



WebSphere MQ Management

Product Overview



Table of Contents

Introduction.....	3
Sentra MQ Management Product Overview.....	5
User Interface.....	6
Data Extraction	8
Service/Process Management.....	9
MQ Message Traffic Analysis.....	10
SLA Rule Analysis & Alerting	11
Sentra MQ Tasks	14
Reporting and Management Information	16
Real Time Dashboard.....	17
Implementation, Training & Services	18
Platform Support & System Requirements	19
Support.....	21

Introduction

SENTRA MQ™ Common Framework



IBM's WebSphere MQ product is used to connect e-commerce systems in many diverse environments. It is essential that the connectivity is robust and available at all times. In addition to this the performance of the infrastructure must be optimal, as timely delivery of business information is of the essence in today's fast moving society.

Any failure in the WebSphere product must be quickly identified and fixes applied as swiftly as possible. This is not so easy if the MQ Environment is spread across multiple platforms with multiple operating system types. In many cases it may well be the application that is receiving or sending the business information that is at fault.

System Managers need to be able to filter all of the information that is produced by a management and monitoring system. The information should be as near to real-time as possible and highly visible.

Sentra WebSphere MQ monitoring has been designed to show this information as clearly as possible and provide several means of alerting support staff to problems before they occur and in many cases automatically fix the error using built in scripting. Sentra MQ will monitor the MQ components of your system as well as the platforms and applications that they connect. You will have an overview of the health of your entire WebSphere network visible in a single console view.

Sentra MQ has been designed to be modular, customisable and incorporates an extensible architecture.

Sentra MQ automatically monitors your Windows NT/2000/2003, UNIX or LINUX and HP NonStop WebSphere MQ environment 24x7. It provides the alerting, querying and reporting tools to maintain the highest levels of availability and performance for the mission-critical services provided by your MQ infrastructure.

Sentra increases systems performance and availability, which leads to improved Quality of Service (QoS) and significant reductions in total cost of ownership (TCO).

Platform and Application Management

Management of your network is a mission critical element within any organisation and a key part of any service providers portfolio. Network and messaging system administrators are continually being asked to meet Service Level Agreements (SLAs), and are measured against their SLA compliance. Sentra provides a means of monitoring WebSphere SLA compliance, and can automatically resolve the causes of problems.

Many messaging systems have evolved in a piecemeal fashion with individual departments or companies (e.g. joined by mergers) having completely different systems in place. Budgetary constraints may mean that these systems cannot be consolidated into a single vendor system, which causes further management headaches for systems administrators and managers.

When managing a network of disparate systems it becomes ever more important to ensure that the service these systems provide is meeting the intense demands placed upon it by its users, and that it will continue to do so in the future. Service failures will mean the transfer of information is damaged, which directly impacts on the financial health of an organisation either through missed opportunities or by damage to its reputation.

In the case of WebSphere specifically, Message Queue Managers, Queues, Channels, Listeners, WebSphere Applications & Systems can all be proactively monitored from a central Sentra MQ console.

Sentra MQ Management Product Overview

The technology basis of Sentra is to employ agents that reside on the monitored platforms and extract data from sources relevant to service provision. Examples of such data sources include WebSphere MQ API, Windows Event Logs, Windows Performance Counters, Unix System Logs and Messaging Server log files. The data is transferred to a central Sentra server and into a Microsoft SQL Server database.

The Sentra server incorporates a powerful rules engine, which enables real time SLA monitoring to be automatically performed against a wide range of WebSphere MQ and application metrics. This is linked to a sophisticated alerting system that can employ a variety of mechanisms to alert individuals and groups to service threats. Sentra also features extensive query tools. These query tools can be used to monitor WebSphere MQ Servers that are running on multiple platform types.

In addition, Sentra provides extensive reporting features, using the industry-standard Microsoft Reporting Services engine. A wide variety of report formats can be generated and exported to MS Exchange public folders, web servers, etc.

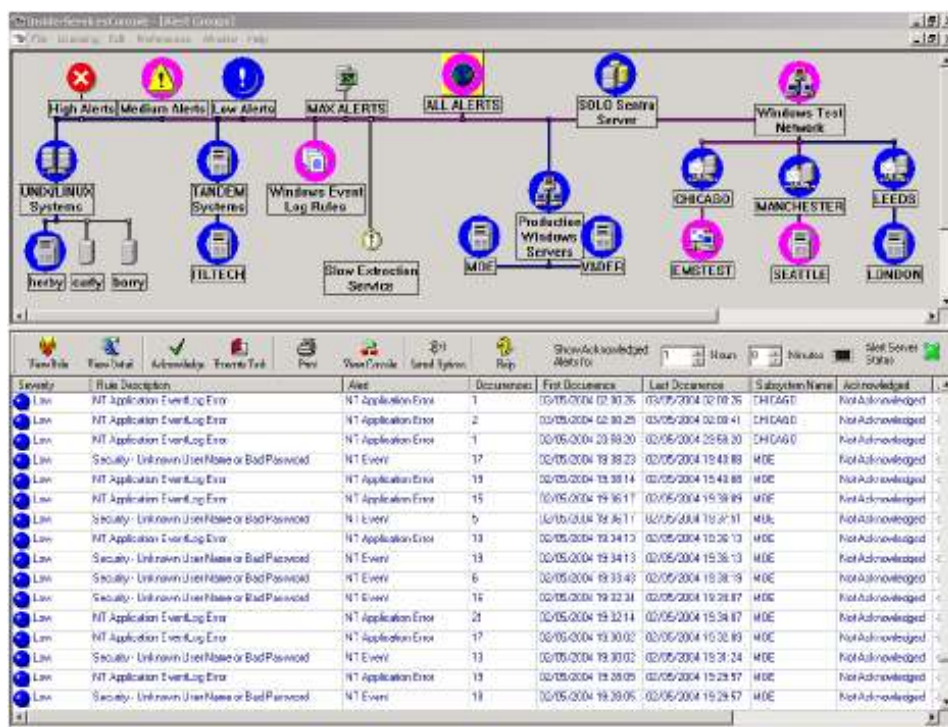
The precise nature of the deployment of Sentra is variable from one customer to another but typical benefits that Sentra provides include:

- Centralised, rules-based system monitoring. Rules can be deployed from a pre-configured rules library.
- Automated alerting to service threats and SLA violations through e-mail, SMS, SNMP trap, script files, batch files.
- Intelligent escalation and automatic fixing of problems as they occur (e.g. restarting services or processes).
- Server and workstation performance measurement and monitoring.
- Platform and application availability monitoring.
- Active Directory and X500 availability and performance monitoring.
- Simplified assessment of whether MQ messaging SLAs are being met.
- Monitoring of WebSphere MQ server performance.
- Integration with SNMP-based Enterprise Network Management Systems. Sentra MQ can also accept SNMP messages from routers and other SNMP enabled Network objects.
- WebSphere MQ traffic pattern assessment.
- Capacity planning.
- Reporting on messaging issues.
- SLA, billing or usage analysis.

User Interface

The concept of Sentra is that it should allow the user to easily and quickly manage all aspects of the managed network or WebSphere MQ system (i.e. the managed service). In order for this to happen the Sentra Graphical User Interface (GUI) has been designed to be easy to navigate and to access required data at all times.

A central feature is the Alert Groups View, which provides a topological representation of the managed service. This view is easily customisable to represent the key logical or physical elements of the managed service and enables the user to see at glance any events or problems that have occurred in any of these elements.

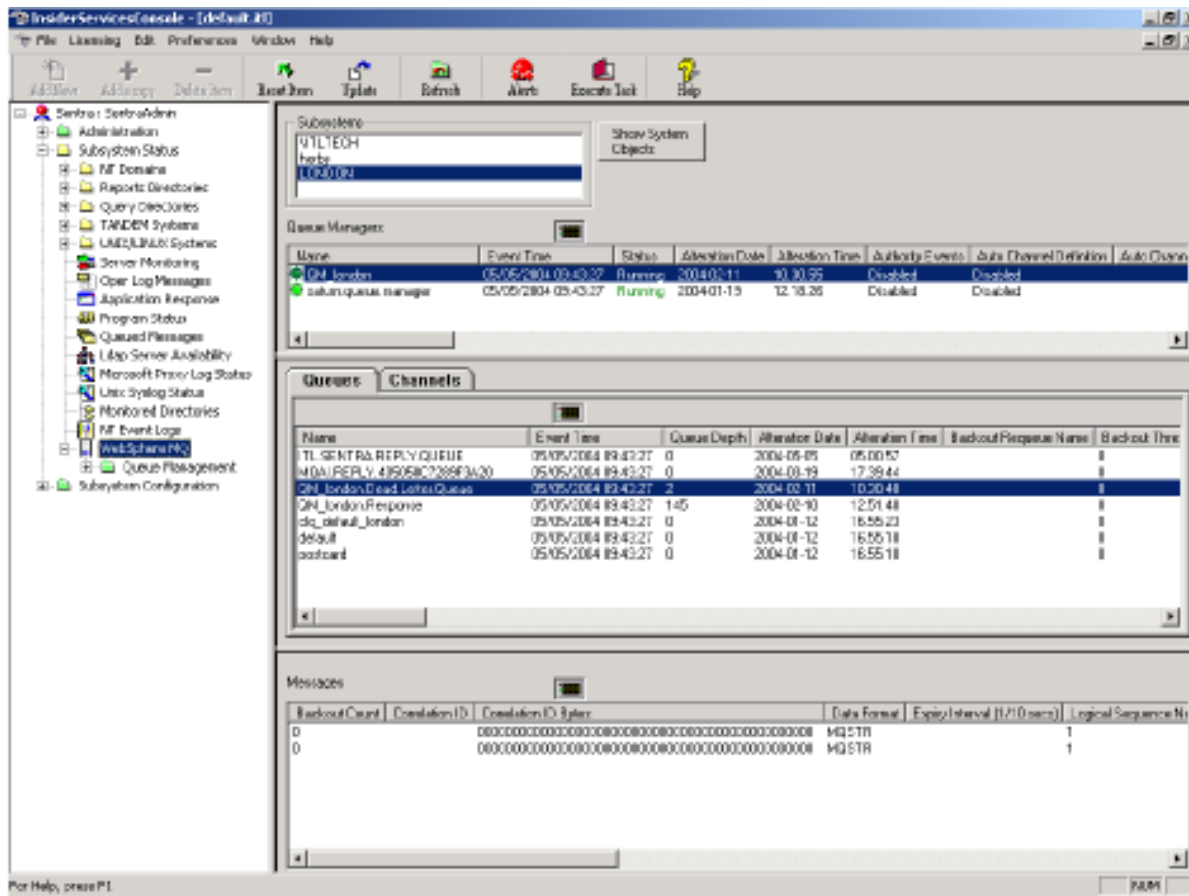


The Insider Services Console uses Explorer Tree methodology (similar to Windows Explorer) to provide an easy means of configuring, managing and monitoring one or more workstations or servers (referred to in Sentra as subsystems). The tree is split into three main categories: Administration, Subsystem Status and Subsystem Configuration. The following general features are supported:

- User, user group and security permissions configuration.
- Configuration of Windows services or Unix processes to be controlled and/or monitored.
- Configuration of Rules and Service level agreements.
- Views summarising WebSphere MQ Queue Manager, Queue and Channel status, platform availability, messaging system performance, enterprise directory (Active Directory and X500) availability and performance.
- Query tools.
- Reporting.

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.

The diagram below is a screenshot of the Sentra explorer tree view, showing the WebSphere MQ Status View.



Data Extraction

Extraction Services are Windows, HP NSK, and UNIX processes (or agents) that are responsible for extracting data from a variety of sources, and then transmitting this data to a central server location. Data transfer is achieved by connecting each extraction service or process to a SQL Server hosted server process (SMTDump), which commits the data to the SQL Server database.

Sentra provides the user with the ability to install extraction services to a remote platform and to configure, control and monitor these services.

The extraction processes can be configured to collect the following information.

- MQ Queue Manager, Queue and Channel Status
- Queue Depth Metrics
- Windows Event Log details
- Windows Performance Counters
- Unix performance information
- Unix Syslog information (/var/adm/messages)
- Windows, Linux and Unix directory information (e.g. number, size or age of files in directories)
- Enterprise Directory Services information (i.e. Active Directory or X500)
- Messaging Events
- Log file contents (from applications that write errors or information messages to a log file)

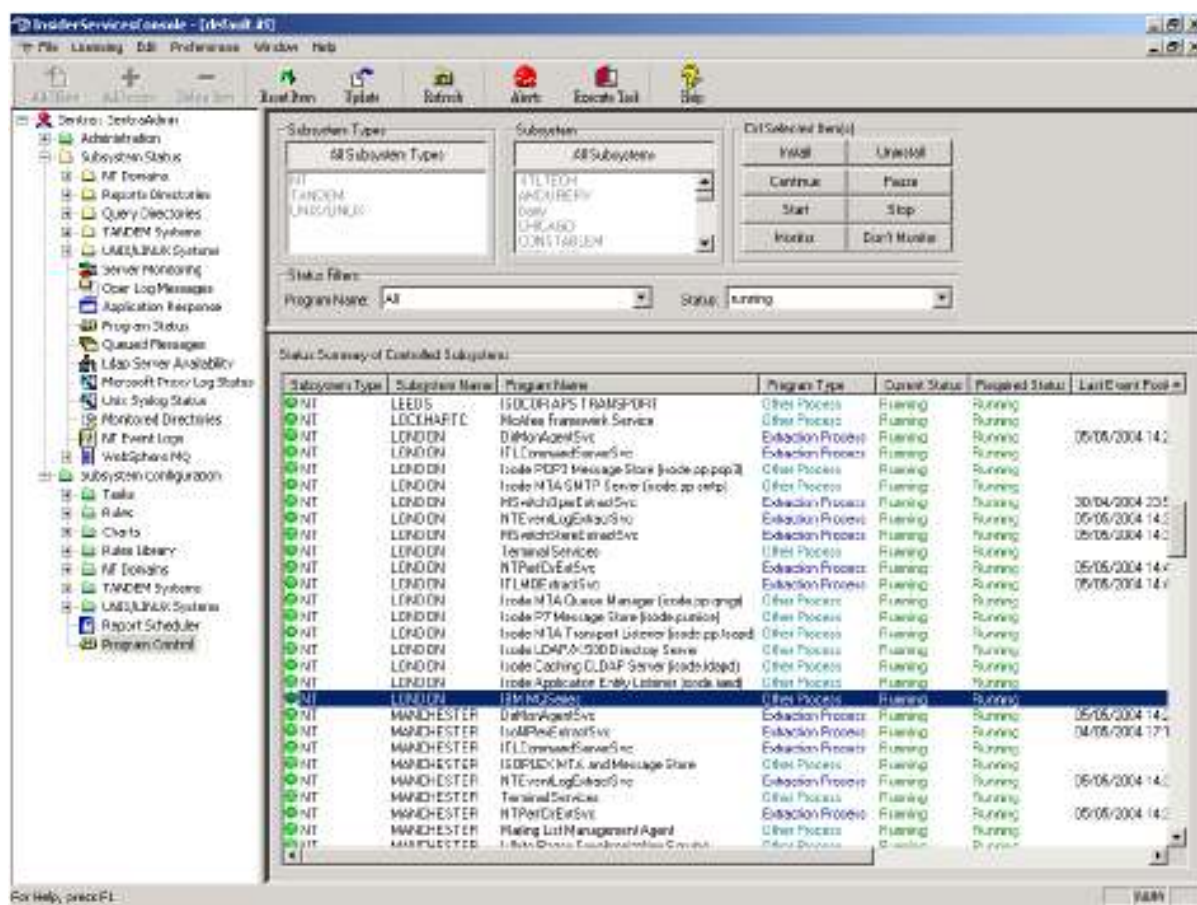
By collecting data in this manner, Sentra enables the user to access data that is generated as a result of actual events occurring in the network. This is superior to methods such as sending test messages and simple pinging of devices. Furthermore, as the data is constantly passed to the central server it is available for interrogation virtually immediately (subject to network availability and transfer rates), thereby providing real-time management of the system. The frequency of data transfer is configurable by the user, and transfer can take place across LANs, WANs or via a dialup link.

Service/Process Management

Sentra provides the facility to remotely install, control and monitor Windows services or processes running on Solaris and Unix platforms. This includes Sentra data extraction processes and any other services or processes, such as core WebSphere MQ services. If required, Sentra can automatically restart any monitored service or process in the case of a failure. Sentra supports rapid deployment of data extraction services across all managed Windows domains.

Rules can be configured to generate an alert based upon the status of one or more monitored services or processes.

Service and process status can be observed either through a global view or through subsystem views, as shown below.



The screenshot displays the 'Insider Services (console - [144x61] 40)' application window. The interface includes a menu bar (File, Learning, Edit, Preferences, Window, Help), a toolbar with icons for 'Add Item', 'Update', 'Refresh', 'Alerts', 'Execute Task', and 'Stop'. A left-hand navigation tree shows categories like 'Administration', 'Subsystems Status', 'Reports Director', 'Query Director', 'TAMDEM Systems', 'UNISPLINK Systems', 'Server Monitoring', 'Clear Log Messages', 'Application Response', 'Program Status', 'Queued Messages', 'LDAP Server Availability', 'Microsoft Proxy Log Status', 'Unix Syslog Status', 'Monitored Directories', 'NT Event Logs', 'WebSphere MQ', 'Subsystem Configuration', 'Tasks', 'Rbac', 'Charts', 'Rules Library', 'NF Domains', 'TAMDEM Systems', 'UNISPLINK Systems', and 'Report Scheduler'. The main area is divided into several sections:

- Subsystems Types:** A list of subsystems including TAMDEM and UNISPLINK.
- Subsystem:** A dropdown menu showing 'All Subsystems' and a list of specific subsystems: ATLTECH, ANDJREBY, LOW, CHICAGO, and CONTAMEN.
- Ctrl Selected Item(s):** Buttons for 'Install', 'Uninstall', 'Continue', 'Pause', 'Start', 'Stop', 'Install', and 'Don't Monitor'.
- Status Filter:** A dropdown menu for 'Program Name' set to 'All' and a dropdown for 'Status' set to 'Running'.
- Status Summary of Controlled Subsystems:** A table with columns: Subsystem Type, Subsystem Name, Program Name, Program Type, Current Status, Required Status, and Last Event Post.

Subsystem Type	Subsystem Name	Program Name	Program Type	Current Status	Required Status	Last Event Post
NT	LEEDS	ISDCORPAPSTRMSGPORT	Other Process	Running	Running	
NT	LOCKHART	Mockee Framework Service	Other Process	Running	Running	
NT	LONDON	DMSAgentSvc	Education Process	Running	Running	
NT	LONDON	ITLCommswServerSvc	Education Process	Running	Running	
NT	LONDON	Isode POP3 Message Store (isode:pp:pop3)	Other Process	Running	Running	
NT	LONDON	Isode NTA SMTP Server (isode:pp:smtp)	Other Process	Running	Running	
NT	LONDON	MS-Exchange-InfoSvc	Education Process	Running	Running	30/04/2004 23:5
NT	LONDON	NTEventLogControlSvc	Education Process	Running	Running	05/05/2004 14:0
NT	LONDON	MS-Exchange-SearchSvc	Education Process	Running	Running	05/05/2004 14:0
NT	LONDON	Terminal Services	Other Process	Running	Running	
NT	LONDON	NTPrefDiagSvc	Education Process	Running	Running	05/05/2004 14:0
NT	LONDON	ITLMDExtractSvc	Education Process	Running	Running	05/05/2004 14:0
NT	LONDON	Isode NTA Queue Manager (isode:pp:qmgr)	Other Process	Running	Running	
NT	LONDON	Isode PT Message Store (isode:pp:ptmsg)	Other Process	Running	Running	
NT	LONDON	Isode NTA Transport Listener (isode:pp:isodt)	Other Process	Running	Running	
NT	LONDON	Isode LDAP/300 Directory Service	Other Process	Running	Running	
NT	LONDON	Isode Coaching LDAP Server (isode:isodc)	Other Process	Running	Running	
NT	LONDON	Isode Application Entry Listener (isode:isodl)	Other Process	Running	Running	
NT	LONDON	ISINFOClient	Other Process	Running	Running	
NT	MANCHESTER	DMSAgentSvc	Education Process	Running	Running	05/05/2004 14:0
NT	MANCHESTER	ISMPREAgentSvc	Education Process	Running	Running	04/05/2004 17:1
NT	MANCHESTER	ITLCommswServerSvc	Education Process	Running	Running	
NT	MANCHESTER	ISDPUCNTS and Message Store	Other Process	Running	Running	
NT	MANCHESTER	NTEventLogControlSvc	Education Process	Running	Running	05/05/2004 14:0
NT	MANCHESTER	Terminal Services	Other Process	Running	Running	
NT	MANCHESTER	NTPrefDiagSvc	Education Process	Running	Running	05/05/2004 14:0
NT	MANCHESTER	Planning List Management Agent	Other Process	Running	Running	
NT	MANCHESTER	Isode Process Execution/Management Console	Other Process	Running	Running	

MQ Message Traffic Analysis

Sentra provides a number of pre-configured message traffic reports that can be generated using the graphical and textual reporting facilities of the general query tool.

This can be used for monitoring and analysing WebSphere MQ message traffic and trends. An example could be analysing messages routed across different MQ servers within a specified period of time. The general Sentra query console 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 are possible, e.g. with totals displayed hourly, daily, weekly.
- Results can be displayed in numerous 2D and 3D graph formats, e.g. pie charts, bar graphs.
- Results can be saved as csv (comma separated value) files and can be easily exported to an Excel (or similar) spreadsheet.

SLA Rule Analysis & Alerting

Sentra contains the ability to define rules that can monitor SLAs and processes running on the machines being monitored. Predefined rules are available for all major data types contained within the database providing an extremely powerful systems management tool. They can be categorised as follows:

- Windows Service Rules
- WebSphere MQ Rules
- Windows Event Log Rules
- Windows Performance Counter Rules
- Unix/Linux Process Rules
- Unix/Linux Syslog Rules
- Messaging Rules
- Server Availability Rules
- Active Directory and X500 Directory Rules
- Windows Files and Folders Rules
- Generic Log File Rules

When a rule's criteria has been met, a number of actions can be invoked in order to intelligently escalate or fix the problem. These include SMS Messages, Email, GUI Alert, SNMP Traps, batch jobs and Script files and apply to **all** rule types.

Rules can be assigned a severity, and can be configured to be active on certain days of the week and/or certain times of day. Thus, rules can be configured to alert an operator between 9 am and 5 pm on weekdays, but to alert an on-call engineer at all other times.

A brief description of some of the different categories of rule that can be configured in Sentra is provided in the following subsections.

MQ Service/Process Rules

Windows Service rules can be used to alert the user to any change in the status of one or more Windows Services. Services can be automatically restarted if they have failed.

Unix/Linux Syslog Rules

Rules can be configured to generate an alert when any type of event or combination of data within an event is written to the system log of a monitored Unix or Linux platform

Windows Event Log Rules

Windows Event Log rules can be configured to generate an alert when any type of event or combination of data within an event is written to the Windows event log of a monitored Windows platform.

Windows Performance Counter Rules

Windows Performance Counter rules can be configured to generate an alert based upon combinations of performance counter values on any monitored Windows platform. For example, rules can be set so that alerts are generated when systems approach their maximum disk capacity or when a process is utilising too much available system resource.

Unix/Linux Process Rules

Process rules can be used to alert the user to any change in the status of one or more monitored Unix or Linux processes. Processes can be automatically restarted if they have failed.

Messaging Rules

Messaging rules can be configured to alert the user to certain aspects of message system or server performance. Examples of the types of rules that can be configured include:

- Detection of non-delivered or rejected message
- Detection of a message or messages stuck in a dead letter queue
- SLA monitoring of end-to-end delivery time (i.e. delivery time through many message servers in a managed messaging service)
- SLA monitoring of message transfer time (i.e. time taken to be processed by a single message server)

Many other messaging rules are available.

Availability Rules

Availability rules can be configured to notify the user to the presence/absence of a monitored TCP/IP based server process, e.g. a Web server. Monitoring of the process is achieved by pinging the port on which the server process listens for connection. Rules can be configured based upon the server availability and the response time, enabling a user to be alerted to any detected server performance degradation.

Active Directory and X500 Directory Rules

Active Directory and X500 directory rules can be configured to notify the user to the presence/absence of an enterprise directory server. Monitoring of the directory is achieved by pinging the port on which the server process listens for connection. Rules can be configured based upon the server availability and the read/write response time, enabling a user to be alerted to any directory server performance degradation.

Monitored Files and Folder Rules

Monitored files and folders rules can be configured to alert the user aspects of one or more monitored directories. Rules can be configured based upon:

- The size of the directory (either in terms of the number of files it contains, or the disk space it occupies)
- The size of one or more files in the directory
- The age of files in a directory
- The creation, modification or deletion of files in a directory.

Generic Log File Rules

Extraction programs can be configured to capture data from any application which writes its performance information or errors to a time-based log file. Once configured, Sentra can allow a user to create rules based upon any combination of data within a line of text written to the log file.

Sentra MQ Tasks

Sentra MQ will allow you to quickly auto-discover the MQ objects in your environment. Once the Sentra agents are deployed to the machines that you wish to manage you will be able to see the overall performance of your MQ network. You will also have full control via the built in tasks which have been designed to simplify common MQ management jobs.

Control

Sentra MQ gives you the ability to control all of your MQ server objects via the Sentra console. This includes:

- Start/Stop Queue Managers
- Start/Stop Queues
- Start/Stop Channels
- Run Listeners
- Run Dead Letter Queue Handler

Security

- Manage Certificates
- Dump Authority
- Display Authority
- Set or Reset Authority
- Set Certificate Revocation List
- Scripting of Security Configuration

MQ Specific Troubleshooting

- Start/Stop Trace
- Start/Stop Trigger Monitor
- Start/Stop Client Trigger Monitor

MQ Rules and Alerts

Sentra MQ offers an alert view that will focus in on the following MQ specific errors:

- Queue Manager Stopped/Paused
- Queue Stopped/Paused
- Channel Stopped/Paused

- Queue Depth Threshold Exceeded
- Queue Time Threshold Exceeded
- Message Time Exceeded
- MQ Server Not Available
- Monitor MQ Error logs and alert on specific error conditions
- MQ Specific Windows Event Log Errors
- MQ Specific Unix Syslog Error Messages
- MQ Specific NSK EMS Events
- High Priority Message in Dead Letter Queue

Sentra is also shipped with many other tasks, e.g.

- Reboot a Windows or UNIX subsystem
- Launch Windows Event Viewer
- Display Anti-Virus Logs
- Show a list of all auto started services that have stopped
- Test Connect to an LDAP server
- Show Disk Capacity on a UNIX box
- Invoke Windows, UNIX or NSK Commands on subsystem
- Show all Sentra Rules that apply to a subsystem
- Show status of all SQL jobs

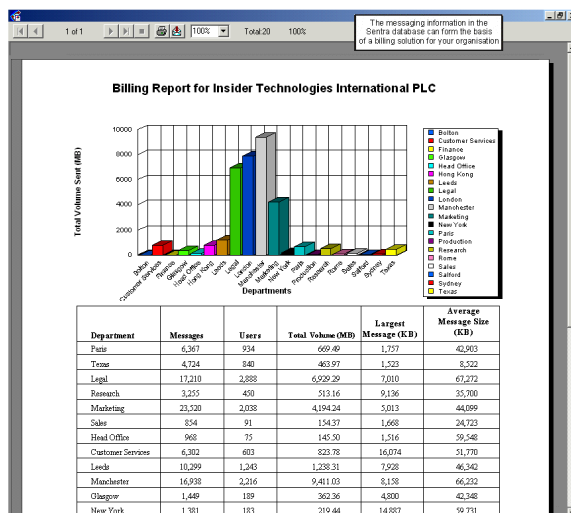
Reporting and Management Information

Sentra features a report viewer which utilises the Microsoft Reporting Services engine. Several pre-configured reports are shipped with Sentra. Users who have previous experience with the Reporting Services designer can design new reports. Alternatively, Insider Technologies team of experienced consultants can configure reports.

Reports can be configured to provide management reports to summarise the performance of the managed service. The following types of reports have been generated using Sentra for many existing customers:

- Bespoke billing reports
- Performance monitoring reports
- Message queue monitoring reports
- Capacity planning reports
- SLA compliance reports

Reports can be exported to a variety of destinations including web servers, Microsoft Exchange public folders, printers and disk files.



MQ Reports

- Queue Managers, Queues and Channels Configured by Subsystem.
- Queue Status Report By Subsystem.
- Channel Status Report by Subsystem.
- Trend of Message Queue Depth.
- WebSphere MQ Exception Report.

Real Time Dashboard

A Sentra 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 lengths can be shown, with one column for each message server.

Below is an example screenshot of a typical Sentra dashboard of four real-time graphs, each showing a different aspect of a WebSphere MQ Environment.



Implementation, Training & 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 Support on +44 (0)161 876 6606 or E-mail - support@insidertech.co.uk

Platform Support & System Requirements

Applications Supported:

- WebSphere MQ Server
- MS Exchange V5.5, 2000, 2003 and 2007
- Critical Path
- HP NSK OSI/MHS
- Messaging Direct
- Nexor
- Infonet
- 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 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

Support

Introduction

All problem registration and resolution support is initially carried out via the Helpdesk.

Hours Available

Provided you are covered by an annual maintenance contract you can contact us and we will do our best to provide you with a prompt solution. Hours of contact will be 9am until 5:30pm (GMT/ BST), Monday to Friday, excluding UK Bank Holidays. Support for hours outside of this can be negotiated in a separate contract.

Problem Reporting

When you call please ask for the Helpdesk. You will then be put through to someone whose responsibility it is to log your problem and if possible provide you with an immediate solution. It will help us if you categorise your problem into one of four types, namely:

Information: You have a general query about a product or need some information – Response within 5 working days.

Minor: You have an isolated problem that does not impact the business operations but you would like the problem corrected in some future releases - Response within 5 working days.

Major: The performance of a system or application has been interrupted and this may occur again unless the problem is solved. The problem is having a significant impact on your business - Response within 2 working days.

Critical: The system or application is down or at high risk of failure. Normal business operations cannot continue - Response within 1 working day.

The action the Help Desk will take will depend on the category of failure. It is therefore vital that you categorise the error correctly so that appropriate resources can be assigned to its resolution.

The response times shown above are standard. Please refer to your **Maintenance Agreement** for individual service levels of support.

What Should You Do?

To assist you in getting a response as quickly as possible you will need to do the following:

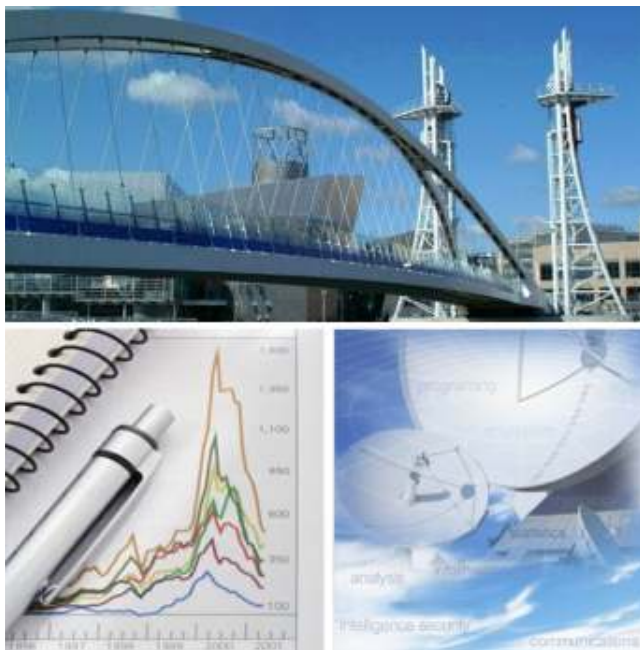
- Call us on **+44 (0)161 876 6606** and ask for the **Helpdesk**.
- Provide your name and Company name
- Provide contact Telephone and Fax details
- Identify the product involved
- State the level of severity of the problem

Describe the problem briefly, we will then provide you with an Issue Reference Number. The Helpdesk may request further information to be sent.

What will the Helpdesk Do?

Once the nature of your problem has been understood irrespective of the type of error, we shall try to resolve the problem immediately. If that is not possible then the problem will be passed to the product development group who are responsible for that particular product.

A Product group representative may then telephone you to get further details and to determine the best way to resolve the problem. Where a workaround or temporary fix is identified this will be agreed and delivered to you as soon as possible. The fix will then be scheduled to be incorporated into the next product release program. Once the fix has been implemented either as a permanent correction or as a temporary fix to become a permanent correction the Helpdesk will document the fact on an Issue Record and agree with you that the problem is now closed.



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
 37 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