

# Sentra

## White Paper



## Table of Contents

<b>Management for Payment, Messaging and Middleware Environments.....</b>	<b>3</b>
<b>Introduction to Sentra.....</b>	<b>4</b>
<b>Sentra Product Overview and Benefits.....</b>	<b>5</b>
<b>Sentra Architecture.....</b>	<b>7</b>
<b>Sentra Console.....</b>	<b>10</b>
<b>Sentra Hypervisor.....</b>	<b>14</b>
<b>Monitoring and Alerting.....</b>	<b>15</b>
<b>Message Tracking.....</b>	<b>17</b>
<b>Mailbox Queries.....</b>	<b>18</b>
<b>Transaction and Payments Monitoring.....</b>	<b>19</b>
<b>XML Monitoring.....</b>	<b>21</b>
<b>Remote Service / Process Management.....</b>	<b>22</b>
<b>Reporting and Management Information.....</b>	<b>23</b>
<b>Reporting Capability.....</b>	<b>24</b>
<b>Self-Refreshing Charts.....</b>	<b>25</b>
<b>Summary of Reporting Component.....</b>	<b>26</b>
<b>Platform Support and System Requirements.....</b>	<b>27</b>
<b>Implementation, Training and Services.....</b>	<b>30</b>

## Management for Payment, Messaging and Middleware Environments

Both transaction processing and messaging are mission critical services within any 21st century organisation and a key element of any service provider's portfolio. However, the demands on these system types are continually increasing.

The volume of payments and messages being sent continues to grow exponentially as users exploit increasing availability and functionality of messaging-based services.

Service Level Agreements (SLAs) between both end-users and service providers are being imposed more frequently (both within organisations and also in outsourcing arrangements). These are often extremely demanding, where **99.999%** availability SLAs are not uncommon, meaning less than one hour downtime per year!

Managing the messaging and payments systems therefore becomes ever more important to ensure that the service it provides is meeting the intense demands placed upon by its users and that it will continue to do so in the future. The consequences of ignoring these issues are potentially severe. Messaging and payment service failures mean transfer of information is compromised, directly impacting on the financial health of an organisation either through missed opportunities or damage to its reputation.

It is therefore vitally important to be alerted immediately to any potential threats to the messaging and payment services. Appropriate escalation and intervention systems should be implemented to ensure that problems are responded to in an appropriate and efficient manner. This will provide a greater confidence that the service is being maintained and SLAs met.

Looking to the future, ensuring that the service continues to meet future demands requires constant monitoring of performance data. Historical data-gathering capability linked to trend analysis provides the means to interpret how systems are performing and, importantly, the basis for effective capacity planning. This will ensure that upgrades and new hardware and software can be acquired at the right time and also in a planned manner, thereby avoiding the need to make sudden or last minute decisions.

Occasionally, due to a number of reasons, message routing and deliveries can fail. It is important in these situations that the message can be tracked and located, particularly where the message represents high value information, is a payment or has high security implications. Often, tracking is a difficult and laborious process, which can take a long time. This conflicts with the need for a quick and accurate resolution to the problem. Very few messaging and payments systems provide this capability.

Also, many messaging systems have grown up in a piecemeal fashion, with individual departments or companies joined by mergers having completely different systems in place. Budgetary constraints may mean that these systems cannot be consolidated into a single vendor system. This causes further management headaches for systems administrators and managers, as monitoring has to be done on an individual system basis rather than in a consolidated manner. This leads to inefficiencies, as extra time needs to be spent managing a number of different systems, rather than all at once.

## Introduction to Sentra

Management of IT infrastructure is often facilitated through SNMP-based Enterprise Network Management Systems. By their nature, these systems must have a wide reach, and thereby usually offer only global fault management and configuration. This often leaves many gaps in some of the more specialised parts of the environment. Sentra fills these gaps by providing a comprehensive set of tools for management of single and multi-platform systems.

Furthermore, Enterprise Management Systems often work at a component level, providing a view of availability and performance of system and application elements. These views alone, however, rarely interpret how overall service levels are impacted. In fact, once the performance of several separate components has degraded, service levels may already be affected.



Sentra is able to collect the appropriate data and interpret and present it in such a way to be able to rapidly identify genuine threats to service provision. This means that threats can be identified and acted upon before they turn into problems, particularly those that affect your users, customers and ultimately, your bottom line.

Once fully implemented, Sentra will produce a significant return on investment by lowering total cost of ownership (TCO), maximising resource utilisation and availability of business functions. The remainder of this document gives an introduction to how Sentra achieves this.

## Sentra Product Overview and Benefits

Sentra is a client-server software application for centralised management of multi-vendor and multi-platform platforms. It provides extensive benefits that enable optimal availability, functionality and performance of service provision.

Sentra achieves this by providing centralised alerting, escalation, intervention, tracking and reporting tools from a single console view. Furthermore, Sentra collects data from many sources (system components, application events, log files) and interprets them in terms of how they affect overall service provision. Real-time views mean that service levels can be proactively maintained. Historical data mining and reporting capability enables efficient resource allocation and capacity planning.

The precise nature of the deployment of Sentra is variable from one customer to another, but most will utilise a combination of the following features:

- Sentra Console is compatible with all modern internet browsers, e.g. IE, Chrome, Firefox
- Centralised, rules-based system, application and service level monitoring.
- Automated alerting to service threats and SLA violations through e-mail, SMS, SNMP trap, script files, batch files.
- Intelligent escalation of alerts to TIVOLI™, HP Operations Centre™, HP ServiceDesk™, BMC Patrol™ and Reflex
- Automated problem resolution, e.g. restarting of failed applications.
- Platform and application availability monitoring.
- Monitoring of the availability and response of key internet services, such as HTTP, FTP, SMTP, POP3 and IMAP4.
- XML monitoring including UNIFI payment formats - <http://www.iso20022.org>
- HPE NonStop monitoring of the Event Management Subsystem (EMS) with complete dynamic filtering of events from any configured collector.
- BASE24™ POS, ATM and Interchange monitoring of both TLF and PTLF transaction log files.
- Simplified Service Level Agreement (SLA) management.
- Graphical, End-to-End message tracking.
- Monitoring of a wide variety of e-mail messaging systems and gateways such as MS Exchange, SendMail, Isode, Nexor, Critical Path, NetTel (Clearswift), ISS Messenger Workplace, ISOCOR and OSI/MHS. Both X400 and SMTP e-mail protocols are supported.

Full auditing of MS Exchange mailbox activity - Identify when mail is read, forwarded, deleted and moved. Monitor when delegate users and unauthorised users access a mailbox. Ideal for high security messaging environments.

Queue Monitoring, Management and Control - Monitor the size and activity of a queue, delete messages and force non-delivery reports.

Monitoring of middleware systems such as IBM WebSphere MQ (formerly known as MQ Series).

NCR Authentic Payments Systems

Mail traffic pattern assessment.

Capacity planning.

Reporting on messaging issues.

Billing or usage analysis.

SNMP IN for monitoring of network components e.g. Routers.

Increased depth of monitoring and intelligent data handling means that relevant data is readily available in either real-time or historical formats. More informed decision-making is therefore possible, improving the ability to respond to problems and to plan effectively for the future. A full implementation of Sentra means that previously labour-intensive tasks can be automated and centralised. This improves resource utilization and reduces total cost of ownership (TCO).

## Sentra Architecture

Sentra employs agents, called extraction programs, to collect and process data from a variety of sources, and transmit this data to a central server location via a TCP/IP (LAN, WAN or dialup) connection. A process on the server is responsible for committing the data to an SQL Server database. Agents can be deployed on Windows, Unix, Linux and HP NSK platforms, to capture both messaging-specific data and platform performance data.

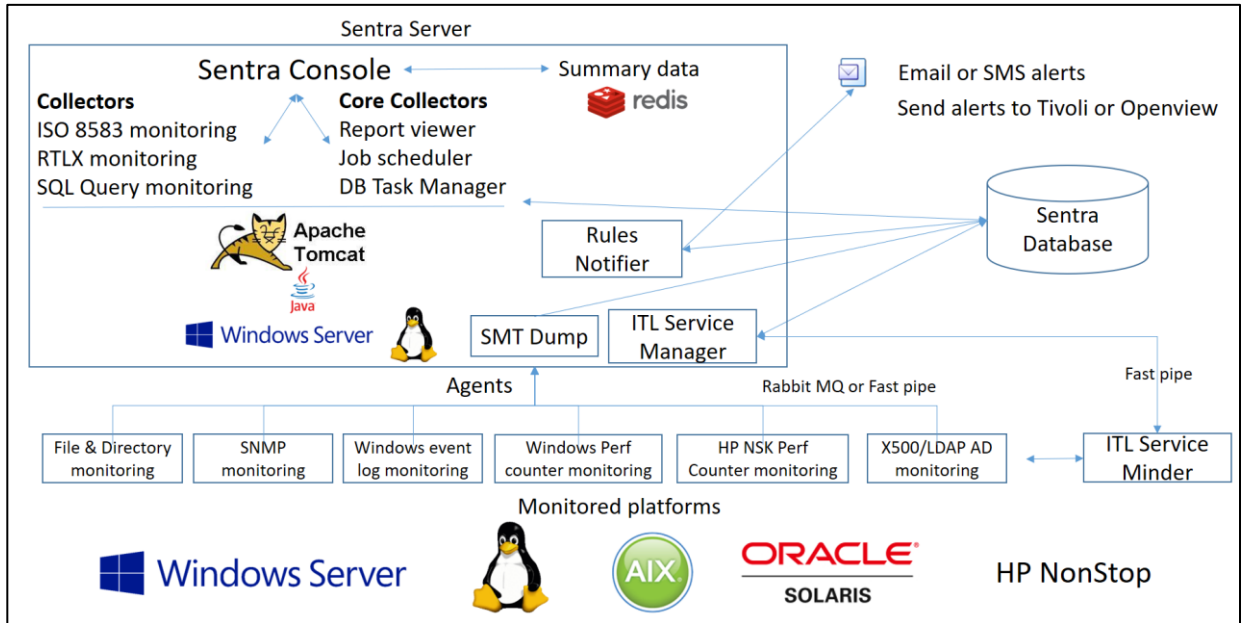
Sentra provides the user with the ability to rapidly deploy these extraction programs across many machines in a corporate network. Sentra enables users to configure, control and monitor these services, all from a central console.

The extraction programs can be configured to collect data and monitor the performance using data from many different sources, such as:

- Messaging and Middleware System Events
- Message and Middleware Queues
- Windows Event Log details
- Windows Performance Counters
- All XML feeds, e.g. BASE24-eps, COPE & STAR by Software Integrators
- ORACLE
- Unix/Linux Performance data
- HPE NonStop EMS log alerts
- HPE NonStop Performance Metrics
- BASE24 TLF and PTLF transactions logs
- NCR Authentic
- Windows file system directories
- Internet services, e.g. HTTP, FTP, SMTP, POP3, IMAP4
- Mailbox Activity Events
- Security Events
- Enterprise X500 Directories
- Unix/Linux Syslog

Sentra also features a user-configurable extraction program, which is able to capture and evaluate data from any application that instruments itself via a structured text log file. This extraction program has been configured to provide support for proprietary messaging applications in the secure government and defence arena, and is also shipped pre-configured to handle Microsoft Proxy Log alerting and reporting.

By collecting data and processing data from these sources, Sentra enables the user to access data that is generated as a result of actual events occurring in the environment being monitored. This is superior to methods such as sending test messages and simple “pinging” of devices as it represents a typical end-users experience of the system. Furthermore, as the data is constantly passed to the central server, it is available for interrogation virtually immediately (subject to network availability and transfer rates), thereby providing real-time management of the system.



The Sentra Server provides several key functions. One of these is message tracking. An extensive query tool enables users to query the database and thereby track individual messages across the entire system (in this case, the information will typically have been captured from e-mail or middleware message system logs or via programmatic interfaces).

Sentra features powerful rules evaluation capabilities. Simple rules can be evaluated by extraction programs as data is captured, e.g. checking for the occurrence of a non-delivered message or a busy CPU. More complex rules are evaluated on the Sentra server. Typical messaging system’s SLAs require an evaluation of the overall end-to-end messaging system processing time. This is usually calculated as the time a message arrives in the monitored environment, to the time it leaves the environment. The message may traverse through several different platforms such as Windows, Solaris, Linux, HPE NonStop and (in the case of email messages) through several different messaging systems. Sentra was specifically designed to monitor these types of SLAs. The rules engine is linked to a sophisticated alerting system. This is able to employ a variety of mechanisms such as SMS or e-mail to alert individuals and groups to service threats.



Reporting is a key feature of Sentra. This is made possible through use of the industry standard Microsoft Reporting Services package, enabling a wide variety of report formats to be generated. Reports can be run on user demand from the Sentra console and Sentra also features a report scheduler. This is typically used to deliver reports to key personnel via e-mail on a daily, weekly or monthly basis. Sentra also provides, through web based Chart and Hypervisor views, user configurable monitoring capabilities. This enables specific information to be targeted at specific audiences.

## Sentra Console

One of the primary aims of Sentra is that it should allow the user to easily and quickly manage all aspects of the messaging environment from a single, central console. With this in mind, the browser console view has been designed to be easy to navigate and to allow rapid access to data at all times.

The Sentra Console uses Explorer Tree methodology (similar to Windows Explorer™) to provide an easy and familiar means of configuring, managing and monitoring one or more subsystems.

The tree is split into three main categories:

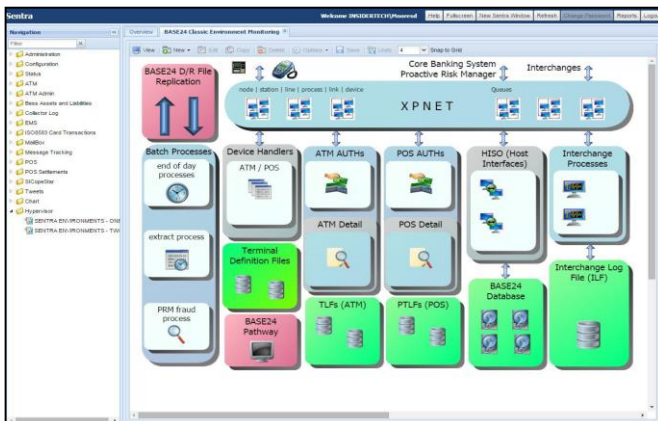
**Administration** – provides access to user and user group management, including specification of user access permissions to key Sentra features.

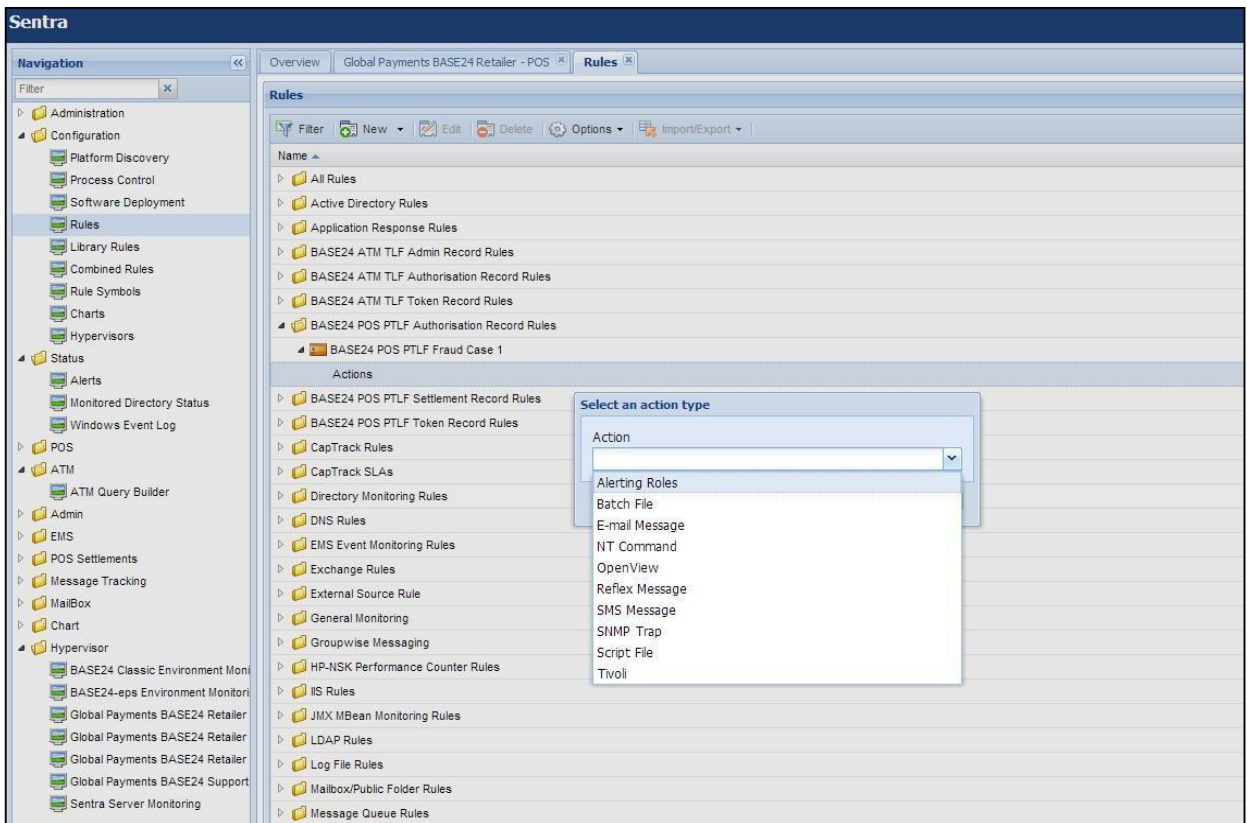
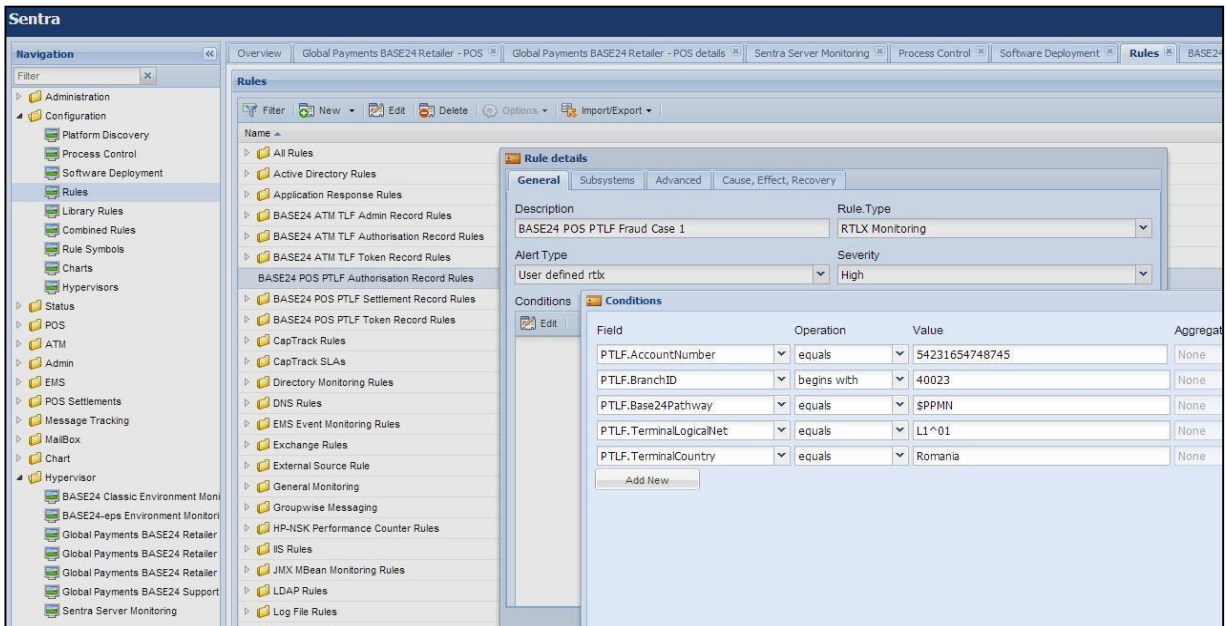
**Subsystem Status** - provides access to any of the data captured by Sentra. This includes access to Sentra's reporting facilities, where users can view reports generated using Microsoft Reporting Services, or query messaging system data. The user can view Windows event logs, Unix system logs, Server and internet service availability and performance, X500 availability and performance, and more

**Configuration** – provides access to extraction program deployment views, and the rules configuration screens.

The main Sentra toolbar is used to add, amend and delete items within the tree. These procedures are generic and are implemented in the same way for every part of the tree structure.

A central feature is the Hypervisor View, which provides a graphical representation of the systems being managed. The view is easily customisable, and can be configured to represent a logical network topology or a messaging service view. The view enables the user to see at glance any events or problems that have occurred on any platform or key service in the overall managed system.





Whilst many users are happy to view their network or messaging systems in a traditional graphical view, others now prefer to view their systems in several different ways.

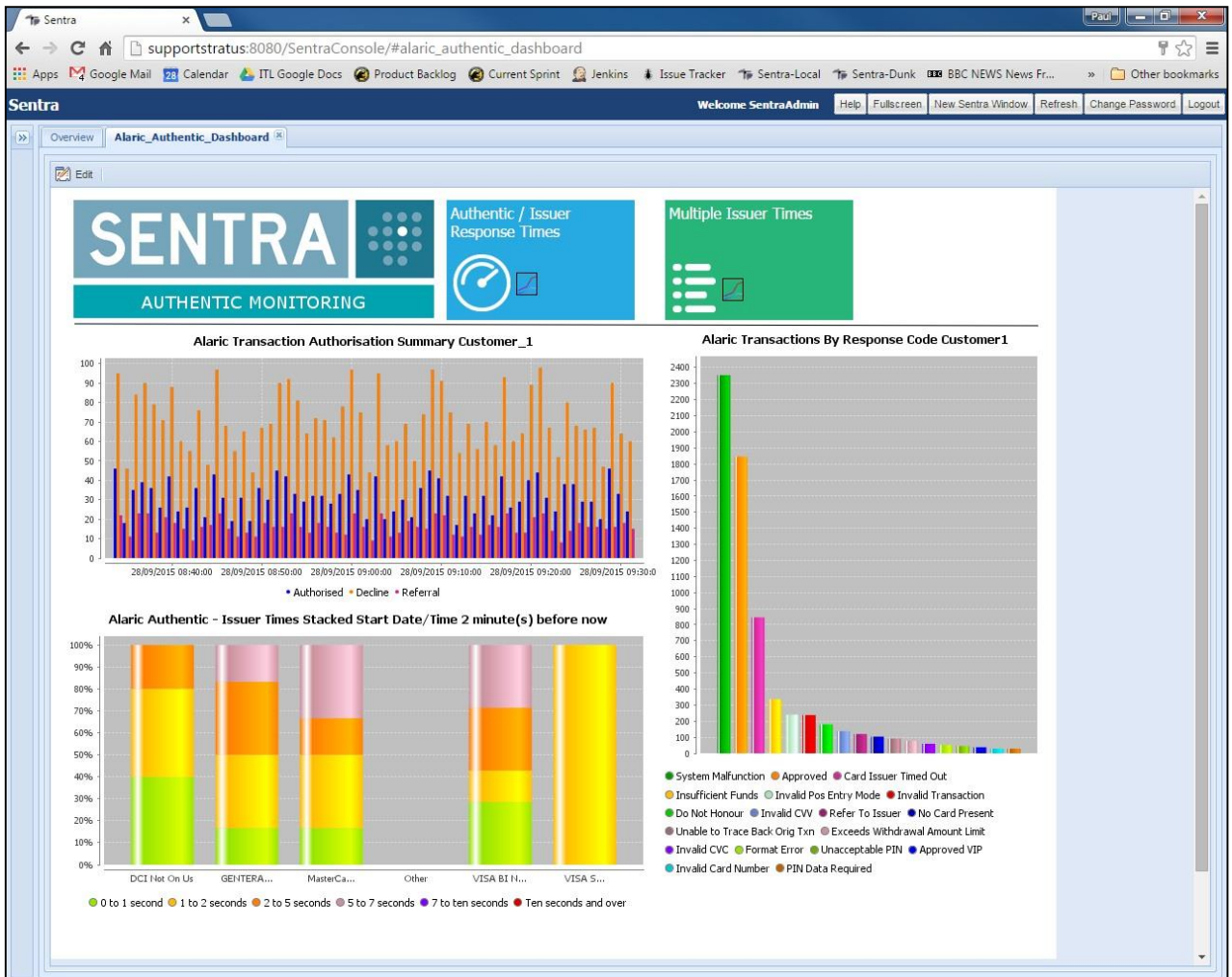
For example, business managers don't wish to see technical problems – they prefer to see issues in terms of the potential impact on the business. In addition, business managers wish to see key business metrics, whereas Technical personnel prefer to see key performance metrics. Sentra provides a means of satisfying all these users' different monitoring requirements with the Sentra Chart and the Sentra Hypervisor views.



## Sentra Real-Time Charts

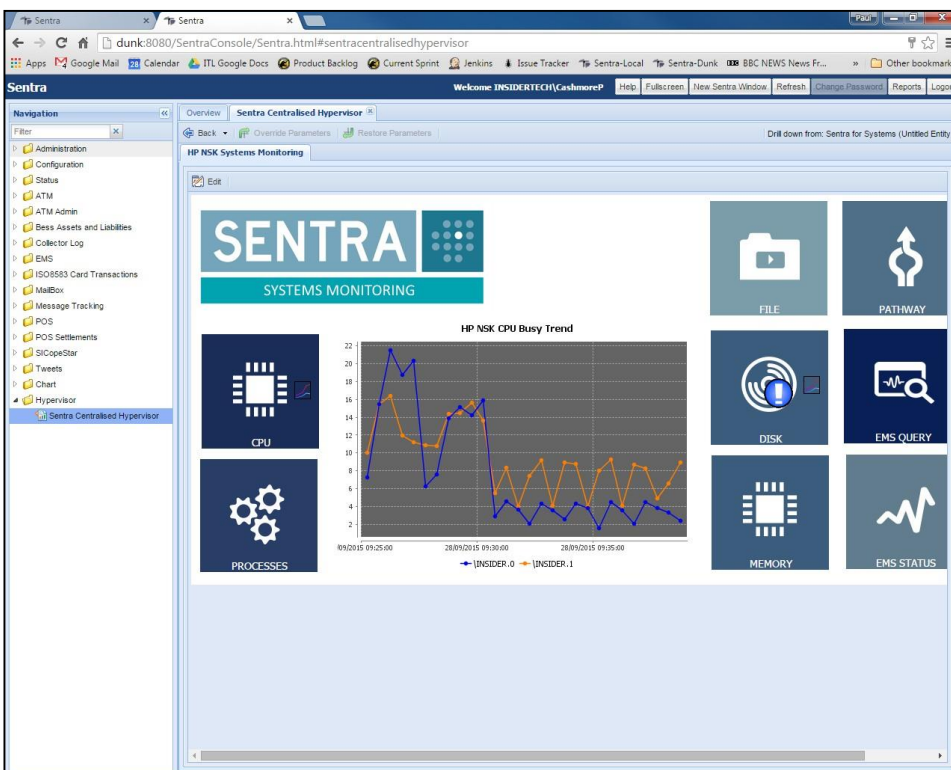
A web-based graphical user interface can be configured to provide a permanent display of key aspects of managed service performance. One or more real-time chart reports can be displayed, each showing a particular aspect of monitored service performance. For example, a graph of message server queue sizes can be shown, showing the relative load across multiple mail servers. Charts can be linked together, to provide drilldown capabilities, e.g. to allow analysis of the contents of a particular message server queue.

Below are example screenshots of a typical Sentra Charts view, contained within a hypervisor:



## Sentra Hypervisor

The Sentra Hypervisor provides users with the ability to design and configure their own monitoring views. Users can create their own views which represent key aspects of their business. These views can be configured to highlight system or business problems, and support drilldown capabilities to enable users to link in more detailed technical views. Users can also provide links to chart views, or to other web-based third party applications.



## Monitoring and Alerting

Sentra provides a centralised, rules-based means of monitoring Service Level Agreements (SLAs) and processes running on the machines being monitored. Predefined rules are available for all major data types contained within the Sentra database, thereby providing an extremely powerful systems management tool. A wide variety of rules are provided. A brief list is given below of some of types of rules that Sentra supports, together with a couple of typical examples:

- Payment and Transaction Rules Examples include: Response from interchange > 1 minute, Transaction Volume down by 10% compared to the same day last week, Denials > 200 per minute, Stand-in (STIP) Transactions > 200 per minute.
- E-mail and middleware messaging system rules Examples include: message delivery failure, message security violation, transfer time SLA across a single message system, end-to end delivery time across multiple systems.
- E-mail and middleware messaging system queue rules Examples include: message stuck in queue, total number of messages in queue > threshold, total size of messages in queue > threshold.
- Mailbox auditing Rules Examples include: meeting declined, task declined, unauthorised mailbox access, delegate access of mailbox, public folder activity.
- Windows Service Rules Examples include: a Windows service has failed
- Windows Event Log Rules Examples include: An application error has been detected, a Windows Security auditing failure has occurred.
- Performance Counter Rules Examples include: CPU Busy > 90%, Disk Space Available < 5% Server
- Availability and Internet Service performance Rules Examples include: Server is down, FTP download response time < 20ms
- X500 Enterprise Directory availability and performance Rules Examples include: Directory is down, LDAP query response time < 50ms
- Application and Database Query Response Monitoring Rules Examples include: SAP Transaction Time > 250ms, SQL query response time < 50ms
- File system directory monitoring rules Examples include: Number of Files in Directory > 20000, Total Size of Files in Directory > 1Gb, File has been deleted, Age of File in Directory > 1 hour

Many other types of rules are also supported.

Sentra also enables rules of different types to be combined. For example, alert if:

```
CPU > 95% BUSY  
AND  
MESSAGING SYSTEM MESSAGES PROCESSED PER SECOND < 10
```

For the above rule, one source of data may be a Windows performance counter, and the other a messaging system log file.

Unlike other enterprise management systems, rules are automatically deployed to all relevant systems; there is no need to physically deploy a new rule onto each monitored platform. A high degree of flexibility in rule configuration is possible, facilitating intelligent problem escalation.

Varying degrees of severity can be set; rules can be excluded from specific platforms; alerts can be configured to be active on certain days of the week and/or different alerts can be generated according to the day and time.

Once a user-defined rule has been violated, a number of actions can be invoked in order to notify appropriate individuals and systems and/or to automate problem resolution routines. These include SMS Messages, Email, Console Alert (through unique Hypervisor service topology view), SNMP Traps, Automatic Process Re-start, Batch Jobs and Script Files.

For SMS and e-mail alert notification, Sentra supports the concept of "Alert Roles" For example, an alert role of "On-call Technical Support Engineer" can be configured. The "On-call Technical Support Engineer" is not a specific individual, but may correspond to a group of individuals who will be on call at different times, according to the time of day and whether the day is a working day or a weekend. A single rule can then be configured to alert the "On-call Technical Support Engineer". When the rule is violated, Sentra will obtain the details of the relevant individual(s) to be notified, based upon the current time.

Alerts can be escalated to more general enterprise management systems such as HP Operations Center and TIVOLI. The alerts can also be forwarded to problem management systems such as HP ServiceDesk and REMEDY.

## Message Tracking

The SENTRA Message Tracking application can track individual and multiple messages across multiple messaging domains using the same console, subject to the appropriate data fields being made available. Sentra can track e-mail messages which use the X.400 and SMTP (Internet) protocols. Middleware messaging systems such as WebSphere MQ are also supported. Message tracking user queries are performed against the central data store using a graphical query builder.

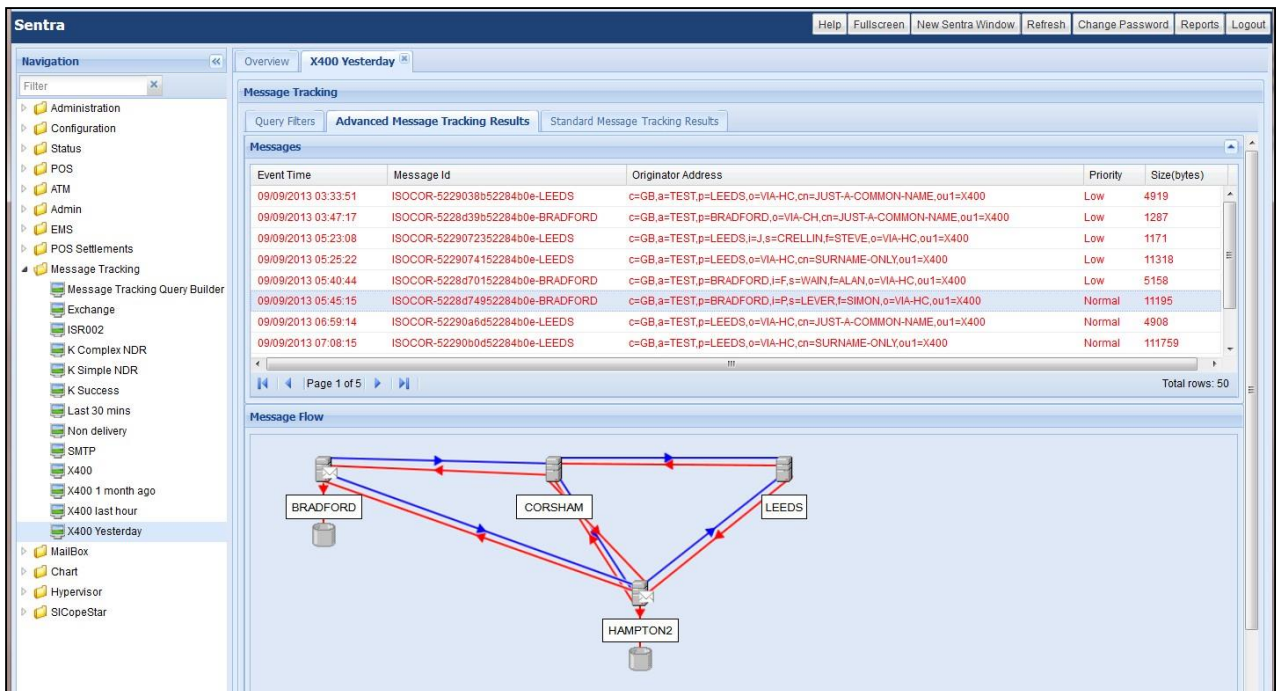
Queries can be as detailed or simple as a user requires. For an e-mail message, typical search details might be Sending Time, Message Identifier, Originator or Recipient address. As searches are performed against a single database, results from many Message Transfer Agents (MTAs) can be displayed in a single view. Furthermore, this is a much quicker process than manually examining message logs, which may be the only viable alternative.

The message results view provides details of all originated messages that meet the search criteria. Drill-down facilities provide recipient and diagnostic information, including all events generated to facilitate delivery of message.

The history pane displays the full life-cycle of a message, including information pertaining to the MTAs through which the message has passed, the reports that it has generated, (i.e. Non Deliveries, Deliveries etc.), and the message IDs that it has had as it has passed through any e-mail gateways, such as an X400, SMTP gateway.

### Summary of Message Tracking Component:

Enables significantly faster message tracking than provided by alternative methods. Messages can be tracked across multiple messaging systems on multiple platforms from a single console.



Event Time	Message Id	Originator Address	Priority	Size(bytes)
09/09/2013 03:33:51	ISOCOR-5229038b52284b0e-LEEDS	c=GB,a=TEST,p=LEEDS,o=VIA-HC,cn=JUST-A-COMMON-NAME,ou1=X400	Low	4919
09/09/2013 03:47:17	ISOCOR-5228d39b52284b0e-BRADFORD	c=GB,a=TEST,p=BRADFORD,o=VIA-CH,cn=JUST-A-COMMON-NAME,ou1=X400	Low	1287
09/09/2013 05:23:08	ISOCOR-5229072352284b0e-LEEDS	c=GB,a=TEST,p=LEEDS,i=J,s=CRELLIN,f=STEVE,o=VIA-HC,ou1=X400	Low	1171
09/09/2013 05:25:22	ISOCOR-5229074152284b0e-LEEDS	c=GB,a=TEST,p=LEEDS,o=VIA-HC,cn=SURNAME-ONLY,ou1=X400	Low	11318
09/09/2013 05:40:44	ISOCOR-5228d70152284b0e-BRADFORD	c=GB,a=TEST,p=BRADFORD,i=F,s=WAIN,f=ALAN,o=VIA-HC,ou1=X400	Low	5158
09/09/2013 05:45:15	ISOCOR-5228d74952284b0e-BRADFORD	c=GB,a=TEST,p=BRADFORD,i=F,s=LEVER,f=SIMON,o=VIA-HC,ou1=X400	Normal	11195
09/09/2013 06:59:14	ISOCOR-52290a6d52284b0e-LEEDS	c=GB,a=TEST,p=LEEDS,o=VIA-HC,cn=JUST-A-COMMON-NAME,ou1=X400	Normal	4908
09/09/2013 07:08:15	ISOCOR-52290b0d52284b0e-LEEDS	c=GB,a=TEST,p=LEEDS,o=VIA-HC,cn=SURNAME-ONLY,ou1=X400	Normal	111759



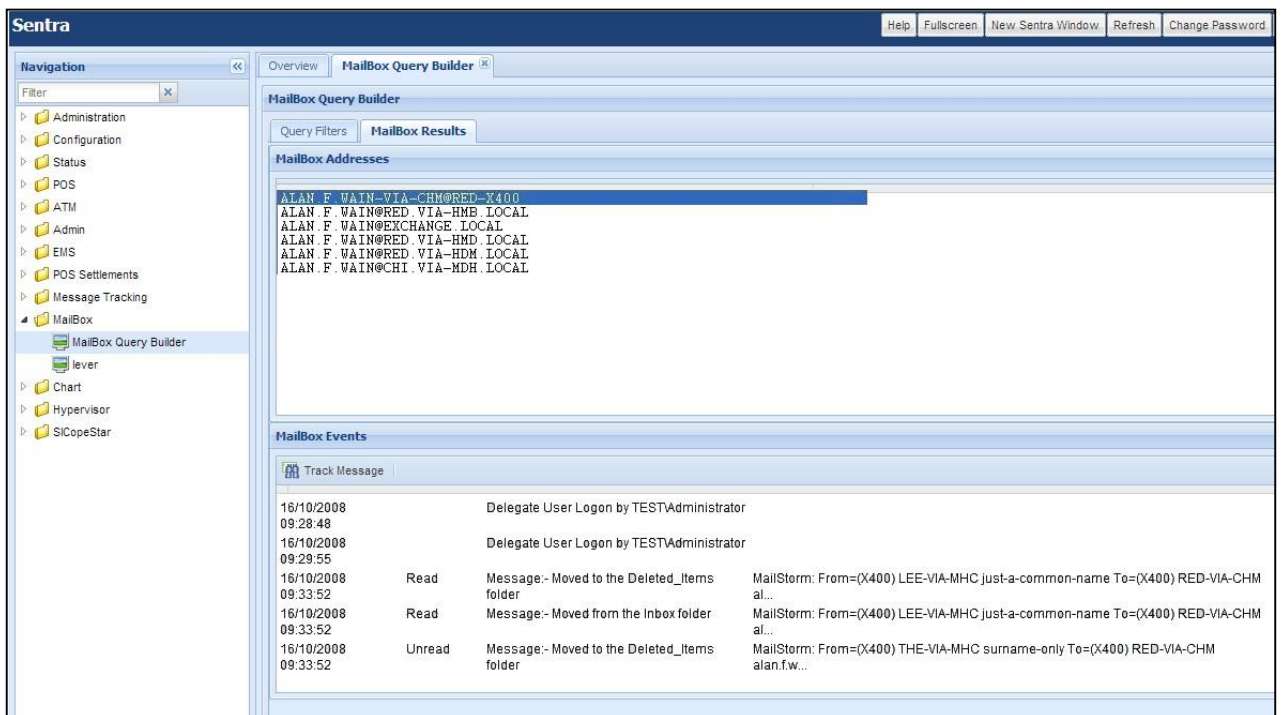
## Mailbox Queries

In addition to collecting data to facilitate Message Tracking, SENTRA can also collect events from some message stores, including the MS Exchange message store. This allows tracking to extend all the way into the mailbox. This information can be viewed using SENTRA's message tracking features, to show how the user handled the email after it was received. This information can also be viewed from the SENTRA Mailbox Query screen.

The Mailbox Query screen allows an email address to be selected by progressively filtering a mailbox address which is known to the system. Once an address is selected, all the mail store events that relate to the address are displayed. The results show when messages are moved or deleted, whether they have been read, and also when delegate users connect to the mailbox. This makes it extremely easy to see when a user last read a message, whether messages are being deleted without being read, or if a delegate user has potentially read or deleted messages. These are questions which would be very difficult to answer by tracking individual messages. The screen also allows a user to track a message back with a single click. This can be done with any store event that contains a message id, thus providing full integration with the existing message tracking features.

Summary of Mailbox Query facility:

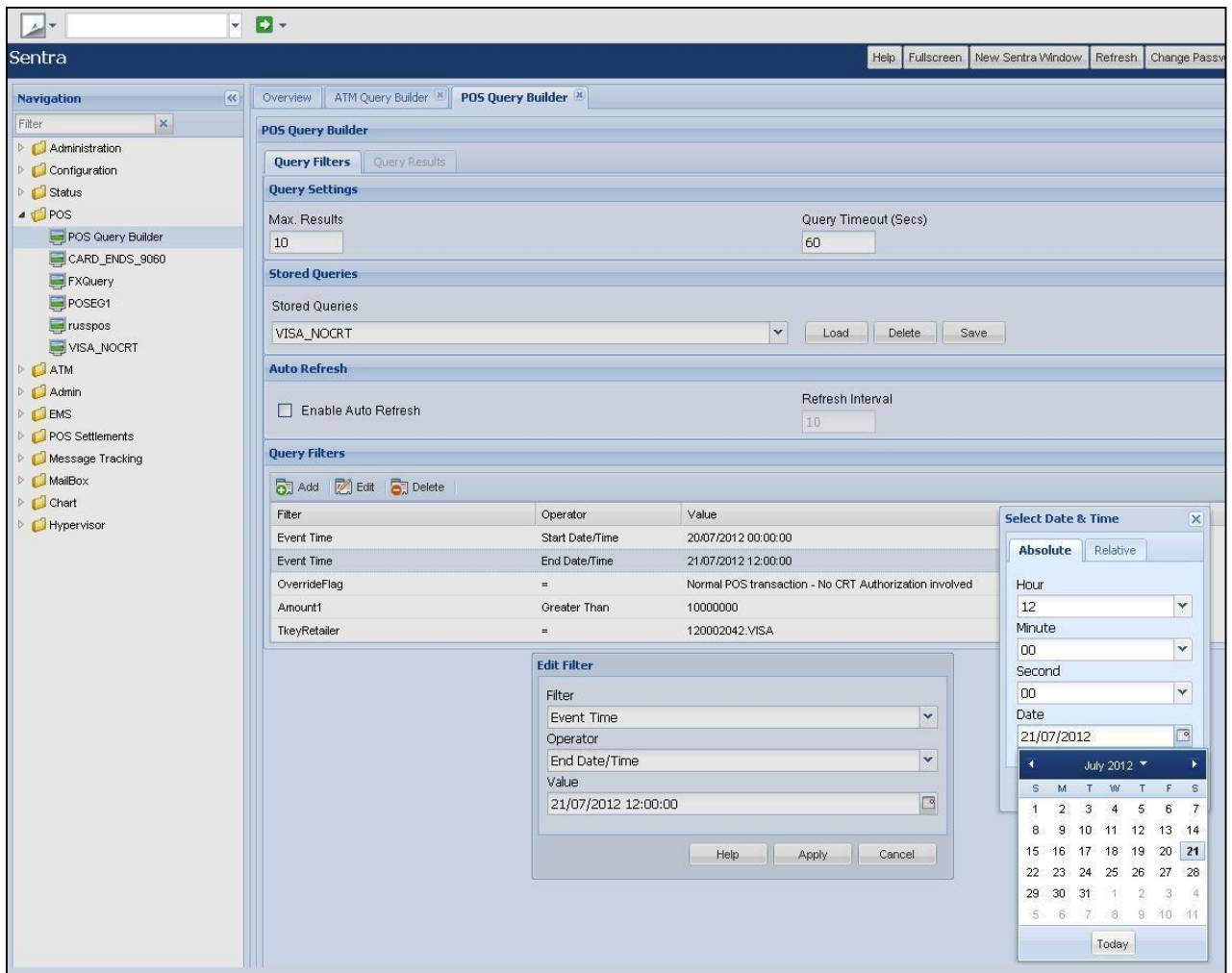
- Shows Delivery, Moves between folders and Deletes (soft and hard).
- Shows Delegate logins to the mailbox using other than the default credentials.
- Provides a powerful overview of mailbox activity.
- Integrated with Message Tracking, providing a convenient alternative method of launching a query.



## Transaction and Payments Monitoring

Insider has created a Sentra module, RTLX, to provide real time monitoring and querying of the transaction flow information created by the ACI BASE24™ ATM/POS application and other payment engines. This Sentra module will maintain a centralised database of transaction data from one or more payment platforms and analyse the information in real time. The outcome of the analysis will be service level alerts, graphs depicting the behaviour of nominated metrics and management reports to help set and achieve Business objectives for the payment application(s) being monitored.

The purpose of the RTLX application is to transfer the payment, ATM and/or POS log information (e.g. BASE24 Classic TLF and PTLF) to a Sentra hosted database in real time so that it can be subjected to standard Sentra processing such as the graphical representation of data, analysis of data based upon rules coupled with alerts and the escalation of alerts to Enterprise Management or mobile technologies. In addition this log database can be retained and accumulated and become the subject of trending analysis and querying including standard and custom transaction tokens.



The screenshot displays the Sentra application interface, specifically the PDS Query Builder module. The interface includes a navigation pane on the left with a tree view of folders such as Administration, Configuration, Status, POS, ATM, Admin, EMS, POS Settlements, Message Tracking, MailBox, Chart, and Hypervisor. The main content area is titled 'PDS Query Builder' and contains several sections:

- Query Settings:** Includes 'Max. Results' (set to 10) and 'Query Timeout (Secs)' (set to 60).
- Stored Queries:** A dropdown menu shows 'VISA\_NOCRT' with 'Load', 'Delete', and 'Save' buttons.
- Auto Refresh:** An option to 'Enable Auto Refresh' is unchecked, with a 'Refresh Interval' of 10.
- Query Filters:** A table lists filters with columns for Filter, Operator, and Value.
 

Filter	Operator	Value
Event Time	Start Date/Time	20/07/2012 00:00:00
Event Time	End Date/Time	21/07/2012 12:00:00
OverrideFlag	=	Normal POS transaction - No CRT Authorization involved
Amount1	Greater Than	10000000
TkeyRetailer	=	120002042.VISA

An 'Edit Filter' dialog box is open, showing the configuration for the 'Event Time' filter. It includes fields for 'Filter', 'Operator', 'End Date/Time', and 'Value'. The 'Value' field contains '21/07/2012 12:00:00'. A 'Select Date & Time' calendar is also visible, showing the date '21/07/2012' selected in a July 2012 calendar view.

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 browser and it is known as Sentra Console.

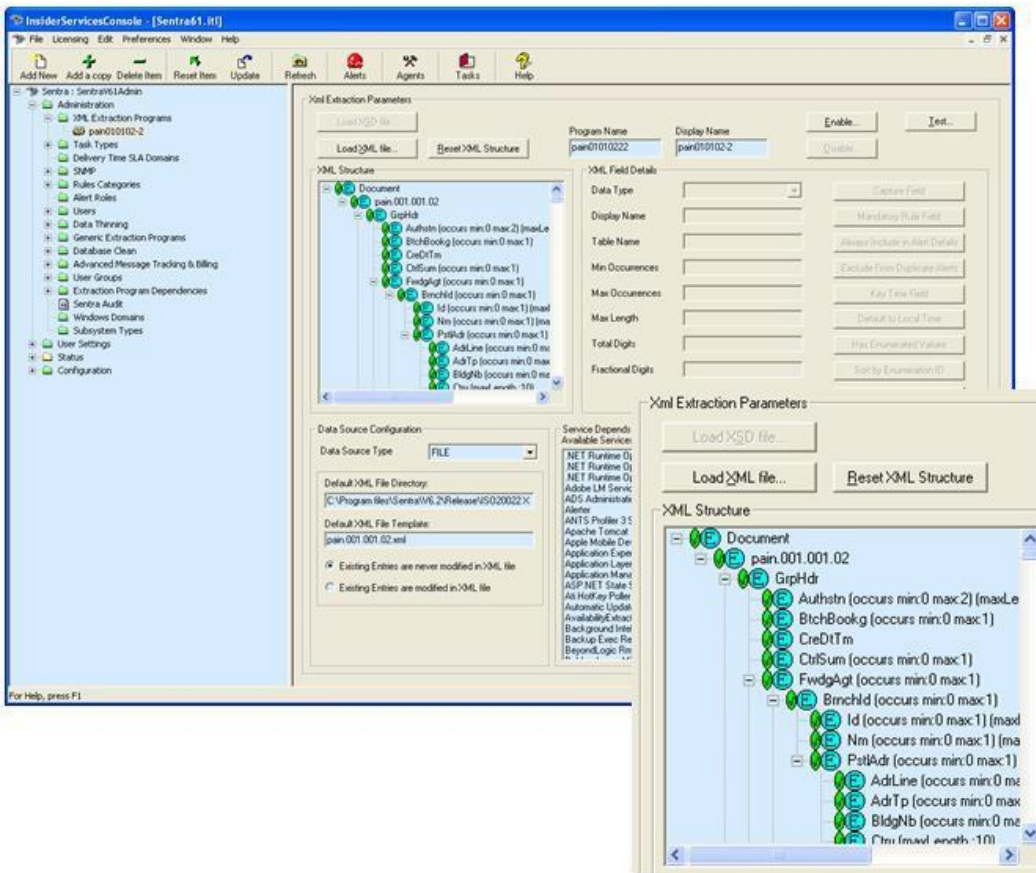
Finally the Sentra database can provide a wealth of intra-day or longer term Management reporting using standard SQL reporting tools such as Microsoft SQL Reporting Services™. An example report would be to trend ATM activity during a calendar month. The product is equipped with standard reports, but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

## XML Monitoring

A general purpose XML agent can be configured to parse any XML data into a hierarchical structure of SQL tables and fields. 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 specifying an XSD schema 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 to monitor any ISO20022-compatible payment or transaction.

A series of these XML agents can be deployed to key monitoring points (waypoints) within a payment processing infrastructure to monitor 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.

The example screenshot below shows the imported Customer Credit Transfer Initiation XML format - pain.001.001.02:

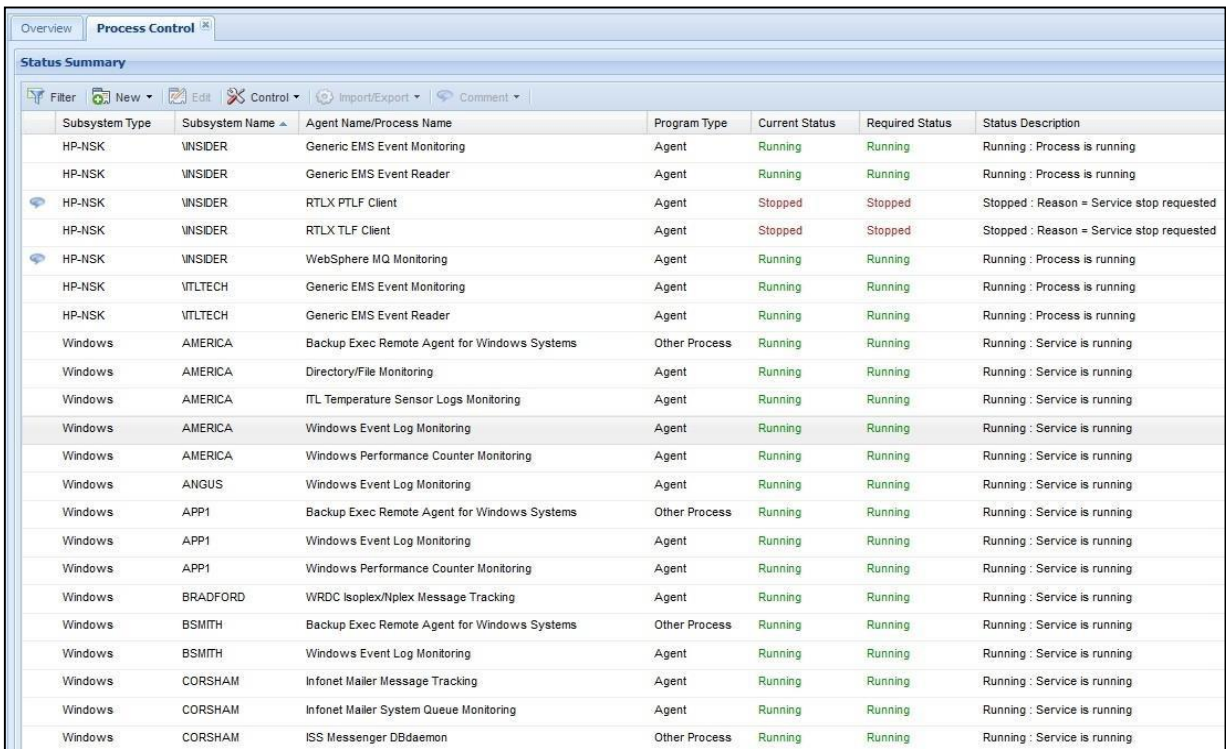


## Remote Service / Process Management

Sentra provides a facility to remotely install, control and monitor Windows Services or programs upon Linux, UNIX, HP NSK and Windows platforms. This includes Sentra data extraction programs, plus any other service or process that normally execute on a given platform. Sentra can automatically restart any monitored programs should they fail. Deployment of Sentra extraction programs across entire Windows domains can be achieved with a few mouse-clicks.

This eliminates the need to physically visit sites to manage systems.

Service and process status can be observed through a global view:



Subsystem Type	Subsystem Name	Agent Name/Process Name	Program Type	Current Status	Required Status	Status Description
HP-NSK	WNSIDER	Generic EMS Event Monitoring	Agent	Running	Running	Running : Process is running
HP-NSK	WNSIDER	Generic EMS Event Reader	Agent	Running	Running	Running : Process is running
HP-NSK	WNSIDER	RTLX PTLF Client	Agent	Stopped	Stopped	Stopped : Reason = Service stop requested
HP-NSK	WNSIDER	RTLX TLF Client	Agent	Stopped	Stopped	Stopped : Reason = Service stop requested
HP-NSK	WNSIDER	WebSphere MQ Monitoring	Agent	Running	Running	Running : Process is running
HP-NSK	VTLTECH	Generic EMS Event Monitoring	Agent	Running	Running	Running : Process is running
HP-NSK	VTLTECH	Generic EMS Event Reader	Agent	Running	Running	Running : Process is running
Windows	AMERICA	Backup Exec Remote Agent for Windows Systems	Other Process	Running	Running	Running : Service is running
Windows	AMERICA	Directory/File Monitoring	Agent	Running	Running	Running : Service is running
Windows	AMERICA	ITL Temperature Sensor Logs Monitoring	Agent	Running	Running	Running : Service is running
Windows	AMERICA	Windows Event Log Monitoring	Agent	Running	Running	Running : Service is running
Windows	AMERICA	Windows Performance Counter Monitoring	Agent	Running	Running	Running : Service is running
Windows	ANGUS	Windows Event Log Monitoring	Agent	Running	Running	Running : Service is running
Windows	APP1	Backup Exec Remote Agent for Windows Systems	Other Process	Running	Running	Running : Service is running
Windows	APP1	Windows Event Log Monitoring	Agent	Running	Running	Running : Service is running
Windows	APP1	Windows Performance Counter Monitoring	Agent	Running	Running	Running : Service is running
Windows	BRADFORD	WRDC Isoplex/Nplex Message Tracking	Agent	Running	Running	Running : Service is running
Windows	BSMITH	Backup Exec Remote Agent for Windows Systems	Other Process	Running	Running	Running : Service is running
Windows	BSMITH	Windows Event Log Monitoring	Agent	Running	Running	Running : Service is running
Windows	CORSHAM	Infonet Mailer Message Tracking	Agent	Running	Running	Running : Service is running
Windows	CORSHAM	Infonet Mailer System Queue Monitoring	Agent	Running	Running	Running : Service is running
Windows	CORSHAM	ISS Messenger DBDaemon	Other Process	Running	Running	Running : Service is running

## Reporting and Management Information

Sentra allows for the production of reports and management information in two ways.

Message traffic analysis can be performed as an extension of the built-in general query tool.

Substantially increased reporting flexibility is also provided by the capability to launch Microsoft Reporting Services within Sentra.

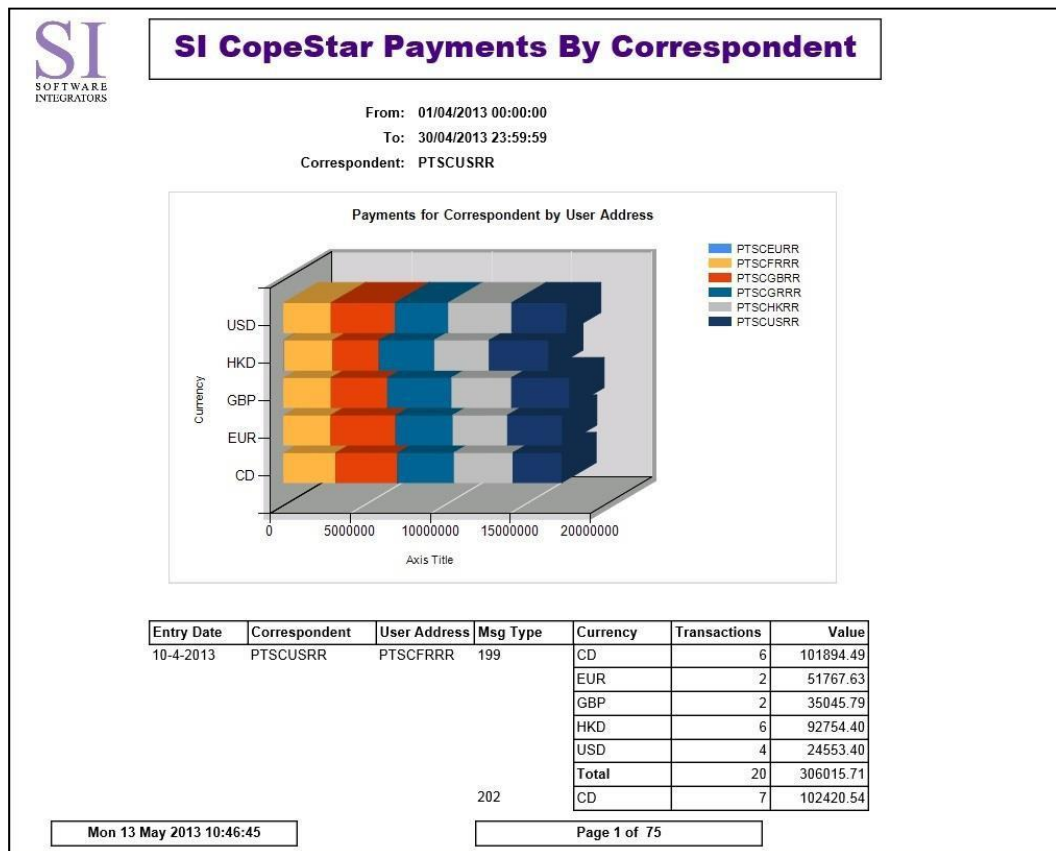
- Message Traffic Analysis
- Message traffic reports can be generated using the graphical and textual reporting facilities of the general query tool.
- This can be used for monitoring and analysing message traffic and trends. An example could be analysing messages routed across different mail servers within a specified period of time. The (General) Sentra Query function provides graphical and textual reporting facilities, which can be used to generate reports based upon data contained in the database. The following are general features applicable to all queries:
- Queries can be generated between a start and end time.
- Trend queries possible, e.g. totals displayed hourly, daily, weekly, to be specified via a time window.
- Results displayed in numerous 2D and 3D graph formats.
- Reports can be saved as CSV (comma separated value) files and can be easily exported to an Excel (or similar) spreadsheet.
- Sentra allows you to E-mail the results of a query, both textual and graphical, to one or more recipients.

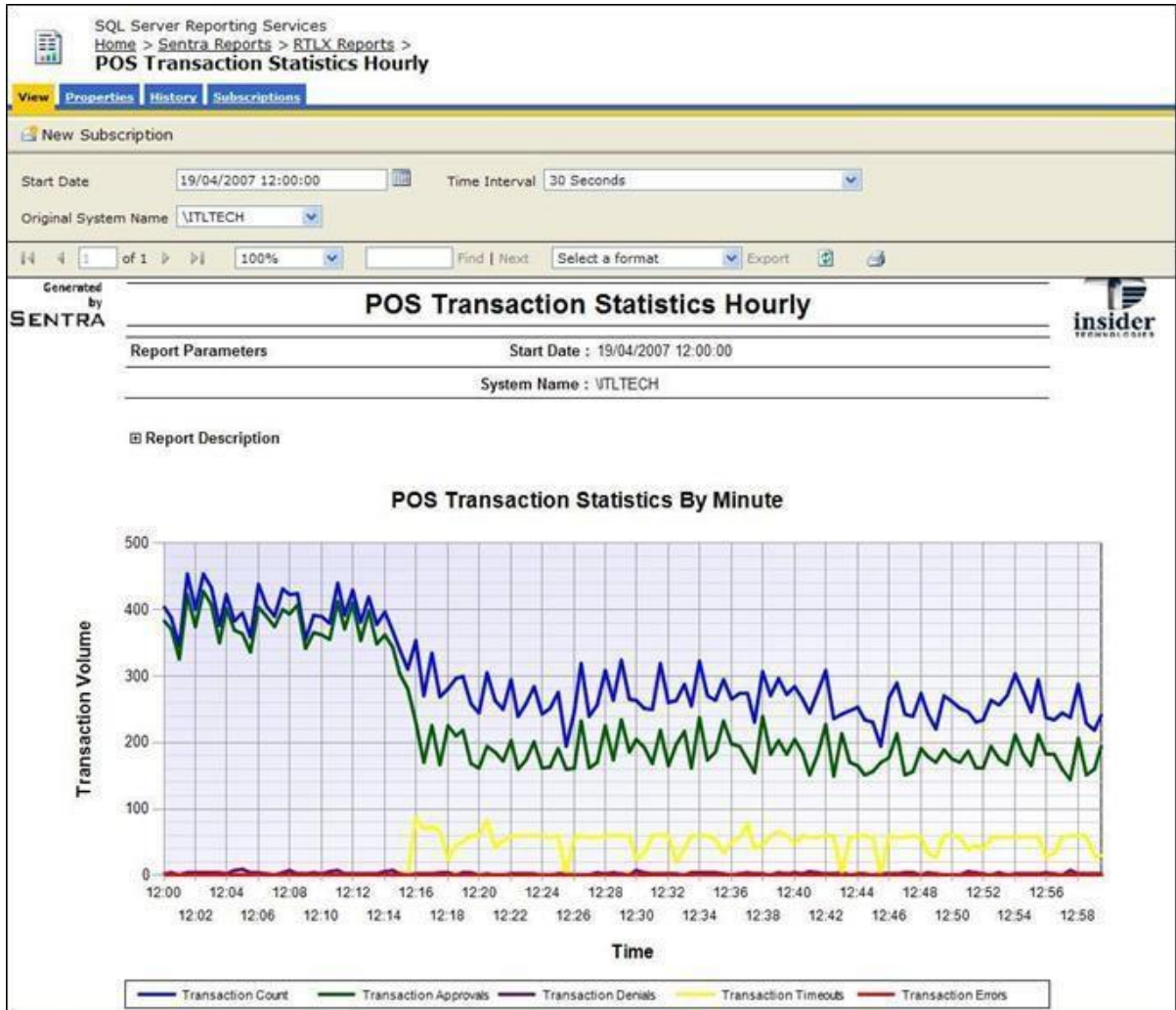
## Reporting Capability

Sentra comes with a number of predefined management reports based on both the industry-standard Microsoft Reporting Services package. These reports allow the Sentra data to be displayed as meaningful management information. SLA analysis, capacity planning chargeback and billing are just some of the many uses that can be made of this.

User-defined reports can be written and then launched from the MS SQL Reporting Services Console. This enables users to write reports based on virtually any data captured by the Sentra server. Furthermore, automatic scheduling along with publishing capabilities allow the reporting process to be automated, e.g. monthly SLA reports can be published on an intranet web site or e-mailed to a business manager without any need for user intervention. Example reports include:

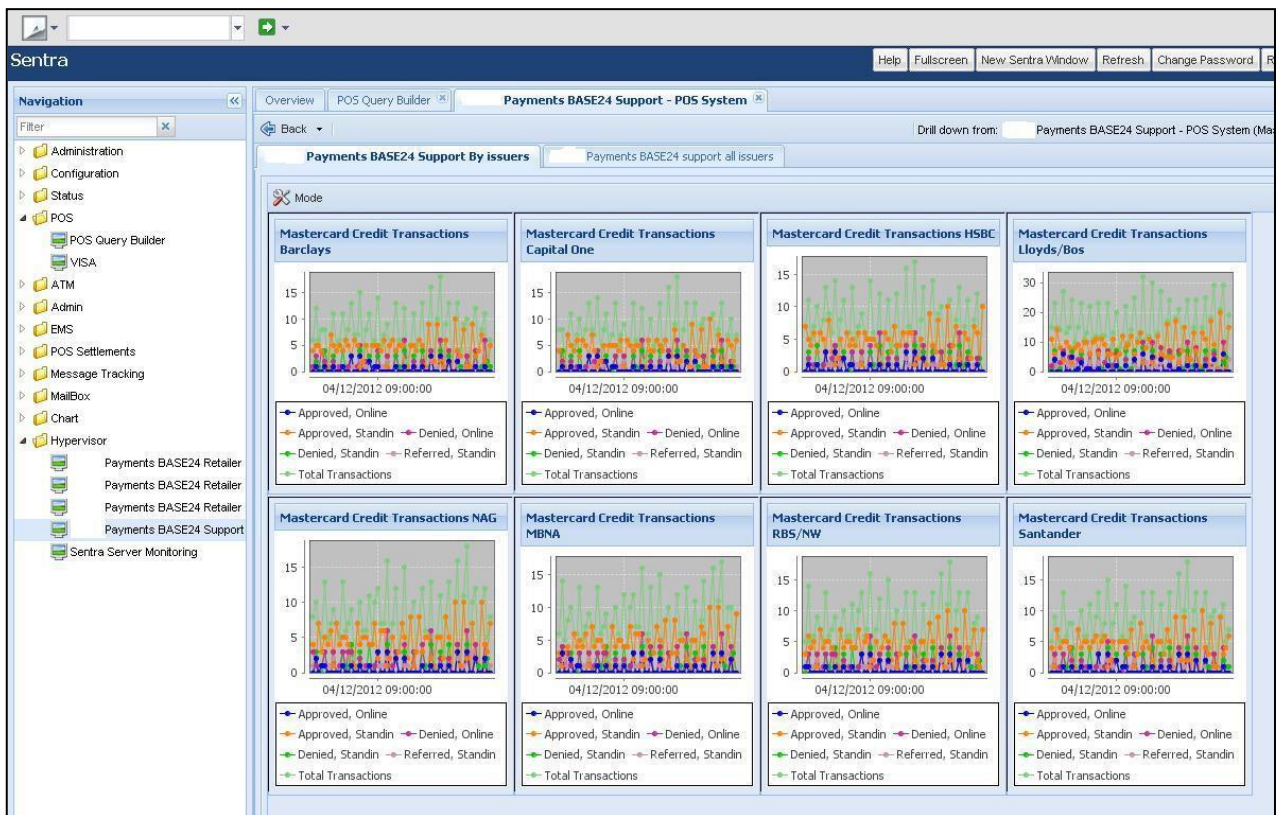
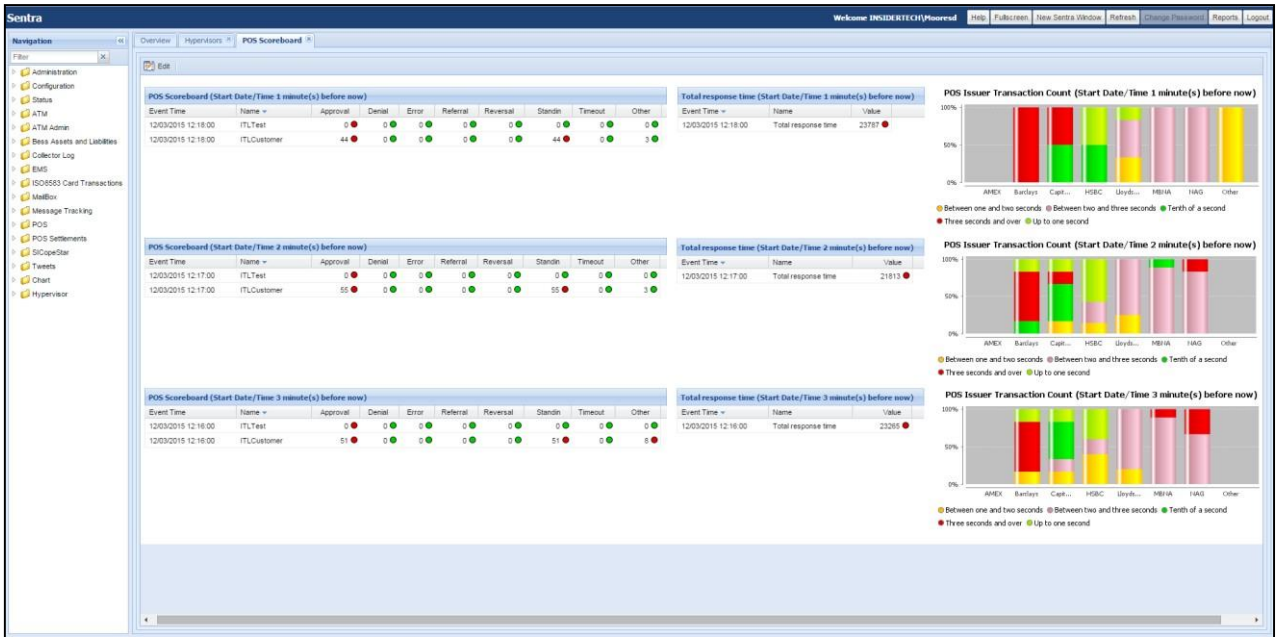
- Messaging Service Availability
- Mail Server Availability
- Mail Server Traffic Analysis
- Mail Server Queue Analysis
- Non-Delivery Reports
- System Availability
- Web Availability
- Alert Detail Per Server
- Alerts Per Subsystem
- Directory Replication
- Disk Space Per Server





## Self-Refreshing Charts

These are graphs which are automatically updated periodically, to provide near real-time information in the form of bar graphs and/or trends of any data captured by Sentra, e.g. CPU usage, daily messaging system throughput and volumes. The graphs can be configured to support drilldown, e.g. so that a user can highlight a bar in a bar graph and zoom in to a more detailed breakdown message system traffic or CPU usage by process.





## Summary of Reporting Component:

Provides single point of data and reporting capability across entire messaging system.

SLA measurement, messaging statistics, capacity planning data reporting.

Automatic scheduling of reports.

Web publishing.

Configurable Real-time chart displays, available from a web console.

Timely and accurate report production facilitates appropriate use of resources along with effective capacity planning. This leads to significant efficiency savings as system resource can be more efficiently employed

## Platform Support and System Requirements

Applications Supported:

- WebSphere MQ Server
- MS Exchange
- Critical Path
- HP NSK OSI/MHS, EMS, BASE24 Classic TLF / PTLF, SI's CopeStar
- Messaging Direct
- CGI (formerly Logica) All Payments Solution – LAPS
- NCR Authentic
- Nexor
- ISS Messenger Workplace
- MS SQL Server
- Oracle

Plus any application that provides instrumentation through Windows Performance Counters or Windows Event Logs.

Platform Environments Supported:

- Windows 2003 / 2008 / 2008 (R2) / 2012/2016
- Unix, e.g. SOLARIS, AIX 64 bit
- LINUX x86 32 and 64 bit
- HP NSK (Tandem) – ServerNet, ntegrity Blade, NonStopX

## Minimum Server Requirements (for Windows Server)

For optimum performance, it is recommended that the minimum specification of your hardware and software is as follows:

- Windows Server 2012 onwards with latest service packs
- Microsoft SQL Server 2012 onwards with latest service.
- Pentium 2 GHz Processor
- 4 Gb RAM recommended
- SCSI interface (SCSI2 Ultra-Wide recommended)
- 10 GB Single Drive for operating system and SQL Server software
- 40 GB Single Drive for the SQL server database (RAID 0+1 recommended)
- 20 GB Single Drive for the SQL server log file (RAID 0+1 recommended)
- Graphics resolution 1024 x 768 recommended
- 17" or larger colour monitor is also recommended.

The above specification is for guidance only. The specification of your server will be dependent on your individual needs. Please contact the Insider Technologies Helpdesk at [support@insidertech.co.uk](mailto:support@insidertech.co.uk) for assistance in establishing the specification of your server.

## SQL Server Versions Supported by Sentra

The Sentra database is compatible with the following variants of SQL Server:

Product Name	Sentra Supported
2012/2014 Standard Edition	Yes
2012/2014 Enterprise Edition	Yes
2012/2014 Express	Yes – the default installation on the CD uses SQL Express 2012 with Advanced services, so that SQL Reporting Services is available

SQL Express editions support databases with a limited maximum size. Users who anticipate large database storage requirements should consider installing the Enterprise edition of Microsoft SQL Server, or contact Insider Technologies for advice.

## SQL Server Client Tools

The Server installation needs SQL Server Client tools to be installed (e.g. osql.exe) in order to install or upgrade a Sentra database.

## Installation of SQL Express

If Microsoft SQL Server is not installed and a Server installation is started, the installation procedure will prompt the user to install the SQL Express version of SQL Server. The user can choose not to install SQL Express, e.g. if the Sentra database is already installed on a separate database server.

## Other SQL Server Recommendations

The SQL Server service "SQL Server" should be set so that it automatically starts after a reboot of the server. This can be checked by navigating to Control Panel...Administrative Tools...Services.

It is recommended that a maintenance task be configured for the Sentra database after installation. This can be configured using the Maintenance Wizard feature in SQL.

### Privileged Domain Account

To discover Windows domains, computers and services on Windows computers, Sentra requires the use of an account that has domain administrator and "logon as a service" user rights for the Sentra server. You will be asked for this account during the installation procedure. Request such an account from your System Administrator. Try not to use an existing user account - if the user changes the password or the password expires, all Sentra services that use the password will have to be reconfigured.

### Browser Versions Supported By Sentra

The Sentra console has been tested with the following browsers and versions.

Product Name	Supported Versions
Microsoft Internet Explorer	8, 9, 10, 11
Google Chrome	35 onwards
Firefox	27 onwards

Note: The product may function correctly in other browser versions, as Google and Firefox provide regular updates. Contact Insider Technologies if you have any further queries.

## **Implementation, Training and Services**

Training of a concise and timely nature is the key to a successful IT department.

Insider Technologies recognises that implementation of Sentra within a complex network may require specific expertise and therefore provides a range of customised courses. These can be presented either in-house, or on-site.

Our courses and training can be tailored to your specific requirements, and provides all the skills and information that you need, whatever your experience level.

If you would like to discuss or book any of these courses, please contact Insider Technologies on +44 (0)161 876 6606 or e-mail - [support@insidertech.co.uk](mailto:support@insidertech.co.uk)

Insider Technologies is a UK-based software and services company, operating in the Financial and Messaging markets.

It provides Service Management, Tracking, Bespoke Software and Information Mediation solutions.

A cross section of our customers 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 at:

Insider Technologies Limited  
2 City Approach  
Albert Street  
Eccles  
Manchester  
M30 0BL  
United Kingdom

Tel: +44 (0)161 876 6606

Fax: +44 (0)161 868 6666

e-mail: [support@insidertech.co.uk](mailto:support@insidertech.co.uk)

Website: <http://www.insidertech.co.uk>

## Microsoft Partner

Gold Application Development

Copyright © 2017. Insider Technologies Limited. All Rights Reserved.