Ignite Technologies
Security and Compliance Solutions

Glossary

SenSage Standard 2016 (v. 6.1.1)

August 4, 2016

401 Congress Avenue Suite 2650
Austin, TX 78701
800-248-0027
info@ignitetech.com

Published June 21, 2016

TABLE OF CONTENTS

PREFACE

This book, the *Glossary*, describes version 6.1.1 of SenSage AP software.

This Preface contains the following sections:

AUDIENCE FOR THIS BOOK

This glossary is intended for all SenSage AP users.

ORGANIZATION OF THIS BOOK

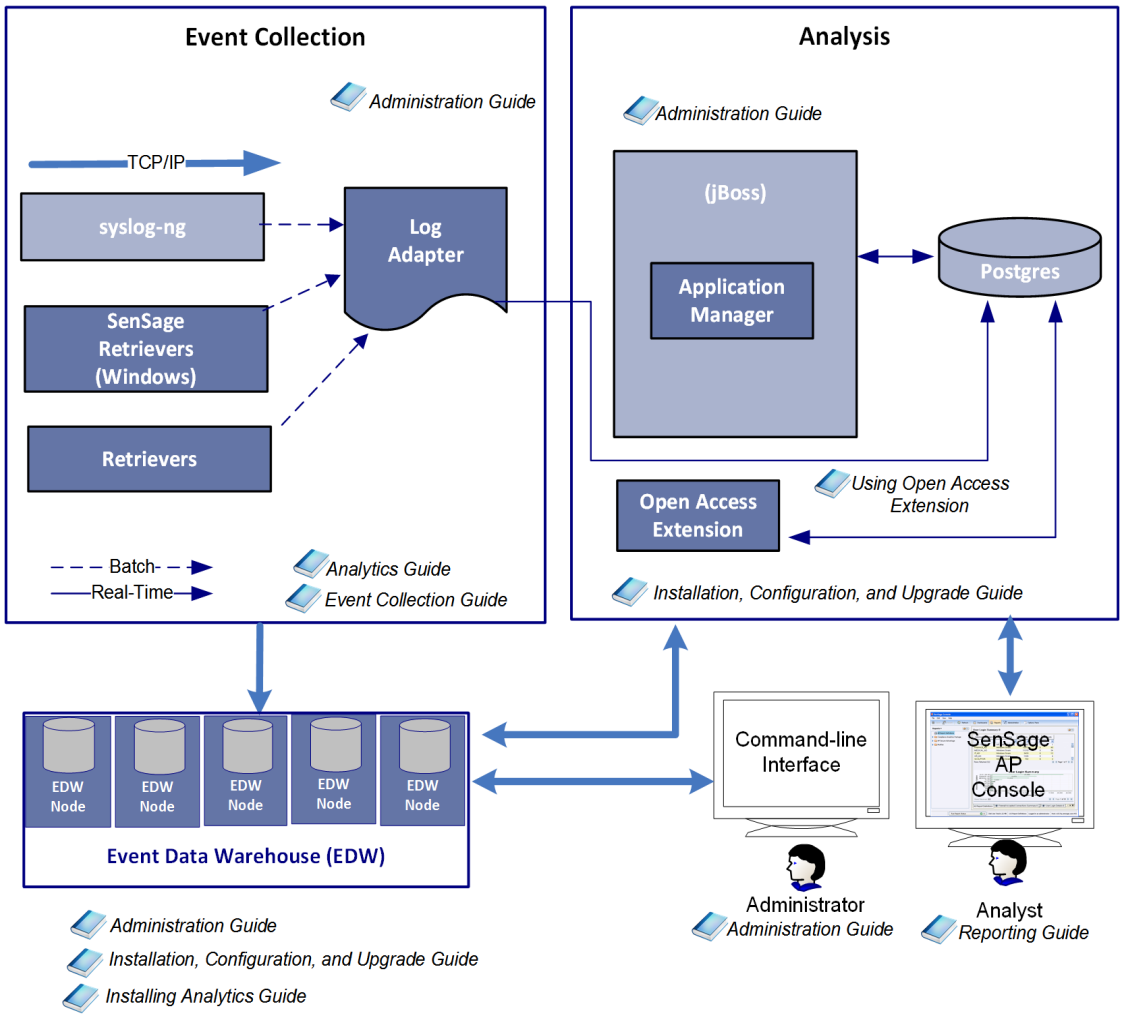
This book comprises the following chapters:

- Glossary—Definitions of terminology used in SenSage AP documentation.

ROAD MAP TO SENSAGE AP DOCUMENTATION

This document, the *Glossary*, is part of the larger documentation set of your SenSage AP system. Figure P-1 illustrates SenSage AP components and modules in the context of their function within the SenSage AP system.

Figure P-1: Road Map to SenSage AP Documentation



The table below describes all the manuals in the SenSage AP documentation set and the user roles to which they are directed.

Role	Tasks	Documentation
Analyst, Report Developer, System Administrator	• Create and edit reports, charts, and models • Create and edit dashboards • Manage SenSage AP Users • Manage SenSage AP Models • Create and edit data models • Write SQL code and queries	*Analyzer Guide*

Role	Tasks	Documentation
Business Analyst or System Administrator	• Learn about Analytics • Use IntelliSchema views • Learn about the Foundation and Compliance Analytics packages • Learn about additional Analytics packages	*Analytics Guide*
Developer, Report Developer or Security Analyst	• Use SenSage AP SQL, SenSage AP SQL functions, and libraries to create reports or query the EDW • Access EDW data using open standards as ANSI SQL, ODBC, and JDBC • Create and use Perl code in SenSage AP SQL statements • Use the DBD Driver to query SenSage AP from other locations	*Event Data Warehouse Guide*
Security System Administrator	• Configure retrievers, receivers, and collectors • Enable/disable log adapters • Configure SenSage Retriever • Create log adapter PTL files	*Collector Guide*
System Administrator	• Install SenSage AP • Configure SenSage AP and its components • Configure Vmware	*Installation, Configuration, and Upgrade Guide*
System Administrator	• Manage the SenSage Event Data Warehouse (EDW) • Manage the Collector • Manage users, groups, and permissions • Archive to nearline storage • Manage assets & monitor security alerts • Monitor log source health • Monitor system health • Troubleshoot • Error Messages	*Administration Guide*
Legal	Monitor third-party licenses	*Third-Party Open Source Licensing*

TIP: You can access the manuals listed above from:

- SenSage AP Welcome page

  Click the **Documentation** hyperlink.

For more information, see “Logging into SenSage AP Console” in the *Administration Guide*.

CONVENTIONS USED IN SENSAGE AP DOCUMENTATION

This convention...	Indicates...	Example
bold text	Names of user interface items, such as field names, buttons, menu choices, and keystrokes	Click **Clear Filter**.
italic text	Indicates a variable name or a new term the first time it appears	`http://<host>:<port>/index.mhtml`
`Courier text`	Indicates a literal value, such as a command name, file name, information typed by the user, or information displayed by the system	`atquery localhost:8072 myquery.sql`
SMALL CAPS	Indicates a key on the computer keyboard	Press ENTER.
`{ }`	In a syntax line, curly braces surround a set of options from which you must choose one and only one. **NOTE**: Syntax specifications for SELECT statements include curly braces as part of the `{INCLUDE_BAD_LOADS]` keyword.	`{ start | stop | restart }`
`[ ]`	In a syntax line, square brackets surround an optional parameter	`atquery [options] <host>:<port> -`

`|`	In a syntax line, a pipe within square brackets or curly braces separates a choice between mutually exclusive parameters
	NOTE: Syntax for defining a Nearline Storage Address (NSA) includes a pipe.
		`{ start | stop | restart }`
		
		`[g|m]`

`...`	In a syntax line, ellipses indicate a repetition of the previous parameter	The following example indicates you can enter multiple, comma-separated options: `<option>[, <option>[…]]`

backslash (\)	A backslash in command-line syntax or in a command example behaves as the escape character on Unix. It removes any special meaning from the character immediately following it. In SenSage AP documentation, a backslash nullifies the special meaning of the newline character as a command terminator. Without the backslash, pressing ENTER at the end of the line causes the Unix system to execute the text preceding the ENTER. Without the backslash, you must allow long commands to wrap over multiple lines as a single line.	`atquery --user=administrator \`
		`--pass=pass:p@ss localhost:8072\`
		`-e='SELECT * FROM system.users;'`

CONTACTING TECHNICAL SUPPORT

For additional help, call +1 855 529-3929. Also you can log into the IgniteTech Technical Support web page under Services at http://www.ignitetech.com for SenSage AP documentation, product downloads, and additional information on contacting support to escalate help on issues that impact your production environment.

GLOSSARY

A

active directory: A Windows-based authentication authority that manages users and user groups; when integrated into an EDW instance, the Active Directory authority authenticates each user's name and password at login.

administrator: A role that by default gives its user account full permission to access, modify, and delete all SenSage AP objects in the Event Data Warehouse and in the SenSage AP Analyzer.

analytics packages: The Hexis Cyber Solutions add-on components that enable the rapid implementation of PTL files, reports, and queries that are tailored to specific industry and organization requirements. Analytics packages enable event data to be available for analysis in the SenSage AP Analyzer .

Analyzer: See SenSage AP Analyzer.

anonymous request: Requests from users or systems that do not have user names and passwords in the Hexis Cyber Solutions. The system uses the guest user for such requests.

aattribute: In the Collector `config.xml` and `errors.xml` files and in rules, an attribute refers to a setting within an XML element tag. For example, `name` is an attribute of the Retriever element and `fs` is its value here:

```
<Retriever name="fs" ....
```

authentication: The security process that and validates a users identity by default through their user name and password.

authorization: The security process that, once authenticated, validates a user's roles and permissions before allowing the identified user to access any object or perform any operation.

B

batched events: Events that are collected from log files and other event repositories maintained by network devices and software applications.

C

character encoding: A scheme by which human-readable characters are represented in computer systems and transported across computer networks. Simple, single-byte character encoding schemes, such as ASCII or ISO 8859-1, represent each character of their character set with the binary equivalent of its code point. For example with ASCII character encoding, the letter "A" is represented with bytes that contain the numeric value 65.

character set: A set of characters and the assigned, numeric code point for each character. For example, the ASCII character set includes the upper- and lower-case letters of the U.S. English alphabet and a few punctuation marks and symbols. A character set does not necessarily equate with a particular character encoding. For example, the Unicode character set can be represented in computers with Unicode character encoding, a fixed, two-byte encoding scheme, or with UTF-8, a variable-width encoding scheme where specific characters are represented by one-, two-, three-, or four-byte bit patterns.

clause: A standard portion of a SELECT statement, such as the WHERE, DURING, ORDER_BY, and GROUP BY clauses. Clauses are expected in a particular sequence. Some clauses are required and some

are optional.

CLI: command-line interface

clustered instance: An EDW instance that runs on multiple hosts.

code point: A decimal number assigned to a particular character in a character set. For example with ASCII character encoding, the letter "A" is assigned the code point 65.

ComboBox: A display field that combines the features of an editable text field and a drop-down list.

computer font: A typeface that determines how computer screens and printers display the characters and symbols of a particular character set.

Collector: The SenSage AP component that pulls event-log data from disparate sources, uses adapters to normalize the data, and loads the data into the EDW. After it has been loaded, the data is available for queries and reports through the SenSage AP Analyzer in both original and normalized views.

Compliance Reports Package: An Analytics package containing report definitions designed to report on events that must be monitored to maintain compliance with various regulations and standards.

config.dtd: DTD file used to verify and enforce the way elements and attributes are defined in config.xml. It is located in:

```
/<HawkEye AP Home>/etc/collector
```

config.xml: Configuration file for the Collector. It is located in:

```
/<HawkEye AP Home>/etc/collector
```

connector view: An IntelliSchema source-specific view used to normalize event data at query-time by enforcing consistent use of column names, data types, and formats, and by consistently presenting disparate event data that indicates the same information.

coupled instance: An EDW instance that shares the same data store as another instance; used in the upgrade process to enable access to the datadir (the `dsroot`) from an earlier version of the EDW; also used to create read/write and read-only instances to segregate people who load log entries from people who query them.

custom interval: The time period of a report query that specifies the start date as well as the end date; see standard interval.

D

Dashboard: A SenSage AP Analyzer function that organizes and displays reports on one or more pages.

data balancing: Movement of data from an old node to a new node in order to maintain proper primary/secondary mirroring.

data redistribution: Movement of data between nodes in a cluster in order to balance the amount of data stored on each EDW node.

drilldown: A link from a high-level summary report to detailed reports that decompose the summarized data for individual rows. The link enables users to drill down from rows on the high-level report to a more detailed report for a given row.

E

element: In the Collector's `config.xml` and `error.xml` files and in rules, an element is an XML tag that contains the relevant configuration setting and its attributes.

errors.xml: File that lists errors, settings for email alerts, and paths to activity.log and error.log. It is located in:

```
/opt/hexis/hawkeye-ap/share/locale/en_QA/collector/errors.xml
/opt/hexis/hawkeye-ap/share/locale/en_US/collector/errors.xml

  /opt/hexis/hawkeye-ap/share/locale/fr_FR/collector/errors.xml
  /opt/hexis/hawkeye-ap/share/locale/de_DE/collector/errors.xml
  /opt/hexis/hawkeye-ap/share/locale/ja_JP/collector/errors.xml
  /opt/hexis/hawkeye-ap/share/locale/sl_SI/collector/errors.xml
  /opt/hexis/hawkeye-ap/share/locale/qa_QA/collector/errors.xml
  /opt/hexis/hawkeye-ap/share/locale/es_ES/collector/errors.xml
```

event: Data representing an action that occurred in some environment at a specific time that flows into the SenSage AP system from network devices and software applications, or is collected from log files and other repositories maintained by network devices and software applications. Events always have a timestamp and never change.

Event Data Warehouse (EDW): A data warehouse built for and dedicated to loading, storing, and analyzing events. It uses sophisticated, application-level clustering to perform all load and query tasks fully in parallel across an arbitrary number of hosts. Its architecture allows users to load and query massive data volumes in a single, logical database instance without partitioning. The EDW uses a proprietary data model that achieves high levels of compression, while still making all data fully available to query. This data model also removes the need for the performance and storage overhead of indices on specific columns.

event type: A high-level categorization of event data, such as a login, startup, or shutdown.

event-type view: An IntelliSchema source-agnostic view that references multiple connector views to create a view used to report on a single event type. See master view.

Exception report: A report designed to find non-normal or exception conditions. In normal conditions the report will return 0 rows. If the report ever returns more than one row it has found an exception.

exception report alert: An alert raised when a scheduled exception report contains one or more rows.

F

filter: Text that limits the value of selected data.

failover: Operational backup mode performed by secondary system components, such as processors, servers, databases, in the event the primary system components become non-operational.

Foundation Report Package: An analytics package that includes report definitions for reporting on event data from Microsoft Windows systems, Unix systems, and the SenSage AP system itself.

H

SenSage AP Analyzer: An HTML-based user interface for monitoring, analyzing, and reporting event data. The console supports reporting drill-down ad-hoc querying, scheduled analytic reporting, dashboards, and data flow modeling.

hierarchical instance: See clustered instance.

home directory: A directory on a host that you specify during installation in which all the SenSage AP software and application files are located.

host: In Unix networks, a computer system with one or more network IP addresses. In Windows networks, a host is called a server.

I

instance: A set of EDW hosts that collectively manage a distributed data store and the access to that data store; the data store and its running service accept load and query requests.

instance reference: An EDW instance reference may be specified by its name (`my_instance`) or by its host and port (`host1.myco.com:7002`).

interval: The time period over which a report runs in SenSage AP Analyzer Intervals are either standard or custom.

IntelliSchema: A set of SQL views that provide an abstraction layer between raw data and normalized event data. Used to create reports based on common event types.

investigation report: An interactive report that provides detailed information about specific attributes such as the destination IP address, the user ID, or hostname.

K

Kerberos: A strong authentication protocol based on key cryptography, that Hexis Cyber Solutions uses to process authentication data between the EDW and Active Directory.

keyword: A word that forms a standard part of a SQL clause, operator, modifier, or is otherwise understood with special significance by the SQL engine.

L

LEA: Log Export API, used by products like CheckPoint FireWall for transporting log files across networks.

loader: A process of the Collector that loads log entries into the EDW.

log adapter: A collection of files, including a PTL file, a Map file, IntelliSchema views, sample data, and documentation which supports loading event-log entries from a particular log source into the EDW and querying the data from the EDW.

log entry: An entry recorded in a log file. Generally, log entries include fields of information for the date and time of day that the entry was recorded, the application or device that recorded the entry, and a message about an event that occurred or a situation that was detected. See Event.

log file: A file that contains log entries and is retrieved and processed by the Collector module.

log host: A host or server computer that produces the logs from which the Collector gathers data.

log queue: A user-specified directory where log files are stored after transfer by retrievers from log hosts. Log files remain in their log queues during processing by retrievers, preprocessors, and loaders.

log source: A system or protocol for recording a log entry.

LUN: Logical Unit Numbers. A term used in Storage Area Network (SAN) configuration. A LUN identifies a storage volume within a SAN.

M

match: A regular expression that describes which matching log files will be run through a preprocessor. For example, "mail" is the same as the `/.*mail.*/` regular expression; it is a substring match anywhere in the original log file name.

master view: An IntelliSchema view that references multiple connector views or event-type views to create a unified view of a single event type from multiple, heterogeneous information systems.

MD5: Message Digest compression algorithm used in checksum processes.

N

Netflow Receiver: Used to collect and analyze network data, providing Network Managers a detailed view of application and traffic flow so that appropriate responses can be applied to network-based threats and intelligence gained about application usage for capacity planning.

node: Another name for a host or a server; one item in a network data.

normalization: A process used to create consistent representations of event data originally presented in different forms. For example, an event log may record a failed login with the word "failure" while another event log may use the words "login failed", or a numeric code. A normalized version of this data records all events using a consistent representation such as "failed login" with a consistent set of columns.

O

operator: Conditional, math or other keywords used to work with expressions, SQL constants and report filters. These include `AND`, `OR`, `NOT`, `EXACT`, `<`, `>`, `=`, `PREFIX`.

P

parameterized query: A query that specifies parameters (or macros) to be replaced with values at runtime.

privileged port: A TCP/IP port number in the range 1-1023.

PTL file: A special SenSage AP file that describes how log entries are parsed, transformed, and loaded into the EDW. PTL files have `.ptl` as their extension and are sometimes pronounced "Pitals" (pea-tals).

Q

query: One or more statements submitted to the EDW that produces a single result set. A query can include multiple `SELECT` statements by using `UNION ALL`, `UNION OVER`, or subqueries. In the Analyzer, a SenSage AP SQL statement that extracts event-log data from the EDW data store and is a required child of every report.

query file: A file created by the Application Manager to track information about queries run in HawkEye AP Console.

quiesce: To render quiet, (that is, temporarily inactive or disabled).

R

receiver: A process within the Collector that listens on a specific port and receives data streams for loading to EDW.

report definition: A specification of a query and how to display the result set in a report including the way the data is arranged and whether the data is also graphically displayed and if so, what type of graph or chart.

report filter: Determines the report data a viewer can see based on a SQL WHERE clause applied to one or more columns. Can be either preset or prompted interactively in parameterized reports.

Report Wizard: A graphical tool that walks you through the process of creating report definitions.

retriever: A process with the Collector that initiates connections with remote systems to gather event data for loading into the EDW.

risk: A condition of an alert that is based on the value of the asset against which it was triggered; the higher the value placed on one asset over another, the higher the risk posed by alerts with the same priority. For example, a failed password attempt on a payroll system probably poses more of risk than a failed password attempt on an email system.

role: Authorization object that determines which permissions an identified set of users can access.

S

SAN: Storage Area Networks. A method of attaching storage devices to an operating system.

sender: A log-specific module that captures log files from remote systems and provides them to a retriever for entrance into the Collector.

SELECT statement: A complete set of instructions to the SQL engine as to how to select desired rows from a given table (either an EDW table or a subquery result set) and transform them into a result set table of rows and columns.

server: In Windows networks, a computer system running Microsoft Windows Server. In Unix networks, a server is often called a host.

SNMP Bridge: Used to trap and send messages into the syslog-ng server when parsing and loading data.

SQL aggregate: A function that returns one result per group of row values processed.

SQL expression: A combination of references to column values, SQL constants, functions, aggregates and operators that evaluates to a single value of any data type.

SQL function: Takes SQL expressions as arguments and returns one result per one or more rows processed.

ssh: Secure shell is an interactive program that enables encrypted network connections between computers. One computer can connect to another for the purpose of running programs on the other computer.

SSL: Secure Sockets Layer. A protocol that uses cryptography to provide secure transmission over the Internet.

standard interval: The time period of a report query that specifies a specific interval (such as 1 week or 5 months) as well as the end date; see custom interval.

streamed events: Events that flow into the SenSage AP as they are created from network devices and software applications that publish the events. See batched events.

system asset: An asset that represents a SenSage AP component, such as a receiver or parser.

T

target: An expression plus an optional target name that defines what is to be returned in a result column.

target list: A set of targets; not the same as an SQL list.

TLS: Transport Layer Security. A protocol that ensures secure communication over the Internet. TLS is the successor to SSL.

V

View filter: A report filter that applies to reports after they run.

Virtual machine: A software emulation of a computer operating system.

W

Workspace: The primary area of SenSage AP Analyzer in which you view and manage data.