV200	string	String variable reserved for customer use. Not stored in database.

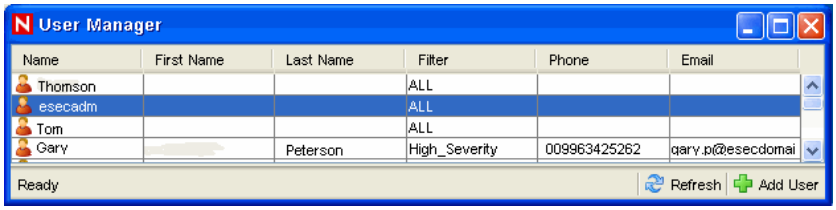
Sentinel Control Center User Permissions

3

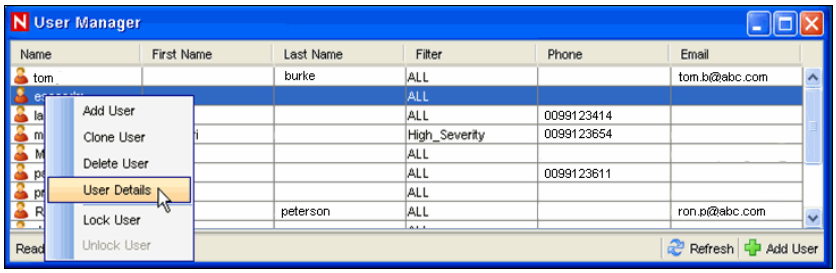
Sentinel allows administrators to set user permissions in the Sentinel Control Center at a granular level. The only user created by default is the esecadm, or Sentinel Administrator. All other users are created by the Sentinel Administrator, or someone with similar permissions.

To change user permissions:

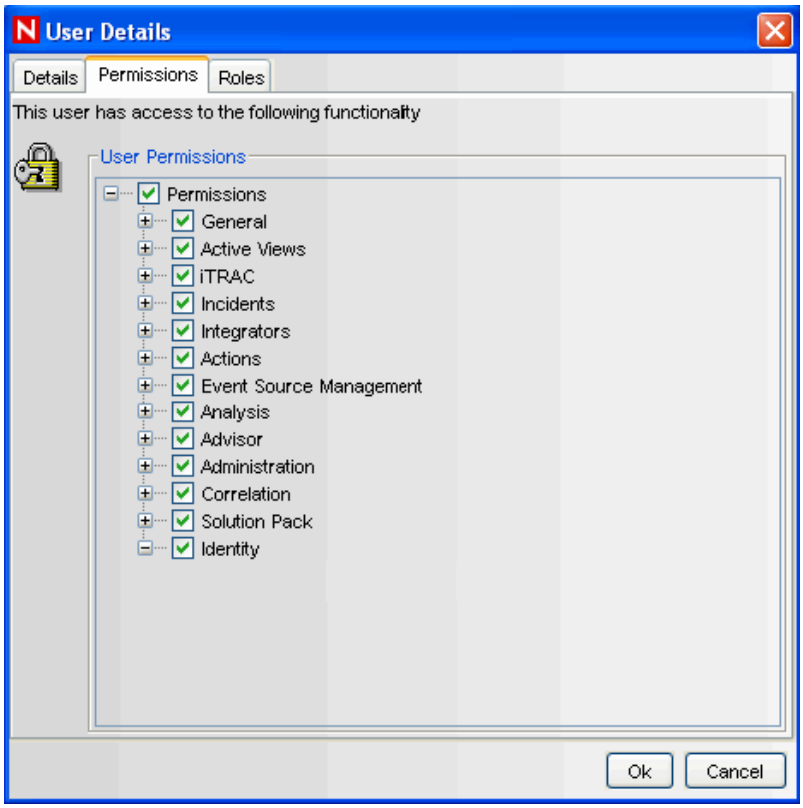
1. Log into the Sentinel Control Center as a user with “User Management” permissions.
2. Click the Admin tab.
3. Select User Configuration from Admin tab. Alternatively, Select User Manager from User Configuration in the Navigator.



4. Right click user and select User Details.



5. Select the Permissions tab.



6 Uncheck the checkboxes for which you want to restrict user.

7 Click OK.

The permissions in the User Manager are grouped into several major categories:

- General (page 35)
- Active Views (page 36)
- iTRAC (page 37)
- Incidents (page 37)
- Integrators (page 38)
- Sentinel Control Center User Permissions (page 33)
- Event Source Management (page 39)
- Analysis Tab (page 39)
- Advisor Tab (page 39)
- Administration (page 40)
- Correlation (page 41)
- Solution Pack (page 41)
- Identity (page 41)

Each of these groups of setting is described in more detail below.

3.1 General

Table 3-1 *Permissions-General*

Permission Name	Description
Save Workspace	Allows user to save preferences. If this permission is unavailable, user will never be prompted to save changes to preferences when logging out or exiting the Sentinel Control Center.
Column Management	Allows user to manage the columns in the Active View tables.
Snapshot	Allows user to take a snapshot of Active View tables.

3.1.1 General – Public Filters

Table 3-2 *Permissions-General-Public Filters*

Permission Name	Description
Create Public Filters	Allows user to create a filter with an owner ID of PUBLIC. If user does not have this permission, then the value PUBLIC will not be listed as one of the owner IDs that user can create a filter for.
Modify Public Filters	Allows user to modify a public filter.
Delete Public Filters	Allows user to delete a public filter.

3.1.2 General – Manage Private Filters of Other Users

Table 3-3 *Permissions-General-Manage Private Filters of Other Users*

Permission Name	Description
Create Private Filters for Other Users	Allows user to create private filters for themselves or for other users.
Modify Private Filters of Other Users	Allows user to modify their own private filters and private filters created by other users.
Delete Private Filters of Other Users	Allows user to delete their own private filters and private filters created by other users.
View/Use Private Filters of Other Users	Allows user to view/use their own private filters and private filters crated by other users.

3.1.3 General – Integration Actions

Table 3-4 *Permissions-General-Integration Actions*

Permission Name	Description
Send to Remedy Help Desk	Allows user to send events, incident and associated objects to Remedy. (requires the optional Remedy integration component)

3.2 Active Views

Table 3-5 *Permissions-Active Views*

Permission Name	Description
View Active Views Tab	Allows user to see and use the Active Views tab, menu and other related functions associated with the Active Views tab.

3.2.1 Active Views – Menu Items

Table 3-6 *Permissions-Active Views-Menu Items*

Permission Name	Description
Use Assigned Menu Items	Allows user to use assigned menu items in the Active Views Events table (the right-click menu).
Add to Existing Incident	Allows user to add events to existing incidents using the Active Views Events table (the right-click menu).
Remove from Incident	Allows user to remove events from an existing incident using the Events tab Events table (the right-click menu).
Email Events	Allows user to e-mail events using the Active Views Events table (the right-click menu).
View Advisor Attack Data	Allows user to view the Advisor Attack Data stream.
View Vulnerability	Allows user to view the vulnerabilities present in the Sentinel database

3.2.2 Active Views – Active Views

Table 3-7 *Permissions-Active Views-Active Views*

Permission Name	Description
Use/View Active Views	Allows user to access the Active Views charts.

3.3 iTRAC

Table 3-8 *Permissions-iTRAC*

Permission Name	Description
View iTRAC Tab	Allows user to see and use the iTRAC tab, menu and other related functions associated with the iTRAC tab.
Activity Management	Allows user to access the Activity Manager.
Manage Work Items Of Users	Gives user administrative control over all workitems, including those assigned to other users

3.3.1 iTRAC - Template Management

Table 3-9 *Permissions-iTRAC-Template Management*

Permission Name	Description
View/Use Template Manager	Allows user to access the Template Manager.
Create/Modify Templates	Allows user to create and modify templates.

3.3.2 iTRAC - Process Management

Table 3-10 *Permissions-iTRAC-Process Management*

Permission Name	Description
View/Use Process Manager	Allows user to access the Process View Manager.
Start/Stop Processes	Allows user to use the Process View Manager.

3.4 Incidents

Table 3-11 *Permissions-Incidents*

Permission Name	Description
View Incidents Tab	Allows user to see and use the Incidents tab, menu and other related functions associated with the View Incidents tab.
Incident Administration	Allows user to modify an incident.
View Incident(s)	Allows user to view/modify the details of an incident. If the user does not have this permission, then the Incident Details window will not be displayed when the user either double-clicks an Incident in the Incident View window or right-clicks the incident or selects the Modify option.

Permission Name	Description
Create Incident(s)	Allows user to create Incidents in the in the Incident View window or by right clicking on the incident and select Modify option. Alternatively you can select Create Incident menu item in the Incidents menu bar and clicking Create Incident option in the tool bar.
Modify Incident(s)	Allows user to modify an incident in the Incident Details window.
Delete Incident(s)	Allows user to delete incidents.
Assign Incident(s)	Allows user to assign an incident in the Modify and Create Incident window.
Email Incidents	Allows user to e-mail Incidents of interest.
Incident Actions	Allows user to view Execute Incident Action menu option in an Incident and to execute actions.
Add Notes	Allows user to add any number notes to an incident.

3.5 Integrators

Table 3-12 *Permissions-Integrators*

Permission Name	Description
View Integrator	Allows user to view Integrators, open Integrator Manager, use update, refresh, help, test buttons and view integrator event details.
Manage Integrator	Allows user to manage (add/modify/delete) the configured Integrators.
Manage Integrator Plugins	Allows user to manage (add/modify/delete) the Integrators plugins.

3.6 Actions

Table 3-13 *Permissions-Action Manager*

Permission Name	Description
View Actions	Allows user to use Action Manager and view Actions.
Manage Actions	Allows user to add/edit/delete actions of type "Execute Action Plugins"
Manage Action Plugins	Allows user to add/edit/delete Action Plugins.

3.7 Event Source Management

Table 3-14 *Permissions-Event Source Management*

Permission Name	Description
View Status	Allows user to view the status of ESM components.
View Scratchpad	Allows user to design and configure ESM components.
Configure ESM Components	Allows you to configure ESM components.
Control ESM Components	Allows you to control and manage ESM components.
Manage Plugins	Allows you to manage Collector and Connector Plugins.
View Raw Data	Allows you to view/parse raw data.
Debug Collector	Allows you to debug Collector.

Command and Control consists of:

- start/stop individual ports
- start/stop all ports
- restart hosts
- rename hosts

3.8 Analysis Tab

Table 3-15 *Permissions-Analysis Tab*

Permission Name	Description
View Analysis Tab	Allows user to see and use the View Analysis tab, menu and other related functions associated with the View System Overview tab.

3.9 Advisor Tab

Table 3-16 *Permissions-Advisor Tab*

Permission Name	Description
View Advisor Tab	Allows user to see and use the View Advisor tab, menu and other related functions associated with the View Advisor tab.

3.10 Administration

Table 3-17 *Permissions-Administration*

Permission Name	Description
View Administration Tab	Allows user to see and use the View Administration tab, menu and other related functions associated with the View Administration tab.
DAS Statistics	Allows user to view DAS activity (DAS binary and query).
Event Configuration	Allows user to rename columns, set mappings from mapping files. This function is associated with Mapping Configuration.
Map Data Configuration	Allows user to add, edit and delete mapping files.
Event Menu Configuration	Allows user to access the Menu Configuration window and add new options that display on the Event menu when you right-click an event.
Report Data Configuration	Allows user to enable or disable summary tables used in aggregation.
User Management	Allows user to add, modify and delete user details
User Session Management	Allows user to view, lock and terminate active users (logins to Sentinel Control Center).
iTRAC Role Management	Allows user to view and use the role manager in the Admin Tab.

3.10.1 Administration – Global Filters

Table 3-18 *Permissions-Administration-Global Filters*

Permission Name	Description
View/Use Global Filters	Allows user to access the Global Filter Configuration window.
Modify Global Filters	Allows user to modify the global filters configuration. **NOTE:** To access this function, View Global Filters permission must also be assigned.

3.10.2 Administration – Server Views

Table 3-19 *Permissions-Administration-Server Views*

Permission Name	Description
View Servers	Allows user to monitor the status of all processes.
Control Servers	Allows user to start, restart and stop processes.

3.11 Correlation

Table 3-20 *Permissions-Correlation*

Permission Name	Description
View Correlation Tab	Allows user to use the Correlation functions.
View/Use Correlation Rule Manager	Allows user to start or stop the Correlation Rules.
View/Use Correlation Engine Manager	Allows user to deploy/undeploy the Correlation Rules.
View/Use Dynamic Lists	Allows user to Create, use, view, modify the Dynamic Lists.

3.12 Solution Pack

Table 3-21 *TPermissions-Solution Pack*

Permission Name	Description
Solution Designer	Allows user to access Solution Designer.
Solution Manager	Allows user to access Solution Manager.

3.13 Identity

Table 3-22 *Permissions-Action Manager*

Permission Name	Description
View/Use Identity Address Book	Allows user to view and use Identity Browser.

Sentinel Correlation Engine RuleLG Language

4

This section is about Sentinel correlation engine Rule LG language.

4.1 Correlation RuleLG Language Overview

The Sentinel Correlation Engine runs rules that are written in the Correlation RuleLg language. Rules are created in the Sentinel Control Center. Users can create rules using a wizard for the following rule types:

- Simple Rule
- Composite Rule
- Aggregate Rule
- Sequence Rule

These rules are converted to the Correlation RuleLg language when the rules are saved. The same rule types, plus even more complex rules, can be created in the Sentinel Control Center using the Custom/Freeform option. To use the Custom/Freeform option, the user must have a good understanding of the Correlation RuleLg language.

RuleLg uses several operations, operators, and event field short tags to define a rule. The Correlation Engine loads the rule definition and uses the rules to evaluate, filter, and store in memory events that meet the criteria specified by the rule. Depending on the rule definition, a correlation rule might fire based on

- the value of one field or multiple fields
- the comparison of an incoming event to past events
- the number of occurrences of similar events within a defined time period
- one or more subrules firing
- one or more subrules firing in a particular order

Each of these constructs is represented by an operation in RuleLg.

4.2 Event Fields

All operations function on event fields, which can be referred to by their labels or by their short tags within the correlation rule language. For a full list of labels and short tags, see “Sentinel Event Fields” section. The label or metatag must also be combined with a prefix to designate whether the event field is part of the incoming event or a past event that is stored in memory.

Examples:

```
e.DestinationIP (Destination IP for the current event)
e.dip (Destination IP for the current event)
w.dip (Destination IP for any stored event)
```

WARNING: If you rename the label of a metatag, do not use the original label name when creating a correlation rule.

4.3 Event Operations

Event operations evaluate, compare, and count events. They include the following operations:

- **Filter:** Evaluates the current to determine whether they could potentially trigger a rule to fire
- **Window:** Compares the current event to past events that have been stored in memory
- **Trigger:** Counts events to determine whether enough events have occurred to trigger a rule

Each operation works on a set of events, receiving a set of events as input and returning a set of events as output. The current event processed by a rule often has a special meaning for the semantic of the language. The current event is always part of the set of events in and out of an operation unless the set is empty. If an input set of an operation is empty, then the operation is not evaluated.

4.3.1 Filter Operation

Filter consists of a Boolean expression that evaluates the current event from the real-time event stream. It compares event attributes to user-specified values using a wide set of operators

The Boolean expression is a composite of comparison and match instructions.

The syntax for filter is:

```
Filter <Boolean expression 1> [NOT|AND|OR <Boolean expression 2] […] [NOT|AND|OR
<Boolean expression n>]
```

Where

```
<Boolean expressions 1…n> are expressions using one or more event field names and
filter operators
```

For example, this rule detects whether the current event has a severity of 4 and the resource event field contains either “FW” or “Comm.”

```
filter(e.sev = 4 and (e.res match regex ("FW") or e.res match regex ("Comm")))
```

Boolean Operators

Filter expressions can be combined using the Boolean operators AND, OR and NOT. The filter boolean operator precedence (from highest [top] to lowest [bottom] precedence) is:

Table 4-1 *Boolean Operators*

Operator	Meaning	Operator Type	Associativity
Not	logical not	unary	None
And	logical and	binary	left to right
Or	logical or	binary	left to right

In addition to Boolean operators, filter supports the following operators.

Standard Arithmetic Operators

Standard arithmetic operators can be used to build a condition that compares the value of a Sentinel metatag and a user-specified value (either a numeric value or a string field). The standard arithmetic operators in Sentinel are =, <, >, !=, <=, and >=.

Examples:

```
filter(e.Severity > 3)
filter(e.BeginTime < 1179217665)
filter(e.SourceUserName != “Administrator”)
```

Match Regex Operators

The match regex operator can be used to build a condition where the value of a metatag matches a user-specified regular expression value specified in the rule. This operator is used only for string tags, and the user-specified values for this operator are case-sensitive.

Examples:

```
filter(e.Collector match regex ("IBM"))
filter(e.EventName match regex ("Attack"))
```

Match Subnet Operators

The match subnet operator can be used to build a condition where the value of a metatag maches a user-specified subnet specified in the rule in CIDR notation. This operator is used only for IP address fields.

Example:

```
filter(e.DestinationIP match subnet (10.0.0.1/22))
```

Inlist Operator

The inlist operator is used to perform a lookup on an existing dynamic list of string values, returning true if the value is present in the list. For more information on Dynamic Lists, see “Correlation Tab” in *Sentinel 6.1 User Guide*.

For example, this filter expression is used to evaluate whether the Source IP of the current event is present on a dynamic list called MailServerList. If the Source IP is present in this list, the expression evaluates to TRUE.

```
filter(e.sip inlist MailServerList)
```

As another example, this filter expression combines the NOT and the INLIST operator. This expression evaluates to TRUE if the Source IP is not present in the dynamic list called MailServerList.

```
filter(not (e.sip inlist MailServerList))
```

This filter expression is used to evaluate whether the event name of the current event equals “File Access” and the Source User Name is also not present on a dynamic list called AuthorizedUsers. If both conditions are true for the current event, the expression evaluates to TRUE.

```
filter(e.evt="File Access" and not(e.sun inlist AuthorizedUsers))
```

ISNULL Operator

The isnull operator returns true if the metatag value is equal to NULL.

Example:

```
Filter(isnull(e.SIP))
```

Output Sets

- The output of a filter is either the empty set (if the Boolean expression evaluates to false) or a set containing the current event and all of the other events from the incoming set (if the Boolean expression evaluates to true).
- If filter is the last or only operation of a correlation rule, then the output set of the filter is used to construct a correlated event. The trigger events are the filter operation output set of events with the current event first.
- If filter is not the last operation of a correlation rule (that is, filter is followed by a flow operatior), then the output set of a filter is used as the input set to other operations (through the flow operator).

Additional Information

- The filter operator can be used to compare metatag values with other metatag values, for example:

  ```
  e.SourceIP=e.DestinationIP
  ```

4.3.2 Window Operation

Window compares the current event to a set of past events that are stored in a “window.” The events in the window can be all past events for a certain time period, or they can be filtered.

The Boolean expression is a composite of comparison instructions and match instructions with the Boolean operators AND, OR and NOT.

The syntax for window is:

```
Window (<Boolean expression>[, <filter expression>, <evaluation period>)
```

Where

```
<Boolean expression> is an expression comparing a metatag value from the current
event to a metatag value from a past event (or a user-specified constant)
<filter expression> is optional and specifies filter criteria for the past events
<evaluation period> specifies the duration for which past events matching the
filter expression are maintained, specified in seconds (s), minutes (m), or hours
(h). If no letter is specified, seconds are assumed.
```

For example, this rule detects whether the current event has a source IP address in the specified subnet (10.0.0.10/22) and matches an event(s) that happened within the past 60 seconds.

```
window(e.sip = w.sip, filter(e.sip match subnet (10.0.0.10/22),60)
```

As another example, this rule is a domino type of rule. An attacker exploits a vulnerable system and uses it as an attack platform.

```
window((e.sip = w.dip AND e.dp = w.dp AND e.evt = w.evt), 1h)
```

This rule identifies a potential security breach after a denial of service attack. The rule fires if the destination of a denial of service attack has a service stopped within 60 seconds of the attack.

```
filter(e.rv51="Service" and e.rv52="Stop" and e.st = "H") flow window (e.sip =
w.dip, filter(e.rv52="Dos"), 60s) flow trigger(1,0))
```

Output Sets

- If any past event evaluates to true with the current event for the simple boolean expression, the output set is the incoming event plus all matching past events.
- If no events in the window match the current event for the simple boolean expression, the output set is empty.
- If a window is the last or only operation of a correlation rule, then the output set of the window is used to construct a correlated event (the correlated events being the window operation output set of events with the current event first).

Additional Information

- You must prepend a metatag name with "e." to specify the current event or with "w." to specify the past events
- All window simple Boolean expressions must include a metatag in the form w.[metatag].
- For more information about valid filter expressions, see Section 4.3.1, “Filter Operation,” on page 44.
- Every event coming in to the Correlation Engine that passes this filter is put into the window of past events
- If no filter expression exists, then all events coming into the Correlation Engine are maintained by the window. With extremely high event rates or long durations, this might require a large amount of memory.
- The current event is not placed into the window until after the current event window evaluation is complete
- To minimize memory usage, only the relevant parts of the past events, not all metatag values, are maintained in memory.

4.3.3 Trigger Operation

Trigger is used to specify a number of events for a user-specified duration.

The syntax for trigger is:

```
Trigger (<number of events>, <evaluation period>[, discriminator (<list of tags>))
```

Where

```
<number of events> is an integer value specifying the number of matching events
that are necessary for the rule to fire
<evaluation period> specifies the duration for which past events matching the
filter expression are maintained, specified in seconds (s), minutes (m), or hours
(h).  If no letter is specified, seconds are assumed.
discriminator is a field to group by
```

For example, this rule detects if 5 events with the same source IP address happen within 10 seconds.

```
trigger(5,10,discriminator(e.sip))
```

Output Sets

- If the specified count is reached within the specified duration, then a set of events containing all of the events maintained by the trigger is output; if not, the empty set is output.
- When receiving a new input set of events, a trigger first discards the outdated events (events that have been maintained for more than the duration) and then inserts the current event. If the number of resulting events is greater than or equal to the specified count, then the trigger outputs a set containing all of the events.
- If a trigger is the last operation (or the only operation) of a correlation rule, then the output set of the trigger is used to construct a correlated event (the correlated events being the trigger operation output set of events with the current event first).
- If a trigger is not the last operation of a correlation rule (that is, it is followed by a flow operator), then the output set of a trigger is used as the input set to other operations (through the flow operator).
- The discriminator (meta-tag list) is a comma-delimited list of meta-tags. A trigger operation keeps different counts for each distinct combination of the discriminator meta-tags.

4.4 Rule Operations

Rule operations work on subrules that have been combined into a compound rule. They include:

- Gate
- Sequence

4.4.1 Gate Operation

The gate operation is used to create a composite rule which is used in identifying complex situations from the occurrence of simple situations.

The composite rule is made up of one or more nested subrules and can be configured to fire if some, any or all of the subrules fire within a specified time window. The subrules can be a simple rule or another composite rule. For more information on Composite Rule, see “Correlation Tab” in *Sentinel 6.1 User Guide*.

The syntax for gate is:

```
Gate(<subrule 1 rulelg>, <subrule 2 rulelg>…<subrule n ruleLg>,  <mode>,
<evaluation period>, discriminator(<list of tags>))
```

Where

```
Subrule Rulelgs are the rulelg definitions for 1 to n subrules
mode = all | any | 1 | 2 | … | n, which is the number of subrules that must be
triggered in order for the gate rule to trigger
<evaluation period> specifies the duration for which past events matching the
filter expression are maintained, specified in seconds (s), minutes (m), or hours
(h).  If no letter is specified, seconds are assumed.
discriminator is a field to group by
```

For example, this rule is a typical perimeter security IDS inside/outside rule

```
filter(e.sev > 3) flow gate(filter(e.sn = "in"), filter(e.sn = "out"), all, 60s,
discriminator(e.dip, e.evt))
```

4.4.2 Sequence Operation

Sequence rules are similar to gate rules, except that all child rules must fire in time order for the sequenced rule to evaluate to true.

The subrules can be a simple rule or another composite rule.

The syntax for sequence is:

```
Sequence(<subrule 1 rulelg>, <subrule 2 rulelg>…<subrule n ruleLg>, <evaluation
period>, discriminator(<list of tags>))
```

Where

```
Subrule Rulelgs are the rulelg definitions for 1 to n subrules
<evaluation period> is a time period expressed in seconds (s), minutes (m), or
hours (h)
discriminator is a field to group by
```

For example, this rule detects three failed logins by a particular user in 10 minutes followed by a successful login by same user.

```
sequence (filter(e.evt="failed logins") flow trigger(3, 600,
discriminator(e.sun,e.dip)), filter(e.evt="goodlogin"), 600, discriminator(e.sun,
e.dip))
```

4.5 Operators

Operators are used to transition between operations or expressions. The fundamental operators used between operations are:

- Flow operator
- Union operator
- Intersection operator
- Discriminator operator

4.5.1 Flow Operator

The output set of events of the left-hand side operation is the input set of events for the right-hand side operation. Flow is typically used to transition from one correlation operation to the next.

For example:

```
filter(e.sev = 5) flow trigger(3, 60)
```

The output of the filter operation is the input of the trigger operation. The trigger only counts events with severity equal to 5.

4.5.2 Union Operator

The union of the left side operation output set and the right side operation output set. The resulting output set contains events from either the left-hand side operation output set or the right-hand side operation output set without duplicates.

For example:

```
filter(e.sev = 5) union filter(e.sip = 10.0.0.1)
```

is equivalent to

```
filter(e.sev = 5 or e.sip = 10.0.0.1)
```

4.5.3 Intersection Operator

The intersection of the left side operation output set and the right side operation output set. The resulting output set contains events that are common in both the left-hand side operation output set and the right-hand side operation output set without duplicates.

For example:

```
filter(e.sev = 5) intersection filter(e.sip = 10.0.0.1)
```

is equivalent to

```
filter(e.sev = 5 and e.sip = 10.0.0.1)
```

4.5.4 Discriminator Operator

The discriminator operator allows users to group by event fields within other event operations. Discriminator can be used within the trigger, gate, or sequence operations. This is the last operation when executing a condition. The input for this operator will generally be the output of other operations, if any.

For example, this filter expression is used to identify five severity 5 events within 60s that all have the same Source IP. Note that the attribute (SIP in this example) can be any value, even a NULL, but it must be the same for all five events in order for the rule to fire.

```
filter(e.sev=5 ) flow trigger(5, 60s, discriminator(e.sip)
```

4.6 Order of Operators

The operator precedence (from highest (top) to lowest (bottom)) are:

Table 4-2 *Operator Precedence*

Operator	Meaning	Operator Type	Associativity
flow	Output set becomes input set	binary	left to right
intersection	Set intersection (remove duplicates)	binary	left to right
union	Set union (remove duplicates)	binary	left to right

4.7 Differences between Correlation in 5.x and 6.x

There are several new functionalities updated / included in 6.0 to widen the usage of Correlation to meet user's requirements and for the ease-of-use.

- Gate Operation: This is new in 6.0.
- Sequence Operation: This is new in 6.0.
- Inlist Operator and Dynamic Lists: These are new in 6.0.
- Isnull Operator: This is new in 6.0. For metatag values equal to null, Sentinel 5.x supported the following syntax which is replaced by the ISNull operator in Sentinel 6.0

  ```
  e.SIP= " "
  ```

- Update Window: This is new in Sentinel 6.0
- Sentinel 6.0 merges the "C" (Correlated Events) and "W" (watchlist events) SensorTypes. All events generated by the Correlation Engine are now labeled "C" in the SensorType field.
- Correlation Actions and Correlation Rules: Correlation Actions and Correlation Rules are decoupled in Sentinel 6.0
- Although the filter operation supported AND and OR Boolean expressions in Sentinel 5.x, the window operation supports Boolean expressions for the first time in Sentinel 6.0. For example:

  ```
  OR: window(e.dip=w.dip OR e.sip=w.sip, filter(e.sev>2),60)
  AND: window(e.evt=w.evt AND e.sun=w.sun, filter(e.sev>2),60)
  ```

- Sentinel 6.0 no longer has the GUI option to create a rule from a PUBLIC filter. The filter criteria must be defined in the correlation wizard or language.
- The update functionality for a rule that is triggered more than once is configurable in Sentinel 6.0. In Sentinel 5.1.3, updates to a rule were based on a sliding window based on the trigger time period. In Sentinel 6.0, the update functionality can be set when the rule is deployed; the rule actions might happen every time the rule is triggered, or they can be set to occur once and then wait for some period of time before the action occurs again. This prevents multiple notifications on a single, ongoing event.
- The in, not in, and difference operators are deprecated in Sentinel 6.0. Correlation rules using these operators must be modified before running them in Sentinel 6.0.
- The e.all metatag has been deprecated. Correlation rules using this operator should be updated to use specific short tags before running them in Sentinel 6.0.

Sentinel Data Access Service

5

The Data Access Service (DAS) process is Sentinel Server's persistence service and provides a message bus interface to the database. Some of the services it provides are event storage, Historical Query, event drill down, vulnerability and Advisor data retrieval, and configuration manipulation.

5.1 DAS Container Files

DAS is a collection of services provided by five different processes. Each process is a container responsible for different types of database operations. These processes are:

- **DAS Query:** Performs general Sentinel Service operations including Login and Historical Query.
- **DAS Binary:** Performs event database insertion.
- **DAS RT:** Provides the server-side functionality for Active Views.
- **DAS Aggregation:** Calculates event data summaries that are used in reports.
- **DAS iTRAC:** Provides the server-side functionality for the Sentinel iTRAC functionality.
- **DAS CMD:** Provides a command line interface to certain DAS services. Used primarily for third-party integration.
- **DAS Proxy:** Provides the server-side of the SSL proxy connection to Sentinel Server.

DAS Proxy is not directly part of the DAS collection of services. It is part of the Communication Server and does not directly connect to the database.

5.1.1 Reconfiguring Database Connection Properties

The primary settings in these configuration files that can be configured using the dbconfig utility are related to the database connection, including:

- username
- password
- hostname
- port number
- database (database name)
- server (oracle, oracle10g, or mssql)

If any of these database connection settings need to be changed, they must be changed in every `das_*.xml` file using the `dbconfig` utility. Using the –a argument, this utility can update all files at the same time (For example, update all files in the %ESEC_HOME%\config or $ESEC_HOME/config directory). Alternately, using the –n argument, this utility can update a single file's contents if only one file need to be updated. Typically, all files should be updated at the same time.

WARNING: Do not manually edit the database connection properties. Use the `dbconfig` utility to change any database connection values within these files.

To Reconfigure Database Connection Properties:

1. Login to the machine where DAS is installed as the esecadm user on UNIX or a user with administrative rights on Windows.
2. Go to:

   For Windows:

   ```
   %ESEC_HOME%\bin
   ```

   For UNIX:

   ```
   $ESEC_HOME/bin
   ```
3. Provide the following command:

   For Windows:

   ```
   dbconfig -a %ESEC_HOME%\config [[-u username] [-p password] | [-winAuth]] [-h
   hostname] [-t portnum] [-d database] [-s server] [-help] [-version]
   ```

   For UNIX:

   ```
   dbconfig -a $ESEC_HOME/config [-u username] [-p password] [-h hostname] [-t
   portnum] [-d database] [-s server] [-help] [-version]
   ```

NOTE: The -winAuth argument is available only on Windows and should be used instead of the `-u` and `-p` arguments if the Sentinel Application User is a Windows Authentication user.

Other settings in the files can be adjusted manually (without using dbconfig):

- maxConnections
- batchSize
- loadSize

Changing these settings might affect database performance and should be done with caution

5.1.2 DAS Logging Properties Configuration Files

The following files are used to configure logging of the DAS process. These files are typically changed when troubleshooting the DAS process.

- das_query_log.prop
- das_binary_log.prop
- das_rt_log.prop
- das_itrac_log.prop
- das_aggregation_log.prop
- das_cmd_log.prop
- das_proxy_log.prop

They are located in the following locations:

For Windows:

```
%ESEC_HOME%\config
```

For UNIX:

```
$ESEC_HOME/config
```

These files contain the configuration that determines how the DAS processes will log messages. The most important part of the configuration is the logging levels, which indicate how verbose the log messages should be. The section of the file to configure these settings is:

```
###### Configure the logging levels
# Logging level rules are read from the top down.
# Start with the most general, then get more specific.
#
# Defaults all loggers to INFO (enabled by default)
.level=INFO
#
# < Set level of specific loggers here >
#
# Turns off all logging (disabled by default)
#.level=OFF
######
```

NOTE: The logger `.level` is a wildcard logger name that refers to all loggers. Setting this logger's level will affect all loggers.

The available logging levels are:

- **OFF:** disables all logging
- **SEVERE (highest value):** indication that a component has malfunctioned or there is a loss/corruption of critical data
- **WARNING:** if an action can cause a component to malfunction in the future or if there is non-critical data loss/corruption
- **INFO:** audit information
- **CONFIG:** for debugging
- **FINE:** for debugging
- **FINER:** for debugging
- **FINEST:** (lowest value) – for debugging
- **ALL:** will log all levels

When one specifies a logging level, all log messages of that level and higher (in the above list) will actually be logged. For example, if one specifies the INFO level, then all INFO, WARNING and SEVERE message will be logged.

NOTE: At 10 second intervals, the logging properties file will be checked to see if any changes have occurred since it was last read. If the file has changed, the LogManagerRefreshService will re-read the logging properties file. Therefore, it is not necessary to restart the processes to begin using the updated logging levels.

Log messages are written to ESEC_HOME%\log (for Windows) or $ESEC_HOME/log (for UNIX), in the following files:

```
das_query_0.*.log
das_binary_0.*.log
das_itrac_0.*.log
das_aggregation0.*.log
das_rt0.*.log
das_cmd0.*.log
das_proxy0.*.log
```

The 0 indicates the unique number to resolve conflicts and the * indicates a generation number to distinguish rotated logs. For example, `das_query0.0.log` is the log with index 0 (latest) file in a rotated set of log files for the DAS Query process.

Log messages are also written to the process's console (standard output). However, since the processes are running as services, users do not have access to the console output. It is possible, however, to capture the console output in the `sentinel0.*.log file`. This is useful, for example, if the process is producing an error that is not printed to the process's own log file. This can be enabled by adding the following line to the `sentinel_log.prop` file:

```
esecurity.base.process.MonitorableProcess.level=FINEST
```

5.1.3 Certificate Management for DAS_Proxy

The DAS_Proxy SSL Server uses an asymmetric key pair, consisting of a certificate (or public key) and a private key, to encrypt communications. When the Sentinel Communication Server is started for the first time, it automatically creates a self-signed certificate which is used by the DAS_Proxy SSL Server.

You can replace the self-signed certificate with a certificate signed by a major Certificate Authority (CA), such as Verisign, Thawte (http://www.thawte.com/), or Entrust (http://www.entrust.com/). You can also replace the self-signed certificate with a certificate signed by a less common CA, such as a CA within your company or organization.

This section describes several certificate management tasks that you can perform in Sentinel:

- Replace the default certificate with a certificate signed by a Certificate Authority (CA)
- Change default keystore and keyEntry passwords. This is recommended on all Sentinel systems.
- Change the location of the .proxyServerKeystore file
- Change the default keyEntry alias to avoid potential conflicts with other keys in the keystore or for simplicity

Replacing the default certificate with a CA-signed certificate

Novell provides a self-signed certificate for the DAS_Proxy SSL Server to use. To improve security, you can replace the default, self-signed certificate that gets installed with a certificate signed by a Certificate Authority (CA). The CA may be a major CA, such as Verisign, Thawte (http://www.thawte.com/), or Entrust (http://www.entrust.com/), or it may be a less widely-known CA, such as one that is within your organization.

The basic steps are to get a CA to sign your certificate and then import that certificate into the keystore for DAS_Proxy to use. To import the certificate, the CA that signed the certificate must be "known" to the keytool utility. Keytool usually recognizes the major certificate authorities, but for other CA's you may need to import a certificate or chain of certificates for the certificate authority before you can successfully import the certificate that DAS_Proxy uses.

NOTE: These instructions are based on the user guide for keytool. For more information, see http://java.sun.com/j2se/1.5.0/docs/tooldocs/solaris/keytool.html (http://java.sun.com/j2se/1.5.0/docs/tooldocs/solaris/keytool.html)

To use a CA-signed certificate:

1 Execute the following command in the console:

```
$ESEC_HOME/jre/bin/keytool -list -keystore $ESEC_HOME/config/
.proxyServerKeystore
```

2 Provide the keystore password (star1111 by default). The contents of the keystore file display:

```
Keystore type: jks
Keystore provider: SUN
Your keystore contains 1 entry
10.0.0.1, Jan 8, 2008, keyEntry,
Certificate fingerprint (MD5): 22:B4:19:63:AC:2D:F9:C0:66:7F:7C:64:85:68:89:AB
```

The keyEntry alias, which is used in the following step, is the IP address in the example above. By default, the keyEntry alias can be the IP address or the host name of the local machine.

3 Execute the following command in the console using the keyEntry alias from .proxyServerKeystore:

```
$ESEC_HOME/jre/bin/keytool -certreq -alias <keyEntry alias> -keystore
$ESEC_HOME/config/.proxyServerKeystore -file <csr_filename.csr>
```

The .csr file is saved in the specified location.

4 Provide the `.csr` file to the CA. The CA will return a signed `.cer` file. (These exact steps will vary based on the Certificate Authority.)

5 If the CA is not well known, you must add the CA's certificate to the "cacerts" keystore using the following steps:

5a Open a command prompt and go to $ESEC_HOME/jre/lib/security. There should be a cacerts file in this directory.

5b Run the following command to import:

```
$ESEC_HOME/jre/bin/keytool -import -trustcacerts -alias
<a_ca_cert_alias_of_your_choosing> -keystore $ESEC_HOME/jre/lib/security/
cacerts -file <ca_cert_filename>
```

NOTE: The default password for this keystore file is "changeit".

5c Execute the preceding steps on the Sentinel Server machine, all Collector Manager systems that are connecting to the Sentinel Server through the SSL Proxy, and all Sentinel Control Center systems.

6 To enable the use of CA signed certificate, edit das_proxy.xml file available on the Sentinel Server. Change the property value to true:

```
<property name="usecacerts">true</property>
```

7 Edit the configuration.xml file on all system with Sentinel Control Center and add the following attribute to the “ssl” element of the “proxied_client” and “proxied_trusted_client” strategies:

```
usecacerts="true"
```

For example:

```
<strategy active="yes" id="proxied_client"
location="com.esecurity.common.communication.strategy.proxystrategy.ProxiedCl
ientStrategyFactory">
<transport type="ssl">
<ssl host="hostname" keystore=”Path of .proxyClientKeystore” port="10013"
usecacerts="true"/>
</transport>
</strategy>
<strategy active="yes" id="proxied_trusted_client"
location="com.esecurity.common.communication.strategy.proxystrategy.ProxiedCl
ientStrategyFactory">
<transport type="ssl">
<ssl host="hostname" keystore=”Path of .proxyClientKeystore” port="10014"
usecacerts="true"/>
</transport>
</strategy>
```

NOTE: The default property of `usecacerts` is false. You must change the property of `usecacerts` to true.

8 Import the `.cer` file into keystore file by executing the following command:

```
$ESEC_HOME/jre/bin/keytool -import -trustcacerts -alias <keyEntry alias> -
keystore $ESEC_HOME/config/.proxyServerKeystore -file <cer_filename.cer>
```

This will replace the self-signed certificate installed with Sentinel.

9 Restart Sentinel Server.

Novell also recommends that you change the keystore and keyEntry passwords after replacing the certificate.

Changing default keystore and keyEntry passwords

By default, the passwords used for keystore and the keyEntry are both set to star1111. It is a good practice to change these to something new.

NOTE: DAS_Proxy requires that the keystore and keyEntry passwords to be identical.

To change the keystore and the keyEntry password:

1 Execute the following command in the console to change the keystore password:

```
$ESEC_HOME/jre/bin/keytool -storepasswd -keystore $ESEC_HOME/config/
.proxyServerKeystore
```

2 Enter the old keystore password (star1111 by default) and a new keystore password. The following example depicts this:

```
Enter keystore password: <old_pass>
New keystore password: <new_pass>
Re-enter new keystore password: <new_pass>
```

3 Verify the keyEntry alias using the following command:

```
$ESEC_HOME/jre/bin/keytool -list -keystore $ESEC_HOME/config/
.proxyServerKeystore
```

Provide the current keystore password. The contents of the keystore file display:

```
Keystore type: jks
Keystore provider: SUN
Your keystore contains 1 entry
10.0.0.1, Jan 8, 2008, keyEntry,
Certificate fingerprint (MD5): 22:B4:19:63:AC:2D:F9:C0:66:7F:7C:64:85:68:89:AB
```

The keyEntry alias is the IP address in the example above. By default, the keyEntry alias is either set to the IP address or the hostname of the local machine.

4 Execute the following command in the console to change the keyEntry password to the same password as the new keystore password:

```
$ESEC_HOME/jre/bin/keytool -keypasswd -alias <keyEntry alias> -keystore
$ESEC_HOME/config/.proxyServerKeystore
```

5 Enter the existing password and the new password. The following example depicts this:

```
Enter keystore password: <new_pass>
Enter key password for <keyEntry alias> <old_pass>
New key password for <keyEntry alias>: <new_pass>
Re-enter new key password for <keyEntry alias>: <new_pass>
```

NOTE: Remember that the keyEntry password and keystore password must be identical.

---

6 Get the encrypted, Base64 value of the new password using the following steps:

- Copy ESEC_HOME/config/das_rt.xml to a file named `temp.xml`:
- Execute the following command to add an encrypted, Base 64 form of the password to `temp.xml` file:

  ```
  $ESEC_HOME/bin/dbconfig -n $ESEC_HOME/config/temp.xml -p <new password for
  keystore and keyEntry>
  ```

- Open `temp.xml` file.
- Copy the value of "password" from the following section of the file: `<property name="password">BSEU8ew2JYsxtOt4hYcYNA==</property>`
- Delete the `temp.xml` file when you are confident that you have successfully copied the encrypted password.

7 Open the das_proxy.xml file.

8 Paste the copied value of the new password to the "keystorePassword" property in the "ProxyService" component property as shown below:

```
<obj-component id="ProxyService">
<class>esecurity.ccs.comp.clientproxy.ClientProxyService</class>
      <property name="clientports">ssl:10013</property>
      <property name="certclientports">ssl:10014</property>
      <property name="keystore"> ../config/.proxyServerKeystore</property>
      <property name="keystorePassword"> BSEU8ew2JYsxtOt4hYcYNA==</property>
    </obj-component>
```

9 Save the `das_proxy.xml` file.

10 Restart Sentinel Server.

Using a new .proxyServerKeystore location

By default the certificate and private key are stored in the file `.proxyServerKeystore` located at `$ESEC_HOME/config`. To change the location of `.proxyServerKeystore` file, you can edit the value of the property “keystore” in the file `$/ESEC_HOME/config/das_proxy.xml`.

You must restart Sentinel Server after making changes.

Using a new keyEntry alias

The default keyEntry alias is either the IP address or the hostname of the local machine. To use a different keyEntry alias, open the das_proxy.xml file and set the value of “certificateAlias” in the component “ProxyService” to the new value.

You must restart Sentinel Server after making changes.

Sentinel Accounts and Password Changes

6

This section discusses users that are created or used during Sentinel installation and normal Sentinel operations. Unless you create domain users in advance in order to use Windows Authentication, these users are created by the Sentinel installer. These user accounts are used for Sentinel's normal operations, such as event inserts into the Sentinel database.

The administrator might select to occasionally change the passwords for these accounts. To ensure continued normal Sentinel operations, there are special procedures necessary to update the passwords in all necessary locations.

6.1 Sentinel Default Users

This section discusses about Sentinel default users.

6.1.1 Native Database Authentication

Installer creates several users during installation if you use native database authentication (Oracle or Microsoft SQL Server). These users are all created as database users in the Oracle or SQL Server database, and the passwords are configurable at install time. The installer will create the users with the following default names:

- **esecdba:** Schema owner
- **esecadm:** Sentinel administrator
- **esecrpt:** Reporter user, same password as the admin user
- **esecapp:** Sentinel application user. Used by Sentinel Server to connect to the database

In addition to creating a database user for the Sentinel administrator, the installer also creates a Sentinel user with the same username and password for the Sentinel Control Center. For UNIX only, the installer creates an operating system user with no password set. To log in as this user, the UNIX administrator must set a password or su to the user as root.

6.1.2 Windows Authentication

If you use Windows authentication, the Windows administrator must create several domain accounts before the installation is started. The credentials for these accounts must be given during the Sentinel installation:

- **Sentinel DB Administrator:** Schema owner
- **Sentinel Administrator:** Sentinel administrator
- **Sentinel Report User:** Reporter user, same password as the admin user.
- **Sentinel Application User:** Sentinel application username for connecting to the database.

Windows Authentication users are supported only when SQL Server is being used and DAS is running on Windows.

6.2 Password Changes

Corporate policy might require that passwords be changed on a regular schedule. Sentinel user passwords can be changed using database utilities. After changing a password, some Sentinel components need to be updated to use the new password.

6.2.1 Changing Password

This section discusses about changing password

SQL Server Accounts

On Windows, this procedure can be used to change the password for the Sentinel Application User, the Sentinel Database User, or the Sentinel Report User. To change the password for the Sentinel Administrator or other Sentinel Control Center user, see Section 6.2.1, “Changing Password,” on page 62.

To change password in MS SQL Server Management Studio:

1. Open the MS SQL Enterprise Manager/ MS SQL and select Security > Logins.
2. Right-click a username from the right pane and select properties.
3. Change the password. Click OK.

   Follow the procedures in Sentinel updates after a password change.

Oracle Accounts

This procedure can be used to change the password for the Sentinel Application User, the Sentinel Database User, or the Sentinel Report User. To change the password for the Sentinel Administrator or other Sentinel Control Center user, see Section 6.2.1, “Changing Password,” on page 62.

To change password in Oracle:

1. Connect to Oracle Enterprise Manager with user having sysdba privilege.
2. Select your specific database from the left pane.
3. In Database > Security > Users, select a user for which you want to change the password.
4. Provide new password and confirm the password. Click Apply.

   Follow the procedures in Sentinel updates after a password Change.

Windows Domain Accounts

If the Sentinel system uses domain user accounts and Windows Authentication, use the following password change procedures. These procedures can be used for the Sentinel Administrator, the Sentinel Database User, the Sentinel Report User, and the Sentinel Application User. It can also be used for any Sentinel Control Center account that uses Windows Authentication.

To change the password for Windows domain accounts:

1. Log into a machine using the account and use standard Windows password change procedures

   or

Request a password change from a Windows administrator.

2 Follow the procedures in Sentinel updates after a password change.

Sentinel Control Center Accounts (Native DB Authentication)

This procedure can be used to change the password for the Sentinel Administrator account or any other Sentinel Control Center user.

To change the Sentinel Administrator password:

1 Login to the Sentinel Control Center as the Sentinel Administrator or another user with User Management permissions.

2 Click Admin > User Configuration. The User Manager window displays.

3 Double-click esecadm user account or right-click User Details.

4 Modify the account password and confirm password. Click OK.

No additional updates are needed in the Sentinel system.

Sentinel Control Center Accounts (Windows Authentication)

Use standard procedures for changing the password for Windows domain accounts.

6.2.2 Sentinel Updates After a Password Change

The passwords for certain Sentinel users, such as the Sentinel Database User and the Sentinel Application User, are encrypted and stored in configuration files and used in normal Sentinel operations. These configuration files must be updated after the passwords are changed.

Updating Sentinel Application User Password

The Sentinel Application User credentials are stored encrypted in the container xml files. After a password change, these files must be updated for Sentinel to continue working.

The procedures are different depending on whether the Sentinel Application User uses Native Database Authentication or Windows Authentication.

To update the Sentinel Application User password (Native DB Authentication):

1 Change the password for the Sentinel Application User (esecapp by default) using database utilities as described in Section 6.2.1, “Changing Password,” on page 62.

2 Using the dbconfig utility, update all container xml files. This is required because these xml files store the (encrypted) esecapp password to allow DAS and Advisor to connect to the database.

The container xml files are located in the following locations:

For Windows:

```
%ESEC_HOME%\config
```

For Oracle:

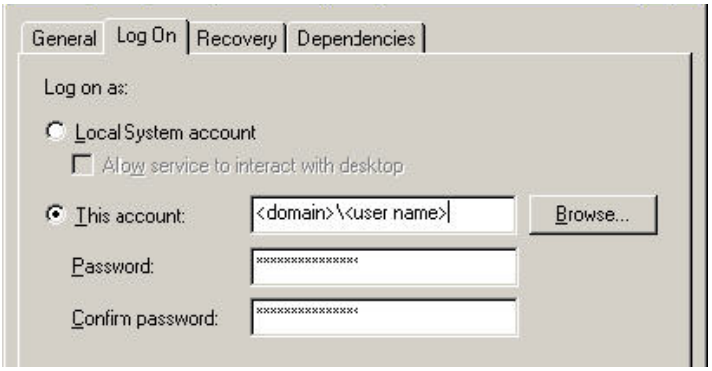
```
$ESEC_HOME/config
```

For more information on usage of the dbconfig utility, see Chapter 5, “Sentinel Data Access Service,” on page 53.

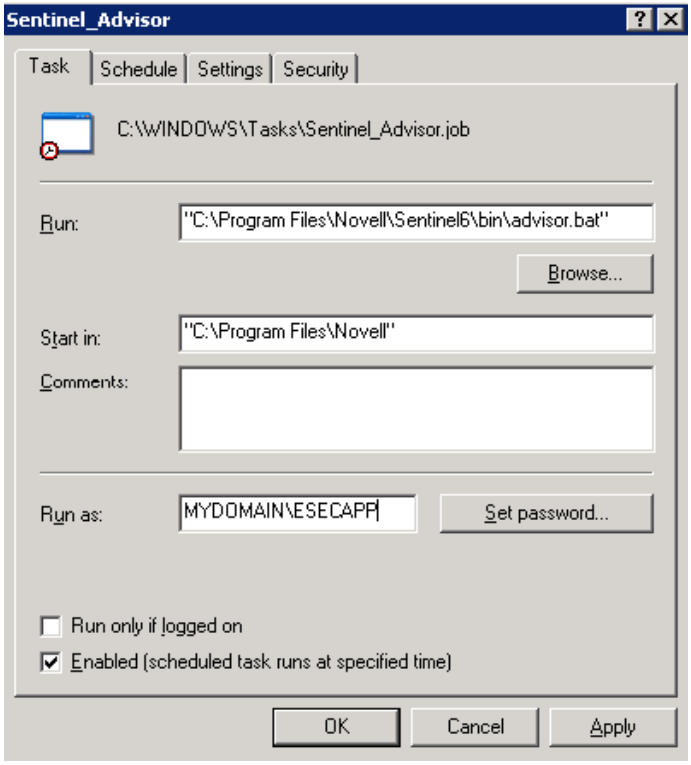
```
dbconfig -a {$ESEC_HOME/config | %ESEC_HOME%\config} -p <password>
```

To update the Sentinel Application User password (Windows Authentication):

1. Change the password for the Sentinel Application User domain account as described in Section 6.2.1, “Changing Password,” on page 62.
2. On your DAS machine, open Windows Services (Control Panel > Administrative Tools > Services).
3. Right-click Sentinel > Properties. Click the Log On tab and update Log on as password. Click Apply and click OK.



4. If you have Advisor installed, you will need to update the Run as property (Control Panel > Scheduled Tasks > right-click Properties) of the Advisor Scheduled task(s).



5 Click Set password. Provide the new password twice and click OK. Click Apply and click OK.

Updating Sentinel Database User Password

These password change procedures are only necessary if extra Sentinel Data Manager jobs have been created and scheduled or the Sentinel Data Manager command line interface is being used.

To change Sentinel DB Administrator password (Windows Authentication):

1 Use the Windows Operating System to change the password as described in Section 6.2.1, “Changing Password,” on page 62.

2 If you are running any SDM command line scheduled tasks in your environment, you will need to update the Run as property (Control Panel > Scheduled Tasks > right-click Properties).

3 Click Set password. Provide the new password twice and click OK. Click Apply and click OK.

To update the Sentinel DB Administrator password (Native DB Authentication):

1 Change the password for the Sentinel DB Administrator User (esec by default) using database utilities password as described in Section 6.2.1, “Changing Password,” on page 62.

2 In order for automated SDM command line tasks to continue to work (if applicable in your environment), update the dbPass in the sdm.connect file with the new esecdba password using the SDM GUI or command line. For more information, see “Sentinel Data Manager” in *Sentinel 6.1 User Guide*.

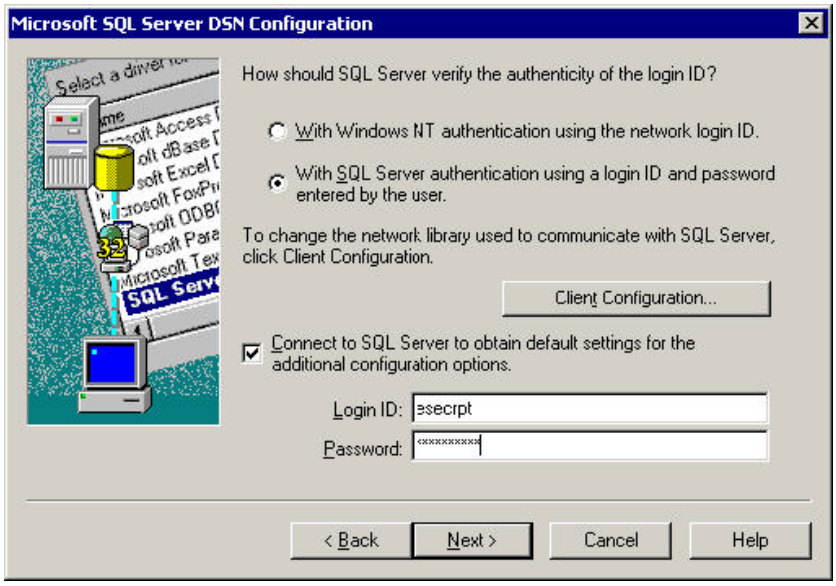
```
sdm -action saveConnection -server <oracle/mssql> -host <hostIp/hostName> -
port <portnum> -database <databaseName/SID> [-driverProps <propertiesFile>] {-
user <dbUser> -password <dbPass>} -connectFile <filenameToSaveConnection>
```

Updating Sentinel Report User Password

This procedure is only necessary for Crystal on Windows. For Crystal on Linux, no changes are necessary.

To update the Sentinel Report User password for Crystal on Windows:

1. Change the password for the Sentinel Report User (esecrpt by default) using database utilities as described in Section 6.2.1, “Changing Password,” on page 62.
2. Log into the Crystal Server machine.
3. Go to Control Panel > Administrative Tools >Data Sources (ODBC) to update the ODBC Data Source Name (DSN).
4. Under the System DSN tab, highlight sentineldb and click Configure.
5. Click Next. Update the password.



6. Click Next until you get a Finish button. Click Finish.

Sentinel Database Views for Oracle

7

This section lists the Sentinel Schema Views for Oracle. The views provide information for developing your own reports (Crystal Reports).

7.1 Views

Below listed are the views available with Sentinel.

7.1.1 ACTVY_PARM_RPT_V

View contains information about iTRAC activities.

Column Name	Datatype	Comment
ACTVY_PARM_ID	varchar2(36)	Activity parameter identifier
ACTVY_ID	varchar2(36)	Activity identifier
PARM_NAME	varchar2(255)	Activity Parameter name
PARM_TYP_CD	varchar2(1)	Activity parameter type code
DATA_TYP	varchar2(50)	Activity parameter data type
DATA_SUBTYP	varchar2(50)	Activity parameter data subtype
RQRD_F	number (1,0)	Required flag
PARM_DESC	varchar2(255)	Activity parameter description
PARM_VAL	varchar2(1000)	Activity parameter value
FORMATTER	varchar2(255)	Activity parameter formatter
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number (38,0)	User who created object
MODIFIED_BY	number (38,0)	User who last modified object

7.1.2 ACTVY_REF_PARM_VAL_RPT_V

View contains information about iTRAC activities.

Column Name	Datatype	Comment
ACTVY_ID	varchar2(36)	Activity identifier
ACTVY_PARM_ID	varchar2(36)	Activity parameter identifier

Column Name	Datatype	Comment
CREATED_BY	number(38,0)	User who created object
DATE_CREATED	Date	Date the entry was created
DATE_MODIFIED	Date	Date the entry was modified
MODIFIED_BY	number(38,0)	User who last modified object
PARM_VAL	varchar2(1000)	Activity parameter value
SEQ_NUM	number(38,0)	Sequence number

7.1.3 ACTVY_REF_RPT_V

View contains information about iTRAC activities.

Column Name	Datatype	Comment
ACTVY_ID	varchar2(36)	Activity identifier
SEQ_NUM	number(38,0)	Sequence number
REFD_ACTVY_ID	varchar2(36)	Referenced activity identifier
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object

7.1.4 ACTVY_RPT_V

View contains information about iTRAC activities

Column Name	Datatype	Comment
ACTVY_ID	varchar2(36)	Activity identifier
ACTVY_NAME	varchar2(255)	Activity name
ACTVY_TYP_CD	varchar2(1)	Activity type code
ACCESS_LVL	varchar2(50)	Access level
EXEC_LOC	varchar2(50)	Execution location
ACTVY_DESC	varchar2(255)	Activity description
PROCESSOR	varchar2(255)	Processor
INPUT_FORMATTER	varchar2(255)	Input formatter
OUTPUT_FORMATTER	varchar2(255)	Output formatter
APP_NAME	varchar2(25)	Application name

Column Name	Datatype	Comment
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object

7.1.5 ADV_ATTACK_MAP_RPT_V

View references ADV_ATTACK_MAP table that stores Advisor map information.

Column Name	Datatype	Comment
ATTACK_KEY	number	ID used to reference the attack entry
SERVICE_PACK_ID	number	ID used to reference the attack entry
ATTACK_NAME	varchar2(256)	Name of the Attack
ATTACK_CODE	varchar2(256)	Attack code
DATE_PUBLISHED	date	Date the attack has been published
DATE_UPDATED	date	Date the attack has been updated
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.6 ADV_ATTACK_PLUGIN_RPT_V

View references ADV_ATTACK_PLUGIN table that stores Advisor plug-in information.

Column Name	Datatype	Comment
PLUGIN_KEY	number	ID used to reference the vulnerability entry
SERVICE_PACK_ID	number	ID of the vulnerability
PLUGIN_ID	varchar2(256)	ID used to reference the vulnerability entry
PLUGIN_NAME	varchar2(256)	Name of the vulnerability
DATE_PUBLISHED	date	Date the vulnerability has been published
DATE_UPDATED	date	Date the vulnerability has been updated
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object

Column Name	Datatype	Comment
MODIFIED_BY	number	User who last modified object

7.1.7 ADV_ATTACK_RPT_V

View references ADV_ATTACK table that stores Advisor attack information.

Column Name	Datatype	Comment
ATTACK_ID	number	ID to identify the attack
TRUSECURE_ATTACK_NAME	varchar2(512)	Name of the attack
FEED_DATE_CREATED	date	Date when the feed first have the information on this attack
FEED_DATE_UPDATED	date	Last date when the information on this attack has been updated
ATTACK_CATEGORY	varchar2(256)	Category of the attack
URGENCY_ID	number	The urgency associated with this attack
SEVERITY_ID	number	Severity associated with this attack
LOCAL	number	Indicates if this attack was executed locally
REMOTE	number	Indicates if this attack was executed from remote
DESCRIPTION	clob	Impact of the attack
SCENARIO	clob	Safeguards that could be followed to avert the attack
IMPACT	clob	Patches for the product to fix the vulnerability exploited by the attack
SAFEGUARDS	clob	False Positives associated with this attack
PATCHES	clob	Date the information on this attack was published
FALSE_POSITIVES	clob	Date the information on this attack was updated
DATE_PUBLISHED	date	ID to identify the attack
DATE_UPDATED	date	Name of the attack
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	By user ID
MODIFIED_BY	number	By user ID

7.1.8 ADV_ATTACK_SIGNATURES

Column Name	Datatype	Comment
ATTACK_KEY	number	Attack ID
ATTACK_SCANNER_NAME	varchar2(128)	Name of the attack scanner or intrusion detection system
ATTACK_NAME	varchar2(256)	Name of the attack
ATTACK_ID	varchar2(256)	ID of the attack

7.1.9 ADV_FEED_RPT_V

View references ADV_FEED table that stores Advisor feed information, such as feed name and date.

Column Name	Datatype	Comment
FEED_NAME	varchar2(128)	Name of feed
FEED_FILE	varchar2(256)	File name that contains the feed data
BEGIN_DATE	date	The date from which this feed file carries the advisor information
END_DATE	date	The date until which this feed file carries the advisor information
FEED_INSERT	number	Number of rows inserted into the advisor schema by this feed file
FEED_UPDATE	number	Number of rows updated into the advisor schema by this feed file
FEED_EXPIRE	number	Number of rows deleted into the advisor schema by this feed file

7.1.10 ADV_MASTER_RPT_V

Column Name	Datatype	Comment
MASTER_ID	number	ID that associates PLUGIN_KEY, ATTACK_KEY and VULN_KB_ID
PLUGIN_KEY	number	ID to reference the ADV_ATTACK_PLUGIN_V
ATTACK_KEY	number	ID to reference the ADV_ATTACK_MAP_V
VULN_KB_ID	number	ID to reference the VULN_KB_ID_V
DATE_PUBLISHED	date	Date the entry was published
DATE_UPDATED	date	Date the entry was updated

Column Name	Datatype	Comment
BEGIN_EFFECTIVE_DATE	date	Date from which the entry is valid
END_EFFECTIVE_DATE	date	Date until which the entry is valid
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.11 ADV_PRODUCT_RPT_V

View references ADV_PRODUCT table that stores Advisor product information such as vendor and product ID.

Column Name	Datatype	Comment
PRODUCT_ID	number	ID of the product
VENDOR_ID	number	ID of the vendor
PRODUCT_CATEGORY_ID	number	ID of the Product Category
PRODUCT_CATEGORY_NAME	varchar2(128)	Product Category Name
PRODUCT_TYPE_ID	integer	ID of the product type
PRODUCT_TYPE_NAME	varchar2(256)	Name of the Product Type
PRODUCT_NAME	varchar2(128)	Product Name
PRODUCT_DESCRIPTION	varchar2(512)	Product Descritpion
FEED_DATE_CREATED	date	Date of the Feed that carried information on this product
FEED_DATE_UPDATED	date	Date of the Feed that updated information on this product
ACTIVE_FLAG	number	Reserved for future use
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.12 ADV_PRODUCT_SERVICE_PACK_RPT_V

View references ADV_PRODUCT_SERVICE _PACK table that stores Advisor service pack information, such as service pack name, version ID and date.

Column Name	Datatype	Comment
SERVICE_PACK_ID	number	Service Pack ID
VERSION_ID	number	Version ID
SERVICE_PACK_NAME	varchar2(32)	Name of the Service Pack
FEED_DATE_CREATED	date	Date of the Feed that carried information on this product
FEED_DATE_UPDATED	date	Date of the Feed that updated information on this product
ACTIVE_FLAG	number	Reserved for future use
BEGIN_EFFECTIVE_DATE	date	Date from which the entry is valid
END_EFFECTIVE_DATE	date	Date until which the entry is valid
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.13 ADV_PRODUCT_VERSION_RPT_V

View references ADV_PRODUCT_VERSION table that stores Advisor product version information, such as version name, product and version ID.

Column Name	Datatype	Comment
VERSION_ID	number	Version ID
PRODUCT_ID	number	Product ID
VERSION_NAME	varchar2(128)	Version Name of the product
FEED_DATE_CREATED	date	Date of the feed that carried the information on the entry
FEED_DATE_UPDATED	date	Date of the feed that carried the update on the entry
ACTIVE_FLAG	number	Reserved for future use
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.14 ADV_VENDOR_RPT_V

View references ADV_VENDOR table that stores Advisor address information.

Column Name	Datatype	Comment
VENDOR_ID	number	ID of the vendor
VENDOR_NAME	varchar2(128)	Name of the vendor
CONTACT_PERSON	varchar2(128)	Contains the contact person name for the vendor
ADDRESS_LINE_1	varchar2(128)	Address of the vendor
ADDRESS_LINE_2	varchar2(128)	Address of the vendor
ADDRESS_LINE_3	varchar2(128)	Address of the vendor
ADDRESS_LINE_4	varchar2(128)	Address of the vendor
CITY	varchar2(128)	City of the vendor
STATE	varchar2(128)	State of the vendor
COUNTRY	varchar2(128)	Country of the vendor
ZIP_CODE	varchar2(128)	Zip code of the vendor
URL	varchar2(256)	Web URL of the vendor
PHONE	varchar2(32)	Contact number of the vendor
FAX	varchar2(32)	Fax number of the vendor
EMAIL	varchar2(128)	Email of the vendor
PAGER	varchar2(32)	Pager of the vendor
FEED_DATE_CREATED	date	Date of the feed that carried the information on the entry
FEED_DATE_UPDATED	date	Date of the feed that carried the update on the entry
ACTIVE_FLAG	number	Reserved for future use
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.15 ADV_VULN_KB_RPT_V

Column Name	Datatype	Comment
VULN_KB_ID	number	Knowledge base ID mapping CVE_ID, OSVDB_ID, BUGTRAQ_ID
CVE_ID	varchar2(10)	CVE ID for the related vulnerability
OSVDB_ID	number	OSVDB ID for the related vulnerability

Column Name	Datatype	Comment
BUGTRAQ_ID	number	Bugtraq id for the related vulnerability
DATE_PUBLISHED	date	Date the entry was published
DATE_UPDATED	date	Date the entry was updated
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.16 ADV_VULN_PRODUCT_RPT_V

View references ADV_VULN_PRODUCT table that stores Advisor vulnerability attack ID and service pack ID.

Column Name	Datatype	Comment
SERVICE_PACK_ID	number	Contains the service pack id
ATTACK_ID	number	Contains the attack id
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.17 ADV_VULN_SIGNATURES

Column Name	Datatype	Comment
VULN_KEY	number	Vulnerability key
VULN_SCANNER_NAME	varchar2(128)	Vulnerability scanner name
VULN_NAME	varchar2(256)	Vulnerability name
VULN_ID	varchar2(256)	Vulnerability ID

7.1.18 ANNOTATIONS_RPT_V

View references ANNOTATIONS table that stores documentation or notes that can be associated with objects in the Sentinel system such as cases and incidents.

Column Name	Datatype	Comment
ANN_ID	number	Annotation identfier - sequence number.

Column Name	Datatype	Comment
TEXT	varchar2(4000)	Documentation or notes.
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
MODIFIED_BY	number	User who last modified object
CREATED_BY	number	User who created object
ACTION	varchar2(255)	Action

7.1.19 ASSET_CATEGORY_RPT_V

View references ASSET_CTGRY table that stores information about asset categories

Column Name	Datatype	Comment
ASSET_CATEGORY_ID	number(38)	Asset category identifier
ASSET_CATEGORY_NAME	varchar2(100)	Asset category name
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.20 ASSET_HOSTNAME_RPT_V

View references ASSET_HOSTNAME table that stores information about alternate host names for assets.

Column Name	Datatype	Comment
ASSET_HOSTNAME_ID	varchar2(36)	Asset alternate hostname identifier
PHYSICAL_ASSET_ID	varchar2(36)	Physical asset identifier
HOST_NAME	varchar2(255)	Host name
CUST_ID	number(38)	Customer identifier
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.21 ASSET_IP_RPT_V

View references ASSET_IP table that stores information about alternate IP addresses for assets.

Column Name	Datatype	Comment
ASSET_IP_ID	varchar2(36)	Asset alternate IP identifier
PHYSICAL_ASSET_ID	varchar2(36)	Physical asset identifier
IP_ADDRESS	number(38)	Asset IP address
CUST_ID	number(38)	Customer identifier
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.22 ASSET_LOCATION_RPT_V

View references ASSET_LOC table that stores information about asset locations.

Column Name	Datatype	Comment
LOCATION_ID	number(38)	Location identifier
CUST_ID	number(38)	Customer identifier
BUILDING_NAME	varchar2(255)	Building name
ADDRESS_LINE_1	varchar2(255)	Address line 1
ADDRESS_LINE_2	varchar2(255)	Address line 2
CITY	varchar2(100)	City
STATE	varchar2(100)	State
COUNTRY	varchar2(100)	Country
ZIP_CODE	varchar2(50)	Zip code
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.23 ASSET_RPT_V

View references ASSET table that stores information about the physical and soft assets.

Column Name	Datatype	Comment
ASSET_ID	varchar2(36)	Asset identifier
CUST_ID	number(38)	Customer identifier

Column Name	Datatype	Comment
ASSET_NAME	varchar2(255)	Asset name
PHYSICAL_ASSET_ID	varchar2(36)	Physical asset identifier
PRODUCT_ID	number(38)	Product identifier
ASSET_CATEGORY_ID	number(38)	Asset category identifier
ENVIRONMENT_IDENTITY_ID	number(38)	Environment identify code
PHYSICAL_ASSET_IND	number(1)	Physical asset indicator
ASSET_VALUE_ID	number(38)	Asset value code
CRITICALITY_ID	number(38)	Asset criticality code
SENSITIVITY_ID	number(38)	Asset sensitivity code
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.24 ASSET_VALUE_RPT_V

View references ASSET_VAL_LKUP table that stores information about the asset value.

Column Name	Datatype	Comment
ASSET_VALUE_ID	number(38)	Asset value code
ASSET_VALUE_NAME	varchar2(50)	Asset value name
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.25 ASSET_X_ENTITY_X_ROLE_RPT_V

View references ASSET_X_ENTITY_X_ROLE table that associates a person or an organization to an asset.

Column Name	Datatype	Comment
PERSON_ID	varchar2(36)	Person identifier
ORGANIZATION_ID	varchar2(36)	Organization identifier
ROLE_CODE	varchar2(5)	Role code
ASSET_ID	varchar2(36)	Asset identifier

Column Name	Datatype	Comment
ENTITY_TYPE_CODE	varchar2(5)	Entity type code
PERSON_ROLE_SEQUENCE	number(38)	Order of persons under a particular role
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.26 ASSOCIATIONS_RPT_V

View references ASSOCIATIONS table that associates users to incidents, incidents to annotations and so on.

Column Name	Datatype	Comment
TABLE1	varchar2(64)	Table name 1. For example, incidents
ID1	varchar2(36)	ID1. For example, incident ID.
TABLE2	varchar2(64)	Table name 2. For example, users.
ID2	varchar2(36)	ID2. For example, user ID.
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.27 ATTACHMENTS_RPT_V

View references ATTACHMENTS table that stores attachment data.

Column Name	Datatype	Comment
ATTACHMENT_ID	number	Attachment identifier
NAME	varchar2(255)	Attachment name
SOURCE_REFERENCE	varchar2(64)	Source reference
TYPE	varchar2(32)	Attachment type
SUB_TYPE	varchar2(32)	Attachment subtype
FILE_EXTENSION	varchar2(32)	File extension
ATTACHMENT_DESCRIPTION	varchar2(255)	Attachment description
DATA	clob	Attachment data
DATE_CREATED	date	Date the entry was created

Column Name	Datatype	Comment
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.28 AUDIT_RECORD_RPT_V

View references AUDIT_RECORD table that stores Sentinel internal audit data.

Column Name	Datatype	Comment
AUDIT_ID	varchar2(36)	Audit record identifier
AUDIT_TYPE	varchar2(255)	Audit type
SRC	varchar2(255)	Audit source
SENDER_HOSTNAME	varchar2(255)	Sender hostname
SENDER_HOST_IP	varchar2(255)	Sender host IP
SENDER_CONTAINER	varchar2(255)	Sender container name
SENDER_ID	varchar2(255)	Sender Identifier
CLIENT	varchar2(255)	Client application that requested audit
EVT_NAME	varchar2(255)	Event name
RES	varchar2(255)	Event resource
SRES	varchar2(255)	Event sub-resource
MSG	varchar2(500)	Event message
CREATED_BY	number(0)	User who created object
MODIFIED_BY	number(0)	User who last modified object
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified

7.1.29 CONFIGS_RPT_V

View references CONFIGS table that stores general configuration information of the application.

Column Name	Datatype	Comment
USR_ID	varchar2(32)	User name.
APPLICATION	varchar2(255)	Application identifier
UNIT	varchar2(64)	Application unit
VALUE	varchar2(255)	Text value if any

Column Name	Datatype	Comment
DATA	clob	XML data
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.30 CONTACTS_RPT_V

View references CONTACTS table that stores contact information.

Column Name	Datatype	Comment
CNT_ID	number	Contact ID - Sequence number
FIRST_NAME	varchar2(20)	Contact first name.
LAST_NAME	varchar2(30)	Contact last name.
TITLE	varchar2(128)	Contact title
DEPARTMENT	varchar2(128)	Department
PHONE	varchar2(64)	Contact phone
EMAIL	varchar2(255)	Contact email
PAGER	varchar2(64)	Contact pager
CELL	varchar2(64)	Contact cell phone
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.31 CORRELATED_EVENTS_RPT_V (legacy view)

This view is provided for backward compatibility. New reports should use CORRELATED_EVENTS_RPT_V1.

7.1.32 CORRELATED_EVENTS_RPT_V1

View contains current and historical correlated events (correlated events imported from archives).

Column Name	Datatype	Comment
PARENT_EVT_ID	varchar2(36)	Event Universal Unique Identifier (UUID) of parent event

Column Name	Datatype	Comment
CHILD_EVT_ID	varchar2(36)	Event Universal Unique Identifier (UUID) of child event
PARENT_EVT_TIME	date	Parent event time
CHILD_EVT_TIME	date	Child event time
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.33 CRITICALITY_RPT_V

View references CRIT_LKUP table that contains information about asset criticality.

Column Name	Datatype	Comment
CRITICALITY_ID	number(38)	Asset criticality code
CRITICALITY_NAME	varchar2(50)	Asset criticality name
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.34 CUST_HIERARCHY_V

View references CUST_HIERARCHY table that stores information about MSSP customer hierarchy.

Column Name	Datatype	Comment
CUST_HIERARCHY_ID	number(38)	Customer hierarchy ID
CUST_NAME	varchar2(255)	Customer
CUST_HIERARCHY_LVL1	varchar2(255)	Customer hierarchy level 1
CUST_HIERARCHY_LVL2	varchar2(255)	Customer hierarchy level 2
CUST_HIERARCHY_LVL3	varchar2(255)	Customer hierarchy level 3
CUST_HIERARCHY_LVL4	varchar2(255)	Customer hierarchy level 4
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object

Column Name	Datatype	Comment
MODIFIED_BY	number	User who last modified object

7.1.35 CUST_RPT_V

View references CUST table that stores customer information for MSSPs.

Column Name	Datatype	Comment
CUST_ID	number(38)	Customer identifier
CUSTOMER_NAME	varchar2(255)	Customer name
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.36 ENTITY_TYPE_RPT_V

View references ENTITY_TYP table that stores information about entity types (person, organization).

Column Name	Datatype	Comment
ENTITY_TYPE_CODE	varchar2(5)	Entity type code
ENTITY_TYPE_NAME	varchar2(50)	Entity type name
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.37 ENV_IDENTITY_RPT_V

View references ENV_IDENTITY_LKUP table that stores information about asset environment identity.

Column Name	Datatype	Comment
ENVIRONMENT_IDENTITY_ID	number(38)	Environment identity code
ENV_IDENTITY_NAME	varchar2(255)	Environment identity name
DATE_CREATED	Date	Date the entry was created
DATE_MODIFIED	Date	Date the entry was modified

Column Name	Datatype	Comment
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.38 ESEC_CONTENT_GRP_CONTENT_RPT_V

View contains information about Solution Packs.

Column Name	Datatype	Comment
CONTENT_GRP_ID	varchar2(36)	Content group identifier
CONTENT_ID	varchar2(255)	Content identifier
CONTENT_TYP	varchar2(100)	Content type
CONTENT_HASH	varchar2(255)	Content hash
DATE_CREATED	Date	Date the entry was created
DATE_MODIFIED	Date	Date the entry was modified
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object

7.1.39 ESEC_CONTENT_GRP_RPT_V

View contains information about Solution Packs.

Column Name	Datatype	Comment
CONTENT_GRP_ID	varchar2(36)	Content group identifier
CONTENT_GRP_NAME	varchar2(255)	Content group name
CONTENT_GRP_DESC	Clob	Content group description
CTRL_ID	varchar2(36)	Control identifier
CONTENT_EXTERNAL_ID	varchar2(255)	Content external identifier
DATE_CREATED	Date	Date the entry was created
DATE_MODIFIED	Date	Date the entry was modified
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object

7.1.40 ESEC_CONTENT_PACK_RPT_V

View contains information about Solution Packs.

Column Name	Datatype	Comment
CONTENT_PACK_ID	varchar2(36)	Content pack identifier
CONTENT_PACK_DESC	Clob	Content pack description
CONTENT_PACK_NAME	varchar2(255)	Content pack name
CONTENT_EXTERNAL_ID	varchar2(255)	Content external identifier
DATE_MODIFIED	Date	Date the entry was modified
DATE_CREATED	Date	Date the entry was created
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object

7.1.41 ESEC_CONTENT_RPT_V

View contains information about Solution Packs.

Column Name	Datatype	Comment
CONTENT_PACK_ID	varchar2(36)	Content pack identifier
CONTENT_ID	varchar2(255)	Content identifier
CONTENT_NAME	varchar2(255)	Content name
CONTENT_STATE	number(38,0)	Content state
CONTENT_TYP	varchar2(100)	Content type
CONTENT_DESC	Clob	Content description
CONTENT_CONTEXT	Clob	Content context
CONTENT_HASH	varchar2(255)	Content hash
DATE_CREATED	Date	Date the entry was created
DATE_MODIFIED	Date	Date the entry was modified
MODIFIED_BY	number(38,0)	User who last modified object
CREATED_BY	number(38,0)	User who created object

7.1.42 ESEC_CTRL_CTGRY_RPT_V

View contains information about Solution Packs.

Column Name	Datatype	Comment
CTRL_CTGRY_ID	varchar2(36)	Control category identifier
CTRL_CTGRY_DESC	Clob	Control category description
CTRL_CTGRY_NAME	varchar2(255)	Control category name

Column Name	Datatype	Comment
CONTENT_PACK_ID	varchar2(36)	Content pack identifier
CONTENT_EXTERNAL_ID	varchar2(255)	Content external identifier
DATE_CREATED	Date	Date the entry was created
DATE_MODIFIED	Date	Date the entry was modified
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object

7.1.43 ESEC_CTRL_RPT_V

View contains information about Solution Packs.

Column Name	Datatype	Comment
CTRL_ID	varchar2(36)	Control identifier
CTRL_NAME	varchar2(255)	Control name
CTRL_DESC	clob	Control description
CTRL_STATE	number(38,0)	Control state
CTRL_NOTES	clob	Control notes
CTRL_CTGRY_ID	varchar2(36)	Control category identifier
CONTENT_EXTERNAL_ID	varchar2(255)	Content external identifier
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object

7.1.44 ESEC_DISPLAY_RPT_V

View references ESEC_DISPLAY table that stores displayable properties of objects. Currently used in renaming meta-tags. Used with Event Configuration (Business Relevance).

Column Name	Datatype	Comment
DISPLAY_OBJECT	varchar2(32)	The parent object of the property
TAG	varchar2(32)	The native tag name of the property
LABEL	varchar2(32)	The display string of tag.
POSITION	number	Position of tag within display.
WIDTH	number	The column width
ALIGNMENT	number	The horizontal alignment

Column Name	Datatype	Comment
FORMAT	number	The enumerated formatter for displaying the property
ENABLED	varchar2(1)	Indicates if the tag is shown.
TYPE	number	Indicates datatype of tag. 1 = string 2 = ulong 3 = date 4 = uuid 5 = ipv4
DESCRIPTION	varchar2(255)	Textual description of the tag
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object
REF_CONFIG	varchar2(4000)	Referential data configuration

7.1.45 ESEC_PORT_REFERENCE_RPT_V

View references ESEC_PORT_REFERENCE table that stores industry standard assigned port numbers.

Column Name	Datatype	Comment
PORT_NUMBER	number	Per http://www.iana.org/assignments/port-numbers (http://www.iana.org/assignments/port-numbers), the numerical representation of the port. This port number is typically associated with the Transport Protocol level in the TCP/IP stack.
PROTOCOL_NUMBER	number	Per http://www.iana.org/assignments/protocol-numbers (http://www.iana.org/assignments/protocol-numbers), the numerical identifiers used to represent protocols that are encapsulated in an IP packet.
PORT_KEYWORD	varchar2(64)	Per http://www.iana.org/assignments/port-numbers (http://www.iana.org/assignments/port-numbers), the keyword representation of the port.
PORT_DESCRIPTION	varchar2(512)	Port description.
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object

Column Name	Datatype	Comment
MODIFIED_BY	number	User who last modified object

7.1.46 ESEC_PROTOCOL_REFERENCE_RPT_V

View references ESEC_PROTOCOL_REFERENCE table that stores industry standard assigned protocol numbers.

Column Name	Datatype	Comment
PROTOCOL_NUMBER	number	Per http://www.iana.org/assignments/protocol-numbers (http://www.iana.org/assignments/protocol-numbers), the numerical identifiers used to represent protocols that are encapsulated in an IP packet.
PROTOCOL_KEYWORD	varchar2(64)	Per http://www.iana.org/assignments/protocol-numbers (http://www.iana.org/assignments/protocol-numbers), the keyword used to represent protocols that are encapsulated in an IP packet.
PROTOCOL_DESCRIPTION	varchar2(512)	IP packet protocol description.
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.47 ESEC_SEQUENCE_RPT_V

View references ESEC_SEQUENCE table that's used to generate primary key sequence numbers for Sentinel tables.

Column Name	Datatype	Comment
TABLE_NAME	varchar2(32)	Name of the table.
COLUMN_NAME	varchar2(255)	Name of the column
SEED	number	Current value of primary key field.
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.48 ESEC_UUID_UUID_ASSOC_RPT_V

Contains information about object relationships. Used internally by Sentinel and not for reporting purposes.

Column Name	Datatype	Comment
OBJECT1	varchar2(64)	Object 1
ID1	varchar2(36)	UUID for object 1
OBJECT2	varchar2(64)	Object 2
ID2	varchar2(36)	UUID for object 2
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object

7.1.49 EVENTS_ALL_RPT_V (legacy view)

This view is provided for backward compatibility. View contains current and historical events (events imported from archives).

7.1.50 EVENTS_ALL_RPT_V1 (legacy view)

This view is provided for backward compatibility. New reports should use EVENTS_RPT_V2. View contains current events.

7.1.51 EVENTS_RPT_V (legacy view)

This view is provided for backward compatibility. New reports should use EVENTS_RPT_V2. View contains current and historical events.

7.1.52 EVENTS_RPT_V1 (legacy view)

This view is provided for backward compatibility. New reports should use EVENT_ALL_RPT_V. View contains current events.

7.1.53 EVENTS_RPT_V2

This is the primary reporting view for Sentinel 6.0. This view contains current event and historical events. It is included for legacy reports but has been replaced in Sentinel 6.1 with EVENTS_RPT_V3.

Column Name	Datatype	Comment
EVENT_ID	varchar2(36)	Event identifier

Column Name	Datatype	Comment
RESOURCE_NAME	varchar2(255)	Resource name
SUB_RESOURCE	varchar2(255)	Subresource name
SEVERITY	integer	Event severity
EVENT_PARSE_TIME	date	Event time
EVENT_DATETIME	date	Event time
EVENT_DEVICE_TIME	date	Event device time
SENTINEL_PROCESS_TIME	date	Sentinel process time
BEGIN_TIME	date	Events begin time
END_TIME	date	Events end time
REPEAT_COUNT	integer	Events repeat count
DESTINATION_PORT_INT	integer	Destination port (integer)
SOURCE_PORT_INT	integer	Source port (integer)
BASE_MESSAGE	varchar2(4000)	Base message
EVENT_NAME	varchar2(255)	Name of the event as reported by the sensor
EVENT_TIME	varchar2(255)	Event time as reported by the sensor
CUST_ID	integer	Customer identifier
SOURCE_ASSET_ID	integer	Source asset identifier
DESTINATION_ASSET_ID	integer	Destination asset identifier
AGENT_ID	integer	Collector identifier
PROTOCOL_ID	integer	Protocol identifier
ARCHIVE_ID	integer	Archive identifier
SOURCE_IP	integer	Source IP address in numeric format
SOURCE_IP_DOTTED	varchar2(16)	Source IP in dotted format
SOURCE_HOST_NAME	varchar2(255)	Source host name
SOURCE_PORT	varchar2(32)	Source port
DESTINATION_IP	integer	Destination IP address in numeric format
DESTINATION_IP_DOTTED	varchar2(16)	Destination in dotted format
DESTINATION_HOST_NAME	varchar2(255)	Destination host name
DESTINATION_PORT	varchar2(32)	Destination port
SOURCE_USER_NAME	varchar2(255)	Source user name
DESTINATION_USER_NAME	varchar2(255)	Destination user name
FILE_NAME	varchar2(1000)	File name

Column Name	Datatype	Comment
EXTENDED_INFO	varchar2(1000)	Extened information
CUSTOM_TAG_1	varchar2(255)	Customer Tag 1
CUSTOM_TAG 2	varchar2(255)	Customer Tag 2
CUSTOM_TAG 3	integer	Customer Tag 3
RESERVED_TAG_1	varchar2(255)	Reserved Tag 1
		Reserved for future use by Novell. This field is used for Advisor information concerning attack descriptions.
RESERVED_TAG_2	varchar2(255)	Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
RESERVED_TAG_3	integer	Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
VULNERABILITY_RATING	integer	Vulnerability rating
CRITICALITY_RATING	integer	Criticality rating
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
RV01 - 10	integer	Reserved Value 1 - 10
		Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV11 - 20	date	Reserved Value 1 - 31
		Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV21 - 25	varchar2(36)	Reserved Value 21 - 25
		Reserved for future use by Novell to store UUIDs. Use of this field for any other purpose might result in data being overwritten by future functionality.

Column Name	Datatype	Comment
RV26 - 31	varchar2(255)	Reserved Value 26 - 31 Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV33	varchar2(255)	Reserved Value 33 Reserved for EventContex Use of this field for any other purpose might result in data being overwritten by future functionality.
RV34	varchar2(255)	Reserved Value 34 Reserved for SourceThreatLevel Use of this field for any other purpose might result in data being overwritten by future functionality.
RV35	varchar2(255)	Reserved Value 35 Reserved for SourceUserContext. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV36	varchar2(255)	Reserved Value 36 Reserved for DataContext. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV37	varchar2(255)	Reserved Value 37 Reserved for SourceFunction. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV38	varchar2(255)	Reserved Value 38 Reserved for SourceOperationalContext. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV40 - 43	varchar2(255)	Reserved Value 40 - 43 Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.

Column Name	Datatype	Comment
RV44	varchar2(255)	Reserved Value 44 Reserved for DestinationThreatLevel. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV45	varchar2(255)	Reserved Value 45 Reserved for DestinationUserContext. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV46	varchar2(255)	Reserved Value 46 Reserved for VirusStatus. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV47	varchar2(255)	Reserved Value 47 Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV48	varchar2(255)	Reserved Value 48 Reserved for DestinationOperationalContext. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV49	varchar2(255)	Reserved Value 49 Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
TAXONOMY_ID	integer	
REFERENCE_ID_01 - 20	integer	Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
CV01 - 10	integer	Custom Value 1 - 10 Reserved for use by Customer, typically for association of Business relevant data

Column Name	Datatype	Comment
CV11 - 20	date	Custom Value 11 - 20 Reserved for use by Customer, typically for association of Business relevant data
CV21 - 29	varchar2(255)	Custom Value 21 – 100 Reserved for use by Customer, typically for association of Business relevant data
CV30 - 34	varchar2(4000)	
CV35 – 100	varchar2(255)	

7.1.54 EVENTS_RPT_V3

This is the primary reporting view for Sentinel 6.1. This view contains current event and historical events. It is included for legacy reports but has been replaced in Sentinel 6.1 with EVENTS_RPT_V3.

Column Name	Datatype	Comment
EVENT_ID	varchar2(36)	Event identifier
RESOURCE_NAME	varchar2(255)	
SUB_RESOURCE	varchar2(255)	Subresource name
SEVERITY	number(38,0)	Event severity
EVENT_PARSE_TIME	date	Event time
EVENT_DATETIME	date	
EVENT_DEVICE_TIME	date	Event device time
SENTINEL_PROCESS_TIME	date	Sentinel process time
BEGIN_TIME	date	Events begin time
END_TIME	date	Events end time
REPEAT_COUNT	number(38,0)	
TARGET_SERVICE_PORT	number(38,0)	Target service port
INIT_SERVICE_PORT	number(38,0)	
BASE_MESSAGE	varchar2(4000)	
EVENT_NAME	varchar2(255)	
EVENT_TIME	varchar2(255)	Event time
CUST_ID	number(38,0)	
INIT_ASSET_ID	number(38,0)	Initiator asset identifier
TARGET_ASSET_ID	number(38,0)	Target asset identifier

Column Name	Datatype	Comment
AGENT_ID	number(38,0)	
PROTOCOL_ID	number(38,0)	
ARCHIVE_ID	number(38,0)	
INIT_IP	number(38,0)	
INIT_IP_DOTTED	varchar2(4000)	
INIT_HOST_NAME	varchar2(255)	
INIT_SERVICE_PORT_NAME	varchar2(32)	
TARGET_IP	number(38,0)	
TARGET_IP_DOTTED	varchar2(4000)	
TARGET_HOST_NAME	varchar2(255)	
TARGET_SERVICE_PORT_NAME	varchar2(32)	
INIT_USER_NAME	varchar2(255)	
TARGET_USER_NAME	varchar2(255)	
FILE_NAME	varchar2(1000)	
EXTENDED_INFO	varchar2(1000)	
CUSTOM_TAG_1	varchar2(255)	Customer Tag 1
CUSTOM_TAG_2	varchar2(255)	Customer Tag 2
CUSTOM_TAG_3	number(38,0)	Customer Tag 3
RESERVED_TAG_1	varchar2(255)	
RESERVED_TAG_2	varchar2(255)	
RESERVED_TAG_3	number(38,0)	
VULNERABILITY_RATING	number(38,0)	
CRITICALITY_RATING	number(38,0)	
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object
RV01	number(38,0)	
EVENT_METRIC	number(38,0)	Event metric
DATA_TAG_ID	number(38,0)	Data tag ID
RV04-RV10	number(38,0)	
RV11-RV20	date	

Column Name	Datatype	Comment
RV21- RV28	varchar2(255)	
INIT_IP_COUNTRY	varchar2(255)	
TARGET_IP_COUNTRY	varchar2(255)	
RV31	varchar2(255)	
RV33	varchar2(255)	
INIT_THREAT_LEVEL	varchar2(255)	Initiator treat level
INIT_USER_DOMAIN	varchar2(255)	Initiator user domain
RV36	varchar2(255)	
INIT_FUNCTION	varchar2(255)	Initiator function
INIT_OPERATIONAL_CONTEXT	varchar2(255)	Initiator operational context
RV40	varchar2(255)	
TARGET_HOST_DOMAIN	varchar2(255)	Target host domain
INIT_HOST_DOMAIN	varchar2(255)	
RV43	varchar2(255)	
TARGET_THREAT_LEVEL	varchar2(255)	Target threat level
TARGET_USER_DOMAIN	varchar2(255)	Target user domain
RV46	varchar2(255)	
TARGET_FUNCTION	varchar2(255)	Target function
TARGET_OPERATIONAL_CONEXT	varchar2(255)	Target operational context
RV49	varchar2(255)	
TAXONOMY_ID	number(38,0)	Taxonomy identifier
REFERENCE_ID_01- REFERENCE_ID_20	number(38,0)	
CV01-CV10	number(38,0)	
CV11-CV20	date	
CV21- CV29	varchar2(255)	
CV30- CV34	varchar2(4000)	
CV35- CV100	varchar2(255)	
INIT_USER_ID	varchar2(255)	Initiator user ID
INIT_USER_IDENTITY	varchar2(36)	Initiator user identity
TARGET_USER_ID	varchar2(255)	Target user ID
TARGET_USER_IDENTITY	varchar2(36)	Target user identity
EFFECTIVE_USER_NAME	varchar2(255)	Effective user name

Column Name	Datatype	Comment
EFFECTIVE_USER_ID	varchar2(255)	Effective user ID
EFFECTIVE_USER_DOMAIN	varchar2(255)	Effective user domain
TARGET_TRUST_NAME	varchar2(255)	Target trust name
TARGET_TRUST_ID	varchar2(255)	Target trust ID
TARGET_TRUST_DOMAIN	varchar2(255)	Target trust domain
OBSERVER_IP	number(38,0)	Observer IP address in numeric format
REPORTER_IP	number(38,0)	Reporter IP address in numeric format
OBSERVER_HOST_DOMAIN	varchar2(255)	Observer host domain
REPORTER_HOST_DOMAIN	varchar2(255)	Reporter host domain
OBSERVER_ASSET_ID	varchar2(255)	Observer asset identifier
REPORTER_ASSET_ID	varchar2(255)	Reporter asset identifier
INIT_SERVICE_COMP	varchar2(255)	Initiator service component
TARGET_SERVICE_COMP	varchar2(255)	Target service component
EVENT_GROUP_ID	varchar2(255)	
CUSTOMER_VAR_101-CUSTOMER_VAR_110	number(38,0)	
CUSTOMER_VAR_111-CUSTOMER_VAR_120	date	
CUSTOMER_VAR_121-CUSTOMER_VAR_130	varchar2(36)	
CUSTOMER_VAR_131-CUSTOMER_VAR_140	number(38,0)	
CUSTOMER_VAR_141-CUSTOMER_VAR_150	varchar2(255)	

7.1.55 EVT_AGENT_RPT_V

View references EVT_AGENT table that stores information about Collectors.

Column Name	Datatype	Comment
AGENT_ID	number(38)	Collector identifier
CUST_ID	number(38)	
AGENT	varchar2(64)	Collector name
PORT	varchar2(64)	Collector port
REPORT_NAME	varchar2(255)	Reporter name
PRODUCT_NAME	varchar2(255)	Product name

Column Name	Datatype	Comment
SENSOR_NAME	varchar2(255)	Sensor name
SENSOR_TYPE	varchar2(5)	Sensor type: H - host-based N - network-based V - virus O – other
DEVICE_CATEGORY	varchar2(255)	Device category
SOURCE_UUID	varchar2(36)	Source component Universal Unique Identifier (UUID)
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.56 EVT_AGENT_RPT_V3

View references EVT_AGENT table that stores information about Collectors. The column names in this view reflects the name change of Sensor to Observer. This view is designed for use in Sentinel 6.1.

Column Name	Datatype	Comment
AGENT_ID	number(38,0)	Collector identifier
CUST_ID	number(38,0)	Customer identifier
AGENT	varchar2(64)	Collector
PORT	varchar2(64)	Port
REPORTER_HOST_NAME	varchar2(255)	Reporter host name
PRODUCT_NAME	varchar2(255)	
OBSERVER_HOST_NAME	varchar2(255)	
SENSOR_TYPE	varchar2(5)	Sensor type: H - host-based N - network-based V - virus O - other
DEVICE_CATEGORY	varchar2(255)	Device category

Column Name	Datatype	Comment
SOURCE_UUID	varchar2(36)	Source component Universal Unique Identifier (UUID)
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object

7.1.57 EVT_ASSET_RPT_V

View references EVT_ASSET table that stores asset information.

Column Name	Datatype	Comment
EVENT_ASSET_ID	number(38)	Event asset identifier
CUST_ID	number(38)	Customer identifier
ASSET_NAME	varchar2(255)	Asset name
PHYSICAL_ASSET_NAME	varchar2(255)	Physical asset name
REFERENCE_ASSET_ID	varchar2(100)	Reference asset identifier, links to source asset management system.
MAC_ADDRESS	varchar2(100)	MAC address
RACK_NUMBER	varchar2(50)	Rack number
ROOM_NAME	varchar2(100)	Room name
BUILDING_NAME	varchar2(255)	Building name
CITY	varchar2(100)	City
STATE	varchar2(100)	State
COUNTRY	varchar2(100)	Country
ZIP_CODE	varchar2(50)	Zip code
ASSET_CATEGORY_NAME	varchar2(100)	Asset category name
NETWORK_IDENTITY_NAME	varchar2(255)	Asset network identity name
ENVIRONMENT_IDENTITY_NAME	varchar2(255)	Environment name
ASSET_VALUE_NAME	varchar2(50)	Asset value name
CRITICALITY_NAME	varchar2(50)	Asset criticality name
SENSITIVITY_NAME	varchar2(50)	Asset sensitivity name
CONTACT_NAME_1	varchar2(255)	Name of contact person/organization 1
CONTACT_NAME_2	varchar2(255)	Name of contact person/organization 2
ORGANIZATION_NAME_1	varchar2(100)	Asset owner organization level 1

Column Name	Datatype	Comment
ORGANIZATION_NAME_2	varchar2(100)	Asset owner organization level 2
ORGANIZATION_NAME_3	varchar2(100)	Asset owner organization level 3
ORGANIZATION_NAME_4	varchar2(100)	Asset owner organization level 4
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.58 EVT_ASSET_RPT_V3

View references EVT_ASSET table that stores asset information. This view is designed for Sentinel 6.1.

Column Name	Datatype	Comment
ASSET_CRITICALITY	varchar2(50)	
ASSET_CLASS	varchar2(100)	
ASSET_FUNCTION	varchar2(255)	
ASSET_DEPARTMENT	varchar2(100)	Asset department
DATE_CREATED	Date	Date the entry was created
DATE_MODIFIED	Date	Date the entry was modified
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object

7.1.59 EVT_DEST_EVT_NAME_SMRY_1_RPT_V

View summarizes event count by destination, taxonomy, event name, severity and event time.

Column Name	Datatype	Comment
DESTINATION_IP	number(38)	Destination IP address
DESTINATION_EVENT_ASSET_ID	number(38)	Event asset identifier
TAXONOMY_ID	number(38)	Taxonomy identifier
EVENT_NAME_ID	number(38)	Event name identifier
SEVERITY	number(38)	Event severity
CUST_ID	number(38)	Customer identifier
EVENT_TIME	date	Event time
EVENT_COUNT	number(38)	Event count

Column Name	Datatype	Comment
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object
DESTINATION_HOST_NAME	varchar2(255)	

7.1.60 EVT_DEST_SMRY_1_RPT_V

View contains event destination summary information.

Column Name	Datatype	Comment
DESTINATION_IP	number(38)	Destination IP address
DESTINATION_EVENT_ASSET_ID	number(38)	Event asset identifier
DESTINATION_PORT	varchar2(32)	Destination port
DESTINATION_USER_ID	number(38)	Destination user identifier
TAXONOMY_ID	number(38)	Taxonomy identifier
EVENT_NAME_ID	number(38)	Event name identifier
RESOURCE_ID	number(38)	Resource identifier
AGENT_ID	number(38)	Collector identifier
PROTOCOL_ID	number(38)	Protocol identifier
SEVERITY	number(38)	Event severity
CUST_ID	number(38)	Customer identifier
EVENT_TIME	date	Event time
EVENT_COUNT	number(38)	Event count
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object
DESTINATION_HOST_NAME	varchar2(255)	

7.1.61 EVT_DEST_TXNMY_SMRY_1_RPT_V

View summarizes event count by destination, taxonomy, severity and event time.

Column Name	Datatype	Comment
DESTINATION_IP	number(38)	Destination IP address
DESTINATION_EVENT_ASSET_ID	number(38)	Event asset identifier
TAXONOMY_ID	number(38)	Taxonomy identifier
SEVERITY	number(38)	Event severity
CUST_ID	number(38)	Customer identifier
EVENT_TIME	date	Event time
EVENT_COUNT	number(38)	Event count
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object
DESTINATION_HOST_NAME	varchar2(255)	

7.1.62 EVT_NAME_RPT_V

View references EVT_NAME table that stores event name information.

Column Name	Datatype	Comment
EVENT_NAME_ID	number(38)	Event name identifier
EVENT_NAME	varchar2(255)	Event name
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.63 EVT_PORT_SMRY_1_RPT_V

View summarizes event count by destination port, severity and event time.

Column Name	Datatype	Comment
DESTINATION_PORT	varchar2(32)	Destination port
SEVERITY	number(38)	Event severity
CUST_ID	number(38)	Customer identifier
EVENT_TIME	date	Event time
EVENT_COUNT	number(38)	Event count

Column Name	Datatype	Comment
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.64 EVT_PRTCL_RPT_V

View references EVT_PRTCL table that stores event protocol information.

Column Name	Datatype	Comment
PROTOCOL_ID	number(38)	Protocol identifier
PROTOCOL_NAME	varchar2(255)	Protocol name
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.65 EVT_PRTCL_RPT_V3

View references EVT_PRTCL table that stores event protocol information.

Column Name	Datatype	Comment
PROTOCOL_ID	number(38,0)	Protocol identifier
PROTOCOL	varchar2(255)	Protocol name
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object

7.1.66 EVT_RSRC_RPT_V

View references EVT_RSRC table that stores event resource information.

Column Name	Datatype	Comment
RESOURCE_ID	number(38)	Resource identifier
CUST_ID	number(38)	Customer Identifier
RESOURCE_NAME	varchar2(255)	Resource name

Column Name	Datatype	Comment
SUB_RESOURCE_NAME	varchar2(255)	Subresource name
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.67 EVT_SEV_SMRY_1_RPT_V

View summarizes event count by severity and event time.

Column Name	Datatype	Comment
SEVERITY	number(38)	Event severity
CUST_ID	number(38)	Customer identifier
EVENT_TIME	date	Event time
EVENT_COUNT	number(38)	Event count
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.68 EVT_SRC_COLLECTOR_RPT_V

View contains information about the Event Source Management configuration.

Column Name	Datatype	Comment
EVT_SRC_COLLECTOR_ID	varchar2(36)	Event source collector identifier
SENTINEL_PLUGIN_ID	varchar2(36)	Sentinel plugin identifier
EVT_SRC_MGR_ID	varchar2(36)	Event source manager identifier
EVT_SRC_COLLECTOR_NAME	varchar2(255)	Event source collector name
STATE_IND	number(1,0)	State indicator
EVT_SRC_COLLECTOR_PROPS	clob	Event source collector prop
MAP_FILTER	clob	Map filter
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object
DATE_CREATED	date	Date the entry was created

Column Name	Datatype	Comment
DATE_MODIFIED	date	Date the entry was modified

7.1.69 EVT_SRC_GRP_RPT_V

View contains information about the Event Source Management configuration.

Column Name	Datatype	Comment
EVT_SRC_GRP_ID	varchar2(36)	Event source group identifier
EVT_SRC_COLLECTOR_ID	varchar2(36)	Event source collector identifier
SENTINEL_PLUGIN_ID	varchar2(36)	Sentinel plugin identifier
EVT_SRC_SRVR_ID	varchar2(36)	Event source server identifier
EVT_SRC_GRP_NAME	varchar2(255)	Event source group name
STATE_IND	number(1,0)	State indicator
EVT_SRC_DEFAULT_CONFIG	clob	Event source default configuration
MAP_FILTER	clob	Map filter
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified

7.1.70 EVT_SRC_MGR_RPT_V

View contains information about the Event Source Management configuration.

Column Name	Datatype	Comment
EVT_SRC_MGR_ID	varchar2(36)	Event source manager identifier
SENTINEL_ID	varchar2(36)	Sentinel identifier
EVT_SRC_MGR_NAME	varchar2(255)	Event source manager name
SENTINEL_HOST_ID	varchar2(36)	Sentinel host identifier
STATE_IND	number(1,0)	State indicator
EVT_SRC_MGR_CONFIG	clob	Event source manager configu
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified

7.1.71 EVT_SRC_OFFSET_RPT_V

View contains information about the Event Source Management configuration.

Column Name	Datatype	Comment
EVT_SRC_ID	varchar2(36)	Event source identifier
OFFSET_VAL	clob	Offset value
OFFSET_TIMESTAMP	date	Offset timestamp
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified

7.1.72 EVT_SRC_RPT_V

View contains information about the Event Source Management configuration.

Column Name	Datatype	Comment
EVT_SRC_ID	varchar2(36)	Event source identifier
EVT_SRC_NAME	varchar2(255)	Event source name
EVT_SRC_GRP_ID	varchar2(36)	Event source group identifier
STATE_IND	number(1,0)	State indicator
MAP_FILTER	clob	Map filter
EVT_SRC_CONFIG	clob	Event source config
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified

7.1.73 EVT_SRC_SMRY_1_RPT_V

View contains event source and destination summary information.

Column Name	Datatype	Comment
SOURCE_IP	number(38)	Source IP address
SOURCE_EVENT_ASSET_ID	number(38)	Source event asset identifier
SOURCE_PORT	varchar2(32)	Source port
SOURCE_USER_ID	number(38)	Source user identifier

Column Name	Datatype	Comment
TAXONOMY_ID	number(38)	Taxonomy identifier
EVENT_NAME_ID	number(38)	Event name identifier
RESOURCE_ID	number(38)	Resource identifier
AGENT_ID	number(38)	Collector identifier
PROTOCOL_ID	number(38)	Protocol identifier
SEVERITY	number(38)	Event severity
CUST_ID	number(38)	Customer identifier
EVENT_TIME	date	Event time
EVENT_COUNT	number(38)	Event count
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object
SOURCE_HOST_NAME	varchar2(255)	

7.1.74 EVT_SRC_SRVR_RPT_V

View contains information about the Event Source Management configuration.

Column Name	Datatype	Comment
EVT_SRC_SRVR_ID	varchar2(36)	Event source server identifier
EVT_SRC_SRVR_NAME	varchar2(255)	Event source server name
EVT_SRC_MGR_ID	varchar2(36)	Event source manager identifier
SENTINEL_PLUGIN_ID	varchar2(36)	Sentinel plugin identifier
STATE_IND	number(1,0)	State indicator
EVT_SRC_SRVR_CONFIG	clob	Event source server configuration
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified

7.1.75 EVT_TXNMY_RPT_V

View references EVT_TXNMY table that stores event taxonomy information.

Column Name	Datatype	Comment
TAXONOMY_ID	number(38)	Taxonomy identifier
TAXONOMY_LEVEL_1	varchar2(100)	Taxonomy level 1
TAXONOMY_LEVEL_2	varchar2(100)	Taxonomy level 2
TAXONOMY_LEVEL_3	varchar2(100)	Taxonomy level 3
TAXONOMY_LEVEL_4	varchar2(100)	Taxonomy level 4
DEVICE_CATEGORY	varchar2(255)	
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.76 EVT_USR_RPT_V

View references EVT_USR table that stores event user information.

Column Name	Datatype	Comment
USER_ID	number(38)	User identifier
USER_NAME	varchar2(255)	User name
USER_DOMAIN	varchar2(255)	
CUST_ID	number(38)	Customer identifier
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.77 EVT_XDAS_TXNMY_RPT_V

Column Name	Datatype	Comment
EVENT_TAXONOMY	varchar2(255)	Event taxonomy name
EVENT_OUTCOME	varchar2(255)	Event outcome name
XDAS_REGISTRY	number(38,0)	XDAS registry
XDAS_PROVIDER	number(38,0)	XDAS provider
XDAS_CLASS	number(38,0)	XDAS class

Column Name	Datatype	Comment
XDAS_IDENTIFIER	number(38,0)	XDAS identifier
XDAS_OUTCOME	number(38,0)	XDAS outcome
XDAS_DETAIL	number(38,0)	XDAS detail
XDAS_TAXONOMY_ID	number(38,0)	XDAS taxonomy identifier
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object

7.1.78 EXTERNAL_DATA_RPT_V

View references EXTERNAL_DATA table that stores external data.

Column Name	Datatype	Comment
EXTERNAL_DATA_ID	number	External data identifier
SOURCE_NAME	varchar2(50)	Source name
SOURCE_DATA_ID	varchar2(255)	Source data identifier
EXTERNAL_DATA	clob	External data
EXTERNAL_DATA_TYPE	varchar2(10)	External data type
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.79 HIST_CORRELATED_EVENTS_RPT_V (legacy view)

This view is provided for backward compatibility. New report should use CORRELATED_EVENTS_RPT_V1 instead.

7.1.80 HIST_EVENTS_RPT_V (legacy view)

This view is provided for backward compatibility. Sentinel 6.0 reports should use EVENTS_RPT_V2 instead. Sentinel 6.1 reports should use EVENTS_RPT_V3 instead.

7.1.81 IMAGES_RPT_V

View references IMAGES table that stores system overview image information.

Column Name	Datatype	Comment
NAME	varchar2(128)	Image name
TYPE	varchar2(64)	Image type
DATA	clob	Image data
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.82 INCIDENTS_ASSETS_RPT_V

View references INCIDENTS_ASSETS table that stores information about the assets that makeup incidents created in the Sentinel Console.

Column Name	Datatype	Comment
INC_ID	number	Incident identifier – sequence number
ASSET_ID	varchar2(36)	Asset Universal Unique Identifier (UUID)
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.83 INCIDENTS_EVENTS_RPT_V

View references INCIDENTS_EVENTS table that stores information about the events that makeup incidents created in the Sentinel Console.

Column Name	Datatype	Comment
INC_ID	number	Incident identifier – sequence number
EVT_ID	varchar2(36)	Event Universal Unique Identifier (UUID)
EVT_TIME	date	Event time
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.84 INCIDENTS_RPT_V

View references INCIDENTS table that stores information describing the details of incidents created in the Sentinel Console.

Column Name	Datatype	Comment
INC_ID	number	Incident identifier – sequence number
NAME	varchar2(255)	Incident name
SEVERITY	number	Incident severity
STT_ID	number	Incident State ID
SEVERITY_RATING	varchar2(32)	Average of all the event severities that comprise an incident.
VULNERABILITY_RATING	varchar2(32)	Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
CRITICALITY_RATING	varchar2(32)	Reserved for future use by Novell. Use of this field for any other purpose might result in data being overwritten by future functionality.
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object
INC_DESC	varchar2(4000)	Incident description
INC_CAT	varchar2(255)	Incident category
INC_PRIORITY	number	Incident priority
INC_RES	varchar2(4000)	Incident resolution

7.1.85 INCIDENTS_VULN_RPT_V

View references INCIDENTS_VULN table that stores information about the vulnerabilities that makeup incidents created in the Sentinel Console.

Column Name	Datatype	Comment
INC_ID	number	Incident identifier – sequence number
VULN_ID	varchar2(36)	Vulnerability Universal Unique Identifier (UUID)
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.86 L_STAT_RPT_V

View references L_STAT table that stores statistical information.

Column Name	Datatype	Comment
RES_NAME	varchar2(32)	Resource name
STATS_NAME	varchar2(32)	Statistic name
STATS_VALUE	varchar2(32)	Value of the statistic
OPEN_TOT_SECS	number(38)	Number of seconds since 1970.

7.1.87 LOGS_RPT_V

View references LOGS_RPT table that stores logging information.

Column Name	Datatype	Comment
LOG_ID	number	Sequence number
TIME	date	Date of Log
MODULE	varchar2(64)	Module log is for
TEXT	varchar2(4000)	Log text

7.1.88 MSSP_ASSOCIATIONS_V

View references MSSP_ASSOCIATIONS table that associates an number key in one table to a UUID in another table.

Column Name	Datatype	Comment
TABLE1	varchar2(64)	Table name 1
ID1	number(38)	ID1
TABLE2	varchar2(64)	Table name 2
ID2	varchar2(36)	ID2
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.89 NETWORK_IDENTITY_RPT_V

View references NETWORK_IDENTITY_LKUP table that stores asset network identity information.

Column Name	Datatype	Comment
NETWORK_IDENTITY_ID	number(38)	Network identity code
NETWORK_IDENTITY_NAME	varchar2(255)	Network identify name
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.90 ORGANIZATION_RPT_V

View references ORGANIZATION table that stores organization (asset) information.

Column Name	Datatype	Comment
ORGANIZATION_ID	varchar2(36)	Organization identifier
ORGANIZATION_NAME	varchar2(100)	Organization name
CUST_ID	number(38)	Customer identifier
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.91 PERSON_RPT_V

View references PERSION table that stores personal (asset) information.

Column Name	Datatype	Comment
PERSON_ID	varchar2(36)	Person identifier
FIRST_NAME	varchar2(255)	First name
LAST_NAME	varchar2(255)	Last name
CUST_ID	number(38)	Customer identifier
PHONE_NUMBER	varchar2(50)	Phone number
EMAIL_ADDRESS	varchar2(255)	Email address
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.92 PHYSICAL_ASSET_RPT_V

View references PHYSICAL_ASSET table that stores physical asset information.

Column Name	Datatype	Comment
PHYSICAL_ASSET_ID	varchar2(36)	Physical asset identifier
CUST_ID	number(38)	Customer identifier
HOST_NAME	varchar2(255)	Host name
IP_ADDRESS	number(38)	IP address
LOCATION_ID	number(38)	Location identifier
NETWORK_IDENTITY_ID	number(38)	Network identity code
MAC_ADDRESS	varchar2(100)	MAC address
RACK_NUMBER	varchar2(50)	Rack number
ROOM_NAME	varchar2(100)	Room name
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.93 PRODUCT_RPT_V

View references PRDT table that stores asset product information.

Column Name	Datatype	Comment
PRODUCT_ID	number(38)	Product identifier
PRODUCT_NAME	varchar2(255)	Product name
PRODUCT_VERSION	varchar2(100)	Product version
VENDOR_ID	number(38)	Vendor identifier
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.94 ROLE_RPT_V

View references ROLE_LKUP table that stores user role (asset) information.

Column Name	Datatype	Comment
ROLE_CODE	varchar2(5)	Role code
ROLE_NAME	varchar2(255)	Role name
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.95 RPT_LABELS_RPT_V

View contains report label translations.

Column Name	Datatype	Comment
RPT_NAME	varchar2(100)	Report name
LABEL_1 - 35	varchar2(2000)	Translated report labels

7.1.96 SENSITIVITY_RPT_V

View references SENSITIVITY_LKUP table that stores asset sensitivity information.

Column Name	Datatype	Comment
SENSITIVITY_ID	number(38)	Asset sensitivity code
SENSITIVITY_NAME	varchar2(50)	Asset sensitivity name
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.97 SENTINEL_HOST_RPT_V

View contains data used internally by Sentinel.

Column Name	Datatype	Comment
SENTINEL_HOST_ID	varchar2(36)	Sentinel host identifier
SENTINEL_ID	varchar2(36)	Sentinel identifier
SENTINEL_HOST_NAME	varchar2(255)	Sentinel host name
HOST_NAME	varchar2(255)	Host name

Column Name	Datatype	Comment
IP_ADDR	varchar2(255)	Host IP address
HOST_OS	varchar2(255)	Host operating system
HOST_OS_VERSION	varchar2(255)	Host operating system version
MODIFIED_BY	number(38,0)	User who last modified object
CREATED_BY	number(38,0)	User who created object
DATE_CREATED	Date	Date the entry was created
DATE_MODIFIED	Date	Date the entry was modified

7.1.98 SENTINEL_PLUGIN_RPT_V

View contains data used internally by Sentinel.

Column Name	Datatype	Comment
SENTINEL_HOST_ID	varchar2(36)	Sentinel host identifier
SENTINEL_ID	varchar2(36)	Sentinel identifier
SENTINEL_HOST_NAME	varchar2(255)	Sentinel host name
HOST_NAME	varchar2(255)	Host name
IP_ADDR	varchar2(255)	Host IP address
HOST_OS	varchar2(255)	Host operating system
HOST_OS_VERSION	varchar2(255)	Host operating system version
MODIFIED_BY	number(38,0)	User who last modified object
CREATED_BY	number(38,0)	User who created object
DATE_CREATED	Date	Date the entry was created
DATE_MODIFIED	Date	Date the entry was modified

7.1.99 SENTINEL_RPT_V

View contains data used internally by Sentinel.

Column Name	Datatype	Comment
SENTINEL_ID	varchar2(36)	Sentinel identifier
SENTINEL_NAME	varchar2(255)	Sentinel name
ONLINE_IND	number(1,0)	Online indicator
STATE_IND	number(1,0)	State indicator
SENTINEL_CONFIG	clob	Sentinel configuration

Column Name	Datatype	Comment
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified

7.1.100 STATES_RPT_V

View references STATES table that stores definitions of states defined by applications or context.

Column Name	Datatype	Comment
STT_ID	number(38)	State ID – sequence number
CONTEXT	varchar2(64)	Context of the state. That is case, incident, user.
NAME	varchar2(64)	Name of the state.
TERMINAL_FLAG	varchar2(1)	Indicates if state of incident is resolved.
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
MODIFIED_BY	number	User who last modified object
CREATED_BY	number	User who created object

7.1.101 UNASSIGNED_INCIDENTS_RPT_V

View references CASES and INCIDENTS tables to report on unassigned cases.

Name	Datatype	Comment
INC_ID	number	
NAME	varchar2(255)	
SEVERITY	number	
STT_ID	number	
SEVERITY_RATING	varchar2(32)	
VULNERABILITY_RATING	varchar2(32)	
CRITICALITY_RATING	varchar2(32)	
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

Name	Datatype	Comment
INC_DESC	varchar2(4000)	
INC_CAT	varchar2(255)	
INC_PRIORITY	number	
INC_RES	varchar2(4000)	

7.1.102 USERS_RPT_V

View references USERS table that lists all users of the application. The users will also be created as database users to accommodate 3rd party reporting tools.

Column Name	Datatype	Comment
USR_ID	number	User identifier – Sequence number
NAME	varchar2(64)	Short, unique user name used as a login
CNT_ID	number	Contact ID – Sequence number
STT_ID	number	State ID. Status is either active or inactive.
DESCRIPTION	varchar2(512)	Comments
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object
PERMISSIONS	varchar2(4000)	Permissions currently assigned to the Sentinel user
FILTER	varchar2(128)	Current security filter assigned to the Sentinel user
UPPER_NAME	varchar2(64)	User name in upper case
DOMAIN_AUTH_IND	number (1)	Domain authentication indication

7.1.103 USR_ACCOUNT_RPT_V

View contains user account information from an identity management system.

Column Name	Datatype	Comment
ACCOUNT_ID	number(38,0)	Account identifier
USER_NAME	varchar2(255)	User name
USER_DOMAIN	varchar2(255)	User domain
CUST_ID	number(38,0)	Customer identifier
BEGIN_EFFECTIVE_DATE	date	Begin effective date
END_EFFECTIVE_DATE	date	End effective date

Column Name	Datatype	Comment
CURRENT_F	number(1,0)	Current flag
USER_STATUS	varchar2(50)	User status
IDENTITY_GUID	varchar2(36)	Identity identifier
SOURCE_USER_ID	varchar2(100)	User ID on source system
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object

7.1.104 USR_IDENTITY_EXT_ATTR_RPT_V

View contains extended attributes information from an identity management system, including name value pairs in the ATTRIBUTE_NAME and ATTRIBUTE_VALUE columns.

Column Name	Datatype	Comment
IDENTITY_GUID	varchar2(36)	Identity identifier
ATTRIBUTE_NAME	varchar2(255)	Attribute name
ATTRIBUTE_VALUE	varchar2(1024)	Attribute value

7.1.105 USR_IDENTITY_RPT_V

View contains user identity information from an identity management system.

Column Name	Datatype	Comment
IDENTITY_GUID	varchar2(36)	Identity identifier
DN	varchar2(255)	Distinguished name
CUST_ID	number(38,0)	Customer identifier
SRC_IDENTITY_ID	varchar2(100)	Source identity identifier
WFID	varchar2(100)	Workforce identifier
FIRST_NAME	varchar2(255)	First name
LAST_NAME	varchar2(255)	Last name
FULL_NAME	varchar2(255)	Full name
JOB_TITLE	varchar2(255)	Job title
DEPARTMENT_NAME	varchar2(100)	Department name
OFFICE_LOC_CD	varchar2(100)	Office location code
PRIMARY_EMAIL	varchar2(255)	Primary email address

Column Name	Datatype	Comment
PRIMARY_PHONE	varchar2(100)	Primary phone number
VAULT_NAME	varchar2(100)	Identity vault name
MGR_GUID	varchar2(36)	Manager identity identifier
PHOTO	clob	Photo
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object

7.1.106 VENDOR_RPT_V

View references VNDR table that stores information about asset product vendors.

Column Name	Datatype	Comment
VENDOR_ID	number(38)	Vendor identifier
VENDOR_NAME	varchar2(255)	Vendor name
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38)	User who created object
MODIFIED_BY	number(38)	User who last modified object

7.1.107 VULN_CALC_SEVERITY_RPT_V

View references VULN_RSRC and VULN to calculate eSecurity vulnerability severity rating base on current vulnerabilities.

Column Name	Datatype	Comment
RSRC_ID	varchar2(36)	Resource identifier
IP	varchar2(32)	IP
HOST_NAME	varchar2(255)	Host name
CRITICALITY	number	Asset criticality code
ASSIGNED_VULN_SEVERITY	number	
VULN_COUNT	number	Vulnerability Count
CALC_SEVERITY	number	Calculated severity

7.1.108 VULN_CODE_RPT_V

View references VULN_CODE table that stores industry assigned vulnerability codes such as Mitre's CVEs and CANs.

Column Name	Datatype	Comment
VULN_CODE_ID	varchar2(36)	Vulnerability code identifier
VULN_ID	varchar2(36)	Vulnerability identifier
VULN_CODE_TYPE	varchar2(64)	Vulnerability code type
VULN_CODE_VALUE	varchar2(255)	Vulnerability code value
URL	varchar2(512)	Web URL
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.109 VULN_INFO_RPT_V

View references VULN_INFO table that stores additional information reported during a scan.

Column Name	Datatype	Comment
VULN_INFO_ID	varchar2(36)	Vulnerability info identifier
VULN_ID	varchar2(36)	Vulnerability identifier
VULN_INFO_TYPE	varchar2(36)	Vulnerability info type
VULN_INFO_VALUE	varchar2(2000)	Vulnerability info value
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.110 VULN_RPT_V

View references VULN table that stores information of scanned system. Each scanner will have its own entry for each system.

Column Name	Datatype	Comment
VULN_ID	varchar2(36)	Vulnerability identifier
RSRC_ID	varchar2(36)	Resource identifier

Column Name	Datatype	Comment
PORT_NAME	varchar2(64)	Port Name
PORT_NUMBER	number	Port Number
NETWORK_PROTOCOL	number	Network Protocol
APPLICATION_PROTOCOL	varchar2(64)	Application Protocol
ASSIGNED_VULN_SEVERITY	number	
COMPUTED_VULN_SEVERITY	number	
VULN_DESCRIPTION	clob	Vulnerability description
VULN_SOLUTION	clob	Vulnerability solution
VULN_SUMMARY	varchar2(1000)	Vulnerability summary
BEGIN_EFFECTIVE_DATE	date	Date from which the entry is valid
END_EFFECTIVE_DATE	date	Date until which the entry is valid
DETECTED_OS	varchar2(64)	Operating system of scanned machine
DETECTED_OS_VERSION	varchar2(64)	Operating system version of scanned machine
SCANNED_APP	varchar2(64)	
SCANNED_APP_VERSION	varchar2(64)	
VULN_USER_NAME	varchar2(64)	Username used by scanner
VULN_USER_DOMAIN	varchar2(64)	Domain of user used by scanned
VULN_TAXONOMY	varchar2(1000)	
SCANNER_CLASSIFICATION	varchar2(255)	
VULN_NAME	varchar2(300)	
VULN_MODULE	varchar2(64)	
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.111 VULN_RSRC_RPT_V

View references VULN_RSRC table that stores each resource scanned for a particular scan.

Column Name	Datatype	Comment
RSRC_ID	varchar2(36)	Resource identifier
SCANNER_ID	varchar2(36)	Scanner identifier

Column Name	Datatype	Comment
IP	varchar2(32)	IP Address
HOST_NAME	varchar2(255)	Host name
LOCATION	varchar2(128)	Location
DEPARTMENT	varchar2(128)	Department
BUSINESS_SYSTEM	varchar2(128)	Business System
OPERATIONAL_ENVIRONMENT	varchar2(64)	Operational environment
CRITICALITY	number	Criticality
REGULATION	varchar2(128)	Regulation
REGULATION_RATING	varchar2(64)	Regulation rating
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.112 VULN_RSRC_SCAN_RPT_V

View references VULN_RSRC_SCAN table that stores each resource scanned for a particular scan.

Column Name	Datatype	Comment
RSRC_ID	varchar2(36)	Resource identifier
SCAN_ID	varchar2(36)	Vulnerability scan identifier
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.113 VULN_SCAN_RPT_V

View references table that stores information pertaining to scans.

Column Name	Datatype	Comment
SCAN_ID	varchar2(36)	Vulnerability scan identifier
SCANNER_ID	varchar2(36)	Vulnerability scanner identifier
SCAN_TYPE	varchar2(10)	Vulnerability scan type
SCAN_START_DATE	date	Scan start date

Column Name	Datatype	Comment
SCAN_END_DATE	date	Scan start date
CONSOLIDATION_SERVER	varchar2(64)	Consolidation server
LOAD_STATUS	varchar2(64)	
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.114 VULN_SCAN_VULN_RPT_V

View references VULN_SCAN_VULN table that stores vulnerabilities detected during scans.

Column Name	Datatype	Comment
SCAN_ID	varchar2(36)	Vulnerability scan identifier
VULN_ID	varchar2(36)	Vulnerability identifier
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.115 VULN_SCANNER_RPT_V

View references VULN_SCANNER table that stores information about vulnerability scanners.

Column Name	Datatype	Comment
SCANNER_ID	varchar2(36)	Vulnerability scanner identifier
PRODUCT_NAME	varchar2(100)	Product Name
PRODUCT_VERSION	varchar2(64)	Product Version
SCANNER_TYPE	varchar2(64)	Vulnerability Scanner Type
VENDOR	varchar2(100)	Vendor
SCANNER_INSTANCE	varchar2(64)	Scanner Instance
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number	User who created object
MODIFIED_BY	number	User who last modified object

7.1.116 WORKFLOW_DEF_RPT_V

Column Name	Datatype	Comment
PKG_NAME	varchar2(255)	Package name
PKG_DATA	clob	Package data
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object

7.1.117 WORKFLOW_INFO_RPT_V

Column Name	Datatype	Comment
INFO_ID	number(38,0)	Info identifier
PROCESS_DEF_ID	varchar2(100)	Process definition identifier
PROCESS_INSTANCE_ID	varchar2(150)	Process instance identifier
DATE_CREATED	date	Date the entry was created
DATE_MODIFIED	date	Date the entry was modified
CREATED_BY	number(38,0)	User who created object
MODIFIED_BY	number(38,0)	User who last modified object

7.2 Deprecated Views

The following legacy views are no longer created in the Sentinel 6 database:

- ADV_ALERT_CVE_RPT_V
- ADV_ALERT_PRODUCT_RPT_V
- ADV_ALERT_RPT_V
- ADV_ATTACK_ALERT_RPT_V
- ADV_ATTACK_CVE_RPT_V
- ADV_CREDIBILITY_RPT_V
- ADV_SEVERITY_RPT_V
- ADV_SUBALERT_RPT_V
- ADV_URGENCY_RPT_V

Sentinel Database Views for Microsoft SQL Server

8

This section lists the Sentinel Schema Views for Microsoft SQL Server. The views provide information for developing your own reports (Crystal Reports).

8.1 Views

Below listed are the views available with Sentinel.

8.1.1 ACTVY_PARM_RPT_V

Column Name	Datatype	Comment
ACTVY_PARM_ID	uniqueidentifier	Activity parameter identifier
ACTVY_ID	uniqueidentifier	Activity identifier
PARM_NAME	varchar/nvarchar(255)	Activity Parameter name
PARM_TYP_CD	varchar/nvarchar(1)	Activity parameter type code
DATA_TYP	varchar/nvarchar(50)	Activity parameter data type
DATA_SUBTYP	varchar/nvarchar(50)	Activity parameter data subtype
RQRD_F	Bit	Required flag
PARM_DESC	varchar/nvarchar(255)	Activity parameter description
PARM_VAL	varchar/nvarchar(1000)	Activity parameter value
FORMATTER	varchar/nvarchar(255)	Activity parameter formatter
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.2 ACTVY_REF_PARM_VAL_RPT_V

Column Name	Datatype	Comment
ACTVY_ID	uniqueidentifier	Activity identifier
SEQ_NUM	int	Sequence number
ACTVY_PARM_ID	uniqueidentifier	Activity parameter identifier

Column Name	Datatype	Comment
PARM_VAL	varchar/nvarchar(1000)	Activity parameter value
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.3 ACTVY_REF_RPT_V

Column Name	Datatype	Comment
ACTVY_ID	uniqueidentifier	Activity identifier
SEQ_NUM	int	Sequenece number
REFD_ACTVY_ID	uniqueidentifier	Referenced activity identifier
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.4 ACTVY_RPT_V

Column Name	Datatype	Comment
ACTVY_ID	uniqueidentifier	Activity identifier
ACTVY_NAME	varchar/nvarchar(255)	Activity name
ACTVY_TYP_CD	varchar/nvarchar(1)	Activity type code
ACCESS_LVL	varchar/nvarchar(50)	Access level
EXEC_LOC	varchar/nvarchar(50)	Execution location
ACTVY_DESC	varchar/nvarchar(255)	Activity description
PROCESSOR	varchar/nvarchar(255)	Processor
INPUT_FORMATTER	varchar/nvarchar(255)	Input formatter
OUTPUT_FORMATTER	varchar/nvarchar(255)	Output formatter
APP_NAME	varchar/nvarchar(25)	Application name
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object

Column Name	Datatype	Comment
MODIFIED_BY	int	User who last modified object

8.1.5 ADV_ATTACK_MAP_RPT_V

View references ADV_ATTACK_MAP table that stores Advisor map information.

Column Name	Datatype	Comment
ATTACK_KEY	int	ID used to reference the attack entry
SERVICE_PACK_ID	int	The Service Pack ID of the product that is effected by this attack
ATTACK_NAME	varchar/nvarchar(256)	Name of the Attack
ATTACK_CODE	varchar/nvarchar(256)	Attack code
DATE_PUBLISHED	datetime	Date the attack has been published
DATE_UPDATED	datetime	Date the attack has been updated
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_By	int	User who last modified object

8.1.6 ADV_ATTACK_PLUGIN_RPT_V

View references ADV_ATTACK_PLUGIN table that stores Advisor plug-in information.

Column Name	Datatype	Comment
PLUGIN_KEY	int	ID used to reference the vulnerability entry
SERVICE_PACK_ID	int	Service Pack ID of the product that is identified this vulnerability
PLUGIN_ID	varchar/nvarchar(256)	ID of the vulnerability
PLUGIN_NAME	varchar/nvarchar(256)	Name of the vulnerability
DATE_PUBLISHED	datetime	Date the vulnerability has been published
DATE_UPDATED	datetime	Date the vulnerability has been updated
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.7 ADV_ATTACK_RPT_V

View references ADV_ATTACK table that stores Advisor attack information.

Column Name	Datatype	Comment
ATTACK_ID	int	ID to identify the attack
TRUSECURE_ATTACK_NAME	varchar/nvarchar(512)	Name of the attack
FEED_DATE_CREATED	datetime	Date when the feed first have the information on this attack
FEED_DATE_UPDATED	datetime	Last date when the information on this attack has been updated
ATTACK_CATEGORY	varchar/nvarchar(256)	Category of the attack
URGENCY_ID	int	The urgency associated with this attack
SEVERITY_ID	int	Severity associated with this attack
LOCAL	int	Indicates if this attack was executed locally
REMOTE	int	Indicates if this attack was executed from remote
DESCRIPTION	Text	Description of the attack
SCENARIO	Text	Scenario how the attack could be made
IMPACT	Text	Impact of the attack
SAFEGUARDS	Text	Safeguards that could be followed to avert the attack
PATCHES	Text	Patches for the product to fix the vulnerability exploited by the attack
FALSE_POSITIVES	Text	False Positives associated with this attack
DATE_PUBLISHED	datetime	Date the information on this attack was published
DATE_UPDATED	datetime	Date the information on this attack was updated
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.8 ADV_ATTACK_SIGNATURES

Column Name	Datatype	Comment
ATTACK_KEY	int	Attack ID
ATTACK_SCANNER_NAME	varchar/nvarchar2(128)	Name of the attack scanner or intrusion detection system
ATTACK_NAME	varchar/nvarchar2(256)	Name of the attack
ATTACK_ID	varchar/nvarchar2(256)	ID of the attack

8.1.9 ADV_FEED_RPT_V

View references ADV_FEED table that stores Advisor feed information, such as feed name and date.

Column Name	Datatype	Comment
FEED_NAME	varchar/nvarchar(128)	Name of feed
FEED_FILE	varchar/nvarchar(256)	File name that contains the feed data
BEGIN_DATE	datetime	The date from which this feed file carries the advisor information
END_DATE	datetime	The date until which this feed file carries the advisor information
FEED_INSERT	int	Number of rows inserted into the advisor schema by this feed file
FEED_UPDATE	int	Number of rows updated into the advisor schema by this feed file
FEED_EXPIRE	int	Number of rows deleted into the advisor schema by this feed file

8.1.10 ADV_MASTER_RPT_V

Column Name	Datatype	Comment
MASTER_ID	int	ID that associates PLUGIN_KEY, ATTACK_KEY and VULN_KB_ID
PLUGIN_KEY	int	ID to reference the ADV_ATTACK_PLUGIN_V
ATTACK_KEY	int	ID to reference the ADV_ATTACK_MAP_V
VULN_KB_ID	int	ID to reference the VULN_KB_ID_V
DATE_PUBLISHED	datetime	Date the entry was published
DATE_UPDATED	datetime	Date the entry was updated

Column Name	Datatype	Comment
BEGIN_EFFECTIVE_DATE	datetime	Date from which the entry is valid
END_EFFECTIVE_DATE	datetime	Date until which the entry is valid
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.11 ADV_PRODUCT_RPT_V

View references ADV_PRODUCT table that stores Advisor product information such as vendor and product ID.

Column Name	Datatype	Comment
PRODUCT_ID	int	ID of the product
VENDOR_ID	int	ID of the vendor
PRODUCT_CATEGORY_ID	int	ID of the Product Category
PRODUCT_CATEGORY_NAME	varchar/nvarchar (128)	Product Category Name
PRODUCT_TYPE_ID	int	ID of the product type
PRODUCT_TYPE_NAME	varchar/nvarchar (256)	Name of the Product Type
PRODUCT_NAME	varchar/nvarchar (128)	Product Name
PRODUCT_DESCRIPTION	varchar/nvarchar (512)	Product Descritpion
FEED_DATE_CREATED	datetime	Date of the Feed that carried information on this product
FEED_DATE_UPDATED	datetime	Date of the Feed that updated information on this product
ACTIVE_FLAG	int	Reserved for future use
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.12 ADV_PRODUCT_SERVICE_PACK_RPT_V

View references ADV_PRODUCT_SERVICE _PACK table that stores Advisor service pack information, such as service pack name, version ID and date.

Column Name	Datatype	Comment
SERVICE_PACK_ID	int	Service Pack ID
VERSION_ID	int	Version ID
SERVICE_PACK_NAME	varchar/nvarchar (32)	Name of the Service Pack
FEED_DATE_CREATED	datetime	Date of the Feed that carried information on this product
FEED_DATE_UPDATED	datetime	Date of the Feed that updated information on this product
ACTIVE_FLAG	int	Reserved for future use
BEGIN_EFFECTIVE_DATE	datetime	Date from which the entry is valid
END_EFFECTIVE_DATE	datetime	Date until which the entry is valid
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.13 ADV_PRODUCT_VERSION_RPT_V

View references ADV_PRODUCT_VERSION table that stores Advisor product version information, such as version name, product and version ID.

Column Name	Datatype	Comment
VERSION_ID	int	Version ID
PRODUCT_ID	int	Product ID
VERSION_NAME	varchar/nvarchar (128)	Version Name of the product
FEED_DATE_CREATED	datetime	Date of the feed that carried the information on the entry
FEED_DATE_UPDATED	datetime	Date of the feed that carried the update on the entry
ACTIVE_FLAG	int	Reserved for future use
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.14 ADV_VENDOR_RPT_V

Column Name	Datatype	Comment
VENDOR_ID	integer	ID of the vendor
VENDOR_NAME	varchar/nvarchar2(128)	Name of the vendor
CONTACT_PERSON	varchar/nvarchar2(128)	Contains the contact person name for the vendor
ADDRESS_LINE_1	varchar/nvarchar2(128)	Address of the vendor
ADDRESS_LINE_2	varchar/nvarchar2(128)	Address of the vendor
ADDRESS_LINE_3	varchar/nvarchar2(128)	Address of the vendor
ADDRESS_LINE_4	varchar/nvarchar2(128)	Address of the vendor
CITY	varchar/nvarchar2(128)	City of the vendor
STATE	varchar/nvarchar2(128)	State of the vendor
COUNTRY	varchar/nvarchar2(128)	Country of the vendor
ZIP_CODE	varchar/nvarchar2(128)	Zip code of the vendor
URL	varchar/nvarchar2(256)	Web URL of the vendor
PHONE	varchar/nvarchar2(32)	Contact number of the vendor
FAX	varchar/nvarchar2(32)	Fax number of the vendor
EMAIL	varchar/nvarchar2(128)	Email of the vendor
PAGER	varchar/nvarchar2(32)	Pager of the vendor
FEED_DATE_CREATED	datetime	Date of the feed that carried the information on the entry
FEED_DATE_UPDATED	datetime	Date of the feed that carried the update on the entry
ACTIVE_FLAG	int	Reserved for future use
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.15 ADV_VULN_KB_RPT_V

Column Name	Datatype	Comment
VULN_KB_ID	int	Knowledge base ID mapping CVE_ID, OSVDB_ID, BUGTRAQ_ID

Column Name	Datatype	Comment
CVE_ID	int	CVE ID for the related vulnerability
OSVDB_ID	int	OSVDB ID for the related vulnerability
BUGTRAQ_ID	int	Bugtraq id for the related vulnerability
DATE_PUBLISHED	datetime	Date the entry was published
DATE_UPDATED	datetime	Date the entry was updated
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.16 ADV_VULN_PRODUCT_RPT_V

View references ADV_VULN_PRODUCT table that stores Advisor vulnerability attack ID and service pack ID.

Column Name	Datatype	Comment
SERVICE_PACK_ID	int	Contains the service pack id
ATTACK_ID	int	Contains the attack id
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.17 ADV_VULN_SIGNATURES

Column Name	Datatype	Comment
VULN_KEY	integer	Vulnerability key
VULN_SCANNER_NAME	varchar/nvarchar2(128)	Vulnerability scanner name
VULN_NAME	varchar/nvarchar2(256)	Vulnerability name
VULN_ID	varchar/nvarchar2(256)	Vulnerability ID

8.1.18 ANNOTATIONS_RPT_V

View references ANNOTATIONS table that stores documentation or notes that can be associated with objects in the Sentinel system such as cases and incidents.

Column Name	Datatype	Comment
ANN_ID	int	Annotation identfier - sequence number.
TEXT	varchar/nvarchar(4000)	Documentation or notes.
ACTION	varchar/nvarchar(255)	Action
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
MODIFIED_BY	int	User who last modified object
CREATED_BY	int	User who created object

8.1.19 ASSET_CATEGORY_RPT_V

View references ASSET_CTGRY table that stores information about asset categories.

Column Name	Datatype	Comment
ASSET_CATEGORY_ID	bigint	Asset category identifier
ASSET_CATEGORY_NAME	varchar/nvarchar2(100)	Asset category name
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

8.1.20 ASSET_HOSTNAME_RPT_V

View references ASSET_HOSTNAME table that stores information about alternate host names for assets.

Column Name	Datatype	Comment
ASSET_HOSTNAME_ID	uniqueidentifier	Asset alternate hostname identifier
PHYSICAL_ASSET_ID	uniqueidentifier	Physical asset identifier
HOST_NAME	varchar/nvarchar(255)	Host name
CUST_ID	bigint	Customer identifier
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.21 ASSET_IP_RPT_V

View references ASSET_IP table that stores information about alternate IP addresses for assets.

Column Name	Datatype	Comment
ASSET_IP_ID	uniqueidentifier	Asset alternate IP identifier
PHYSICAL_ASSET_ID	uniqueidentifier	Physical asset identifier
IP_ADDRESS	int	Asset IP address
CUST_ID	bigint	Customer identifier
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.22 ASSET_LOCATION_RPT_V

View references ASSET_LOC table that stores information about asset locations.

Column Name	Datatype	Comment
LOCATION_ID	bigint	Location identifier
CUST_ID	bigint	Customer identifier
BUILDING_NAME	varchar/nvarchar(255)	Building name
ADDRESS_LINE_1	varchar/nvarchar(255)	Address line 1
ADDRESS_LINE_2	varchar/nvarchar(255)	Address line 2
CITY	varchar/nvarchar(100)	City
STATE	varchar/nvarchar(100)	State
COUNTRY	varchar/nvarchar(100)	Country
ZIP_CODE	varchar/nvarchar(50)	Zip code
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.23 ASSET_RPT_V

View references ASSET table that stores information about the physical and soft assets.

Column Name	Datatype	Comment
ASSET_ID	uniqueidentifier	Asset identifier
CUST_ID	bigint	Customer identifier
ASSET_NAME	varchar/nvarchar(255)	Asset name
PHYSICAL_ASSET_ID	uniqueidentifier	Physical asset identifier
PRODUCT_ID	bigint	Product identifier
ASSET_CATEGORY_ID	bigint	Asset category identifier
ENVIRONMENT_IDENTITY_CD	bigint	Environment identify code
PHYSICAL_ASSET_IND	bit	Physical asset indicator
ASSET_VALUE_CODE	bigint	Asset value code
CRITICALITY_ID	bigint	Asset criticality code
SENSITIVITY_ID	bigint	Asset sensitivity code
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.24 ASSET_VALUE_RPT_V

View references ASSET_VAL_LKUP table that stores information about the asset value.

Column Name	Datatype	Comment
ASSET_VALUE_ID	bigint	Asset value code
ASSET_VALUE_NAME	varchar/nvarchar(50)	Asset value name
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.25 ASSET_X_ENTITY_X_ROLE_RPT_V

View references ASSET_X_ENTITY_X_ROLE table that associates a person or an organization to an asset.

Column Name	Datatype	Comment
PERSON_ID	uniqueidentifier	Person identifier

Column Name	Datatype	Comment
ORGANIZATION_ID	uniqueidentifier	Organization identifier
ROLE_CODE	varchar/nvarchar(5)	Role code
ASSET_ID	uniqueidentifier	Asset identifier
ENTITY_TYPE_CODE	varchar/nvarchar(5)	Entity type code
PERSON_ROLE_SEQUENCE	int	Order of persons under a particular role
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.26 ASSOCIATIONS_RPT_V

View references ASSOCIATIONS table that associates users to incidents, incidents to annotations and so on.

Column Name	Datatype	Comment
TABLE1	varchar/nvarchar(64)	Table name 1. For example, incidents
ID1	int	ID1. For example, incident ID.
TABLE2	varchar/nvarchar(64)	Table name 2. For example, users.
ID2	int	ID2. For example, user ID.
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.27 ATTACHMENTS_RPT_V

View references ATTACHMENTS table that stores attachment data.

Column Name	Datatype	Comment
ATTACHMENT_ID	int	Attachment identifier
NAME	varchar/nvarchar(255)	Attachment name
SOURCE_REFERENCE	varchar/nvarchar(64)	Source reference
TYPE	varchar/nvarchar(32)	Attachment type
SUB_TYPE	varchar/nvarchar(32)	Attachment subtype
FILE_EXTENSION	varchar/nvarchar(32)	File extension

Column Name	Datatype	Comment
ATTACHMENT_DESCRIPTION	varchar/nvarchar(255)	Attachment description
DATA	ntext	Attachment data
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.28 AUDIT_RECORD_RPT_V

View reference AUDIT_RECORD table that stores Sentinel internal audit data.

Column Name	Datatype	Comment
AUDIT_ID	uniqueidentifier	Audit record identifier
AUDIT_TYPE	varchar/nvarchar(255)	Audit type
SRC	varchar/nvarchar(255)	Audit source
SENDER_HOSTNAME	varchar/nvarchar(255)	Sender hostname
SENDER_HOST_IP	varchar/nvarchar(255)	Sender host IP
SENDER_CONTAINER	varchar/nvarchar(255)	Sender container name
SENDER_ID	varchar/nvarchar(255)	Sender Identifier
CLIENT	varchar/nvarchar(255)	Client application that requested audit
EVT_NAME	varchar/nvarchar(255)	Event name
RES	varchar/nvarchar(255)	Event resource
SRES	varchar/nvarchar(255)	Event sub-resource
MSG	varchar/nvarchar(500)	Event message
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified

8.1.29 CONFIGS_RPT_V

View references CONFIGS table that stores general configuration information of the application.

Column Name	Datatype	Comment
USR_ID	varchar/nvarchar(32)	User name.

Column Name	Datatype	Comment
APPLICATION	varchar/nvarchar(255)	Application identifier
UNIT	varchar/nvarchar(64)	Application unit
VALUE	varchar/nvarchar(255)	Text value if any
DATA	ntext	XML data
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.30 CONTACTS_RPT_V

View references CONTACTS table that stores contact information.

Column Name	Datatype	Comment
CNT_ID	int	Contact ID - Sequence number
FIRST_NAME	varchar/nvarchar(20)	Contact first name.
LAST_NAME	varchar/nvarchar(30)	Contact last name.
TITLE	varchar/nvarchar(128)	Contact title
DEPARTMENT	varchar/nvarchar(128)	Department
PHONE	varchar/nvarchar(64)	Contact phone
EMAIL	varchar/nvarchar(255)	Contact email
PAGER	varchar/nvarchar(64)	Contact pager
CELL	varchar/nvarchar(64)	Contact cell phone
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.31 CORRELATED_EVENTS_RPT_V (legacy view)

This view is provided for backward compatibility. New reports should use CORRELATED_EVENTS_RPT_V1 because this view does not include archived correlated events that have been imported back into the database.

8.1.32 CORRELATED_EVENTS_RPT_V1

View contains current and historical correlated events (correlated events imported from archives).

Column Name	Datatype	Comment
PARENT_EVT_ID	uniqueidentifier	Event Universal Unique Identifier (UUID) of parent event
CHILD_EVT_ID	uniqueidentifier	Event Universal Unique Identifier (UUID) of child event
PARENT_EVT_TIME	datetime	Parent event time
CHILD_EVT_TIME	datetime	Child event time
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.33 CRITICALITY_RPT_V

View references CRIT_LKUP table that contains information about asset criticality.

Column Name	Datatype	Comment
CRITICALITY_ID	bigint	Asset criticality code
CRITICALITY_NAME	varchar/nvarchar(50)	Asset criticality name
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.34 CUST_HIERARCHY_V

View references CUST_HIERARCHY table that stores information about MSSP customer hierarchy.

Column Name	Datatype	Comment
CUST_HIERARCHY_ID	bigint	Customer hierarchy ID
CUST_NAME	varchar/nvarchar (255)	Customer
CUST_HIERARCHY_LVL1	varchar/nvarchar (255)	Customer hierarchy level 1
CUST_HIERARCHY_LVL2	varchar/nvarchar (255)	Customer hierarchy level 2
CUST_HIERARCHY_LVL3	varchar/nvarchar (255)	Customer hierarchy level 3
CUST_HIERARCHY_LVL4	varchar/nvarchar (255)	Customer hierarchy level 4
DATE_CREATED	datetime	Date the entry was created

Column Name	Datatype	Comment
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.35 CUST_RPT_V

View references CUST table that stores customer information for MSSPs.

Column Name	Datatype	Comment
CUST_ID	bigint	Customer identifier
CUSTOMER_NAME	varchar/nvarchar(255)	Customer name
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.36 ENTITY_TYPE_RPT_V

View references ENTITY_TYP table that stores information about entity types (person, organization).

Column Name	Datatype	Comment
ENTITY_TYPE_CODE	varchar/nvarchar(5)	Entity type code
ENTITY_TYPE_NAME	varchar/nvarchar(50)	Entity type name
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.37 ENV_IDENTITY_RPT_V

View references ENV_IDENTITY_LKUP table that stores information about asset environment identity.

Column Name	Datatype	Comment
ENVIRONMENT_IDENTITY_ID	bigint	Environment identity code
ENV_IDENTITY_NAME	varchar/nvarchar(255)	Environment identity name

Column Name	Datatype	Comment
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.38 ESEC_CONTENT_GRP_CONTENT_RPT_V

Column Name	Datatype	Comment
CONTENT_GRP_ID	uniqueidentifier	Content group identifier
CONTENT_ID	varchar/nvarchar(255)	Content identifier
CONTENT_TYP	varchar/nvarchar(100)	Content type
CONTENT_HASH	varchar/nvarchar(255)	Content hash
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.39 ESEC_CONTENT_GRP_RPT_V

Column Name	Datatype	Comment
CONTENT_GRP_ID	uniqueidentifier	Content group identifier
CONTENT_GRP_NAME	varchar/nvarchar(255)	Content group name
CONTENT_GRP_DESC	text	Content group description
CTRL_ID	uniqueidentifier	Control identifier
CONTENT_EXTERNAL_ID	varchar/nvarchar(255)	Content external identifier
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.40 ESEC_CONTENT_PACK_RPT_V

Column Name	Datatype	Comment
CONTENT_PACK_ID	uniqueidentifier	Content pack identifier
CONTENT_PACK_DESC	text	Content pack description
CONTENT_PACK_NAME	varchar/nvarchar(255)	Content pack name
CONTENT_EXTERNAL_ID	varchar/nvarchar(255)	Content external identifier
DATE_MODIFIED	datetime	Date the entry was modified
DATE_CREATED	datetime	Date the entry was created
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.41 ESEC_CONTENT_RPT_V

Column Name	Datatype	Comment
CONTENT_ID	varchar/nvarchar(255)	Content identifier
CONTENT_NAME	varchar/nvarchar(255)	Content name
CONTENT_DESC	text	Content description
CONTENT_STATE	int	Content state
CONTENT_TYP	varchar/nvarchar(100)	Content type
CONTENT_CONTEXT	text	Content context
CONTENT_HASH	varchar/nvarchar(255)	Content hash
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
MODIFIED_BY	int	User who last modified object
CREATED_BY	int	User who created object

8.1.42 ESEC_CTRL_CTGRY_RPT_V

Column Name	Datatype	Comment
CTRL_CTGRY_ID	uniqueidentifier	Control category identifier
CTRL_CTGRY_DESC	text	Control category description
CTRL_CTGRY_NAME	varchar/nvarchar(255)	Control category name
CONTENT_PACK_ID	uniqueidentifier	Content pack identifier

Column Name	Datatype	Comment
CONTENT_EXTERNAL_ID	varchar/nvarchar(255)	Content external identifier
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.43 ESEC_CTRL_RPT_V

Column Name	Datatype	Comment
CTRL_ID	uniqueidentifier	Control identifier
CTRL_NAME	varchar/nvarchar(255)	Control name
CTRL_DESC	text	Control description
CTRL_STATE	int	Control state
CTRL_NOTES	text	Control notes
CTRL_CTGRY_ID	uniqueidentifier	Control category identifier
CONTENT_EXTERNAL_ID	varchar/nvarchar(255)	Content external identifier
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.44 ESEC_DISPLAY_RPT_V

View references ESEC_DISPLAY table that stores displayable properties of objects. Currently used in renaming meta-tags. Used with Event Configuration (Business Relevance).

Column Name	Datatype	Comment
DISPLAY_OBJECT	varchar/nvarchar(32)	The parent object of the property
TAG	varchar/nvarchar(32)	The native tag name of the property
LABEL	varchar/nvarchar(32)	The display string of tag.
POSITION	int	Position of tag within display.
WIDTH	int	The column width
ALIGNMENT	int	The horizontal alignment
FORMAT	int	The enumerated formatter for displaying the property

Column Name	Datatype	Comment
ENABLED	bit	Indicates if the tag is shown.
TYPE	int	Indicates datatype of tag. 1 = string 2 = ulong 3 = date 4 = uuid 5 = ipv4
DESCRIPTION	varchar/nvarchar(255)	Textual description of the tag
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object
REF_CONFIG	varchar/nvarchar(4000)	Referential data configuration

8.1.45 ESEC_PORT_REFERENCE_RPT_V

View references ESEC_PORT_REFERENCE table that stores industry standard assigned port numbers.

Column Name	Datatype	Comment
PORT_NUMBER	int	Per http://www.iana.org/assignments/port-numbers (http://www.iana.org/assignments/port-numbers), the numerical representation of the port. This port number is typically associated with the Transport Protocol level in the TCP/IP stack.
PROTOCOL_NUMBER	int	Per http://www.iana.org/assignments/protocol-numbers (http://www.iana.org/assignments/protocol-numbers), the numerical identifiers used to represent protocols that are encapsulated in an IP packet.
PORT_KEYWORD	varchar/nvarchar(64)	Per http://www.iana.org/assignments/port-numbers (http://www.iana.org/assignments/port-numbers), the keyword representation of the port.
PORT_DESCRIPTION	varchar/nvarchar(512)	Port description.
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified

Column Name	Datatype	Comment
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.46 ESEC_PROTOCOL_REFERENCE_RPT_V

View references ESEC_PROTOCOL_REFERENCE table that stores industry standard assigned protocol numbers.

Column Name	Datatype	Comment
PROTOCOL_NUMBER	int	Per http://www.iana.org/assignments/protocol-numbers (http://www.iana.org/assignments/protocol-numbers), the numerical identifiers used to represent protocols that are encapsulated in an IP packet.
PROTOCOL_KEYWORD	varchar/nvarchar(64)	Per http://www.iana.org/assignments/protocol-numbers (http://www.iana.org/assignments/protocol-numbers), the keyword used to represent protocols that are encapsulated in an IP packet.
PROTOCOL_DESCRIPTION	varchar/nvarchar(512)	IP packet protocol description.
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.47 ESEC_SEQUENCE_RPT_V

View references ESEC_SEQUENCE table that's used to generate primary key sequence numbers for Sentinel tables.

Column Name	Datatype	Comment
TABLE_NAME	varchar/nvarchar(32)	Name of the table.
COLUMN_NAME	varchar/nvarchar(255)	Name of the column
SEED	int	Current value of primary key field.
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.48 ESEC_UUID_UUID_ASSOC_RPT_V

Column Name	Datatype	Comment
OBJECT1	varchar/nvarchar(64)	Object 1
ID1	uniqueidentifier	UUID for object 1
OBJECT2	varchar/nvarchar(64)	Object 2
ID2	uniqueidentifier	UUID for object 2
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.49 EVENTS_ALL_RPT_V (legacy view)

This view is provided for backward compatibility. View contains current and historical events (events imported from archives).

8.1.50 EVENTS_ALL_RPT_V1 (legacy view)

This view is provided for backward compatibility. New reports should use EVENTS_RPT_V2. View contains current events.

8.1.51 EVENTS_ALL_V (legacy view)

This view is provided for backward compatibility. New reports should use EVENTS_RPT_V2.

8.1.52 EVENTS_RPT_V (legacy view)

This view is provided for backward compatibility. New reports should use EVENTS_RPT_V2. View contains current and historical events.

8.1.53 EVENTS_RPT_V1 (legacy view)

This view is provided for backward compatibility. New reports should use EVENTS_RPT_V2. View contains current events.

8.1.54 EVENTS_RPT_V2

This is the primary reporting view. View contains current event and historical events.

Column Name	Datatype	Comment
EVENT_ID	uniqueidentifier	Event identifier

Column Name	Datatype	Comment
RESOURCE_NAME	varchar/nvarchar(255)	Resource name
SUB_RESOURCE	varchar/nvarchar(255)	Subresource name
SEVERITY	int	Event severity
EVENT_PARSE_TIME	datetime	Event time
EVENT_DATETIME	datetime	Event time
EVENT_DEVICE_TIME	datetime	Event device time
SENTINEL_PROCESS_TIME	datetime	Sentinel process time
BEGIN_TIME	datetime	Events begin time
END_TIME	datetime	Events end time
REPEAT_COUNT	int	Events repeat count
DESTINATION_PORT_Int	int	Destination port (integer)
SOURCE_PORT_Int	int	Source port (integer)
BASE_MESSAGE	varchar/nvarchar(4000)	Base message
EVENT_NAME	varchar/nvarchar(255)	Name of the event as reported by the sensor
EVENT_TIME	varchar/nvarchar(255)	Event time as reported by the sensor
AGENT_ID	bigint	Collector identifier
SOURCE_IP	int	Source IP address in numeric format
SOURCE_IP_DOTTED	varchar/nvarchar (16)	Source IP in dotted format
SOURCE_HOST_NAME	varchar/nvarchar(255)	Source host name
SOURCE_PORT	varchar/nvarchar(32)	Source port
DESTINATION_IP	int	Destination IP address in numeric format
DESTINATION_IP_DOTTED	varchar/nvarchar (16)	Destination IP in dotted format
DESTINATION_HOST_NAME	varchar/nvarchar(255)	Destination host name
DESTINATION_PORT	varchar/nvarchar(32)	Destination port
SOURCE_USER_NAME	varchar/nvarchar(255)	Source user name
DESTINATION_USER_NAME	varchar/nvarchar(255)	Destination user name
FILE_NAME	varchar/nvarchar(1000)	File name
EXTENDED_INFO	varchar/nvarchar(1000)	Extened information
CUSTOM_TAG_1	varchar/nvarchar(255)	Customer Tag 1
CUSTOM_TAG 2	varchar/nvarchar(255)	Customer Tag 2
CUSTOM_TAG 3	int	Customer Tag 3

Column Name	Datatype	Comment
RESERVED_TAG_1	varchar/nvarchar(255)	Reserved Tag 1 Reserved for future use by Sentinel. This field is used for Advisor information concerning attack descriptions.
RESERVED_TAG_2	varchar/nvarchar(255)	Reserved for future use by Sentinel. Use of this field for any other purpose might result in data being overwritten by future functionality.
RESERVED_TAG_3	int	Reserved for future use by Sentinel. Use of this field for any other purpose might result in data being overwritten by future functionality.
Vulnerability_Rating	int	Vulnerability rating
Criticality_Rating	int	Criticality rating
RV01 - 10	int	Reserved Value 1 - 10 Reserved for future use by Sentinel. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV11 - 20	DATETIME	Reserved Value 1 - 31 Reserved for future use by Sentinel. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV21 - 25	uniqueidentifier	Reserved Value 21 - 25 Reserved for future use by Sentinel to store UUIDs. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV26 - 31	varchar/nvarchar(255)	Reserved Value 26 - 31 Reserved for future use by Sentinel. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV33	varchar/nvarchar(255)	Reserved Value 33 Reserved for EventContex Use of this field for any other purpose might result in data being overwritten by future functionality.

Column Name	Datatype	Comment
RV34	varchar/nvarchar(255)	Reserved Value 34 Reserved for SourceThreatLevel Use of this field for any other purpose might result in data being overwritten by future functionality.
RV35	varchar/nvarchar(255)	Reserved Value 35 Reserved for SourceUserContext. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV36	varchar/nvarchar(255)	Reserved Value 36 Reserved for DataContext. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV37	varchar/nvarchar(255)	Reserved Value 37 Reserved for SourceFunction. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV38	varchar/nvarchar(255)	Reserved Value 38 Reserved for SourceOperationalContext. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV39	varchar/nvarchar(255)	
RV40 - 43	varchar/nvarchar(255)	Reserved Value 40 - 43 Reserved for future use by Sentinel. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV44	varchar/nvarchar(255)	Reserved Value 44 Reserved for DestinationThreatLevel. Use of this field for any other purpose might result in data being overwritten by future functionality.

Column Name	Datatype	Comment
RV45	varchar/nvarchar(255)	Reserved Value 45 Reserved for DestinationUserContext. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV46	varchar/nvarchar(255)	Reserved Value 46 Reserved for VirusStatus. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV47	varchar/nvarchar(255)	Reserved Value 47 Reserved for future use by Sentinel. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV48	varchar/nvarchar(255)	Reserved Value 48 Reserved for DestinationOperationalContext. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV49	varchar/nvarchar(255)	Reserved Value 49 Reserved for future use by Sentinel. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV50-53	varchar/nvarchar(255)	
REFERENCE_ID 01 - 20	bigint	Reserved for future use by Sentinel. Use of this field for any other purpose might result in data being overwritten by future functionality.
CV01 - 10	int	Custom Value 1 - 10 Reserved for use by Customer, typically for association of Business relevant data
CV11 - 20	datetime	Custom Value 11 - 20 Reserved for use by Customer, typically for association of Business relevant data
CV21 - 100	varchar/nvarchar(255)	Custom Value 21 – 100 Reserved for use by Customer, typically for association of Business relevant data
CV30 - 34	varchar/nvarchar(4000)	

Column Name	Datatype	Comment
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.55 EVENTS_RPT_V3

Column Name	Datatype	Comment
Event_ID	uniqueidentifier	Event identifier
Sub_Resource_Name	varchar/nvarchar(255)	Subresource name
Severity	int	Event severity
Event_Parse_Time	datetime	Event time
Event_Device_Time	datetime	Event device time
Device_Event_Time	datetime	
Sentinel_Process_Time	datetime	Sentinel process time
Begin_Time	datetime	Events begin time
End_Time	datetime	Events end time
Target_Service_Port	int	Target service port
Event_Time	varchar/nvarchar(255)	Event time
Init_Asset_id	bigint	Initiator asset identifier
Target_Asset_id	bigint	Target asset identifier
Target_IP	int	Target IP address in numeric format
Target_IP_Dotted	varchar/nvarchar (16)	Target IP address in dotted format
Target_Host_Name	varchar/nvarchar(255)	Target host name
Init_User_Name	varchar/nvarchar(255)	Initiator user name
Target_User_Name	varchar/nvarchar(255)	Target user name
File_Name	varchar/nvarchar(1000)	File name
Extended_Info	varchar/nvarchar(1000)	Extened information
Init_User_ Id	varchar/nvarchar(255)	Initiator user ID
Init_Usr_Identity	uniqueidentifier	Initiator user identity
Target_User_Id	varchar/nvarchar(255)	Target user ID
Target_User_Identity	uniqueidentifier	Target user identity
Effective_User_Name	varchar/nvarchar(255)	Effective user name

Column Name	Datatype	Comment
Effective_User_Sys_Id	varchar/nvarchar(255)	Effective user ID
Effective_User_Domain	varchar/nvarchar(255)	Effective user domain
Target_Trust_Name	varchar/nvarchar(255)	Target trust name
Target_Trust_Sys_Id	varchar/nvarchar(255)	Target trust ID
Target_Trust_Domain	varchar/nvarchar(255)	Target trust domain
Observer_Ip	int	Observer IP address in numeric format
Reporter_Ip	int	Reporter IP address in numeric format
Observer_Host_Domain	varchar/nvarchar(255)	Observer host domain
Reporter_Host_Domain	varchar/nvarchar(255)	Reporter host domain
Observer_Asset_Id	varchar/nvarchar(255)	Observer asset identifier
Reporter_Asset_Id	varchar/nvarchar(255)	Reporter asset identifier
Init_Service_Comp	varchar/nvarchar(255)	Initiator service component
Target_Service_Comp	varchar/nvarchar(255)	Target service component
Custom_Tag_1	varchar/nvarchar(255)	Customer Tag 1
Custom_Tag_2	varchar/nvarchar(255)	Customer Tag 2
Custom_Tag_3	int	Customer Tag 3
Reserved_Tag_1	varchar/nvarchar(255)	
Reserved_Tag_2	varchar/nvarchar(255)	
Reserved_Tag_3	int	
Vulnarability_Rating	int	
Criticality_Rating	int	
Date_Created	datetime	Date the entry was created
Date_Modified	datetime	Date the entry was modified
Created_By	int	User who created object
Modified_By	int	User who last modified object
RV01	int	
Event_Metric	int	Event metric
Data_Tag_Id	int	Data tag ID
RV04-RV10	int	
RV11-RV20	datetime	
RV21-RV28	varchar/nvarchar(255)	
Init_IP_Country	varchar/nvarchar(255)	Initiator country

Column Name	Datatype	Comment
Target_IP_Country	varchar/nvarchar(255)	Target country
RV31	varchar/nvarchar(255)	
RV33		
RV36		
RV40		
RV43		
RV46		
RV49		
Init_Threat_Level	varchar/nvarchar(255)	Initiator threat level
Init_User_Domain	varchar/nvarchar(255)	Initiator user domain
Init_Function	varchar/nvarchar(255)	Initiator function
Init_Operational_Context	varchar/nvarchar(255)	Initiator operational context
Target_Host_Domain	varchar/nvarchar(255)	Target host domain
Target_Threat_Level	varchar/nvarchar(255)	Target threat level
Target_User_Domain	varchar/nvarchar(255)	Target user domain
Target_Function	varchar/nvarchar(255)	Target function
Target_Operational_Context	varchar/nvarchar(255)	Target operational context
Taxonomy_id	bigint	Taxonomy identifier
Reference_id_1	bigint	
XDAS_Taxonomy_Id	bigint	XDAS Taxonomy identifier
Reference_id_2-Reference_id_20		
CV01-CV10	int	
CV11-CV20	datetime	
CV21-CV29	varchar/nvarchar(255)	
CV30-CV34	varchar/nvarchar(4000)	
CV35-CV100	varchar/nvarchar(255)	
Customer_Var_101-Customer_Var_110	int	
Customer_Var_111-Customer_Var_120	datetime	
Customer_Var_121-Customer_Var_130	uniqueidentifier	
Customer_Var_131-Customer_Var_140	int	

Column Name	Datatype	Comment
Customer_Var_141-Customer_Var_150	varchar/nvarchar(255)	

8.1.56 EVT_AGENT_RPT_V

View references EVT_AGENT table that stores information about Collectors.

Column Name	Datatype	Comment
Agent_ID	bigint	Collector identifier
CUST_ID	bigint	Customer identifier
Agent	varchar/nvarchar(64)	Collector name
Port	varchar/nvarchar(64)	Collector port
Report_Name	varchar/nvarchar(255)	Reporter name
Product_Name	varchar/nvarchar(255)	Product name
Sensor_Name	varchar/nvarchar(255)	Sensor name
Sensor_Type	varchar/nvarchar(5)	Sensor type: H - host-based N - network-based V - virus O - other
Device_Category	varchar/nvarchar(255)	Device category
Source_UUID	uniqueidentifier	Source component Universal Unique Identifier (UUID)
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.57 EVT_AGENT_RPT_V3

Column Name	Datatype	Comment
Agent_ID	bigint	Collector identifier
Cust_ID	bigint	Customer identifier
Agent	varchar/nvarchar(64)	Collector
Port	varchar/nvarchar(64)	Port

Column Name	Datatype	Comment
Reporter_Host_Name	varchar/nvarchar(255)	Reporter host name
Sensor_Type	varchar/nvarchar(5)	Sensor type: H - host-based N - network-based V - virus O - other
Device_Category	varchar/nvarchar(255)	Device category
Source_UUID	uniqueidentifier	Source component Universal Unique Identifier (UUID)
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.58 EVT_ASSET_RPT_V

View references EVT_ASSET table that stores asset information.

Column Name	Datatype	Comment
Event_Asset_ID	bigint	Event asset identifier
CUST_ID	bigint	Customer identifier
Asset_Name	varchar/nvarchar(255)	Asset name
Physical_Asset_Name	varchar/nvarchar(255)	Physical asset name
Reference_Asset_IDvarchar/ nvarchar(100)	Reference asset identifier, links to source asset management system.	Reference_Asset_IDvarchar/ nvarchar(100)
Mac_Address	varchar/nvarchar(100)	MAC address
Rack_Number	varchar/nvarchar(50)	Rack number
Room_Name	varchar/nvarchar(100)	Room name
Building_Name	varchar/nvarchar(255)	Building name
City	varchar/nvarchar(100)	City
State	varchar/nvarchar(100)	State
Country	varchar/nvarchar(100)	Country
Zip_Code	varchar/nvarchar(50)	Zip code
Asset_Category_Name	varchar/nvarchar(100)	Asset category name

Column Name	Datatype	Comment
Network_Identity_Name	varchar/nvarchar(255)	Asset network identity name
Environment_Identity_Name	varchar/nvarchar(255)	Environment name
Asset_Value_Name	varchar/nvarchar(50)	Asset value name
Criticality_Name	varchar/nvarchar(50)	Asset criticality name
Sensitivity_Name	varchar/nvarchar(50)	Asset sensitivity name
Contact_Name_1	varchar/nvarchar(255)	Name of contact person/ organization 1
Contact_Name_2	varchar/nvarchar(255)	Name of contact person/ organization 2
Organization_Name_1	varchar/nvarchar(100)	Asset owner organization level 1
Organization_Name_2	varchar/nvarchar(100)	Asset owner organization level 2
Organization_Name_3	varchar/nvarchar(100)	Asset owner organization level 3
Organization_Name_4	varchar/nvarchar(100)	Asset owner organization level 4
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.59 EVT_ASSET_RPT_V3

Asset_Department	varchar/nvarchar(100)	Asset department
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.60 EVT_DEST_EVT_NAME_SMRY_1_RPT_V

View summarizes event count by destination, taxonomy, event name, severity and event time.

Column Name	Datatype	Comment
Destination_IP	int	Destination IP address
Destination_Event_Asset_ID	bigint	Event asset identifier
Taxonomy_ID	bigint	Taxonomy identifier
Event_Name_ID	bigint	Event name identifier

Column Name	Datatype	Comment
Severity	int	Event severity
CUST_ID	bigint	Customer identifier
Event_Tme	datetime	Event time
Event_Count	int	Event count
Date_Created	datetime	Date the entry was created
Date_Modified	datetime	Date the entry was modified
Created_By	int	User who created object
Modified_By	int	User who last modified object
Destination_Host_Name	varchar/nvarchar(255)	Destination host name

8.1.61 EVT_DEST_SMRY_1_RPT_V

View contains event destination summary information.

Column Name	Datatype	Comment
Destination_IP	int	Destination IP address
Destination_Event_Asset_ID	bigint	Event asset identifier
Destination_Port	varchar/nvarchar(32)	Destination port
Destination_Usr_ID	bigint	Destination user identifier
Taxonomy_ID	bigint	Taxonomy identifier
Event_Name_ID	bigint	Event name identifier
Resource_ID	bigint	Resource identifier
Agent_ID	bigint	Collector identifier
Protocol_ID	bigint	Protocol identifier
Severity	int	Event severity
CUST_ID	bigint	Customer identifier
Event_Time	datetime	Event time
XDAS_Taxonomy_id	bigint	XDAS taxonomy identifier
Target_User_Identity	uniqueidentifier	Target user identity
Event_Count	int	Event count
Date_Created	datetime	Date the entry was created
Date_Modified	datetime	Date the entry was modified
Created_By	int	User who created object
Modified_By	int	User who last modified object

Column Name	Datatype	Comment
Destination_Host_Name	varchar/nvarchar(255)	Destination host name

8.1.62 EVT_DEST_TXNMY_SMRY_1_RPT_V

View summarizes event count by destination, taxonomy, severity and event time.

Column Name	Datatype	Comment
Destination_IP	int	Destination IP address
Destination_Event_Asset_ID	bigint	Event asset identifier
Taxonomy_ID	bigint	Taxonomy identifier
Severity	int	Event severity
CUST_ID	bigint	Customer identifier
Event_Time	datetime	Event time
XDAS_Taxonomy_id	bigint	XDAS taxonomy identifier
Event_Count	int	Event count
Date_Created	datetime	Date the entry was created
Date_Modified	datetime	Date the entry was modified
Created_By	int	User who created object
Modified_By	int	User who last modified object
Destination_Host_Name	varchar/nvarchar(255)	Destination host name

8.1.63 EVT_NAME_RPT_V

View references EVT_NAME table that stores event name information.

Column Name	Datatype	Comment
Event_Name_ID	bigint	Event name identifier
Event_Name	varchar/nvarchar(255)	Event name
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.64 EVT_PORT_SMRY_1

Column Name	Datatype	Comment
DEST_PORT	varchar/nvarchar(32)	Destination port
SEV	int	Severity
CUST_ID	bigint	Customer identifier
EVT_TIME	datetime	Event time
EVT_CNT	int	Event count
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.65 EVT_PORT_SMRY_1_RPT_V

View summarizes event count by destination port, severity and event time.

Column Name	Datatype	Comment
Destination_Port	varchar/nvarchar(32)	Destination port
Severity	int	Event severity
Cust_ID	bigint	Customer identifier
Event_Time	datetime	Event time
Event_Count	int	Event count
Date_Created	datetime	Date the entry was created
Date_Modified	datetime	Date the entry was modified
Created_By	int	User who created object
Modified_By	int	User who last modified object

8.1.66 EVT_PRTCL_RPT_V

View references EVT_PRTCL table that stores event protocol information.

Column Name	Datatype	Comment
Protocol_ID	bigint	Protocol identifier
Protocol_Name	varchar/nvarchar(255)	Protocol name
DATE_CREATED	datetime	Date the entry was created

Column Name	Datatype	Comment
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.67 EVT_RSRC_RPT_V

View references EVT_RSRC table that stores event resource information.

Column Name	Datatype	Comment
Resource_ID	bigint	Resource identifier
CUST_ID	bigint	Customer identifier
Resource_Name	varchar/nvarchar(255)	Resource name
Sub_Resource_Name	varchar/nvarchar(255)	Subresource name
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.68 EVT_SEV_SMRY_1_RPT_V

View summarizes event count by severity and event time.

Column Name	Datatype	Comment
Severity	int	Event severity
CUST_ID	bigint	Customer identifier
Event_Time	datetime	Event time
Event_Count	int	Event count
Date_Created	datetime	Date the entry was created
Date_Modified	datetime	Date the entry was modified
Created_By	int	User who created object
Modified_By	int	User who last modified object

8.1.69 EVT_SRC_COLLECTOR_RPT_V

Column Name	Datatype	Comment
EVT_SRC_COLLECTOR_ID	uniqueidentifier	Event source collector identifier
SENTINEL_PLUGIN_ID	uniqueidentifier	Sentine plugin identifier
EVT_SRC_MGR_ID	uniqueidentifier	Event source manager identifier
EVT_SRC_COLLECTOR_NAME	varchar/nvarchar(255)	Event source collector name
STATE_IND	bit	State indicator
EVT_SRC_COLLECTOR_PROPS	ntext	Event source collector prop
MAP_FILTER	ntext	Map filter
CREATED_BY	int	Date the entry was created
MODIFIED_BY	int	Date the entry was modified
DATE_CREATED	datetime	User who created object
DATE_MODIFIED	datetime	User who last modified object

8.1.70 EVT_SRC_GRP_RPT_V

Column Name	Datatype	Comment
EVT_SRC_GRP_ID	uniqueidentifier	Event source group identifier
EVT_SRC_COLLECTOR_ID	uniqueidentifier	Event source collector identifier
SENTINEL_PLUGIN_ID	uniqueidentifier	Sentinel plugin identifier
EVT_SRC_SRVR_ID	uniqueidentifier	Event source server identifier
EVT_SRC_GRP_NAME	varchar/nvarchar(255)	Event source group name
STATE_IND	bit	State indicator
MAP_FILTER	ntext	Map filter
EVT_SRC_DEFAULT_CONFIG	ntext	Event source default configuration
CREATED_BY	int	Date the entry was created
MODIFIED_BY	int	Date the entry was modified
DATE_CREATED	datetime	User who created object
DATE_MODIFIED	datetime	User who last modified object

8.1.71 EVT_SRC_MGR_RPT_V

Column Name	Datatype	Comment
EVT_SRC_MGR_ID	uniqueidentifier	Event source manager identifier
SENTINEL_ID	uniqueidentifier	Sentinel identifier
SENTINEL_HOST_ID	uniqueidentifier	Sentinel host identifier
EVT_SRC_MGR_NAME	varchar/nvarchar(255)	Event source manager name
STATE_IND	bit	State indicator
EVT_SRC_MGR_CONFIG	ntext	Event source manager configu
CREATED_BY	int	Date the entry was created
MODIFIED_BY	int	Date the entry was modified
DATE_CREATED	datetime	User who created object
DATE_MODIFIED	datetime	User who last modified object

8.1.72 EVT_SRC_OFFSET_RPT_V

Column Name	Datatype	Comment
EVT_SRC_ID	uniqueidentifier	Event source identifier
OFFSET_VAL	ntext	Offset value
OFFSET_TIMESTAMP	datetime	Offset timestamp
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified

8.1.73 EVT_SRC_RPT_V

Column Name	Datatype	Comment
EVT_SRC_ID	uniqueidentifier	Event source identifier
EVT_SRC_NAME	varchar/nvarchar(255)	Event source name
EVT_SRC_GRP_ID	uniqueidentifier	Event source group identifier
STATE_IND	bit	State indicator
MAP_FILTER	ntext	Map filter
EVT_SRC_CONFIG	ntext	Event source config

Column Name	Datatype	Comment
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified

8.1.74 EVT_SRC_SMRY_1_RPT_V

View contains event source and destination summary information.

Column Name	Datatype	Comment
Source_IP	int	Source IP address
Source_Event_Asset_ID	bigint	Event asset identifier
Source_Port	varchar/nvarchar(32)	Source port
Source_User_ID	bigint	User identifier
Taxonomy _ID	bigint	Taxonomy identifier
Event_Name_ID	bigint	Event name identifier
Resource_ID	bigint	Resource identifier
Agent_ID	bigint	Collector identifier
Protocol _ID	bigint	Protocol identifier
Severity	int	Event severity
CUST_ID	bigint	Customer identifier
Event_Time	datetime	Event time
XDAS_Taxonomy_id	bigint	XDAS taxonomy id
Init_User_Identity	uniqueidentifier	Initiator user identity
Event_Count	int	Event count
Date_Created	datetime	Date the entry was created
Date_Modified	datetime	Date the entry was modified
Created_By	int	User who created object
Modified_By	int	User who last modified object
Source_Host_Name	varchar/nvarchar(255)	Source host name

8.1.75 EVT_SRC_SRVR_RPT_V

Column Name	Datatype	Comment
EVT_SRC_SRVR_ID	uniqueidentifier	Event source server identifier
EVT_SRC_SRVR_NAME	varchar/nvarchar(255)	Event source server name
EVT_SRC_MGR_ID	uniqueidentifier	Event source manager identifier
SENTINEL_PLUGIN_ID	uniqueidentifier	Sentinel plugin identifier
STATE_IND	bit	State indicator
EVT_SRC_SRVR_CONFIG	ntext	Event source server configuration
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified

8.1.76 EVT_TXNMY_RPT_V

View references EVT_TXNMY table that stores event taxonomy information.

Column Name	Datatype	Comment
Taxonomy _ID	bigint	Taxonomy identifier
Taxonomy _ Level _1	varchar/nvarchar(100)	Taxonomy level 1
Taxonomy _ Level _2	varchar/nvarchar(100)	Taxonomy level 2
Taxonomy _ Level _3	varchar/nvarchar(100)	Taxonomy level 3
Taxonomy _ Level _4	varchar/nvarchar(100)	Taxonomy level 4
Device_Category	varchar/nvarchar(255)	
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.77 EVT_USR_RPT_V

View references EVT_USR table that stores event user information.

Column Name	Datatype	Comment
User_ID	bigint	User identifier

Column Name	Datatype	Comment
User_Name	varchar/nvarchar(255)	User name
User_Domain	varchar/nvarchar(255)	
CUST_ID	bigint	Customer identifier
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.78 EVT_XDAS_TXNMY_RPT_V

Column Name	Datatype	Comment
XDAS_TXNMY_NAME	varchar/nvarchar(255)	XDAS taxonomy name
XDAS_OUTCOME_NAME	varchar/nvarchar(255)	XDAS outcome name
Xdas_Registry	int	XDAS registry
Xdas_Provider	int	XDAS provider
Xdas_Class	int	XDAS class
Xdas_Identifier	int	XDAS identifier
Xdas_Outcome	int	XDAS outcome
Xdas_Detail	int	XDAS detail
Xdas_Taxonomy_Id	bigint	XDAS taxonomy identifier
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.79 EXTERNAL_DATA_RPT_V

View references EXTERNAL_DATA table that stores external data.

Column Name	Datatype	Comment
EXTERNAL_DATA_ID	int	External data identifier
SOURCE_NAME	varchar/nvarchar(50)	Source name
SOURCE_DATA_ID	varchar/nvarchar(255)	Source data identifier
EXTERNAL_DATA	ntext	External data

Column Name	Datatype	Comment
EXTERNAL_DATA_TYPE	varchar/nvarchar(10)	External data type
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.80 HIST_CORRELATED_EVENTS

Column Name	Datatype	Comment
PARENT_EVT_ID	uniqueidentifier	Event Universal Unique Identifier (UUID) of parent event
CHILD_EVT_ID	uniqueidentifier	Event Universal Unique Identifier (UUID) of child event
PARENT_EVT_TIME	datetime	Parent event created time
CHILD_EVT_TIME	datetime	Child event created time
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.81 HIST_CORRELATED_EVENTS_RPT_V (legacy view)

This view is provided for backward compatibility. New reports should use CORRELATED_EVENTS_RPT_V1.

8.1.82 HIST_EVENTS

Column Name	Datatype	Comment
EVT_ID	uniqueidentifier	Event Universal Unique Identifier (UUID)
EVT_TIME	datetime	Event time
CUST_ID	bigint	Customer identifier
SRC_ASSET_ID	bigint	Source Asset ID
DEST_ASSET_ID	bigint	Destination Asset ID
TXNMY_ID	bigint	Taxonomy ID

Column Name	Datatype	Comment
PRTCL_ID	bigint	Protocol ID
AGENT_ID	bigint	Collector Identifier
ARCH_ID	bigint	
DEVICE_EVT_TIME	datetime	Device Event Time
SENTINEL_PROCESS_TIME	datetime	Sentinel Process Time
BEGIN_TIME	datetime	Events begin time
END_TIME	datetime	Events end time
REPEAT_CNT	int	Events repeat count
DP_INT	int	
SP_INT	int	
RES	varchar/nvarchar(255)	Resolution
SRES	varchar/nvarchar(255)	
SEV	int	Severity
EVT	varchar/nvarchar(255)	Events
ET	varchar/nvarchar(255)	
SIP	int	
SHN	varchar/nvarchar(255)	
SP	varchar/nvarchar(32)	
DIP	int	
DHN	varchar/nvarchar(255)	
DP	varchar/nvarchar(32)	
SUN	varchar/nvarchar(255)	
DUN	varchar/nvarchar(255)	
FN	varchar/nvarchar(1000)	
VULN	int	Vulnerability
CT1	varchar/nvarchar(255)	
CT2	varchar/nvarchar(255)	
CT3	int	
RT1	varchar/nvarchar(255)	
RT2	varchar/nvarchar(255)	
RT3	int	
CRIT	int	

Column Name	Datatype	Comment
MSG	varchar/nvarchar(4000)	Message
EI	varchar/nvarchar(1000)	
INIT_USR_SYS_ID	varchar/nvarchar(255)	
INIT_USR_IDENTITY_GUID	uniqueidentifier	
TRGT_USR_SYS_ID	varchar/nvarchar(255)	
TRGT_USR_IDENTITY_GUID	uniqueidentifier	
EFFECTIVE_USR_NAME	varchar/nvarchar(255)	
EFFECTIVE_USR_SYS_ID	varchar/nvarchar(255)	
EFFECTIVE_USR_DOMAIN	varchar/nvarchar(255)	
TRGT_TRUST_NAME	varchar/nvarchar(255)	
TRGT_TRUST_SYS_ID	varchar/nvarchar(255)	
TRGT_TRUST_DOMAIN	varchar/nvarchar(255)	
OBSRVR_IP	int	
RPTR_IP	int	
OBSRVR_HOST_DOMAIN	varchar/nvarchar(255)	
RPTR_HOST_DOMAIN	varchar/nvarchar(255)	
OBSRVR_ASSET_ID	varchar/nvarchar(255)	
RPTR_ASSET_ID	varchar/nvarchar(255)	
INIT_SRVC_COMP	varchar/nvarchar(255)	
TARGET_SRVC_COMP	varchar/nvarchar(255)	
EVT_GRP_ID	varchar/nvarchar(255)	
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object
RV01-RV10	int	
RV11-RV20	datetime	
RV21-RV25	uniqueidentifier	
RV26-RV38	varchar/nvarchar(255)	
RV40-RV49		
RV101-RV120	datetime	
RV121-RV130	uniqueidentifier	

Column Name	Datatype	Comment
RV131-RV140	int	
RV141-RV150	varchar/nvarchar(255)	
RID01-RID20	bigint	
CV01-CV10	int	
CV11-CV20	datetime	
CV21-CV29	varchar/nvarchar(255)	
CV35-CV100		
CV30-CV34	varchar/nvarchar(4000)	
CV101-CV110	int	
CV131-CV140		
CV111-CV120	datetime	
CV121-CV130	uniqueidentifier	
CV141-CV147	varchar/nvarchar(255)	

8.1.83 HIST_EVENTS_RPT_V (legacy view)

This view is provided for backward compatibility. New reports should use EVENTS_RPT_V2.

8.1.84 IMAGES_RPT_V

View references IMAGES table that stores system overview image information.

Column Name	Datatype	Comment
NAME	varchar/nvarchar(128)	Image name
TYPE	varchar/nvarchar(64)	Image type
DATA	ntext	Image data
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.85 INCIDENTS_ASSETS_RPT_V

View references INCIDENTS_ASSETS table that stores information about the assets that makeup incidents created in the Sentinel Console.

Column Name	Datatype	Comment
INC_ID	int	Incident identifier – sequence number
ASSET_ID	uniqueidentifier	Asset Universal Unique Identifier (UUID)
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.86 INCIDENTS_EVENTS_RPT_V

View references INCIDENTS_EVENTS table that stores information about the events that makeup incidents created in the Sentinel Console.

Column Name	Datatype	Comment
INC_ID	int	Incident identifier – sequence number
EVT_ID	uniqueidentifier	Event Universal Unique Identifier (UUID)
EVT_TIME	datetime	Event time
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.87 INCIDENTS_RPT_V

View references INCIDENTS table that stores information describing the details of incidents created in the Sentinel Console.

Column Name	Datatype	Comment
INC_ID	int	Incident identifier – sequence number
NAME	varchar/nvarchar(255)	Incident name
INC_CAT	varchar/nvarchar(255)	Incident category
INC_DESC	varchar/nvarchar(4000)	Incident description
INC_PRIORITY	int	Incident priority
INC_RES	varchar/nvarchar(4000)	Incident resolution
SEVERITY	int	Incident severity
STT_ID	int	Incident State ID

Column Name	Datatype	Comment
SEVERITY_RATING	varchar/nvarchar(32)	Average of all the event severities that comprise an incident.
VULNERABILITY_RATING	varchar/nvarchar(32)	Reserved for future use by Sentinel. Use of this field for any other purpose might result in data being overwritten by future functionality.
CRITICALITY_RATING	varchar/nvarchar(32)	Reserved for future use by Sentinel. Use of this field for any other purpose might result in data being overwritten by future functionality.
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.88 INCIDENTS_VULN_RPT_V

View references INCIDENTS_VULN table that stores information about the vulnerabilities that makeup incidents created in the Sentinel Console.

Column Name	Datatype	Comment
INC_ID	int	Incident identifier – sequence number
VULN_ID	uniqueidentifier	Vulnerability Universal Unique Identifier (UUID)
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.89 L_STAT_RPT_V

View references L_STAT table that stores statistical information.

Column Name	Datatype	Comment
RES_NAME	varchar/nvarchar(32)	Resource name
STATS_NAME	varchar/nvarchar(32)	Statistic name
STATS_VALUE	varchar/nvarchar(32)	Value of the statistic
OPEN_TOT_SECS	numeric(18,0)	Number of seconds since 1970.

8.1.90 LOGS_RPT_V

View references LOGS_RPT table that stores logging information.

Column Name	Datatype	Comment
LOG_ID	int	Sequence number
TIME	datetime	Date of Log
MODULE	varchar/nvarchar(64)	Module log is for
TEXT	varchar/nvarchar(4000)	Log ntext

8.1.91 MSSP_ASSOCIATIONS_V

View references MSSP_ASSOCIATIONS table that associates an integer key in one table to a uuid in another table.

Column Name	Datatype	Comment
TABLE1	varchar/nvarchar (64)	Table name 1
ID1	bigint	ID1
TABLE2	varchar/nvarchar (64)	Table name 2
ID2	uniqueidentifier	ID2
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.92 NETWORK_IDENTITY_RPT_V

View references NETWORK_IDENTITY_LKUP table that stores asset network identity information.

Column Name	Datatype	Comment
NETWORK_IDENTITY_ID	bigint	Network identity code
NETWORK_IDENTITY_NAME	varchar/nvarchar(255)	Network identify name
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.93 ORGANIZATION_RPT_V

View references ORGANIZATION table that stores organization (asset) information.

Column Name	Datatype	Comment
ORGANIZATION_ID	uniqueidentifier	Organization identifier
ORGANIZATION_NAME	varchar/nvarchar(100)	Organization name
CUST_ID	bigint	Customer identifier
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.94 PERSON_RPT_V

View references PERSION table that stores personal (asset) information.

Column Name	Datatype	Comment
PERSON_ID	uniqueidentifier	Person identifier
FIRST_NAME	varchar/nvarchar(255)	First name
LAST_NAME	varchar/nvarchar(255)	Last name
CUST_ID	bigint	Customer identifier
PHONE_NUMBER	varchar/nvarchar(50)	Phone number
EMAIL_ADDRESS	varchar/nvarchar(255)	Email address
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.95 PHYSICAL_ASSET_RPT_V

View references PHYSICAL_ASSET table that stores physical asset information.

Column Name	Datatype	Comment
PHYSICAL_ASSET_ID	uniqueidentifier	Physical asset identifier
CUST_ID	bigint	Customer identifier
LOCATION_ID	bigint	Location identifier
HOST_NAME	varchar/nvarchar(255)	Host name

Column Name	Datatype	Comment
IP_ADDRESS	int	IP address
NETWORK_IDENTITY_ID	bigint	Network identity code
MAC_ADDRESS	varchar/nvarchar(100)	MAC address
RACK_NUMBER	varchar/nvarchar(50)	Rack number
ROOM_NAME	varchar/nvarchar(100)	Room name
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.96 PRODUCT_RPT_V

View references PRDT table that stores asset product information.

Column Name	Datatype	Comment
PRODUCT _ID	bigint	Product identifier
PRODUCT _NAME	varchar/nvarchar(255)	Product name
PRODUCT _VERSION	varchar/nvarchar(100)	Product version
VENDOR _ID	bigint	Vendor identifier
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.97 ROLE_RPT_V

View references ROLE_LKUP table that stores user role (asset) information.

Column Name	Datatype	Comment
ROLE_CODE	varchar/nvarchar(5)	Role code
ROLE_NAME	varchar/nvarchar(255)	Role name
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.98 RPT_LABELS_RPT_V

This view contains localized report labels for reports in non-English languages.

Column Name	Datatype	Comment
RPT_NAME	varchar/nvarchar(100)	Report name
LABEL_1 – LABEL_35	varchar/nvarchar(2000)	Translated report labels

8.1.99 SENSITIVITY_RPT_V

View references SENSITIVITY_LKUP table that stores asset sensitivity information.

Column Name	Datatype	Comment
SENSITIVITY_ID	bigint	Asset sensitivity code
SENSITIVITY_NAME	varchar/nvarchar(50)	Asset sensitivity name
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.100 SENTINEL_HOST_RPT_V

Column Name	Datatype	Comment
SENTINEL_HOST_ID	uniqueidentifier	Sentinel host identifier
SENTINEL_ID	uniqueidentifier	Sentinel identifier
SENTINEL_HOST_NAME	varchar/nvarchar(255)	Sentinel host name
HOST_NAME	varchar/nvarchar(255)	Host name
IP_ADDR	varchar/nvarchar(255)	IP address
HOST_OS	varchar/nvarchar(255)	Host operating system
HOST_OS_VERSION	varchar/nvarchar(255)	Host operating system version
MODIFIED_BY	int	User who last modified object
CREATED_BY	int	User who created object
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified

8.1.101 SENTINEL_PLUGIN_RPT_V

Column Name	Datatype	Comment
SENTINEL_PLUGIN_ID	uniqueidentifier	Sentinel plugin identifier
SENTINEL_PLUGIN_NAME	varchar/nvarchar(255)	Sentinel plugin name
SENTINEL_PLUGIN_TYPE	varchar/nvarchar(255)	Sentinel plugin type
FILE_NAME	varchar/nvarchar(512)	File name
CONTENT_PKG	ntext	Content package
FILE_HASH	varchar/nvarchar(255)	File hash code
AUX_FILE_NAME	varchar/nvarchar(512)	Auxiliary file name
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified

8.1.102 SENTINEL_RPT_V

Column Name	Datatype	Comment
SENTINEL_ID	uniqueidentifier	Sentinel identifier
SENTINEL_NAME	varchar/nvarchar(255)	Sentinel name
ONLINE_IND	bit	Online indicator
STATE_IND	bit	State indicator
SENTINEL_CONFIG	ntext	Sentinel configuration
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified

8.1.103 STATES_RPT_V

View references STATES table that stores definitions of states defined by applications or context.

Column Name	Datatype	Comment
STT_ID	int	State ID – sequence number

Column Name	Datatype	Comment
CONTEXT	varchar/nvarchar(64)	Context of the state. That is case, incident, user.
NAME	varchar/nvarchar(64)	Name of the state.
TERMINAL_FLAG	varchar/nvarchar(1)	Indicates if state of incident is resolved.
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
MODIFIED_BY	int	User who last modified object
CREATED_BY	int	User who created object

8.1.104 UNASSIGNED_INCIDENTS_RPT_V

View references CASES and INCIDENTS tables to report on unassigned cases.

Name	Datatype	Comment
INC_ID	int	Incident identifier – sequence number
NAME	varchar/nvarchar(255)	Short, unique user name used as a login
SEVERITY	int	Incident severity
STT_ID	int	State ID. Status is either active or inactive.
SEVERITY_RATING	varchar/nvarchar(32)	Average of all the event severities that comprise an incident.
VULNERABILITY_RATING	varchar/nvarchar(32)	Vulnerability rating
CRITICALITY_RATING	varchar/nvarchar(32)	Criticality rating
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object
INC_DESC	varchar/nvarchar(4000)	Incident description
INC_CAT	varchar/nvarchar(255)	Incident category
INC_PRIORITY	int	Incident priority
INC_RES	varchar/nvarchar(4000)	Incident resolution

8.1.105 USERS_RPT_V

View references USERS table that lists all users of the application. The users will also be created as database users to accommodate 3rd party reporting tools.

Column Name	Datatype	Comment
USR_ID	int	User identifier – Sequence number
NAME	varchar/nvarchar(64)	Short, unique user name used as a login
CNT_ID	int	Contact ID – Sequence number
STT_ID	int	State ID. Status is either active or inactive.
DESCRIPTION	varchar/nvarchar(512)	Comments
PERMISSIONS	varchar/nvarchar(4000)	Permissions currently assigned to the Sentinel user
FILTER	varchar/nvarchar(128)	Current security filter assigned to the Sentinel user
UPPER_NAME	varchar/nvarchar(64)	User name in upper case
DOMAIN_AUTH_IND	bit	Domain authentication indication
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.106 USR_ACCOUNT_RPT_V

Column Name	Datatype	Comment
ACCOUNT_ID	bigint	Account identifier
USER_DOMAIN	varchar/nvarchar(255)	User domain
CUST_ID	bigint	Customer identifier
BEGIN_EFFECTIVE_DATE	datetime	Begin effective date
END_EFFECTIVE_DATE	datetime	End effective date
CURRENT_F	bit	Current flag
USER_STATUS	varchar/nvarchar(50)	User status
IDENTITY_GUID	uniqueidentifier	Identity identifier
SOURCE_USER_ID	varchar/nvarchar(100)	User ID on source system
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.107 USR_IDENTITY_EXT_ATTR_RPT_V

Column Name	Datatype	Comment
IDENTITY_GUID	uniqueidentifier	Identity identifier
ATTRIBUTE_NAME	varchar/nvarchar(255)	Attribute name
ATTRIBUTE_VALUE	varchar/nvarchar(1024)	Attribute value

8.1.108 USR_IDENTITY_RPT_V

Column Name	Datatype	Comment
IDENTITY_GUID	uniqueidentifier	Identity identifier
DN	varchar/nvarchar(255)	Distinguished name
CUST_ID	bigint	Customer identifier
SRC_IDENTITY_ID	varchar/nvarchar(100)	Source identity identifier
WFID	varchar/nvarchar(100)	Workforce identifier
FIRST_NAME	varchar/nvarchar(255)	First name
LAST_NAME	varchar/nvarchar(255)	Last name
FULL_NAME	varchar/nvarchar(255)	Full name
JOB_TITLE	varchar/nvarchar(255)	Job title
DEPARTMENT_NAME	varchar/nvarchar(100)	Department name
OFFICE_LOC_CD	varchar/nvarchar(100)	Office location code
PRIMARY_EMAIL	varchar/nvarchar(255)	Primary email address
PRIMARY_PHONE	varchar/nvarchar(100)	Primary phone number
VAULT_NAME	varchar/nvarchar(100)	Identity vault name
MGR_GUID	uniqueidentifier	Manager identity identifier
PHOTO	text	Photo
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.109 VENDOR_RPT_V

View references VNDR table that stores information about asset product vendors.

Column Name	Datatype	Comment
VENDOR_ID	bigint	Vendor identifier
VENDOR_NAME	varchar/nvarchar(255)	Vendor name
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.110 VULN_CALC_SEVERITY_RPT_V

View references VULN_RSRC and VULN to calculate eSecurity vulnerability severity rating base on current vulnerabilities.

Column Name	Datatype	Comment
RSRC_ID	uniqueidentifier	
IP	varchar/nvarchar(32)	IP
HOST_NAME	varchar/nvarchar(255)	Host name
CRITICALITY	int	Asset criticality code
ASSIGNED_VULN_SEVERITY	int	
VULN_COUNT	int	Vulnerability Count
CALC_SEVERITY	numeric(14,2)	

8.1.111 VULN_CODE_RPT_V

View references VULN_CODE table that stores industry assigned vulnerability codes such as Mitre's CVEs and CANs.

Column Name	Datatype	Comment
VULN_CODE_ID	uniqueidentifier	
VULN_ID	uniqueidentifier	Vulnerability identifier
VULN_CODE_TYPE	varchar/nvarchar(64)	Vulnerability code type
VULN_CODE_VALUE	varchar/nvarchar(255)	Vulnerability code value
URL	varchar/nvarchar(512)	Web URL
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object

Column Name	Datatype	Comment
MODIFIED_BY	int	User who last modified object

8.1.112 VULN_INFO_RPT_V

View references VULN_INFO table that stores additional information reported during a scan.

Column Name	Datatype	Comment
VULN_INFO_ID	uniqueidentifier	
VULN_ID	uniqueidentifier	Vulnerability identifier
VULN_INFO_TYPE	varchar/nvarchar(36)	
VULN_INFO_VALUE	varchar/nvarchar(2000)	
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.113 VULN_RPT_V

View references VULN table that stores information of scanned system. Each scanner will have its own entry for each system.

Column Name	Datatype	Comment
VULN_ID	uniqueidentifier	Vulnerability identifier
RSRC_ID	uniqueidentifier	Resource identifier
PORT_NAME	varchar/nvarchar(64)	Port Name
PORT_NUMBER	int	Port Number
NETWORK_PROTOCOL	int	Network Protocol
APPLICATION_PROTOCOL	varchar/nvarchar(64)	Application Protocol
ASSIGNED_VULN_SEVERITY	int	
COMPUTED_VULN_SEVERITY	int	
VULN_DESCRIPTION	ntext	
VULN_SOLUTION	ntext	
VULN_SUMMARY	varchar/nvarchar(1000)	
BEGIN_EFFECTIVE_DATE	datetime	Date from which the entry is valid
END_EFFECTIVE_DATE	datetime	Date until which the entry is valid
DETECTED_OS	varchar/nvarchar(64)	

Column Name	Datatype	Comment
DETECTED_OS_VERSION	varchar/nvarchar(64)	
SCANNED_APP	varchar/nvarchar(64)	
SCANNED_APP_VERSION	varchar/nvarchar(64)	
VULN_USER_NAME	varchar/nvarchar(64)	
VULN_USER_DOMAIN	varchar/nvarchar(64)	
VULN_TAXONOMY	varchar/nvarchar(1000)	
SCANNER_CLASSIFICATION	varchar/nvarchar(255)	
VULN_NAME	varchar/nvarchar(300)	
VULN_MODULE	varchar/nvarchar(64)	
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.114 VULN_RSRC_RPT_V

View references VULN_RSRC table that stores each resource scanned for a particular scan.

Column Name	Datatype	Comment
RSRC_ID	uniqueidentifier	
SCANNER_ID	uniqueidentifier	Scanner identifier
IP	varchar/nvarchar(32)	IP Address
HOST_NAME	varchar/nvarchar(255)	Host name
LOCATION	varchar/nvarchar(128)	Location
DEPARTMENT	varchar/nvarchar(128)	Department
BUSINESS_SYSTEM	varchar/nvarchar(128)	Business System
OPERATIONAL_ENVIRONMENT	varchar/nvarchar(64)	Operational environment
CRITICALITY	int	Criticality
REGULATION	varchar/nvarchar(128)	Regulation
REGULATION_RATING	varchar/nvarchar(64)	Regulation rating
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.115 VULN_RSRC_SCAN_RPT_V

View references VULN_RSRC_SCAN table that stores each resource scanned for a particular scan.

Column Name	Datatype	Comment
RSRC_ID	uniqueidentifier	
SCAN_ID	uniqueidentifier	
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.116 VULN_SCAN_RPT_V

View references table that stores information pertaining to scans.

Column Name	Datatype	Comment
SCAN_ID	uniqueidentifier	Vulnerability scan identifier
SCANNER_ID	uniqueidentifier	Vulnerability scanner identifier
SCAN_TYPE	varchar/nvarchar(10)	Vulnerability scan type
SCAN_START_DATE	datetime	Scan start date
SCAN_END_DATE	datetime	Scan start date
CONSOLIDATION_SERVER	varchar/nvarchar(64)	Consolidation server
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.117 VULN_SCAN_VULN_RPT_V

View references VULN_SCAN_VULN table that stores vulnerabilities detected during scans.

Column Name	Datatype	Comment
SCAN_ID	uniqueidentifier	
VULN_ID	uniqueidentifier	
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object

Column Name	Datatype	Comment
MODIFIED_BY	int	User who last modified object

8.1.118 VULN_SCANNER_RPT_V

View references VULN_SCANNER table that stores information about vulnerability scanners.

Column Name	Datatype	Comment
SCANNER_ID	uniqueidentifier	
PRODUCT_NAME	varchar/nvarchar(100)	Product Name
PRODUCT_VERSION	varchar/nvarchar(64)	Product Version
SCANNER_TYPE	varchar/nvarchar(64)	Vulnerability Scanner Type
VENDOR	varchar/nvarchar(100)	Vendor
SCANNER_INSTANCE	varchar/nvarchar(64)	Scanner Instance
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.119 WORKFLOW_DEF_RPT_V

Column Name	Datatype	Comment
PKG_NAME	varchar/nvarchar(255)	Package name
PKG_DATA	ntext	Package data
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.1.120 WORKFLOW_INFO_RPT_V

Column Name	Datatype	Comment
INFO_ID	bigint	Info identifier
PROCESS_DEF_ID	varchar/nvarchar(100)	Process definition identifier
PROCESS_INSTANCE_ID	varchar/nvarchar(150)	Process instance identifier

Column Name	Datatype	Comment
DATE_CREATED	datetime	Date the entry was created
DATE_MODIFIED	datetime	Date the entry was modified
CREATED_BY	int	User who created object
MODIFIED_BY	int	User who last modified object

8.2 Deprecated Views

The following legacy views are no longer created in the Sentinel 6 database:

- ADV_ALERT_CVE_RPT_V
- ADV_ALERT_PRODUCT_RPT_V
- ADV_ALERT_RPT_V
- ADV_ATTACK_ALERT_RPT_V
- ADV_ATTACK_CVE_RPT_V
- ADV_CREDIBILITY_RPT_V
- ADV_SEVERITY_RPT_V
- ADV_SUBALERT_RPT_V
- ADV_URGENCY_RPT_V
- HIST_INCIDENTS_RPT_V

Sentinel Troubleshooting Checklist

A

This checklist is provided to aid in diagnosing a problem. By filling in this checklist, you can solve common issues or reduce the amount of time needed to solve more complex issues.

Table A-1 *Checklist*

Checklist Item	Information	Example
Novell Version:		V6.0
Novell Platform and OS Version:		SuSE Linux Enterprise Server 10
Database Platform and OS Version:		Oracle 10.2.0.3 with critical patch #5881721
Sentinel Server Hardware Configuration ◆ Processor ◆ Memory ◆ Other		4 CPU @ 3 GHz 5 GB RAM
Database Server Hardware Configuration ◆ Processor ◆ Memory ◆ Other (if separate Box)		4 CPU @ 3.0 GHz 8 GB RAM
Database Storage Configuration (NAS, SAN, Local and so on.)		Local with offsite backup
Reporting Server OS and Configuration (Crystal Server)		Crystal XI SuSE Linux Enterprise Server 10 with MySQL

NOTE: Depending upon how your Sentinel system is configured (distributed), you might need to expand the above table. For instance additional information might be needed for DAS, Advisor, Sentinel Control Center, Collector Builder and communication layer.

1. Check the Novell Customer Center (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup) for your particular issue:
   - Is this a known issue with a work-around?
   - Is this issue fixed in the latest patch release or hot-fix?
   - Is this issue currently scheduled to be fixed in a future release?

2 Determine the nature of the problem.

- Can it be reproduced? Can the steps to reproduce the problem be enumerated?
- What user action, if any, will cause the problem?
- Is the issue periodic in nature?

3 Determine the severity of this problem.

- Is the system still useable?

4 Understand the environment and systems involved.

- What platforms and product versions are involved?
- Are there any non-standard or custom components involved?
- Is it a high event rate environment?
- What is the rate of events being collected?
- What is the event rate of insertion into the database?
- How many concurrent users are there?
- Is Crystal reporting used? When are reports run?
- Is correlation used? How many rules are deployed?

Collect configuration files, log files and system information from appropriate subdirectories in $ESEC_HOME or %ESEC_HOME%. Assemble this information for possible future knowledge transfer.

5 Check the health of the system.

- Can you log into the Sentinel Control Center?
- Are events being generated and inserted into the database?
- Can events be seen on the Sentinel Control Center?
- Can events be retrieved from the database using quick query?
- Check the RAM usage, disk space, process activity, CPU usage and network connectivity of the hosts involved.
- Verify all expected Sentinel processes are running. Microsoft Task Manager can be used in a Windows environment. In UNIX, the command `ps –ef|grep esecadm` can be used.
- Check for any core dumps in any of the sub-directories of ESEC_HOME. Find out which process core dumped. (cd $ESEC_HOME, find `. –name core –print`)
- Check for the sqlplus net access. Check for the tablespaces.
- Make sure the Sonic broker is running. Connectivity can be verified using the Sonic management console. Check that the various connections are active from Novell processes. Make sure that a lock file is not preventing Sonic from starting. Optionally telnet to that server on the sonic port (that is telnet sentinel.company.com 10012)
- Check whether the wrapper service is running on the server. (`ps –ef | grep wrapper`)
- Are any errors visible in the Servers View of the Sentinel Control Center? Are any errors visible in the Event Source Management Live View in the Sentinel Control Center? What is the OS resource consumption on the Collector Managers?

6 Is there a problem with the Database?

- Using sqlplus, can you log into the database?
- Does the database allow a sqlplus login using the Novell dba account into the ESEC schema?
- Does querying on one of the table succeed?
- Does a select statement on a database table succeed?
- Check the JDBC drivers, their locations and class path settings.
- If Oracle, do they have Partitioning installed (provide "`select * from v$version;`") and used?
- Is the database being maintained by an administrator? By anyone?
- Has the database been modified by that administrator?
- Is SDM being used to maintain the partitions and archive/delete the partitions to make more room in the database?
- Using SDM what is the current partition? Is it P_MAX?

7 Inspect whether the product environment settings are correct.

- Verify the sanity of User login shell scripts, environment variables, configurations, java home settings.
- Are the environment variable set to run the correct jvm?
- Verify the proper permissions on the folders for the installed product.
- Check if any cron jobs are setup causing interference with our product's functionality.
- If the product is installed on NFS mounts, check the sanity of NFS mounts & NFS/NIS services.

8 Is there a possible memory leak?

- Obtain the statistics on how fast the memory is being consumed and by which process.
- Gather the metrics of the events throughput per Collector.
- Run the prstat command on Solaris. This will give the process runtime statistics.
- In Windows you can check the process size and handle count in task manager.

This issue, if not resolved, is now ready for escalation. Possible results of escalation are:

- Configuration file changes
- Hot fixes or patches to your system
- Enhancement request
- Temporary workaround.

Sentinel Service Logon Account

B

The purpose of this document is to describe in detail of how to set up Sentinel service logon account as NT AUTHORITY\NetworkService instead of Domain user account. This has been tested on the Windows 2003 platform only.

B.1 Sentinel Services

Sentinel Services should be set to run in order to use Sentinel application. To run a service you need to login to the machine where Sentinel is installed using a logon Account. The different logon accounts and advantages of using a logon account are discussed in this document.

B.2 Introduction to Service Logon Accounts

A service must log on to an account to access resources and objects on the operating system. If you select an account that does not have permission to log on as a service, the Services snap-in automatically grants that account the user rights that are required to log on as a service on the computer that you are managing. However, this does not guarantee that the service will start. For example, it is recommended that the user accounts that are used to log on as a service have the Password never expires check box selected in their properties dialog box and that they have strong passwords. If account lockout policy is enabled and the account is locked out, the service will malfunction.

The following table describes the service logon accounts and how they are used.

Table B-1 *Usage of Service Logon Accounts*

Logon Account	Description
Local System Account	The Local System account is a powerful account that has full access to the system, including the directory service on domain controllers. If a service logs onto the Local System account on a domain controller, that service has access to the entire domain. Some services are configured by default to log on to the Local System account. Do not change the default service setting. Local System account is a predefined local account that is used to start a service and provide the security context for that service. The name of the account is NT AUTHORITY\System. This account does not have a password and any password information that you supply is ignored. The Local System account has full access to the system, including the directory service on domain controllers. Because the Local System account acts as a computer on the network, it has access to network resources.

Logon Account	Description
Local Service Account	The Local Service account is a special built-in account that is similar to an authenticated user account. The Local Service account has the same level of access to resources and objects as members of the Users group. This limited access helps safeguard your system if individual services or processes are compromised. Services that run as the Local Service account access network resources as a null session with no credentials. Local Service account is a predefined local account that is used to start a service and provide the security context for that service. The name of the account is NT AUTHORITY\LocalService. The Local Service account has limited access to the local computer and Anonymous access to network resources.
Network Service Account	The Network Service account is a special, built-in account that is similar to an authenticated user account. The Network Service account has the same level of access to resources and objects as members of the Users group. This limited access helps safeguard your system if individual services or processes are compromised. Services that run as the Network Service account access network resources using the credentials of the computer account. Network Service account is a predefined local account that is used to start a service and provide the security context for that service. The name of the account is NT AUTHORITY\NetworkService. The Network Service account has limited access to the local computer and authenticated access (as the computer account) to network resources.

B.2.1 Disadvantages of running a service in the context of a user logon

1. The account must be created before the service can run. If the setup program for the service creates the account, Setup must run from an account that has sufficient administrative credentials to create accounts in the directory service.
2. Service account names and passwords are stored on each computer on which the service is installed. If the password for a service account on a computer is changed or expires, the service cannot start on that computer until the password is set to the new password for that service. The recommendation is to use LocalService and Network Service instead of using an account that requires a password: this simplifies password management.
3. If a service account is renamed, locked out, disabled, or deleted, the service cannot start on that computer until the account is reset.

Because of the above disadvantages, Novell has tested out running Sentinel service under NT AUTHORITY\NetworkService account. NT AUTHORITY\LocalService account does not have enough privilege for this purpose, because DAS processes need to communicate to database server on the network.

NOTE: Novell has tested and recommends choosing Network Service account option.

B.3 To Setup NT AUTHORITY\NetworkService as the Logon Account for Sentinel Service

To setup NT AUTHORITY\NetworkService as the logon account for Sentinel service, you need to perform the following:

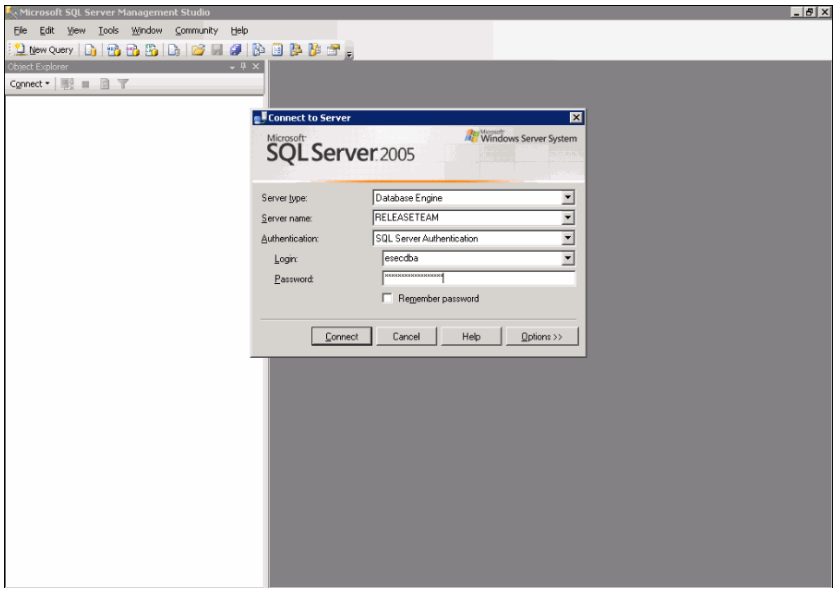
- Add the machine that runs Sentinel Service as a login account to ESEC and ESEC_WF database instances (performed on the database machine)
- Change the logon account for Sentinel service to NT AUTHORITY\NetworkService (performed on your remote machine)
- Setting the Sentinel startup (performed on your remote machine)

B.3.1 Adding Sentinel Service as a Login Account to ESEC and ESEC_WF DB Instances

To add a login of a remote machine to the database server:

NOTE: As an example, the following are steps to add secnet\case1 as a login to the database server.

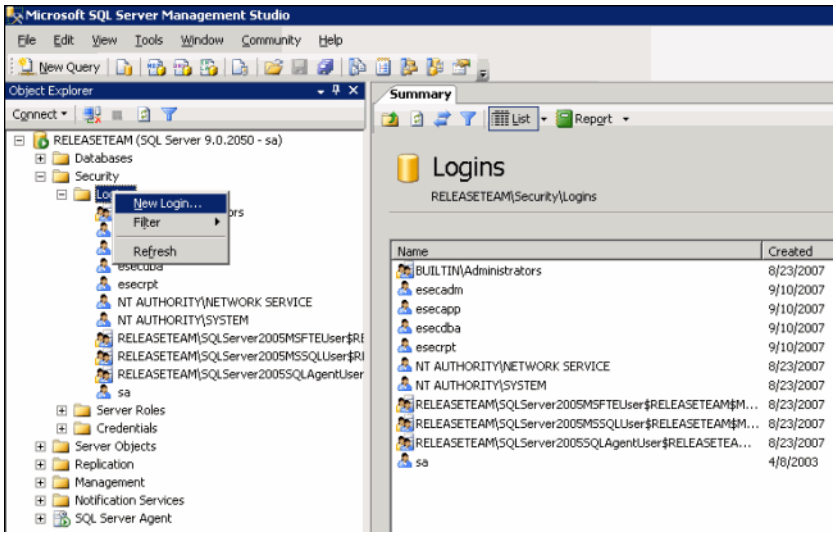
1 On your database machine, open up SQL Server Management Studio. Specify the user credentials in the Login window.



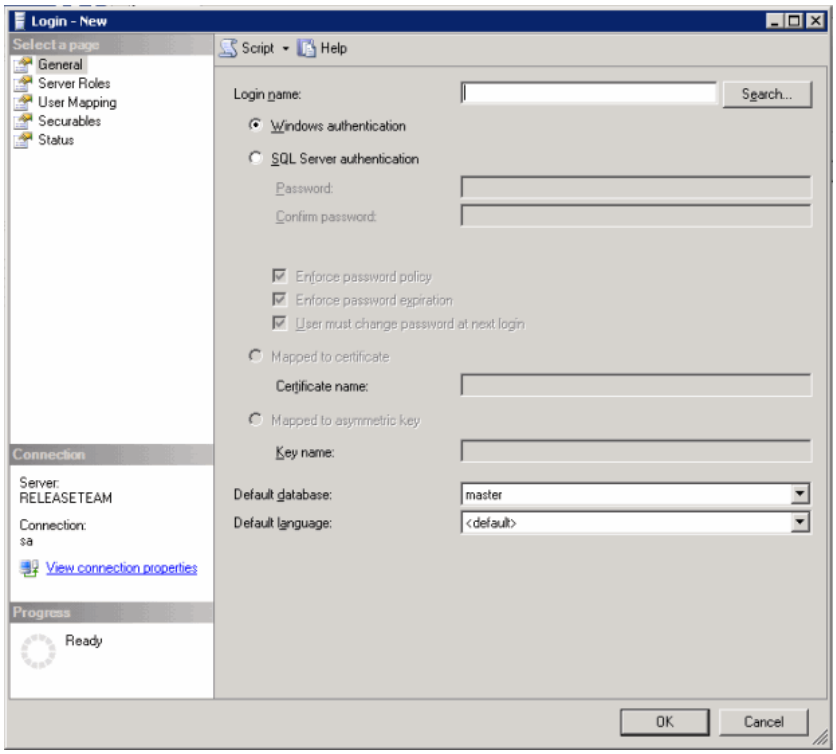
Click Connect

2 In the Object Explorer pane, under SQL Server Group, expand Security folder and highlight Logins folder.

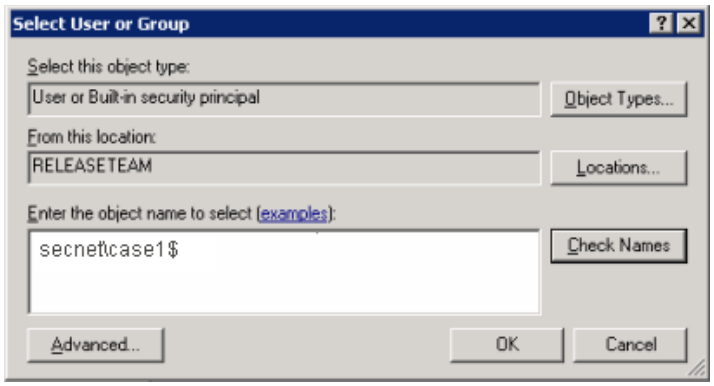
3 Right-click Logins > New login.



4 In the Login-New window, provide the Login name.

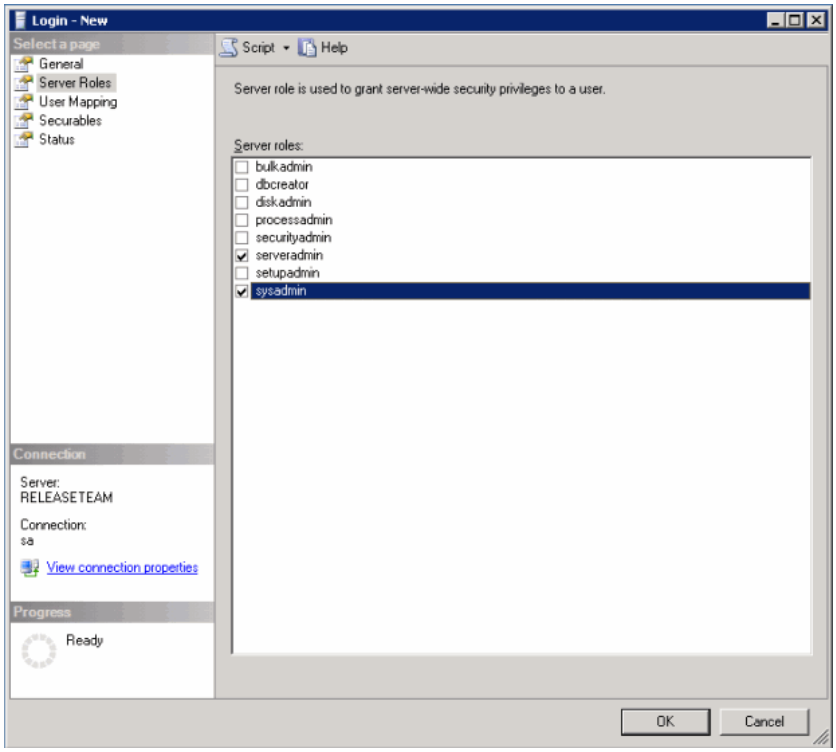


Alternatively, you can click the Search button next to the Login name field. The following screen displays:

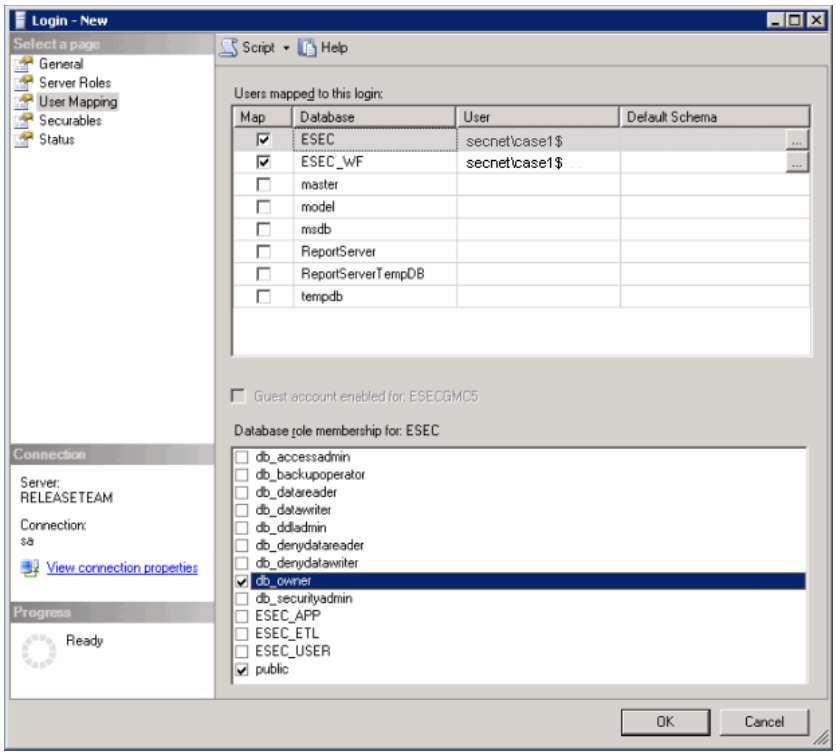


5 In the Enter the object name to select field, provide a domain name and user name (secnet\case1$ is provided as an example). This is the machine <domain name>\<name of machine>$ you are adding as a login to the database server. Click OK.

6 Click Server Roles in the Select a page navigation pane. Select `sysadmin` and `serveradmin` as Server Roles as shown below:



7 Click User Mapping in the Select a page navigation pane. Select access to ESEC and ESEC_WF as “public” and “db_owner” as shown below:

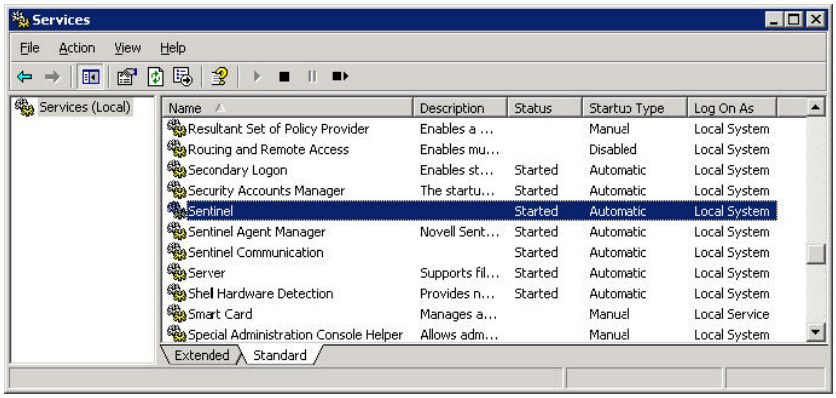


Click OK.

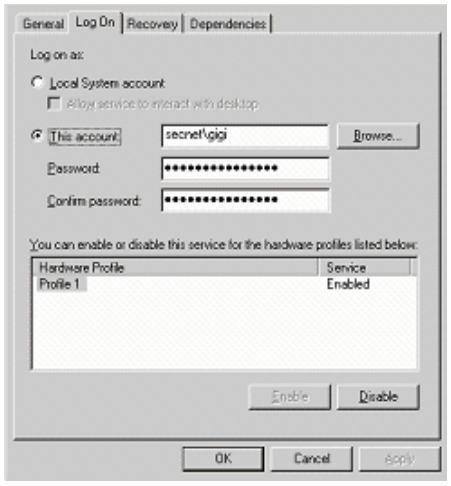
B.3.2 Changing logon account

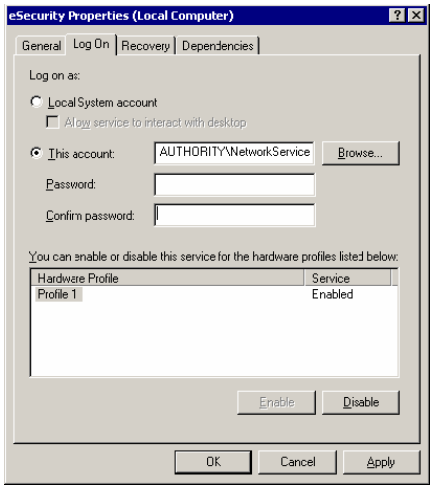
To change the logon for Sentinel Service to NT AUTHORITY\NetworkService:

1. On your remote machine you are connecting to the database, click Start > Programs > Administrative Tools > Services.

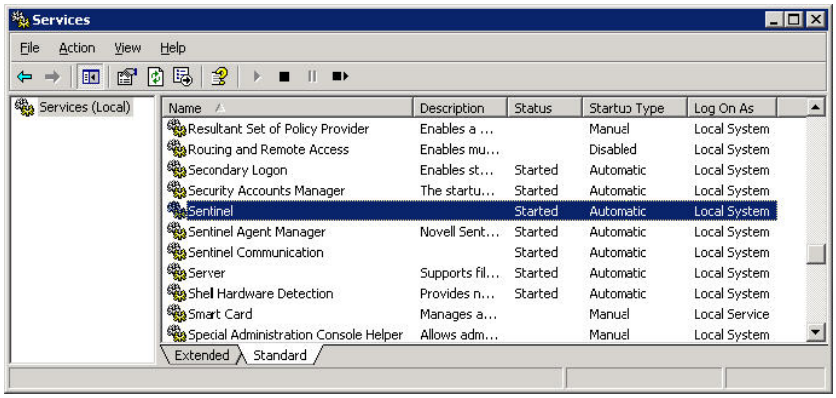


2. Stop the Sentinel service, right-click > Properties > Log On tab.
3. Click This account and in the field provide `NT AUTHORITY\NetworkService`. Clear the Password and Confirm password fields.





4 Click OK. The Services window for the Sentinel Service should indicate Network Service under the Log On As column.



B.3.3 Setting the Sentinel Service to Start Successfully

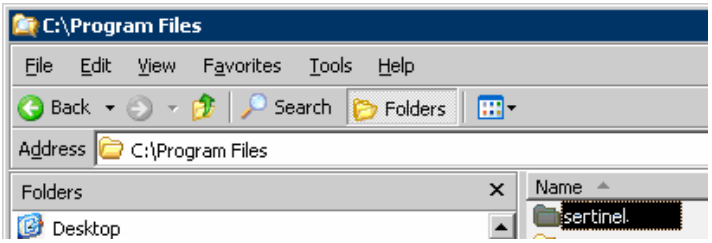
In order for the Sentinel Service to start successfully, NT AUTHORITY\NetworkService account should have write permission to %ESEC_HOME%. According to Microsoft documentation, the NetworkService account has the following privileges:

- SE_ASSIGNPRIMARYTOKEN_NAME (disabled)
- SE_AUDIT_NAME (disabled)
- SE_CHANGE_NOTIFY_NAME (enabled)
- SE_CREATE_GLOBAL_NAME (enabled)
- SE_IMPERSONATE_NAME (enabled)
- SE_INCREASE_QUOTA_NAME (disabled)
- SE_SHUTDOWN_NAME (disabled)
- SE_UNDOCK_NAME (disabled)
- Any privileges assigned to users and authenticated users

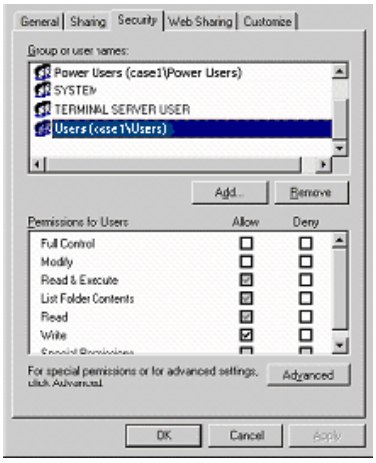
You must grant write access to %ESEC_HOME% to the Users group.

To set the Sentinel Service to start successfully:

1. Open Window's Explorer and navigate to %ESEC_HOME%.
2. Right-click the Sentinel parent folder (Typically named sentinel6) > Properties > Security tab.



3. Highlight Users group. Grant Read & Execute, List Folder Contents, Read, Write permissions.



Click OK.

4. In the Services window, restart the Sentinel service.

Sentinel Service Permission Tables

C

The purpose of this document is to describe in detail various Sentinel Services and the Permissions they require for their functioning.

C.1 Advisor

Table C-1 *Table C-1: Advisor*

Sentinel Component	Sentinel Service	Sentinel Process	Function summary	Permission's required	Permission Explanation
Advisor	Sentinel	java	Download (optional) and processes Advisor attack data.	Network access Internet access over port 443 (optional) File read access to: ◆ ESEC_HOME /config ◆ ESEC_HOME /lib ◆ ESEC_HOME /jre File write access to: ◆ ESEC_HOME /data ◆ ESEC_HOME /log	It connects to the database to read and insert data. It communicates over the network with iSCALE to notify other processes it is down processing a feed. It reads local configuration files and uses the java executable. It writes log files as well as caches data in the local file system.

C.2 Collector Manager

Table C-2 *Collector Manager*

Sentinel Component	Sentinel Service	Sentinel Process	Function summary	Permissions required	Permission Explanation
Collector Manager	Sentinel	java agentengine (child process)	Manages Connectors and Collectors. It spawns off an agentengine process for each Collector it manages. Collector Manager also publishes system status messages, performs global filtering of events, and performs referential mappings. The agentengine process runs as an interpreter for Collector scripts, which normalize unprocessed (raw) events from security devices and systems producing event, vulnerability, and asset data that Sentinel can analyze and store in its database.	Network access (both outgoing access and local access to bind to ports greater than 1024) File read access to: ◆ ESEC_HOME /config ◆ ESEC_HOME /lib ◆ ESEC_HOME /jre File write access to: ◆ ESEC_HOME /data ◆ ESEC_HOME /log **NOTE:** Additionally, will need access to other resources depending which Connectors it is configured to run and which Event Sources it connecting to. Please refer to the individual Connector documentation for any additional permission requirements.	It communicates with iSCALE for configuration, event processing, and mapping data. It reads local configuration files and uses the java executable. It writes log files as well as caches data in the local file system.

C.3 Correlation Engine

Table C-3 *Correlation Engine*

Sentinel Component	Sentinel Service	Sentinel Process	Function summary	Permission's required	Permission Explanation
Correlation Engine	Sentinel	java	Receives events from the Collector Manager and publishes correlated events based on user-defined correlation rules.	Network access File read access to: ◆ ESEC_HOME /config ◆ ESEC_HOME /lib ◆ ESEC_HOME /jre File write access to: ◆ ESEC_HOME /data ◆ ESEC_HOME /log	It communicates over the network with iSCALE for configuration, event processing, and correlated event generation. It reads local configuration files and uses the java executable. It writes log files as well as caches data in the local file system.

C.4 Data Access Server (DAS)

Table C-4 *DATA Access Server (DAS)*

Sentinel Component	Sentinel Service	Sentinel Process	Function summary	Permission's required	Permission Explanation
DAS	Sentinel	java (das_binary)	Responsible for event insertion.	Network access Database Access File read access to: ◆ ESEC_HOME /config ◆ ESEC_HOME /lib ◆ ESEC_HOME /jre File write access to: ◆ ESEC_HOME /data ◆ ESEC_HOME /log	It connects to the database to read and insert data. It communicates over the network with iSCALE for configuration and event processing and other general data processing. It reads local configuration files and uses the java executable. It writes log files as well as caches data in the local file system.
		java (das_query)	Provides general database access services, map data server, exploit detection data generation, Sentinel user login, and other general services.		
		java (das_rt)	Provides data that drives the Active View charts.		
		java (das_itrac)	Provides services to use and manage iTRAC workflow processes.		
		java (das_aggregation)	Summaries event data into summary database tables, primarily for use by reports.		

C.5 Sentinel Communication Server

Table C-5 *Sentinel Communication Server*

Sentinel Component	Sentinel Service	Sentinel Process	Function summary	Permission's required	Permission Explanation
Communication Server (iSCALE / MOM)	Sentinel	java (Sonic)	iSCALE: A Message Oriented Middleware (MOM). The iSCALE component provides a Java Message Service (JMS) framework for inter-process communication. Processes communicate through a broker, which is responsible for routing and buffering messages.	Network access (binds to port greater than 1024) File read access to: ◆ ESEC_HOME/jre File write access to: ◆ ESEC_HOME/3rdparty/SonicMQ/MQ7.0	It binds to local ports to accept TCP connections in order to perform its duties as a communication server. It reads local configuration files and uses the java executable. It writes to Sonic's internal database on the local file system.
		java (das_proxy)	iSCALE also has an SSL proxy that acts as an SSL bridge between the message bus and a client connecting through SSL.	Network access (binds to ports greater than 1024) File read access to: ◆ ESEC_HOME/config ◆ ESEC_HOME/lib ◆ ESEC_HOME/jre File write access to: ◆ ESEC_HOME/3rdparty/SonicMQ/MQ7.0 ◆ ESEC_HOME/data ◆ ESEC_HOME/log ◆ ESEC_HOME/config	It binds to local ports to accept SSL connections in order to perform its duties as a communication server. It reads local configuration files and uses the java executable. It writes log files, caches data, and writes to Sonic's internal database on the local file system. It also will write certificates to config directory when required.

C.6 Sentinel Service

Table C-6 *Sentinel Service*

Sentinel Component	Sentinel Service	Sentinel Process	Function summary	Permission's required	Permission Explanation
Sentinel Service	Sentinel	wrapper	Registers as a service with the operating system and, when executed, launches the java Sentinel Service.	Network access File read access to: ◆ ESEC_HOME /config ◆ ESEC_HOME /lib ◆ ESEC_HOME /jre File write access to: ◆ ESEC_HOME /log	It communicates over the network with iSCALE for configuration and status reporting. It reads local configuration files and uses the java executable. It writes log files to the local file system.
		java (sentinel)	The java Sentinel Service process that is responsible for launching, restarting, and reporting status on the other Sentinel Server processes.		

C.7 Reporting Server

Table C-7 *Reporting Server*

Sentinel Component	Sentinel Application	Sentinel Service	Sentinel Process	Function summary	Permission's required
Reports	-	-	-	Crystal Reports XI or Crystal Enterprise 9 Standard is one of the reporting tools with Sentinel.	-

Microsoft SQL Users, Roles,and Access Permissions for Sentinel

D

The purpose of this document is to provide a detailed breakdown of Sentinel database users, roles and their access permissions.

D.1 Sentinel Database Instance

Below listed are the Sentinel database instances

D.1.1 ESEC

This instance have:

Users:

- esecadm
- esecapp
- esecdba
- esecrpt
- Other users

NOTE: Other users are created through User Manager. For detailed access permissions, see Section D.3, “Sentinel Database Roles,” on page 209.

Roles:

- ESEC_APP: The same permission as db_owner
- ESEC_ETL
- ESEC_USER

D.1.2 ESEC_WF

- **Users:** esecapp: For detailed access permissions see the Section D.2, “Sentinel Database Users,” on page 207.
- **Roles:** ESEC_APP: For detailed access permissions see the Section D.3, “Sentinel Database Roles,” on page 209.

D.2 Sentinel Database Users

Below listed are the Sentinel database users

D.2.1 Summary

Table D-1 *Sentinel Database Users-Summary*

User Name	Group Name	Login Name	Default DB Name
Esecadm	ESEC_USER	esecadm	ESEC
Esecapp	ESEC_APP	esecapp	ESEC
Esecapp	ESEC_ETL	esecapp	ESEC
Esecapp	db_owner	esecapp	ESEC
Esecdba	db_owner	esecdba	ESEC
Esecrpt	ESEC_USER	esecrpt	ESEC

D.2.2 esecadm

Table D-2 *Sentinel Database Users-esecadm*

Login Name	DB Name	User Name	User of Alias
Esecadm	ESEC	ESEC_USER	MemberOf
Esecadm	ESEC	esecadm	User

D.2.3 esecapp

Table D-3 *Sentinel Database Users-esecapp*

Login Name	DB Name	User Name	User of Alias
Esecapp	ESEC	ESEC_APP	MemberOf
Esecapp	ESEC	ESEC_ETL	MemberOf
Esecapp	ESEC	esecapp	User
Esecapp	ESEC	db_owner	MemberOf
Esecapp	ESEC_WF	ESEC_APP	MemberOf
Esecapp	ESEC_WF	esecapp	User

D.2.4 esecdba

Table D-4 *Sentinel Database Users-esecdba*

Login Name	DB Name	User Name	User of Alias
Esecdba	ESEC	db_owner	MemberOf
Esecdba	ESEC	esecdba	User

D.2.5 esecrpt

Table D-5 *Sentinel Database Users-esecrpt*

Login Name	DB Name	User Name	User of Alias
Esecrpt	ESEC	ESEC_USER	MemberOf
Esecrpt	ESEC	esecrpt	User

D.3 Sentinel Database Roles

Below listed are the Sentinel database roles

D.3.1 Summary

- **ESEC_APP:** It is a database role for ESEC and ESEC_WF. It has the same permission as db_owner for ESEC instance.
- **ESEC_ETL:** It is a database role for ESEC instance.
- **ESEC_USER:** A role for ESEC instance.

D.3.2 ESEC_APP

For ESEC instance, ESEC_APP has the same permission as db_owner. ESEC_APP performs the activities of all database roles, as well as other maintenance and configuration activities in the database. The permissions of this role span all of the other fixed database roles.

For ESEC_WF instance, these are the permission for ESEC_APP role:

Table D-6 *Sentinel Database Roles-ESEC_APP*

Role Name	Object Name	Action	Type
ESEC_APP	Activities	193 SELECT	U User table
ESEC_APP	Activities	195 INSERT	U User table
ESEC_APP	Activities	196 DELETE	U User table
ESEC_APP	Activities	197 UPDATE	U User table

Role Name	Object Name	Action	Type
ESEC_APP	ActivityData	193 SELECT	U User table
ESEC_APP	ActivityData	195 INSERT	U User table
ESEC_APP	ActivityData	196 DELETE	U User table
ESEC_APP	ActivityData	197 UPDATE	U User table
ESEC_APP	ActivityDataBLOBs	193 SELECT	U User table
ESEC_APP	ActivityDataBLOBs	195 INSERT	U User table
ESEC_APP	ActivityDataBLOBs	196 DELETE	U User table
ESEC_APP	ActivityDataBLOBs	197 UPDATE	U User table
ESEC_APP	ActivityDataWOB	193 SELECT	U User table
ESEC_APP	ActivityDataWOB	195 INSERT	U User table
ESEC_APP	ActivityDataWOB	196 DELETE	U User table
ESEC_APP	ActivityDataWOB	197 UPDATE	U User table
ESEC_APP	ActivityStateEventAudits	193 SELECT	U User table
ESEC_APP	ActivityStateEventAudits	195 INSERT	U User table
ESEC_APP	ActivityStateEventAudits	196 DELETE	U User table
ESEC_APP	ActivityStateEventAudits	197 UPDATE	U User table
ESEC_APP	ActivityStates	193 SELECT	U User table
ESEC_APP	ActivityStates	195 INSERT	U User table
ESEC_APP	ActivityStates	196 DELETE	U User table
ESEC_APP	ActivityStates	197 UPDATE	U User table
ESEC_APP	AndJoinTable	193 SELECT	U User table
ESEC_APP	AndJoinTable	195 INSERT	U User table
ESEC_APP	AndJoinTable	196 DELETE	U User table
ESEC_APP	AndJoinTable	197 UPDATE	U User table
ESEC_APP	AssignmentEventAudits	193 SELECT	U User table
ESEC_APP	AssignmentEventAudits	195 INSERT	U User table
ESEC_APP	AssignmentEventAudits	196 DELETE	U User table
ESEC_APP	AssignmentEventAudits	197 UPDATE	U User table
ESEC_APP	AssignmentsTable	193 SELECT	U User table
ESEC_APP	AssignmentsTable	195 INSERT	U User table
ESEC_APP	AssignmentsTable	196 DELETE	U User table
ESEC_APP	AssignmentsTable	197 UPDATE	U User table

Role Name	Object Name	Action	Type
ESEC_APP	Counters	193 SELECT	U User table
ESEC_APP	Counters	195 INSERT	U User table
ESEC_APP	Counters	196 DELETE	U User table
ESEC_APP	Counters	197 UPDATE	U User table
ESEC_APP	CreateProcessEventAudits	193 SELECT	U User table
ESEC_APP	CreateProcessEventAudits	195 INSERT	U User table
ESEC_APP	CreateProcessEventAudits	196 DELETE	U User table
ESEC_APP	CreateProcessEventAudits	197 UPDATE	U User table
ESEC_APP	DataEventAudits	193 SELECT	U User table
ESEC_APP	DataEventAudits	195 INSERT	U User table
ESEC_APP	DataEventAudits	196 DELETE	U User table
ESEC_APP	DataEventAudits	197 UPDATE	U User table
ESEC_APP	Deadlines	193 SELECT	U User table
ESEC_APP	Deadlines	195 INSERT	U User table
ESEC_APP	Deadlines	196 DELETE	U User table
ESEC_APP	Deadlines	197 UPDATE	U User table
ESEC_APP	EventTypes	193 SELECT	U User table
ESEC_APP	EventTypes	195 INSERT	U User table
ESEC_APP	EventTypes	196 DELETE	U User table
ESEC_APP	EventTypes	197 UPDATE	U User table
ESEC_APP	GroupGroupTable	193 SELECT	U User table
ESEC_APP	GroupGroupTable	195 INSERT	U User table
ESEC_APP	GroupGroupTable	196 DELETE	U User table
ESEC_APP	GroupGroupTable	197 UPDATE	U User table
ESEC_APP	GroupTable	193 SELECT	U User table
ESEC_APP	GroupTable	195 INSERT	U User table
ESEC_APP	GroupTable	196 DELETE	U User table
ESEC_APP	GroupTable	197 UPDATE	U User table
ESEC_APP	GroupUser	193 SELECT	U User table
ESEC_APP	GroupUser	195 INSERT	U User table
ESEC_APP	GroupUser	196 DELETE	U User table
ESEC_APP	GroupUser	197 UPDATE	U User table

Role Name	Object Name	Action	Type
ESEC_APP	GroupUserPackLevelParticipant	193 SELECT	U User table
ESEC_APP	GroupUserPackLevelParticipant	195 INSERT	U User table
ESEC_APP	GroupUserPackLevelParticipant	196 DELETE	U User table
ESEC_APP	GroupUserPackLevelParticipant	197 UPDATE	U User table
ESEC_APP	GroupUserProcLevelParticipant	193 SELECT	U User table
ESEC_APP	GroupUserProcLevelParticipant	195 INSERT	U User table
ESEC_APP	GroupUserProcLevelParticipant	196 DELETE	U User table
ESEC_APP	GroupUserProcLevelParticipant	197 UPDATE	U User table
ESEC_APP	LockTable	193 SELECT	U User table
ESEC_APP	LockTable	195 INSERT	U User table
ESEC_APP	LockTable	196 DELETE	U User table
ESEC_APP	LockTable	197 UPDATE	U User table
ESEC_APP	NewEventAuditData	193 SELECT	U User table
ESEC_APP	NewEventAuditData	195 INSERT	U User table
ESEC_APP	NewEventAuditData	196 DELETE	U User table
ESEC_APP	NewEventAuditData	197 UPDATE	U User table
ESEC_APP	NewEventAuditDataBLOBs	193 SELECT	U User table
ESEC_APP	NewEventAuditDataBLOBs	195 INSERT	U User table
ESEC_APP	NewEventAuditDataBLOBs	196 DELETE	U User table
ESEC_APP	NewEventAuditDataBLOBs	197 UPDATE	U User table
ESEC_APP	NewEventAuditDataWOB	193 SELECT	U User table
ESEC_APP	NewEventAuditDataWOB	195 INSERT	U User table
ESEC_APP	NewEventAuditDataWOB	196 DELETE	U User table
ESEC_APP	NewEventAuditDataWOB	197 UPDATE	U User table
ESEC_APP	NextXPDLVersions	193 SELECT	U User table
ESEC_APP	NextXPDLVersions	195 INSERT	U User table
ESEC_APP	NextXPDLVersions	196 DELETE	U User table
ESEC_APP	NextXPDLVersions	197 UPDATE	U User table
ESEC_APP	NormalUser	193 SELECT	U User table
ESEC_APP	NormalUser	195 INSERT	U User table
ESEC_APP	NormalUser	196 DELETE	U User table
ESEC_APP	NormalUser	197 UPDATE	U User table

Role Name	Object Name	Action	Type
ESEC_APP	ObjectId	193 SELECT	U User table
ESEC_APP	ObjectId	195 INSERT	U User table
ESEC_APP	ObjectId	196 DELETE	U User table
ESEC_APP	ObjectId	197 UPDATE	U User table
ESEC_APP	OldEventAuditData	193 SELECT	U User table
ESEC_APP	OldEventAuditData	195 INSERT	U User table
ESEC_APP	OldEventAuditData	196 DELETE	U User table
ESEC_APP	OldEventAuditData	197 UPDATE	U User table
ESEC_APP	OldEventAuditDataBLOBs	193 SELECT	U User table
ESEC_APP	OldEventAuditDataBLOBs	195 INSERT	U User table
ESEC_APP	OldEventAuditDataBLOBs	196 DELETE	U User table
ESEC_APP	OldEventAuditDataBLOBs	197 UPDATE	U User table
ESEC_APP	OldEventAuditDataWOB	193 SELECT	U User table
ESEC_APP	OldEventAuditDataWOB	195 INSERT	U User table
ESEC_APP	OldEventAuditDataWOB	196 DELETE	U User table
ESEC_APP	OldEventAuditDataWOB	197 UPDATE	U User table
ESEC_APP	PackLevelParticipant	193 SELECT	U User table
ESEC_APP	PackLevelParticipant	195 INSERT	U User table
ESEC_APP	PackLevelParticipant	196 DELETE	U User table
ESEC_APP	PackLevelParticipant	197 UPDATE	U User table
ESEC_APP	PackLevelXPDLApp	193 SELECT	U User table
ESEC_APP	PackLevelXPDLApp	195 INSERT	U User table
ESEC_APP	PackLevelXPDLApp	196 DELETE	U User table
ESEC_APP	PackLevelXPDLApp	197 UPDATE	U User table
ESEC_APP	PackLevelXPDLAppTAAppDetail	193 SELECT	U User table
ESEC_APP	PackLevelXPDLAppTAAppDetail	195 INSERT	U User table
ESEC_APP	PackLevelXPDLAppTAAppDetail	196 DELETE	U User table
ESEC_APP	PackLevelXPDLAppTAAppDetail	197 UPDATE	U User table
ESEC_APP	PackLevelXPDLAppTAAppDetailUsr	193 SELECT	U User table
ESEC_APP	PackLevelXPDLAppTAAppDetailUsr	195 INSERT	U User table
ESEC_APP	PackLevelXPDLAppTAAppDetailUsr	196 DELETE	U User table
ESEC_APP	PackLevelXPDLAppTAAppDetailUsr	197 UPDATE	U User table

Role Name	Object Name	Action	Type
ESEC_APP	PackLevelXPDLAppTAAppUser	193 SELECT	U User table
ESEC_APP	PackLevelXPDLAppTAAppUser	195 INSERT	U User table
ESEC_APP	PackLevelXPDLAppTAAppUser	196 DELETE	U User table
ESEC_APP	PackLevelXPDLAppTAAppUser	197 UPDATE	U User table
ESEC_APP	PackLevelXPDLAppToolAgentApp	193 SELECT	U User table
ESEC_APP	PackLevelXPDLAppToolAgentApp	195 INSERT	U User table
ESEC_APP	PackLevelXPDLAppToolAgentApp	196 DELETE	U User table
ESEC_APP	PackLevelXPDLAppToolAgentApp	197 UPDATE	U User table
ESEC_APP	ProcessData	193 SELECT	U User table
ESEC_APP	ProcessData	195 INSERT	U User table
ESEC_APP	ProcessData	196 DELETE	U User table
ESEC_APP	ProcessData	197 UPDATE	U User table
ESEC_APP	ProcessDataBLOBs	193 SELECT	U User table
ESEC_APP	ProcessDataBLOBs	195 INSERT	U User table
ESEC_APP	ProcessDataBLOBs	196 DELETE	U User table
ESEC_APP	ProcessDataBLOBs	197 UPDATE	U User table
ESEC_APP	ProcessDataWOB	193 SELECT	U User table
ESEC_APP	ProcessDataWOB	195 INSERT	U User table
ESEC_APP	ProcessDataWOB	196 DELETE	U User table
ESEC_APP	ProcessDataWOB	197 UPDATE	U User table
ESEC_APP	ProcessDefinitions	193 SELECT	U User table
ESEC_APP	ProcessDefinitions	195 INSERT	U User table
ESEC_APP	ProcessDefinitions	196 DELETE	U User table
ESEC_APP	ProcessDefinitions	197 UPDATE	U User table
ESEC_APP	Processes	193 SELECT	U User table
ESEC_APP	Processes	195 INSERT	U User table
ESEC_APP	Processes	196 DELETE	U User table
ESEC_APP	Processes	197 UPDATE	U User table
ESEC_APP	ProcessRequesters	193 SELECT	U User table
ESEC_APP	ProcessRequesters	195 INSERT	U User table
ESEC_APP	ProcessRequesters	196 DELETE	U User table
ESEC_APP	ProcessRequesters	197 UPDATE	U User table

Role Name	Object Name	Action	Type
ESEC_APP	ProcessStateEventAudits	193 SELECT	U User table
ESEC_APP	ProcessStateEventAudits	195 INSERT	U User table
ESEC_APP	ProcessStateEventAudits	196 DELETE	U User table
ESEC_APP	ProcessStateEventAudits	197 UPDATE	U User table
ESEC_APP	ProcessStates	193 SELECT	U User table
ESEC_APP	ProcessStates	195 INSERT	U User table
ESEC_APP	ProcessStates	196 DELETE	U User table
ESEC_APP	ProcessStates	197 UPDATE	U User table
ESEC_APP	ProcLevelParticipant	193 SELECT	U User table
ESEC_APP	ProcLevelParticipant	195 INSERT	U User table
ESEC_APP	ProcLevelParticipant	196 DELETE	U User table
ESEC_APP	ProcLevelParticipant	197 UPDATE	U User table
ESEC_APP	ProcLevelXPDLApp	193 SELECT	U User table
ESEC_APP	ProcLevelXPDLApp	195 INSERT	U User table
ESEC_APP	ProcLevelXPDLApp	196 DELETE	U User table
ESEC_APP	ProcLevelXPDLApp	197 UPDATE	U User table
ESEC_APP	ProcLevelXPDLAppTAAppDetail	193 SELECT	U User table
ESEC_APP	ProcLevelXPDLAppTAAppDetail	195 INSERT	U User table
ESEC_APP	ProcLevelXPDLAppTAAppDetail	196 DELETE	U User table
ESEC_APP	ProcLevelXPDLAppTAAppDetail	197 UPDATE	U User table
ESEC_APP	ProcLevelXPDLAppTAAppDetailUsr	193 SELECT	U User table
ESEC_APP	ProcLevelXPDLAppTAAppDetailUsr	195 INSERT	U User table
ESEC_APP	ProcLevelXPDLAppTAAppDetailUsr	196 DELETE	U User table
ESEC_APP	ProcLevelXPDLAppTAAppDetailUsr	197 UPDATE	U User table
ESEC_APP	ProcLevelXPDLAppTAAppUser	193 SELECT	U User table
ESEC_APP	ProcLevelXPDLAppTAAppUser	195 INSERT	U User table
ESEC_APP	ProcLevelXPDLAppTAAppUser	196 DELETE	U User table
ESEC_APP	ProcLevelXPDLAppTAAppUser	197 UPDATE	U User table
ESEC_APP	ProcLevelXPDLAppToolAgentApp	193 SELECT	U User table
ESEC_APP	ProcLevelXPDLAppToolAgentApp	195 INSERT	U User table
ESEC_APP	ProcLevelXPDLAppToolAgentApp	196 DELETE	U User table
ESEC_APP	ProcLevelXPDLAppToolAgentApp	197 UPDATE	U User table

Role Name	Object Name	Action	Type
ESEC_APP	ResourcesTable	193 SELECT	U User table
ESEC_APP	ResourcesTable	195 INSERT	U User table
ESEC_APP	ResourcesTable	196 DELETE	U User table
ESEC_APP	ResourcesTable	197 UPDATE	U User table
ESEC_APP	StateEventAudits	193 SELECT	U User table
ESEC_APP	StateEventAudits	195 INSERT	U User table
ESEC_APP	StateEventAudits	196 DELETE	U User table
ESEC_APP	StateEventAudits	197 UPDATE	U User table
ESEC_APP	ToolAgentApp	193 SELECT	U User table
ESEC_APP	ToolAgentApp	195 INSERT	U User table
ESEC_APP	ToolAgentApp	196 DELETE	U User table
ESEC_APP	ToolAgentApp	197 UPDATE	U User table
ESEC_APP	ToolAgentAppDetail	193 SELECT	U User table
ESEC_APP	ToolAgentAppDetail	195 INSERT	U User table
ESEC_APP	ToolAgentAppDetail	196 DELETE	U User table
ESEC_APP	ToolAgentAppDetail	197 UPDATE	U User table
ESEC_APP	ToolAgentAppDetailUser	193 SELECT	U User table
ESEC_APP	ToolAgentAppDetailUser	195 INSERT	U User table
ESEC_APP	ToolAgentAppDetailUser	196 DELETE	U User table
ESEC_APP	ToolAgentAppDetailUser	197 UPDATE	U User table
ESEC_APP	ToolAgentAppUser	193 SELECT	U User table
ESEC_APP	ToolAgentAppUser	195 INSERT	U User table
ESEC_APP	ToolAgentAppUser	196 DELETE	U User table
ESEC_APP	ToolAgentAppUser	197 UPDATE	U User table
ESEC_APP	ToolAgentUser	193 SELECT	U User table
ESEC_APP	ToolAgentUser	195 INSERT	U User table
ESEC_APP	ToolAgentUser	196 DELETE	U User table
ESEC_APP	ToolAgentUser	197 UPDATE	U User table
ESEC_APP	UserGroupTable	193 SELECT	U User table
ESEC_APP	UserGroupTable	195 INSERT	U User table
ESEC_APP	UserGroupTable	196 DELETE	U User table
ESEC_APP	UserGroupTable	197 UPDATE	U User table

Role Name	Object Name	Action	Type
ESEC_APP	UserPackLevelParticipant	193 SELECT	U User table
ESEC_APP	UserPackLevelParticipant	195 INSERT	U User table
ESEC_APP	UserPackLevelParticipant	196 DELETE	U User table
ESEC_APP	UserPackLevelParticipant	197 UPDATE	U User table
ESEC_APP	UserProcLevelParticipant	193 SELECT	U User table
ESEC_APP	UserProcLevelParticipant	195 INSERT	U User table
ESEC_APP	UserProcLevelParticipant	196 DELETE	U User table
ESEC_APP	UserProcLevelParticipant	197 UPDATE	U User table
ESEC_APP	UserTable	193 SELECT	U User table
ESEC_APP	UserTable	195 INSERT	U User table
ESEC_APP	UserTable	196 DELETE	U User table
ESEC_APP	UserTable	197 UPDATE	U User table
ESEC_APP	XPDLApplicationPackage	193 SELECT	U User table
ESEC_APP	XPDLApplicationPackage	195 INSERT	U User table
ESEC_APP	XPDLApplicationPackage	196 DELETE	U User table
ESEC_APP	XPDLApplicationPackage	197 UPDATE	U User table
ESEC_APP	XPDLApplicationProcess	193 SELECT	U User table
ESEC_APP	XPDLApplicationProcess	195 INSERT	U User table
ESEC_APP	XPDLApplicationProcess	196 DELETE	U User table
ESEC_APP	XPDLApplicationProcess	197 UPDATE	U User table
ESEC_APP	XPDLData	193 SELECT	U User table
ESEC_APP	XPDLData	195 INSERT	U User table
ESEC_APP	XPDLData	196 DELETE	U User table
ESEC_APP	XPDLData	197 UPDATE	U User table
ESEC_APP	XPDLHistory	193 SELECT	U User table
ESEC_APP	XPDLHistory	195 INSERT	U User table
ESEC_APP	XPDLHistory	196 DELETE	U User table
ESEC_APP	XPDLHistory	197 UPDATE	U User table
ESEC_APP	XPDLHistoryData	193 SELECT	U User table
ESEC_APP	XPDLHistoryData	195 INSERT	U User table
ESEC_APP	XPDLHistoryData	197 UPDATE	U User table
ESEC_APP	XPDLHistoryData	196 DELETE	U User table

Role Name	Object Name	Action	Type
ESEC_APP	XPDLParticipantPackage	193 SELECT	U User table
ESEC_APP	XPDLParticipantPackage	195 INSERT	U User table
ESEC_APP	XPDLParticipantPackage	196 DELETE	U User table
ESEC_APP	XPDLParticipantPackage	197 UPDATE	U User table
ESEC_APP	XPDLParticipantProcess	193 SELECT	U User table
ESEC_APP	XPDLParticipantProcess	195 INSERT	U User table
ESEC_APP	XPDLParticipantProcess	196 DELETE	U User table
ESEC_APP	XPDLParticipantProcess	197 UPDATE	U User table
ESEC_APP	XPDLReferences	193 SELECT	U User table
ESEC_APP	XPDLReferences	195 INSERT	U User table
ESEC_APP	XPDLReferences	196 DELETE	U User table
ESEC_APP	XPDLReferences	197 UPDATE	U User table
ESEC_APP	XPDLS	193 SELECT	U User table
ESEC_APP	XPDLS	195 INSERT	U User table
ESEC_APP	XPDLS	196 DELETE	U User table
ESEC_APP	XPDLS	197 UPDATE	U User table

D.3.3 ESEC_ETL

Table D-7 *Sentinel Database Roles-ESEC_ETL*

Role Name	Object Name	Action	Type
ESEC_ETL	ACTVY	193 SELECT	U User table
ESEC_ETL	ACTVY_PARM	193 SELECT	U User table
ESEC_ETL	ACTVY_REF	193 SELECT	U User table
ESEC_ETL	ACTVY_REF_PARM_VAL	193 SELECT	U User table
ESEC_ETL	ADV_ALERT	193 SELECT	U User table
ESEC_ETL	ADV_ALERT_CVE	193 SELECT	U User table
ESEC_ETL	ADV_ALERT_PRODUCT	193 SELECT	U User table
ESEC_ETL	ADV_ATTACK	193 SELECT	U User table
ESEC_ETL	ADV_ATTACK_ALERT	193 SELECT	U User table
ESEC_ETL	ADV_ATTACK_CVE	193 SELECT	U User table
ESEC_ETL	ADV_ATTACK_MAP	193 SELECT	U User table

Role Name	Object Name	Action	Type
ESEC_ETL	ADV_ATTACK_PLUGIN	193 SELECT	U User table
ESEC_ETL	ADV_CREDIBILITY	193 SELECT	U User table
ESEC_ETL	ADV_FEED	193 SELECT	U User table
ESEC_ETL	ADV_PRODUCT	193 SELECT	U User table
ESEC_ETL	ADV_PRODUCT_SERVICE_PACK	193 SELECT	U User table
ESEC_ETL	ADV_PRODUCT_VERSION	193 SELECT	U User table
ESEC_ETL	ADV_SEVERITY	193 SELECT	U User table
ESEC_ETL	ADV_SUBALERT	193 SELECT	U User table
ESEC_ETL	ADV_URGENCY	193 SELECT	U User table
ESEC_ETL	ADV_VENDOR	193 SELECT	U User table
ESEC_ETL	ADV_VULN_PRODUCT	193 SELECT	U User table
ESEC_ETL	ANNOTATIONS	193 SELECT	U User table
ESEC_ETL	ASSET	193 SELECT	U User table
ESEC_ETL	ASSET_CTGRY	193 SELECT	U User table
ESEC_ETL	ASSET_HOSTNAME	193 SELECT	U User table
ESEC_ETL	ASSET_IP	193 SELECT	U User table
ESEC_ETL	ASSET_LOC	193 SELECT	U User table
ESEC_ETL	ASSET_VAL_LKUP	193 SELECT	U User table
ESEC_ETL	ASSET_X_ENTITY_X_ROLE	193 SELECT	U User table
ESEC_ETL	ASSOCIATIONS	193 SELECT	U User table
ESEC_ETL	ATTACHMENTS	193 SELECT	U User table
ESEC_ETL	AUDIT_RECORD	193 SELECT	U User table
ESEC_ETL	CONFIGS	193 SELECT	U User table
ESEC_ETL	CONTACTS	193 SELECT	U User table
ESEC_ETL	CORR_ACT_DEF	193 SELECT	U User table
ESEC_ETL	CORR_ACT_META	193 SELECT	U User table
ESEC_ETL	CORR_ACT_PARM	193 SELECT	U User table
ESEC_ETL	CORR_ACT_PARM_DEF	193 SELECT	U User table
ESEC_ETL	CORR_DEPLOY_CONFIG	193 SELECT	U User table
ESEC_ETL	CORR_ENGINE_CONFIG	193 SELECT	U User table
ESEC_ETL	CORR_RULE	193 SELECT	U User table
ESEC_ETL	CORR_RULE_CFG	193 SELECT	U User table

Role Name	Object Name	Action	Type
ESEC_ETL	CORRELATED_EVENTS_P_MAX	193 SELECT	U User table
ESEC_ETL	CORRELATED_EVENTS_P_MIN	193 SELECT	U User table
ESEC_ETL	CRIT_LKUP	193 SELECT	U User table
ESEC_ETL	CUST	193 SELECT	U User table
ESEC_ETL	CUST_HIERARCHY	193 SELECT	U User table
ESEC_ETL	ENTITY_TYP_LKUP	193 SELECT	U User table
ESEC_ETL	ENV_IDENTITY_LKUP	193 SELECT	U User table
ESEC_ETL	ESEC_ARCHIVE_CONFIG	193 SELECT	U User table
ESEC_ETL	ESEC_ARCHIVE_LOG_FILES	193 SELECT	U User table
ESEC_ETL	ESEC_ARCHIVE_LOGS	193 SELECT	U User table
ESEC_ETL	ESEC_DB_PATCHES	193 SELECT	U User table
ESEC_ETL	ESEC_DB_VERSION	193 SELECT	U User table
ESEC_ETL	ESEC_DISPLAY	193 SELECT	U User table
ESEC_ETL	ESEC_JOB_CONFIG	193 SELECT	U User table
ESEC_ETL	ESEC_JOB_STS	193 SELECT	U User table
ESEC_ETL	ESEC_NAMESPACE	193 SELECT	U User table
ESEC_ETL	ESEC_NAMESPACE_LEAF	193 SELECT	U User table
ESEC_ETL	ESEC_PARTITION_CONFIG	193 SELECT	U User table
ESEC_ETL	ESEC_PORT_REFERENCE	193 SELECT	U User table
ESEC_ETL	ESEC_PROTOCOL_REFERENCE	193 SELECT	U User table
ESEC_ETL	ESEC_SDM_LOCK	193 SELECT	U User table
ESEC_ETL	ESEC_SEQUENCE	193 SELECT	U User table
ESEC_ETL	ESEC_TABLE_GROUPS	193 SELECT	U User table
ESEC_ETL	ESEC_UUID_UUID_ASSOC	193 SELECT	U User table
ESEC_ETL	EVENTS_P_MAX	193 SELECT	U User table
ESEC_ETL	EVENTS_P_MIN	193 SELECT	U User table
ESEC_ETL	EVT_AGENT	193 SELECT	U User table
ESEC_ETL	EVT_ASSET	193 SELECT	U User table
ESEC_ETL	EVT_DEST_EVT_NAME_SMRY_1_P_MAX	193 SELECT	U User table
ESEC_ETL	EVT_DEST_EVT_NAME_SMRY_1_P_MAX	195 INSERT	U User table
ESEC_ETL	EVT_DEST_EVT_NAME_SMRY_1_P_MAX	196 DELETE	U User table
ESEC_ETL	EVT_DEST_EVT_NAME_SMRY_1_P_MAX	197 UPDATE	U User table

Role Name	Object Name	Action	Type
ESEC_ETL	EVT_DEST_EVT_NAME_SMRY_1_P_MIN	193 SELECT	U User table
ESEC_ETL	EVT_DEST_SMRY_1_P_MAX	193 SELECT	U User table
ESEC_ETL	EVT_DEST_SMRY_1_P_MAX	195 INSERT	U User table
ESEC_ETL	EVT_DEST_SMRY_1_P_MAX	196 DELETE	U User table
ESEC_ETL	EVT_DEST_SMRY_1_P_MAX	197 UPDATE	U User table
ESEC_ETL	EVT_DEST_SMRY_1_P_MIN	193 SELECT	U User table
ESEC_ETL	EVT_DEST_TXNMY_SMRY_1_P_MAX	193 SELECT	U User table
ESEC_ETL	EVT_DEST_TXNMY_SMRY_1_P_MAX	195 INSERT	U User table
ESEC_ETL	EVT_DEST_TXNMY_SMRY_1_P_MAX	196 DELETE	U User table
ESEC_ETL	EVT_DEST_TXNMY_SMRY_1_P_MAX	197 UPDATE	U User table
ESEC_ETL	EVT_DEST_TXNMY_SMRY_1_P_MIN	193 SELECT	U User table
ESEC_ETL	EVT_NAME	193 SELECT	U User table
ESEC_ETL	EVT_NAME	195 INSERT	U User table
ESEC_ETL	EVT_NAME	196 DELETE	U User table
ESEC_ETL	EVT_NAME	197 UPDATE	U User table
ESEC_ETL	EVT_PORT_SMRY_1_P_MAX	193 SELECT	U User table
ESEC_ETL	EVT_PORT_SMRY_1_P_MAX	195 INSERT	U User table
ESEC_ETL	EVT_PORT_SMRY_1_P_MAX	196 DELETE	U User table
ESEC_ETL	EVT_PORT_SMRY_1_P_MAX	197 UPDATE	U User table
ESEC_ETL	EVT_PORT_SMRY_1_P_MIN	193 SELECT	U User table
ESEC_ETL	EVT_PRTCL	193 SELECT	U User table
ESEC_ETL	EVT_RSRC	193 SELECT	U User table
ESEC_ETL	EVT_SEV_SMRY_1_P_MAX	193 SELECT	U User table
ESEC_ETL	EVT_SEV_SMRY_1_P_MAX	195 INSERT	U User table
ESEC_ETL	EVT_SEV_SMRY_1_P_MAX	196 DELETE	U User table
ESEC_ETL	EVT_SEV_SMRY_1_P_MAX	197 UPDATE	U User table
ESEC_ETL	EVT_SEV_SMRY_1_P_MIN	193 SELECT	U User table
ESEC_ETL	EVT_SRC	193 SELECT	U User table
ESEC_ETL	EVT_SRC_COLLECTOR	193 SELECT	U User table
ESEC_ETL	EVT_SRC_GRP	193 SELECT	U User table
ESEC_ETL	EVT_SRC_MGR	193 SELECT	U User table
ESEC_ETL	EVT_SRC_OFFSET	193 SELECT	U User table

Role Name	Object Name	Action	Type
ESEC_ETL	EVT_SRC_SMRY_1_P_MAX	193 SELECT	U User table
ESEC_ETL	EVT_SRC_SMRY_1_P_MAX	195 INSERT	U User table
ESEC_ETL	EVT_SRC_SMRY_1_P_MAX	196 DELETE	U User table
ESEC_ETL	EVT_SRC_SMRY_1_P_MAX	197 UPDATE	U User table
ESEC_ETL	EVT_SRC_SMRY_1_P_MIN	193 SELECT	U User table
ESEC_ETL	EVT_SRC_SRVR	193 SELECT	U User table
ESEC_ETL	EVT_TXNMY	193 SELECT	U User table
ESEC_ETL	EVT_USR	193 SELECT	U User table
ESEC_ETL	EVT_USR	195 INSERT	U User table
ESEC_ETL	EVT_USR	196 DELETE	U User table
ESEC_ETL	EVT_USR	197 UPDATE	U User table
ESEC_ETL	EXT_DATA	193 SELECT	U User table
ESEC_ETL	HIST_CORRELATED_EVENTS_P_MAX	193 SELECT	U User table
ESEC_ETL	HIST_EVENTS_P_MAX	193 SELECT	U User table
ESEC_ETL	IMAGES	193 SELECT	U User table
ESEC_ETL	INCIDENTS	193 SELECT	U User table
ESEC_ETL	INCIDENTS_ASSETS	193 SELECT	U User table
ESEC_ETL	INCIDENTS_EVENTS	193 SELECT	U User table
ESEC_ETL	INCIDENTS_VULN	193 SELECT	U User table
ESEC_ETL	L_STAT	193 SELECT	U User table
ESEC_ETL	LOGS	193 SELECT	U User table
ESEC_ETL	MD_CONFIG	193 SELECT	U User table
ESEC_ETL	MD_EVT_FILE_STS	193 SELECT	U User table
ESEC_ETL	MD_EVT_FILE_STS	195 INSERT	U User table
ESEC_ETL	MD_EVT_FILE_STS	196 DELETE	U User table
ESEC_ETL	MD_EVT_FILE_STS	197 UPDATE	U User table
ESEC_ETL	MD_SMRY_STS	193 SELECT	U User table
ESEC_ETL	MD_SMRY_STS	195 INSERT	U User table
ESEC_ETL	MD_SMRY_STS	196 DELETE	U User table
ESEC_ETL	MD_SMRY_STS	197 UPDATE	U User table
ESEC_ETL	MD_VIEW_CONFIG	193 SELECT	U User table
ESEC_ETL	MSSP_ASSOCIATIONS	193 SELECT	U User table

Role Name	Object Name	Action	Type
ESEC_ETL	NETWORK_IDENTITY_LKUP	193 SELECT	U User table
ESEC_ETL	NLS_CONFIG	193 SELECT	U User table
ESEC_ETL	NLS_MSG_TRANSLATION	193 SELECT	U User table
ESEC_ETL	NORM_ATTACK_CD_MAP	193 SELECT	U User table
ESEC_ETL	OBJ_STORE	193 SELECT	U User table
ESEC_ETL	OFFLINE_QRY_STS	193 SELECT	U User table
ESEC_ETL	ORGANIZATION	193 SELECT	U User table
ESEC_ETL	PERSON	193 SELECT	U User table
ESEC_ETL	PHYSICAL_ASSET	193 SELECT	U User table
ESEC_ETL	PRDT	193 SELECT	U User table
ESEC_ETL	ROLE_LKUP	193 SELECT	U User table
ESEC_ETL	RPT_TRANSLATION	193 SELECT	U User table
ESEC_ETL	SENSITIVITY_LKUP	193 SELECT	U User table
ESEC_ETL	SENTINEL	193 SELECT	U User table
ESEC_ETL	SENTINEL_HOST	193 SELECT	U User table
ESEC_ETL	SENTINEL_PLUGIN	193 SELECT	U User table
ESEC_ETL	STATES	193 SELECT	U User table
ESEC_ETL	TXNMY_NODE	193 SELECT	U User table
ESEC_ETL	USERS	193 SELECT	U User table
ESEC_ETL	VNDR	193 SELECT	U User table
ESEC_ETL	VULN	193 SELECT	U User table
ESEC_ETL	VULN_CODE	193 SELECT	U User table
ESEC_ETL	VULN_INFO	193 SELECT	U User table
ESEC_ETL	VULN_RSRC	193 SELECT	U User table
ESEC_ETL	VULN_RSRC_SCAN	193 SELECT	U User table
ESEC_ETL	VULN_SCAN	193 SELECT	U User table
ESEC_ETL	VULN_SCAN_VULN	193 SELECT	U User table
ESEC_ETL	VULN_SCANNER	193 SELECT	U User table
ESEC_ETL	WORKFLOW_DEF	193 SELECT	U User table
ESEC_ETL	WORKFLOW_INFO	193 SELECT	U User table

D.3.4 ESEC_USER

Table D-8 *Sentinel Database Roles-ESEC_USER*

Role Name	Object Name	Action	Type
ESEC_USER	ADV_ALERT_CVE_RPT_V	193 SELECT	V View
ESEC_USER	ADV_ALERT_PRODUCT_RPT_V	193 SELECT	V View
ESEC_USER	ADV_ALERT_RPT_V	193 SELECT	V View
ESEC_USER	ADV_ATTACK_ALERT_RPT_V	193 SELECT	V View
ESEC_USER	ADV_ATTACK_CVE_RPT_V	193 SELECT	V View
ESEC_USER	ADV_ATTACK_PLUGIN_RPT_V	193 SELECT	V View
ESEC_USER	ADV_ATTACK_RPT_V	193 SELECT	V View
ESEC_USER	ADV_CREDIBILITY_RPT_V	193 SELECT	V View
ESEC_USER	ADV_FEED_RPT_V	193 SELECT	V View
ESEC_USER	ADV_PRODUCT_RPT_V	193 SELECT	V View
ESEC_USER	ADV_PRODUCT_SERVICE_PACK_RPT_V	193 SELECT	V View
ESEC_USER	ADV_PRODUCT_VERSION_RPT_V	193 SELECT	V View
ESEC_USER	ADV_SEVERITY_RPT_V	193 SELECT	V View
ESEC_USER	ADV_SUBALERT_RPT_V	193 SELECT	V View
ESEC_USER	ADV_URGENCY_RPT_V	193 SELECT	V View
ESEC_USER	ADV_VENDOR_RPT_V	193 SELECT	V View
ESEC_USER	ADV_VULN_PRODUCT_RPT_V	193 SELECT	V View
ESEC_USER	ANNOTATIONS_RPT_V	193 SELECT	V View
ESEC_USER	ASSET_CATEGORY_RPT_V	193 SELECT	V View
ESEC_USER	ASSET_HOSTNAME_RPT_V	193 SELECT	V View
ESEC_USER	ASSET_IP_RPT_V	193 SELECT	V View
ESEC_USER	ASSET_LOCATION_RPT_V	193 SELECT	V View
ESEC_USER	ASSET_RPT_V	193 SELECT	V View
ESEC_USER	ASSET_VALUE_RPT_V	193 SELECT	V View
ESEC_USER	ASSET_X_ENTITY_X_ROLE_RPT_V	193 SELECT	V View
ESEC_USER	ASSOCIATIONS_RPT_V	193 SELECT	V View
ESEC_USER	ATTACHMENTS_RPT_V	193 SELECT	V View
ESEC_USER	CONFIGS_RPT_V	193 SELECT	V View
ESEC_USER	CONTACTS_RPT_V	193 SELECT	V View

Role Name	Object Name	Action	Type
ESEC_USER	CORRELATED_EVENTS	193 SELECT	V View
ESEC_USER	CORRELATED_EVENTS_RPT_V	193 SELECT	V View
ESEC_USER	CORRELATED_EVENTS_RPT_V1	193 SELECT	V View
ESEC_USER	CRITICALITY_RPT_V	193 SELECT	V View
ESEC_USER	CUST_HIERARCHY_V	193 SELECT	V View
ESEC_USER	CUST_RPT_V	193 SELECT	V View
ESEC_USER	ENTITY_TYPE_RPT_V	193 SELECT	V View
ESEC_USER	ENV_IDENTITY_RPT_V	193 SELECT	V View
ESEC_USER	ESEC_DISPLAY_RPT_V	193 SELECT	V View
ESEC_USER	ESEC_PORT_REFERENCE_RPT_V	193 SELECT	V View
ESEC_USER	ESEC_PROTOCOL_REFERENCE_RPT_V	193 SELECT	V View
ESEC_USER	ESEC_SEQUENCE_RPT_V	193 SELECT	V View
ESEC_USER	esec_check_patch	224 EXECUTE	FN Function
ESEC_USER	get_string	224 EXECUTE	FN Function
ESEC_USER	esec_toBase	224 EXECUTE	FN Function
ESEC_USER	esec_toDecimal	224 EXECUTE	FN Function
ESEC_USER	esec_toIpChar	224 EXECUTE	FN Function
ESEC_USER	esec_toIpNum	224 EXECUTE	FN Function
ESEC_USER	getAlertId	224 EXECUTE	FN Function
ESEC_USER	getCve	224 EXECUTE	FN Function
ESEC_USER	isArchived	224 EXECUTE	FN Function
ESEC_USER	getArchSeq	224 EXECUTE	FN Function
ESEC_USER	fn_hex_to_char	224 EXECUTE	FN Function
ESEC_USER	esec_get_next_partition_name	224 EXECUTE	FN Function
ESEC_USER	isSQL2005	224 EXECUTE	FN Function
ESEC_USER	EVENTS	193 SELECT	V View
ESEC_USER	EVENTS_ALL_RPT_V	193 SELECT	V View
ESEC_USER	EVENTS_ALL_RPT_V1	193 SELECT	V View
ESEC_USER	EVENTS_ALL_V	193 SELECT	V View
ESEC_USER	EVENTS_RPT_V	193 SELECT	V View
ESEC_USER	EVENTS_RPT_V1	193 SELECT	V View
ESEC_USER	EVENTS_RPT_V2	193 SELECT	V View

Role Name	Object Name	Action	Type
ESEC_USER	EVT_AGENT_RPT_V	193 SELECT	V View
ESEC_USER	EVT_ASSET_RPT_V	193 SELECT	V View
ESEC_USER	EVT_DEST_EVT_NAME_SMRY_1	193 SELECT	V View
ESEC_USER	EVT_DEST_EVT_NAME_SMRY_1_RPT_V	193 SELECT	V View
ESEC_USER	EVT_DEST_SMRY_1	193 SELECT	V View
ESEC_USER	EVT_DEST_SMRY_1_RPT_V	193 SELECT	V View
ESEC_USER	EVT_DEST_TXNMY_SMRY_1	193 SELECT	V View
ESEC_USER	EVT_DEST_TXNMY_SMRY_1_RPT_V	193 SELECT	V View
ESEC_USER	EVT_NAME_RPT_V	193 SELECT	V View
ESEC_USER	EVT_PORT_SMRY_1	193 SELECT	V View
ESEC_USER	EVT_PORT_SMRY_1_RPT_V	193 SELECT	V View
ESEC_USER	EVT_PRTCL_RPT_V	193 SELECT	V View
ESEC_USER	EVT_RSRC_RPT_V	193 SELECT	V View
ESEC_USER	EVT_SEV_SMRY_1	193 SELECT	V View
ESEC_USER	EVT_SEV_SMRY_1_RPT_V	193 SELECT	V View
ESEC_USER	EVT_SRC_SMRY_1	193 SELECT	V View
ESEC_USER	EVT_SRC_SMRY_1_RPT_V	193 SELECT	V View
ESEC_USER	EVT_TXNMY_RPT_V	193 SELECT	V View
ESEC_USER	EVT_USR_RPT_V	193 SELECT	V View
ESEC_USER	EXTERNAL_DATA_RPT_V	193 SELECT	V View
ESEC_USER	HIST_CORRELATED_EVENTS	193 SELECT	V View
ESEC_USER	HIST_CORRELATED_EVENTS_RPT_V	193 SELECT	V View
ESEC_USER	HIST_EVENTS	193 SELECT	V View
ESEC_USER	HIST_EVENTS_RPT_V	193 SELECT	V View
ESEC_USER	HIST_EVT_DEST_EVT_NAME_SMRY_1	193 SELECT	V View
ESEC_USER	HIST_EVT_DEST_SMRY_1	193 SELECT	V View
ESEC_USER	HIST_EVT_DEST_TXNMY_SMRY_1	193 SELECT	V View
ESEC_USER	HIST_EVT_PORT_SMRY_1	193 SELECT	V View
ESEC_USER	HIST_EVT_SEV_SMRY_1	193 SELECT	V View
ESEC_USER	HIST_EVT_SRC_SMRY_1	193 SELECT	V View
ESEC_USER	IMAGES_RPT_V	193 SELECT	V View
ESEC_USER	INCIDENTS_ASSETS_RPT_V	193 SELECT	V View

Role Name	Object Name	Action	Type
ESEC_USER	INCIDENTS_EVENTS_RPT_V	193 SELECT	V View
ESEC_USER	INCIDENTS_RPT_V	193 SELECT	V View
ESEC_USER	INCIDENTS_VULN_RPT_V	193 SELECT	V View
ESEC_USER	L_STAT_RPT_V	193 SELECT	V View
ESEC_USER	LOGS_RPT_V	193 SELECT	V View
ESEC_USER	MSSP_ASSOCIATIONS_V	193 SELECT	V View
ESEC_USER	NETWORK_IDENTITY_RPT_V	193 SELECT	V View
ESEC_USER	ORGANIZATION_RPT_V	193 SELECT	V View
ESEC_USER	PERSON_RPT_V	193 SELECT	V View
ESEC_USER	PHYSICAL_ASSET_RPT_V	193 SELECT	V View
ESEC_USER	PRODUCT_RPT_V	193 SELECT	V View
ESEC_USER	ROLE_RPT_V	193 SELECT	V View
ESEC_USER	RPT_LABELS_RPT_V	193 SELECT	V View
ESEC_USER	SENSITIVITY_RPT_V	193 SELECT	V View
ESEC_USER	STATES_RPT_V	193 SELECT	V View
ESEC_USER	UNASSIGNED_INCIDENTS_RPT_V	193 SELECT	V View
ESEC_USER	USERS_RPT_V	193 SELECT	V View
ESEC_USER	VENDOR_RPT_V	193 SELECT	V View
ESEC_USER	VULN_CALC_SEVERITY_RPT_V	193 SELECT	V View
ESEC_USER	VULN_CODE_RPT_V	193 SELECT	V View
ESEC_USER	VULN_INFO_RPT_V	193 SELECT	V View
ESEC_USER	VULN_RPT_V	193 SELECT	V View
ESEC_USER	VULN_RSRC_RPT_V	193 SELECT	V View
ESEC_USER	VULN_RSRC_SCAN_RPT_V	193 SELECT	V View
ESEC_USER	VULN_SCAN_RPT_V	193 SELECT	V View
ESEC_USER	VULN_SCAN_VULN_RPT_V	193 SELECT	V View
ESEC_USER	VULN_SCANNER_RPT_V	193 SELECT	V View

D.4 Sentinel Server Roles

Table D-9 *Sentinel Server Roles*

Server Role	Description	Sentinel User
sysadmin	System Administrators	esecdba
securityadmin	Security Administrators	esecapp
serveradmin	Server Administrators	esecdba
setupadmin	Setup Administrators	
processadmin	Process Administrators	
diskadmin	Disk Administrators	
dbcreator	Database Creators	
bulkadmin	Bulk Insert Administrators	

D.5 Windows Domain Authentication DB users and permissions

A domain user will be associated with esecadm, esecapp, esecdba and esecrpt user according to the configuration at install time. Those domain users will have the same privilege as specified by the previous sections.

NOTE: The installer takes care of the database user permissions

Sentinel Log Locations

E

The purpose of this document is to provide information of the log file locations for the following components of Sentinel.

- Sentinel Data Manager
- iTRAC
- Advisor
- Event Insertion
- Database Queries
- Active ViewsAggregation
- Wrapper (formerly Sentinel Watchdog)
- Collector Manager
- Correlation
- Sentinel Control Center
- DAS Proxy

The naming convention for the log files is that they include with the name of the process, the instance number (almost always 0 unless there are multiple instances of das_binary installed), and the log number in the log rotation sequence. For examples, see below.

E.1 Sentinel Data Manager

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

For Windows:

```
%ESEC_HOME%\log\SDM0.*.log
```

For UNIX:

```
$ESEC_HOME/log/SDM0.*.log
```

E.2 iTRAC

Logs activities related to iTRAC.

For Windows:

```
%ESEC_HOME%\log\das_itrac0.*.log
%ESEC_HOME%\log\itrac_engine.log
```

For UNIX:

```
$ESEC_HOME/log/das_itrac0.*.log
$ESEC_HOME/log/itrac_engine.log
```

E.3 Advisor

Logs activities related to Advisor data download and process.

For Windows:

```
%ESEC_HOME%\log\advisor_script.log
%ESEC_HOME%\log\advisor0.*.log
```

For UNIX:

```
$ESEC_HOME/log/advisor_script.log
$ESEC_HOME/log/advisor0.*.log
```

E.4 Event Insertion

Logs activities related to event insertion into the database.

For Windows:

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

For UNIX:

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

E.5 Database Queries

Logs activities related to database queries, Collector, Collector Manager health, identity insertion, and all other DAS activities not performed by other DAS components.

For Windows:

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

For UNIX:

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

E.6 Active Views

Logs activities related to Active Views.

For Windows:

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

For UNIX:

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

E.7 Aggregation

Logs activities related to Aggregation.

For Windows:

```
%ESEC_HOME%\log\das_aggregation0.*.log
```

For UNIX:

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

E.8 Wrapper

Logs activities related to Wrapper.

NOTE: `sentinel_wrapper.log` is for the service wrapper.

For Windows:

```
%ESEC_HOME%\log\sentinel0.*.log
%ESEC_HOME%\log\sentinel_wrapper.log
```

For UNIX:

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

E.9 Collector Manager

Logs activities related to Collector Manager.

For Windows:

```
%ESEC_HOME%\log\collector_mgr0.*.log
```

For UNIX:

```
$ESEC_HOME/log/collector_mgr0.*.log
```

E.10 Correlation Engine

Logs activities related to Correlation Engine.

For Windows:

```
%ESEC_HOME%\log\correlation_engine0.*.log
```

For UNIX:

```
$ESEC_HOME/log/correlation_engine0.*.log
```

E.11 Sentinel Control Center

Logs activities related to the Sentinel Control Center.

For Windows:

```
%ESEC_HOME%\log\control_center0.*.log
```

For UNIX:

```
$ESEC_HOME/log/control_center0.*.log
```

E.12 DAS Proxy

Logs activities related to Proxy Communication.

For Windows:

```
%ESEC_HOME%\log\das_proxy0.*.log
```

For UNIX:

```
$ESEC_HOME/log/das_proxy0.*.log
```

E.13 Solution Designer

Logs activities related to Solution Designer.

For Windows:

```
%ESEC_HOME%\log\solution_designer0.*.log
```

For UNIX:

```
$ESEC_HOME/log/solution_designer0.*.log
```

E.14 Multiple Instances

In some environments, there can be multiple instances of a process running, such as DAS Binary, the Sentinel Control Center, or Sentinel Data Manager. If so, the first instance's log files are named as described above (For example, das_binary0.0.log). The second instance will substitute a 1 for the first 0 in the log file name (For example, das_binary1.0.log).

If other processes have log files indicating that more than one instance is running, that could indicate a system problem.

Documentation Updates

F

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

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

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

This document was updated on the following dates:

- Section F.1, "March 2009," on page 233

F.1 March 2009

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

Table F-1 *Updates*

Location	Description
"Third-Party Materials" on page 3	Removed references to Third-Party guides. Fixed Bug#455535 (https://bugzilla.novell.com/show_bug.cgi?id=455535)
Section 2.2, "List of Fields and Representations," on page 23	Added missing fields and representations to Table 2-1 on page 24.