



Sentra White Paper



Table of Contents

Management for Messaging and Middleware Environments.....	3
Introduction to Sentra.....	4
Sentra Product Overview and Benefits.....	5
Sentra Architecture.....	7
Windows User Interface.....	10
Web User Interface.....	12
Sentra Dashboard.....	13
Sentra Hypervisor.....	14
Monitoring and Alerting.....	15
Message Tracking.....	17
Mailbox Query.....	18
Transaction and Payments Monitoring.....	19
XML Monitoring.....	20
Remote Service/Process Management.....	21
Operator-Initiated Tasks.....	22
Reporting and Management Information.....	23
Platform Support and System Requirements.....	27
Implementation, Training and Services.....	29

Management for Messaging and Middleware Environments

Messaging is a mission critical service within any 21st century organisation and a key element of any service provider's portfolio. However, the demands on messaging systems are continually increasing.

The volume of 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: **99.999%** availability SLAs are not uncommon, but this means less than 1-hour downtime per year!

Managing the messaging system 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 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 service. Not only that, but appropriate escalation and intervention systems should be implemented to ensure that problems are responded to in an appropriate and efficient manner to ensure that the service is maintained.

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 systems provide this capability.

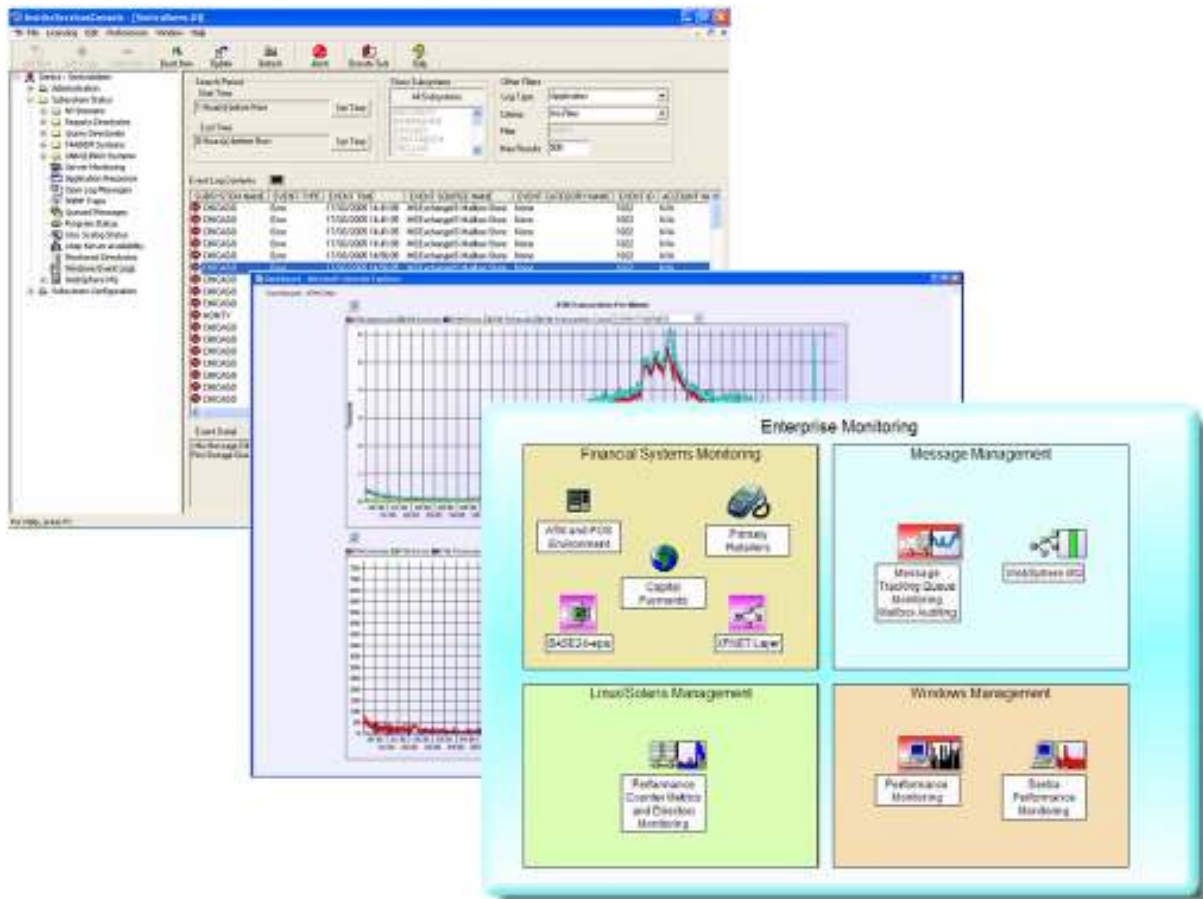
Also, many messaging systems have grown up in a piecemeal fashion, with individual departments or companies joined by mergers having completely different systems in place. Budgetary constraints may mean that these systems cannot be consolidated into a single vendor system. This causes further management 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 messaging 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 messaging systems. It provides extensive benefits that enable optimal availability, functionality and performance of messaging 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:

- Choice of Windows User Interface and Web consoles
- 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 Center™, 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,IMAP4.
- XML monitoring including UNIFI payment formats - <http://www.iso20022.org>
- HP NonStop monitoring of the Event Management Subsystem (EMS) with complete dynamic filtering of events from any configured collector(s).
- 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 5.5/2000/2003/2007, 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 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).
- Mailbox auditing on Exchange 2003/2007, including read/moved/deleted status of a message.
- Mail traffic pattern assessment.
- Capacity planning.
- Reporting on messaging issues.
- Billing or usage analysis.
- Operator initiated tasks to perform manual problem resolution and to launch other diagnostic applications, all from a single, central console.
- 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 a 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.

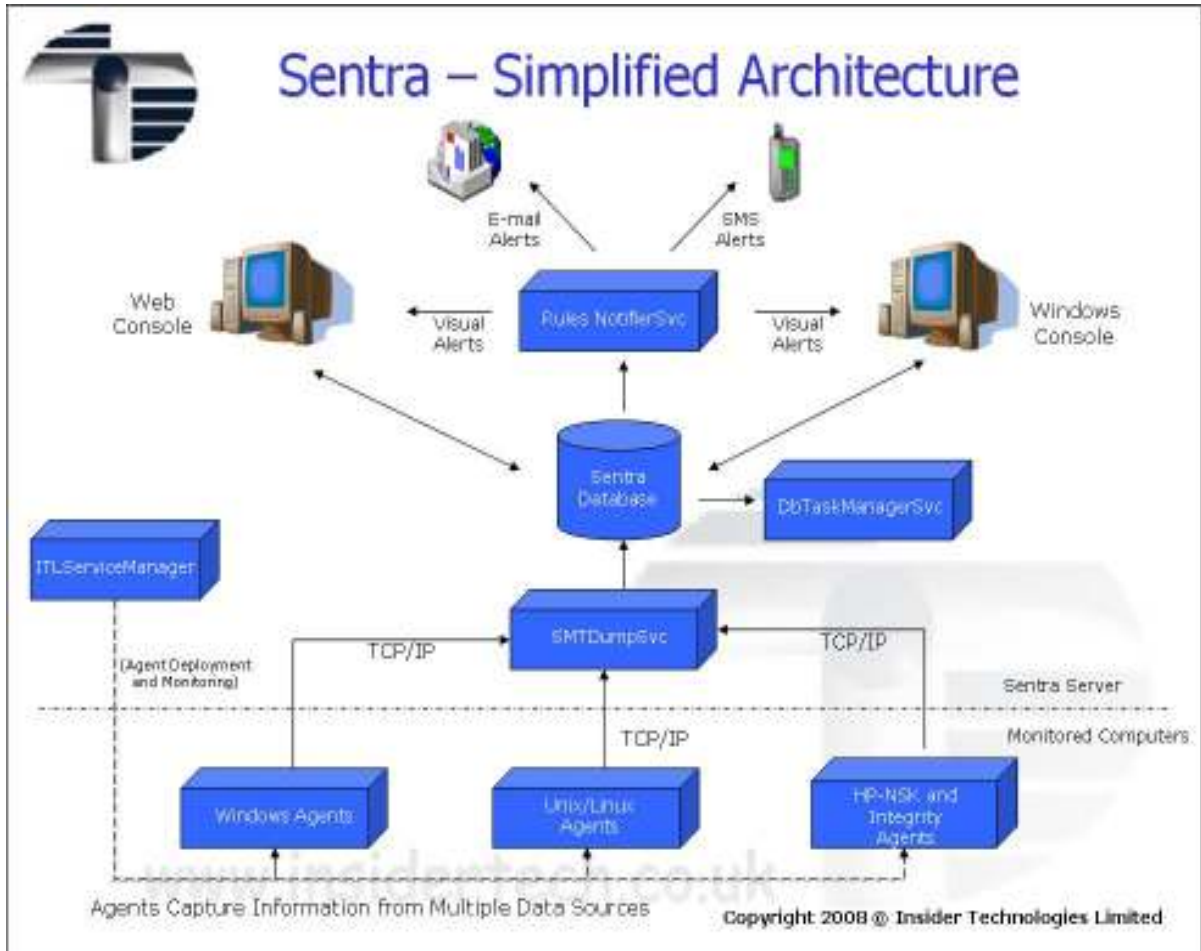
Sentra provides the user with the ability to rapidly deploy these extraction programs across many machines in a corporate network. Sentra enables users to configure, control and monitor these services, all from a central console.

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
- ORACLE
- Unix/Linux Performance data
- HP NonStop EMS log alerts
- BASE24 TLF and PTLF transactions logs
- 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).

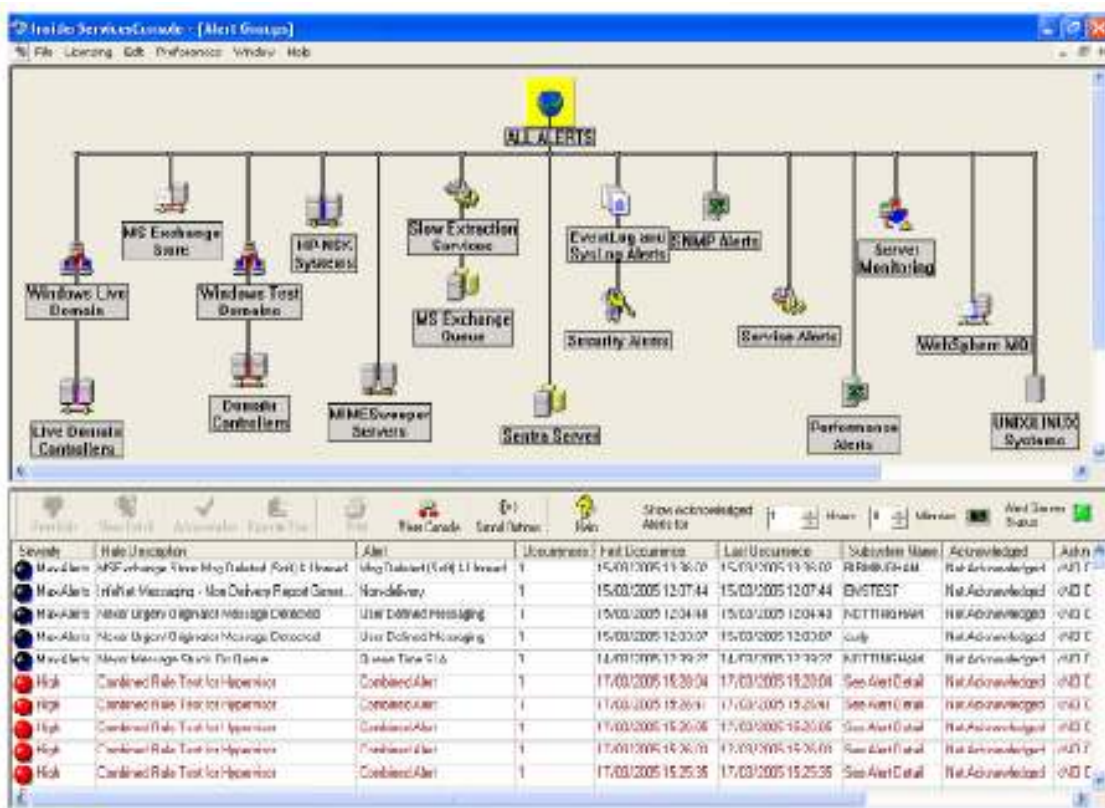
Sentra features powerful rules evaluation capabilities. Simple rules can be evaluated by extraction programs as data is captured, e.g. checking for the occurrence of a non-delivered message or a busy CPU. More complex rules are evaluated on the Sentra server. Typical messaging systems SLAs require an 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, HP NonStop and (in the case of e-mail 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 Dashboard and Hypervisor views, user configurable monitoring capabilities. This enables specific information to be targeted at specific audiences.

Windows User Interface

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 Graphical User Interface (GUI) has been designed to be easy to navigate and to allow rapid access to data at all times.

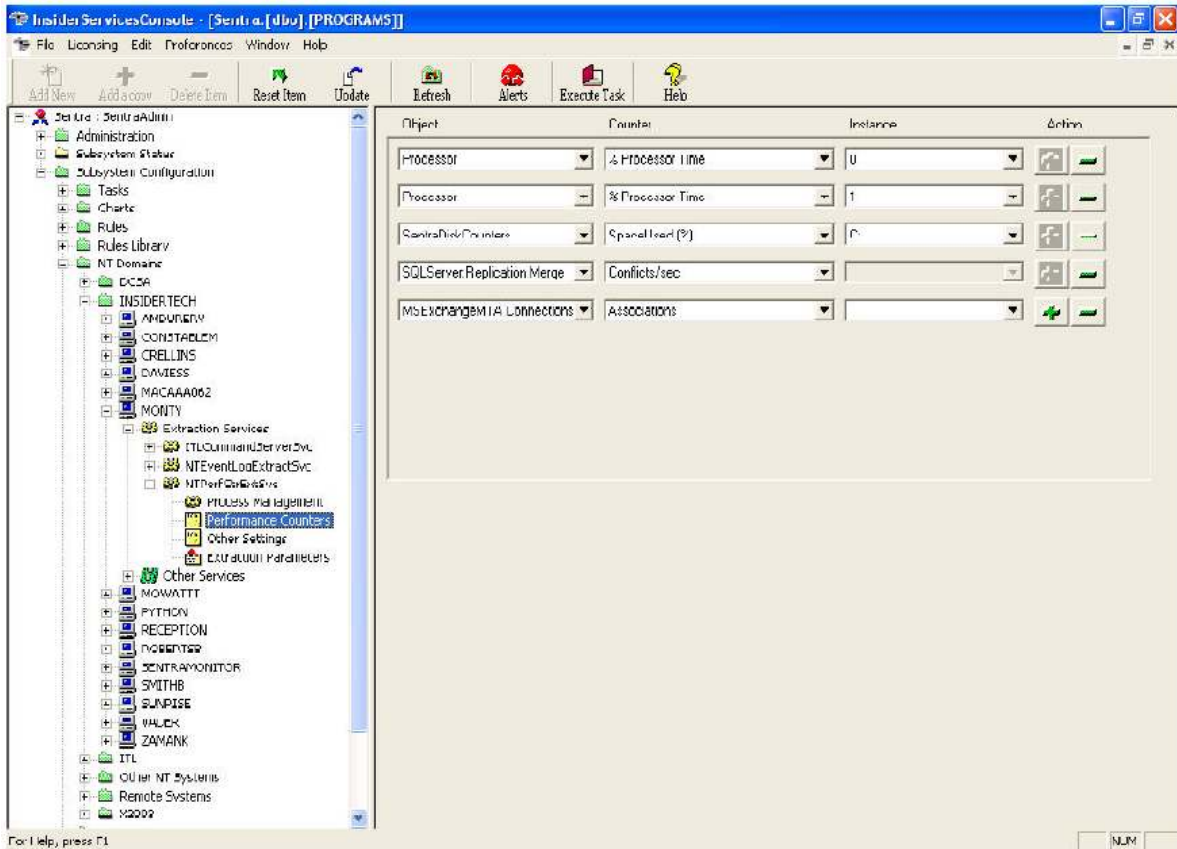
A central feature is the Alert Groups View, which provides a topological representation of the systems being managed. The view is easily customisable, and can be configured to represent a logical network topology or a messaging service view. The view enables the user to see at glance any events or problems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



The Insider 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
- Subsystem Configuration – provides access to extraction program deployment views, and the rules configuration screens.

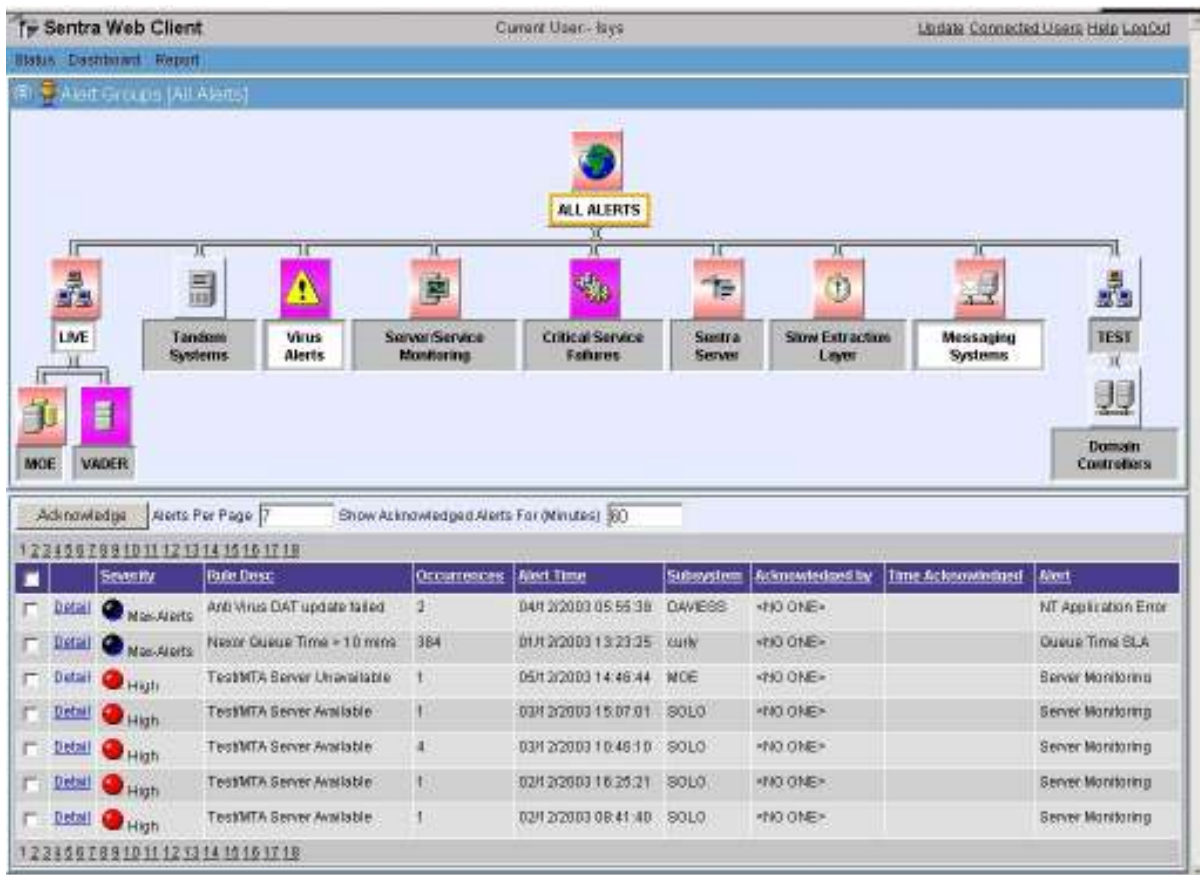
The main Sentra toolbar is used to add, amend and delete items within the tree. These procedures are generic and are implemented in the same way for every part of the tree structure.



Web User Interface

Sentra also ships with a web console. This has been specifically designed to provide a subset of the Windows User Interface features. Currently, the web console provides an alert view and all the functionality of the Windows User Interface console as featured in the Subsystem Status area of the Windows User Interface console tree. Example screenshots, included below, demonstrate that the web console is by no means a 'poor-relation' of the Windows User Interface console, which is normally the case with offerings from other vendors.

The Sentra web console also provides configurable real-time digital dashboard displays. This is discussed in more detail later in this document.

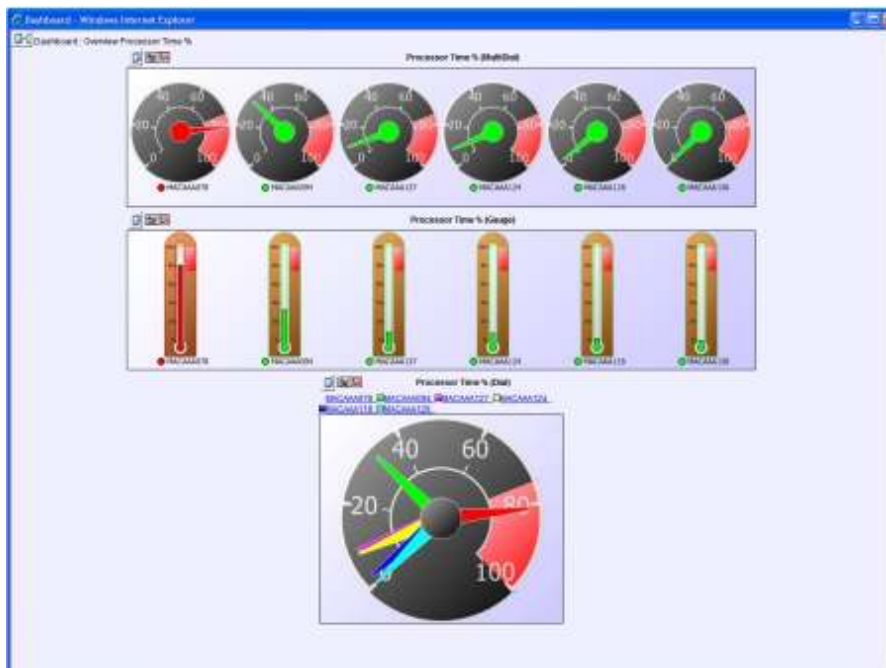
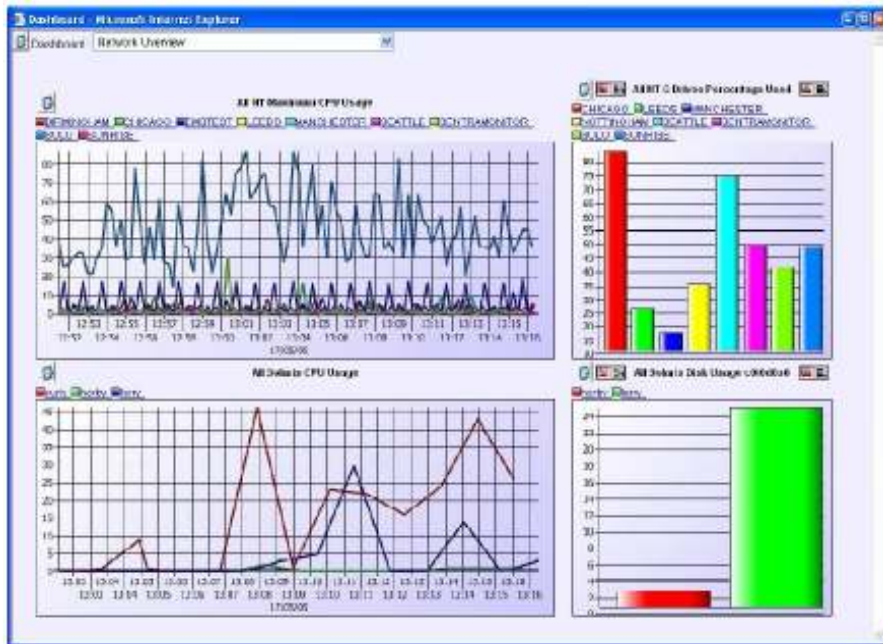


Whilst many users are happy to view their network or messaging systems in a traditional topological view, others now prefer to view their systems in several different ways. For example, business managers don't wish to see technical problems – they prefer to see issues in terms of the potential impact 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 Dashboard and the Sentra Hypervisor.

Sentra Dashboard

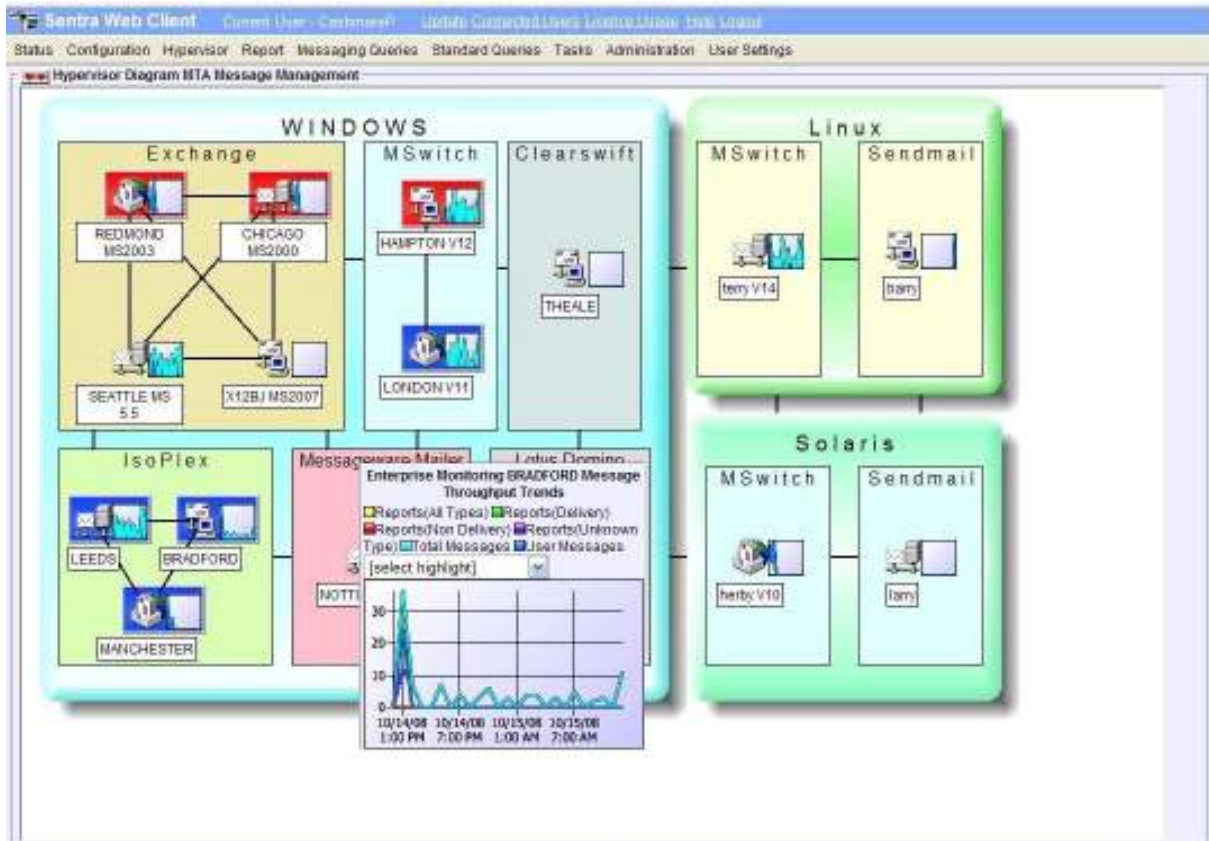
A web-based graphical user interface can be configured to provide a permanent display of key aspects of managed service performance. One or more real-time dashboard reports can be displayed, each showing a particular aspect of monitored service performance. For example, a graph of message server queue sizes can be shown, showing the relative load across multiple mail servers. Dashboards 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 dashboard:



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 dashboard 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 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, GUI 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.

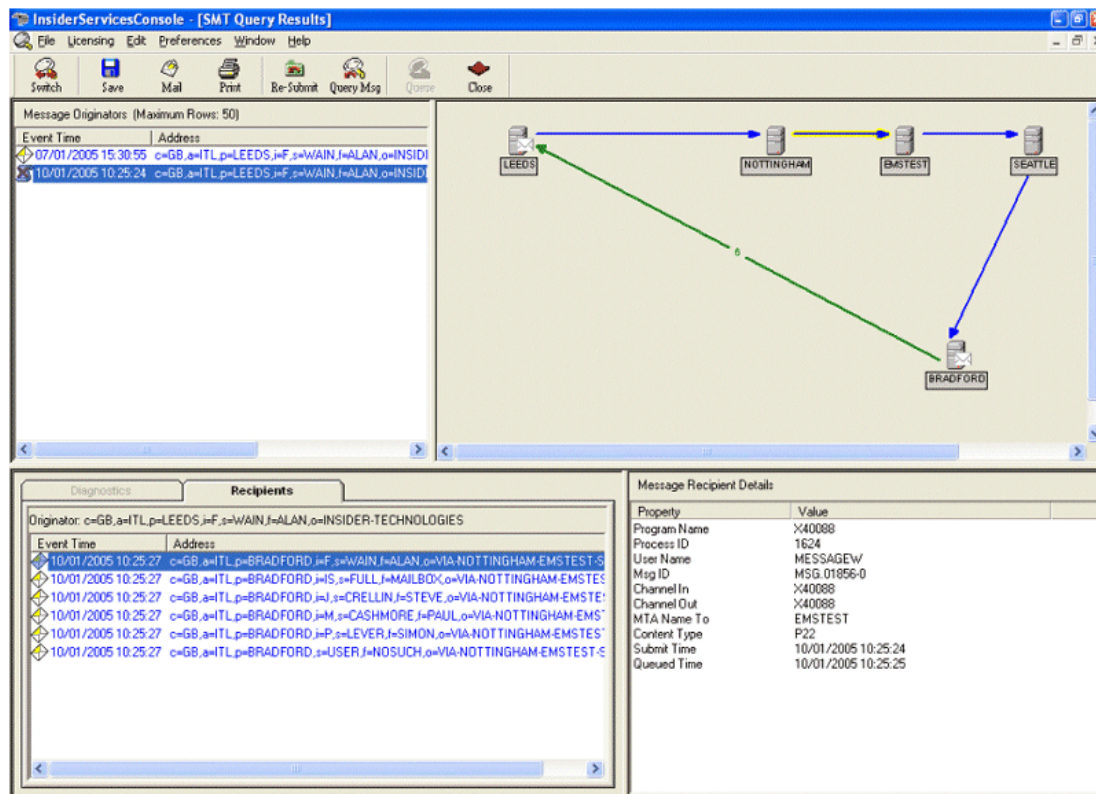
Queries can be as detailed or simple as a user requires. For an e-mail message, typical search details might be Sending Time, Message Identifier, Originator or Recipient address. As searches are performed against a single database, results from many Message Transfer Agents (MTAs) can be displayed in 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.



Mailbox Query

In addition to collecting data to facilitate Message Tracking, SENTRA can also collect events from some message stores, including the MExchange 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.

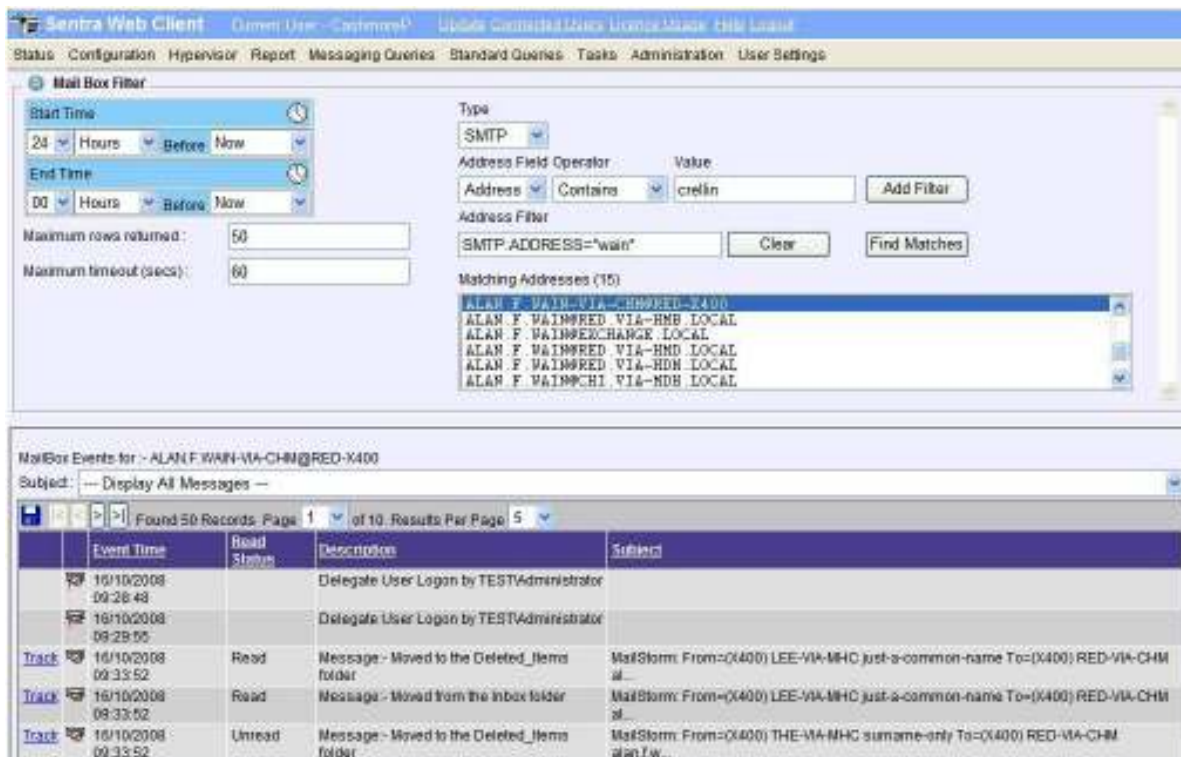
The Mailbox Query screen allows an email address to be selected by progressively filtering a mailbox address which is known to the system. Once an address is selected, all the mail store events that relate to the address are displayed. The results show when messages are moved or deleted, whether they 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 then the default credentials.
- Provides a powerful overview of mailbox activity.
- Integrated with Message Tracking, providing a convenient alternative method of launching a query.



The screenshot shows the 'Mail Box Filter' section with the following configuration:

- Start Time: 24 Hours Before Now
- End Time: 00 Hours Before Now
- Maximum rows returned: 50
- Maximum timeout (secs): 60
- Type: SMTP
- Address Field Operator: Contains
- Value: crelin
- Address Filter: SMTP:ADDRESS="wain"

Matching Addresses (15):

- ALAN.F.WAIN-VIA-CHN@RED-X400
- ALAN.F.WAIN@RED-VIA-RMB LOCAL
- ALAN.F.WAIN@EXCHANGE LOCAL
- ALAN.F.WAIN@RED-VIA-RND LOCAL
- ALAN.F.WAIN@RED-VIA-RDH LOCAL
- ALAN.F.WAIN@RED-VIA-RDB LOCAL

MailBox Events for: ALAN.F.WAIN-VIA-CHN@RED-X400

Event Time	Read Status	Description	Subject
16/10/2008 09:28:48		Delegate User Logon by TESTAdministrator	
16/10/2008 09:29:55		Delegate User Logon by TESTAdministrator	
16/10/2008 09:33:52	Read	Message - Moved to the Deleted_Items folder	MailStorm: From=(X400) LEE-VIA-MHC just-a-common-name To=(X400) RED-VIA-CHM al...
16/10/2008 09:33:52	Read	Message - Moved from the Inbox folder	MailStorm: From=(X400) LEE-VIA-MHC just-a-common-name To=(X400) RED-VIA-CHM al...
16/10/2008 09:33:52	Unread	Message - Moved to the Deleted_Items folder	MailStorm: From=(X400) THE-VIA-MHC surname-only To=(X400) RED-VIA-CHM alan.f.w...

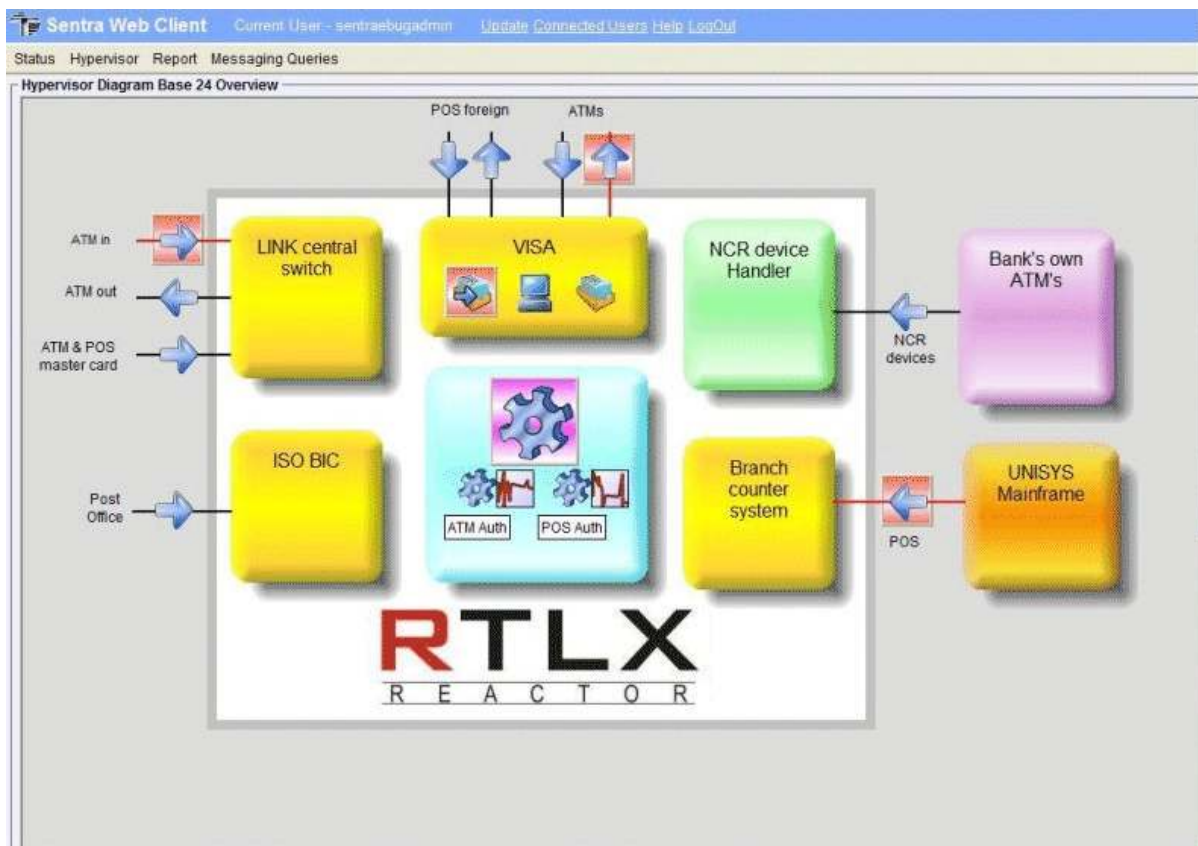
Transaction and Payments Monitoring

Insider has created a Sentra module, RTLX, to provide real time monitoring of the transaction flow information created by the ACI BASE24™ ATM/POS application. This Sentra module will maintain a centralised database of transaction data from one or more BASE24™ nodes 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 Base24™ world.

The purpose of the RTLX application is to transfer the ATM and POS log information (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.

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 Web.

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.

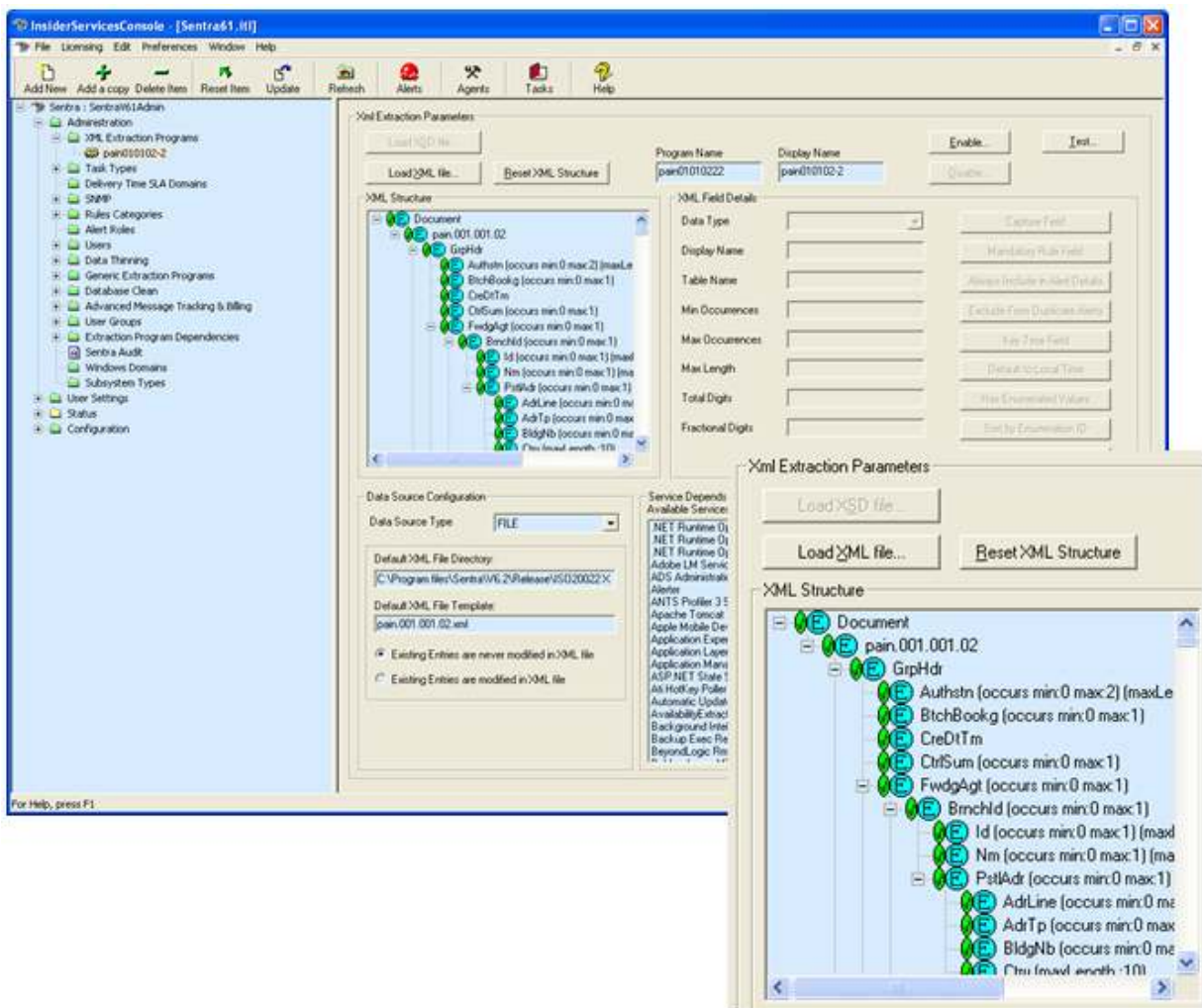


XML Monitoring

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:

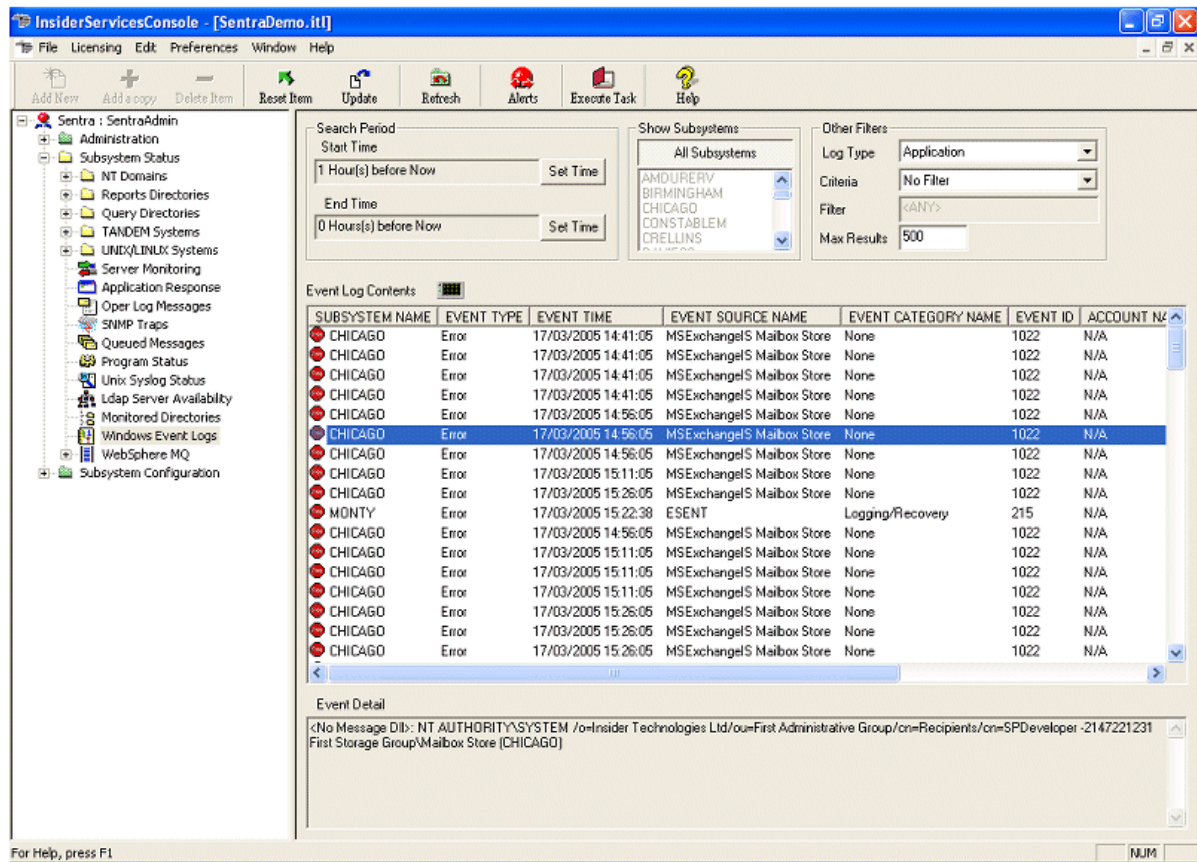


Remote Service/Process Management

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:



The screenshot shows the InsiderServicesConsole application interface. On the left is a tree view of system components. The main area displays search filters and a table of event log contents.

Search Period: Start Time: 1 Hour(s) before Now, End Time: 0 Hours(s) before Now.

Show Subsystems: All Subsystems (dropdown menu).

Other Filters: Log Type: Application, Criteria: No Filter, Filter: <ANY>, Max Results: 500.

SUBSYSTEM NAME	EVENT TYPE	EVENT TIME	EVENT SOURCE NAME	EVENT CATEGORY NAME	EVENT ID	ACCOUNT NAME
CHICAGO	Error	17/03/2005 14:41:05	MSExchangeIS Mailbox Store	None	1022	N/A
CHICAGO	Error	17/03/2005 14:41:05	MSExchangeIS Mailbox Store	None	1022	N/A
CHICAGO	Error	17/03/2005 14:41:05	MSExchangeIS Mailbox Store	None	1022	N/A
CHICAGO	Error	17/03/2005 14:41:05	MSExchangeIS Mailbox Store	None	1022	N/A
CHICAGO	Error	17/03/2005 14:56:05	MSExchangeIS Mailbox Store	None	1022	N/A
CHICAGO	Error	17/03/2005 14:56:05	MSExchangeIS Mailbox Store	None	1022	N/A
CHICAGO	Error	17/03/2005 15:11:05	MSExchangeIS Mailbox Store	None	1022	N/A
CHICAGO	Error	17/03/2005 15:26:05	MSExchangeIS Mailbox Store	None	1022	N/A
MOINTY	Error	17/03/2005 15:22:38	ESENT	Logging/Recovery	215	N/A
CHICAGO	Error	17/03/2005 14:56:05	MSExchangeIS Mailbox Store	None	1022	N/A
CHICAGO	Error	17/03/2005 15:11:05	MSExchangeIS Mailbox Store	None	1022	N/A
CHICAGO	Error	17/03/2005 15:11:05	MSExchangeIS Mailbox Store	None	1022	N/A
CHICAGO	Error	17/03/2005 15:11:05	MSExchangeIS Mailbox Store	None	1022	N/A
CHICAGO	Error	17/03/2005 15:26:05	MSExchangeIS Mailbox Store	None	1022	N/A
CHICAGO	Error	17/03/2005 15:26:05	MSExchangeIS Mailbox Store	None	1022	N/A
CHICAGO	Error	17/03/2005 15:26:05	MSExchangeIS Mailbox Store	None	1022	N/A

Event Detail: <No Message DB>: NT.AUTHORITY\SYSTEM /o=Insider Technologies Ltd/ou=First Administrative Group/cn=Recipients/cn=SPDeveloper -2147221231 First Storage Group\Mailbox Store (CHICAGO)

Operator-Initiated Tasks

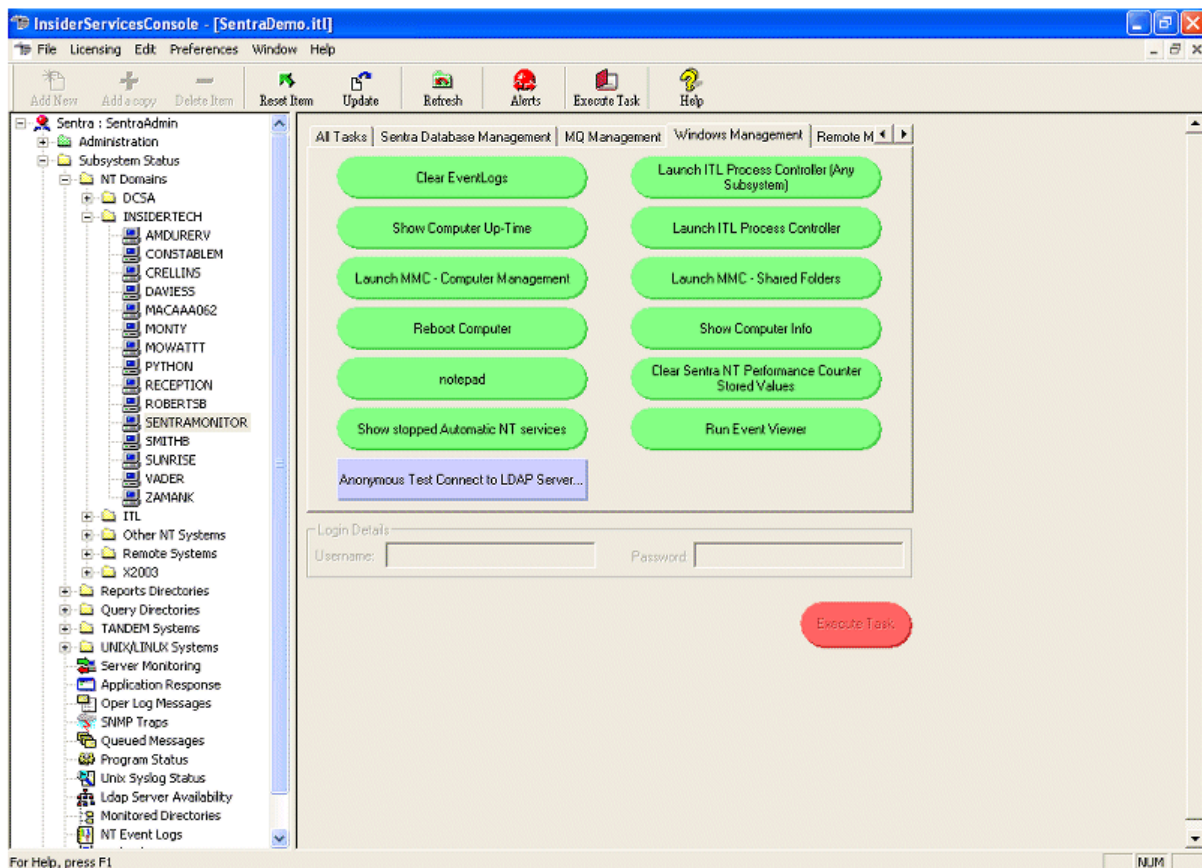
Sentra provides the user with a means of invoking tasks from the Windows User Interface console. Sentra is shipped with a set of pre-configured tasks, and new tasks can be easily defined by the user. Tasks can be configured to execute programs on the same platform as the Windows User Interface console, and support is provided for launching tasks on remote platforms using remote procedure calls for Windows platforms, secure shell (SSH) for Unix and Linux platforms or Telnet for Unix, Linux and HP NSK platforms. Tasks can be configured as commands containing one or more variables as command arguments. The variables are substituted with actual values when the task is launched.

Consider the following example:

DeleteAStuckMessageFromQueue \$(subsystemName) \$(messageId)

This task could be invoked by an operator when an alert is generated to indicate that a message with an identifier of "msg.12345" is stuck in a message queue on a computer named "OUTGOING_PAYMENTS". When the task is invoked, the command would be issued as:

DeleteAStuckMessageFromQueue OUTGOING_PAYMENTS msg.12345



Reporting and Management Information

Sentra allows 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 field) 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.

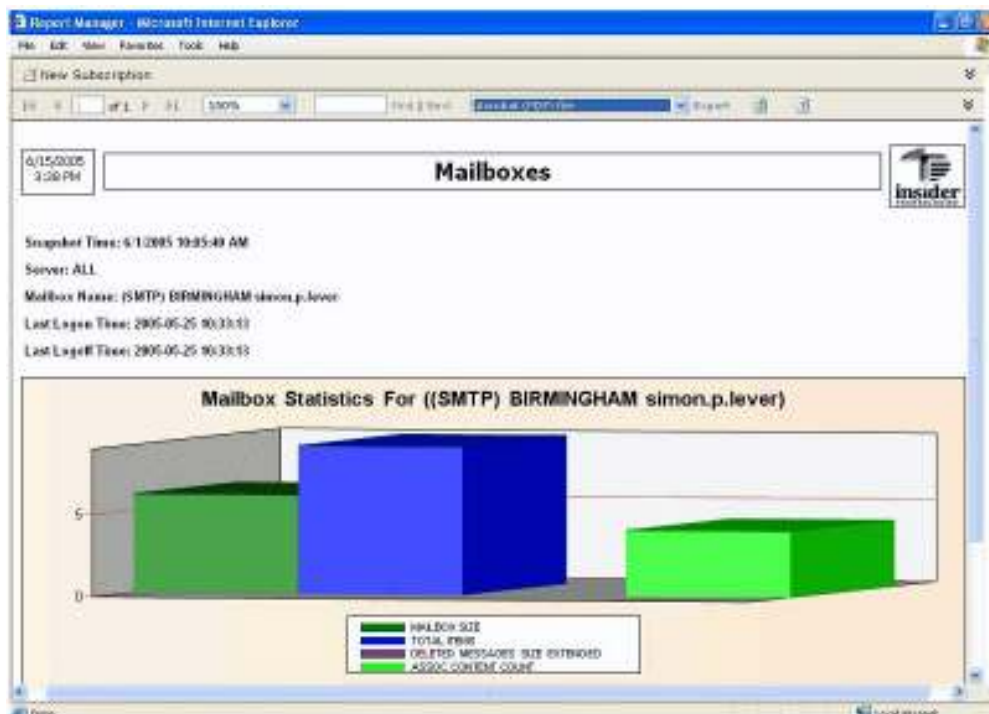
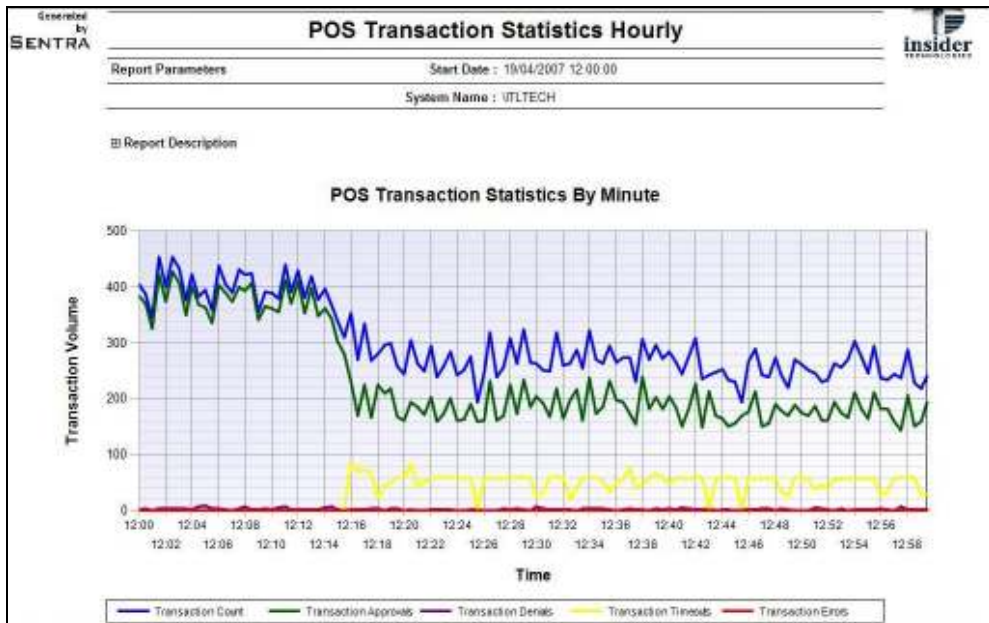
Reporting Capability

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 Sentra GUI. 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:

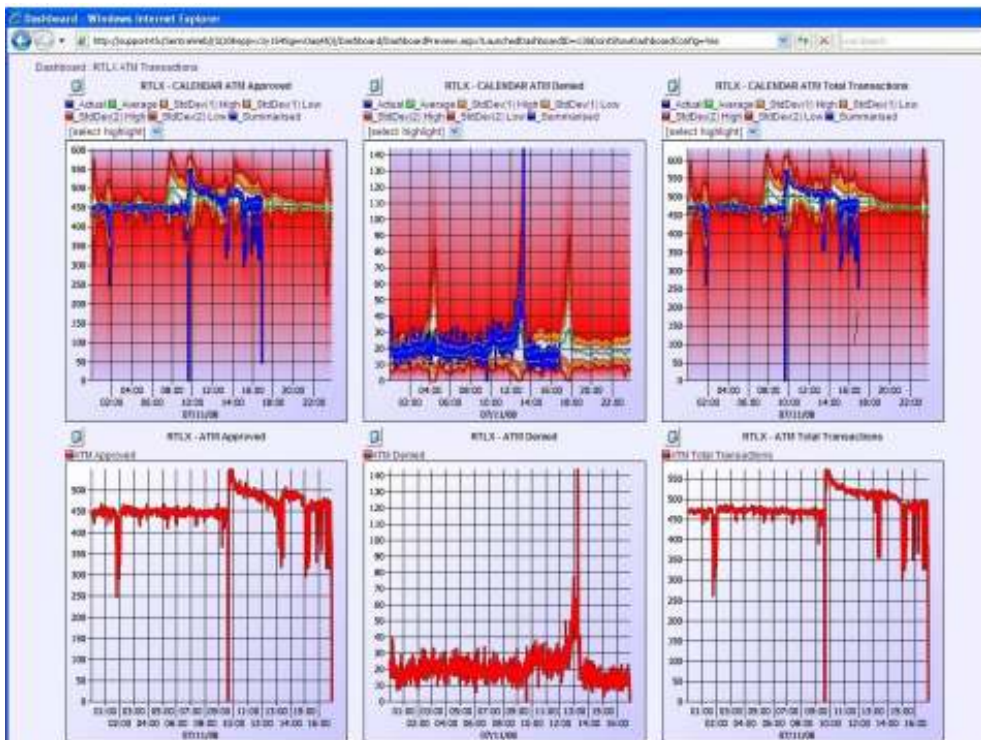
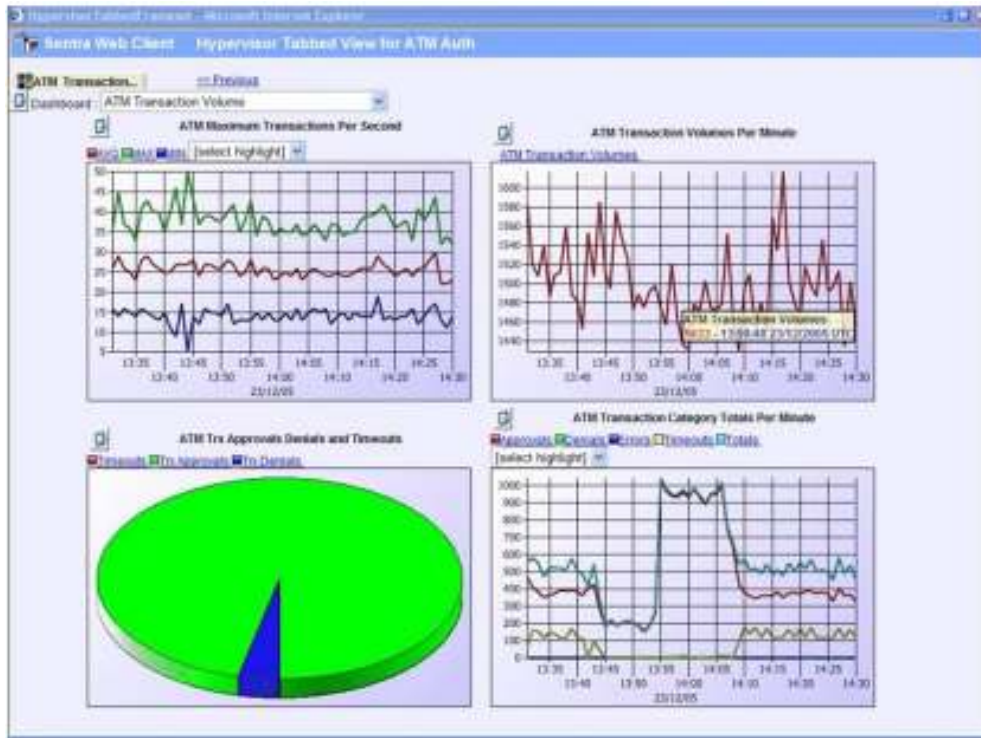
- Messaging Service Availability
- Mail Server Availability
- Mail Server Traffic Analysis
- Mail Server Queue Analysis
- Non-Delivery Reports

- 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 dashboard 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 V5.5, 2000, 2003 and 2007
- Critical Path
- HP NSK OSI/MHS
- Messaging Direct
- Nexor
- ISS Messenger Workplace
- MS SQL Server

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

Platform Environments Supported:

- Windows XP/2000/2003/2008
- Unix, e.g. SOLARIS
- LINUX
- HP NSK (Tandem)

Hardware requirements:

The Sentra software has been developed on an IBM-compatible PC. For optimum performance, it is recommended that the minimum specification of your hardware is as follows:

Sentra Server

One server running Windows 2003/2008 and Microsoft SQL Server, with a minimum specification of:

- Pentium 2 GHz Processor Dual Core
- 4 GB Memory
- SCSI interface (SCSI2 Ultra-Wide recommended)
- 20 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 database log (RAID 0+1 Recommended)
- Graphics resolution 1024 x 768 recommended
- A 17" or larger colour monitor is also recommended.

Client:

Any standard desktop PC should be sufficient. A standard web browser is required for the Sentra Web Console.

Software Requirements:

Sentra Server

- Microsoft Windows 2003/2008 and relevant Service Packs
- TCP/IP protocol stack

Note: The Sentra database is compatible with the following variants of Microsoft SQL server:

- Microsoft SQL Server 2005/2008 Standard Edition
- Microsoft SQL Server 2005/2008 Enterprise Edition
- Microsoft SQL Express 2005 with Advanced Services*

*edition supports databases with a maximum size of 4Gb. Users who anticipate large database storage requirements should consider installing the Enterprise edition of Microsoft SQL Server, or contact Insider technologies for advice.

Windows Workstation

- Microsoft Windows (XP/2000/2003/2008)
- A TCP/IP protocol stack

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



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