

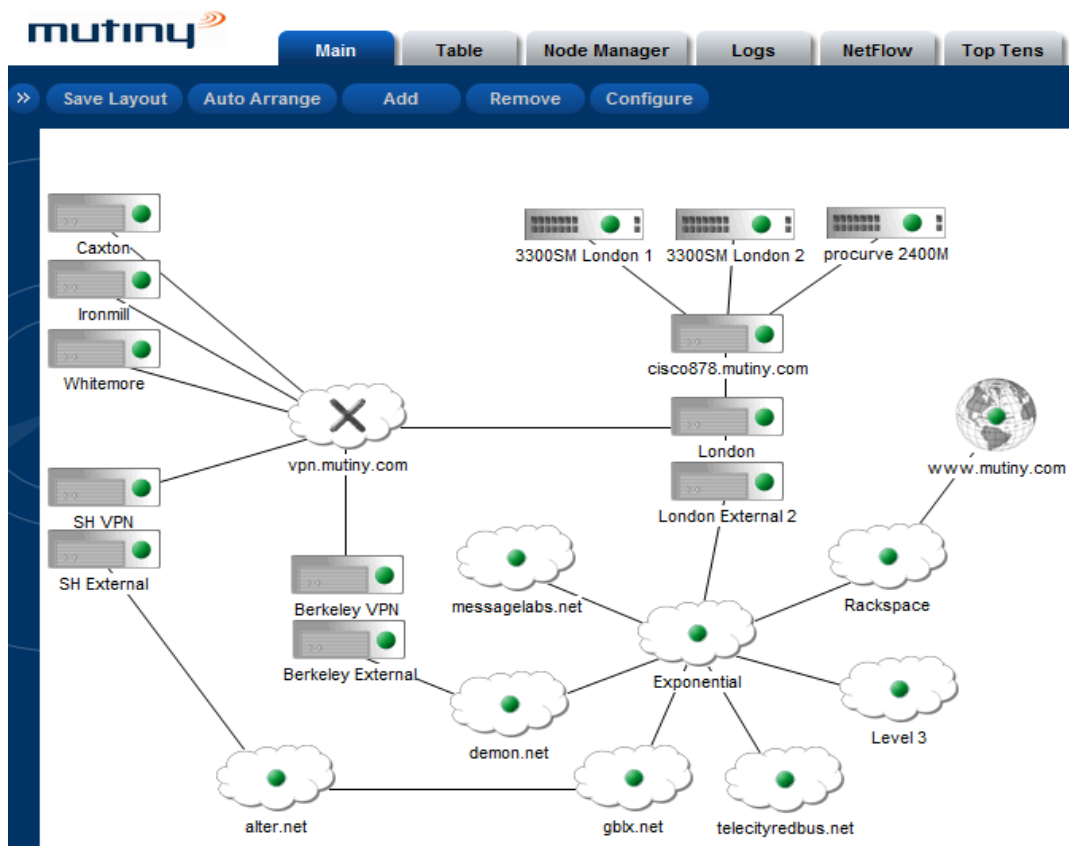
Mutiny at the heart of your network

Mutiny SNMP Monitor uses industry standard SNMP to gather information from IT Infrastructure, process and display the results in a multi-user web front-end that allows administrators and managers alike to quickly assess the health of their estate. Features include;

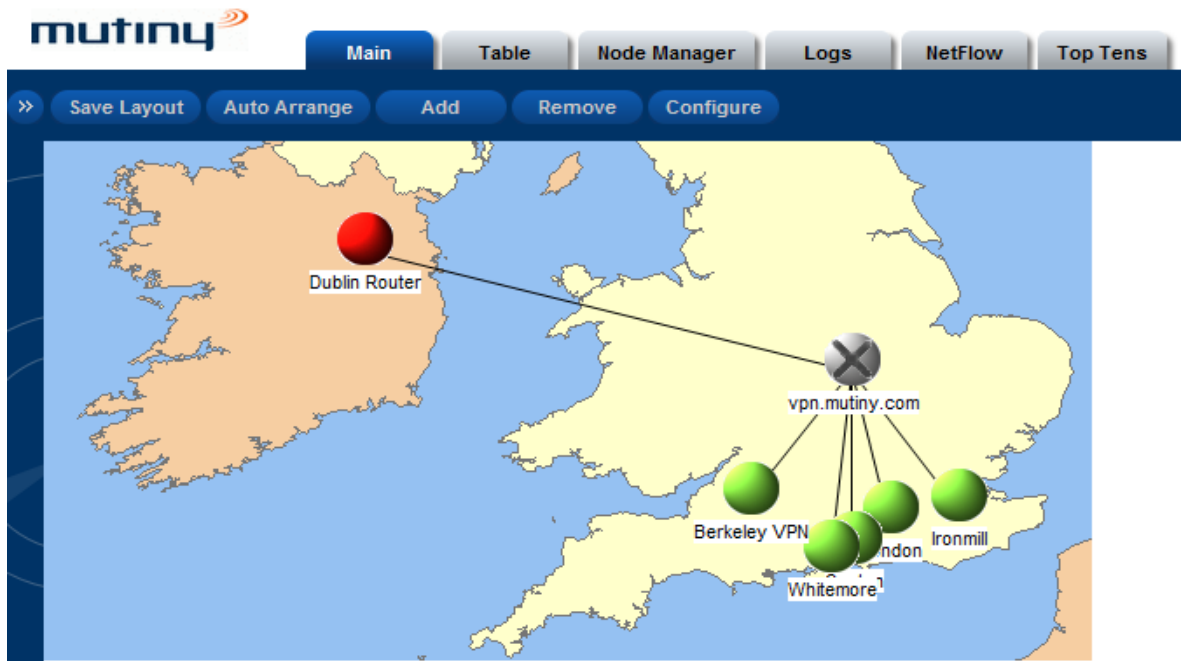
- Multi-user web based graphical interface.
- Flexible SMS and Email alert options to provide reliable notification of service related issues.
- Comprehensive polling options to minimise the impact on network traffic.
- Data collection and graphing facilities to analyse network trends.
- Rapid methods of discovering networked devices to ensure quick installation and simple configuration.

Display options

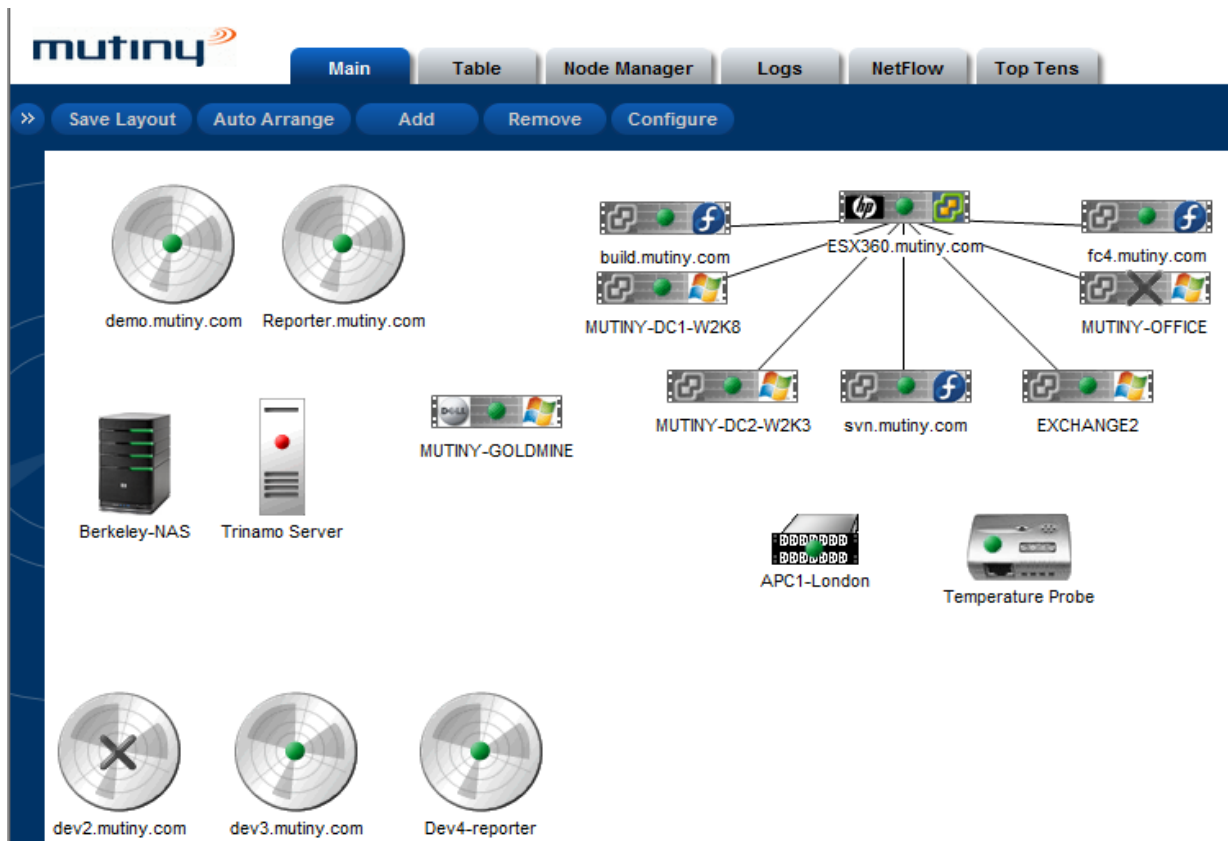
Mutiny is a web based appliance therefore it is naturally multi-user. The straight forward yet consistent approach to the display of data make it easy to see what is happening and also to publish selected views to a portal or intranet..



Views can display hierarchy and this helps non technical users understand the impact of problems in a network.



With the clever use of background images users can graphically see who is experiencing issues.



Clever use of icons help you see at a glance what type of technology is deployed.

The screenshot shows the Mutiny web interface with a drill-down path highlighted by red arrows: **Node Name** (London) → **Interfaces: London** → **WAN2** → **Interface Traffic: WAN2** graph.

Node Details (London):

- Node Name: London
- IP Address: 192.168.100.1
- DNS Name: gw-whitechapel.mutiny.com
- sysName: london
- OS: Unknown

Interfaces List:

Index	Description
0	
1	LAN
4	ADSL
5	WAN2
6	
7	

Interface Traffic: WAN2 Graph:

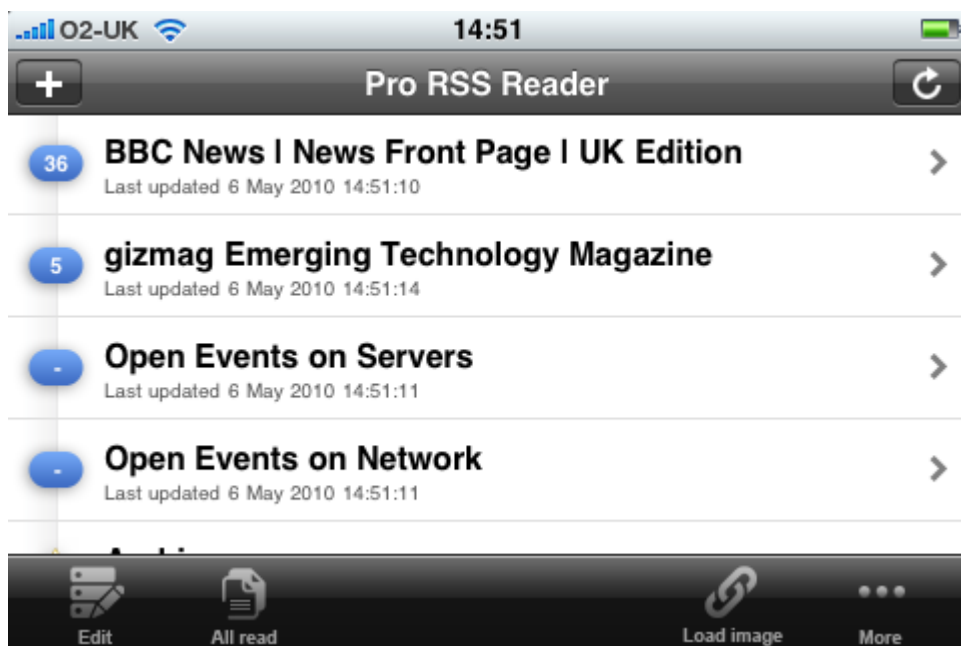
- Y-axis: b1 ts/s (0 to 300 k)
- X-axis: Time (Fri 30 to Wed 05)
- Legend: Out (Green), In (Blue)
- Buttons: Save Data, Apply, Close

The more you drill in the more detail you can see.

On the move?



Mobile browser Interface to allow you to browse your Mutiny whilst on the move.



RSS feeds from any view to allow you to keep on top of the situation.

In the Network Operations Centre

Date	Duration	Node	IP Address	Event	ID
1/5/10 04:04	6 days	mutiny-whitemore.mutiny.com	192.168.101.150	Processes Critical	117495
1/5/10 00:00	6 days	mutiny-whitemore.mutiny.com	192.168.101.150	Agent Critical	117466
30/4/10 12:31	6 days	Dublin Router	192.168.109.1	Ping Fail	117403
4/5/10 08:27	56 hours	Eagle-i	192.168.100.19	Agent Warning	117926
30/4/10 15:38	6 days	Trinamo Printer	192.168.20.77	Agent Warning	117425

Open events view with large fonts to display on large screens or LCD Projectors.

What you can get from each "Node" as we call them depends on what it runs and what additional vendor SNMP agents they have for example;

A ping only node on the Internet;

- Ping with RTT graphing
- Various port based service tests like web page content tests, mail relay etc.

Any wintel box with Microsoft's SNMP service installed will give us;

- Ping with RTT graphing
- SNMP service test
- Interface and traffic data
- CPU utilisation
- Memory usage
- Hard disk capacity

- Processes running
- Various port based service tests like web page content tests, mail relay etc.
- Graphing of system and interface data

A HP or Dell server with Insight or OpenManage agents installed;

- Ping with RTT graphing
- SNMP service test
- Interface and traffic
- CPU utilisation
- Memory usage
- Hard disk capacity
- Processes running
- Server environment, RAID status, CPU, Fans, temperature and redundant PSU status
- Various port based service tests like web page content tests, mail relay etc.
- Graphing of System and interface data

A Solaris box running net-SNMP (default in Solaris 10 available for older)

- Ping with RTT graphing
- SNMP service test
- Interface and traffic
- CPU Load factor
- Memory usage
- Hard disk capacity
- Processes running
- Various port service tests like web page content, mail relay etc.
- Graphing of System and interface data

A VMware ESX server running on HP with insight manager

- Ping with RTT graphing
- SNMP service test
- Interface and traffic
- CPU Load factor
- Memory usage
- Hard disk capacity
- processes running
- Server environment, RAID status, CPU, Fans, temperature and redundant PSU status
- Various port based service tests like web page content tests, mail relay etc.
- Graphing of System and interface data

A VMware virtual server

- Same as the appropriate server above.
- Cisco Switches and Routers
- Ping with RTT graphing
- SNMP service test
- Interface and traffic graphing with utilisation alerts etc.
- QoS monitoring and graphing
- ISDN 30 channel monitoring with utilisation graphs
- CPU utilisation
- Memory usage
- Chassis status including PSUs etc (if chassis has this capability)
- Graphing of System, interface data and QoS Data
- NetFlowTM
- Traps
- Energywise
- Other vendor Switches and routers
- Ping with RTT graphing

- SNMP service test
- Traps
- Interface and traffic graphing with utilisation alerts etc.
- Graphing interface data

APC and other RFC standard UPS manufacturers

- Ping with RTT graphing
- SNMP service test
- Graphing of power
- UPS agent to alert on status, battery and time to run etc.
- Various environmental probes
- Ping with RTT graphing
- SNMP service test
- Temperature graphing/alerting etc.

Reporting is important in any management situation and infrastructure is no exception. Being able to spot a trend, justify an upgrade, find application problems or simply report on the current state of play is an important, but often tedious task.

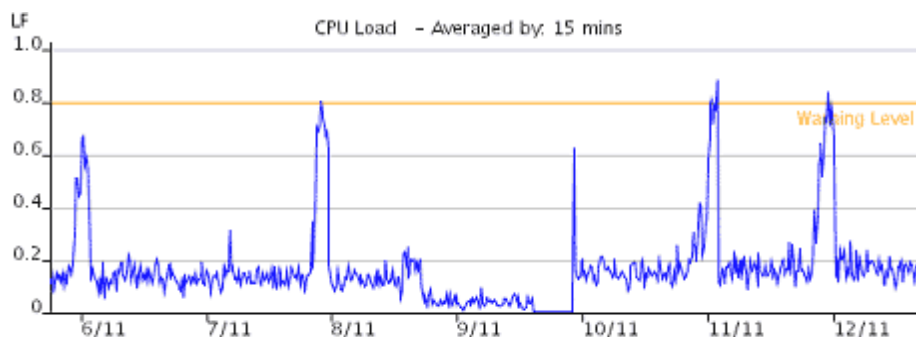
Mutiny has a variety of methods to arm the user with the necessary data required to satisfy the majority of reporting needs. But when the complex format of reports is required, Mutiny provides the raw data in an exportable CSV format, allowing the user to format or re-import the raw data into the reporting tool of choice.

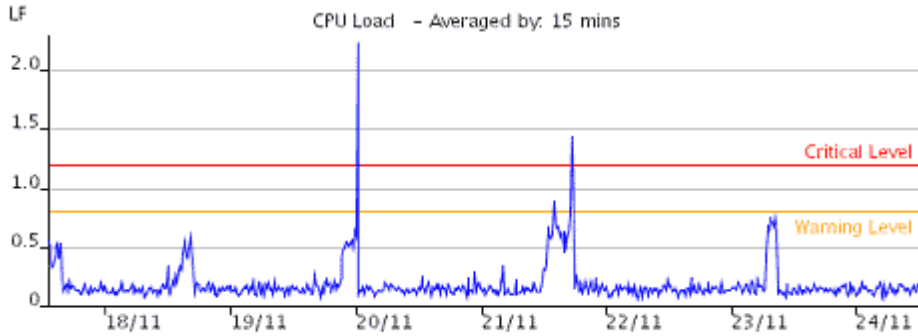
Graphing

Using the data collected every polling cycle, Mutiny can produce graphs for any given period. Auto-averaging in real-time means that you always have access to the real peaks, however long ago they were recorded.

All graphing data is available as a CSV output directly from the browser.

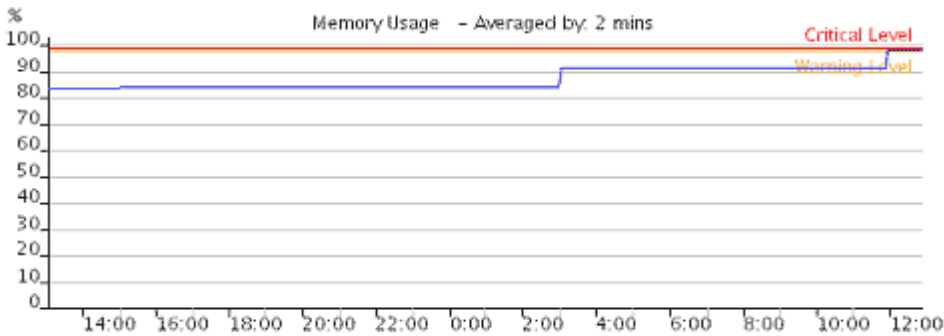
CPU Graph





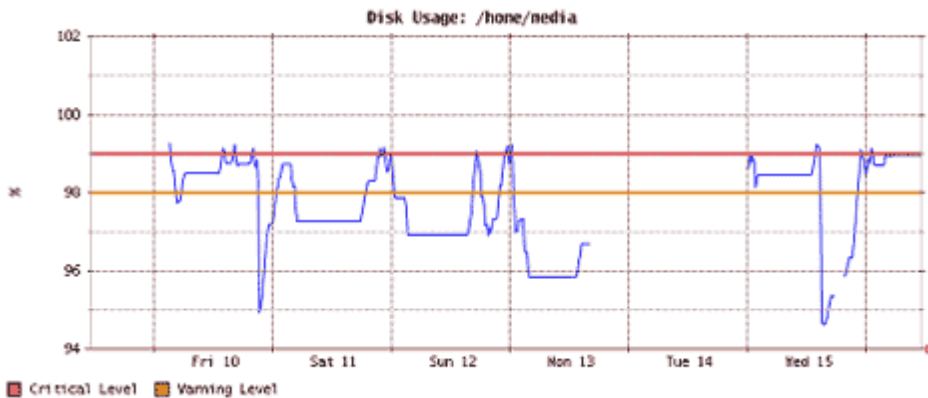
The CPU graph allows Managers to assess the current level of load any given node is experiencing. Whether you are looking at the daily peaks and assessing whether they are up to their daily duties, or looking long-term at a constant rise in load, the business can plan long-term on the viability of its hardware investment.

Memory Graph



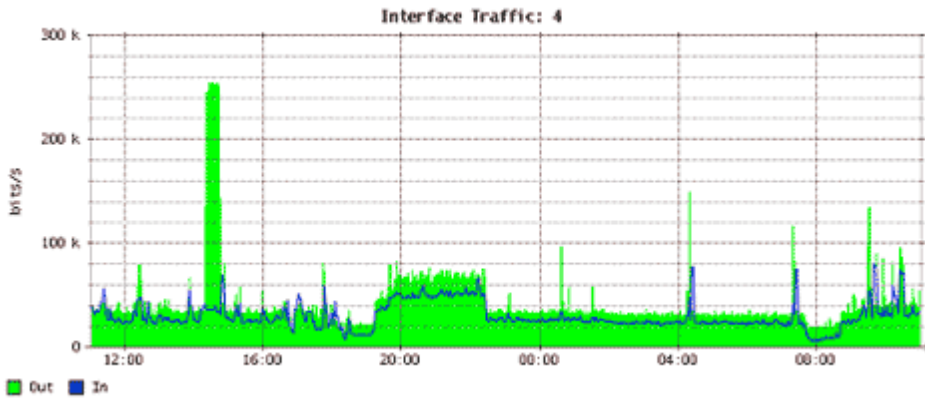
In a similar way to that of CPU graphs, the information displayed in the memory graphs can be vital in picking up issues on a particular node, like application memory leaks, terminal server overloads.

Disk Graphs



Whether you are reacting to a critical disk alert or just auditing the overall capacity of the hard drives on your critical nodes, these graphs will allow the Managers to assess the long-term capacity needs.

Interface Traffic Graphing



Traffic data can be stored from interfaces on Servers as well as router or switch interfaces.

Unlike a number of our competitors, Mutiny keeps all the data gathered during polling in its original form, allowing us to draw accurate graphs for any given time period. In addition, the raw data can be downloaded in CSV form for use in external reporting tools.

Event Log

Time Period:

Sort By:

Filter By:

	Date	Node	IP Address	Event	Details
●	24/11/04 17:43	dev2	127.0.0.1	CPU Load OK	ID 22375 Closed (2 mins) - Load Factor 0.67
●	24/11/04 17:42	Caxton	192.168.104.1	Ping OK	ID 22369 Closed (53 mins) - Node Ok
●	24/11/04 17:42	Caxton	192.168.104.1	SNMP OK	ID 22370 Closed (53 mins) - Response OK
●	24/11/04 17:40	demo.mutiny.com	193.123.1.201	Agent OK	check_polling - 1 minute since last poll
⊠	24/11/04 17:40	dev2	127.0.0.1	CPU Load Warning	ID 22375 Open - Load Factor 0.81
●	24/11/04 17:39	demo.mutiny.com	193.123.1.201	Agent OK	check_polling - 2 minutes since last poll
●	24/11/04 17:38	dev2	127.0.0.1	CPU Load OK	ID 22374 Closed (2 mins) - Load Factor 0.60
⊠	24/11/04 17:36	dev2	127.0.0.1	CPU Load Warning	ID 22374 Open - Load Factor 0.85
●	24/11/04 17:36	cori	192.168.101.2	IP Service OK	ID 22367 Closed (47 mins) - All IP Ports Ok
●	24/11/04 17:36	icornill	192.168.102.1	Ping OK	ID 22373 Closed (47 mins) - Node Ok
●	24/11/04 17:34	Whitemore	192.168.101.1	Ping OK	ID 22366 Closed (45 mins) - Node Ok
●	24/11/04 16:57	Bedford Square	192.168.110.1	Ping OK	ID 22371 Closed (8 mins) - Node Ok
●	24/11/04 16:54	Berkeley	192.168.103.1	Ping OK	ID 22368 Closed (5 mins) - Node Ok
●	24/11/04 16:54	demo.mutiny.com	193.123.1.201	Agent OK	check_polling - 1 minute since last poll
●	24/11/04 16:53	demo.mutiny.com	193.123.1.201	Agent OK	check_polling - 2 minutes since last poll
●	24/11/04 16:51	demo.mutiny.com	193.123.1.201	IP Service OK	ID 22372 Closed (2 mins) - All IP Ports Ok
●	24/11/04 16:49	Bedford Square	192.168.110.1	Ping Fail	ID 22371 Open - Node Down?
●	24/11/04 16:49	Berkeley	192.168.103.1	Ping Fail	ID 22368 Open - Node Down?
●	24/11/04 16:49	Caxton	192.168.104.1	Ping Fail	ID 22369 Open - Node Down?
●	24/11/04 16:49	Caxton	192.168.104.1	No SNMP Response	ID 22370 Open - SNMP Down?
●	24/11/04 16:49	cori	192.168.101.2	IP Service Critical	ID 22367 Open - "web" Critical
●	24/11/04 16:49	demo.mutiny.com	193.123.1.201	IP Service Critical	ID 22372 Open - "http" Critical
●	24/11/04 16:49	icornill	192.168.102.1	Ping Fail	ID 22373 Open - Node Down?

Mutiny keeps a log of all events that occur on the monitored network. The detail part of each event uses a series of unique ID numbers to allow for the matching of paired events. In addition



to this detail, the time between the IDs is calculated and displayed as time in brackets. This provides an instant SLA feedback.

Event Log CSV output

Date	Node	IP Address	Status	Event	Details
24/11/2004 21:12	192.168.105.10	192.168.105.10	Ok	Ping OK	ID 22353 Closed (675 mins) - Node Ok
24/11/2004 21:12	Tring	192.168.105.1	Ok	Ping OK	ID 22354 Closed (672 mins) - Node Ok
24/11/2004 21:01	demo.mutiny.com	193.123.1.201	Ok	Agent OK	check_polling - 1 minute since last poll
24/11/2004 21:00	demo.mutiny.com	193.123.1.201	Ok	Agent OK	check_polling - 2 minutes since last poll
24/11/2004 19:41	dev2	127.0.0.1	Ok	CPU Load OK	ID 22384 Closed (19 mins) - Load Factor 0.72
24/11/2004 19:41	dev2	127.0.0.1	Ok	CPU Load OK	ID 22383 Closed (33 mins) - Load Factor 0.72
24/11/2004 19:22	dev2	127.0.0.1	Critical	CPU Load Critical	ID 22384 Open - Load Factor 1.36
24/11/2004 19:08	dev2	127.0.0.1	Warning	CPU Load Warning	ID 22383 Open - Load Factor 1.10
24/11/2004 19:06	dev2	127.0.0.1	Ok	CPU Load OK	ID 22382 Closed (2 mins) - Load Factor 0.79
24/11/2004 19:04	dev2	127.0.0.1	Warning	CPU Load Warning	ID 22382 Open - Load Factor 0.82
24/11/2004 19:01	dev2	127.0.0.1	Ok	CPU Load OK	ID 22381 Closed (7 mins) - Load Factor 0.66
24/11/2004 18:54	dev2	127.0.0.1	Warning	CPU Load Warning	ID 22381 Open - Load Factor 0.92
24/11/2004 18:52	dev2	127.0.0.1	Ok	CPU Load OK	ID 22380 Closed (4 mins) - Load Factor 0.78
24/11/2004 18:52	dev2	127.0.0.1	Ok	CPU Load OK	ID 22379 Closed (14 mins) - Load Factor 0.78
24/11/2004 18:48	dev2	127.0.0.1	Critical	CPU Load Critical	ID 22380 Open - Load Factor 1.52
24/11/2004 18:37	dev2	127.0.0.1	Warning	CPU Load Warning	ID 22379 Open - Load Factor 0.99
24/11/2004 18:36	dev2	127.0.0.1	Ok	CPU Load OK	ID 22378 Closed (8 mins) - Load Factor 0.76
24/11/2004 18:28	dev2	127.0.0.1	Warning	CPU Load Warning	ID 22378 Open - Load Factor 0.97
24/11/2004 18:28	demo.mutiny.com	193.123.1.201	Ok	Agent OK	check_polling - 1 minute since last poll
24/11/2004 18:25	demo.mutiny.com	193.123.1.201	Ok	Agent OK	check_polling - 2 minutes since last poll
24/11/2004 18:25	dev2	127.0.0.1	Ok	CPU Load OK	ID 22377 Closed (6 mins) - Load Factor 0.73
24/11/2004 18:19	dev2	127.0.0.1	Warning	CPU Load Warning	ID 22377 Open - Load Factor 0.83
24/11/2004 18:18	dev2	127.0.0.1	Ok	CPU Load OK	ID 22376 Closed (2 mins) - Load Factor 0.71
24/11/2004 18:16	dev2	127.0.0.1	Warning	CPU Load Warning	ID 22376 Open - Load Factor 0.91
24/11/2004 17:43	dev2	127.0.0.1	Ok	CPU Load OK	ID 22375 Closed (2 mins) - Load Factor 0.67
24/11/2004 17:42	Caxton	192.168.104.1	Ok	Ping OK	ID 22369 Closed (53 mins) - Node Ok
24/11/2004 17:42	Caxton	192.168.104.1	Ok	SNMP OK	ID 22370 Closed (53 mins) - Response OK
24/11/2004 17:40	demo.mutiny.com	193.123.1.201	Ok	Agent OK	check_polling - 1 minute since last poll
24/11/2004 17:40	dev2	127.0.0.1	Warning	CPU Load Warning	ID 22375 Open - Load Factor 0.81
24/11/2004 17:39	demo.mutiny.com	193.123.1.201	Ok	Agent OK	check_polling - 2 minutes since last poll
24/11/2004 17:38	dev2	127.0.0.1	Ok	CPU Load OK	ID 22374 Closed (2 mins) - Load Factor 0.60
24/11/2004 17:36	dev2	127.0.0.1	Warning	CPU Load Warning	ID 22374 Open - Load Factor 0.85
24/11/2004 17:36	cori	192.168.101.2	Ok	IP Service OK	ID 22367 Closed (47 mins) - All IP Ports Ok
24/11/2004 17:36	Ironmill	192.168.102.1	Ok	Ping OK	ID 22373 Closed (47 mins) - Node Ok

The CSV output is useful for producing an overall SLA report showing, for example, the availability of all Servers or all WAN links, etc.

Alerting is critical to Mutiny; the ability to get the right message to the right person at the right time.

Mutiny is able to offer a highly flexible alerting engine that allows any number of people or groups to receive messages by a combination of:

- Email
- SMS/text
- Pop-up
- Helpdesk
- Lights on screen



Furthermore, Mutiny's shift pattern encourages the team to set up robust and efficient procedures. For example, it is likely that you will want to take email alerts during the day, and text alerts from, say, 6pm till 9pm. Beyond 9pm, alerts can be sent to a 3rd party helpdesk or to the individual on the night shift!

Contact List:

Name	Shift	Email	Delay	Page/SMS	Delay	Repeat
Andy Murray	1	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
	2	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
	3	<input type="checkbox"/>	<input type="text"/>	<input checked="" type="checkbox"/>	90	3
Tom Jones	1	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
	2	<input checked="" type="checkbox"/>	<input type="text"/>	<input checked="" type="checkbox"/>	30	<input type="text"/>
	3	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

The other key to Mutiny alerting lies in its ability to set up groups and integrate into helpdesk systems, like remedy, therefore triggering a ticket in advance of a problem.

Efficient Alerting

Users are encouraged to set alerts that are aimed at the expert. Some organisations will ensure that network and bandwidth issues are sent to the networking specialist, whilst server and application alerts go those specialists.

No false alarms

We recognise that one of the problems often experienced with other tools is the barrage of false alerts when, actually, services are not being compromised. There are a number of features that ensure only the relevant and necessary alerts will get through.

Root Cause Analysis - A feature unique to Mutiny that isolates the root cause of a problem. For example, if a link to a remote office were to fail, our competitor products might be inclined to send you alerts for the nodes at that site it can no longer see. This leads to confusion at the helpdesk, as front-line staff may be stifled by the information overload. Mutiny, on the other hand, will show the far end router as down and all other equipment unknown. This helps to focus eyes on the real issue.

Transient suppression - Mutiny also enables you to delay alerts. For example, if you have a CPU problem at 99%, it might be that this is a 3-minute 'spike'. Mutiny enables you to set a delay on this of, say, 30 minutes, so that the alert only gets triggered if this event is still a problem after that time.

Escalation - The Delay parameter in the alerting panels also enables a pattern of escalation to be enforced. You can, for example, send the initial alert to the helpdesk; then after a delay of, say, 60 minutes, escalate the alert to a supervisor or line manager.



Text Repeats - To ensure the most severe problems are actioned, Mutiny can send text alerts repeatedly until action is taken.

Thresholds and Reporting - Mutiny is installed with factory settings for thresholds and we encourage users to run these for a period of a week or so. This will allow you to find your own natural 'watermarks' and tweak your threshold configuration accordingly. For example, a machine running at permanent 95% CPU usage might be perfectly normal - the threshold should be moved to accommodate this, once again helping to reduce false alerts.

Mutiny's fundamental objective is to ensure that a company's network services support both revenue generation and time/cost savings.

Mutiny achieves this by:

- ensuring network services are increasingly available and more efficient
- reducing overall costs associated with providing network support
- Free up skilled staff from daily tasks