

Guide

Novell[®] Identity Audit

1.0

October 27, 2008

www.novell.com



Legal Notices

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

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

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

Copyright © 2008 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc., 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 \(http://www.novell.com/company/legal/patents/\)](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 \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

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

Third-Party Materials

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

Contents

About This Guide	11
1 Introduction	13
1.1 Product Overview	13
1.1.1 Comparison to Novell Audit 2.0.2	13
1.1.2 Comparison to Novell Sentinel	14
1.2 Interface	14
1.3 Architecture	15
2 System Requirements	17
2.1 Hardware Requirements	17
2.2 Supported Operating Systems	18
2.3 Supported Browsers	18
2.4 Supported Platform Agent Version	18
2.5 Supported Event Sources	18
3 Installation	19
3.1 Prerequisites	19
3.2 Installing Novell Identity Audit	19
3.2.1 Quick Installation (as root)	19
3.2.2 Non-root Installation	21
3.3 Configuring Event Sources	23
3.3.1 Installing the Platform Agent	23
3.3.2 Configuring the Platform Agent	24
3.3.3 Configuring the Auditing Level	25
3.4 Logging In to Identity Audit	25
3.5 Uninstalling	25
4 Reporting	27
4.1 Running Reports	27
4.1.1 Manually Running a Report	27
4.1.2 Scheduling a Report	29
4.2 Viewing Reports	30
4.3 Managing Reports	31
4.3.1 Adding Reports	32
4.3.2 Creating New Reports	33
4.3.3 Renaming Report Results	33
4.3.4 Deleting Reports	34
4.3.5 Updating Report Definitions	34
4.4 Default Reports	34
5 Data Collection	37
5.1 Data Collection Status	37
5.1.1 Enabling and Disabling Data Collection	37

5.1.2	Viewing Audit Server Health	38
5.1.3	Viewing Event Source Health	39
5.2	Managing Event Sources	40
5.2.1	Adding Event Sources	40
5.2.2	Deleting Event Sources	40
5.3	Audit Server Options	40
5.3.1	Port Configuration and Port Forwarding	42
5.3.2	Client Authentication	42
5.4	Event Sources	45
6	Searching	47
6.1	Running an Event Search	47
6.1.1	Basic Search	47
6.1.2	Advanced Search	48
6.2	Viewing Search Results	49
6.2.1	Basic Event View	50
6.2.2	Event View with Details	50
6.2.3	Refining Search Results	51
6.3	Event Fields	52
7	Data Storage	57
7.1	Database Health	57
7.2	Data Storage Configuration	58
7.3	Database Setup	59
7.3.1	Database Structure	60
7.3.2	Database Users	60
7.3.3	Database Stored Procedures	60
8	Rules	61
8.1	Rules Overview	61
8.2	Configuring Rules	62
8.2.1	Filter Criteria	62
8.2.2	Adding a Rule	62
8.2.3	Ordering Rules	63
8.2.4	Editing a Rule	63
8.2.5	Deleting a Rule	63
8.2.6	Activating or Deactivating a Rule	63
8.3	Configuring Actions	64
8.3.1	Send to E-Mail	64
8.3.2	Send to Syslog	65
8.3.3	Write to File	65
9	User Administration	67
9.1	Adding a User	67
9.2	Editing User Details	68
9.2.1	Editing Your Own Profile	68
9.2.2	Changing Your Own Password	69
9.2.3	Editing Another User's Profile (admin only)	70
9.2.4	Resetting Another User's Password (admin only)	70
9.3	Deleting a User	70

A	Troubleshooting	71
B	Truststore	73
B.1	Creating a Keystore	73
C	Novell Identity Audit Database Views for PostgreSQL Server	75
C.1	Views	75
C.1.1	ACTVY_PARM_RPT_V	75
C.1.2	ACTVY_REF_PARM_VAL_RPT_V	75
C.1.3	ACTVY_REF_RPT_V	76
C.1.4	ACTVY_RPT_V	76
C.1.5	ADV_ATTACK_MAP_RPT_V	77
C.1.6	ADV_ATTACK_PLUGIN_RPT_V	77
C.1.7	ADV_ATTACK_RPT_V	77
C.1.8	ADV_ATTACK_SIGNATURES	78
C.1.9	ADV_FEED_RPT_V	79
C.1.10	ADV_MASTER_RPT_V	79
C.1.11	ADV_PRODUCT_RPT_V	80
C.1.12	ADV_PRODUCT_SERVICE_PACK_RPT_V	80
C.1.13	ADV_PRODUCT_VERSION_RPT_V	81
C.1.14	ADV_VENDOR_RPT_V	81
C.1.15	ADV_VULN_KB_RPT_V	82
C.1.16	ADV_VULN_PRODUCT_RPT_V	83
C.1.17	ADV_VULN_SIGNATURES	83
C.1.18	ANNOTATIONS_RPT_V	83
C.1.19	ASSET_CATEGORY_RPT_V	84
C.1.20	ASSET_HOSTNAME_RPT_V	84
C.1.21	ASSET_IP_RPT_V	84
C.1.22	ASSET_LOCATION_RPT_V	85
C.1.23	ASSET_RPT_V	85
C.1.24	ASSET_VALUE_RPT_V	86
C.1.25	ASSET_X_ENTITY_X_ROLE_RPT_V	86
C.1.26	ASSOCIATIONS_RPT_V	87
C.1.27	ATTACHMENTS_RPT_V	87
C.1.28	AUDIT_RECORD_RPT_V	88
C.1.29	CONFIGS_RPT_V	88
C.1.30	CONTACTS_RPT_V	89
C.1.31	CORRELATED_EVENTS_RPT_V (legacy view)	89
C.1.32	CORRELATED_EVENTS_RPT_V1	89
C.1.33	CRITICALITY_RPT_V	90
C.1.34	CUST_HIERARCHY_V	90
C.1.35	CUST_RPT_V	91
C.1.36	ENTITY_TYPE_RPT_V	91
C.1.37	ENV_IDENTITY_RPT_V	91
C.1.38	ESEC_CONTENT_GRP_CONTENT_RPT_V	92
C.1.39	ESEC_CONTENT_GRP_RPT_V	92
C.1.40	ESEC_CONTENT_PACK_RPT_V	93
C.1.41	ESEC_CONTENT_RPT_V	93
C.1.42	ESEC_CTRL_CTGRY_RPT_V	93
C.1.43	ESEC_CTRL_RPT_V	94
C.1.44	ESEC_DISPLAY_RPT_V	94
C.1.45	ESEC_PORT_REFERENCE_RPT_V	95
C.1.46	ESEC_PROTOCOL_REFERENCE_RPT_V	96
C.1.47	ESEC_SEQUENCE_RPT_V	96
C.1.48	ESEC_UUID_UUID_ASSOC_RPT_V	97
C.1.49	EVENTS_ALL_RPT_V (legacy view)	97

C.1.50	EVENTS_ALL_RPT_V1 (legacy view)	97
C.1.51	EVENTS_ALL_V (legacy view)	97
C.1.52	EVENTS_RPT_V (legacy view)	97
C.1.53	EVENTS_RPT_V1 (legacy view)	97
C.1.54	EVENTS_RPT_V2	97
C.1.55	EVENTS_RPT_V3	102
C.1.56	EVT_AGENT_RPT_V	105
C.1.57	EVT_AGENT_RPT_V3	106
C.1.58	EVT_ASSET_RPT_V	106
C.1.59	EVT_ASSET_RPT_V3	107
C.1.60	EVT_DEST_EVT_NAME_SMRY_1_RPT_V	108
C.1.61	EVT_DEST_SMRY_1_RPT_V	108
C.1.62	EVT_DEST_TXNMY_SMRY_1_RPT_V	109
C.1.63	EVT_NAME_RPT_V	110
C.1.64	EVT_PORT_SMRY_1	110
C.1.65	EVT_PORT_SMRY_1_RPT_V	110
C.1.66	EVT_PRTCL_RPT_V	111
C.1.67	EVT_RSRC_RPT_V	111
C.1.68	EVT_SEV_SMRY_1_RPT_V	111
C.1.69	EVT_SRC_COLLECTOR_RPT_V	112
C.1.70	EVT_SRC_GRP_RPT_V	112
C.1.71	EVT_SRC_MGR_RPT_V	113
C.1.72	EVT_SRC_OFFSET_RPT_V	113
C.1.73	EVT_SRC_RPT_V	114
C.1.74	EVT_SRC_SMRY_1_RPT_V	114
C.1.75	EVT_SRC_SRV_RPT_V	115
C.1.76	EVT_TXNMY_RPT_V	115
C.1.77	EVT_USR_RPT_V	116
C.1.78	EVT_XDAS_TXNMY_RPT_V	116
C.1.79	EXTERNAL_DATA_RPT_V	117
C.1.80	HIST_CORRELATED_EVENTS	117
C.1.81	HIST_CORRELATED_EVENTS_RPT_V (legacy view)	118
C.1.82	HIST_EVENTS	118
C.1.83	HIST_EVENTS_RPT_V (legacy view)	120
C.1.84	IMAGES_RPT_V	120
C.1.85	INCIDENTS_ASSETS_RPT_V	121
C.1.86	INCIDENTS_EVENTS_RPT_V	121
C.1.87	INCIDENTS_RPT_V	122
C.1.88	INCIDENTS_VULN_RPT_V	122
C.1.89	L_STAT_RPT_V	123
C.1.90	LOGS_RPT_V	123
C.1.91	MSSP_ASSOCIATIONS_V	123
C.1.92	NETWORK_IDENTITY_RPT_V	124
C.1.93	ORGANIZATION_RPT_V	124
C.1.94	PERSON_RPT_V	124
C.1.95	PHYSICAL_ASSET_RPT_V	125
C.1.96	PRODUCT_RPT_V	125
C.1.97	ROLE_RPT_V	126
C.1.98	RPT_LABELS_RPT_V	126
C.1.99	SENSITIVITY_RPT_V	126
C.1.100	SENTINEL_HOST_RPT_V	127
C.1.101	SENTINEL_PLUGIN_RPT_V	127
C.1.102	SENTINEL_RPT_V	127
C.1.103	STATES_RPT_V	128
C.1.104	UNASSIGNED_INCIDENTS_RPT_V	128
C.1.105	USERS_RPT_V	129
C.1.106	USR_ACCOUNT_RPT_V	130
C.1.107	USR_IDENTITY_EXT_ATTR_RPT_V	130
C.1.108	USR_IDENTITY_RPT_V	130

C.1.109	VENDOR_RPT_V	131
C.1.110	VULN_CALC_SEVERITY_RPT_V	131
C.1.111	VULN_CODE_RPT_V	132
C.1.112	VULN_INFO_RPT_V	132
C.1.113	VULN_RPT_V	133
C.1.114	VULN_RSRC_RPT_V	134
C.1.115	VULN_RSRC_SCAN_RPT_V	134
C.1.116	VULN_SCAN_RPT_V	134
C.1.117	VULN_SCAN_VULN_RPT_V	135
C.1.118	VULN_SCANNER_RPT_V	135
C.1.119	WORKFLOW_DEF_RPT_V	136
C.1.120	WORKFLOW_INFO_RPT_V	136
C.2	Deprecated Views	136

D Documentation Updates 139

D.1	October 2009	139
-----	--------------------	-----

About This Guide

This guide covers the installation and configuration of Novell® Identity Audit.

- ♦ Chapter 1, “Introduction,” on page 13
- ♦ Chapter 2, “System Requirements,” on page 17
- ♦ Chapter 3, “Installation,” on page 19
- ♦ Chapter 6, “Searching,” on page 47
- ♦ Chapter 4, “Reporting,” on page 27
- ♦ Chapter 5, “Data Collection,” on page 37
- ♦ Chapter 7, “Data Storage,” on page 57
- ♦ Chapter 8, “Rules,” on page 61
- ♦ Chapter 9, “User Administration,” on page 67
- ♦ Appendix A, “Troubleshooting,” on page 71
- ♦ Appendix B, “Truststore,” on page 73
- ♦ Appendix C, “Novell Identity Audit Database Views for PostgreSQL Server,” on page 75
- ♦ Appendix D, “Documentation Updates,” on page 139

Audience

This guide is intended for Novell Identity Audit administrators and end users.

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, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of the *Novell Identity Audit 1.0 Guide*, visit the [Identity Audit documentation Web site](http://www.novell.com/documentation/identityaudit) (<http://www.novell.com/documentation/identityaudit>).

Additional Documentation and Support

To download additional plug-ins (for example, reports), go to the [Identity Audit Content Web page](http://support.novell.com/products/sentinel/secure/identityaudit.html) (<http://support.novell.com/products/sentinel/secure/identityaudit.html>).

For more information about building your own plug-ins (for example, Jasper Reports*), go to the [Sentinel™ SDK Web page](http://developer.novell.com/wiki/index.php/Develop_to_Sentinel) (http://developer.novell.com/wiki/index.php/Develop_to_Sentinel). The build environment for Identity Audit report plug-ins is identical to what is documented for Novell Sentinel.

Documentation Conventions

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

Introduction

1

Novell® Identity Audit provides event reporting and monitoring for the Novell Identity and Security Management environment, including Novell eDirectory™, Novell Identity Manager, Novell Access Manager, Novell Modular Authentication Services (NMAS™), Novell SecureLogin, and Novell SecretStore®.

- ♦ [Section 1.1, “Product Overview,” on page 13](#)
- ♦ [Section 1.2, “Interface,” on page 14](#)
- ♦ [Section 1.3, “Architecture,” on page 15](#)

1.1 Product Overview

Novell Identity Audit 1.0 is an easy to use, lightweight tool for collecting, aggregating, and storing events from Novell Identity Manager, Novell Access Manager, Novell eDirectory, and other Novell identity and security products and technologies. Key features include:

- ♦ Web-based administration and reporting interfaces
- ♦ Full-event search tool allows searches across multiple event fields
- ♦ Selected event output to several channels
- ♦ Embedded JasperReports engine allows the use of open source tools for customizing included reports or creating new reports
- ♦ Built-in database eliminates the need for external database licenses or administration
- ♦ Simple, intuitive data management tools

Novell Identity Audit is a replacement for Novell Audit and is related to Novell Sentinel™, but there are significant differences.

- ♦ [Section 1.1.1, “Comparison to Novell Audit 2.0.2,” on page 13](#)
- ♦ [Section 1.1.2, “Comparison to Novell Sentinel,” on page 14](#)

1.1.1 Comparison to Novell Audit 2.0.2

Novell Identity Audit 1.0 is designed as a replacement product for the Novell Audit product line, which leaves general support in February 2009. Identity Audit is comparable in functionality, but with major improvements in architecture, reporting, and data management. Novell Identity Audit 1.0 is a drop-in replacement for the Novell Audit 2.0.2 Secure Logging Server for products in the Novell Identity and Security product line. Because Novell Identity Audit uses a new embedded database, customers should keep existing Novell Audit events in the archived Novell Audit database rather than attempting to migrate legacy data.

The Novell Audit client component, also known as the Platform Agent, is still used as the data transport mechanism for Novell Identity Audit. This will continue to be supported according to the life cycles of Novell Identity and Access Management products that still use the Platform Agent.

1.1.2 Comparison to Novell Sentinel

Novell Identity Audit is built on a robust technological foundation, because much of the underlying code is shared with Novell Sentinel. However, Sentinel collects data from a broader range of devices, supports a higher event rate, and provides more tools than Novell Identity Audit. Sentinel provides additional Security Information and Event Management (SIEM) features, such as real-time dashboards, multi-event correlation, incident tracking and automated remediation, and data collection from non-Novell products. Identity Audit is designed to integrate into a future Sentinel deployment.

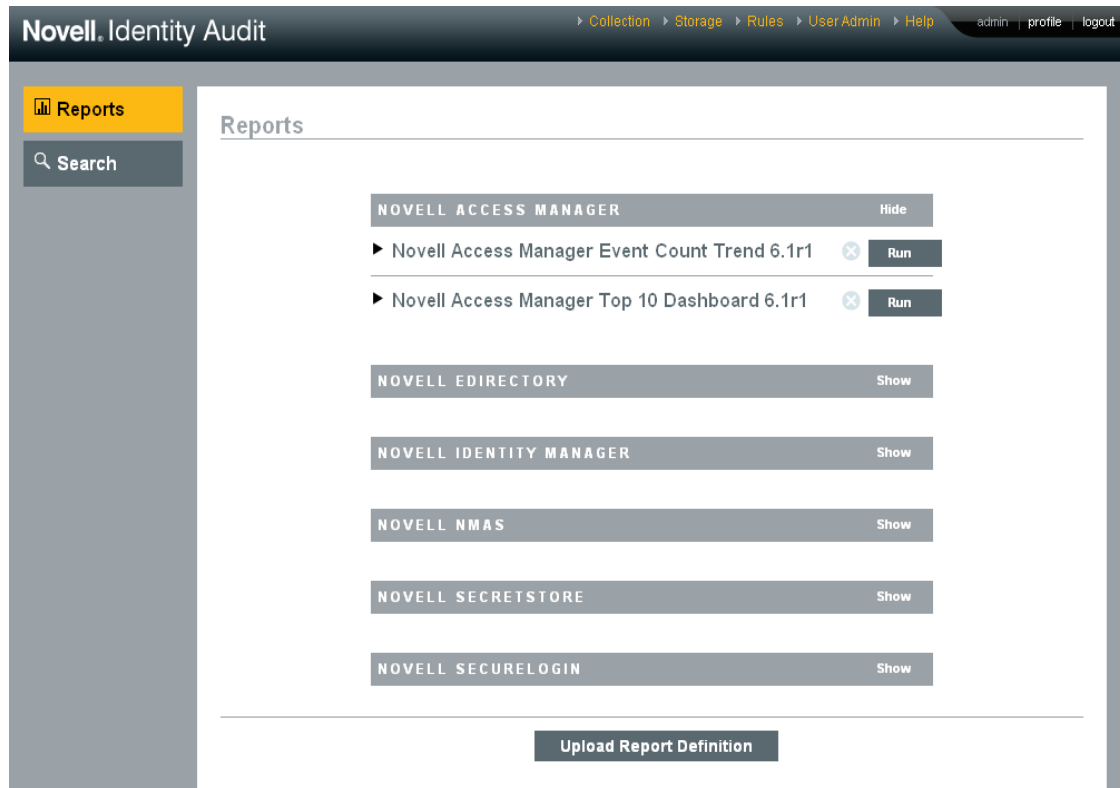
Novell Identity Audit 1.0 is not part of the Novell Compliance Management Platform (CMP) and does not include the advanced identity and security integration features delivered in that platform. Sentinel 6.1 is presently the identity audit and monitoring component of the CMP.

1.2 Interface

The Novell Identity Audit Web interface provides the ability to perform the following tasks:

- ◆ Upload, run, view, and delete reports
- ◆ Search for events
- ◆ Edit user profile details
- ◆ Create, edit, and delete users and assign administrative rights (administrators only)
- ◆ Configure data collection and view the health of event sources (administrator only)
- ◆ Configure data storage and view the health of the database (administrators only)
- ◆ Create filtering rules and configure associated actions to send matching event data to output channels (administrators only)

Figure 1-1 Novell Identity Audit interface (Administrator View)



The Identity Audit pages automatically refresh every 30 seconds to show updates by other users, if applicable.

The interface is available in multiple languages (English, French, German, Italian, Japanese, Portuguese, Spanish, Simplified Chinese, and Traditional Chinese). It defaults to the browser's default language, but users can select another language at login.

NOTE: Although the interface is localized into double-byte languages, the current release of Identity Audit does not process double-byte event data.

1.3 Architecture

Identity Audit collects data from multiple Novell identity and security applications. These application servers are configured to generate event records, and each hosts a Platform Agent. Event data is forwarded by the Platform Agent to an Audit Connector that resides on the Identity Audit Server.

The Audit Connector passes events to the Data Collection component, which parses the events and puts them on the Communication Bus, which is the backbone of the system and brokers most communication between components. As part of Data Collection, incoming events are evaluated by a set of filtering rules. These rules filter events and send them to output channels such as a file, a syslog relay, or an SMTP relay.

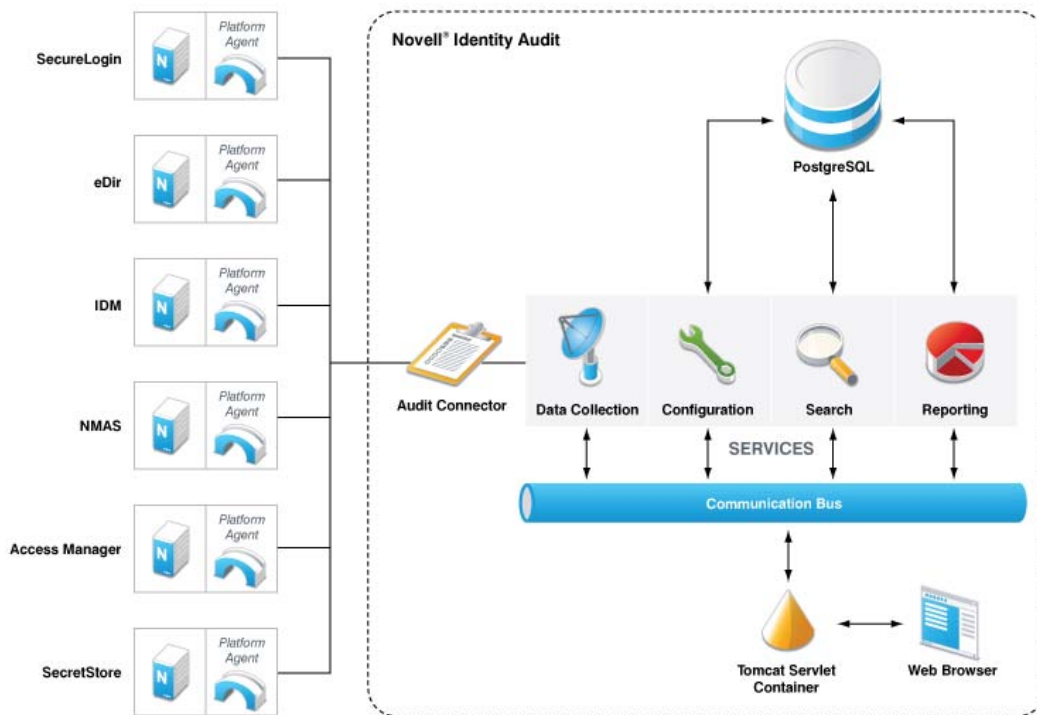
In addition, all events are stored in the Identity Audit database (powered by PostgreSQL*), in partitioned tables.

The Configuration component retrieves, adds, and modifies configuration information such as data collection and storage settings, rule definitions, and report definitions. It also manages user authentication.

The Search component performs fast, indexed searches and retrieves events from the database to present search result sets to the user.

The Reporting component runs reports and formats report results.

Figure 1-2 Architecture for Identity Audit



Users interact with the Identity Audit server and all of its functionality via a Web browser, which connects to an Apache* Tomcat Web server. The Web server makes calls to the various Identity Audit components via the Communications Bus.

System Requirements

2

In addition to the hardware, operating system, browser, and event source compatibility requirements described below, the user must also have root access for some installation steps.

- ♦ [Section 2.1, “Hardware Requirements,” on page 17](#)
- ♦ [Section 2.2, “Supported Operating Systems,” on page 18](#)
- ♦ [Section 2.3, “Supported Browsers,” on page 18](#)
- ♦ [Section 2.4, “Supported Platform Agent Version,” on page 18](#)
- ♦ [Section 2.5, “Supported Event Sources,” on page 18](#)

2.1 Hardware Requirements

Novell Identity Audit is supported on 64-bits intel Xeon* and AMD Opteron* hardware. It is not supported on Itanium* hardware. Novell recommends the following hardware for a production system that holds 90 days of online data:

- ♦ 1x Quad Core (x86-64)
- ♦ 16 GB RAM
- ♦ 1.5 TB usable disk space - 3x 500GB (3 usable), 10K RPM drives in a hardware RAID configuration
 - ♦ Approximately 2/3 of the usable disk space is used for database files
 - ♦ Approximately 1/3 of the usable disk space is used for the search index and temp files
 - ♦ A small amount of storage is available for archived data that has been removed from the database, but Novell recommends that you move archived data files from the Identity Audit server to a long-term storage location.

Table 2-1 Performance

Metric	Value	Description
Events per second (eps) - steady state	100	Average event rate during normal operations
Events per second (eps) - peak	500	Peak event rate during a spike (up to 10 minutes)
Events per second (eps) - peak per application	300	Peak event rate from each type of Novell application <ul style="list-style-type: none">♦ Event rates are typically low (less than 15 eps) for Identity Manager, SecureLogin, SecretStore®, and NMASTM)♦ Event rates can be very high from eDirectoryTM and Access Manager. Event filtering should be implemented to ensure a manageable rate.♦ Even during an event spike, no one application can send more than this many events per second.

Metric	Value	Description
Online data	90 days or 750 million events	Amount of data Identity Audit can store at a steady state rate of approximately 100 eps, with the recommended storage

2.2 Supported Operating Systems

Identity Audit is certified to run on 64-bits SUSE Linux Enterprise Server 10 SP1 and SP2.

NOTE: Identity Audit is not supported on Novell Open Enterprise Server 2.

2.3 Supported Browsers

The following browsers are supported by Identity Audit. Other browsers may not display information as expected.

- ♦ Mozilla* Firefox* 2
- ♦ Mozilla Firefox 3
- ♦ Microsoft* internet Explorer* 7

The performance of searches and report viewing seems to vary by browser. Novell has observed particularly good performance from Mozilla Firefox 3.

2.4 Supported Platform Agent Version

Identity Audit 1.0 supports collecting log events from many applications that were supported by Novell Audit and its Platform Agent. Platform Agent version 2.0.2 SP6 or above is required for Identity Audit.

NOTE: Some Novell applications are bundled with a previous version of the Platform Agent. The recommended version includes important bug fixes, so you should upgrade the Platform Agent if you have a previous version.

2.5 Supported Event Sources

Identity Audit supports collecting data from the Novell identity and security applications. Some applications require a specific patch level in order to collect data correctly.

- ♦ Novell Access Manager 3.0
- ♦ Novell eDirectory 8.8.3 with the eDirectory instrumentation patch found on the [Novell Support Web Site \(http://download.novell.com/Download?buildid=RH_B5b3M6EQ~\)](http://download.novell.com/Download?buildid=RH_B5b3M6EQ~)
- ♦ Novell Identity Manager 3.6
- ♦ Novell NMAS 3.1
- ♦ Novell SecretStore 3.4
- ♦ Novell SecureLogin 6.0

This section describes how to install Novell® Identity Audit and configure the event sources to send data to it. These instructions assume that the minimum requirements for each system component have been met. For more information, see [Chapter 2, “System Requirements,” on page 17](#).

- ♦ [Section 3.1, “Prerequisites,” on page 19](#)
- ♦ [Section 3.2, “Installing Novell Identity Audit,” on page 19](#)
- ♦ [Section 3.3, “Configuring Event Sources,” on page 23](#)
- ♦ [Section 3.4, “Logging In to Identity Audit,” on page 25](#)
- ♦ [Section 3.5, “Uninstalling,” on page 25](#)

3.1 Prerequisites

Before installing Identity Audit, be sure you meet the system requirements in [Chapter 2, “System Requirements,” on page 17](#). In particular, you need to have the supported patch levels for some Novell applications in order to receive high-quality events from those event sources.

3.2 Installing Novell Identity Audit

The Identity Audit installation package installs everything you need to run Identity Audit: the Identity Audit application and communications bus, the database to store events and configuration information, the Web-based user interface, and the reporting server. There are two installation options, a simple installation that can be run as `root`, or a multi-step installation that uses `root` as little as possible.

3.2.1 Quick Installation (as root)

This simple installation must be run as `root`.

- 1 Log in as `root` to the server where you want to install Identity Audit.
- 2 Download or copy `identity_audit_1.0_x86-64.tar.gz` to a temporary directory.
- 3 Change to the temporary directory (if necessary).

- 4 Extract the install script from the file by using the following command:

```
tar xfz identity_audit_1.0_x86-64.tar.gz identity_audit_1.0_x86-64/setup
```

- 5 Run the `root_install_all.sh` script with `root` privileges.

```
identity_audit_1.0_x86-64/setup/root_install_all.sh
identity_audit_1.0_x86-64.tar.gz
```

NOTE: You can log in as `root` and run the command above or use the `sudo` command to run the command.

- 6 Choose a language by entering a number.

The end user license agreement displays in the selected language.

- 7 Read the end user license and enter 1 or y if you agree to the terms and want to continue installation.

The installation begins. If the previously selected language is not available for the installer (for example, Polish), the installer continues in English.

```
Creating group novell ...
Creating user novell ...
Creating installation directory /opt/novell ...
Extracting files...
Starting the installation of the software...

Updating novell's environment...
Adding /opt/novell/identity_audit_1.0_x86-64/bin to PATH...

Generating web server certs ...

Generating jms broker certs ...

Generating jms client certs ...
^P
Generating postgresql server certs ...
Generating a 1024 bit RSA private key
.....++++++
.,++++++
writing new private key to '/opt/novell/identity_audit_1.0_x86-64/3rdparty/postg
resql/data/privkey.pem'
```

The novell user and novell group are created, if they do not already exist.

The novell user is created without a password. If you want to be able to log in as the novell user later (for example, to install patches), you can create a password for this user after the installation is completed.

- 8 Enter the password for database administrator (dbauser).
- 9 Confirm the password for database administrator (dbauser).
- 10 Enter the password for the admin user.
- 11 Confirm the password for the admin user.

```

What should the 'dbauser' password be set to? =>
Confirm Password =>
What should the 'admin' password be set to? =>
Confirm Password =>
Setting the new passwords in the database and configuration files...
Adding initial partitions to database...

Starting Identity Audit...

Point your web browser to https:// sles10server :8443/novellidentityaudit to start
using this software.
Username: admin
Password: <use the password you entered above>
This URL may take a short time to become available as the server starts up.
To see if the service is listening, use the following command:
netstat -an | grep 'LISTEN ' | grep 8443

Done!
Starting the installation of the Identity Audit service...

Cleaning up previous installation settings (if present)...

Installing startup script in /etc/init.d ...

Configuring automatic startup at boot ...
identity_audit      0:off 1:off 2:off 3:on  4:off 5:on  6:off

Done!

```

The dbauser credentials are used to create tables and partitions in the PostgreSQL database. Identity Audit is configured to start up with runlevels 3 and 5 (Multi-User Mode with boot-up in console or X-Windows mode).

After the Identity Audit service starts, you can log in to the URL (for example: <https://10.10.10.10:8443/novellidentityaudit>) specified in the installation output. The system starts processing internal audit events immediately, and it is fully functional after you **configure event sources** to send data to Identity Audit.

3.2.2 Non-root Installation

If organizational policy prohibits running the full installation process as `root`, the installation can be run in two steps. The first part of the installation procedure must be performed with `root`-level access, and the second part is performed as the Identity Audit administrative user (created during the first part).

- 1 Log in as `root` to the server where you want to install Identity Audit.
- 2 Download or copy `identity_audit_1.0_x86-64.tar.gz` to the `/tmp` directory.
- 3 (Conditional) If the `novell` user and `novell` group do not exist on the server:
 - 3a Extract the script to create the `novell` user and `novell` group from the Identity Audit tar file. For example:

```
tar xzf identity_audit_1.0_x86-64.tar.gz identity_audit_1.0_x86-64/
setup/root_create_novell_user.sh
```

- 3b As `root`, execute the script by using this command:

```
identity_audit_1.0_x86-64/setup/root_create_novell_user.sh
```

The `novell` user and `novell` group will own the installation and the running processes of Identity Audit.

- 4 Create a directory for Identity Audit. For example:

```
mkdir -p /opt/novell
```

- 5 Set the directory to be owned by the novell user and novell group. For example:

```
chown -R novell:novell /opt/novell
```

- 6 Log in as the novell user:

```
su novell
```

- 7 Extract the Identity Audit tar file to the directory you just created. For example:

```
cd /opt/novell
tar xzf /tmp/identity_audit_1.0_x86-64.tar.gz
```

- 8 Execute the installation script. For example:

```
/opt/novell/identity_audit_1.0_x86-64/setup/install.sh
```

- 9 Choose a language by entering a number.

The end user license agreement displays in the selected language.

- 10 Read the end user license and enter `1` or `y` if you agree to the terms and want to continue installation.

The installation begins. If the previously selected language is not available for the installer (for example, Polish), the installer continues in English.

```
Starting the installation of the software...

Updating novell's environment...
Adding /opt/novell/identity_audit_1.0_x86/bin to PATH...

Generating web server certs ...

Generating jms broker certs ...

Generating jms client certs ...

Generating postgresql server certs ...
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to '/opt/novell/identity_audit_1.0_x86/3rdparty/postgres
ql/data/privkey.pem'
-----
writing RSA key
Certificate was added to keystore

What should the 'dbauser' password be set to? => █
```

- 11 Enter the password for database administrator (dbauser).
- 12 Confirm the password for database administrator (dbauser).
- 13 Enter the password for the admin user.
- 14 Confirm the password for the admin user.
- 15 Log out and log back in as novell. This loads the PATH environment variable changes made by the `install.sh` script.
- 16 Execute the `root_install_service.sh` script to enable Identity Audit to start up as a service. This step requires root level access. For example:

```
sudo /opt/novell/identity_audit_1.0_x86-64/setup/root_install_service.sh
```

```

root's password:
Starting the installation of the Identity Audit service...

Cleaning up previous installation settings (if present)...

Installing startup script in /etc/init.d ...

Configuring automatic startup at boot ...
identity_audit      0:off 1:off 2:off 3:on  4:off 5:on  6:off

Done!

```

17 Enter the `root` password.

Identity Audit is configured to start up with runlevels 3 and 5 (Multi-User Mode with boot-up in console or X-Windows mode).

After the Identity Audit service starts, you can log in to the URL (for example: `https://10.10.10.10:8443/novellidentityaudit`) specified in the installation output. The system starts processing internal audit events immediately, and it is fully functional after you configure event sources to send data to Identity Audit.

3.3 Configuring Event Sources

Identity Audit 1.0 supports collecting log events from applications that were supported by the old Novell Audit product and its Platform Agent. Before completing the steps in this section, ensure that your Novell products are supported. For more information, see [Section 2.4, “Supported Platform Agent Version,”](#) on page 18.

- ♦ The [32-bits Platform Agent](http://download.novell.com/Download?buildid=109cbsOIO8Y~) (<http://download.novell.com/Download?buildid=109cbsOIO8Y~>) can be downloaded as part of the Novell Audit product. This URL is current for Audit 2.0.2 SP6.
- ♦ The [64-bits Platform Agent](http://download.novell.com/Download?buildid=8hsF_IYQZJM~) (http://download.novell.com/Download?buildid=8hsF_IYQZJM~) can be downloaded as a standalone client. This URL is current for 2.0.2 SP6. This URL is current for Audit 2.0.2 SP6.
- ♦ [Section 3.3.1, “Installing the Platform Agent,”](#) on page 23
- ♦ [Section 3.3.2, “Configuring the Platform Agent,”](#) on page 24
- ♦ [Section 3.3.3, “Configuring the Auditing Level,”](#) on page 25

3.3.1 Installing the Platform Agent

The Platform Agent must be at least the minimum version recommended for Identity Audit. For more information, see [Section 2.4, “Supported Platform Agent Version,”](#) on page 18. The appropriate Platform Agent (32-bits or 64-bits) must be installed or updated on all event source machines.

The instructions for installing or upgrading the Platform Agent vary slightly by operating system. The sample instructions below are for a 32-bits Linux* Platform Agent.

- 1** Download the `.iso` file for the supported version of Novell Audit to the `/tmp` directory on the event source machine.
- 2** Create a directory for Audit. For example, `mkdir -p audit202`.
- 3** Log in as `root`.

- 4 Mount the Audit .iso file.

```
mount -o loop ./NAudit202.iso ./audit202
```

- 5 Go to the audit202 directory.

- 6 Go to the appropriate directory for the operating system on your event source. For example:

```
cd Linux
```

- 7 Run pinstall.lin.

```
./pinstall.lin
```

- 8 Read the license agreement and enter `y` if you are willing to accept the terms.

- 9 Enter `P` to install the Platform Agent.

- 10 Enter `Y` to keep any previous configurations to the `logevent.conf` file.

The Platform Agent is installed.

- 11 To verify that the Platform Agent version is correct, enter the following command:

```
rpm -qa | grep AUDT
```

The version of novell-AUDTplatformagent should be at least the supported version listed in [Section 2.4, “Supported Platform Agent Version,” on page 18](#).

3.3.2 Configuring the Platform Agent

After installation, the Platform Agent must be configured to send data to the Identity Audit server and, if desired, to send event signatures from the event sources.

IMPORTANT: Configuring the Platform Agent to generate signatures can negatively impact the performance of the event source machines.

To configure the Platform Agent:

- 1 Log into the event source machine.
- 2 Open the `logevent` file for editing. The file is in a different location depending on the operating system:
 - ♦ Linux: `/etc/logevent.conf`
 - ♦ Windows*: `C:\WINDOWS\logevent.cfg`
 - ♦ NetWare®: `SYS:\etc\logevent.cfg`
 - ♦ Solaris*: `/etc/logevent.conf`
- 3 Set `LogHost` to the IP address of the Identity Audit server.
- 4 Set `LogEnginePort=1289`, if this entry does not already exist.)
- 5 If you want the event source to send event signatures, enter `LogSigned=always`.
- 6 Save the file.
- 7 Restart the Platform Agent. The method varies by operating system and application. Reboot the machine or refer to the application-specific documentation on the [Novell Documentation Web Site \(http://www.novell.com/documentation\)](http://www.novell.com/documentation) for more instructions.

3.3.3 Configuring the Auditing Level

The events for which each application generates records are configured differently for each application monitored by Identity Audit. The URLs below have more information about each application.

- ♦ Access Manager (<http://www.novell.com/documentation/novellaccessmanager/adminguide/index.html?page=/documentation/novellaccessmanager/adminguide/data/b8cvd21.html#b8cvd21>)
- ♦ eDirectory (<http://www.novell.com/documentation/novellaudit20/index.html?page=/documentation/novellaudit20/novellaudit20/data/b296n3h.html>)
- ♦ Identity Manager (http://www.novell.com/documentation/idm36/idm_sentinel/data/bookinfo.html)
- ♦ NMAS (<http://www.novell.com/documentation/nmas32/admin/index.html?page=/documentation/nmas32/admin/data/ahefojr.html>)
- ♦ SecretStore (<http://www.novell.com/documentation/secretstore33/index.html?page=/documentation/secretstore33/nssadm/data/bsqjxv.htm>)
- ♦ SecureLogin (<http://www.novell.com/documentation/securelogin60/index.html>) (see the Auditing link)

3.4 Logging In to Identity Audit

The administrative user created during the install can log into the Identity Audit application and create more users, run preloaded reports, upload new reports, perform event searches, and more.

To log into Identity Audit:

- 1 Open a supported Web browser. For more information, see [Section 2.3, “Supported Browsers,” on page 18](#).
- 2 Go to the Novell Identity Audit page (for example: <https://10.10.10.10:8443/novellidentityaudit>).
- 3 If this is the first time you have logged into Identity Audit, you are presented with a certificate. You must accept it to proceed.
- 4 Enter `admin`.
- 5 Enter the admin password you configured during installation.
- 6 Select the language for the Identity Audit interface (English, Portuguese, French, Italian, German, Spanish, Japanese, Traditional Chinese, or Simplified Chinese).
- 7 Click *Login*.

3.5 Uninstalling

To fully uninstall an Identity Audit installation, you must run the uninstall script and then perform some manual cleanup steps.

- 1 Log into the Identity Audit server as `root`.
- 2 Stop the Identity Audit service:

```
/etc/init.d/identity_audit stop
```

3 Run the uninstallation script:

```
/opt/novell/identity_audit_1.0_x86-64/setup/root_uninstall_service.sh
```

4 Delete the Identity Audit home directory and its contents.

```
rm -rf /opt/novell/identity_audit_1.0_x86-64
```

The final steps depend on whether you want to retain any information related to the novell user and group.

5 (Conditional) If you do not want to retain any information related to the novell user, run the following command to remove the user, its home directory, and the group:

```
userdel -r novell && groupdel novell
```

6 (Conditional) If you do want to retain the novell user and its home directory but want to remove all Identity-Audit-related settings:

6a Remove the following environment variable entries for Identity Audit from the novell user's profile (in `~novell/.bashrc`):

```
APP_HOME=/opt/novell/identity_audit_1.0_x86-64
export PATH=$APP_HOME/bin:$PATH
```

6b Remove the dbauser entry from the PostgreSQL file `~novell/.pgpass`.

```
*:*:*:dbauser:password
```

Although the dbauser password is shown in clear text, the contents of this file are only visible to the novell and root users, which already have full access to all functions on the Identity Audit server.

Novell® Identity Audit is installed with a core set of report templates related to Novell applications. Any Identity Audit user can run a report by using the desired parameters (such as start and end date), and the report results are saved with a name of the user's choosing. After the report runs, the results can be retrieved by any Identity Audit user and viewed as a PDF file

Reports are organized by category. Identity Audit is installed with reports for each supported event source.

- ♦ [Section 4.1, "Running Reports," on page 27](#)
- ♦ [Section 4.2, "Viewing Reports," on page 30](#)
- ♦ [Section 4.3, "Managing Reports," on page 31](#)
- ♦ [Section 4.4, "Default Reports," on page 34](#)

4.1 Running Reports

Identity Audit is installed with a set of reports organized into several product categories. Reports run asynchronously, so users can continue to do other things in the application while the report is running. The PDF report results can be viewed by any user after the report finishes running.







Many report definitions include parameters. The user is prompted to set these before running the reports. Depending on how the report developer designed the report, the report parameters can be text, numbers, bits values, or dates. A parameter might have a default value or a list based on values in the Identity Audit database.

- ♦ [Section 4.1.1, "Manually Running a Report," on page 27](#)
- ♦ [Section 4.1.2, "Scheduling a Report," on page 29](#)

4.1.1 Manually Running a Report

- 1 In Identity Audit, click *Reports* to display the available reports.

Reports

NOVELL ACCESS MANAGER		Hide
▶ Novell Access Manager Event Count Trend 6.1r1		Run
▶ Novell Access Manager Top 10 Dashboard 6.1r1		Run
NOVELL EDIRECTORY		Hide
▶ Novell eDirectory Account Trust Assignments 6.1r1		Run
▶ Novell eDirectory Authentication by Server 6.1r1		Run
▶ Novell eDirectory Authentication by User 6.1r1		Run
▶ Novell eDirectory Event Count Trend 6.1r1		Run

If desired, click a report definition to expand it. If you see a *Sample Report* link, you can click *View* to find out how the completed report looks with a set of sample data.

- 2 Select the report you want to run and click *Run*.

Run Novell Access Manager Event Count Trend 6.1r1

Run Option:

Name:

Language:

Date Range:

From Date:

To Date:

Minimum Severity:

Maximum Severity:

Email Report To:

- 3 Set the schedule for running the report. If you want the report to run later, you must also enter a start time.
 - ♦ **Now:** This is the default. It runs the report immediately.
 - ♦ **Once:** Runs the report once at the specified date and time.
 - ♦ **Daily:** Runs the report once a day at the specified time.
 - ♦ **Weekly:** Runs the report once a week on the same day at the specified time.
 - ♦ **Monthly:** Runs the report on the same day of the month every month, starting at the specified date and time. For example, if the start date and time is October 28 at 2 P.M., the report will run on the 28th day of the month at 2 P.M every month.

All time settings are based on the browser's local time.

- 4 Specify a name to identify the report results.

Because the username and time are also used to identify the report results, the report name need not to be unique.

- 5 Choose the language in which the report labels and descriptions should be displayed (English, French, German, Italian, Japanese, Traditional Chinese, Simplified Chinese, Spanish, or Portuguese).

The data in the report will be displayed in whatever language it was originally produced by the event source.

- 6 If the report includes time period parameters, choose the date range. All time periods are based on the local time for the browser.

- ♦ **Current Day:** Shows events from midnight of the current day until 11:59 of the current day. If the current time is 8AM, the report will show 8 hours of data.
- ♦ **Previous Day:** Shows events from midnight yesterday until 11:59PM yesterday.
- ♦ **Week To Date:** Shows events from midnight Sunday of the current week until the end of the current day.
- ♦ **Previous Week:** Shows last seven days of events.
- ♦ **Month to Date:** Shows events from midnight the first day of the current month until the end of the current day.
- ♦ **Previous Month:** Shows a month of events, from midnight of the first day of the previous month until 11:59 PM of the last day of the previous month
- ♦ **Custom Date Range:** For this setting only, you also need to set a start date and end date below.

- 7 If you selected *Custom Date Range*, set the start date (From Date) and the end date (To Date) for the report.

If any of the other settings is selected for the report type, these time settings are ignored.

- 8 Set the *Minimum Severity* events to be included in the report.

- 9 Set the *Maximum Severity* events to be included in the report.

- 10 If the report should be mailed to a user or users, enter their e-mail addresses, separated by commas.

To enable mailing reports, the administrator must configure the mail relay under *Rules > Configuration*.

- 11 Click *Run*.

A report results entry is created and mailed to the designated recipients.

4.1.2 Scheduling a Report

When you run a report, you can run the report immediately or schedule it to be run later, either once or on a recurring basis. For scheduled reports, you must choose a frequency and enter a time at which the report should run.

- ♦ **Now:** This is the default. It runs the report immediately.
- ♦ **Once:** Runs the report once at the specified date and time.
- ♦ **Daily:** Runs the report once a day at the specified time.
- ♦ **Weekly:** Runs the report once a week on the same day at the specified time.
- ♦ **Monthly:** Runs the report on the same day of the month every month, starting at the specified date and time. For example, if the start date and time is October 28 at 2PM, the report will run on the 28th day of the month at 2PM every month.

NOTE: All time settings are based on the browser's local time.

Figure 4-1 Scheduled Reports

Reports

NOVELL ACCESS MANAGER Hide

- ▶ **Novell Access Manager Event Count Trend 6.1r1** × Run
- ▼ **Novell Access Manager Top 10 Dashboard 6.1r1** × Run
 - Daily Access Manager Top 10 Report runs daily at 11:50 PM [Delete](#) [Edit](#)
 - Weekly Access Manager Top 10 runs every Friday at 11:45 PM [Delete](#) [Edit](#)
- ▶ **Access Manager Top 10 Oct. 31** × View
 - run at 10/31/08 12:09 am by admin
 - [show parameters](#)

Report schedules can be removed or modified by using the *Delete* and *Edit* links.

4.2 Viewing Reports

Identity Audit users can view reports in the Identity Audit application. Other users might receive report .pdf files in e-mail.

- 1 To view the list of report results, click *View*.

All previously run reports are shown with the user-defined report name, the user who ran them, and what time the report was run.

NOVELL IDENTITY MANAGER Hide

- ▶ **Novell Identity Manager Account Access Assignments 6.1r1** × Run
- ▶ **Novell Identity Manager Account Trust Assignments 6.1r1** × Run
- ▼ **Novell Identity Manager Administrative Activity 6.1r1** × Run
 - ▶ **Daily Admin Report** × View
 - run at 10/20/2008 9:47 pm by admin
 - [show parameters](#)
 - ▶ **Report 3** × View
 - run at 10/19/2008 10:27 pm by admin
 - [show parameters](#)

If the server was restarted while a report was processing, you will see buttons to cancel or restart the report. If you restart the report, it uses the same parameters as the first time it was run. In cases where the report was run using a relative time setting (such as Current Day), the time period for the rerun report is based on the current date and time, not the date and time at which the report was originally run.

- 2 Click *show parameters* to see the exact values used to run the report.

Run Novell eDirectory User Account Provisioning 6.1r2 Help

Run Option:

Name:

Language:

Date Range:

From Date:

To Date:

Email Report To:

- ◆ For Date Range, D=Current Day, PD=Previous Day, W=Week To Date, PW=Previous Week, M=Month To Date, PM=Previous Month, and DR=Custom Date Range.
 - ◆ For Language, en=English, fr=French, de=German, it=Italian, ja=Japanese, pt=Brazilian Portuguese, es=Spanish, zh=Simplified Chinese, and zh_TW=Traditional Chinese.
- 3 Click *View* for the report results you want to see. The report results are displayed in a new window in .pdf format.

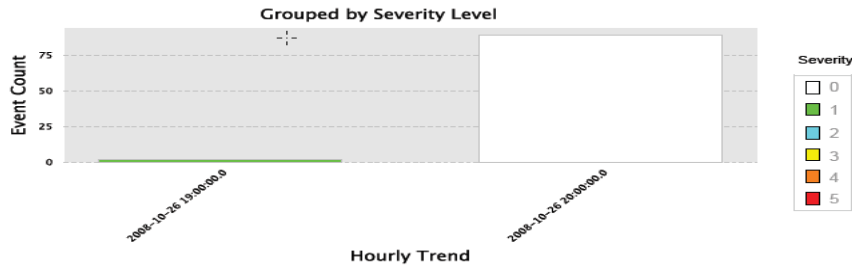
Event Count Trend: Daily

Novell eDirectory

October 26, 2008 12:00:00 AM to October 26, 2008 11:59:59 PM MDT

Severity: All Severities

This report shows event count trends for events captured by Novell eDirectory. The graph below shows event trends for each selected severity within the selected date range.



This cross chart summary indicates the number of events in each Severity category per hour

Severity	0	1	Total
Event Date/Time			
10/26/08 7:00 PM	0	2	2
10/26/08 8:00 PM	89	0	89

TIP: Report results are organized from newest to oldest.

4.3 Managing Reports

Identity Audit users can add, delete, update, and schedule reports.

- ◆ [Section 4.3.1, “Adding Reports,” on page 32](#)
- ◆ [Section 4.3.2, “Creating New Reports,” on page 33](#)
- ◆ [Section 4.3.3, “Renaming Report Results,” on page 33](#)
- ◆ [Section 4.3.4, “Deleting Reports,” on page 34](#)
- ◆ [Section 4.3.5, “Updating Report Definitions,” on page 34](#)

4.3.1 Adding Reports

Any user can add or update reports in Identity Audit.

- ♦ “Downloading New or Updated Reports” on page 32
- ♦ “Adding New Reports to Identity Audit” on page 32

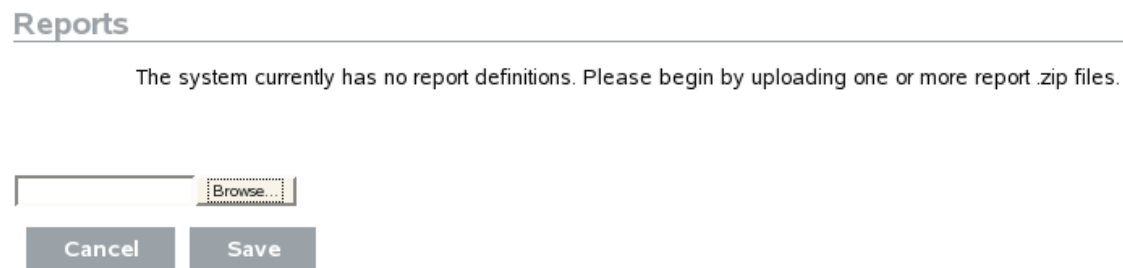
Downloading New or Updated Reports

New or updated reports by Novell can be downloaded from the [Identity Audit 1.0 Plugins Web site](http://support.novell.com/products/sentinel/identityaudit.html) (<http://support.novell.com/products/sentinel/identityaudit.html>).

Adding New Reports to Identity Audit

Identity Audit comes preloaded with reports, but new report plug-ins (special .zip files that include the report definition plus metadata) can be uploaded into Identity Audit. If there are no reports in the system, the following screen displays:

Figure 4-2 *No Reports Loaded*



To add a report:

- 1 Click the *Reports* button on the left side of the screen.
- 2 Click the *Upload Report* button.
- 3 Browse and select the report plug-in .zip file on your local machine.
- 4 Click *Open*.
- 5 Click *Save*.
- 6 If the same report already exists in the report repository (based on the report's unique ID), decide whether to replace the existing report.

Identity Audit displays the details of both the report in the system and the one being imported. In the case below, the imported report is the same version as the existing report.



Replace Report Definition

There is an existing report definition has the same ID with the one you are uploading, do you want to replace it?

Attribute	In the repository	In the file being imported
Name	Novell- eDirectory_Password- Resets_6.1r1	Novell- eDirectory_Password- Resets_6.1r1
Type	JASPER_REPORT	JASPER_REPORT
Version	6.1r1	6.1r1
Release Date	Tue Oct 21 07:09:29 MDT 2008	Tue Oct 21 07:09:29 MDT 2008
Description	This report shows all password changes on users by administrators captured by Novell eDirectory within the selected date range, grouped by the domain within which the target account exists and then grouped by the account name.	This report shows all password changes on users by administrators captured by Novell eDirectory within the selected date range, grouped by the domain within which the target account exists and then grouped by the account name.

Cancel

Replace

The new report definition is added to the list in alphabetical order and can be run immediately, if desired.

4.3.2 Creating New Reports

Users can modify or write reports by using JasperForge iReport, a graphical report designer for JasperReports. iReport is an open source report development tool that is available for download from [JasperForge.org \(http://jasperforge.org/plugins/project/project_home.php?group_id=83\)](http://jasperforge.org/plugins/project/project_home.php?group_id=83) (as of the time of this publication).

New or modified reports can include additional database fields that are not presented in the Identity Audit Web interface. They must adhere to the file and format requirements of the report plug-ins. For more information about database fields and file and format requirements for report plug-ins, see the [Sentinel SDK Web site \(http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel\)](http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel).


4.3.3 Renaming Report Results

Report results (but not report definitions) can be renamed in the Identity Audit interface.

- 1 Click the *Reports* button on the left side of the screen.
- 2 Click a report name to expand it.

- 3 Click the name of the report results you want to rename.
- 4 Specify the new name.
- 5 Click *Rename*.

4.3.4 Deleting Reports

Users can delete either a report result set or a report definition by using the  button. If a report definition is deleted, all associated report results are also deleted.

If a report in progress is canceled by using the *Cancel* link, the query on the database is canceled.

4.3.5 Updating Report Definitions

Users can upload updated reports to Identity Audit to replace an existing report. For more information, see [Section 4.3.1, “Adding Reports,” on page 32](#).

4.4 Default Reports

This section lists the pre-installed reports of Novell Identity Audit:

- ◆ Novell Access Manager Event Count Trend
- ◆ Novell Access Manager Top 10 Dashboard
- ◆ Novell eDirectory Account Trust Assignments
- ◆ Novell eDirectory Authentication by Server
- ◆ Novell eDirectory Authentication by User
- ◆ Novell eDirectory Event Count Trend
- ◆ Novell eDirectory Inactive Users
- ◆ Novell eDirectory Object Provisioning
- ◆ Novell eDirectory Password Management
- ◆ Novell eDirectory Password Resets
- ◆ Novell eDirectory Periodic Password Change Violations
- ◆ Novell eDirectory Per Object Modification
- ◆ Novell eDirectory Per Trust Modification
- ◆ Novell eDirectory Per User Modification
- ◆ Novell eDirectory Self Password Changes
- ◆ Novell eDirectory Top 10 Dashboard
- ◆ Novell eDirectory Trust Management
- ◆ Novell eDirectory Trust Provisioning
- ◆ Novell eDirectory User Account Provisioning
- ◆ Novell eDirectory User Status Management
- ◆ Novell Identity Manager Account Trust Assignments
- ◆ Novell Identity Manager Administrative Activity
- ◆ Novell Identity Manager Authentication by Server

- ◆ Novell Identity Manager Authentication by User
- ◆ Novell Identity Manager Configuration Changes
- ◆ Novell Identity Manager Event Count Trend
- ◆ Novell Identity Manager Management Approval Overview 6.1r1.rpz
- ◆ Novell Identity Manager Password Management
- ◆ Novell Identity Manager Password Resets
- ◆ Novell Identity Manager Periodic Password Change Violations
- ◆ Novell Identity Manager Per User Modification
- ◆ Novell Identity Manager Resource Request Errors
- ◆ Novell Identity Manager Resource Requests by Process
- ◆ Novell Identity Manager Resource Requests by User
- ◆ Novell Identity Manager Resource Requests Rejected
- ◆ Novell Identity Manager Top 10 Dashboard
- ◆ Novell Identity Manager Trust Management
- ◆ Novell Identity Manager User Status Management
- ◆ Novell Identity Manager Workflow Proxy Delegation Management
- ◆ Novell NMAS Event Count Trend
- ◆ Novell NMAS Inactive Users
- ◆ Novell NMAS Top 10 Dashboard
- ◆ Novell SecretStore Event Count Trend
- ◆ Novell SecretStore Top 10 Dashboard
- ◆ Novell SecureLogin Event Count Trend
- ◆ Novell SecureLogin Top 10 Dashboard

Administrators can configure and monitor data collection for Novell® Identity Audit. Identity Audit is installed with the ability to collect data from a variety of Novell applications by using the Novell Audit. For information on the supported versions of the, see [Section 2.4, “Supported Platform Agent Version,”](#) on page 18.

- ♦ [Section 5.1, “Data Collection Status,”](#) on page 37
- ♦ [Section 5.2, “Managing Event Sources,”](#) on page 40
- ♦ [Section 5.3, “Audit Server Options,”](#) on page 40
- ♦ [Section 5.4, “Event Sources,”](#) on page 45

5.1 Data Collection Status

Administrators can enable or disable data collection and view health information about the audit server and event sources.

- ♦ [Section 5.1.1, “Enabling and Disabling Data Collection,”](#) on page 37
- ♦ [Section 5.1.2, “Viewing Audit Server Health,”](#) on page 38
- ♦ [Section 5.1.3, “Viewing Event Source Health,”](#) on page 39

5.1.1 Enabling and Disabling Data Collection

- 1 Log into Identity Audit as an administrator.
- 2 Click *Collection* in the upper right corner of the page.

● **Audit Server**
 ON OFF

 Healthy

EVENT SOURCES	ON	OFF
● Novell Access Manager Warning (0.0 eps) show details	<input checked="" type="radio"/>	<input type="radio"/>
● Novell eDirectory Healthy (0.0 eps)	<input checked="" type="radio"/>	<input type="radio"/>
● Novell Identity Manager Healthy (0.0 eps)	<input checked="" type="radio"/>	<input type="radio"/>
● Novell NMAS Healthy (0.0 eps)	<input checked="" type="radio"/>	<input type="radio"/>
● Novell SecretStore Warning (0.0 eps) show details	<input checked="" type="radio"/>	<input type="radio"/>
● Novell SecureLogin Warning (0.0 eps) show details	<input checked="" type="radio"/>	<input type="radio"/>

- In the *Audit Server* section, administrators can enable or disable data collection at a global level by using the *On* and *Off* options. For more information about audit server health status, refer to [Section 5.1.2, “Viewing Audit Server Health,” on page 38](#).
- In the *Event Sources* section, administrators can enable data collection at the application level by using the *On* and *Off* options. These settings might affect data collection for several servers (for example, multiple eDirectory™ instances). They do not start or stop services on the event source machines.

For more information about event source health status, see [Section 5.1.3, “Viewing Event Source Health,” on page 39](#).

Changes on this page take effect immediately.

5.1.2 Viewing Audit Server Health

The Audit Server is a server that listens for connections from Novell applications.

- Log into Identity Audit as an administrator.
- Click *Collection* in the upper right corner of the page.
- A colored icon beside the Audit Server indicates its health.

Healthy: A green indicator means that the Audit Server is healthy (it is turned on, is listening on a port, and doesn’t have any unresolved errors).

Error: A red indicator means that the Audit Server has experienced an error. For more information, view the `server0.*.log` files.

Offline: A black indicator means that the Audit Server has been taken offline by an administrator.

5.1.3 Viewing Event Source Health

The health status for each Novell application is indicated by a colored icon. For each online data source, Identity Audit also shows the calculated event rate for incoming events. The event rate is recalculated every 60 seconds.

For more information about the health status, including the IP addresses of the individual event sources, click *show details*.

- 1 Log into Identity Audit as an administrator.
- 2 Click *Collection* in the upper right corner of the page.
- 3 A colored icon beside the Novell application indicates its health.

Healthy: A green indicator means that the event source is healthy and Identity Audit has received data from it.

Warning: A yellow indicator indicates a warning condition. A frequent cause is that the application is turned on in Identity Audit but has not sent any data. For example, this could happen if the event source is not configured properly to send data to Identity Audit or if event logging is not enabled for the application.

Error: A red indicator means that the Identity Audit server is reporting an error connecting to or receiving data from this application.

Offline: A black indicator means that the event source has been turned off. Identity Audit is not processing any data from it.

- 4 Click *show details* to see more information, including IP addresses for individual event sources and their associated status.

Data Collection | Status [Configuration](#)

Audit Server ON OFF
Healthy

EVENT SOURCES	ON	OFF
Novell Access Manager Warning (0.0 eps) hide details No connections from this application	<input checked="" type="radio"/>	<input type="radio"/>
Novell eDirectory Healthy (45.93 eps / 1 connection) hide details 10.0.0.4 Healthy	<input checked="" type="radio"/>	<input type="radio"/>
Novell Identity Manager Error (0.0 eps / 1 connection) hide details X 10.0.0.0 Lost connection to application DirXML on machine 10.0.0.2	<input checked="" type="radio"/>	<input type="radio"/>

5.2 Managing Event Sources

Although Identity Audit is preconfigured to accept data from supported Novell applications, the application servers themselves must be configured to send data to the Identity Audit server. This is part of the basic setup for Identity Audit. For more information, see [Section 3.3, “Configuring Event Sources,”](#) on page 23.

- ♦ [Section 5.2.1, “Adding Event Sources,”](#) on page 40
- ♦ [Section 5.2.2, “Deleting Event Sources,”](#) on page 40

5.2.1 Adding Event Sources

After new event sources start sending data to Identity Audit, the IP addresses for those event sources are automatically added to the list of IPs that shows when you click *show details* for a Novell application.

5.2.2 Deleting Event Sources

If there is an error with the connection for an event source, the event source can be deleted using the yellow icon to the left of the IP address. If the event source starts sending data again, the connection will be automatically re-established.



5.3 Audit Server Options

Administrators can change some settings regarding how Identity Audit listens for data from the event source applications, including the port on which Identity Audit listens and the type of authentication between the event source and Identity Audit.

- 1 Log into Identity Audit as an administrator.
- 2 Click the *Collection* link at the top of the screen.
- 3 Click the *Configuration* link on the right side of the screen.
- 4 Make sure that the *Audit Server* tab is selected.

The screenshot shows the 'Event Sources' configuration window for the Identity Audit server. It has two tabs: 'Audit Server' and 'Event Sources'. The 'Event Sources' tab is active. The configuration includes:

- Listen on port:** A text box containing '1289' with a green checkmark and the text 'port is valid and open.' below it. A note states: 'Ports less than 1024 on Linux and UNIX server will require root privileges.'
- Client authentication:** Three radio button options: 'Open - no authentication required.' (selected), 'Loose - requires client certificate.', and 'Strict - requires client certificate signed by an authority.'
- Server key pairs:** Two radio button options: 'Internal (default)' (selected) and 'Custom'.
- If too many events received:** Two radio button options: 'Temporarily pause connections (recommended)' (selected) and 'Drop oldest messages'.
- Idle Connection:** A checked checkbox followed by the text 'Pause connection if idle for' and a text box containing '15' followed by 'minutes'.
- Event Signatures:** An unchecked checkbox followed by the text 'Request Novell Audit Event Signatures'.

At the bottom right of the dialog are 'Cancel' and 'Save' buttons.

5 Specify the port on which the Identity Audit server will listen for messages from the event sources. For more information, see [Section 5.3.1, “Port Configuration and Port Forwarding,” on page 42.](#)

6 Set the appropriate client authentication and server key pairs settings. For more information, see [Section 5.3.2, “Client Authentication,” on page 42.](#)

7 Select the Identity Audit server behavior when the buffer fills with too many events.

Temporarily pause connections: Drops the existing connections and stops accepting new connections until the buffer has space for the new messages. In the meantime, messages are cached by the event sources.

Drop oldest messages: Drops the oldest messages in order to accept new messages.

WARNING: There is no supported method for recovering dropped messages if you select *Drop oldest messages*.

8 Select *Idle Connection* to disconnect event sources that have not sent data for a certain period of time.

The event source connections are automatically re-created when they start sending data again.

9 Specify the number of minutes before an idle connection is disconnected.

- 10 Select *Event Signatures* to receive a signature with the event.

To receive a signature, the Platform Agent on the event source must be configured properly. For more information, see [Section 5.2, “Managing Event Sources,” on page 40](#).

- 11 Click *Save*.

5.3.1 Port Configuration and Port Forwarding

The default port on which Identity Audit listens for messages from the s is port 1289. When the port is set, the system checks whether the port is valid and open.

Binding to ports less than 1024 requires root privileges. Instead, Novell recommends that you use a port greater than 1024. You can change the source devices to send to a higher port or use port forwarding on the Identity Audit server.

To change the event source to send to a different port:

- 1 Log into the event source machine.
- 2 Open the `logevent` file for editing. The file is in a different location depending on the operating system:
 - ♦ Linux: `/etc/logevent.conf`
 - ♦ Windows: `C:\WINDOWS\logevent.cfg`
 - ♦ NetWare: `SYS:\etc\logevent.cfg`
 - ♦ Solaris: `/etc/logevent.conf`
- 3 Set the `LogEnginePort` parameter to the desired port.
- 4 Save the file.
- 5 Restart the Platform Agent. The method varies by operating system and application. Reboot the machine or refer to the application-specific documentation on the [Novell Documentation Web Site \(http://www.novell.com/documentation\)](http://www.novell.com/documentation) for more instructions.

To configure port forwarding on the Identity Audit server:

- 1 Log into the Identity Audit server operating system as `root` (or `su to root`).
- 2 Open the file `/etc/init.d/boot.local` for editing.
- 3 Add the following command near the end of the bootup process:

```
iptables -A PREROUTING -t nat -p protocol --dport incoming port -j DNAT --to-destination IP:rerouted port
```

where *protocol* is `tcp` or `udp`, *incoming port* is the port on which the messages are arriving, and *IP:rerouted port* are the IP address of the local machine and an available port above 1024
- 4 Save the changes.
- 5 Reboot. If you cannot reboot immediately, run the `iptables` command above from a command line.

5.3.2 Client Authentication

Event sources send their data over an SSL connection, and the *Client authentication* setting for the Identity Audit server determines what kind of authentication is performed for the certificates from the s on the event sources.

Open: No authentication is required. Identity Audit does not request, require, or validate a certificate from the event source.

Loose: A valid X.509 certificate is required from the event source, but the certificate is not validated. It does not have to be signed by a Certificate Authority.

Strict: A valid X.509 certificate is required from the event source, and it must be signed by a trusted Certificate Authority. If the event source does not present a valid certificate, Identity Audit does not accept its event data.

- ♦ “Creating a Truststore” on page 43
- ♦ “Importing a Truststore” on page 43
- ♦ “Server Key Pair” on page 44

Creating a Truststore

For strict authentication, you must have a truststore that contains either the event source’s certificate or the certificate for the Certificate Authority (CA) that signed the event source’s certificate. After you have a DER or PEM certificate, you can create the truststore by using the CreateTruststore utility that comes with Identity Audit.

- 1 Log in to the Identity Audit server as novell.
- 2 Go to `/opt/novell/identity_audit_1.0_x86/data/updates/done`.
- 3 Unzip the file `audit_connector.zip`.

```
unzip audit_connector.zip
```

- 4 Either copy `TruststoreCreator.sh` or `TruststoreCreator.bat` to the machine with the certificates or copy the certificates to the machine with the `TruststoreCreator` utility.
- 5 Run the `TruststoreCreator.sh` utility.

```
TruststoreCreator.sh -keystore /tmp/my.keystore -password password1 -certs  
/tmp/cert1.pem,/tmp/cert2.pem
```

In this example, the `TruststoreCreator` utility creates a keystore file called `my.keystore` that contains two certificates (`cert1.pem` and `cert2.pem`) in it. It is protected by the password `password1`.

Importing a Truststore

For strict authentication, the administrator can import a truststore by using the *Import* button. This helps ensure that only authorized event sources are sending data to Identity Audit. The truststore must include either the event source’s certificate or the certificate of the Certificate Authority that signed it.

The following procedure must be run on the machine that has the truststore on it. You can open a Web browser on the machine with the truststore or move the truststore to any machine with a Web browser.

To import a truststore:

- 1 Log into Identity Audit as an administrator.
- 2 Click the *Collection* link at the top of the screen.
- 3 Click the *Configuration* link on the right side of the screen.

- 4 Make sure that the *Audit Server* tab is selected.
- 5 Select the *Strict* option under *Client authentication*.
- 6 Click *Browse* and browse to the truststore file (for example, `my.keystore`)
- 7 Enter the password for the truststore file.
- 8 Click *Import*.
- 9 If desired, click *Details* to see more information about the truststore.

Client authentication: Open - no authentication required.
 Loose - requires client certificate.
 Strict - requires client certificate signed by an authority.

Principle	Issuer
CN=sles10vm64-scout,O=client	CN=sles10vm64-scout,O=client
CN=sles10vm64-scout,O=broker	CN=sles10vm64-scout,O=broke

Cancel

- 10 Click *Save*.

After the truststore is imported successfully, you can click *Details* to see the certificates included in the truststore.

Server Key Pair

Identity Audit is installed with a built-in certificate, used to authenticate the Identity Audit server to the event sources. This certificate can be overridden with a certificate signed by a public certificate authority (CA).

To replace the built-in certificate:

- 1 Log into Identity Audit as an administrator.
- 2 Click the *Collection* link at the top of the screen.
- 3 Click the *Configuration* link on the right side of the screen.
- 4 Make sure that *Audit Server* is selected.
- 5 Under *Server key pairs*, select *Custom*.
- 6 Click *Browse* and browse to the truststore file.
- 7 Enter the password for the truststore file.
- 8 Click *Import*.

Audit Server | Event Sources

Listen on port: ✔ port is valid and open.
Ports less than 1024 on Linux and UNIX server will require root privileges.

Client authentication: Open - *no authentication required.*
 Loose - *requires client certificate.*
 Strict - *requires client certificate signed by an authority.*

Server key pairs: Internal (default)
 Custom

key1
 key2

If there is more than one public-private key pair in the file, select the desired key pair and click *OK*.

- 9 Click *Details* to see more information about the server key pair.
- 10 Click *Save*.

5.4 Event Sources

The Event Sources page allows administrators to configure how time is determined for events from each event source. The event time can be based on the time stamp from the event source (“trust event time”) or the time stamp from the Identity Audit server. The time stamp affects the order in which events are displayed in a search if you sort by time. The time stamp also affects the display time in reports. The default is to use the Identity Audit server time.

NOTE: An NTP server is recommended to keep time synchronized on all machines in the Identity Audit system. If an NTP server is available, you should trust the event time for the applications. If an NTP server is not available, you should use the Identity Audit server time for all applications (which is the default setting) to correct for any time differences between machines.

To change the event time options:

- 1 Log into Identity Audit as an administrator.
- 2 Click the *Collection* link at the top of the screen.
- 3 Click the *Configuration* link on the right side of the screen.
- 4 Click *Event Source*.

- 5 Select all applications for which Identity Audit should use the event time stamp from the original application.

Data Collection | Configuration

Audit Server | **Event Sources**

Trust the event time associated with the following applications: [\(what's this?\)](#):

- Novell Access Manager
- Novell eDirectory
- Novell Identity Manager
- Novell NMAS
- Novell SecretStore
- Novell SecureLogin

Cancel Save

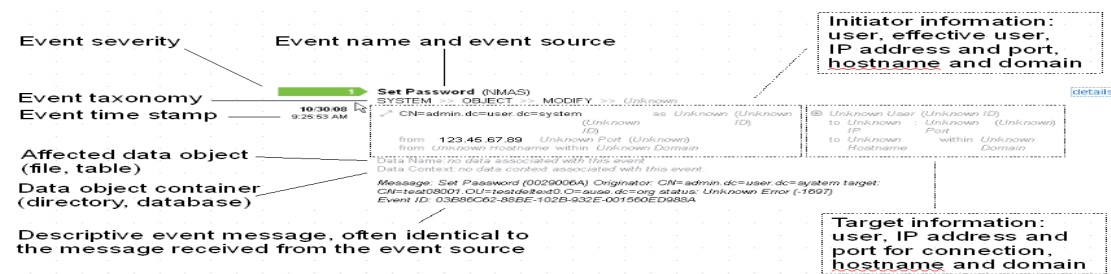
For all others, the Identity Audit server time stamp replaces the time stamp from the original application.

The changes take effect immediately for all new incoming events. It might take some time for events already in the queue to be processed.

Novell Identity Audit provides the ability to perform a search on events. The search includes all online data currently in the database, but internal events generated by the Identity Audit system are excluded unless the user selects *Include System Events*. By default, events are sorted based on the search engine’s relevancy algorithm.

Basic event information includes event name, source, time, severity, information about the initiator (represented by an arrow icon), and information about the target (represented by a bull’s-eye icon).

Figure 6-1 Event Fields



- ◆ [Section 6.1, “Running an Event Search,”](#) on page 47
- ◆ [Section 6.2, “Viewing Search Results,”](#) on page 49
- ◆ [Section 6.3, “Event Fields,”](#) on page 52

6.1 Running an Event Search

Users can run simple and advanced searches.

- ◆ [Section 6.1.1, “Basic Search,”](#) on page 47
- ◆ [Section 6.1.2, “Advanced Search,”](#) on page 48

6.1.1 Basic Search

A basic search runs against all of the event fields in [Table 6-1 on page 52](#). Some sample basic searches include the following:

- ◆ root
- ◆ 127.0.0.1
- ◆ Lock*
- ◆ driverset0

NOTE: If time is not synchronized between the end user machine and the Identity Audit server (for example, one machine is 25 minutes behind), you might get unexpected results from your search. Searches such as *Last 1 hour* or *Last 24 hours* are based on the end user’s machine time.

1 Click the *Search* link on the left.

Identity Audit is configured to run a default search for non-system events with severity 3 to 5 the first time a user clicks the *Search* link. Otherwise, it defaults to the last search term the user entered.

Search

[Search Tips](#)

Include System Events
 Sort By Time

No Results
No events found for "sev:[3 TO 5]"

- 2 For a different search, type a search term in the search field (for example, *admin*). The search is not case-sensitive.
- 3 Select a time period for which the search should be performed. Most of the time settings are self-explanatory, and the default is *Last 30 Days*.
 - ♦ *Custom* allows you select a start date and time and an end date and time for the query. The start date must be before the end date, and the time is based is based on the browser’s local time.
 - ♦ *All time* searches all the data in the database.
- 4 Select *Include System Events* to include events that are generated by Identity Audit system operations.
- 5 Select *Sort By Time* to arrange data with the most recent events at the beginning.
Sorting by time takes longer than sorting by relevance, which is the default.
- 6 Click *Search*.

All fields in the index are searched for the specified text. A spinning icon indicates that the search is taking place.

The event summaries are displayed.

1

Set Password (NMAS) [details+](#)

SYSTEM >> OBJECT >> MODIFY >> *Unknown*

10/30/08
9:25:53 AM

↗ CN=admin.dc=user.dc=system from *Unknown* within *Unknown* @ *Unknown* to *Unknown* within *Unknown*
Hostname Domain User Hostname Domain

6.1.2 Advanced Search

An advanced search can search for a value in a specific event field or fields. The advanced search criteria are based on the short names for each event field and the search logic for the index. To view the field names and descriptions, the short names that are used in advanced searches, and whether the fields are visible in the basic and detailed event views. see [Table 6-1 on page 52](#).

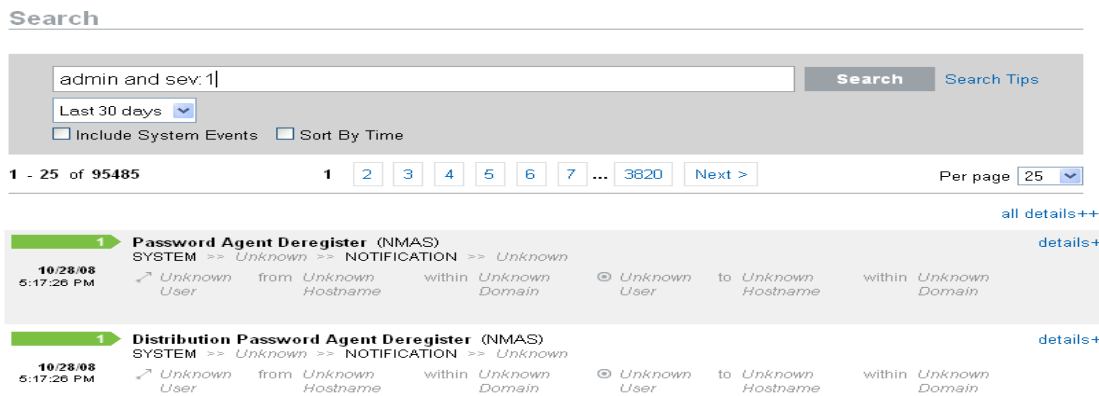
To search for a value in a specific field, use the short name of the field, a colon, and the value. For example, to search for an authentication attempt to Identity Audit by user2, use the following text in the search field:

- ♦ `evt:authentication AND sun:user2`

Other advanced searches might include:

- ♦ `pn:NMAS AND sev:5`
- ♦ `sip:123.45.67.89 AND evt:"Set Password"`

Figure 6-2 Advanced Search Example



Multiple advanced search criteria can be combined by using the following bits operators:

- ♦ AND (must be capitalized)
- ♦ OR (must be capitalized)
- ♦ NOT (must be capitalized and cannot be used as the only search criterion)
- ♦ +
- ♦ -

Special characters must be escaped by using a \ symbol:

+ - & | ! () { } [] ^ " ~ * ? : \

The advanced search criteria are modeled on the search criteria for the Apache Lucene* open source package. More detail about the search criteria is available on the Web: [Lucene Query Parser Syntax \(http://lucene.apache.org/java/2_3_2/queryparsersyntax.html\)](http://lucene.apache.org/java/2_3_2/queryparsersyntax.html).

6.2 Viewing Search Results

Searches return a set of events. Users can view basic or detailed event information and configure the number of results per page. Search results are returned in batches. The default batch size is 25 results, but this is easily configured.

When results are sorted by relevance, only the top 100,000 events can be viewed. When they are sorted by time, this limitation does not exist.

- ♦ [Section 6.2.1, “Basic Event View,” on page 50](#)

- ◆ Section 6.2.2, “Event View with Details,” on page 50
- ◆ Section 6.2.3, “Refining Search Results,” on page 51

6.2.1 Basic Event View

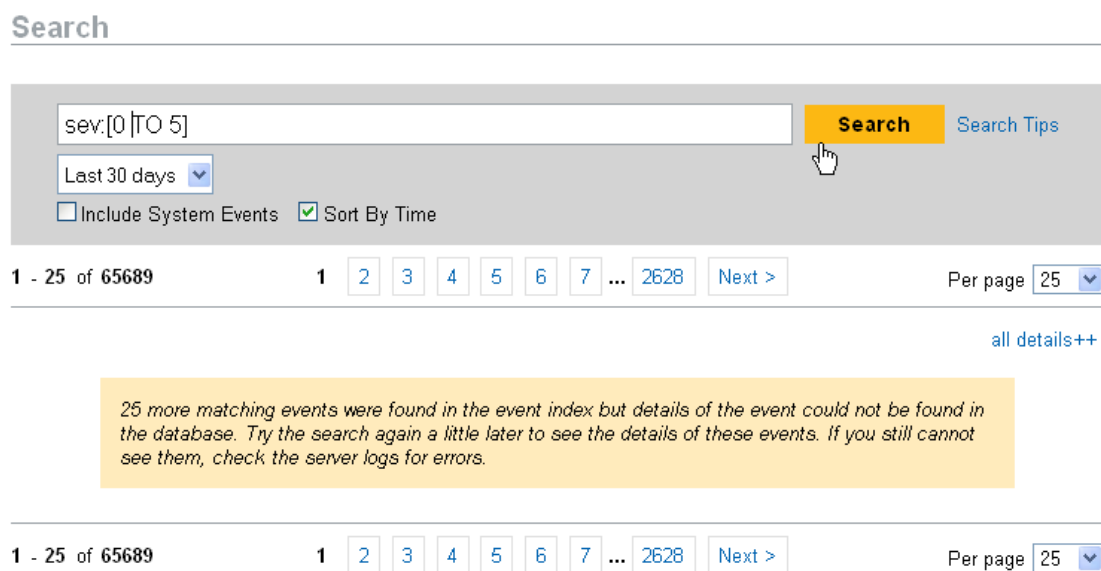
The information in each event is grouped into Initiator information and Target information. If data isn’t available for a particular event field, the fields are labeled *Unknown*.

Figure 6-3 Basic Event View



Occasionally, the search engine might index events faster than they are inserted into the database. If a user runs a search that returns events that have not been inserted into the database, the user gets a message that some events match the search query but could not be found in the database. Generally if the search is run again later, the events are in the database and the search is successful.

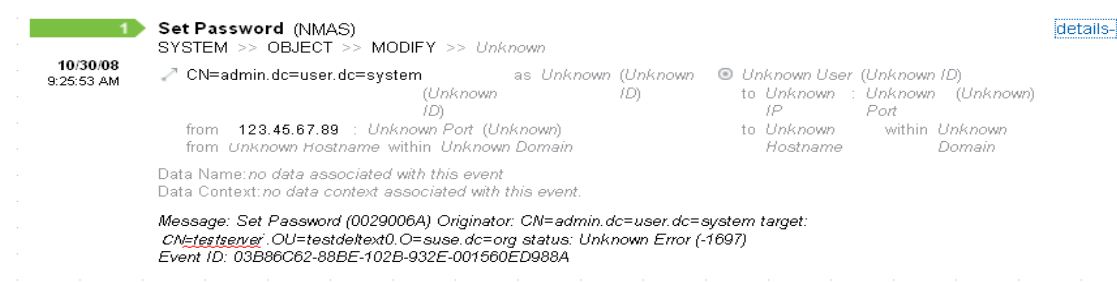
Figure 6-4 Events Indexed but Not Yet in Database



6.2.2 Event View with Details

Users can view additional details about any event or events by clicking the *details* link on the right side of the page. The details for all events on a page can be expanded or collapsed by using the All Details++ or *All details--* link. This preference is retained as you scan through multiple pages of results or execute new searches.

Figure 6-5 Event View with Details



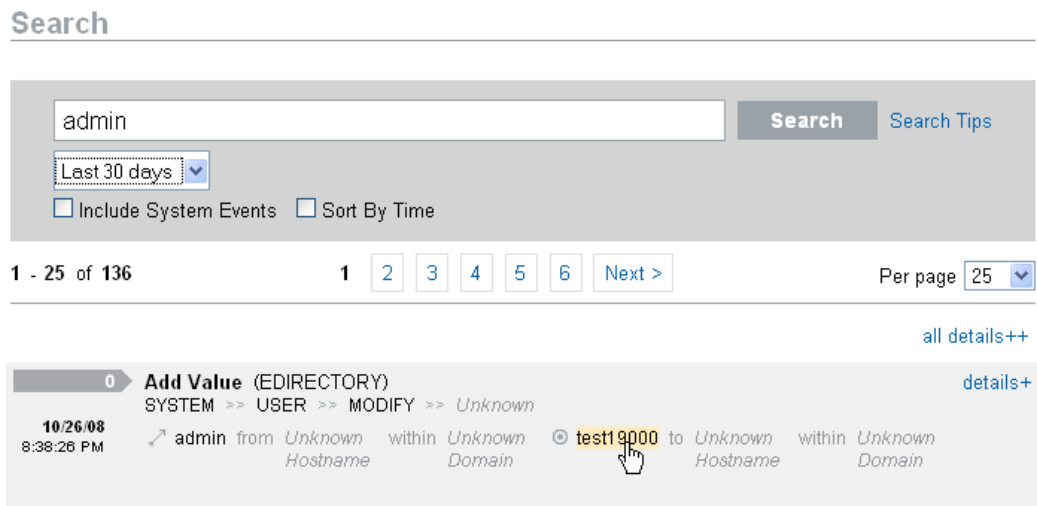
The event above shows the same event as in Figure 6-3 on page 50 but with an expanded view that shows additional data fields that might have been populated.

6.2.3 Refining Search Results

After viewing the results of a search, it might be necessary to refine the search results and add additional search criteria. For example, you might see one initiator user's name appear several times in the search results and want to see more events from that initiator.

To filter the search results using a specific value appearing in the search results:

- 1 Identify the desired filter criteria in the search results.
- 2 Click the value (for example, target hostname test1900) by which you want to filter the results.



TIP: This adds the value to your filter with an AND operator. To add the value to your filter with an NOT operator, press the Alt key as you click the value.

3 Click *Search*.

Search

Search
[Search Tips](#)

Last 30 days
 Include System Events
 Sort By Time

1 - 25 of 36
1 2 [Next >](#)
Per page 25

0
Add Value (EDIRECTORY)
details+

SYSTEM >> USER >> MODIFY >> *Unknown*

10/26/08
8:38:26 PM
↗ admin from *Unknown* within *Unknown* © test19000 to *Unknown* within *Unknown*

Hostname
Domain
Hostname
Domain

Some fields cannot be selected to refine a search this way:

- ◆ EventTime
- ◆ Message
- ◆ Any field related to the Reporter
- ◆ Any field related to the Observer
- ◆ Any field related to TargetTrust
- ◆ Any field with a value *Unknown*

6.3 Event Fields

Each event has fields that might or might not be populated, depending on the specific event. The values for these event fields can be viewed by using a search or running a report. Each field has a short name that is used in advanced searches. The values for most of these fields are visible in the detailed event view; other values are also visible in the basic event view.

Table 6-1 *Event Fields*

Field	Short Name	Description	Visible in Basic View	Visible in Detailed View
Severity	sev	Normalized severity of event on a scale of 0 (informational) to 5 (critical)	X	X
EventTime	dt	Time stamp of event. Can be the Identity Audit server time stamp or the time stamp from the original event source (if <i>trust event time</i> is enabled)	X	X
EventName	evt	Short name of the event	X	X

Field	Short Name	Description	Visible in Basic View	Visible in Detailed View
Message	msg	Detailed event message		X
ProductName	pn	Product that generated the event; the event source Displayed after the event name.	X	X
InitUserName	sun	Username of the user who initiated the event	X	X
InitUserID	iuid	User ID of the user who initiated the event, based on the raw data reported by the device.		X
InitUserDomain	rv35	Domain of the user who initiated the event Searchable but not displayed in either event view		
InitHostName	shn	Hostname of the machine from which the event initiated	X	X
InitHostDomain	rv42	Domain of the machine from which the event initiated	X	X
InitIP	sip	IP address of the machine from which the event initiated		X
InitServicePort	spint	Port number from which the event initiated (for example, HTTP)		X
InitServicePortName	sp	Type of port from which the event initiated (for example, HTTP)		X
TargetUserName	dun	Username of the user who was the target of the event	X	X
TargetUserID	tuid	User ID of the user who was the target of the event, based on the raw data reported by the device.		X
TargetUserDomain	rv45	Domain of the user who was the target of the event Searchable but not displayed in either event view		X
TargetHostName	dhn	Hostname of the machine that was the target of event	X	X
TargetHostDomain	rv41	Domain of the machine that was the target of event	X	X
TargetIP	dip	IP address of the machine that was the target of event		X
TargetServicePort	dpint	Port number that was the target of event (for example, 80)		X

Field	Short Name	Description	Visible in Basic View	Visible in Detailed View
TargetServicePortName	dp	Type of port that was the target of event (for example, HTTP)		X
TargetTrustName	ttn	Role of the user that was a target of the event (for example, FinanceAdmin) Searchable but not displayed in either event view		
TargetTrustID	ttid	Numerical ID representing the role of the user that was a target of the event Searchable but not displayed in either event view		
TargetTrustDomain	ttd	Domain (namespace) within which the target trust exists. Searchable but not displayed in either event view		
EffectiveUserName	euname	Name of the user that the InitUser is impersonating (<code>root</code> using <code>su</code> , for example); follows <i>Initiator Username (Initiator User ID)</i> as in the detailed event view		X
EffectiveUserID	eid	Numerical ID of the user that the InitUser is impersonating (<code>root</code> using <code>su</code> , for example), based on the raw data reported by the device.		X
ObserverHostName	sn	Hostname of the machine that forwarded the event to the security information event management system (for example, the hostname of a syslog server) Searchable but not displayed in either event view		
ObserverHostDomain	obsdom	Domain of the machine that forwarded the event to the security information event management system (for example, the domain of a syslog server) Searchable but not displayed in either event view		
ObserverIP	obsip	IP address of the machine that forwarded the event to the security information event management system (for example, the IP address of a syslog server) Searchable but not displayed in either event view		

Field	Short Name	Description	Visible in Basic View	Visible in Detailed View
ReporterHostName	rn	<p>Hostname of the machine that reported the event to an observer</p> <p>Searchable but not displayed in either event view</p>		
ReporterHostDomain	reptom	<p>Domain of the machine that reported the event to an observer</p> <p>Searchable but not displayed in either event view</p>		
ReporterIP	repip	<p>IP address of the machine that reported the event to an observer</p> <p>Searchable but not displayed in either event view</p>		
SensorType	st	<p>The single character designator for the sensor type (N=network, H=host, O=operating system, A and I=Identity Audit auditing events, P=Identity Audit performance events)</p> <p>Searchable but not displayed in either event view</p>		
DataName/Filename	fn	Data object name reported in the event (for example, the file name or database table name)		X
DataCotext	rv36	Container for the FileName data object (for example, a directory for a file or a database instance for a database table)		X
TaxonomyLevel1	rv50	<p>Target classification for event. Displayed under the event name in the format:</p> <p>TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4</p>	X	X
TaxonomyLevel2	rv51	<p>Subtarget classification for the event. Displayed under the event name in the format:</p> <p>TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4</p>	X	X
TaxonomyLevel3	rv52	<p>Action information for the event. Displayed under the event name in the format:</p> <p>TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4</p>	X	X
TaxonomyLevel4	rv53	<p>Detail information for the event. Displayed under the event name in the format:</p> <p>TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4</p>	X	X

Some fields are tokenized. Tokenizing the fields makes it possible to search for an individual word in the field without a wildcard. The fields are tokenized based on spaces and other special characters. For these fields, articles such as “a” or “the” are removed from the search index.

- ◆ EventName
- ◆ Message
- ◆ ProductName
- ◆ FileName
- ◆ DataCotext
- ◆ TaxonomyLevel1
- ◆ TaxonomyLevel2
- ◆ TaxonomyLevel3
- ◆ TaxonomyLevel4

Data Storage

7

Novell® Identity Audit installation installs a PostgreSQL database with all the necessary tables and users to run Identity Audit. The database also includes stored procedures designed to manage database partitions and archive old data. Administrators can manage the database storage and archiving settings via the Web interface.

- ◆ [Section 7.1, “Database Health,” on page 57](#)
- ◆ [Section 7.2, “Data Storage Configuration,” on page 58](#)
- ◆ [Section 7.3, “Database Setup,” on page 59](#)

7.1 Database Health

The Data Storage Health page, available only to administrators, shows database health based on the number of partitions available in the database and the success of the stored procedures to create new partitions and archive data (if configured).

To view database health:

- 1 Log into Identity Audit as an administrator.
- 2 Click the Storage link in the upper right corner of the page.

The health page displays. If Identity Audit is configured to delete old data, the health page for a healthy database looks like this:

The screenshot shows the 'Data Storage | Health' page with a 'Configuration' link. It features two green bullet points: 'Online Database' with details 'Days Requested: 90 Days Online: 2' and 'Your database for online storage is currently healthy.', and 'Online Database Jobs' with the text 'There are no problems with your online database jobs.'

If Identity Audit is configured to archive and delete old data, the health page for a healthy database looks like this:

The screenshot shows the 'Data Storage | Health' page with a 'Configuration' link. It features three green bullet points: 'Online Database' with details 'Days Requested: 90 Days Online: 3' and 'Your database for online storage is currently healthy.', 'Archive Database' with the text 'There are no problems with your archive storage.', and 'Online Database Jobs' with the text 'There are no problems with your online database jobs.'

This page shows whether several database functions are in a healthy state (green), a warning state (yellow), or an error state (red).

Online Database: This indicator shows whether the expected number of partitions exists in the database for each of the partitioned tables. The expected number of partitions is based on the number of days configured to be online (or the number of days since installation, if the installation is recent).

If the number of partitions is not as expected, the page shows the name of the table, the number of partitions that were expected, and the actual number of partitions in the database.

Online Database Jobs: This indicator turns red if there were any errors the last time the stored procedures to add partitions and delete data were run. If archiving is enabled, this indicator only shows whether there were errors the last time the job to add partitions was run. If there are errors, the page displays the name, time stamp, and details associated with the failed job.

Archive Database: This indicator is only displayed if archiving is enabled. It turns red if there were any errors the last time the stored procedure to archive data was run. If there are errors, the page displays the name, time stamp, and details associated with the failed job.

7.2 Data Storage Configuration

The database is the repository for incoming events, configuration information, and report results. Identity Audit provides database management procedures to prevent the database from filling up. The Data Storage page, accessible only to administrators, provides the ability to configure several aspects of data storage.

Figure 7-1 Data Storage Configuration

Data Storage | Configuration

Keep data online for: days

After online period expires: Delete data

Archive data

Perform maintenance every day at: : GMT-0600 (server time)

Cancel

Save

Keep data online for: Administrators can specify the number of days to keep data in the database for reporting purposes. The minimum is one day, and the number must be a whole number (no decimals).

After online period expires: After the online data retention period expires, any event data older than the time period above is either deleted or moved out of the database to an archive directory.

WARNING: Deleted data cannot be recovered, so choose the *Delete* option with care.

Archive to this database directory: If the *Archive data* option is chosen, data is archived to a specified location before it is deleted. This directory must already exist and the novell user must have write access to it. By default, this location is set to `data/db_archive` in the Identity Audit home directory. The default directory is created with the proper permissions during Identity Audit installation.

Figure 7-2 Configuration Page when Archive Data is Selected

Data Storage | Configuration

Keep data online for: days

After online period expires: Delete data
 Archive data

Archive to this database directory: [\(What is this?\)](#)

Perform maintenance every day at: : GMT-0400 (server time)

IMPORTANT: The archive files should be moved periodically to a long-term storage location to avoid filling the hard disk.

Test: If the *Archive data* option is chosen, the *Test* button verifies whether the archive directory exists and is writable by the novell user.

Perform maintenance every day at: Specify the time of day for the maintenance routines to be performed. The time is based on the Identity Audit server's local time. At the scheduled maintenance time, a stored procedure runs to add partitions to the database. Two hours later, a stored procedure runs to archive or delete data older than the configured number of days.

Data archiving should be planned for a time of day when the database usage is relatively low.

7.3 Database Setup

The installer creates and configures a PostgreSQL database with a predefined structure, users, and stored procedures.

- ◆ [Section 7.3.1, "Database Structure," on page 60](#)

- ♦ [Section 7.3.2, “Database Users,” on page 60](#)
- ♦ [Section 7.3.3, “Database Stored Procedures,” on page 60](#)

7.3.1 Database Structure

The database for this security and information event management system created by the installer is named SIEM, and the default tablespace is named SENDATA1.

The eight largest tables in the database, which store events, events on which actions have taken place, and aggregated events, are partitioned by day to enable easy management and querying.

7.3.2 Database Users

There are several users created by default:

dbauser: This user is the database owner (database administrator user) and the password is set during the installation process.

appuser: This user is used by the Identity Audit server process (the ConnectionManager) to log into the database. The password is randomly generated during the installation process, and it is intended for internal use only.

admin: This user is the administrator and can be used to log into the Identity Audit Web interface. The password is set during the installation process.

7.3.3 Database Stored Procedures

At the scheduled maintenance time a job runs to determine whether to add new partitions to the database. The number of partitions added is governed by the data storage configuration settings, which are stored in the ESEC_JOB_CONFIG table in the database. The following settings are in this table:

ADD_MIN: If there are fewer than this number of future (empty) partitions in the database (7, by default), the stored procedure ESEC_ADD_REQUIRED_PARTITION adds new partitions to the database.

ADD_MAX: Two hours after the scheduled maintenance time, the stored procedure ESEC_OFFLINE_PARTITIONS runs to archive or delete all data older than the time period configured by the administrator. At this time, the following things happen:

1. The archived data is written to flat files in the specified archive directory
2. The archive operation is logged to the ESEC_JOB_STS table in the database
3. The archived data is deleted from the database
4. The search indexes are updated to remove indexes for data that have been removed from the database

There are two aggregation tables that are used for default reports. The aggregation service is enabled by default for EventDestSummary (for Target data) and EventSourceSummary (for Initiator data).

This section describes the event channels that can be used to send events from Identity Audit to another system.

- ♦ [Section 8.1, “Rules Overview,” on page 61](#)
- ♦ [Section 8.2, “Configuring Rules,” on page 62](#)
- ♦ [Section 8.3, “Configuring Actions,” on page 64](#)

8.1 Rules Overview

The Rules interface provides the ability to define rules to evaluate all incoming events and deliver selected events to designated output channels. For example, each severity 5 event can be e-mailed to a security analysts distribution list or an administrator.

NOTE: All events are also delivered to the database.

An incoming event is evaluated against each filtering rule in order until a match is found, and then the delivery actions associated with that rule are executed:

Send to e-mail: Send the event to a user or users by using a configured SMTP relay

Write to File: Write the event to a specified file on the Identity Audit server

Send to Syslog: Forward the event to a configured syslog server

TIP: Events are processed by the associated actions one at a time. You should therefore consider performance implications when selecting which output channel to which events are sent. For example, the Write to File action is the least resource-intensive, so it can be used to test rule criteria to determine the data volume before sending a flood of events to e-mail or syslog.

Also, when you set up the *Send to e-mail* action, you should consider how many events the recipient can effectively handle and adjust the filtering on the rule accordingly.

Event output is in JavaScript* Object Notation (JSON) which is a lightweight data exchange format. Events consist of field names (such as “evt” for Event Name) followed by a colon and a value (such as “Start”), separated by commas.

```
{"st":"I","evt":"Start","sev":"1","sres":"Collector","res":"CollectorManager",
"rv99":"0","rv1":"0","repassetid":"0","rv77":"0","agent":"Novell
SecureLogin","obsassetid":"0","vul":"0","port":"Novell
SecureLogin","msg":"Processing started for Collector Novell SecureLogin (ID
D892E9F0-3CA7-102B-B5A1-005056C00005).","dt":"1224204655689","id":"751D97B0-
7E13-112B-B933-000C29E8CEDE","src":"D892E9F0-3CA7-102B-B5A2-005056C00004"}
```

8.2 Configuring Rules

Identity Audit rules can be configured to filter events based on one or more of the searchable fields. For a list of the Identity Audit searchable event fields, see [Table 6-1 on page 52](#). Each rule can be associated with one or more of the configured actions.

- ◆ [Section 8.2.1, “Filter Criteria,” on page 62](#)
- ◆ [Section 8.2.2, “Adding a Rule,” on page 62](#)
- ◆ [Section 8.2.3, “Ordering Rules,” on page 63](#)
- ◆ [Section 8.2.4, “Editing a Rule,” on page 63](#)
- ◆ [Section 8.2.5, “Deleting a Rule,” on page 63](#)
- ◆ [Section 8.2.6, “Activating or Deactivating a Rule,” on page 63](#)

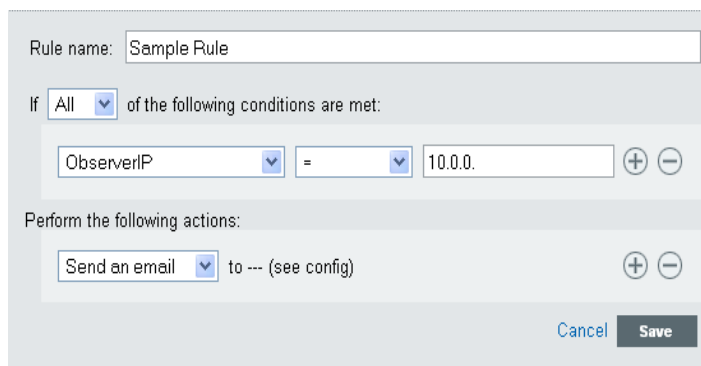
8.2.1 Filter Criteria

Rules can be based on any searchable event field. For a list of these fields, see [Table 6-1 on page 52](#). The available operators depend on the data type of the event field. For example, `match_subnet` is available for IP addresses, and `match_regex` is available for text fields.

8.2.2 Adding a Rule

Administrators can add a filter-based rule and then define one or more channels to which to output the events that meet the rule criteria.

- 1 Log into Identity Audit as an administrator.
- 2 Click *Rules* in the upper right corner of the page.
- 3 Click *Add Rule*.
- 4 Specify a rule name.
- 5 If you will create multiple conditions, select *All* to join the conditions with an AND operator. Select *Any* to join the conditions with an OR operator.
- 6 Select the event field, the operator, and the value for the filter.



The screenshot shows a web-based configuration form for adding a rule. At the top, there is a text input field labeled "Rule name:" containing the text "Sample Rule". Below this, there is a section for filter criteria. It starts with "If" followed by a dropdown menu set to "All", and the text "of the following conditions are met:". Underneath, there is a row of three dropdown menus: the first is set to "ObserverIP", the second is set to "=", and the third is set to "10.0.0.". To the right of these dropdowns are two small circular buttons with "+" and "-" signs. Below the filter criteria section, there is a section for actions. It starts with "Perform the following actions:". Underneath, there is a row of two dropdown menus: the first is set to "Send an email" and the second is set to "to --- (see config)". To the right of these dropdowns are two small circular buttons with "+" and "-" signs. At the bottom right of the form, there are two buttons: "Cancel" and "Save".

- 7 Select an action that will be performed on every event that meets the filter criteria. The action details are based on the configuration information seen if you click the *Configuration* link.

- 8 Configure additional actions, as desired.
- 9 Click *Save*.

8.2.3 Ordering Rules

Because events are evaluated by rules in order until a match is made, you should order rules accordingly. More narrowly defined rules and more important rules should be placed at the beginning of the list. When there is more than one rule, rules can be reordered by using drag-and-drop.

To reorder rules:

- 1 Log into Identity Audit as an administrator.
- 2 Click *Rules* in the upper right corner of the page.
- 3 Mouse over the icon to the left of the rule numbering to enable drag-and-drop. The cursor changes.

Rules [Configuration](#)

	On	Name		
⇅ 1	<input checked="" type="checkbox"/>	High Severity Events	edit	remove
≡ 2	<input checked="" type="checkbox"/>	Login Failures	edit	remove

[Add Rule](#)

- 4 Drag and drop the rule to the correct place in the ordered list.

8.2.4 Editing a Rule

Click the *edit* link beside the rule to change a rule definition.

8.2.5 Deleting a Rule

Click the *remove* link beside the rule to delete it. If there are already events in queue for an action or actions when you delete a rule, it might take some time to flush that queue after the rule is deactivated.

8.2.6 Activating or Deactivating a Rule

To the left of each rule, in a column headed *On*, is a check box to activate that rule. New rules are activated by default. If you deactivate a rule, incoming events are no longer evaluated according to that rule. If there are already events in queue for an action or actions, it might take some time to flush that queue after the rule is deactivated.

8.3 Configuring Actions

An event is delivered to one or more channels when it meets the criteria specified by one of the rules. Before the events can be output to a channel, the action to send to that channel must be configured with the appropriate connection information (and authentication credentials, if needed for the SMTP relay). The Identity Audit system can have only one configured connection per action type (for example, all events that are written to a file must be written to the same file).

- ♦ [Section 8.3.1, “Send to E-Mail,” on page 64](#)
- ♦ [Section 8.3.2, “Send to Syslog,” on page 65](#)
- ♦ [Section 8.3.3, “Write to File,” on page 65](#)

8.3.1 Send to E-Mail

To configure the *Send to e-mail* action, you need the connection information for an SMTP relay (IP address and port number), and the To and From addresses. You can send to more than one e-mail address by entering a comma-separated list.

NOTE: To avoid overwhelming your SMTP relay or e-mail recipients, this action should only be used with rules that generate a low volume of events.

This SMTP relay configuration is also used to deliver reports to users.

- 1 Log into Identity Audit as an administrator.
- 2 Click *Rules* in the upper right corner of the page.
- 3 Click *Configuration*.
- 4 Under *e-mail*, enter the name and port of an available SMTP relay. If desired, click *Test* to validate the hostname or IP address, port, username, and password fields.

The *Test* button does not actually send a test e-mail message.

Email

SMTP:	<input type="text" value="mail.company.com"/>	Port:	<input type="text" value="25"/>	<input type="button" value="Test"/>
test successful. ✓				
Username:	<input type="text"/>	Password:	<input type="password"/>	
From:	<input type="text" value="IdentityAudit@company.com"/>			
Send to:	<input type="text" value="jabbott@company.com"/>			

Separate multiple email addresses with a comma.

- 5 If the SMTP relay requires authentication, specify a username and password.
- 6 Specify an address from which the e-mail messages will come.
- 7 Specify one or more e-mail addresses, separated by commas.
- 8 Click *Save*.

All Identity Audit events meeting the filter criteria for which the *Send to e-mail* action is defined are sent to the same SMTP relay and set of addresses.

8.3.2 Send to Syslog

To configure the *Send to Syslog* action, you need the connection information for the syslog server (IP address and port number).

- 1 Log into Identity Audit as an administrator.
- 2 Click *Rules* in the upper right corner of the page.
- 3 Click *Configuration*.
- 4 Under *Syslog*, specify a name or IP address and open UDP port of a syslog server. If desired, click *Test* to test that the destination server and port are formatted correctly.

Syslog

Destination:	<input type="text" value="localhost"/>	Port:	<input type="text" value="514"/>	Test
--------------	--	-------	----------------------------------	-------------

- 5 Click *Save*.

All Identity Audit events meeting the filter criteria for which the *Send to Syslog* action is defined are sent to the same syslog server.

8.3.3 Write to File

To configure the *Write to File* action, you need the name and path of the file to which the events will be written. The directory must already exist and the novell user must have permissions to write to it. If the file does not already exist, Identity Audit creates it.

- 1 Log into Identity Audit as an administrator.
- 2 Click *Rules* in the upper right corner of the page.
- 3 Click *Configuration*.
- 4 Under *Filename*, specify the path to the file to which you want the events to be written, either an absolute path or a relative path (where the working directory is data under the application's home directory). If desired, click *Test* to test permissions and create a zero-byte file to hold the data.

Filename

Destination:	<input type="text" value="../data/log_to_file_events.txt"/>	Test
--------------	---	-------------

- 5 Click *Save*.

All Identity Audit events meeting the filter criteria for which the *Write to File* action is defined are written to the same file.

User Administration

9

Administrators can add, edit, and delete users in Novell® Identity Audit and grant administrative rights. Users can edit the details of their own user profile.

- ♦ [Section 9.1, “Adding a User,” on page 67](#)
- ♦ [Section 9.2, “Editing User Details,” on page 68](#)
- ♦ [Section 9.3, “Deleting a User,” on page 70](#)

9.1 Adding a User

Adding a user in the Identity Audit system creates an application user who can then log into the Identity Audit application.

Selecting the *Grant administrative rights* option gives the user administrative rights in the Identity Audit system. Administrative rights include the ability to manage the following functions:

- ♦ User Administration
- ♦ Data Collection
- ♦ Data Storage
- ♦ Rules

To add a user:

- 1 Log into Identity Audit as an administrator.
- 2 Click *User Admin* in the upper right corner of the page.
- 3 Click *Add a user*.
- 4 Specify the user information.

User Admin

Provide the name and email address of the user.

First Name:	<input type="text"/>
Last Name:	<input type="text"/>
Email:	<input type="text"/>
<input type="checkbox"/>	Grant administrative rights

Choose a username and password for this user.

Username: *	<input type="text"/>
Password: *	<input type="text"/>
Verify: *	<input type="text"/>

The fields with an asterisk (*) are required, and the username must be unique.

The e-mail address format is validated, but the phone number fields allow any format. Be sure you enter a valid phone number.

5 (Optional) Select *Grant administrative rights*.

6 Click *Save*.

9.2 Editing User Details

Administrators can edit user information for any user in the system. Users can edit their own profiles except for the username and administrative privileges.

- ♦ [Section 9.2.1, “Editing Your Own Profile,” on page 68](#)
- ♦ [Section 9.2.2, “Changing Your Own Password,” on page 69](#)
- ♦ [Section 9.2.3, “Editing Another User’s Profile \(admin only\),” on page 70](#)
- ♦ [Section 9.2.4, “Resetting Another User’s Password \(admin only\),” on page 70](#)

9.2.1 Editing Your Own Profile

1 Click *profile* in the upper right corner.

Novell.Scout Data Collection

Reports

Search

User Profile

First Name:

Last Name:

Email:

Allow user to Administer Scout

Change your password using these fields. Leave them blank to keep your current password.

Username:

Current Password

Password:

Verify:

The following information is optional, but could come in handy if someone needs to contact you directly.

Title:

Office #: ext.

Mobile #:

Fax #:

Cancel

- 2 Edit any available field.
- 3 Click *Save*.

9.2.2 Changing Your Own Password

You can change your own password if you know the current password. Otherwise, an administrator must reset the password.

- 1 Click *profile* in the upper right corner.
- 2 Enter your current password.
- 3 Enter your new password.

- 4 Confirm your new password.
- 5 Click *Save*.

9.2.3 Editing Another User's Profile (admin only)

- 1 Log into Identity Audit as an administrator.
- 2 Click *User Admin* in the upper right corner of the page.
- 3 Click *Edit* under the user you want to edit.
- 4 Edit any fields (except the username).
- 5 Click *Save*.

Changes to *Grant Administrative Rights* take effect the next time the user logs in.

9.2.4 Resetting Another User's Password (admin only)

To reset another user's password, see [Section 9.2.3, "Editing Another User's Profile \(admin only\),"](#) on page 70.

9.3 Deleting a User

Administrators can delete a user from the system.

- 1 Log into Identity Audit as an administrator.
- 2 Click *User Admin* in the upper right corner of the page.
- 3 Click *Edit* under the user you want to delete.
- 4 Click *Delete this user* in the upper right corner of the page.
- 5 Click *Delete* to confirm.

Troubleshooting

A

Log files are located in the `./identity_audit/log` directory. There are logs for Identity Audit and the ActiveMQ* message bus, PostgreSQL database, JasperReports server, and Tomcat Web server. Most of the logs are numbered because they rotate.

Table A-1 Log Files in Identity Audit

Log File Name	Purpose
<code>activemq.log</code>	Logs for the message bus.
<code>db.1.log</code> (through <code>db.7.log</code>)	Database logs for the most recent Monday (through Sunday).
<code>db_start.log</code>	Startup logs for PostgreSQL database.
<code>db_stop.log</code>	Shutdown logs for PostgreSQL database.
<code>server0.*.log</code>	Logs for Identity Audit server process, including search and reporting messages. Logging properties for this log are set in the <code>config/server_log.prop</code> file. These changes take effect immediately.
<code>server_wrapper.log</code>	Logs for Identity Audit wrapper process, which owns the server process.
<code>admin.date.log</code>	Logs for the Web server. Located in the <code>./tomcat</code> directory.
<code>catalina.date.log</code>	Logs for the Web server, including events related to the servlets that upload report plug-ins and manage viewing for report results, report samples, and report help files. Located in the <code>./tomcat</code> directory. Logging properties for this log are set in the <code>3rdparty/tomcat/conf/logging.properties</code> file. These changes take effect after Tomcat is restarted.
<code>host-manager.date.log</code>	Logs for the Web server. Located in the <code>./tomcat</code> directory.
<code>localhost.date.log</code>	Logs for the Web server. Located in the <code>./tomcat</code> directory.
<code>manager.date.log</code>	Logs for the Web server. Located in the <code>./tomcat</code> directory.

The following logging settings can be changed in the `config/server_log.prop` file:

- ◆ `esecurity.ccs.comp.reporting.jasper=ALL` (reporting)
- ◆ `com.novell.reports.jasper=ALL` (reporting)
- ◆ `esecurity.ccs.comp.scheduler.level=ALL` (report scheduling)
- ◆ `esecurity.ccs.comp.textsearch.level=ALL` (searching)

The following logging settings can be changed in the `3rdparty/tomcat/conf/logging.properties` file:

- ◆ `com.novell.sentinel.scout.server.ReportUploadServlet.level=ALL`

- ◆ `com.novell.sentinel.scout.server.ReportViewServlet.level=ALL`
- ◆ `com.novell.sentinel.scout.server.level=ALL` (this is equivalent to the previous two settings)

Truststore

B

Using strict authentication for the connection between Identity Audit and the Novell applications it collects data from can improve data security.

B.1 Creating a Keystore

A keystore can be created using the Java* “keytool” executable, which comes with any JRE* installation. This keystore holds a public and private keypair that can be used to replace the default certificate that comes with Identity Audit. There are basic instructions below, but for more info on keytool, see the [Sun* Web site \(http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html\)](http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html).

- 1 Go to the `/bin` directory for Java (for example, `$JAVA_HOME/bin`).
- 2 Run the following command:

```
keytool -genkey -alias alias -keystore .keystore
```
- 3 Enter a password for the keystore. This password is used when you import the truststore.
- 4 Enter the following information:
 - ♦ First and last name
 - ♦ Organizational unit
 - ♦ Organization
 - ♦ City or locality
 - ♦ State or province
 - ♦ Two-digit country code
- 5 Verify the information.
- 6 Press Enter to use the same password as the keystore password.

A `.keystore` file is created with a private key and corresponding public key (certificate).

Novell Identity Audit Database Views for PostgreSQL Server



This section lists the Novell Identity Audit Schema Views for PostgreSQL Server.

C.1 Views

Below listed are the views available with Identity Audit.

C.1.1 ACTVY_PARM_RPT_V

Column Name	Datatype	Comment
ACTVY_PARM_ID	uuid	Activity parameter identifier
ACTVY_ID	uuid	Activity identifier
PARM_NAME	character varying(255)	Activity Parameter name
PARM_TYP_CD	character varying(1)	Activity parameter type code
DATA_TYP	character varying(50)	Activity parameter data type
DATA_SUBTYP	character varying(50)	Activity parameter data subtype
RQRD_F	boolean	Required flag
PARM_DESC	character varying(255)	Activity parameter description
PARM_VAL	character varying(1000)	Activity parameter value
FORMATTER	character varying(255)	Activity parameter formatter
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.2 ACTVY_REF_PARM_VAL_RPT_V

Column Name	Datatype	Comment
ACTVY_ID	uuid	Activity identifier
SEQ_NUM	integer	Sequence number
ACTVY_PARM_ID	uuid	Activity parameter identifier
PARM_VAL	character varying(1000)	Activity parameter value

Column Name	Datatype	Comment
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.3 ACTVY_REF_RPT_V

Column Name	Datatype	Comment
ACTVY_ID	uuid	Activity identifier
SEQ_NUM	integer	Sequenece number
REFD_ACTVY_ID	uuid	Referenced activity identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.4 ACTVY_RPT_V

Column Name	Datatype	Comment
ACTVY_ID	uuid	Activity identifier
ACTVY_NAME	character varying(255)	Activity name
ACTVY_TYP_CD	character varying(1)	Activity type code
ACCESS_LVL	character varying(50)	Access level
EXEC_LOC	character varying(50)	Execution location
ACTVY_DESC	character varying(255)	Activity description
PROCESSOR	character varying(255)	Processor
INPUT_FORMATTER	character varying(255)	Input formatter
OUTPUT_FORMATTER	character varying(255)	Output formatter
APP_NAME	character varying(25)	Application name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.5 ADV_ATTACK_MAP_RPT_V

View references ADV_ATTACK_MAP table that stores Advisor map information.

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

C.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	integer	ID used to reference the vulnerability entry
SERVICE_PACK_ID	integer	Service Pack ID of the product that is identified this vulnerability
PLUGIN_ID	character varying(256)	ID of the vulnerability
PLUGIN_NAME	character varying(256)	Name of the vulnerability
DATE_PUBLISHED	timestamp with time zone	Date the vulnerability has been published
DATE_UPDATED	timestamp with time zone	Date the vulnerability has been updated
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.7 ADV_ATTACK_RPT_V

View references ADV_ATTACK table that stores Advisor attack information.

Column Name	Datatype	Comment
ATTACK_ID	integer	ID to identify the attack
TRUSECURE_ATTACK_NAME	character varying(512)	Name of the attack
FEED_DATE_CREATED	timestamp with time zone	Date when the feed first have the information on this attack
FEED_DATE_UPDATED	timestamp with time zone	Last date when the information on this attack has been updated
ATTACK_CATEGORY	character varying(256)	Category of the attack
URGENCY_ID	integer	The urgency associated with this attack
SEVERITY_ID	integer	Severity associated with this attack
LOCAL	integer	Indicates if this attack was executed locally
REMOTE	integer	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	timestamp with time zone	Date the information on this attack was published
DATE_UPDATED	timestamp with time zone	Date the information on this attack was updated
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.8 ADV_ATTACK_SIGNATURES

Column Name	Datatype	Comment
ATTACK_KEY	integer	Attack ID

Column Name	Datatype	Comment
ATTACK_SCANNER_NAME	character varying(128)	Name of the attack scanner or intrusion detection system
ATTACK_NAME	character varying(256)	Name of the attack
ATTACK_ID	character varying(256)	ID of the attack

C.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	character varying(128)	Name of feed
FEED_FILE	character varying(256)	File name that contains the feed data
BEGIN_DATE	timestamp with time zone	The date from which this feed file carries the advisor information
END_DATE	timestamp with time zone	The date until which this feed file carries the advisor information
FEED_INSERT	integer	Number of rows inserted into the advisor schema by this feed file
FEED_UPDATE	integer	Number of rows updated into the advisor schema by this feed file
FEED_EXPIRE	integer	Number of rows deleted into the advisor schema by this feed file

C.1.10 ADV_MASTER_RPT_V

Column Name	Datatype	Comment
MASTER_ID	integer	ID that associates PLUGIN_KEY, ATTACK_KEY and VULN_KB_ID
PLUGIN_KEY	integer	ID to reference the ADV_ATTACK_PLUGIN_V
ATTACK_KEY	integer	ID to reference the ADV_ATTACK_MAP_V
VULN_KB_ID	integer	ID to reference the VULN_KB_ID_V
DATE_PUBLISHED	timestamp with time zone	Date the entry was published
DATE_UPDATED	timestamp with time zone	Date the entry was updated
BEGIN_EFFECTIVE_DATE	timestamp with time zone	Date from which the entry is valid
END_EFFECTIVE_DATE	timestamp with time zone	Date until which the entry is valid
DATE_CREATED	timestamp with time zone	Date the entry was created

Column Name	Datatype	Comment
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	integer	ID of the product
VENDOR_ID	integer	ID of the vendor
PRODUCT_CATEGORY_ID	integer	ID of the Product Category
PRODUCT_CATEGORY_NAME	character varying(128)	Product Category Name
PRODUCT_TYPE_ID	integer	ID of the product type
PRODUCT_TYPE_NAME	character varying(256)	Name of the Product Type
PRODUCT_NAME	character varying(128)	Product Name
PRODUCT_DESCRIPTION	character varying(512)	Product Description
FEED_DATE_CREATED	timestamp with time zone	Date of the Feed that carried information on this product
FEED_DATE_UPDATED	timestamp with time zone	Date of the Feed that updated information on this product
ACTIVE_FLAG	integer	Reserved for future use
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	integer	Service Pack ID
VERSION_ID	integer	Version ID
SERVICE_PACK_NAME	character varying(32)	Name of the Service Pack

Column Name	Datatype	Comment
FEED_DATE_CREATED	timestamp with time zone	Date of the Feed that carried information on this product
FEED_DATE_UPDATED	timestamp with time zone	Date of the Feed that updated information on this product
ACTIVE_FLAG	integer	Reserved for future use
BEGIN_EFFECTIVE_DATE	timestamp with time zone	Date from which the entry is valid
END_EFFECTIVE_DATE	timestamp with time zone	Date until which the entry is valid
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	integer	Version ID
PRODUCT_ID	integer	Product ID
VERSION_NAME	character varying(128)	Version Name of the product
FEED_DATE_CREATED	timestamp with time zone	Date of the feed that carried the information on the entry
FEED_DATE_UPDATED	timestamp with time zone	Date of the feed that carried the update on the entry
ACTIVE_FLAG	integer	Reserved for future use
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.14 ADV_VENDOR_RPT_V

Column Name	Datatype	Comment
VENDOR_ID	bigint	ID of the vendor
VENDOR_NAME	character varying(128)	Name of the vendor

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

C.1.15 ADV_VULN_KB_RPT_V

Column Name	Datatype	Comment
VULN_KB_ID	integer	Knowledge base ID mapping CVE_ID, OSVDB_ID, BUGTRAQ_ID
CVE_ID	integer	CVE ID for the related vulnerability
OSVDB_ID	integer	OSVDB ID for the related vulnerability
BUGTRAQ_ID	integer	Bugtraq id for the related vulnerability
DATE_PUBLISHED	timestamp with time zone	Date the entry was published

Column Name	Datatype	Comment
DATE_UPDATED	timestamp with time zone	Date the entry was updated
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	integer	Contains the service pack id
ATTACK_ID	integer	Contains the attack id
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.17 ADV_VULN_SIGNATURES

Column Name	Datatype	Comment
VULN_KEY	integer	Vulnerability key
VULN_SCANNER_NAME	character varying(128)	Vulnerability scanner name
VULN_NAME	character varying(256)	Vulnerability name
VULN_ID	character varying(256)	Vulnerability ID

C.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	integer	Annotation identifier - sequence number.
TEXT	character varying(4000)	Documentation or notes.
ACTION	character varying(255)	Action

Column Name	Datatype	Comment
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
MODIFIED_BY	integer	User who last modified object
CREATED_BY	integer	User who created object

C.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	character varying(100)	Asset category name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	uuid	Asset alternate hostname identifier
PHYSICAL_ASSET_ID	uuid	Physical asset identifier
HOST_NAME	character varying(255)	Host name
CUST_ID	bigint	Customer identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	uuid	Asset alternate IP identifier
PHYSICAL_ASSET_ID	uuid	Physical asset identifier
IP_ADDRESS	integer	Asset IP address
CUST_ID	bigint	Customer identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	character varying(255)	Building name
ADDRESS_LINE_1	character varying(255)	Address line 1
ADDRESS_LINE_2	character varying(255)	Address line 2
CITY	character varying(100)	City
STATE	character varying(100)	State
COUNTRY	character varying(100)	Country
ZIP_CODE	character varying(50)	Zip code
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.23 ASSET_RPT_V

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

Column Name	Datatype	Comment
ASSET_ID	uuid	Asset identifier
CUST_ID	bigint	Customer identifier
ASSET_NAME	character varying(255)	Asset name
PHYSICAL_ASSET_ID	uuid	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	boolean	Physical asset indicator
ASSET_VALUE_CODE	bigint	Asset value code
CRITICALITY_ID	bigint	Asset criticality code
SENSITIVITY_ID	bigint	Asset sensitivity code
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	character varying(50)	Asset value name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	uuid	Person identifier

Column Name	Datatype	Comment
ORGANIZATION_ID	uuid	Organization identifier
ROLE_CODE	character varying(5)	Role code
ASSET_ID	uuid	Asset identifier
ENTITY_TYPE_CODE	character varying(5)	Entity type code
PERSON_ROLE_SEQUENCE	integer	Order of persons under a particular role
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	character varying(64)	Table name 1. For example, incidents
ID1	integer	ID1. For example, incident ID.
TABLE2	character varying(64)	Table name 2. For example, users.
ID2	integer	ID2. For example, user ID.
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.27 ATTACHMENTS_RPT_V

View references ATTACHMENTS table that stores attachment data.

Column Name	Datatype	Comment
ATTACHMENT_ID	integer	Attachment identifier
NAME	character varying(255)	Attachment name
SOURCE_REFERENCE	character varying(64)	Source reference
TYPE	character varying(32)	Attachment type
SUB_TYPE	character varying(32)	Attachment subtype
FILE_EXTENSION	character varying(32)	File extension

Column Name	Datatype	Comment
ATTACHMENT_DESCRIPTION	character varying(255)	Attachment description
DATA	text	Attachment data
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.28 AUDIT_RECORD_RPT_V

View reference AUDIT_RECORD table that stores Sentinel internal audit data.

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

C.1.29 CONFIGS_RPT_V

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

Column Name	Datatype	Comment
USR_ID	character varying(32)	User name.

Column Name	Datatype	Comment
APPLICATION	character varying(255)	Application identifier
UNIT	character varying(64)	Application unit
VALUE	character varying(255)	Text value if any
DATA	text	XML data
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.30 CONTACTS_RPT_V

View references CONTACTS table that stores contact information.

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

C.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.

C.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	uuid	Event Universal Unique Identifier (UUID) of parent event
CHILD_EVT_ID	uuid	Event Universal Unique Identifier (UUID) of child event
PARENT_EVT_TIME	timestamp with time zone	Parent event time
CHILD_EVT_TIME	timestamp with time zone	Child event time
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	character varying(50)	Asset criticality name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	character varying(255)	Customer
CUST_HIERARCHY_LVL1	character varying(255)	Customer hierarchy level 1
CUST_HIERARCHY_LVL2	character varying(255)	Customer hierarchy level 2
CUST_HIERARCHY_LVL3	character varying(255)	Customer hierarchy level 3
CUST_HIERARCHY_LVL4	character varying(255)	Customer hierarchy level 4
DATE_CREATED	timestamp with time zone	Date the entry was created

Column Name	Datatype	Comment
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	character varying(255)	Customer name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	character varying(5)	Entity type code
ENTITY_TYPE_NAME	character varying(50)	Entity type name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	character varying(255)	Environment identity name

Column Name	Datatype	Comment
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.38 ESEC_CONTENT_GRP_CONTENT_RPT_V

Column Name	Datatype	Comment
CONTENT_GRP_ID	uuid	Content group identifier
CONTENT_ID	character varying(255)	Content identifier
CONTENT_TYP	character varying(100)	Content type
CONTENT_HASH	character varying(255)	Content hash
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.39 ESEC_CONTENT_GRP_RPT_V

Column Name	Datatype	Comment
CONTENT_GRP_ID	uuid	Content group identifier
CONTENT_GRP_NAME	character varying(255)	Content group name
CONTENT_GRP_DESC	text	Content group description
CTRL_ID	uuid	Control identifier
CONTENT_EXTERNAL_ID	character varying(255)	Content external identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.40 ESEC_CONTENT_PACK_RPT_V

Column Name	Datatype	Comment
CONTENT_PACK_ID	uuid	Content pack identifier
CONTENT_PACK_DESC	text	Content pack description
CONTENT_PACK_NAME	character varying(255)	Content pack name
CONTENT_EXTERNAL_ID	character varying(255)	Content external identifier
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
DATE_CREATED	timestamp with time zone	Date the entry was created
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.41 ESEC_CONTENT_RPT_V

Column Name	Datatype	Comment
CONTENT_ID	character varying(255)	Content identifier
CONTENT_NAME	character varying(255)	Content name
CONTENT_DESC	text	Content description
CONTENT_STATE	integer	Content state
CONTENT_TYP	character varying(100)	Content type
CONTENT_CONTEXT	text	Content cotext
CONTENT_HASH	character varying(255)	Content hash
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
MODIFIED_BY	integer	User who last modified object
CREATED_BY	integer	User who created object

C.1.42 ESEC_CTRL_CTGRY_RPT_V

Column Name	Datatype	Comment
CTRL_CTGRY_ID	uuid	Control category identifier
CTRL_CTGRY_DESC	text	Control category description
CTRL_CTGRY_NAME	character varying(255)	Control category name
CONTENT_PACK_ID	uuid	Content pack identifier

Column Name	Datatype	Comment
CONTENT_EXTERNAL_ID	character varying(255)	Content external identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.43 ESEC_CTRL_RPT_V

Column Name	Datatype	Comment
CTRL_ID	uuid	Control identifier
CTRL_NAME	character varying(255)	Control name
CTRL_DESC	text	Control description
CTRL_STATE	integer	Control state
CTRL_NOTES	text	Control notes
CTRL_CTGRY_ID	uuid	Control category identifier
CONTENT_EXTERNAL_ID	character varying(255)	Content external identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	character varying(32)	The parent object of the property
TAG	character varying(32)	The native tag name of the property
LABEL	character varying(32)	The display string of tag.
POSITION	integer	Position of tag within display.
WIDTH	integer	The column width
ALIGNMENT	integer	The horizontal alignment
FORMAT	integer	The enumerated formatter for displaying the property

Column Name	Datatype	Comment
ENABLED	boolean	Indicates if the tag is shown.
TYPE	integer	Indicates datatype of tag. 1 = string 2 = ulong 3 = date 4 = uuid 5 = ipv4
DESCRIPTION	character varying(255)	Textual description of the tag
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
REF_CONFIG	character varying(4000)	Referential data configuration

C.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	integer	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	integer	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	character varying(64)	Per http://www.iana.org/assignments/port-numbers (http://www.iana.org/assignments/port-numbers), the keyword representation of the port.
PORT_DESCRIPTION	character varying(512)	Port description.
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified

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

C.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	integer	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	character varying(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	character varying(512)	IP packet protocol description.
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	character varying(32)	Name of the table.
COLUMN_NAME	character varying(255)	Name of the column
SEED	integer	Current value of primary key field.
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.48 ESEC_UUID_UUID_ASSOC_RPT_V

Column Name	Datatype	Comment
OBJECT1	character varying(64)	Object 1
ID1	uuid	UUID for object 1
OBJECT2	character varying(64)	Object 2
ID2	uuid	UUID for object 2
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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).

C.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.

C.1.51 EVENTS_ALL_V (legacy view)

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

C.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.

C.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.

C.1.54 EVENTS_RPT_V2

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

Column Name	Datatype	Comment
EVENT_ID	uuid	Event identifier

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

Column Name	Datatype	Comment
EXTENDED_INFO	character varying(1000)	Extended information
CUSTOM_TAG_1	character varying(255)	Customer Tag 1
CUSTOM_TAG_2	character varying(255)	Customer Tag 2
CUSTOM_TAG_3	integer	Customer Tag 3
RESERVED_TAG_1	character varying(255)	Reserved Tag 1 Reserved for future use by Sentinel. This field is used for Advisor information concerning attack descriptions.
RESERVED_TAG_2	character varying(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	integer	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	integer	Vulnerability rating
CRITICALITY_RATING	integer	Criticality rating
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	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 Sentinel. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV11 - 20	timestamp with time zone	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	uuid	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.

Column Name	Datatype	Comment
RV26 - 31	character varying(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	character varying(255)	Reserved Value 33 Reserved for EventContext Use of this field for any other purpose might result in data being overwritten by future functionality.
RV34	character varying(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	character varying(255)	Reserved Value 35 Reserved for SourceUserCotext. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV36	character varying(255)	Reserved Value 36 Reserved for DataCotext. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV37	character varying(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	character varying(255)	Reserved Value 38 Reserved for SourceOperationalCotext. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV40 - 43	character varying(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.

Column Name	Datatype	Comment
RV44	character varying(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	character varying(255)	Reserved Value 45 Reserved for DestinationUserCotext. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV46	character varying(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	character varying(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	character varying(255)	Reserved Value 48 Reserved for DestinationOperationalCotext. Use of this field for any other purpose might result in data being overwritten by future functionality.
RV49	character varying(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.
TAXONOMY_ID	bigint	Taxonomy ID
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	integer	Custom Value 1 - 10 Reserved for use by Customer, typically for association of Business relevant data

Column Name	Datatype	Comment
CV11 - 20	timestamp with time zone	Custom Value 11 - 20 Reserved for use by Customer, typically for association of Business relevant data
CV21 - 29	character varying(255)	Custom Value 21 – 29 Reserved for use by Customer, typically for association of Business relevant data
CV30 - 34	character varying(4000)	Custom Value 30 – 34 Reserved for use by Customer, typically for association of Business relevant data
CV35 - 100	character varying(255)	Custom Value 35 – 100 Reserved for use by Customer, typically for association of Business relevant data

C.1.55 EVENTS_RPT_V3

Column Name	Datatype	Comment
Event_ID	uuid	Event identifier
Resource_Name	character varying(255)	Resource name
Sub_Resource	character varying(255)	Subresource name
Severity	integer	Event severity
Event_Parse_Time	timestamp with time zone	Event time
Event_datetime	timestamp with time zone	Event date time
Event_Device_Time	timestamp with time zone	Event device time
Sentinel_Process_Time	timestamp with time zone	Sentinel process time
Begin_Time	timestamp with time zone	Events begin time
End_Time	timestamp with time zone	Events end time
repeat_count	integer	Repeat count
Target_Service_Port	integer	Target service port
Event_Time	character varying(255)	Event time
Init_Asset_id	bigint	Initiator asset identifier
Target_Asset_id	bigint	Target asset identifier
Target_IP	integer	Target IP address in numeric format
Target_IP_Dotted	character varying(16)	Target IP address in dotted format
Target_Host_Name	character varying(255)	Target host name

Column Name	Datatype	Comment
Init_User_Name	character varying(255)	Initiator user name
Target_User_Name	character varying(255)	Target user name
File_Name	character varying(1000)	File name
Extended_Info	character varying(1000)	Extened information
Init_User_Id	character varying(255)	Initiator user ID
Init_Usr_Identity	uuid	Initiator user identity
Target_User_Id	character varying(255)	Target user ID
Target_User_Identity	uuid	Target user identity
Effective_User_Name	character varying(255)	Effective user name
Effective_User_Sys_Id	character varying(255)	Effective user ID
Effective_User_Domain	character varying(255)	Effective user domain
Target_Trust_Name	character varying(255)	Target trust name
Target_Trust_Sys_Id	character varying(255)	Target trust ID
Target_Trust_Domain	character varying(255)	Target trust domain
Observer_Ip	integer	Observer IP address in numeric format
Reporter_Ip	integer	Reporter IP address in numeric format
Observer_Host_Domain	character varying(255)	Observer host domain
Reporter_Host_Domain	character varying(255)	Reporter host domain
Observer_Asset_Id	character varying(255)	Observer asset identifier
Reporter_Asset_Id	character varying(255)	Reporter asset identifier
Init_Service_Comp	character varying(255)	Initiator service component
Target_Service_Comp	character varying(255)	Target service component
Custom_Tag_1	character varying(255)	Customer Tag 1
Custom_Tag_2	character varying(255)	Customer Tag 2
Custom_Tag_3	integer	Customer Tag 3
Reserved_Tag_1	character varying(255)	
Reserved_Tag_2	character varying(255)	
Reserved_Tag_3	integer	
Vulnerability_Rating	integer	
Criticality_Rating	integer	
Date_Created	timestamp with time zone	Date the entry was created
Date_Modified	timestamp with time zone	Date the entry was modified

Column Name	Datatype	Comment
Created_By	integer	User who created object
Modified_By	integer	User who last modified object
RV01	integer	
Event_Metric	integer	Event metric
Data_Tag_Id	integer	Data tag ID
RV04-RV10	integer	
RV11-RV20	timestamp with time zone	
RV21-RV28	character varying(255)	
Init_IP_Country	character varying(255)	Initiator country
Target_IP_Country	character varying(255)	Target country
RV31	character varying(255)	
RV33		
RV36		
RV40		
RV43		
RV46		
RV49		
Init_Threat_Level	character varying(255)	Initiator threat level
Init_User_Domain	character varying(255)	Initiator user domain
Init_Function	character varying(255)	Initiator function
Init_Operational_Cotext	character varying(255)	Initiator operational cotext
Target_Host_Domain	character varying(255)	Target host domain
Target_Threat_Level	character varying(255)	Target threat level
Target_User_Domain	character varying(255)	Target user domain
Target_Function	character varying(255)	Target function
Target_Operational_Cotext	character varying(255)	Target operational cotext
Taxonomy_id	bigint	Taxonomy identifier
Reference_id_1	bigint	
XDAS_Taxonomy_Id	bigint	XDAS Taxonomy identifier
Reference_id_2-Reference_id_20		
CV01-CV10	integer	
CV11-CV20	timestamp with time zone	

Column Name	Datatype	Comment
CV21-CV29	character varying(255)	
CV30-CV34	character varying(4000)	
CV35-CV100	character varying(255)	
Customer_Var_101- Customer_Var_110	integer	
Customer_Var_111- Customer_Var_120	timestamp with time zone	
Customer_Var_121- Customer_Var_130	uuid	
Customer_Var_131- Customer_Var_140	integer	
Customer_Var_141- Customer_Var_150	character varying(255)	

C.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	character varying(64)	Collector name
Port	character varying(64)	Collector port
Report_Name	character varying(255)	Reporter name
Product_Name	character varying(255)	Product name
Sensor_Name	character varying(255)	Sensor name
Sensor_Type	character varying(5)	Sensor type: H - host-based N - network-based V - virus O - other
Device_Category	character varying(255)	Device category
Source_UUID	uuid	Source component Universal Unique Identifier (UUID)
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified

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

C.1.57 EVT_AGENT_RPT_V3

Column Name	Datatype	Comment
Agent_ID	bigint	Collector identifier
Cust_ID	bigint	Customer identifier
Agent	character varying(64)	Collector
Port	character varying(64)	Port
Reporter_Host_Name	character varying(255)	Reporter host name
Sensor_Type	character varying(5)	Sensor type: H - host-based N - network-based V - virus O - other
Device_Category	character varying(255)	Device category
Source_UUID	uuid	Source component Universal Unique Identifier (UUID)
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	character varying(255)	Asset name
Physical_Asset_Name	character varying(255)	Physical asset name

Column Name	Datatype	Comment
Reference_Asset_ID	character varying(100)	Reference asset identifier, links to source asset management system.
Mac_Address	character varying(100)	MAC address
Rack_Number	character varying(50)	Rack number
Room_Name	character varying(100)	Room name
Building_Name	character varying(255)	Building name
City	character varying(100)	City
State	character varying(100)	State
Country	character varying(100)	Country
Zip_Code	character varying(50)	Zip code
Asset_Category_Name	character varying(100)	Asset category name
Network_Identity_Name	character varying(255)	Asset network identity name
Environment_Identity_Name	character varying(255)	Environment name
Asset_Value_Name	character varying(50)	Asset value name
Criticality_Name	character varying(50)	Asset criticality name
Sensitivity_Name	character varying(50)	Asset sensitivity name
Contact_Name_1	character varying(255)	Name of contact person/organization 1
Contact_Name_2	character varying(255)	Name of contact person/organization 2
Organization_Name_1	character varying(100)	Asset owner organization level 1
Organization_Name_2	character varying(100)	Asset owner organization level 2
Organization_Name_3	character varying(100)	Asset owner organization level 3
Organization_Name_4	character varying(100)	Asset owner organization level 4
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.59 EVT_ASSET_RPT_V3

Asset_Department	character varying(100)	Asset department
DATE_CREATED	timestamp with time zone	Date the entry was created

Asset_Department	character varying(100)	Asset department
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	integer	Destination IP address
Destination_Event_Asset_ID	bigint	Event asset identifier
Taxonomy_ID	bigint	Taxonomy identifier
Event_Name_ID	bigint	Event name identifier
Severity	integer	Event severity
CUST_ID	bigint	Customer identifier
Event_Tme	timestamp with time zone	Event time
Event_Count	integer	Event count
Date_Created	timestamp with time zone	Date the entry was created
Date_Modified	timestamp with time zone	Date the entry was modified
Created_By	integer	User who created object
Modified_By	integer	User who last modified object
Destination_Host_Name	character varying(255)	Destination host name

C.1.61 EVT_DEST_SMRY_1_RPT_V

View contains event destination summary information.

Column Name	Datatype	Comment
Destination_IP	integer	Destination IP address
Destination_Event_Asset_ID	bigint	Event asset identifier
Destination_Port	character varying(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

Column Name	Datatype	Comment
Agent_ID	bigint	Collector identifier
Protocol_ID	bigint	Protocol identifier
Severity	integer	Event severity
CUST_ID	bigint	Customer identifier
Event_Time	timestamp with time zone	Event time
XDAS_Taxonomy_id	bigint	XDAS taxonomy identifier
Target_User_Identity	uuid	Target user identity
Event_Count	integer	Event count
Date_Created	timestamp with time zone	Date the entry was created
Date_Modified	timestamp with time zone	Date the entry was modified
Created_By	integer	User who created object
Modified_By	integer	User who last modified object
Destination_Host_Name	character varying(255)	Destination host name

C.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	integer	Destination IP address
Destination_Event_Asset_ID	bigint	Event asset identifier
Taxonomy_ID	bigint	Taxonomy identifier
Severity	integer	Event severity
CUST_ID	bigint	Customer identifier
Event_Time	timestamp with time zone	Event time
XDAS_Taxonomy_id	bigint	XDAS taxonomy identifier
Event_Count	integer	Event count
Date_Created	timestamp with time zone	Date the entry was created
Date_Modified	timestamp with time zone	Date the entry was modified
Created_By	integer	User who created object
Modified_By	integer	User who last modified object
Destination_Host_Name	character varying(255)	Destination host name

C.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	character varying(255)	Event name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.64 EVT_PORT_SMRY_1

Column Name	Datatype	Comment
DEST_PORT	character varying(32)	Destination port
SEV	integer	Severity
CUST_ID	bigint	Customer identifier
EVT_TIME	timestamp with time zone	Event time
EVT_CNT	integer	Event count
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	character varying(32)	Destination port
Severity	integer	Event severity
Cust_ID	bigint	Customer identifier
Event_Time	timestamp with time zone	Event time
Event_Count	integer	Event count
Date_Created	timestamp with time zone	Date the entry was created

Column Name	Datatype	Comment
Date_Modified	timestamp with time zone	Date the entry was modified
Created_By	integer	User who created object
Modified_By	integer	User who last modified object

C.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	character varying(255)	Protocol name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	character varying(255)	Resource name
Sub_Resource_Name	character varying(255)	Subresource name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.68 EVT_SEV_SMRY_1_RPT_V

View summarizes event count by severity and event time.

Column Name	Datatype	Comment
Severity	integer	Event severity
CUST_ID	bigint	Customer identifier

Column Name	Datatype	Comment
Event_Time	timestamp with time zone	Event time
Event_Count	integer	Event count
Date_Created	timestamp with time zone	Date the entry was created
Date_Modified	timestamp with time zone	Date the entry was modified
Created_By	integer	User who created object
Modified_By	integer	User who last modified object

C.1.69 EVT_SRC_COLLECTOR_RPT_V

Column Name	Datatype	Comment
EVT_SRC_COLLECTOR_ID	uuid	Event source collector identifier
SENTINEL_PLUGIN_ID	uuid	Sentine plugin identifier
EVT_SRC_MGR_ID	uuid	Event source manager identifier
EVT_SRC_COLLECTOR_NAME	character varying(255)	Event source collector name
STATE_IND	boolean	State indicator
EVT_SRC_COLLECTOR_PROPS	text	Event source collector prop
MAP_FILTER	text	Map filter
CREATED_BY	integer	Date the entry was created
MODIFIED_BY	integer	Date the entry was modified
DATE_CREATED	timestamp with time zone	User who created object
DATE_MODIFIED	timestamp with time zone	User who last modified object

C.1.70 EVT_SRC_GRP_RPT_V

Column Name	Datatype	Comment
EVT_SRC_GRP_ID	uuid	Event source group identifier
EVT_SRC_COLLECTOR_ID	uuid	Event source collector identifier
SENTINEL_PLUGIN_ID	uuid	Sentinel plugin identifier
EVT_SRC_SRVR_ID	uuid	Event source server identifier
EVT_SRC_GRP_NAME	character varying(255)	Event source group name

Column Name	Datatype	Comment
STATE_IND	boolean	State indicator
MAP_FILTER	text	Map filter
EVT_SRC_DEFAULT_CONFIG	text	Event source default configuration
CREATED_BY	integer	Date the entry was created
MODIFIED_BY	integer	Date the entry was modified
DATE_CREATED	timestamp with time zone	User who created object
DATE_MODIFIED	timestamp with time zone	User who last modified object

C.1.71 EVT_SRC_MGR_RPT_V

Column Name	Datatype	Comment
EVT_SRC_MGR_ID	uuid	Event source manager identifier
SENTINEL_ID	uuid	Sentinel identifier
SENTINEL_HOST_ID	uuid	Sentinel host identifier
EVT_SRC_MGR_NAME	character varying(255)	Event source manager name
STATE_IND	boolean	State indicator
EVT_SRC_MGR_CONFIG	text	Event source manager configu
CREATED_BY	integer	Date the entry was created
MODIFIED_BY	integer	Date the entry was modified
DATE_CREATED	timestamp with time zone	User who created object
DATE_MODIFIED	timestamp with time zone	User who last modified object

C.1.72 EVT_SRC_OFFSET_RPT_V

Column Name	Datatype	Comment
EVT_SRC_ID	uuid	Event source identifier
OFFSET_VAL	text	Offset value
OFFSET_TIMESTAMP	timestamp with time zone	Offset timestamp
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
DATE_CREATED	timestamp with time zone	Date the entry was created

Column Name	Datatype	Comment
DATE_MODIFIED	timestamp with time zone	Date the entry was modified

C.1.73 EVT_SRC_RPT_V

Column Name	Datatype	Comment
EVT_SRC_ID	uuid	Event source identifier
EVT_SRC_NAME	character varying(255)	Event source name
EVT_SRC_GRP_ID	uuid	Event source group identifier
STATE_IND	boolean	State indicator
MAP_FILTER	text	Map filter
EVT_SRC_CONFIG	text	Event source config
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified

C.1.74 EVT_SRC_SMRY_1_RPT_V

View contains event source and destination summary information.

Column Name	Datatype	Comment
Source_IP	integer	Source IP address
Source_Event_Asset_ID	bigint	Event asset identifier
Source_Port	character varying(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	integer	Event severity
CUST_ID	bigint	Customer identifier
Event_Time	timestamp with time zone	Event time

Column Name	Datatype	Comment
XDAS_Taxonomy_id	bigint	XDAS taxonomy id
Init_User_Identity	uuid	Initiator user identity
Event_Count	integer	Event count
Date_Created	timestamp with time zone	Date the entry was created
Date_Modified	timestamp with time zone	Date the entry was modified
Created_By	integer	User who created object
Modified_By	integer	User who last modified object
Source_Host_Name	character varying(255)	Source host name

C.1.75 EVT_SRC_SRVR_RPT_V

Column Name	Datatype	Comment
EVT_SRC_SRVR_ID	uuid	Event source server identifier
EVT_SRC_SRVR_NAME	character varying(255)	Event source server name
EVT_SRC_MGR_ID	uuid	Event source manager identifier
SENTINEL_PLUGIN_ID	uuid	Sentinel plugin identifier
STATE_IND	boolean	State indicator
EVT_SRC_SRVR_CONFIG	text	Event source server configuration
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified

C.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	character varying(100)	Taxonomy level 1
Taxonomy_Level_2	character varying(100)	Taxonomy level 2
Taxonomy_Level_3	character varying(100)	Taxonomy level 3
Taxonomy_Level_4	character varying(100)	Taxonomy level 4
Device_Category	character varying(255)	

Column Name	Datatype	Comment
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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
User_Name	character varying(255)	User name
User_Domain	character varying(255)	
CUST_ID	bigint	Customer identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.78 EVT_XDAS_TXNMY_RPT_V

Column Name	Datatype	Comment
XDAS_TXNMY_NAME	character varying(255)	XDAS taxonomy name
XDAS_OUTCOME_NAME	character varying(255)	XDAS outcome name
Xdas_Registry	integer	XDAS registry
Xdas_Provider	integer	XDAS provider
Xdas_Class	integer	XDAS class
Xdas_Identifier	integer	XDAS identifier
Xdas_Outcome	integer	XDAS outcome
Xdas_Detail	integer	XDAS detail
Xdas_Taxonomy_Id	bigint	XDAS taxonomy identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object

Column Name	Datatype	Comment
MODIFIED_BY	integer	User who last modified object

C.1.79 EXTERNAL_DATA_RPT_V

View references EXTERNAL_DATA table that stores external data.

Column Name	Datatype	Comment
EXTERNAL_DATA_ID	integer	External data identifier
SOURCE_NAME	character varying(50)	Source name
SOURCE_DATA_ID	character varying(255)	Source data identifier
EXTERNAL_DATA	text	External data
EXTERNAL_DATA_TYPE	character varying(10)	External data type
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.80 HIST_CORRELATED_EVENTS

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

C.1.81 HIST_CORRELATED_EVENTS_RPT_V (legacy view)

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

C.1.82 HIST_EVENTS

Column Name	Datatype	Comment
EVT_ID	uuid	Event Universal Unique Identifier (UUID)
EVT_TIME	timestamp with time zone	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
PRTCL_ID	bigint	Protocol ID
AGENT_ID	bigint	Collector Identifier
ARCH_ID	bigint	
DEVICE_EVT_TIME	timestamp with time zone	Device Event Time
SENTINEL_PROCESS_TIME	timestamp with time zone	Sentinel Process Time
BEGIN_TIME	timestamp with time zone	Events begin time
END_TIME	timestamp with time zone	Events end time
REPEAT_CNT	integer	Events repeat count
DP_integer	integer	
SP_integer	integer	
RES	character varying(255)	Resolution
SRES	character varying(255)	
SEV	integer	Severity
EVT	character varying(255)	Events
ET	character varying(255)	
SIP	integer	
SHN	character varying(255)	
SP	character varying(32)	
DIP	integer	
DHN	character varying(255)	
DP	character varying(32)	

Column Name	Datatype	Comment
SUN	character varying(255)	
DUN	character varying(255)	
FN	character varying(1000)	
VULN	integer	Vulnerability
CT1	character varying(255)	
CT2	character varying(255)	
CT3	integer	
RT1	character varying(255)	
RT2	character varying(255)	
RT3	integer	
CRIT	integer	
MSG	character varying(4000)	Message
EI	character varying(1000)	
INIT_USR_SYS_ID	character varying(255)	
INIT_USR_IDENTITY_GUID	uuid	
TRGT_USR_SYS_ID	character varying(255)	
TRGT_USR_IDENTITY_GUID	uuid	
EFFECTIVE_USR_NAME	character varying(255)	
EFFECTIVE_USR_SYS_ID	character varying(255)	
EFFECTIVE_USR_DOMAIN	character varying(255)	
TRGT_TRUST_NAME	character varying(255)	
TRGT_TRUST_SYS_ID	character varying(255)	
TRGT_TRUST_DOMAIN	character varying(255)	
OBSRVR_IP	integer	
RPTR_IP	integer	
OBSRVR_HOST_DOMAIN	character varying(255)	
RPTR_HOST_DOMAIN	character varying(255)	
OBSRVR_ASSET_ID	character varying(255)	
RPTR_ASSET_ID	character varying(255)	
INIT_SRVC_COMP	character varying(255)	
TARGET_SRVC_COMP	character varying(255)	
EVT_GRP_ID	character varying(255)	

Column Name	Datatype	Comment
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
RV01-RV10	integer	
RV11-RV20	timestamp with time zone	
RV21-RV25	uuid	
RV26-RV38	character varying(255)	
RV40-RV49		
RV101-RV120	timestamp with time zone	
RV121-RV130	uuid	
RV131-RV140	integer	
RV141-RV150	character varying(255)	
RID01-RID20	bigint	
CV01-CV10	integer	
CV11-CV20	timestamp with time zone	
CV21-CV29	character varying(255)	
CV35-CV100		
CV30-CV34	character varying(4000)	
CV101-CV110	integer	
CV131-CV140		
CV111-CV120	timestamp with time zone	
CV121-CV130	uuid	
CV141-CV147	character varying(255)	

C.1.83 HIST_EVENTS_RPT_V (legacy view)

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

C.1.84 IMAGES_RPT_V

View references IMAGES table that stores system overview image information.

Column Name	Datatype	Comment
NAME	character varying(128)	Image name

Column Name	Datatype	Comment
TYPE	character varying(64)	Image type
DATA	text	Image data
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	integer	Incident identifier – sequence number
ASSET_ID	uuid	Asset Universal Unique Identifier (UUID)
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	integer	Incident identifier – sequence number
EVT_ID	uuid	Event Universal Unique Identifier (UUID)
EVT_TIME	timestamp with time zone	Event time
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	integer	Incident identifier – sequence number
NAME	character varying(255)	Incident name
INC_CAT	character varying(255)	Incident category
INC_DESC	character varying(4000)	Incident description
INC_PRIORITY	integer	Incident priority
INC_RES	character varying(4000)	Incident resolution
SEVERITY	integer	Incident severity
STT_ID	integer	Incident State ID
SEVERITY_RATING	character varying(32)	Average of all the event severities that comprise an incident.
VULNERABILITY_RATING	character varying(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	character varying(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	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	integer	Incident identifier – sequence number
VULN_ID	uuid	Vulnerability Universal Unique Identifier (UUID)
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified

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

C.1.89 L_STAT_RPT_V

View references L_STAT table that stores statistical information.

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

C.1.90 LOGS_RPT_V

View references LOGS_RPT table that stores logging information.

Column Name	Datatype	Comment
LOG_ID	integer	Sequence number
TIME	timestamp with time zone	Date of Log
MODULE	character varying(64)	Module log is for
TEXT	character varying(4000)	Log text

C.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	character varying(64)	Table name 1
ID1	bigint	ID1
TABLE2	character varying(64)	Table name 2
ID2	uuid	ID2
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	character varying(255)	Network identify name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.93 ORGANIZATION_RPT_V

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

Column Name	Datatype	Comment
ORGANIZATION_ID	uuid	Organization identifier
ORGANIZATION_NAME	character varying(100)	Organization name
CUST_ID	bigint	Customer identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.94 PERSON_RPT_V

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

Column Name	Datatype	Comment
PERSON_ID	uuid	Person identifier
FIRST_NAME	character varying(255)	First name
LAST_NAME	character varying(255)	Last name
CUST_ID	bigint	Customer identifier
PHONE_NUMBER	character varying(50)	Phone number
EMAIL_ADDRESS	character varying(255)	Email address
DATE_CREATED	timestamp with time zone	Date the entry was created

Column Name	Datatype	Comment
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.95 PHYSICAL_ASSET_RPT_V

View references PHYSICAL_ASSET table that stores physical asset information.

Column Name	Datatype	Comment
PHYSICAL_ASSET_ID	uuid	Physical asset identifier
CUST_ID	bigint	Customer identifier
LOCATION_ID	bigint	Location identifier
HOST_NAME	character varying(255)	Host name
IP_ADDRESS	integer	IP address
NETWORK_IDENTITY_ID	bigint	Network identity code
MAC_ADDRESS	character varying(100)	MAC address
RACK_NUMBER	character varying(50)	Rack number
ROOM_NAME	character varying(100)	Room name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	character varying(255)	Product name
PRODUCT_VERSION	character varying(100)	Product version
VENDOR_ID	bigint	Vendor identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object

Column Name	Datatype	Comment
MODIFIED_BY	integer	User who last modified object

C.1.97 ROLE_RPT_V

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

Column Name	Datatype	Comment
ROLE_CODE	character varying(5)	Role code
ROLE_NAME	character varying(255)	Role name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.98 RPT_LABELS_RPT_V

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

Column Name	Datatype	Comment
RPT_NAME	character varying(100)	Report name
LABEL_1 – LABEL_35	character varying(2000)	Translated report labels

C.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	character varying(50)	Asset sensitivity name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.100 SENTINEL_HOST_RPT_V

Column Name	Datatype	Comment
SENTINEL_HOST_ID	uuid	Sentinel host identifier
SENTINEL_ID	uuid	Sentinel identifier
SENTINEL_HOST_NAME	character varying(255)	Sentinel host name
HOST_NAME	character varying(255)	Host name
IP_ADDR	character varying(255)	IP address
HOST_OS	character varying(255)	Host operating system
HOST_OS_VERSION	character varying(255)	Host operating system version
MODIFIED_BY	integer	User who last modified object
CREATED_BY	integer	User who created object
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified

C.1.101 SENTINEL_PLUGIN_RPT_V

Column Name	Datatype	Comment
SENTINEL_PLUGIN_ID	uuid	Sentinel plugin identifier
SENTINEL_PLUGIN_NAME	character varying(255)	Sentinel plugin name
SENTINEL_PLUGIN_TYPE	character varying(255)	Sentinel plugin type
FILE_NAME	character varying(512)	File name
CONTENT_PKG	text	Content package
FILE_HASH	character varying(255)	File hash code
AUX_FILE_NAME	character varying(512)	Auxiliary file name
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified

C.1.102 SENTINEL_RPT_V

Column Name	Datatype	Comment
SENTINEL_ID	uuid	Sentinel identifier

Column Name	Datatype	Comment
SENTINEL_NAME	character varying(255)	Sentinel name
ONLINE_IND	boolean	Online indicator
STATE_IND	boolean	State indicator
SENTINEL_CONFIG	text	Sentinel configuration
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified

C.1.103 STATES_RPT_V

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

Column Name	Datatype	Comment
STT_ID	integer	State ID – sequence number
COtext	character varying(64)	Cotext of the state. That is case, incident, user.
NAME	character varying(64)	Name of the state.
TERMINAL_FLAG	character varying(1)	Indicates if state of incident is resolved.
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
MODIFIED_BY	integer	User who last modified object
CREATED_BY	integer	User who created object

C.1.104 UNASSIGNED_INCIDENTS_RPT_V

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

Name	Datatype	Comment
INC_ID	integer	Incident identifier – sequence number
NAME	character varying(255)	Short, unique user name used as a login
SEVERITY	integer	Incident severity
STT_ID	integer	State ID. Status is either active or inactive.

Name	Datatype	Comment
SEVERITY_RATING	character varying(32)	Average of all the event severities that comprise an incident.
VULNERABILITY_RATING	character varying(32)	Vulnerability rating
CRITICALITY_RATING	character varying(32)	Criticality rating
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object
INC_DESC	character varying(4000)	Incident description
INC_CAT	character varying(255)	Incident category
INC_PRIORITY	integer	Incident priority
INC_RES	character varying(4000)	Incident resolution

C.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	integer	User identifier – Sequence number
NAME	character varying(64)	Short, unique user name used as a login
CNT_ID	integer	Contact ID – Sequence number
STT_ID	integer	State ID. Status is either active or inactive.
DESCRIPTION	character varying(512)	Comments
PERMISSIONS	character varying(4000)	Permissions currently assigned to the Sentinel user
FILTER	character varying(128)	Current security filter assigned to the Sentinel user
UPPER_NAME	character varying(64)	User name in upper case
DOMAIN_AUTH_IND	boolean	Domain authentication indication
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.106 USR_ACCOUNT_RPT_V

Column Name	Datatype	Comment
ACCOUNT_ID	bigint	Account identifier
USER_DOMAIN	character varying(255)	User domain
CUST_ID	bigint	Customer identifier
BEGIN_EFFECTIVE_DATE	timestamp with time zone	Begin effective date
END_EFFECTIVE_DATE	timestamp with time zone	End effective date
CURRENT_F	boolean	Current flag
USER_STATUS	character varying(50)	User status
IDENTITY_GUID	uuid	Identity identifier
SOURCE_USER_ID	character varying(100)	User ID on source system
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.107 USR_IDENTITY_EXT_ATTR_RPT_V

Column Name	Datatype	Comment
IDENTITY_GUID	uuid	Identity identifier
ATTRIBUTE_NAME	character varying(255)	Attribute name
ATTRIBUTE_VALUE	character varying(1024)	Attribute value

C.1.108 USR_IDENTITY_RPT_V

Column Name	Datatype	Comment
IDENTITY_GUID	uuid	Identity identifier
DN	character varying(255)	Distinguished name
CUST_ID	bigint	Customer identifier
SRC_IDENTITY_ID	character varying(100)	Source identity identifier
WFID	character varying(100)	Workforce identifier
FIRST_NAME	character varying(255)	First name
LAST_NAME	character varying(255)	Last name

Column Name	Datatype	Comment
FULL_NAME	character varying(255)	Full name
JOB_TITLE	character varying(255)	Job title
DEPARTMENT_NAME	character varying(100)	Department name
OFFICE_LOC_CD	character varying(100)	Office location code
PRIMARY_EMAIL	character varying(255)	Primary email address
PRIMARY_PHONE	character varying(100)	Primary phone number
VAULT_NAME	character varying(100)	Identity vault name
MGR_GUID	uuid	Manager identity identifier
PHOTO	text	Photo
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	character varying(255)	Vendor name
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	uuid	
IP	character varying(32)	IP
HOST_NAME	character varying(255)	Host name
CRITICALITY	integer	Asset criticality code

Column Name	Datatype	Comment
ASSIGNED_VULN_SEVERITY	integer	
VULN_COUNT	integer	Vulnerability Count
CALC_SEVERITY	numeric(14,2)	

C.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	uuid	
VULN_ID	uuid	Vulnerability identifier
VULN_CODE_TYPE	character varying(64)	Vulnerability code type
VULN_CODE_VALUE	character varying(255)	Vulnerability code value
URL	character varying(512)	Web URL
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	uuid	
VULN_ID	uuid	Vulnerability identifier
VULN_INFO_TYPE	character varying(36)	
VULN_INFO_VALUE	character varying(2000)	
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	uuid	Vulnerability identifier
RSRC_ID	uuid	Resource identifier
PORT_NAME	character varying(64)	Port Name
PORT_NUMBER	integer	Port Number
NETWORK_PROTOCOL	integer	Network Protocol
APPLICATION_PROTOCOL	character varying(64)	Application Protocol
ASSIGNED_VULN_SEVERITY	integer	
COMPUTED_VULN_SEVERITY	integer	
VULN_DESCRIPTION	text	
VULN_SOLUTION	text	
VULN_SUMMARY	character varying(1000)	
BEGIN_EFFECTIVE_DATE	timestamp with time zone	Date from which the entry is valid
END_EFFECTIVE_DATE	timestamp with time zone	Date until which the entry is valid
DETECTED_OS	character varying(64)	
DETECTED_OS_VERSION	character varying(64)	
SCANNED_APP	character varying(64)	
SCANNED_APP_VERSION	character varying(64)	
VULN_USER_NAME	character varying(64)	
VULN_USER_DOMAIN	character varying(64)	
VULN_TAXONOMY	character varying(1000)	
SCANNER_CLASSIFICATION	character varying(255)	
VULN_NAME	character varying(300)	
VULN_MODULE	character varying(64)	
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	uuid	
SCANNER_ID	uuid	Scanner identifier
IP	character varying(32)	IP Address
HOST_NAME	character varying(255)	Host name
LOCATION	character varying(128)	Location
DEPARTMENT	character varying(128)	Department
BUSINESS_SYSTEM	character varying(128)	Business System
OPERATIONAL_ENVIRONMENT	character varying(64)	Operational environment
CRITICALITY	integer	Criticality
REGULATION	character varying(128)	Regulation
REGULATION_RATING	character varying(64)	Regulation rating
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	uuid	
SCAN_ID	uuid	
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.116 VULN_SCAN_RPT_V

View references table that stores information pertaining to scans.

Column Name	Datatype	Comment
SCAN_ID	uuid	Vulnerability scan identifier
SCANNER_ID	uuid	Vulnerability scanner identifier
SCAN_TYPE	character varying(10)	Vulnerability scan type
SCAN_START_DATE	timestamp with time zone	Scan start date
SCAN_END_DATE	timestamp with time zone	Scan start date
CONSOLIDATION_SERVER	character varying(64)	Consolidation server
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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	uuid	
VULN_ID	uuid	
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.118 VULN_SCANNER_RPT_V

View references VULN_SCANNER table that stores information about vulnerability scanners.

Column Name	Datatype	Comment
SCANNER_ID	uuid	
PRODUCT_NAME	character varying(100)	Product Name
PRODUCT_VERSION	character varying(64)	Product Version
SCANNER_TYPE	character varying(64)	Vulnerability Scanner Type
VENDOR	character varying(100)	Vendor
SCANNER_INSTANCE	character varying(64)	Scanner Instance
DATE_CREATED	timestamp with time zone	Date the entry was created

Column Name	Datatype	Comment
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.119 WORKFLOW_DEF_RPT_V

Column Name	Datatype	Comment
PKG_NAME	character varying(255)	Package name
PKG_DATA	text	Package data
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.1.120 WORKFLOW_INFO_RPT_V

Column Name	Datatype	Comment
INFO_ID	bigint	Info identifier
PROCESS_DEF_ID	character varying(100)	Process definition identifier
PROCESS_INSTANCE_ID	character varying(150)	Process instance identifier
DATE_CREATED	timestamp with time zone	Date the entry was created
DATE_MODIFIED	timestamp with time zone	Date the entry was modified
CREATED_BY	integer	User who created object
MODIFIED_BY	integer	User who last modified object

C.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

Documentation Updates

D

This section contains information about documentation content changes made to the *Novell Identity Audit Guide 1.0*. If you are an existing user, review the change entries to identify modified content. If you are a new user, simply read the guide in its current state.

Refer to the publication date that appears on title page to determine the release date of this guide. For the most recent version of the *Novell Identity Audit Guide*, see the [Novell Identity Audit 1.0 documentation Web site \(http://www.novell.com/documentation/identityaudit/\)](http://www.novell.com/documentation/identityaudit/).

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

This document was updated on the following dates:

- ◆ [Section D.1, “October 2009,” on page 139](#)

D.1 October 2009

Updates are made to the following section:

Table D-1 *Updates*

Location	Changes
Chapter 2, “System Requirements,” on page 17	Updated the Section 2.2, “Supported Operating Systems,” on page 18 .
Chapter 4, “Reporting,” on page 27	Added the new Section 4.4, “Default Reports,” on page 34 to list all the pre-installed reports with Identity Audit.
Entire Guide	Updated the document with the user comments.

