



Sentra as an Information Server



Table of Contents

Introduction.....	3
Sentra Overview	5
Sentra Agents	6
Data Analysis	9
Sample Alerts, Graphs and Reports.....	10

Introduction

What is Sentra?

Sentra is a tool that captures data and metadata from a wide variety of different sources and stores it in a central repository. Data can be captured in real-time or can be scheduled to be captured at specific periods each day.

Sentra provides a flexible means of reporting the captured data to both business and operations users in the format that best meet those users' needs. Sentra is therefore said to be acting as an information server. The product has the flexibility to provide the complete range of management views, including:

- Transaction life cycle Business Activity Monitoring (BAM) views
- Alert views – as the data is captured, it can be analysed against a set of business or technical rules. If the captured data meets any of these rules criteria, alerts are generated.
- Alerts are represented visually in the Sentra console applications. These alerts can also be escalated via e-mail, SMS or to other enterprise management tools.
- Ad-hoc query views, providing users with full flexibility in how they wish to view the captured data.
- Trend analysis views. The data stored in the central repository can be retained for user definable periods, enabling long-term trending analysis reports to be produced.
- Business reports – Sentra includes a tool to enable business reports to be produced and automatically delivered to users, e.g. via e-mail.

The product has been successfully deployed in a number of key areas:

- Payment systems workflow monitoring – Insider Technologies have been working for several years with Logica, to provide complete lifecycle monitoring of payments through the LAPS (Logica All Payments System) product. A number of different agents are deployed to perform this monitoring, capturing data from databases, XML data streams, log files, system logs, java applications and IBM WebSphere MQ queues. The captured data is then represented in the form of business overview and technical overview diagrams, thus simplifying the monitoring of complex systems.
- Payment transaction monitoring – Sentra has been deployed in high-volume to capture transaction data from ATM and POS applications, giving operators unprecedented real-time access to trends of ATM and POS activity.
- e-mail monitoring – agents capture information from e-mail systems and email tracking log files. The user can perform messaging queries to show the path that e-mail has taken through multiple e-mail servers. Agents are provided for many different e-mail system vendors (Microsoft Exchange being the most well-known) and different operating systems, including Windows, Solaris and Linux.
- Log file monitoring – agents capture data from many different structured log files, e.g. comma-separated variable format, with tailored views to represent the captured data in a way that each customer's preferences.
- Systems monitoring – Sentra features agents which can be used to monitor the performance of multiple computers in a corporate network.

What This Document Provides

This paper provides a brief overview of the core Sentra facilities when used as an information server. For information on some of the other features of Sentra, refer to the standard Sentra White Paper document.

Who Should Read This Document

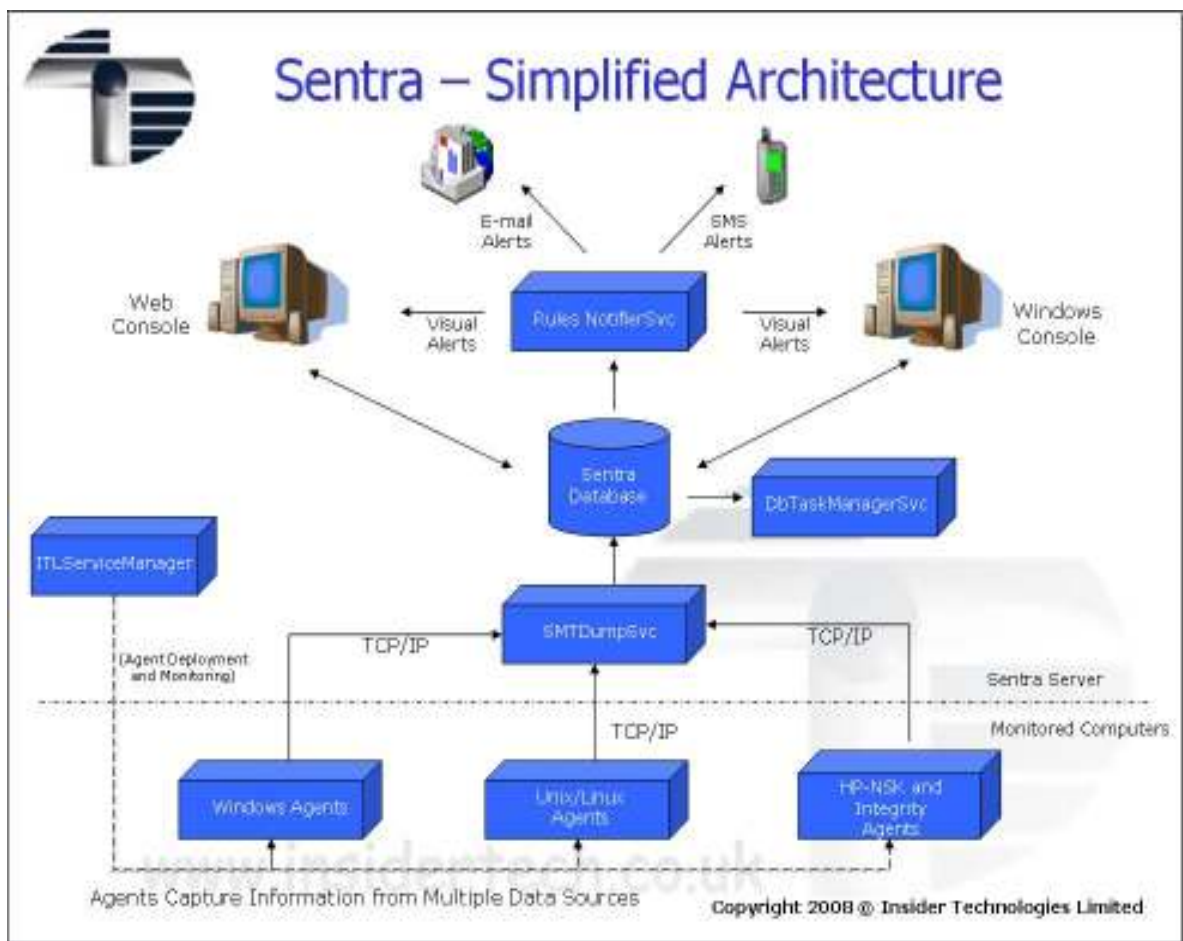
The document will provide an excellent introduction to individuals who are considering a product evaluation and who are looking for a more detailed product description outside of the information provided by Insider Technologies' sales and web site literature.

Sentra Overview

This section provides a brief overview of the Insider Technologies Sentra product. If further detailed technical Sentra information is required, then this can be obtained on request from Insider Technologies at support@insidertech.co.uk.

General Sentra Principles

The basic objective of the Sentra product is to allow users to create a centralised repository of information that can then be processed by a variety of other Sentra modules, to help provide a set of query and reporting facilities. To achieve this, Sentra ships with a comprehensive list of agents that can capture data from many different sources. The agents can be deployed on key computers throughout a corporate network, to gather information and forward it to a central repository.



Sentra Agents

The agent programs that read and relay the service data are known as 'extraction agents'. These agents can be installed, started, stopped and managed from the central server that also hosts the information repository, i.e. a database. The status of all agents can be viewed through a central 'program control' screen.

A variety of options exist to extract metadata from 'standard' locations such as SQL tables, XML format files and structured log files. The key agents that satisfy this requirement are discussed in more detail below. For a more comprehensive list of Sentra agents, refer to the Sentra Data Collection Agents White Paper.

XML Data Collection Agent

A general purpose XML agent can be configured to parse any XML data into a hierarchical structure of SQL tables and fields for storage in the Sentra repository. This makes the information much easier to process and report on, whilst maintaining the relationships between the XML elements.

The agent can be configured by loading an existing XSD schema file that defines the data format, or, (where a schema is not available), by loading examples of the XML structure to be captured. The agent can collect XML data from files, MQ queues, or from TCP/IP socket-based messages sent directly to it.

XML agents can be configured in a matter of minutes and deployed to monitor UNIFI and ISO20022-compatible payments and transactions

A series of these XML agents can be deployed to key monitoring points (waypoints) within a payment processing infrastructure to monitor payment flow, transaction volumes and trends, payment volumes and trends and end-to-end processing times. Rules can be configured to monitor service level compliance and abnormal processing volumes.

Generic Log File Agent

Sentra uses a general purposes 'Generic' log file agent that can collect data from any structured text log file. The Sentra Windows console enables a user to configure a new agent and specify the format of the data that the agent is required to capture. For example, a new agent can rapidly be configured to capture the contents of any comma-separated variable (CSV) format file. Sentra ships with pre-configured setups for some common structured log files, e.g. the Microsoft ISA Firewall log file, the Microsoft ISA Packet Filter log file, the BEA WebLogic log file and Tuxedo log file.

As with all Sentra agents, rules can be configured to evaluate captured data. Alerts will be generated if the rules criteria are met.

SQL Query Monitoring Agent

The Sentra SQL agent can be configured to schedule execution of queries of the Sentra database or any other ODBC-compliant database, including SQL Server, ORACLE, DB2 and MySQL. This agent is typically used to store summary information from a number of database sources so that long term trends can be summarised and alerts generated if any rules are broken. For example this could be used to produce an escalation of a problem if the number of alerts for a server broke a nominated limit. This agent has been used to monitor a high-performance payment system that utilised an ORACLE database. The agent issued scheduled queries to monitor payment volumes; if the payment volume fell below a preset threshold, an alert was generated.

X500 Enterprise Directory and Active Directory Monitoring Agent

The enterprise directory monitoring agent monitors the availability and performance of X500 or Windows Active Directory based enterprise directories. Statistics such as percentage availability and directory query response time can be recorded. Agents can be deployed to multiple locations around a network to determine the availability and responsiveness of the enterprise directory from across the whole organisation. The agents can also be configured to capture data from X500 enterprise directories and transfer the data to the Sentra repository.

Email Agents

Sentra collects email message events from a wide range of e-mail system vendors and transforms them into a unified format in the Sentra database. Agents are provided for capture of both SMTP and X400 mail system tracking log files. This allows messages to be tracked across multiple vendors and between X400 and SMTP environments and through mail gateways.

Typical mail systems supported on a variety of different operating systems include:

- Microsoft Exchange 5.5, 2000, 2003, 2007
- Boldon James X400 Bridgehead Connector for Microsoft Exchange 2007
- Lotus Notes/Domino
- Sendmail
- Clearswift
- Nexor
- Isode MSwitch
- ISS Messenger Workplace

In many cases mail queues can also be monitored for messages that have been stuck for specified period of time, providing an early warning of potential performance or connectivity problems.

For Microsoft Exchange 2003 and 2007, mailboxes activity can be monitored for events such as messages being deleted before they are read, copying of messages to another folder, and delegate user logins.

Bespoke Agents

If data is in a proprietary format or can only be accessed using an application-specific API, new agents can easily be created as a bespoke client development. Once the client has been created, how it is installed, started, provided with its run time parameters and how it relays information to the central Sentra repository database are all based on standard Sentra practices, whatever the nature of the client.

Data Analysis

As the central repository is being updated by the extraction agents, the information can be processed in real time by a variety of standard Sentra techniques.

Rules can be built to analyse the data and alert to a console, an enterprise manager or a mobile technology. The alert can be a simple case of checking the level of a value in a table row. More complicated rules based on aggregating data from a number of rows, or tables, or systems, or over time can be built on request as part of a customer installation.

Graphs or charts can be constructed to show the progression of real time metrics and alerts. An example would be transaction throughput. The charts can be linked together to create a drill down approach to identifying root causes. At the highest level, a non-technical Service oriented view, known as the Hypervisor, can be used as the entry point to the lower level charts. This graphical view is available through a web browser.

Finally, the Sentra database can provide a wealth of intra-day or longer term Management reporting using standard SQL reporting tools such as Microsoft SQL Reporting Services. An example report would be to trend payment system activity during a calendar month. The product is equipped with standard reports, but users can produce their own.

The retention period for any data stored in the repository can be configured by the Sentra Administrator, e.g. data older than 'x' days will be deleted automatically by a core Sentra module.

Sentra is equipped with its own database replication facilities. Alternatively, RAID technology can be used to protect data.

The Sentra web application facilities can be used to construct a view of the captured data. The underlying charts can show alerts that have been configured in the rules engine or the progression of a performance metric such as a throughput rate, over time. If the alert has been generated for a specific transaction, e.g. a targeted queue, then the full record image can be displayed.

The content, style and display sequence of the charts are totally at the discretion of the user. Example alerts and charts can be found at the end of this paper.

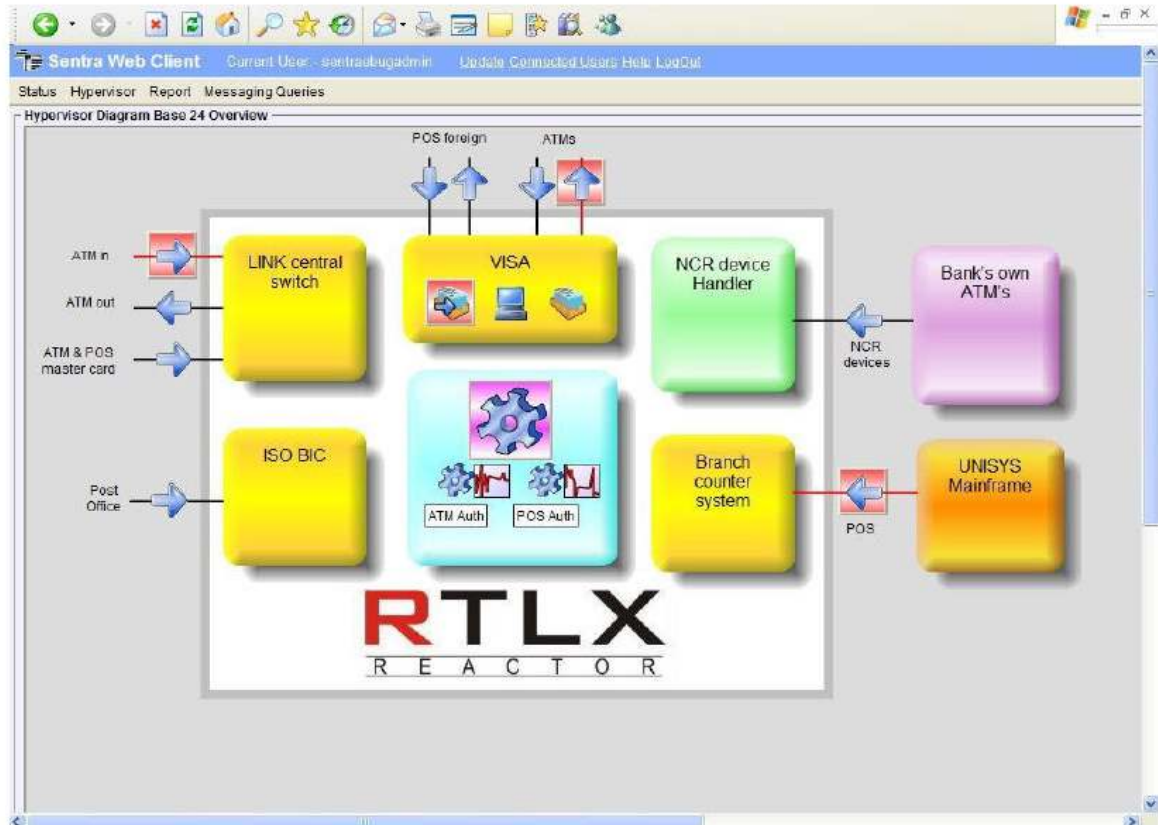
Users can also build and submit ad-hoc database queries by creating a filter consisting of a selection of database fields and values. This query can be saved for regular submission.

The Sentra product is also equipped with a standard set of reports, produced using the Microsoft SQL Reporting Services facility. Users can create their own reports using an ODBC-compliant application. Reports executed by Sentra can be scheduled to run automatically and the results can be emailed if required.

Sample Alerts, Graphs and Reports

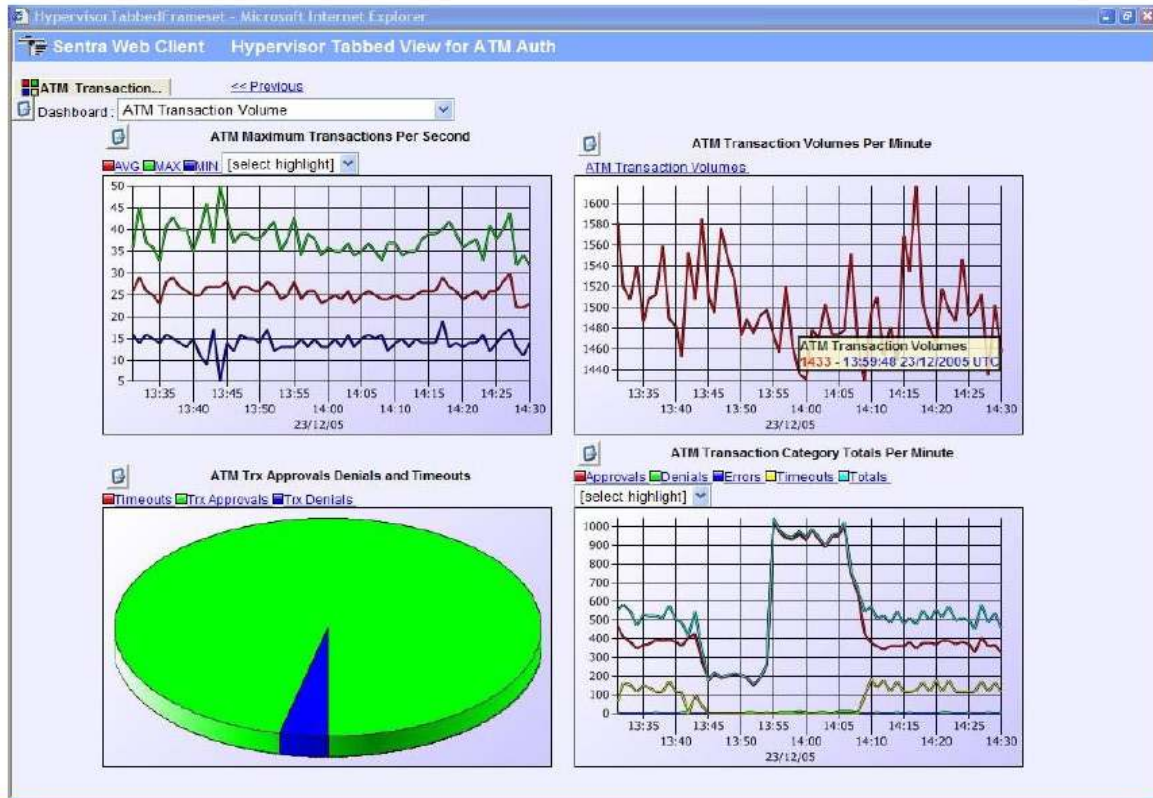
Hypervisor Diagrams

Once the data has been transferred to the Sentra Server, it is available for analysis and reporting. Sentra enables users to configure their own views to match their individual reporting requirements. These views are known as Hypervisor diagrams. An example of one of these diagrams views is given below. The diagram represents a simple monitoring solution for a payments gateway system:



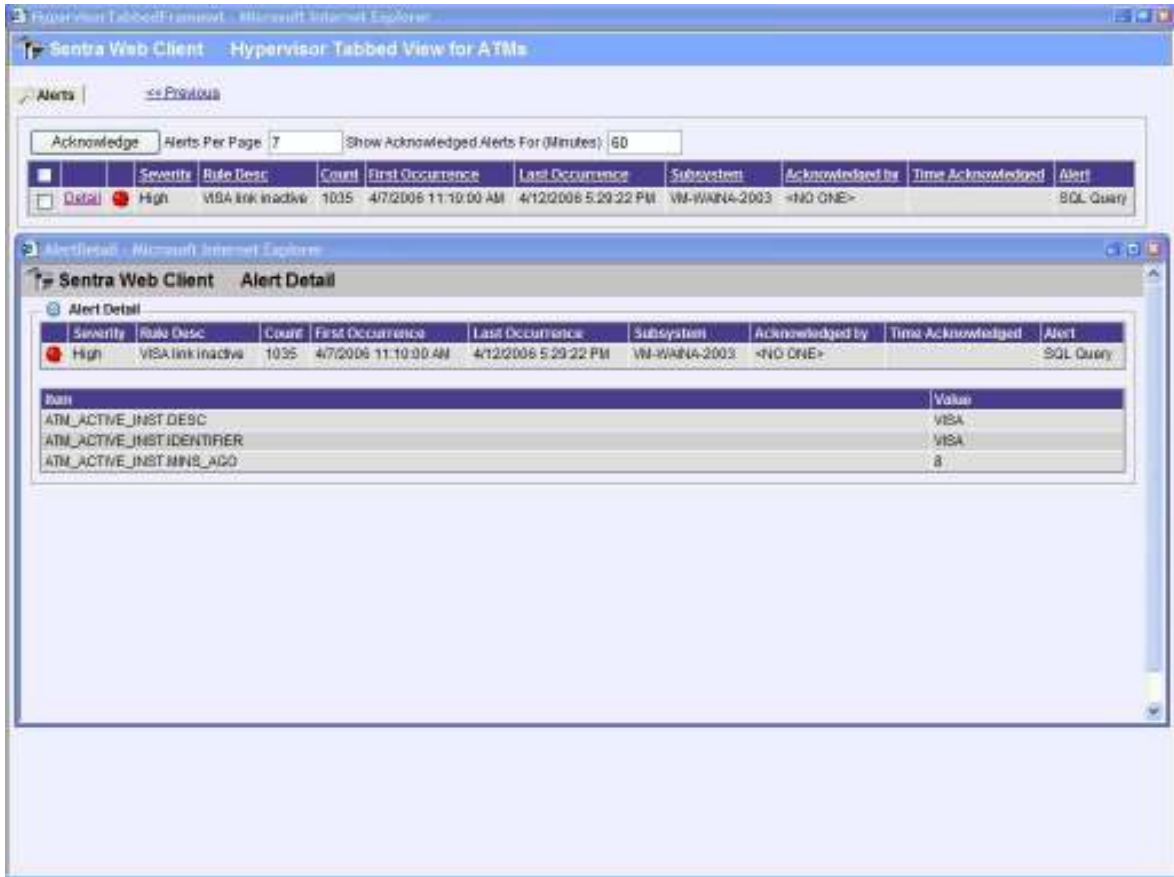
Dashboard

From the previous Hypervisor view, users can drilldown into dashboards that show more detailed metrics of the payments gateway system, as shown below. The content of the underlying charts and the sequence in which they are displayed is at the discretion of the user.



Alert Views

The Rules engine can trap pre-defined conditions. Associated errors can be escalated to a local console linked into the Hypervisor view as depicted below, an Enterprise Management platform or to a mobile technology such as SMS or Email.



The screenshot shows two browser windows from the Sentra Web Client. The top window, titled 'Hypervisor Tabbed View for ATMs', displays a list of alerts. The bottom window, titled 'Alert Detail', provides a detailed view of a selected alert.

Alert List (Top Window):

Severity	Rule Desc	Count	First Occurrence	Last Occurrence	Subsystem	Acknowledged by	Time Acknowledged	Alert
High	VISA link inactive	1035	4/7/2006 11:10:00 AM	4/12/2006 5:29:22 PM	VM-WANA-2003	<NO ONE>		SQL Query

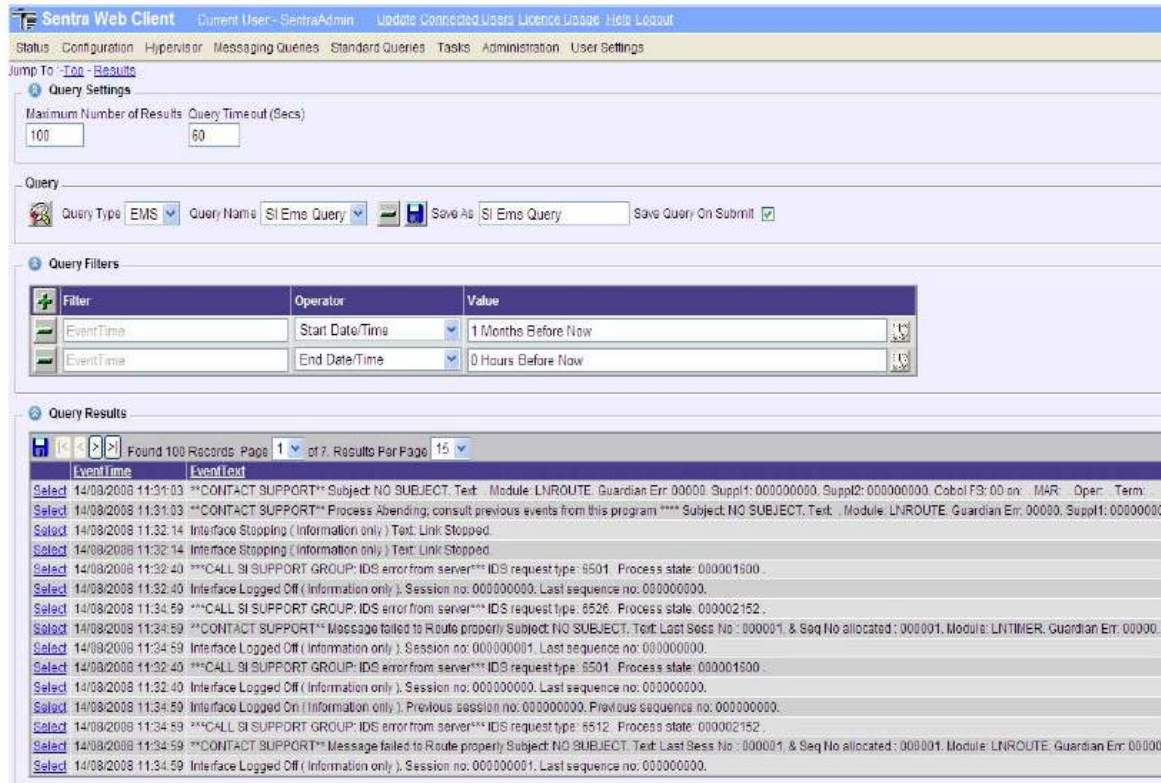
Alert Detail (Bottom Window):

Severity	Rule Desc	Count	First Occurrence	Last Occurrence	Subsystem	Acknowledged by	Time Acknowledged	Alert
High	VISA link inactive	1035	4/7/2006 11:10:00 AM	4/12/2006 5:29:22 PM	VM-WANA-2003	<NO ONE>		SQL Query

Item	Value
ATM_ACTIVE_INST.DESC	VISA
ATM_ACTIVE_INST.IDENTIFIER	VISA
ATM_ACTIVE_INST.MINS_AGO	8

Ad-hoc Queries and Reports

Users can build an ad-hoc query against the collected data, using a combination of data attributes. The query can be saved and resubmitted at a later date if required. This example shows an ad-hoc query executed against some operating system events, captured using a generic log file agent.



The screenshot displays the Sentra Web Client interface. At the top, there is a navigation bar with options like 'Status', 'Configuration', 'Hypervisor', etc. Below this, the 'Query Settings' section includes input fields for 'Maximum Number of Results' (set to 100) and 'Query Timeout (Secs)' (set to 60). The 'Query' section shows 'Query Type' as 'EMS' and 'Query Name' as 'SI Ems Query'. The 'Query Filters' section contains a table with two filters:

Filter	Operator	Value
EventTime	Start Date/Time	1 Months Before Now
EventTime	End Date/Time	0 Hours Before Now

The 'Query Results' section shows a list of 100 records. The first few records are as follows:

EventTime	EventText
14/08/2008 11:31:03	**CONTACT SUPPORT** Subject: NO SUBJECT, Text: Module: LNROUTE, Guardian Err: 00000, Suppl1: 000000000, Suppl2: 000000000, Cobol FS: 00 on: MAR, Oper: Term:
14/08/2008 11:31:03	**CONTACT SUPPORT** Process Abending, consult previous events from this program **** Subject: NO SUBJECT, Text: Module: LNROUTE, Guardian Err: 00000, Suppl1: 000000000
14/08/2008 11:32:14	Interface Stopping (Information only), Text: Link Stopped.
14/08/2008 11:32:14	Interface Stopping (Information only), Text: Link Stopped.
14/08/2008 11:32:40	***CALL SI SUPPORT GROUP: IDS error from server*** IDS request type: 6501, Process state: 000001600.
14/08/2008 11:32:40	Interface Logged Off (Information only), Session no: 000000000, Last sequence no: 000000000.
14/08/2008 11:34:59	***CALL SI SUPPORT GROUP: IDS error from server*** IDS request type: 6526, Process state: 000002152.
14/08/2008 11:34:59	**CONTACT SUPPORT** Message failed to Route properly Subject: NO SUBJECT, Text: Last Sess No: 0000001, & Seq No allocated: 000001, Module: LNTIMER, Guardian Err: 00000.
14/08/2008 11:34:59	Interface Logged Off (Information only), Session no: 000000001, Last sequence no: 000000000.
14/08/2008 11:32:40	***CALL SI SUPPORT GROUP: IDS error from server*** IDS request type: 6501, Process state: 000001600.
14/08/2008 11:32:40	Interface Logged Off (Information only), Session no: 000000000, Last sequence no: 000000000.
14/08/2008 11:34:59	Interface Logged On (Information only), Previous session no: 000000000, Previous sequence no: 000000000.
14/08/2008 11:34:59	**CONTACT SUPPORT** Message failed to Route properly Subject: NO SUBJECT, Text: Last Sess No: 0000001, & Seq No allocated: 000001, Module: LNROUTE, Guardian Err: 00000.
14/08/2008 11:34:59	***CALL SI SUPPORT GROUP: IDS error from server*** IDS request type: 6512, Process state: 000002152.
14/08/2008 11:34:59	**CONTACT SUPPORT** Message failed to Route properly Subject: NO SUBJECT, Text: Last Sess No: 0000001, & Seq No allocated: 000001, Module: LNROUTE, Guardian Err: 00000.
14/08/2008 11:34:59	Interface Logged Off (Information only), Session no: 000000001, Last sequence no: 000000000.

A4 Style Business Reports

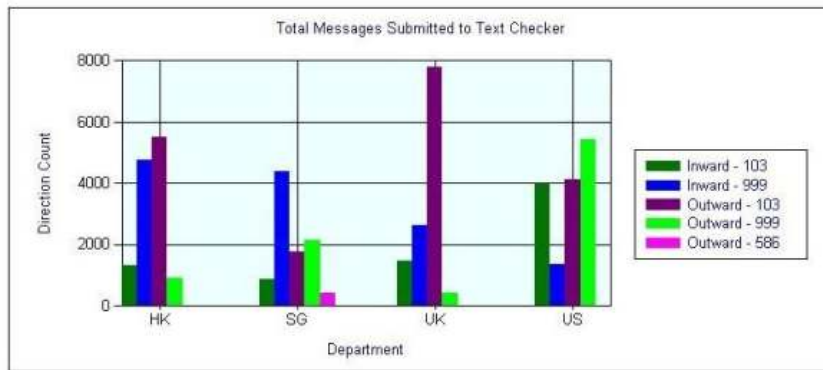
This graphic below shows an example of an A4-style business report detailing the payment messages processed by fraud-detection module that was being monitored by the Sentra application.



Total Messages Submitted to Text Checker

Report Parameters

Date Range : 17/08/2008 09:00:00 to 20/08/2008 16:00:00





Insider Technologies is a UK-based software and services company quality certificated to ISO 9001:2008 and TickIT. Operating in the Financial and Messaging markets, it provides Service Management, Tracking, Bespoke Software and Information Mediation solutions.

A cross section of our customers would include Banking and Financial Services, Telecommunications Providers and Government and Military Institutions.

For details about the full range of products and services available from Insider Technologies Limited, please contact our Product Development Centre in Salford Quays (home to MediaCityUK), at:

Insider Technologies Limited
Spinnaker Court
Chandlers Point
Broadway
Salford Quays
MANCHESTER, M50 2YR
United Kingdom

Tel: +44 (0)161 876 6606
Fax: +44 (0)161 868 6666

e-mail: support@insidertech.co.uk
Website: <http://www.insidertech.co.uk>



ISV/Software Solutions