

SyAM Software, Inc.

**Server Monitor Central
Desktop Monitor Central
V3.21**

**Central System Management Software
User Manual**

Revision A
October 2006

© 2006 SyAM Software, Inc.
All rights reserved. SyAM Software and the SyAM Software logo are trademarks of SyAM
Software, Inc.
All other trademarks are the property of their respective owners.

Information contained in this document is assumed to be accurate at the time of
publishing. SyAM Software reserves the right to make changes to the information
contained in this document at any time without notice.

For additional information, sales, or technical support, contact SyAM Software

www.syamssoftware.com

Part Number 010110A-EN

Table of Contents

Introduction.....	7
SyAM Software Modules.....	8
Compatibility.....	8
Deployment Options.....	9
Chapter 1: Installation and Configuration.....	10
Installation Instructions – Windows.....	11
Installation Instructions – Linux.....	11
Firewall Security	11
SyAM Program Menu Options (Windows).....	12
Uninstalling SyAM (Windows).....	13
Uninstalling SyAM (Linux).....	13
Chapter 2: Logging In.....	14
Browsing to the SyAM Web Server.....	15
Ending the Session.....	16
Chapter 3: The SyAM Central System Management User Interface.....	17
The SyAM Central System Management User Interface.....	18
Interface Layout.....	18
Health Colors.....	19
Icons.....	20
Adding Systems to the Management Tree.....	21
Filter by, Grouping and Sorting Options for the Management Tree.....	24
Expanding the Server/Desktop Monitor Central Tree.....	26
Chapter 4: License Management.....	28
License Management.....	29
Chapter 5: Remote Management.....	31
Remote Management.....	32
System State.....	32
Wake on LAN.....	33
Remote Console.....	34
AMT (Intel Active Management Technology).....	38
IPMI Event Log.....	45
IPMI Over LAN.....	47
Chapter 6: Central Event Logging.....	49
Central Event Logging	50
Chapter 7: Central Reporting.....	52
Reporting.....	53
Chapter 8: Configuring System and Central Alerts	56
System Alert Matrix – System Level Alerting.....	57
Monitored Sensor Types.....	58
Logical Sensors.....	58
Notification Settings.....	59
Disabling Notifications	59
Removing a Sensor Instance From the System Alert Matrix.....	60
Notification Settings – Configuring email alerting.....	61
Central Alert Matrix.....	63
Types of monitored events	63
SyAM Integration into Enterprise Frameworks	65
Chapter 9: Accessing System Information.....	66
System Detail Tab.....	67
Power Management Tab	69
Hardware Detail Tab.....	71
Network Detail Tab.....	72
Storage Detail Tab.....	72
RAID Management.....	74
Deleting a RAID Set.....	78
Software Detail Tab.....	79
Chapter 10: Configuring Platform Event Trap Support.....	81

Platform Event Traps.....	82
Configuring Server Monitor Central to Receive Platform Event Traps.....	83
Chapter 11: Contact Details & Glossary.....	86
Contact Details.....	87
Glossary.....	87

Table of Figures

Figure 1: Servers, Desktops and Notebooks being managed by a system running the Server Monitor Central software.....	9
Figure 2: Desktops and Notebooks being managed by a system running the Desktop Monitor Central software.....	9
Figure 3: SyAM's program menu.....	12
Figure 4: SyAM programs Utilities Menu.....	12
Figure 5: Removing SyAM - Windows.....	13
Figure 6: Removing SyAM - Linux.....	13
Figure 7: Windows and Linux Login Screens.....	15
Figure 8: Successful Logout.....	16
Figure 9: SyAM Central Manager User Interface Layout.....	18
Figure 10: Header Bar.....	18
Figure 11: SyAM Health State Colors.....	19
Figure 12: Adding Managed Systems using an IP Address range	21
Figure 13: Status showing 6 systems added	22
Figure 14: Removing a system from the Management Tree.....	22
Figure 15: Systems Grouped by Location in IP Address Order shown with and without subgrouping.....	24
Figure 16: Management Tree Filter By, Group By and Sorting Options.....	25
Figure 17: Examples of the Filter By Option.....	25
Figure 18: Management Tree – Contracted Groups.....	26
Figure 19: Management Tree – Expanded Group with contracted Systems.....	26
Figure 20: Management Tree – Fully expanded Group and Systems.....	27
Figure 21: License Management Screen – Within Evaluation Period.....	29
Figure 22: License Management Screen – With Purchased License Key.....	30
Figure 23: Remote Management Option.....	32
Figure 24: System Status and Wake on LAN Capabilities.....	32
Figure 25: Wake On LAN (WOL).....	33
Figure 26: Remote Console Enabled and Running.....	34
Figure 27: Remote Console Login.....	35
Figure 28: Remote Console – Managing a remote System.....	35
Figure 29: Remote Console – Changing the User Settings.....	36
Figure 30: Remote Console – Starting the Remote Console Service.....	36
Figure 31: Remote Console – Clipboard.....	37
Figure 32: Remote Console – Disconnect.....	37
Figure 33: AMT Login Tab.....	38
Figure 34: Launching the AMT Console.....	38
Figure 35: Establish AMT Connection.....	39
Figure 36: AMT Remote Control.....	40
Figure 37: Serial Over LAN (In Use showing BIOS Re-configuration).....	40
Figure 38: IDE-R (Configured to boot off CD-Rom).....	41
Figure 39: IDE-R (In Use showing remote boot off CD-Rom).....	42
Figure 40: AMT System Defense (Establish AMT Connection).....	43
Figure 41: Download SyAM Policies.....	43
Figure 42: AMT System Defense Policies.....	44
Figure 43: IPMI Event Log.....	45
Figure 44: IPMI Event Log Retrieval.....	46
Figure 45: IPMI Over LAN – Enter details for accessing the BMC.....	47
Figure 46: IPMI Over LAN – Details applied.....	47
Figure 47: IPMI Over LAN – Connected.....	48
Figure 48: Event Log.....	51
Figure 49: Central Manager Reports.....	53
Figure 50: Summary and Detailed Reports.....	55
Figure 51: System Alert Matrix.....	57
Figure 52: Setting Category and Instance-Level Notifications.....	59
Figure 53: Entering Notification Information.....	62

Figure 54: Central Alert Matrix.....	64
Figure 55: System Detail Tab.....	67
Figure 56: System Detail Tab Continued.....	67
Figure 57: Power Management Tab.....	69
Figure 58: Hardware Detail Tab.....	71
Figure 59: Network Detail Tab.....	72
Figure 60: Storage Detail Tab.....	72
Figure 61: Storage Details – Managed RAID Controllers.....	74
Figure 62: RAID Controller Details Screen.....	75
Figure 63: Physical Drives – Choosing drives for the Array.....	76
Figure 64: Available Array - Configuring the RAID Set.....	76
Figure 65: RAID Set Details – Information on Configured RAID Set.....	77
Figure 66: Removing a Hot Spare drive.....	77
Figure 67: RAID Set Details – Deleting a RAID set.....	78
Figure 68: Software Detail Tab.....	79
Figure 69: End the Process.....	79
Figure 70: Confirm to End the Process.....	79
Figure 71: Starting a Service.....	80
Figure 72: Confirm to Start the Service	80
Figure 73: Stopping a Service.....	80
Figure 74: Confirm to Stop the Service	80
Figure 75: Example of a PET email alert.....	82
Figure 76: Example of PET information in the Event Log.....	82

Introduction

SyAM Software provides a comprehensive, simple to use set of system management products called Server Monitor, Desktop Monitor, and Notebook Monitor. Each of these products have features specific to their relevant system's capabilities and functions, as well as a large number of common features. Their user interfaces are identical. These products enable several IT benefits. Among them are predictive alerting to pending failures, system configuration, unattended monitoring and alerting, remote management, and reporting. The products dynamically discover the hardware and software operating environment, and manage all physical environmental sensors available and operating system resources. Users can view them and be alerted if they exceed their thresholds.

There are two levels of system management. Local System Management software provides a single system view. Central System Management software provides a unified view of all of your systems, and also provides more comprehensive features.

The Local System Management products are:

- *Server Monitor Local*
- *Desktop Monitor Local*
- *Notebook Monitor Local*

The Central System Management products are:

- *Server Monitor Central*
- *Desktop Monitor Central.*

(An instance of Server Monitor Central or Desktop Monitor Central is also referred to as a "Central Manager" in the remainder of this document.)

This user manual describes the Central System Management software. The following sections will describe the product functionality of the Central System Management software itself, and also explain how managing other systems via a Central Manager unlocks features in those systems.

SyAM Software Modules

Central System Management software contains two products;

- **Server Monitor Central** – This software provides the ability to manage Servers, Desktops and Notebook platforms running the Local Management Software.
- **Desktop Monitor Central** - This software provides the ability to manage Desktops and Notebook platforms running the Local Management Software.

These products can be installed on any Intel architecture x86/x64 platform running one of the supported operating systems.

Compatibility

<i>Operating System</i>	<i>Server Monitor Central</i>	<i>Desktop Monitor Central</i>
<i>Windows 2003 Server</i>	■	
<i>Windows 2000 Server (SP3 or above)</i>	■	
<i>Windows XP Professional (SP1 or above)</i>	■	■
<i>Windows 2000 Professional (SP3 or above)</i>	■	■
<i>Redhat Enterprise Server 4, ES3 (Update 4) (2.6.9-5.ELsmp / 2.4.21-27.ELsmp)</i>	■	
<i>Redhat Workstation 4, WS3 (Update 4) (2.6.9-5.ELsmp / 2.4.21-9.ELsmp)</i>	■	■
<i>Redhat Desktop 9 (2.4.20-8smp)</i>	■	■
<i>SuSE Enterprise Server 9 (2.6.5-7.97-default)</i>	■	
<i>SuSE Professional 9.2 (2.6.8-24-default)</i>	■	■
<i>Novell Linux Desktop 9 (2.6.5-7.111-default)</i>	■	■
<i>Fedora Core 3 (2.6.9-1.667)</i>	■	

Linux x64 Operating System Requirements

If you are running a Redhat/Fedora Core x64 Linux distribution, you must load the Compatibility Arch Support (Multilib Support Packages). To check if this is loaded look in: system settings, add/remove applications and scroll to the bottom to verify that this package is installed. If not please install it.

System Requirements

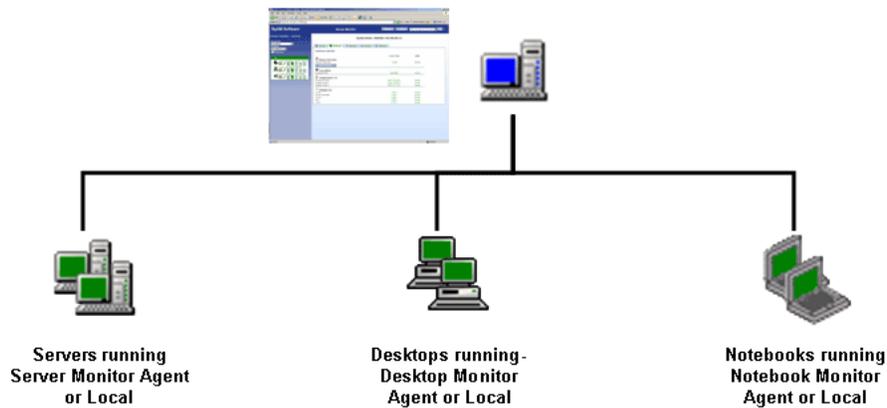
- 200MB Disk space
- 512MB Memory

Browser Requirements

- Internet Explorer 6+ (Service Pack 1)
- Mozilla Firefox (V1.0.x or above)

Deployment Options

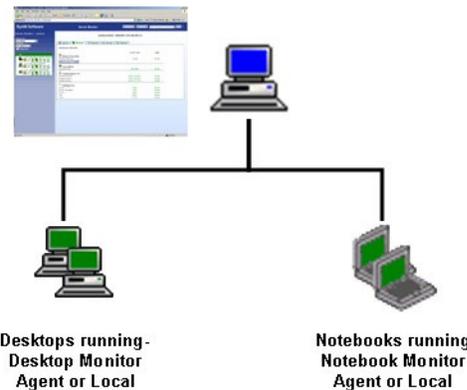
Administrator's use Internet Explorer or Firefox to browse to the Central Manager interface to manage all systems



Agents send event notification messages to administrators via email, SMS/Pager, network message, SNMP Trap, System Event Log or event to the Central Manager

Figure 1: Servers, Desktops and Notebooks being managed by a system running the Server Monitor Central software.

Administrator's use Internet Explorer or Firefox to browse to the Central Manager interface to manage all systems



Agents send event notification messages to administrators via email, SMS/Pager, network message, SNMP Trap, System Event Log or event to the Central Manager

Figure 2: Desktops and Notebooks being managed by a system running the Desktop Monitor Central software.

Chapter 1: Installation and Configuration

This chapter provides step-by-step installation and configuration instructions for SyAM Central System Management software on Windows and Linux Operating System Platforms

It is recommended that you print off the quick start guide before installing the software too. This simple document will step you through installation and email configuration in a few minutes.

Installation Instructions – Windows

1. Either load the SyAM Software CD and from the menu choose the product version you wish to install, or double click the downloaded SyAM executable. Then just follow the Install Wizard instructions.
2. Choose the language of the user interface.
3. Choose the destination folder (This can not contain any spaces in the name)
4. Do not change the RMI port default value of 1099 unless you know that port number is already in use
5. To enable security through 128-bit data encryption from the SyAM Server Web Server to the browser, choose the SSL option. (default=No)
6. After the installation has finished, the SyAM services will start and dynamically discover and configure your system's monitoring environment.

Installation Instructions – Linux

1. Download the required product version or copy it from the SyAM Software CD, to the Linux system.
2. Extract the files and change permission to execute the files
3. Enter `./install` – then follow the on screen instructions
4. Choose the language of the user interface.
5. Choose the destination folder (This can not contain any spaces in the name)
6. Do not change the RMI port default value of 1099 unless you know that port number is already in use
7. To enable security through 128-bit data encryption from SyAM Server Web Server to the browser, choose the SSL option. (default=No)
8. After the installation has finished, the SyAM services will start and dynamically discover and configure your system's monitoring environment.

Firewall Security

The following ports must be opened if you are using a firewall on your Linux system. They are automatically opened on Windows 2003 and XP Pro systems during the installation.

- 3894 – Used for Agent management service
- 3895 – Used for Central management service
- 3930 – Used for Web server service
- 5800 – Used for Remote Console access from Central Manager
- 5900 – Used for Remote Console access from Central Manager
- 58900 – AMT SOL – Session #1
- 58901 – AMT SOL – Session #2
- 58902 – AMT SOL – Session #3

SyAM Program Menu Options (Windows)

For Windows installations a set of options under the Programs Menu are provided.

Menu Options

On the start menu, select

<Programs>

<SyAM>

<Utilities>

<Enable SCSI SMART Monitoring>

<XP-2003 Port Update>

<Release Notes>

<Remote Console User Settings>

<SyAM Server/Desktop Console>

<User Manual>

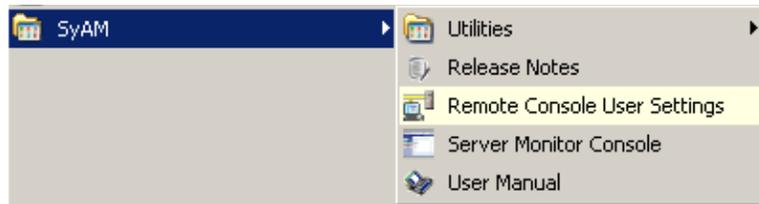


Figure 3: SyAM's program menu

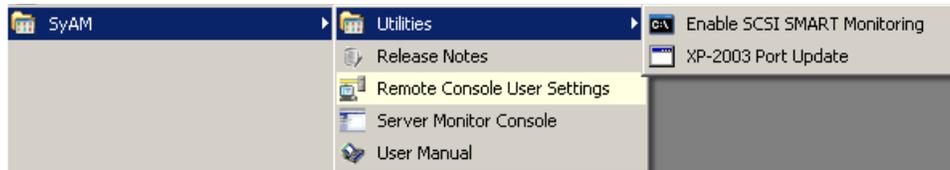


Figure 4: SyAM programs Utilities Menu

If Windows XP / 2003 Service packs are updated to the system after the software is installed, then you must open up the required firewall port by running the XP-2003 Port Update from the Utilities Menu. This will open up the required firewall ports to allow the software to function correctly.

By default your system's drives are SMART-monitored for predictive-drive failure analysis if they are ATA or S-ATA. However if your system utilizes a SCSI Disk drive then you must choose "Enable SCSI SMART Monitoring" and reboot your system to enable this feature.

Uninstalling SyAM (Windows)

To remove the SyAM software from the windows system:

1. On the start menu, select <Settings> <Control Panel> <Add/Remove Programs>
2. Highlight SyAM and select <Remove>. You will be prompted to confirm this action.
3. Following removal, if SyAM software is to be reinstalled then a system restart is required.



Figure 5: Removing SyAM - Windows

Uninstalling SyAM (Linux)

To remove the SyAM software from the Linux system:

1. Go to the top-level directory where the SyAM software was installed.
2. `./uninstall`

The software will be uninstalled.

```
d915glvg-emc:/syam #
d915glvg-emc:/syam #
d915glvg-emc:/syam #
d915glvg-emc:/syam #
d915glvg-emc:/syam #
d915glvg-emc:/syam #
d915glvg-emc:/syam # ls
. . . java jetty smad system_monitor uninstall
d915glvg-emc:/syam # ./uninstall
are you sure you want to uninstall [y/n]? y
uninstalling product...
shutting down services... done
removing services from system service list... done
removing /syam... done
uninstall complete
d915glvg-emc:/syam #
```

Figure 6: Removing SyAM - Linux

Chapter 2: Logging In

This chapter provides details on logging into the SyAM User Interface

Browsing to the SyAM Web Server

Open a supported web browser on any system and access the SyAM user interface on any system with the SyAM Central Manager installed. Then enter:

<http://IPADDRESS> or the MACHINENAME:3930

Example <http://192.168.1.19:3930>

Example <http://FILESERVER:3930>

If you enabled SSL during installation, you are required to type “https” instead of “http”:

Example: <https://IPADDRESS> or <https://MACHINENAME:3930>

This will bring you to the log in screen.

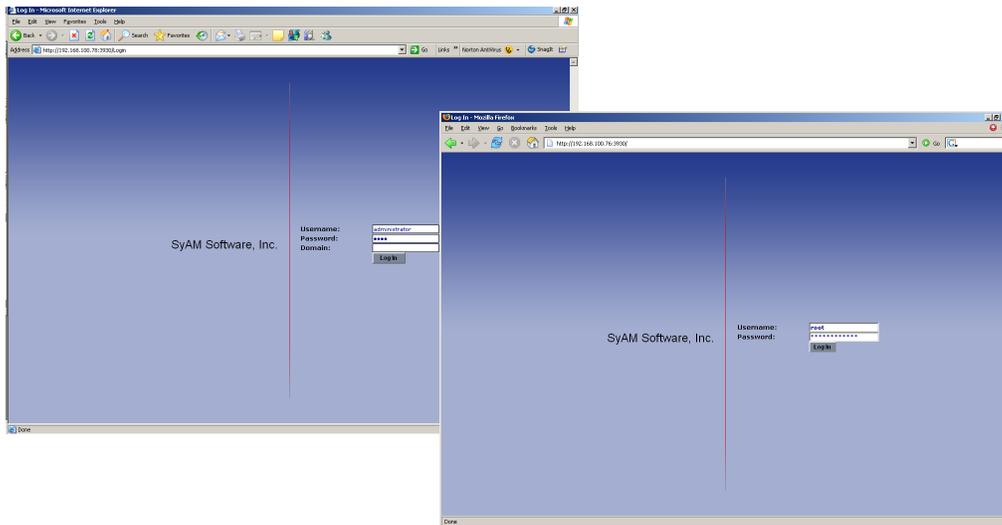


Figure 7: Windows and Linux Login Screens

The SyAM web server does not maintain its own separate set of users and passwords. It requests the operating system to log you in, so uses the accounts that are already in place on your system. To login you must satisfy the following conditions:

For Standalone systems (not in a Windows Domain)

- The User name and Password must be valid on the system you are logging into.
- The User must have Administrator rights on the system.

For systems within a Windows Domain

- The User name and Password must be valid in the Domain.
- The User must have "Domain Admin" rights within the Windows Domain
- A Valid Domain Name for the system must be entered in the Domain field.

For Linux systems

- The User name and Password must be valid on the system you are logging into.

Ending the Session

When you have completed your management session, choose the Log Out button on the main header bar. Successful logout returns you to the login screen:

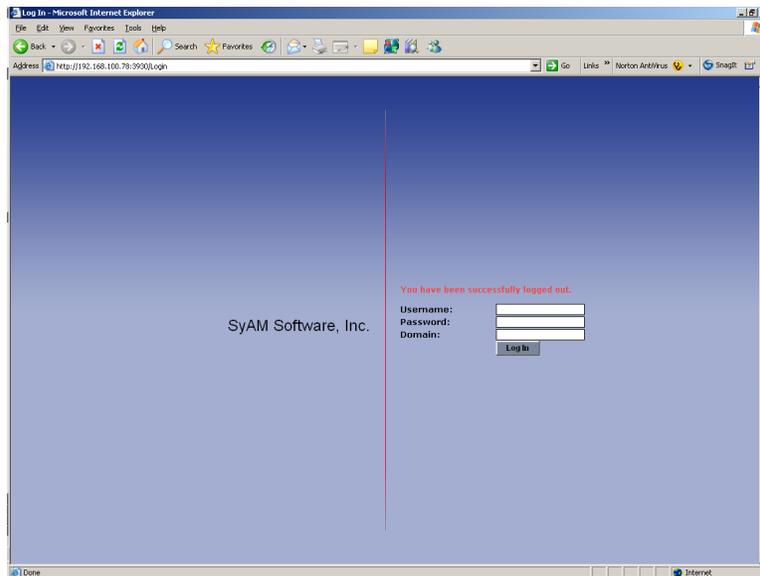


Figure 8: Successful Logout

For added security you will be logged out automatically after 30 minutes of inactivity. A message box will appear on screen if you are using Internet Explorer to let you know that you need to log back in. If you are using a Firefox browser you will be logged out and put back to the login screen.

Chapter 3: The SyAM Central System Management User Interface

This chapter describes how to use the SyAM Central System Management software. It also points out the enhancements made to the systems running the Local System Management software when those systems are managed centrally.

The SyAM Central System Management User Interface

SyAM Central System Management software provides administrators with the ability to manage a set of systems from a single user interface.

Interface Layout

The structure of the interface is identical whether you are using Desktop or Server Monitor Central. All of the systems being managed are represented in the tree on the left hand side. Detailed information about a specific system being accessed is presented on the main right hand side.

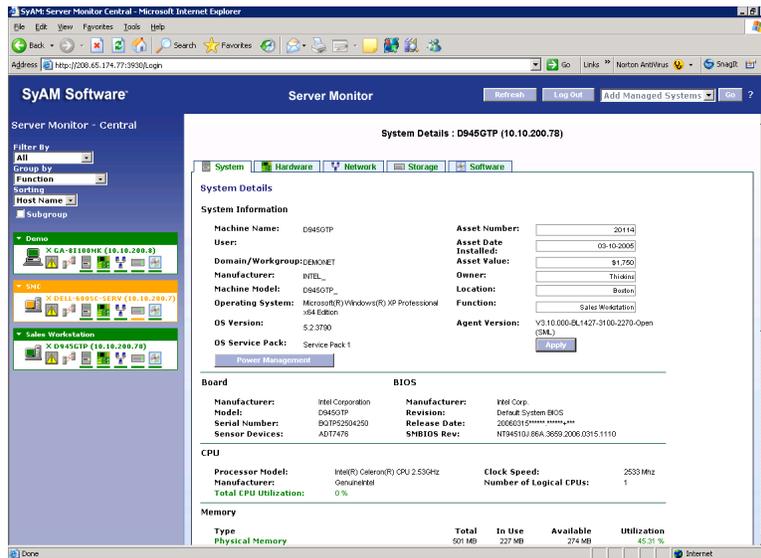


Figure 9: SyAM Central Manager User Interface Layout

Header Bar

The header bar has three function buttons – Refresh, Log out and Online Help and a Drop Down menu for the central management functions – Add Managed Systems, Welcome Page, Central Alert Matrix, Event Log, Report and License Management.



Figure 10: Header Bar

Health Colors

In order to quickly identify and correct system problems, SyAM software uses a consistent color scheme to represent the health and functionality of systems and their components. These colors can be seen in every level of monitoring, from the instance of the component to the component category and section.. The health of each monitored system is updated on a regular interval. Any change in the status of the system will cause a change in the health color. The health color will remain in the changed state until the issue is resolved.

	Green = Fully Functional
	Amber = Warning
	Red = Critical
	Grey = System state pending, currently unknown
	Purple = System is no longer responding
	Blue = Agent service has been manually shutdown
	Black = System has been shutdown
	Cyan = System has expired Central Management License Key

Figure 11: SyAM Health State Colors

Icons

There are three icons that represent the type of SyAM software running on the managed system.

Server Monitor Local/Central



Desktop Monitor Local/Central



Notebook Monitor Local



Adding Systems to the Management Tree

Systems must be added to the Management Tree before they can be managed centrally through the Server/Desktop Monitor Central software.

You can only add systems that are running SyAM software, and may only add those systems up to the limit set by your license key.

Once a system is added it will automatically unlock the Local System Management software running on that system, which will now send event messages to the Server/Desktop Monitor Central software.

To add a system or discover systems to be added to the Server/Desktop Monitor Central choose Add Managed Systems from the Drop down menu on the header bar.

1. Enter the IP Addresses in the **From** and **To** fields

To add a single system enter the same IP address in the **From** and **To** fields
To discover systems across a network address range, enter the lower IP Address in the **From** field and the higher IP address in the **To** field.

It is recommended to keep the IP address range "dense". The longest wait times occur when trying to sample IP addresses that are not in use.

2. Enter the **Location** and **Function** that is to be applied to the discovered systems (These values are used in grouping and sorting of the tree.)
3. Press the **Apply** button
4. Once discovery has been completed the **Status** will show the amount of systems successfully added

Add Managed Systems

Add Managed Systems

Add Systems to be Managed

You may add systems up to the maximums permitted by your license. Select License Management for details on licensing.

IP Address Range: **From:** **To:**

Enter the information to be used for grouping the managed systems within the tree

Location:

Function:

Status

Addition in progress, started on Sun Mar 05 12:11:00 PST 2006

Figure 12: Adding Managed Systems using an IP Address range

Add Managed Systems

Add Managed Systems

Add Systems to be Managed

You may add systems up to the maximums permitted by your license. Select License Management for details on licensing.

IP Address Range: From: To:

Enter the information to be used for grouping the managed systems within the tree

Location:

Function:

Status

Completed on Sun Mar 05 12:11:10 PST 2006, 6 systems were added.

Figure 13: Status showing 6 systems added

Changing to which Server/Desktop Monitor Central the system reports

Remove the system from the first Server/Desktop Monitor Central tree to stop the system from reporting. Once this is done, add the system to the second Server/Desktop Monitor Central tree by following the instructions "Add Managed System"

Removing Managed Systems

If you wish to remove a managed system from the Server/Desktop Monitor Central Tree:

- Click on the <X> next to the name of the system
- You will be prompted to confirm the deletion of this system

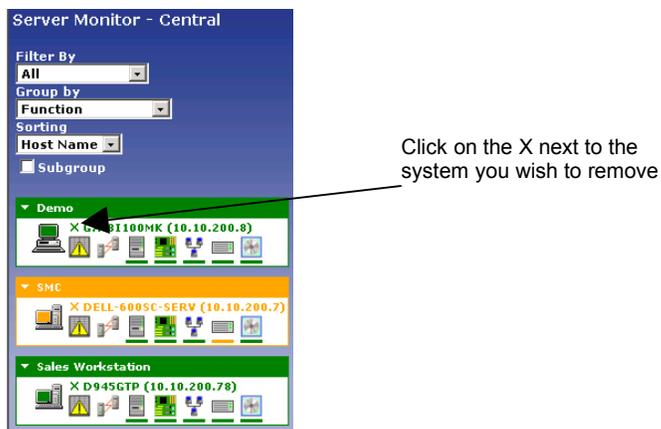


Figure 14: Removing a system from the Management Tree

Once a system has been removed from the Management Tree the Local System Management software will go back to email alerting only and will not report its events to the Server/Desktop Monitor Central.

The system you removed is still being monitored for health by the management agent on that system, which will alert via email to any issues it discovers. You may add the system back into the Central Manager tree at any time.

If you wish to completely disable this monitoring on the removed system, uninstall the software on that system.

Filter by, Grouping and Sorting Options for the Management Tree

Systems listed on the Management Tree are filtered by showing all health states and grouped by operating system and sorted by machine name by default. By using the Filter By drop down menu, administrators can choose to only show a certain health state, helping the administrator to narrow down their view to only systems with a certain health state.

By using the Group By drop down menu, administrators can choose to view groups of systems by location or by function, helping the administrator to narrow down issues in environments with large numbers of systems.

By using the Sorting drop down menu, administrators can select to view the systems within the groups by Machine Name or IP Address within the groups; this reverses the display order to IP Address/Machine name for IP sorting order and Machine Name/IP Address for Machine Name sorting order.

The administrator can modify the **Location** and **Function** fields in the System screen for each managed system. If this information has not been specified for some managed systems, the grouping function will display the systems as “Ungrouped” as the name for the location or function.

If Server, Desktops and Notebooks are being monitored the Subgroup option will be displayed.

By clicking on the Subgroup check box, the tree will be shown where the sorting within the chosen group will show the all Servers first, then Desktops and then Notebooks.

If Subgroup is not chosen then the sorting will be in the chosen order without any sub grouping of server/desktop/notebook.

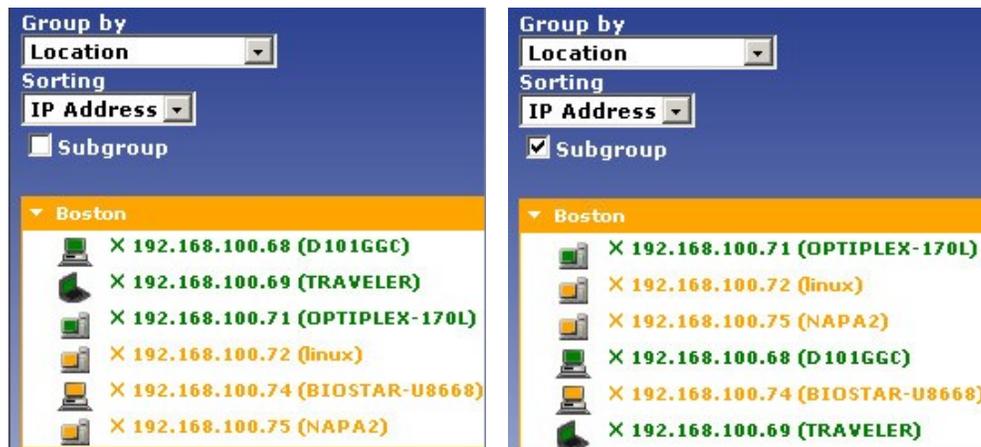


Figure 15: Systems Grouped by Location in IP Address Order shown with and without subgrouping

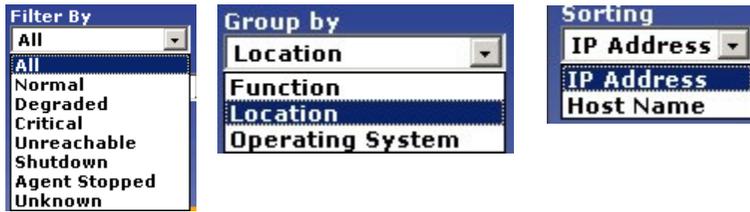


Figure 16: Management Tree Filter By, Group By and Sorting Options

The administrator can use the Filter By to choose to only show systems at a specific Health State.

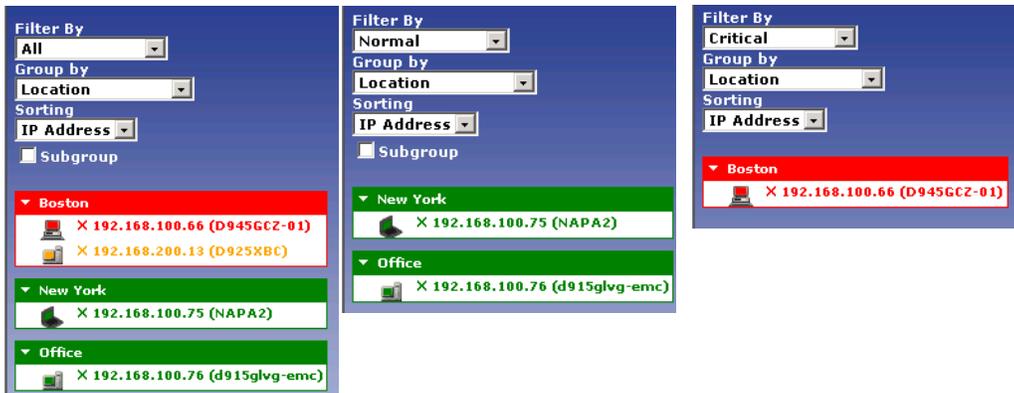


Figure 17: Examples of the Filter By Option

Expanding the Server/Desktop Monitor Central Tree

Server/Desktop Monitor Central provides administrators with an overall view of managed system, and the capability to drill down to each system and individual components.

Click on the name of the operating system, function, or location to expand the list of systems in each group. The names and IP addresses of each system will be displayed in the left hand window.

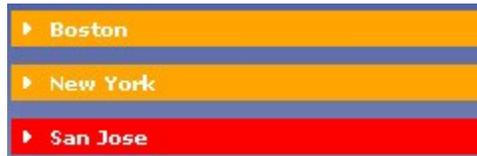


Figure 18: Management Tree – Contracted Groups



Figures 19: Management Tree – Expanded Group with contracted Systems

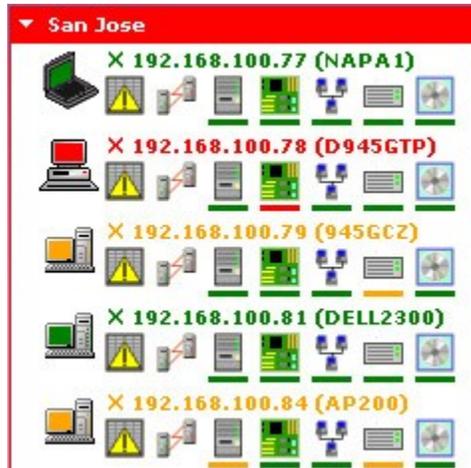


Figure 20: Management Tree – Fully expanded Group and Systems

Tree Icons

	System Alert Matrix – Provides access to the thresholds, sample, reset periods and notification options for all of the monitored hardware and software sensors within the system
	Remote Management – Provides access to the remote functions, Shutdown, Restart, Wake on LAN and Remote Console which provides the administrator full access to the remote systems keyboard, mouse and screen. IPMI – Provides access to IPMI Event log data while system is running, also provides IPMI Over LAN Power Management and Event Log access out of band (system may be powered off).
	System – Provides system board, memory, CPU, slot, display, port information and status of the CPU and Memory utilization being monitored, in addition memory error information is displayed.
	Hardware – Provides sensor information and current status on physical sensors being monitored within the system
	Network – Provides network adapter configuration information and performance for all configured adapters within the system
	Storage – Provides physical storage device, storage controller, logical device information and health status for the storage devices and managed RAID controllers.
	Software – Provides information on OS services, processes, and installed applications. Also provides remote and process management.

Chapter 4: License Management

This chapter describes how to process License Keys for continued use of Server/Desktop Monitor Central after the evaluation period has expired, and to increase in the number of systems the Central Manager can manage.

License Management

Server/Desktop Monitor Central provides the ability to manage up to 500 systems from a single user interface. The amount of systems that can be managed is controlled through a license key.

The software ships with a 15 day evaluation license that enables full central management capabilities to a limited number of systems.

Note: If the evaluation period expires, almost all of the Central Manager functions will be disabled. However you will still be able to access the License Management screen and obtain a new license key.

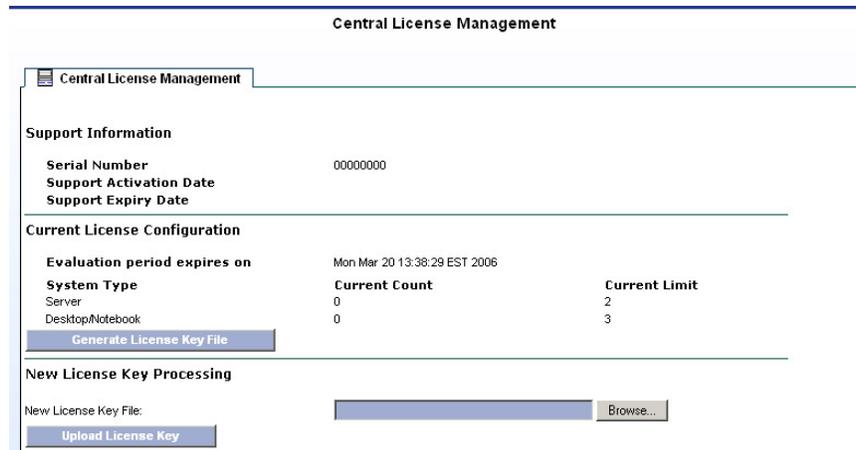


Figure 21: License Management Screen – Within Evaluation Period

To unlock the ability to manage more systems or for continued use after the evaluation period has expired a license key must be purchased.

To access the License Management Screen you choose it from the Drop Down menu on the header bar.

When purchasing a license key you must follow these steps otherwise your License Key can not be generated..

1. Generate the License Key from your Server/Desktop Monitor Central
 - a) Open up the License Management screen on the system that you wish to purchase the license key for
 - b) Click on the Generate License Key File button
2. Provide the file to your Reseller or have it available to provide online when purchasing the new license key directly from www.syamsoftware.com.
3. Provide the Reseller or enter in the www.syamsoftware.com web site the number of desktops/notebook and servers you wish to manage.
4. When your order is processed, a new License Key File is generated that contains this information.
5. Your reseller or www.syamsoftware.com will provide you with this new License Key File
6. Open up the License Management screen on the system that you are purchasing the license key for and click on the Browse button
 - a) Now browse to where you have stored the new License Key File
 - b) Once chosen click on the Upload License Key button
7. The Server/Desktop Monitor Central will process the license key File and the current limits will be increased to the limits that you purchased.

8. If this is the first time you purchased a key for this Central Manager you will be provided with a support serial number and the date when the 12 months of maintenance and support expires.
9. If you have upgraded the number of systems you are managing you will get a new serial number, and the 12 months maintenance and support will be extended out from the new License Key date.

Central License Management

Central License Management

Support Information

Serial Number	00010115
Support Activation Date	Sat Mar 04 10:13:38 PST 2006
Support Expiry Date	Sun Mar 04 10:13:38 PST 2007

Current License Configuration

System Type	Current Count	Current Limit
Server	2	25
Desktop/Notebook	2	25

New License Key Processing

New License Key File:

Figure 22: License Management Screen – With Purchased License Key

Please Note even if the Support Expiry Date has been exceeded the software will continue to work.

Chapter 5: Remote Management

This chapter describes how to use the Remote Management capabilities within the Central System Management User Interface.

Remote Management

Server/Desktop Monitor Central provides remote management functions for its managed systems, including Wake on LAN, Shutdown, Restart, Remote Console and for AMT enabled system it provides, AMT power Management, for IPMI enabled systems it provides IPMI Event Log and IPMI Over LAN for IPMI.

To access remote management; choose this option from the listed system on the Server/Desktop Monitor Central tree.

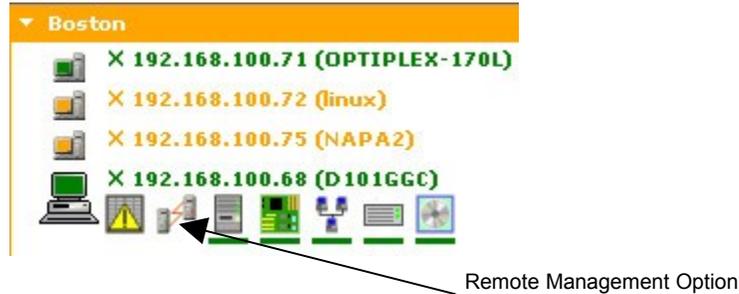


Figure 23: Remote Management Option

System State

The system state screen contains information on the current condition of the selected system, using the same health color scheme. Server/Desktop Monitor Central remote management provides Shutdown / Restart, Wake on LAN and Remote Console management options. In order to use the Shutdown, Restart, and Remote Console management options, the Local System Management software must be running.

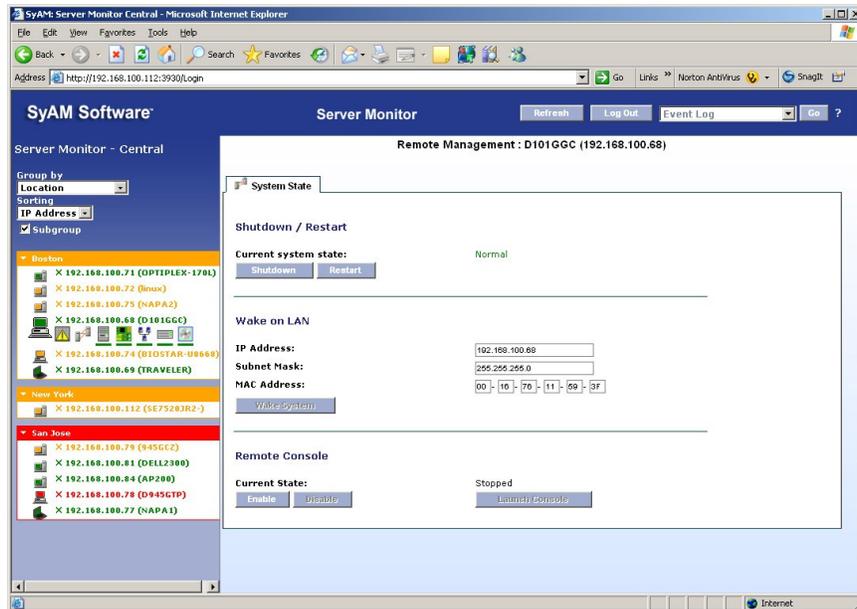


Figure 24: System Status and Wake on LAN Capabilities

To shutdown or restart the system, the system must be in Normal, Warning or Critical health states.

- To shutdown a system, click <shutdown>
- You will be prompted to confirm this action
- To restart a system, click <restart>

- You will be prompted to confirm this action

Wake on LAN

Wake on LAN capability allows central administrators to power up a WOL enabled managed system. In order for Wake on LAN to function properly, the administrator must have enabled this capability within the managed system's BIOS.

To wake a system, the system must be in the Shutdown health state.

- The IP address and MAC address of the system is automatically populated by the Server/Desktop Monitor Central.
- Click the <wake system> button to wake the system remotely

The administrator can change the MAC Address and IP Address of the network connection to be notified with the WOL command. Use this when the managed system is reporting to the Server/Desktop Monitor Central on the non WOL-enabled network adapter. Note that Server/Desktop Monitor Central will need to be able to access the WOL enabled Network adapter for this function to work.

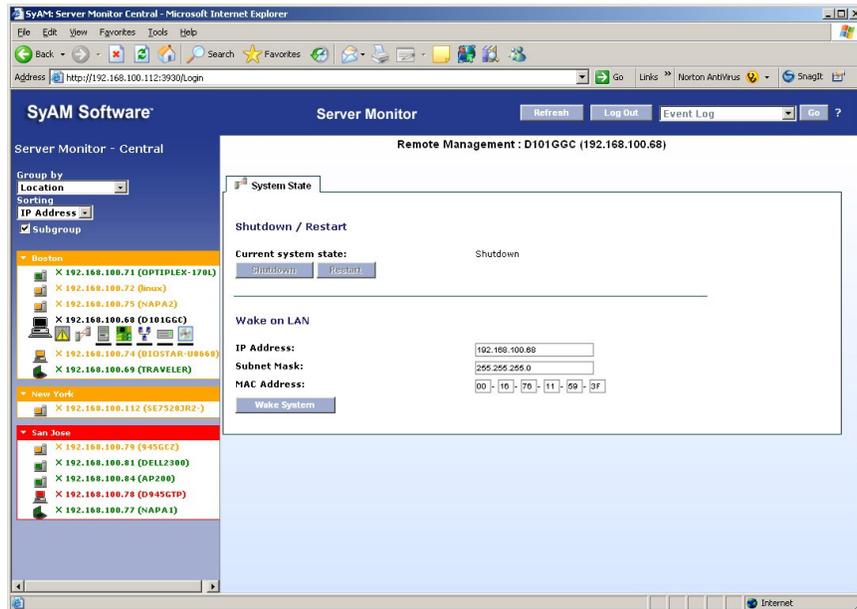


Figure 25: Wake On LAN (WOL)

Remote Console

Remote Console provides the capability of taking control of a managed systems local screen, keyboard and mouse directly through the Server/Desktop Monitor interface.

To access the Remote Console, select the system from the Management Tree, click on the Remote Management icon, which opens the remote management screen. The bottom section of the screen shows the Remote Console status and Enable/Disable and Launch Console buttons.

The status must be running if you wish to launch the console.

Click on the Enable button to start the service on the remote managed system.
Click on the Disable button to stop the service on the remote managed system.
Click on the Launch Console button to establish a remote console session.

We recommend you disable the remote console feature (which stops the software from running) after each use; however the software will automatically be stopped once the managed system is rebooted.

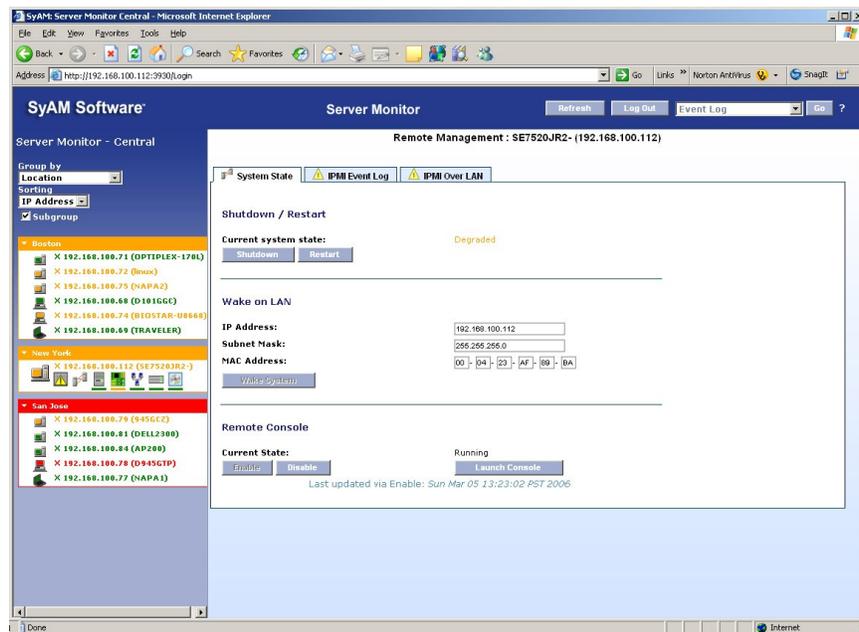


Figure 26: Remote Console Enabled and Running

Once you launch the console enter the password (Windows Default is 1234 / Linux Default is 12345678) and this console session now provides access to the remote system.



Figure 27: Remote Console Login

Now the windows represents the screen of the managed system, once finished click on Disconnect and close the window.

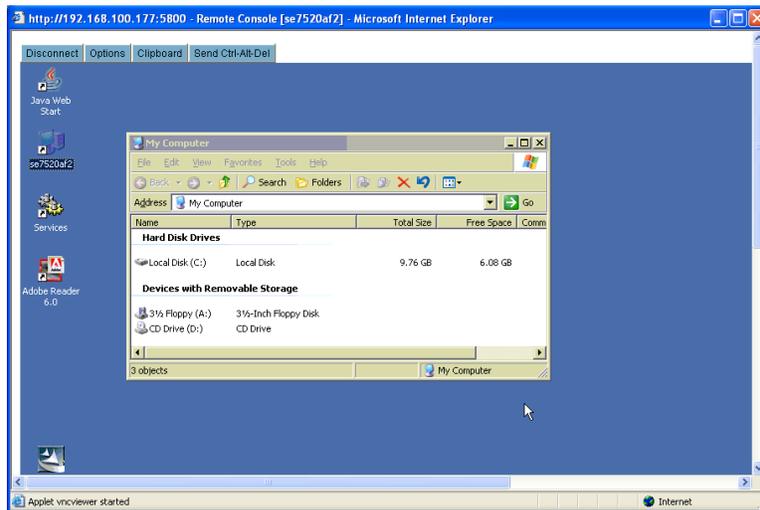


Figure 28: Remote Console – Managing a remote System

Changing the Default Password

To change the password from the default:

On Windows:

select the Remote Console Default User Settings from the SyAM Program menu on the managed system and enter the new password. Maximum number of characters for the password is 8. (You must have administrator privileges to change the password).



Figure 29: Remote Console – Changing the User Settings

However, the Remote Console service must be running on the local system.

The Remote Console service can be enabled from Server/Desktop Monitor Central by selecting the remote management options for a particular managed system or by starting the service on the local system.

To start the service on the local system execute the following.

Goto: START -> Programs -> Administrative Tools ->Computer Management> Services

Scroll down to the Remote Console and select the service.

Now, at the top of the Services menu click the start service icon.

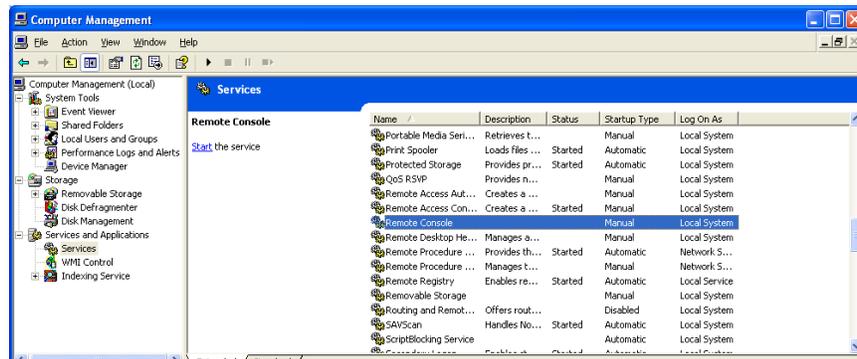


Figure 30: Remote Console – Starting the Remote Console Service

Once the Service is started, the Remote Console Default password can be changed.

On Linux:

cd to the top-level directory where the Central Manager software was installed. From there:

```
cd system_monitor/remote_console  
./vncpassword
```

You will be prompted to enter and then confirm the new password.

Using the Clipboard

To copy information from the managed system to the local Server/Desktop Monitor Central, select the information to copy and use the edit/copy command, then click on the Clipboard button at the top menu, then paste the information to the clipboard. Now select the information in the clipboard and copy/paste it into a file on the local system.



Figure 31: Remote Console – Clipboard

Ending the Remote Console Session

To end the Remote Console session, click the disconnect button at the top menu. Settings.

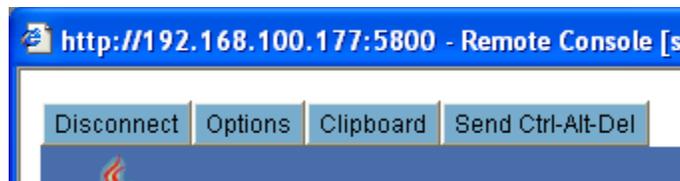


Figure 32: Remote Console – Disconnect

AMT (Intel Active Management Technology)

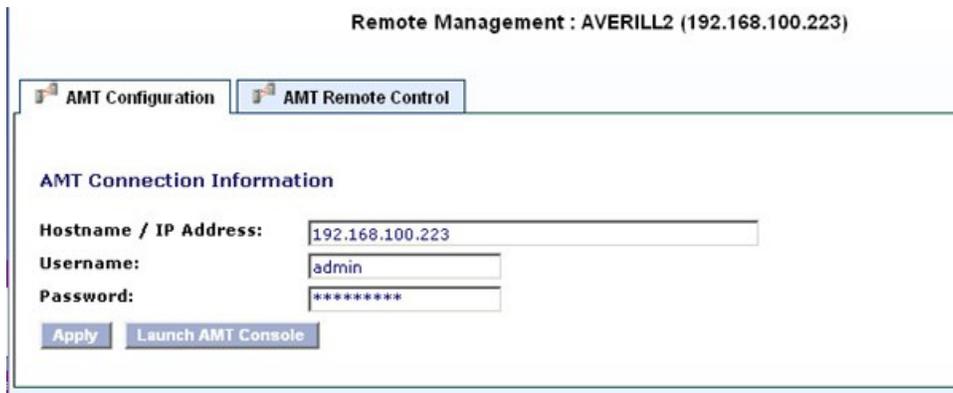
The AMT Tab will only appear if the system running the Local System Management is identified as having Intel AMT technology onboard.

Server/Desktop/Notebook Monitor can provide power management and AMT Console access when the system is in either an operating system-present or -absent state.

Please check www.syamsoftware.com for validated AMT configurations

You must first configure the AMT Port IP address and Password using the vendor provided utilities before you can utilize this AMT feature.

Enter the user name, password and IP address of the AMT port for the managed system, then click on the apply button to save this data.



Remote Management : AVERILL2 (192.168.100.223)

AMT Configuration | AMT Remote Control

AMT Connection Information

Hostname / IP Address: 192.168.100.223

Username: admin

Password: *****

Apply Launch AMT Console

Figure 33: AMT Login Tab

Click on Launch AMT Console to open up a new browser window and login directly into the embedded AMT web server.

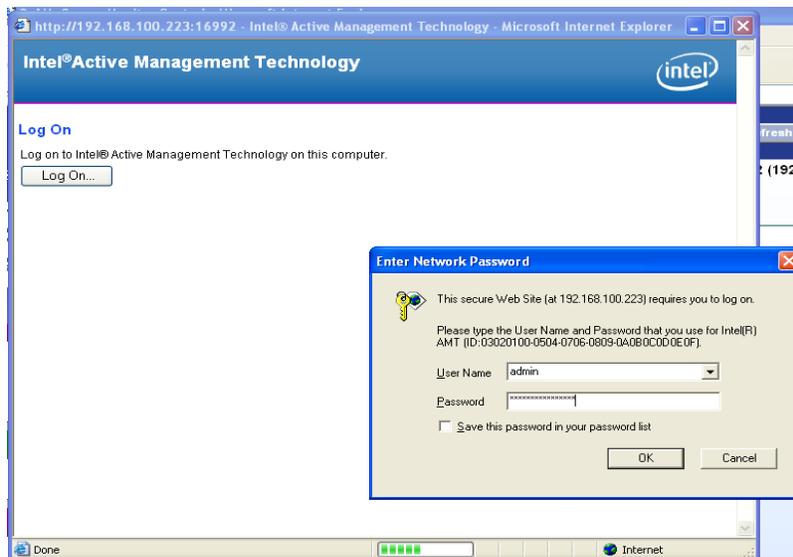


Figure 34: Launching the AMT Console

Once you have saved the User name, password and IP Address you can click on the Establish AMT Connection button under the AMT Remote Control Tab to access the managed system's AMT over the LAN.

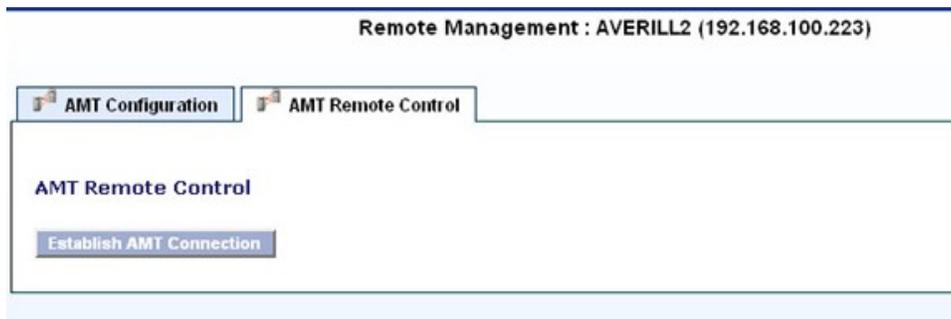


Figure 35: Establish AMT Connection

Once connected you can perform the following power options.

Power Off

This will perform a forced power off not a graceful shutdown.

Power On

This will perform a forced power on.

Power Reset

This will perform a power reset not a graceful reset.

Power Cycle Reset

This will perform a power cycle reset.

Serial Over LAN enables a user to remotely reboot a system. When a user reboots with SOL enabled, the SOL session is presented in the user's browser.

In order to create an SOL session, the user must verify the current power status.

Next, click the 'Launch SOL Session' box, and then click on the 'Send Command Button'.

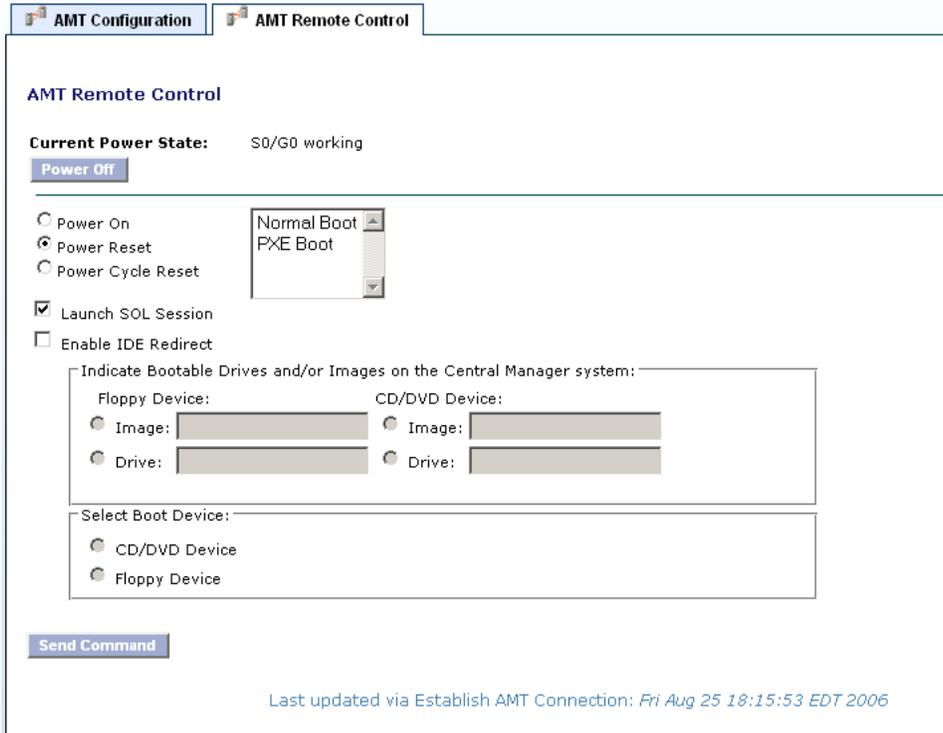


Figure 36: AMT Remote Control

Please Note: When using an SOL session, you are only able to boot the system normally. You cannot specify special commands such as PXE.

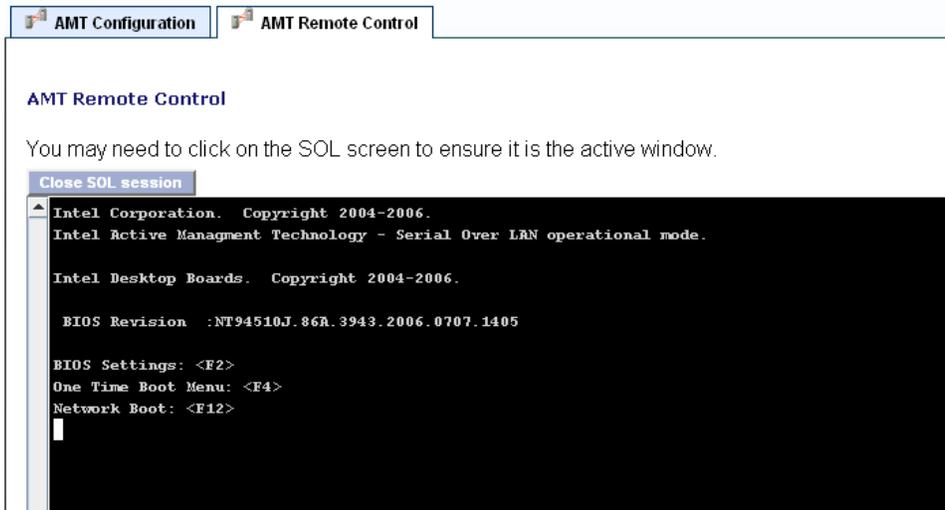


Figure 37: Serial Over LAN (In Use showing BIOS Re-configuration)

IDE-Redirect allows an AMT managed system on the Central Management tree to boot from an image, floppy, CD or DVD device which is located in the system running Server Monitor or Desktop Monitor Central. IDE-Redirect is only available when using SOL. Part of the AMT IDE Redirect process is verifying a valid image or device. If you do not have a physical floppy device you must chose the image as the Floppy Device. Both a floppy drive or image, AND a CD/DVD drive or image, must be specified. These drives or images are on the computer running Server/Desktop Monitor Central, NOT on the computer running your web browser.

To invoke the IDE Redirect either click on the Power Reset or Power On buttons and click in the SOL and IDE-R check boxes. Under image or drive, indicate which image or drive you want the system to boot from, then select the boot device, and click 'Send Command'.

Remote Management : D945GCZ-22 (10.10.200.69)

AMT Configuration **AMT Remote Control**

AMT Remote Control

Current Power State: S0/G0 working

Power Off

Power On Normal Boot
 Power Reset PXE Boot
 Power Cycle Reset

Launch SOL Session
 Enable IDE Redirect

Indicate Bootable Drives and/or Images on the Central Manager system:

Floppy Device: <input type="radio"/> Image: <input type="text"/> <input checked="" type="radio"/> Drive: <input type="text" value="a:"/>	CD/DVD Device: <input type="radio"/> Image: <input type="text"/> <input checked="" type="radio"/> Drive: <input type="text" value="d:"/>
--	--

Select Boot Device:

CD/DVD Device
 Floppy Device

Send Command

Figure 38: IDE-R (Configured to boot off CD-Rom)

When using either a Windows or Linux Server / Desktop Monitor Central you need to use the correct corresponding Windows or Linux syntax for the Floppy disk device and CD ROM device.

If you are unsure of what the logical letter of the CD ROM device is, browse to the Storage screen of the Central Manager.

If no floppy disk drive is present then you must select the bootable image.

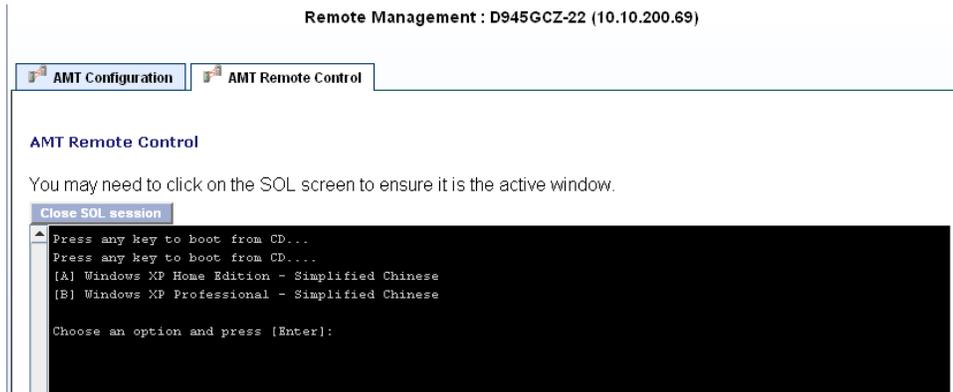


Figure 39: IDE-R (In Use showing remote boot off CD-Rom)

Examples of IDE-R Drive and Image Syntax

Server/Desktop Monitor Central running on a Windows Operating System

Floppy Device Drive **a:**

Floppy Device Image **c:\win98dos.img** or **c:\win98doscd.iso**

CD Rom Device Drive **d:**

CD Rom Device Image **c:\win98doscd.iso**

Server/Desktop Monitor Central running on a Linux Operating System

Floppy Device Drive **/dev/fd0**

CD Rom Device Drive **/dev/hda**

System Defense allows the Central Manager to define and enforce network security policies.

After clicking on the AMT System Defense tab, you will need to establish a connection with the AMT machine by clicking on the Establish AMT Connection button.

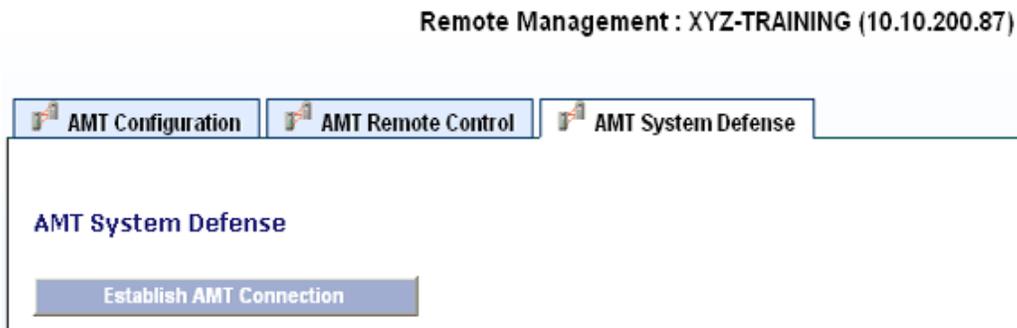


Figure 40: AMT System Defense (Establish AMT Connection)

When you first access the system defense screen, any policies that have been configured in the AMT Management Engine are presented.

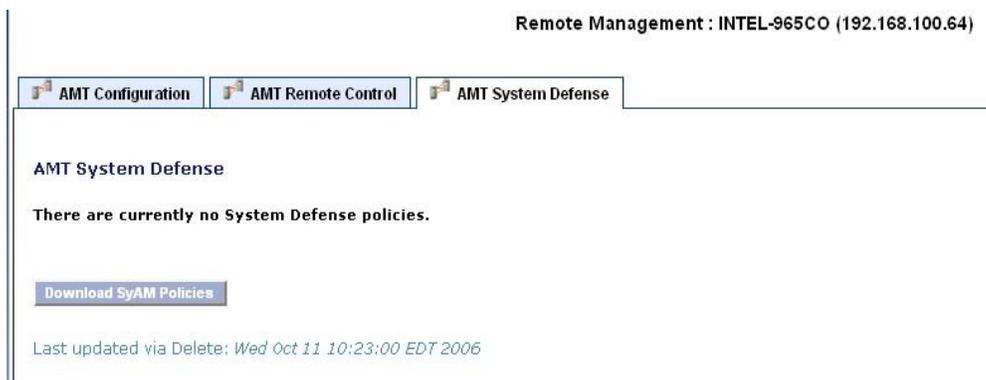


Figure 41: Download SyAM Policies

If the SyAM-Quarantine and the SyAM-Management Policies are not programmed into the AMT Management Engine you will be presented with a download button. This will allow the SyAM Policies to be configured in the AMT Management Engine.

The Screen will refresh automatically and then the two SyAM-Management Policies policies will appear on the screen.

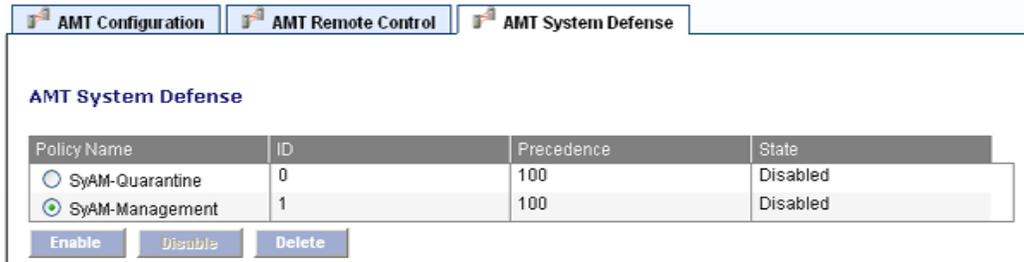


Figure 42: AMT System Defense Policies

Initially the three buttons enable, disable and delete are not available. Once you select a Policy, the Enable and Delete buttons become available. This allows you to enable a policy or remove the policy from the AMT Management Engine.

Once a policy is enabled, its status changes to active so you can see which policy is currently active. Only one policy may be enabled at a time.

When the currently active Policy is selected the Disable and Delete buttons become available. This allow the policy to be disabled or removed from the AMT Management Engine.

The “SyAM-Quarantine” policy causes the Intel AMT device to block all packets to/from the operating system running on the client. So the administrator would have to go to the system to troubleshoot or repair the system.

The “SyAM-Management” policy causes the Intel AMT device to block all packets to/from the operating system running on the client, except those sent to and from SyAM’s management components.

This allows the Administrator to access the Intel AMT client system using SyAM Server/Desktop Monitor remote console capability while the operating system is running, in order to inspect or repair the system, but without providing general access to/from the system.

IPMI Event Log

Server Monitor can monitor physical events occurring on IPMI-enabled servers that are being managed. These events are recorded in the IPMI Event Log, which is accessible through Server Monitor Central. Each event is given a unique number and dated. This information, as well as a description of the event type, sensor type affected, and event alert type are recorded in the IPMI Event Log.

In addition, the IPMI event log lists the version of the log, the number of entries in the log, the last time an entry was added, the last time the log was cleared, and the free space remaining for the log.

The log can be reviewed/filtered by listing all events, or by filtering by an event range. The results can be displayed on the screen or exported to a file in a .CSV format without clearing the log.

The IPMI Event Log allows administrators to retrieve and view all events occurring and reported by a specific server. In order to access the IPMI Event Log, the system must be IPMI-enabled and running a valid version of Server Monitor Agent.

Fields included in this screen are:

- IPMI Version
- Number of entries in the log
- Last time an entry was made in the log
- Time of last log clear
- Free space

The screenshot shows the SyAM Server Monitor Central interface. The main content area displays the IPMI Event Log for server SET7520JR2- (192.168.100.112). The summary statistics are as follows:

IPMI version	02.00
Number of entries in log	216
Time of last log entry	Mar 4, 2006 2:29:21 AM
Time of last log clear	Feb 21, 2006 1:19:34 AM
Free space remaining for log entries	61212 kb

Below the summary, there are filtering options and a table of event log entries.

Event Log Filtering Options:

- Event ID Range: [] To []
- Buttons: Retrieve Events, Generate CSV

ID	Timestamp	Sensor Type	Description	Event Type
4	Feb 21, 2006 1:19:34 AM	Event Log Disabled	(09) Logging Disabled	Asserted: Discrete/Sensor Type-Specific
24	Feb 21, 2006 1:24:41 AM	System Event	(B3) System Event	Asserted: Discrete/Sensor Type-Specific
44	Feb 21, 2006 1:24:43 AM	Drive Slot	(0B)	Asserted: State Deasserted
64	Feb 21, 2006 1:24:48 AM	Drive Slot	(0C)	Asserted: State Deasserted
84	Feb 21, 2006 1:24:53 AM	Drive Slot	(0D)	Asserted: State Deasserted

Figure 43: IPMI Event Log

The IPMI Event Log provides administrators with the option to clear or purge the log, by clicking the <clear> button. Note: this action cannot be undone.

IPMI Event Retrieval

The IPMI Event Log provides administrators with the option of retrieving and viewing some or all events recorded for the server, and sorting them by type.

To retrieve all of the events from the IPMI event log stored on the BMC, click on the radio button next to "All".

To retrieve a subset of events, enter a beginning and ending Event ID. The beginning Event ID value must be either 0 (to retrieve from the beginning of the log), or an actual Event ID number. You will receive an error message if a non-0 Event ID cannot be found.

Then click on the Retrieve button. The results will be displayed in the detail window at the bottom of the screen.

Event Log Filtering Options

All

Event ID Range To

ID	Timestamp	Sensor Type	Description	Event Type
24	Dec 31, 2004 6:38:06 AM	Session Audit	(0A) Session Audit	Asserted: Discrete/Sensor Type-Specific
44	Dec 31, 2004 6:38:14 AM	Session Audit	(0A) Session Audit	Asserted: Discrete/Sensor Type-Specific
64	Dec 31, 2004 6:39:06 AM	Session Audit	(0A) Session Audit	Asserted: Discrete/Sensor Type-Specific
84	Dec 31, 2004 6:44:42 AM	System Event	(83) System Event	Asserted: Discrete/Sensor Type-Specific

Last updated via Retrieve Events: Fri Jan 07 09:57:03 EST 2005

Figure 44: IPMI Event Log Retrieval

The ID values assigned to events are generated by the IPMI controller, and are dependent on how the system's firmware has been configured. As a result, the Event ID may differ by server platform.

Generate CSV

This button retrieves the events and saves them to a CSV file.

IPMI Over LAN

Server Monitor can provide IPMI Over LAN power management and event log capabilities when the system is in either a operating system-present or -absent state.

You must first configure the BMC's IP address and Password using the vendor provided utilities before you can utilize this IPMI Over LAN feature.

Enter the user name, password and IP address of the BMC for the managed system, then click on the apply button to save this data.

Remote Management : SE7520JR2- (192.168.100.112)

System State | IPMI Event Log | IPMI Over LAN

IPMI Over LAN Chassis Options

IPMI Over LAN Status: Not Connected

Username:

Password:

IP Address:

Apply Connect

Power Off
Power On
Power Reset
Identify

Figure 45: IPMI Over LAN – Enter details for accessing the BMC

Remote Management : SE7520JR2- (192.168.100.112)

System State | IPMI Event Log | IPMI Over LAN

IPMI Over LAN Chassis Options

IPMI Over LAN Status: Not Connected

Username:

Password:

IP Address:

Apply Connect

Power Off
Power On
Power Reset
Identify

Figure 46: IPMI Over LAN – Details applied

Once you have saved the User name, password and IP Address you can click on the Connect button to access the managed system's BMC over the LAN.

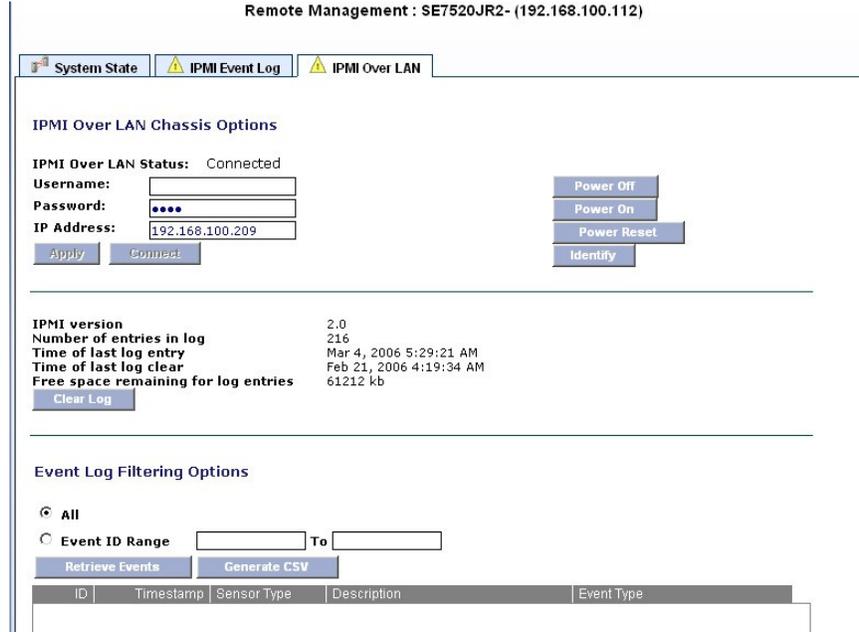


Figure 47: IPMI Over LAN – Connected

Once connected you can perform the following options.

Power Off

This will perform a forced power off not a graceful shutdown. **The operating system may or may not receive notification and shut down, this varies by hardware platform.**

Power On

This will perform a forced power on.

Power Reset

This will perform a power reset not a graceful reset. **The operating system may or may not receive notification and shut down, this varies by hardware platform.**

Identify

This will light the identification LED of the system. This feature is not supported in all hardware platforms.

Event Log

The IPMI Event Log is accessed in exactly the same manner described above.

Chapter 6: Central Event Logging

This chapter provides instruction on how to access the Central System Management Software's centralized event logging facility.

Administrators can use the SyAM event log to quickly identify trends across system events.

Central Event Logging

All systems being managed by Server/Desktop Monitor Central (are present in the Management Tree) have their events automatically recorded in the Central Manager Event Log. Each event is given a unique identification number and dated, and lists the location of the event by system name, IP address, and category (storage, network, hardware, etc.)

Below the main event screen is a detail screen which provides information on the event.

You can sort the event log by clicking on the chosen column heading; this can be in ascending or descending order.

Filtering Options

The Server/Desktop Monitor Central Event Log advanced filtering options allow administrators to sort the log by event log number ranges, machine name, IP address, and event type. Results are displayed in the main Event Log window, and can be exported to another application.

To filter the Event Log by Event Number:

- Enter the beginning and ending range for the events in the appropriate field
- Click on the "Retrieve" button
- Matching events within the range will be displayed in the main events window

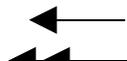
To filter the Event Log by Machine Name or IP Address:

- Enter the machine name or IP address in the appropriate field
- Click on the "Retrieve" button
- Matching events for that IP address or system name will be displayed in the main events window

To filter the Event Log by Event Type:

- Select the event type from the Drop Down menu
 - All
 - Platform Event Trap
 - Hardware Event
 - Network Event
 - Storage Event
 - Performance Utilization Event
 - Asset Monitoring Event
 - System Absent
- Click on the "Retrieve" button
- Matching events of the type selected will be displayed in the main events window

To narrow the search, complete the appropriate fields to filter the Event Log by more than category.



Event Log

Event Log

Event Number	Date	Event Type	IP Address	Machine Name
190	Sun Mar 05 11:38:14 PST 2006	System Absent	192.168.100.74	BIOSTAR-U8668
189	Sun Mar 05 11:38:14 PST 2006	System Absent	192.168.100.68	D101GGC
180	Sat Mar 04 17:31:20 PST 2006	Hardware Events	192.168.100.78	D945GTP
165	Sat Mar 04 15:36:46 PST 2006	Storage Events	192.168.100.72	linux
162	Sat Mar 04 15:32:49 PST 2006	Hardware Events	192.168.100.74	BIOSTAR-U8668
161	Sat Mar 04 15:31:44 PST 2006	Hardware Events	192.168.100.74	BIOSTAR-U8668
154	Sat Mar 04 13:21:25 PST 2006	Hardware Events	192.168.100.112	SE7520JR2-
143	Sat Mar 04 12:34:46 PST 2006	Storage Events	192.168.200.12	GA-7VT600
140	Sat Mar 04 12:25:11 PST 2006	Performance Utilization Events	192.168.200.12	GA-7VT600

Details

BIOSTAR-U8668 (192.168.100.74) Sun Mar 05 11:38:14 PST 2006: Is unreachable

Event Log Filtering Options

Event Number - Event Type

Machine Name IP Address

Figure 48: Event Log

Exporting Event Log Ranges

The resulting filtered events can be exported to another program, where they can be archived or printed. After making filtering selections, click the “Export” button to export the resulting events as a Comma Separated Values (CSV) file, which can be opened in Microsoft Excel.

Deleting Event Log Ranges

Filtered or selected ranges of events can be deleted from the log. After making filtering selections, click the “Delete” button to delete the resulting events. This operation cannot be undone.

Chapter 7: Central Reporting

This chapter provides instruction on how to access the reporting capabilities within the Central System Management Software.

Administrators can quickly and efficiently produce summary or detailed reports on their Server, Desktop and Notebook assets.

Reporting

Through the Server/Desktop Monitor Central software, administrators can run summary and detailed reports on the managed systems that it monitors, view it on screen, and print or export to file in CSV or XML format. You can choose to report on a single managed system, a group of systems, or all of the managed systems.

Administrators are given the option of sorting the report by Machine name or IP address.

Report

Report

Report On
 Group Location Boston
 Single System

Sorting Report Type
 Host Name Summary
 IP Address Detailed

Figure 49: Central Manager Reports

Managed System Summary Report

The managed system summary report will contain the following information:

- Machine Name
- Health State
- IP Address
- Operating System Version / Service Pack
- Location
- Function
- Asset Number / Value / Date Installed / Owner
- Number of Logical CPU's and type
- Total amount of Physical and Virtual Memory installed and number of Memory banks used
- Number of Logical Disks and capacity available
- RAID Controllers installed
- Number of Installed Applications

Managed System Detailed Report

The managed system detailed report will contain the fields from the summary report, as well as the following additional information:

- Machine Model / Manufacturer
- Board Model / Manufacturer
- Sensor Devices Discovered
- Display Adapter Model/Memory
- Monitor Name / Serial Number
- Total amount of Memory installed
- Individual Memory Bank Label and Capacity
- Virtual and Physical Total Memory and Memory in Use
- Total Physical Disk capacity
- Physical disk Size / Device Information
- Individual Physical disk Label and Capacity
- Logical drive – Letter – Available and Total Capacity
- RAID Controller Model / Status / RAID Level / Capacity / # Drives
- Removable Device Name / Description
- Network Adapter Number / Description / DHCP / IP Address / MAC Address
- PCI Slot Label and Status
- Applications Installed – Name / Vendor / Version

http://192.168.100.112:3930 - Report - Microsoft Internet Explorer

Print Close Window

Machine Name: SE7520JR2 | System State: Degraded

IP Address	192.168.100.112
Operating System	Microsoft(R) Windows(R) Server 2003, Standard Edition
OS Version	5.2.3790
OS Service Pack	
Location	New York
Function	Email Server
Asset Number	AST-1234-43
Asset Value	2750.00
Asset Date Installed	1/15/2006
Owner	IT
Machine Model	SJR2A084
Manufacturer	Intel
Number of Logical CPUs	2
Processor Model	Intel(R) Xeon(TM) CPU 2.80GHz
Number of Memory Banks Used	2
Physical Memory	1024 MB
Virtual Memory	3.41 GB
Number of Logical Drives	1
Total Disk Capacity Available	12.77 GB
RAID Controller Model	3Ware
Installed Applications	2

Done Internet

http://192.168.100.112:3930 - Report - Microsoft Internet Explorer

Print Close Window

Machine Name: SE7520JR2 | System State: Degraded

IP Address	192.168.100.112
Operating System	Microsoft(R) Windows(R) Server 2003, Standard Edition
OS Version	5.2.3790
OS Service Pack	
Location	New York
Function	Email Server
Asset Number	AST-1234-43
Asset Value	2750.00
Asset Date Installed	1/15/2006
Owner	IT
Machine Model	SJR2A084
Manufacturer	Intel

Board	
Number of Logical CPUs	2
Processor Model	Intel(R) Xeon(TM) CPU 2.80GHz
Model	SE7520JR23D
Manufacturer	Intel
Sensor Devices	Device ID 20 Rev 01 FW Rev 00.48

Display Adapter	
Model	RAGE XL PCI Family (Microsoft Corporation)
Memory	8

Monitor Name	
Monitor Serial Number	

Memory		
Location	Size (MB)	Label
DIMM 1A	512 MB	BANK 1 (#2465338423)
DIMM 1B	512 MB	BANK 1 (#4045676137)
Total		In Use
Physical Memory	1024 MB	232 MB
Virtual Memory	3.41 GB	371 MB

Physical Disks		
Device ID	Total Size	Device Information
\\PHYSICALDRIVE0	74.53 GB	ST380817AS (#5MRGH1N0)
\\PHYSICALDRIVE1	37.27 GB	3ware (#)
Total	111.79 GB	

Done Internet

Figure 50: Summary and Detailed Reports

Chapter 8: Configuring System and Central Alerts

SyAM Central System Management software provides the ability to configure alerts at individual system and central levels.

By using Central System Management users may configure thresholds, and sample/reset periods for each monitored resource. And several new notification methods become available, such as via SNMP Traps or Operating System Event Logs.

System Alert Matrix – System Level Alerting

The System Alert Matrix provides a detailed, color-coded view of the status of all monitored components in a specific managed system.

Settings such as notification methods, thresholds, sample periods, etc for each sensor type category are automatically applied to all discovered sensor instances of that type.

Alerts : Desktop Monitor Local : XEON (192.168.100.78)

System Alert Matrix

Physical Sensors	Lower Threshold		Upper Threshold		Warning Alerts						Critical Alerts							
	Description	Critical	Warning	Current	Warning	Critical	Email /Pager	SMS	DMC	Network Message	SNMP Trap	System Event Log	Email /Pager	SMS	DMC	Network Message	SNMP Trap	System Event Log
Physical Security																		
Fans (RPM)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				
Temperature (°C)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				
Voltagess (v)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				
Restore Physical Sensor Thresholds																		
Logical Sensors																		
Description	Current		Threshold		Alerts						Intervals							
					Email /Pager	SMS	DMC	Network Message	SNMP Trap	System Event Log	Sample Period	Reset Period						
Network Adapters																		
Physical Disks																		
Logical Disks			90		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	8 Hr	180 Hr						
CPU Utilization (%)			90		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	4 Min	15 Min						
Memory Utilization (%)			90		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	4 Min	15 Min						
Notification Settings																		
Email Address	<input type="text" value="admin@syamssoftware.com"/>						<input type="text" value="admin@company.com"/>											
SMS/Pager Address	<input type="text"/>																	
Network Message Machine Name	<input type="text" value="XEON"/>						<input type="text" value="192.168.1.1"/>											
DHC System	<input type="text" value="192.168.200.13"/>						<input type="text" value="192.168.1.1"/>											
Username	<input type="text" value="usernam"/>						<input type="text" value="Username"/>											
Sender's Email Address	<input type="text" value="admin@syamssoftware.com"/>						<input type="text" value="Local.Admin@company.com"/>											
Sender's Email Password	<input type="password" value="*****"/>																	
Mail Server	<input type="text" value="mailserver.syamssoftware.com"/>						<input type="text" value="smtp.company.com"/>											
SNMP Trap Receiver	<input type="text" value="snmp.company.com"/>																	
<input type="button" value="Reset Form"/> <input type="button" value="Test Notifications"/> <input type="button" value="Apply"/>																		
Last updated via Apply: Tue Feb 14 15:50:43 EST 2006																		

Figure 51: System Alert Matrix

Monitored Sensor Types

Physical Sensors

	Security – If/when the system chassis is opened, the intrusion will trigger a sensor alert, provided that the connected board/BIOS support this information reporting.
	Fans – Monitored for rotational speed provided the fan is connected to a board/BIOS that supports the information reporting.
	Voltages – Monitored for the functionality that the connected board/BIOS supports.
	Temperature – Monitored for the functionality that the connected board/BIOS supports.
	Redundant Power Loss – Monitors IPMI managed servers and alerts upon when redundant power systems loose their redundancy

Logical Sensors

	Network Adapters – Monitors Ethernet operational state.
	Physical Disk – Monitors the presence and percent usage of a physical disk in the system and/or a RAID Set available to the operating system through a RAID controller.
	Logical Disks – The percent of capacity used by the logical disk formatted and mounted by the operating system is reported. If the disk has not been formatted, it will be reported as a failed disk. Removable Device – Removable devices that are represented to the operating system will be reported as mounted as long as they are present in the system.
	Managed RAID Controller – RAID Controller health.
	Total CPU utilization – Percentage of CPU usage.
	Total Memory utilization – Percentage of Physical and Virtual Memory usage.
	Memory Error Rate – Number of Single- and Multi- Bit errors that have occurred (requires ECC memory and support by the server board)

Notification Settings

When a system is managed from the Server/Desktop Monitor Central, it enables users to modify any of the thresholds, sample periods, reset periods, and notification methods. It also enables alerts to be sent via the other notification methods such as SMS/pager, Network Message, send to the SyAM Central Manager (for it to perform central alerting methods), SNMP Trap, or write the event to the System Event Log. (Note this System Event Log means events will be written to the local Windows Event Log or Linux syslog.) Clicking on each sensor category tree expands it to reveal all instances in the category. To select an entire category of sensors for the alert, click on the bolded category header. To select individual instances, click on the appropriate boxes for each instance.

Physical Sensors

Description	Lower Threshold			Upper Threshold			Warning Alerts					Critical Alerts				
	Critical	Warning	Current	Warning	Critical	Email/SMS/Pager	SMC Message	Network Message	SNMP Trap	System Event Log	Email/SMS/Pager	SMC Message	Network Message	SNMP Trap	System Event Log	
Physical Security	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					
Fans (RPM)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					
Temperature (°C)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					
Baseboard Temp	5	10	26.0°C	60	80	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
FanPnl Amb Temp	0	5	24.0°C	44	48	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
CPU 1 Temp	5	10	36.0°C	70	88	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Voltages (v)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>					

Notification at the Category Level Notification at the Individual Sensor Instance Level

Figure 52: Setting Category and Instance-Level Notifications

Each sensor category provides the default notification options, thresholds, sample periods and reset periods that will automatically be applied to newly discovered sensor instances within that category.

Disabling Notifications

If you wish to disable notifications for a specific sensor or sensor category you can by clicking on the No Monitoring check box.

This disables the sensor instance or sensor category from having any alerts notified, thus they will not be monitored or be represented in the health state of that sensor category, section the system or systems health.

Physical Sensor Upper and Lower Thresholds

Each physical sensor instance has its own range of safe operating values with lower and upper warning and critical thresholds. These values are discovered if the hardware platform supports that information, or are calculated from available data.

Physical Sensor Warning and Critical Alerts

Since physical sensors may enter warning or critical health states, separate alerting methods may be configured for each.

Logical Sensor Thresholds

Monitored resources that are not physical sensors are called "Logical Sensors". Each instance of the logical sensor types Logical Disk, CPU Utilization, and Memory Utilization, has a utilization threshold.

Logical Sensor Warning Alerts

Logical sensors, by design, may enter the warning health state but not critical. So there is only a single set of alerting methods available.

Sample Period

CPU and Memory Utilization are gathered several times over a period of time, so that transient spikes are not reported. This time period is configurable by the administrator, and is known as the sample period. The pre-set sample period options are from 4-8 minutes. If 80% of the gathered readings exceed the threshold, a transition to warning state occurs.

The sample period for an instance of Logical Disk that is a removable device (floppy or CD-ROM drive) is similar to that of other sensors. A set of four readings is gathered during the sample period. If the device (floppy disk or CD) is present through all of them, a transition to warning state occurs.

Reset Period

When a logical sensor transitions to a warning health state, an event is raised and alerts are sent according to the Warning Alerts settings. The reset period is the amount of time during which no additional alerts will be issued after the initial alert.

Removing a Sensor Instance From the System Alert Matrix

When a sensor instance, such as a specific logical or physical disk, has been removed from the system, or has otherwise entered a critical state, it is displayed in red and an "X" appears next to it. Click on the "X" to permanently delete this sensor instance from the alert matrix. Only do this if the instance is not being replaced. Once the sensor has been replaced it will automatically be monitored and the new health state will be represented.

Notification Settings – Configuring email alerting

Notification Settings

Email Address	<input type="text" value="admin@syamssoftware.com"/>
SMS/Pager Address	<input type="text"/>
Network Message Machine Name	<input type="text" value="XEON"/>
DMC System	<input type="text" value="192.168.200.13"/>
Username	<input type="text" value="username"/>
Sender's Email Address	<input type="text" value="admin@syamssoftware.com"/>
Sender's Email Password	<input type="password" value="••••••"/>
Mail Server	<input type="text" value="mailserver.syamssoftware.com"/>
SNMP Trap Receiver	<input type="text"/>

Figure 53: Entering Notification Information

Enter the destination email address, the sender's email address, and the mail server hostname or IP address. Enter the user name and password if outgoing email is authenticated. Click the Apply button to save changes. Use the Test Notification button to send a test email, and ensure your configuration is correct.

Central Alert Matrix

The Central Alert Matrix is accessed from the Drop down menu on the header bar . It provides the ability to configure the appropriate notification options for events that are sent to this Central Manager, from all of the systems it is managing.

Notifications can be configured to be sent via email, SMS/Pager and can be assigned to administrator one or two for each type of event, in addition to sending SNMP Traps.

Types of monitored events

	<p>Platform Event Traps PET's – PET 1.0 formatted SNMP traps received are converted to plain text and alerted upon.</p>
	<p>Hardware Events – When a threshold is exceeded by a physical component within the system. Hardware Events include: physical chassis security, fan speed variation, chassis temperature fluctuation, voltage fluctuation or power redundancy loss</p>
	<p>Network Events – Network connectivity is lost due to an adapter failure.</p>
	<p>Storage Events – A logical disk has reached its utilization threshold, a logical or physical disk is lost (removed or not functioning), or a removable disk has remained present on the system for an extended period of time and may cause boot up issues.</p>
	<p>Performance Utilization Events – CPU or memory utilization threshold has been exceeded.</p>
	<p>Asset Monitoring Events – Server Monitor records an inventory of the system components being monitored (i.e. CPUs, Memory, Disks, Software applications installed or removed, etc), and compares it each time the system is booted. Any discrepancy in the information when the agent is started is reported as an asset-monitoring event.</p>
	<p>System Absent Events – When the Server/Desktop Monitor Central is no longer able to communicate with a managed system, it is reported as being absent, unless it was correctly shutdown.</p>

Alerts : Server Monitor Central

Central Alert Matrix

Event Category	Email #1 SMS/Pager #1	Email #2 SMS/Pager #2	SNMP Trap
Platform Event Traps	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Hardware Events	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Network Events	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Storage Events	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Performance Utilization Events	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Asset Monitoring Events	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
System Absent	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Click to choose notification method

Example

Email Address #1 for Alerts:

SMS/Pager Address #1 for Alerts:

Email Address #2 for Alerts:

SMS/Pager Address #2 for Alerts:

Username:

Sender's Email Address:

Sender's Email Password:

Mail Server:

SNMP Trap Receiver:

Enter administrator contact information, SMC as the sender information, and email server information

Figure 54: Central Alert Matrix

SyAM Integration into Enterprise Frameworks

System Area Management (SyAM) MIB

The SyAM MIB must be installed into the Enterprise Framework server before it can decipher traps sent from a managed system.

Please consult your Enterprise Framework application on how to install a 3rd party MIB.

The MIB file is installed in <Installed Directory>/system_monitor/syam.mib.

System Area Management (SyAM) Integration into Microsoft Operations Manager (MOM)

The SyAM Management Pack for Microsoft Operations Manager must be loaded into the MOM server, before it can decipher Windows events written by SyAM Management Agents. Also the MOM agent must be configured on each managed system to forward events to the MOM server.

Please consult your MOM documentation on how to load 3rd party Management Packs into the MOM server, and how to configure the MOM agent.

The MOM Management Pack file is installed in:
<InstalledDirectory>/system_monitor/syam.akm.

Chapter 9: Accessing System Information

This chapter provides instruction on how to access a managed system to obtain detailed information from each of the the sections/tabs.

System Detail Tab

The System Tab displays detailed information on the system's configuration, including BIOS, vendor information, operating system, location, machine name, function, memory and CPU utilization, etc. Administrators can choose to enter additional system information by filling in the fields at the top of the screen. The system's power management policies can be viewed and re-configured remotely by clicking on the Power Management button.

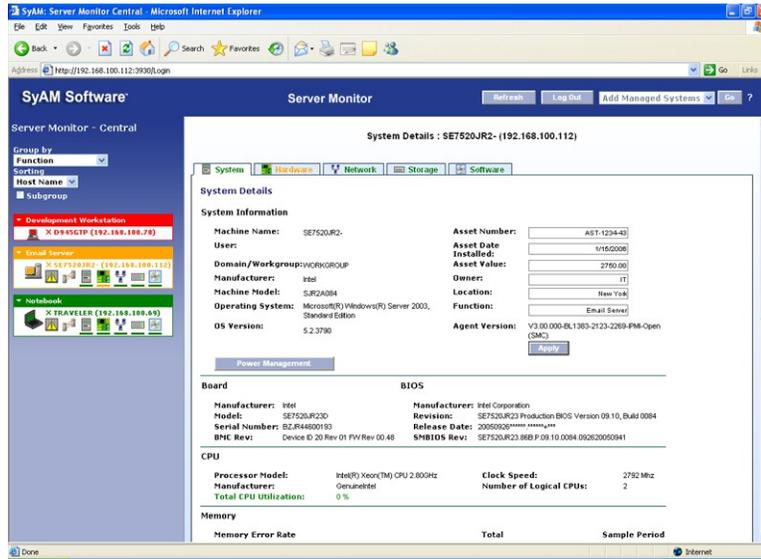


Figure 55: System Detail Tab

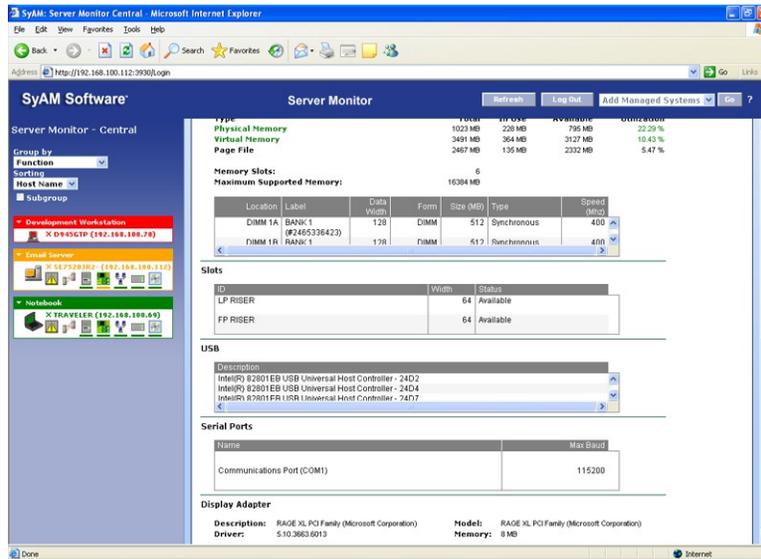


Figure 56: System Detail Tab Continued

Monitoring Memory Errors

SyAM provides real time monitoring and alerting of single- and multi-bit memory errors on systems with supported ECC Memory error monitoring.

The default alerting thresholds are to notify the administrator immediately on a multi-bit error or when two single-bit errors occur within a day.

Through the SyAM Central System Management Interface the administrator can adjust the thresholds and polling interval periods for both single- and multi-bit errors, and configure their notification methods.

Power Management Tab

The Power Management tab lets the user display and reconfigure the power management policies for the managed system.

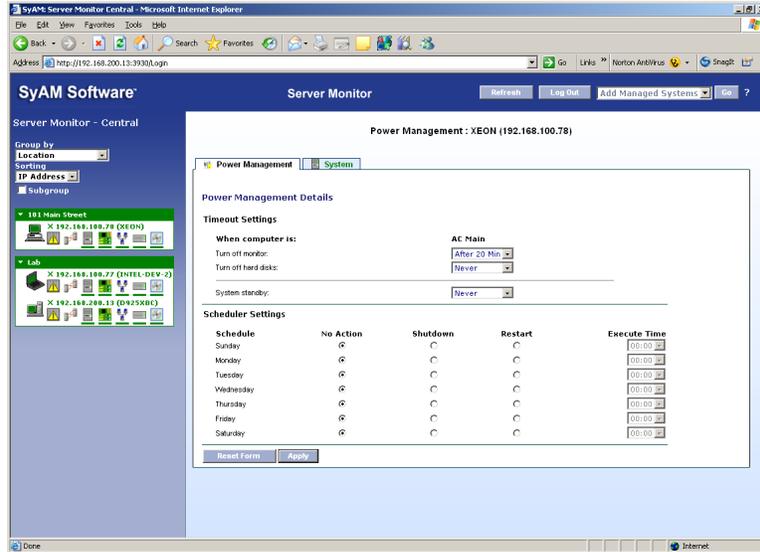


Figure 57: Power Management Tab

Timeout Settings

From here you can configure the power scheme settings for the managed system. If the managed system is a notebook there will be two separate sets of settings: one set that will be applied when connected to AC Power, and the other set for when running on battery.

The options are;

- Turn off monitor
- Turn off hard disks
- System standby
- Hibernate – This will only be displayed if the system has hibernation enabled

Battery

This information is only displayed if the managed system is a notebook.

- Current Power Source – States if the system is plugged in using AC Power Cord or is running from the battery
- Battery Charging – States if the battery is in a charging state.
- Battery Level – Current health state of the battery.
- Battery Charge – The % of the battery life available.

Scheduler Settings

You can configure the managed system to be scheduled to perform a graceful system shutdown or restart at any time for each of the days.

To enable, click on the appropriate radio button for the action to be taken that day. (No Action / Shutdown / Restart). Then set the time using the drop down box.

Different actions can be set at different times for each of the days of the week.

Only one action per day can be scheduled.

Press the Apply Button to save the changes made.

Hardware Detail Tab

All environmental sensors discovered on your platform are displayed in the Hardware Tab. This includes fans, temperatures, voltages, power redundancy loss and physical security. The number and type of sensors displayed is dependent upon the system platform and its configuration.

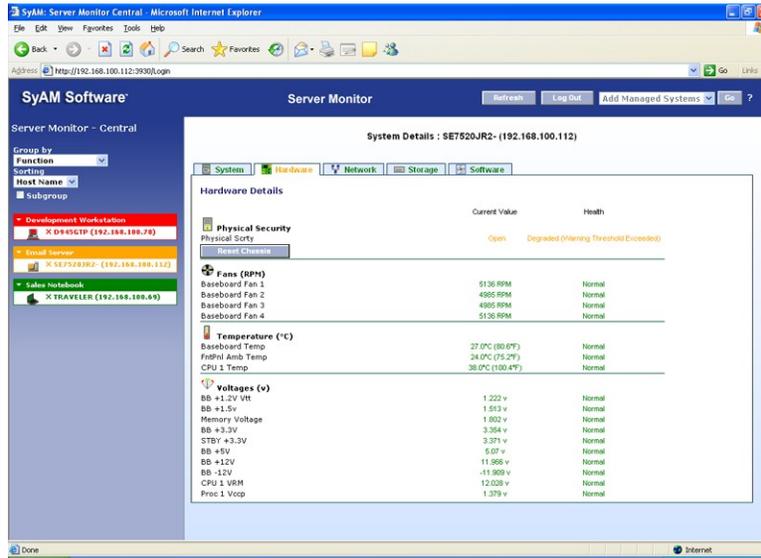


Figure 58: Hardware Detail Tab

Reset Chassis Intrusion

Some hardware platforms that support a chassis intrusion sensor, do not automatically reset the sensor state to normal when the chassis is closed. For such systems the Reset Chassis button causes the platform to reset the state of the sensor to normal.

Network Detail Tab

The Network Tab displays detailed information on adapters connecting the managed system to the network, including adapter and connection speed, connection status, IP address, and MAC address. Additionally the send and receive byte counts and calculated utilization over the last approximately 20 seconds is provided.

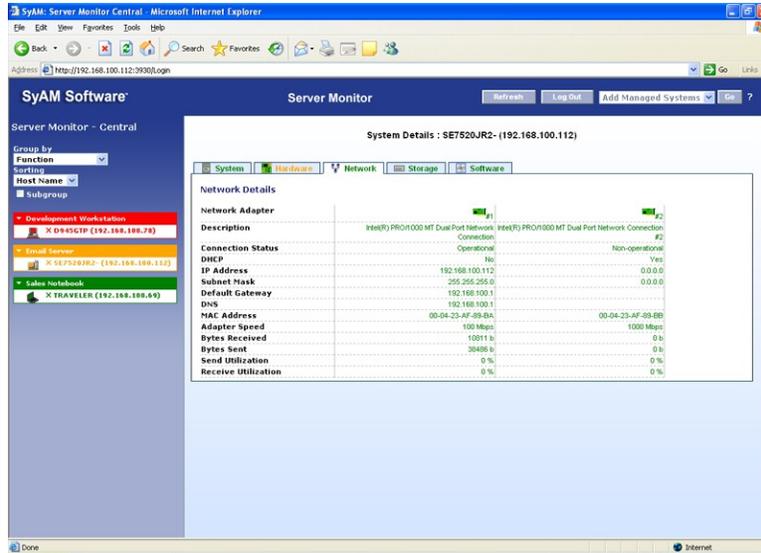


Figure 59: Network Detail Tab

Storage Detail Tab

The Storage Tab displays detailed information on physical and logical disks associated with the system being monitored. Physical disk attributes reported include vendor information, device ID, SCSI ID, and size. Logical disk attributes reported include name, size, space allocation, and utilization.

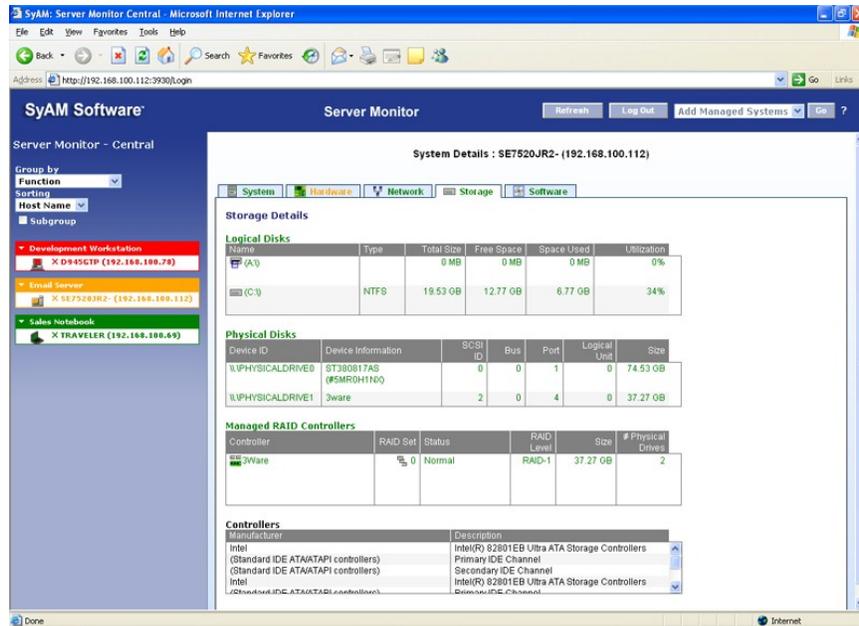


Figure 60: Storage Detail Tab

RAID Management

SyAM Server Monitor performs integrated monitoring of PCI RAID Controllers. All discovered PCI RAID Controllers that we support will be monitored, and their summary configuration and status displayed under "Managed RAID Controllers" within the Storage tab.

SyAM Server Monitor will discover RAID Controllers that it can manage only if the required RAID drivers are installed. If a new RAID Controller is installed after SyAM Server Monitor has been started, then restart the system for it to discover the new Managed RAID Controller.

Please check the release Notes for the list of RAID Controller compatibility for the version of software you are using.

SMART Drive Pre- Failure Monitoring

Directly attached disk drives that are SMART capable are checked daily. Supported disk technologies include P-ATA, S-ATA, SCSI and FC. The administrator can be notified of bad disk drives before they fail and potentially lose data. Notification of a bad SMART status (Pending failure) is done via the notification options configured for the drive.

The Storage Details tab visually shows physical drive status. A physical drive in the warning state (amber colored) is pending failure and has reported a bad SMART status.

RAID Management

Managed PCI RAID controllers can be configured with SyAM Server Monitor Central. Navigation begins from the Storage Details tab

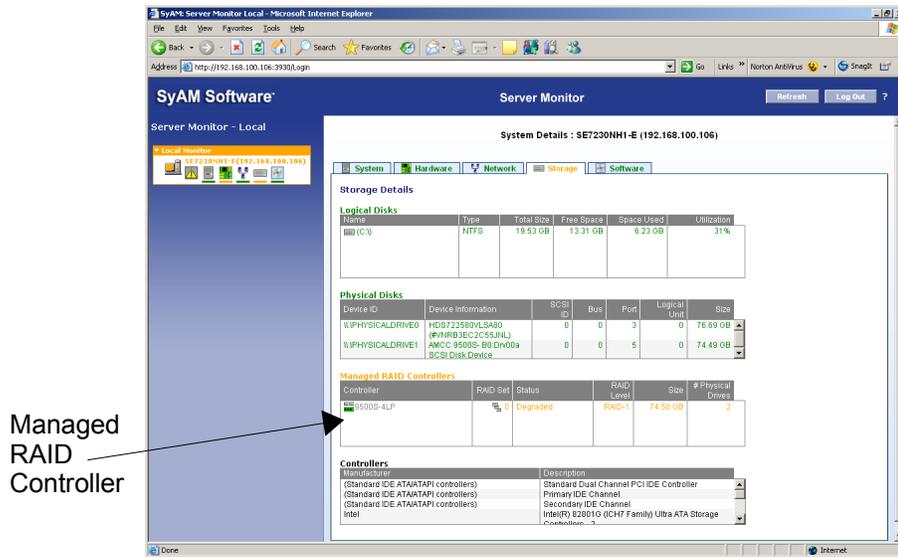


Figure 61: Storage Details – Managed RAID Controllers

Click on the RAID Controller to open up the RAID Controller window.

RAID Controller Details Screen

The RAID Controller screen is divided into 4 parts.

RAID Controller Details – Displays the controller model, firmware version, Cache if present, Number of Bus, ID, BIOS Version, BBU Presence and Max Devices per Buses

RAID Set Details – Displays the current RAID sets configured on this controller, including their description , RAID Set #, and Status (Normal, Init, Rebuild, Degraded, Failed). A RAID Set (also called a RAID Array) appears to the operating system as a physical disk.

Physical Drives – Displays the physical drives connected to the RAID controller, including their location on the BUS, ID, Status, Capacity, Vendor and Model. Physical drives in use by a RAID controller are typically not visible to the operating system.

Available Arrays – Displays the physical arrays defined by the RAID controller. A physical array is a grouping of drives on which RAID Sets are created. The display includes the RAID levels and capacities available for creating additional RAID sets.

RAID Controller Details : SE7230NH1-E (192.168.100.106)

RAID Controller
Storage

RAID Controller Details

RAID Controller Model:	9500S-4LP	Controller ID:	0
Firmware version:	FE9X 2.04.00.005	BIOS version:	BE9X 2.03.01.047
Controller Cache Memory:		BBU Presence:	Normal
Number of Buses:	4	Max Device per bus:	1

Mute Alarm
Rescan

RAID Set Details

RAID Set #	Status	RAID Level	Capacity (MB)	# Drives in RAID set	Caching	Stripe Size	Array #
C 0	Degraded	RAID-1	74.50 GB	2	Disabled		0

Delete RAID Set

Physical Drives

Choose the physical drive(s) to create an Array or add as Spare.

ID	Status	Capacity	Vendor	Model
ID 2	Full - Array # 0	76.33 GB	Maxtor	6Y080M0
ID 3	Free	76.33 GB	Maxtor	6Y080M0

Create Array
Add Global Spare
Remove Global Spare

Available Arrays

Array #	# Drives in Array	Free Space (MB)	RAID Level	Capacity (MB)	Caching	Stripe Size
C 0	1	0		0	Disabled	64 KB

Create RAID Set
Use as Array

Figure 62: RAID Controller Details Screen

Steps in Creating a RAID Set

1. Decide if you will create a RAID Set on an existing Physical Array, or want to first create a new Physical Array for the RAID Set. If you will use an existing Physical Array proceed to step 4.
2. To create a Physical Array, choose the physical drives that you wish to make up the array by clicking on their check box. (Remember only drives not in use in other arrays or as hot spares can be used.)
3. Click on the Create Array button – wait for the screen to update

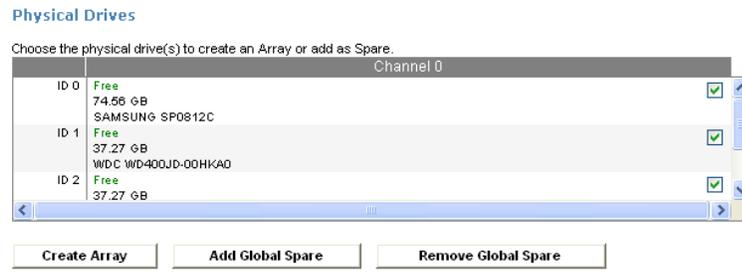


Figure 63: Physical Drives – Choosing drives for the Array

4. Now click on the Physical Array that you wish to create the RAID Set on. (**Physical Arrays with no available capacity will not display any available RAID Set configurations.**)
5. Choose the RAID level from the drop down box. Only RAID levels supported for the particular set of drives in the Physical Array will be presented. The maximum capacity available for the selected RAID level is calculated and displayed. You may enter a lower capacity to be used for this RAID Set.

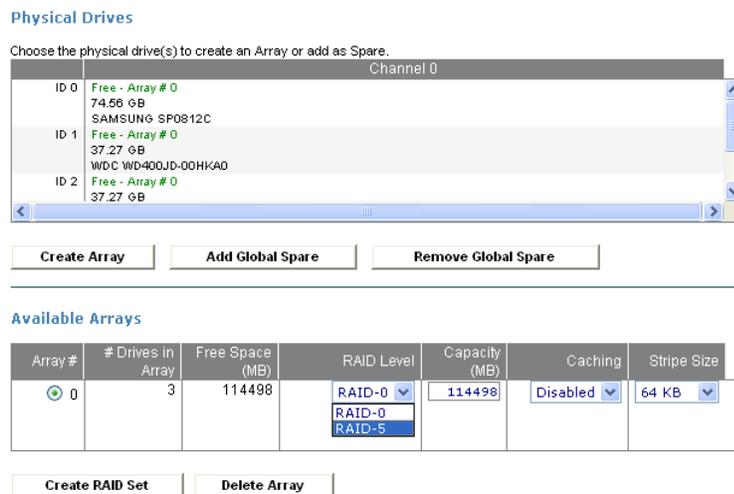


Figure 64: Available Array - Configuring the RAID Set

6. Next choose the Caching policy and stripe size from the drop down boxes.
7. Click the Create RAID Set button to create the RAID Set.
8. The system will now process your configuration and will create the RAID Set. If for any reason the create operation fails, a message will be displayed at the top of the screen explaining the cause for failure.
9. The new RAID Set will now appear under the RAID Set Details
10. If you created a Physical Array in Step 3 and decided not to create a RAID Set on it, you may dismiss it by selecting it and clicking the Delete Array button. You cannot delete Physical Arrays that have RAID Sets created on them.

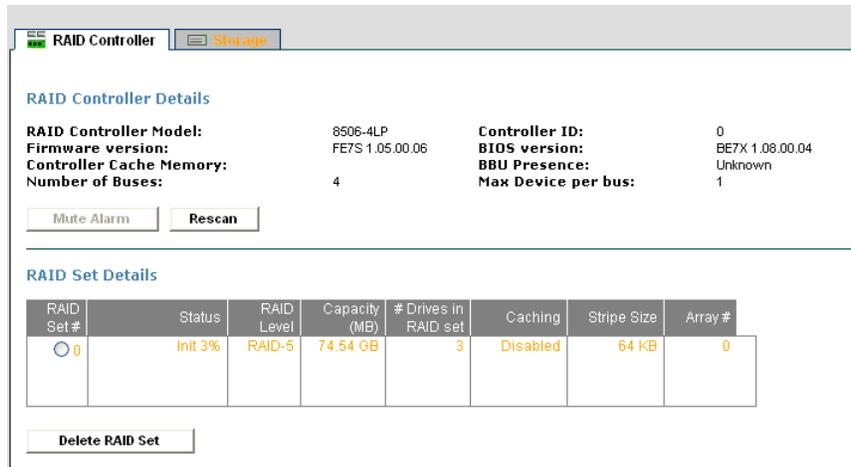


Figure 65: RAID Set Details – Information on Configured RAID Set

Adding/Removing a Global Spare

1. Choose the physical drive that you wish to become a global spare to the RAID Set by clicking on its check box, then click on the Add Global Spare button.
2. To remove a global spare click on the check box next to the drive that is currently displayed as a hot spare, then click the Remove Global Spare button.

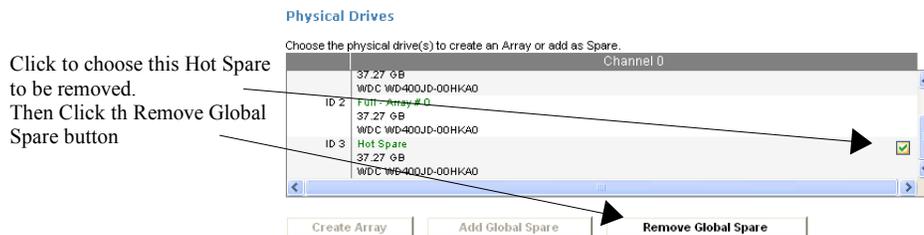


Figure 66: Removing a Hot Spare drive

Deleting a RAID Set

1. Under RAID Set Details click the radio button next to the RAID Set to delete. Then click on the Delete RAID Set button. Note that when multiple RAID Sets are present on the same Physical Array, only the last RAID Set displays a radio button and may be selected to delete.

The screenshot shows the RAID Controller Storage interface. At the top, there are tabs for 'RAID Controller' and 'Storage'. Below this is the 'RAID Controller Details' section, which includes fields for RAID Controller Model (8506-4LP), Firmware version (FE7S 1.05.00.06), Controller ID (0), BIOS version (BETX 1.08.00.04), Controller Cache Memory, Number of Buses (4), BBU Presence (Unknown), and Max Device per bus (1). There are 'Mute Alarm' and 'Rescan' buttons below this section.

The 'RAID Set Details' section contains a table with the following data:

RAID Set #	Status	RAID Level	Capacity (MB)	# Drives in RAID set	Caching	Stripe Size	Array #
0	Normal	RAID-5	74.54 GB	3	Disabled	64 KB	0

Below the table is a 'Delete RAID Set' button. Arrows point from the radio button in the table row and the 'Delete RAID Set' button to a text box on the right that reads: 'Click the button to choose the RAID Set to be deleted, then click the Delete RAID Set button'.

Figure 67: RAID Set Details – Deleting a RAID set

Software Detail Tab

The Software Tab displays detailed information on the processes, services, and applications installed and running on the system being monitored.

End Process – Start/Stop Service

The administrator can stop a running process, and start or stop a service of a managed system, without having to physically visit that system. The startup type and current status of each service is displayed.

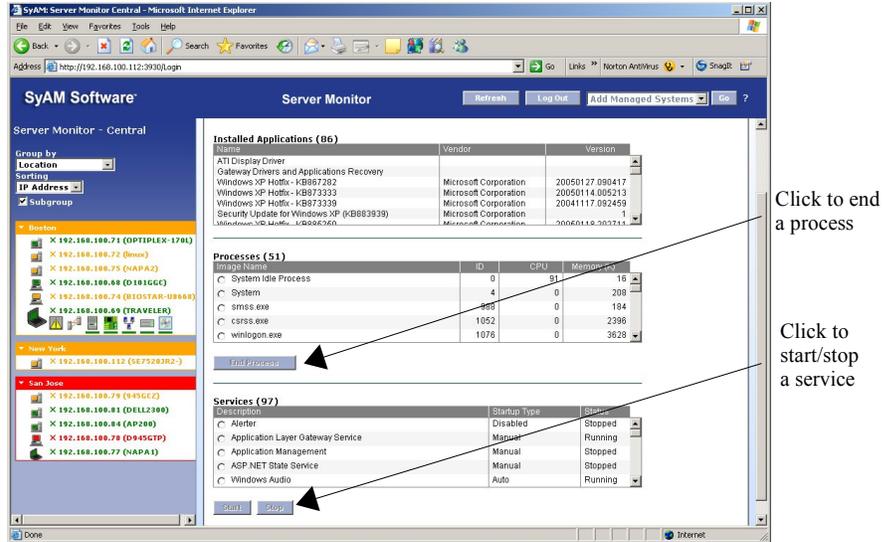


Figure 68: Software Detail Tab

To end a process, chose the process by clicking on the radio button to the left of the Process Name, then click the End Process button .

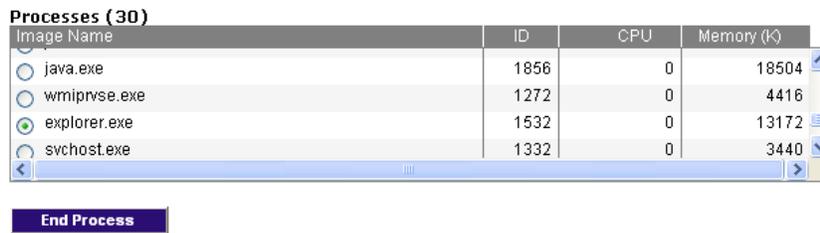


Figure 69: End the Process



Figure 70: Confirm to End the Process

To Start a Service choose the service by clicking on the radio button to the left of the Service Name, then click on the Start button. The service must be in a stopped state in order to be started.



Figure 71: Starting a Service



Figure 72: Confirm to Start the Service

To Stop a Service choose the service by clicking on the radio button to the left of the Service Name, then click on the Stop button. The service must be in a running state in order to be stopped.



Figure 73: Stopping a Service



Figure 74: Confirm to Stop the Service

Chapter 10: Configuring Platform Event Trap Support

This chapter provides instruction on how to configure the system running the Server Monitor Central software to receive Platform Event Traps

Platform Event Traps

Server Monitor Central is able to receive SNMP alerts in the Platform Event Trap Format (PETs).

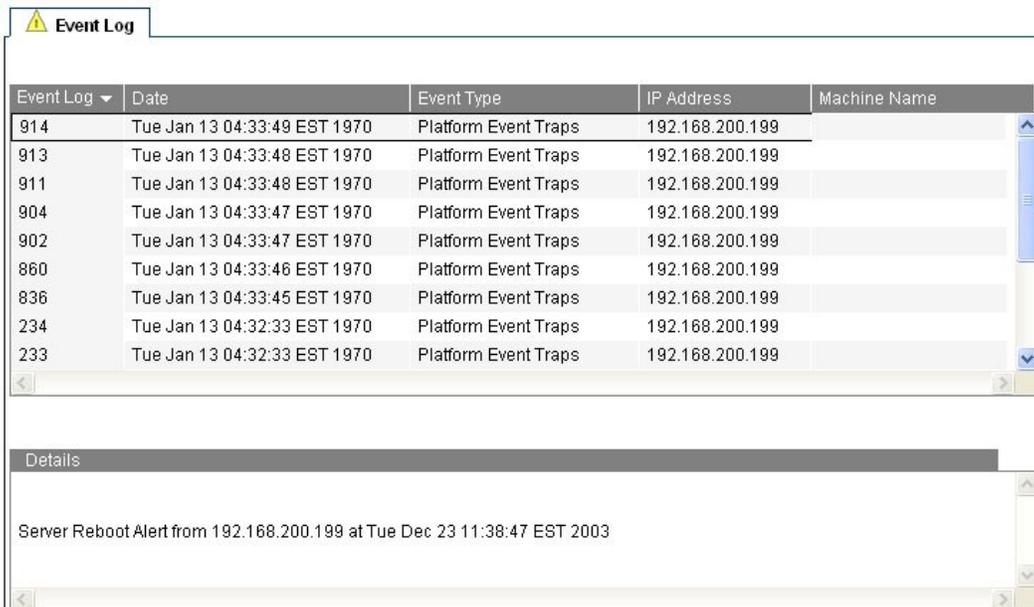
The Baseboard Management Controller (BMC) that performs the IPMI management is able to issue SNMP traps when a physical sensor event occurs. The SNMP Trap is formatted to a Platform Event Trap (PET) standard. Server Monitor Central is able to capture these PET's and notify the central administrators via a chosen notification method designated in the Central Alert Matrix. Server Monitor Central converts the SNMP trap information into a simple description of the event, providing the administrator with information to identify which server sent the event, as well as the type and severity of the event.

In addition to being notified about the PET, Server Monitor Central stores the complete SNMP Trap information within its Event Log for later review.

-----Original Message-----
From: Server/Desktop Monitor Central@8GM.com
[mailto:Server/Desktop Monitor Central@8GM.com]
Sent: Sunday, December 28, 2003 3:44 PM
To: John.Doe@company.com
Subject: Server Monitor Central Alert

Voltage Over Max Threshold Alert from 192.168.200.199 at Sun Dec 28

Figure 75: Example of a PET email alert



The screenshot shows the 'Event Log' window with a table of events and a 'Details' pane below it.

Event Log	Date	Event Type	IP Address	Machine Name
914	Tue Jan 13 04:33:49 EST 1970	Platform Event Traps	192.168.200.199	
913	Tue Jan 13 04:33:48 EST 1970	Platform Event Traps	192.168.200.199	
911	Tue Jan 13 04:33:48 EST 1970	Platform Event Traps	192.168.200.199	
904	Tue Jan 13 04:33:47 EST 1970	Platform Event Traps	192.168.200.199	
902	Tue Jan 13 04:33:47 EST 1970	Platform Event Traps	192.168.200.199	
860	Tue Jan 13 04:33:46 EST 1970	Platform Event Traps	192.168.200.199	
836	Tue Jan 13 04:33:45 EST 1970	Platform Event Traps	192.168.200.199	
234	Tue Jan 13 04:32:33 EST 1970	Platform Event Traps	192.168.200.199	
233	Tue Jan 13 04:32:33 EST 1970	Platform Event Traps	192.168.200.199	

Details

Server Reboot Alert from 192.168.200.199 at Tue Dec 23 11:38:47 EST 2003

Figure 76: Example of PET information in the Event Log

PET Sensor Types Supported:

- Temperature
- Voltage
- Current
- Fan
- Physical Security
- Platform Security
- Processor
- Power Supply
- Power Unit
- Cooling Devices
- Memory
- Boot Error
- OS Critical Stop

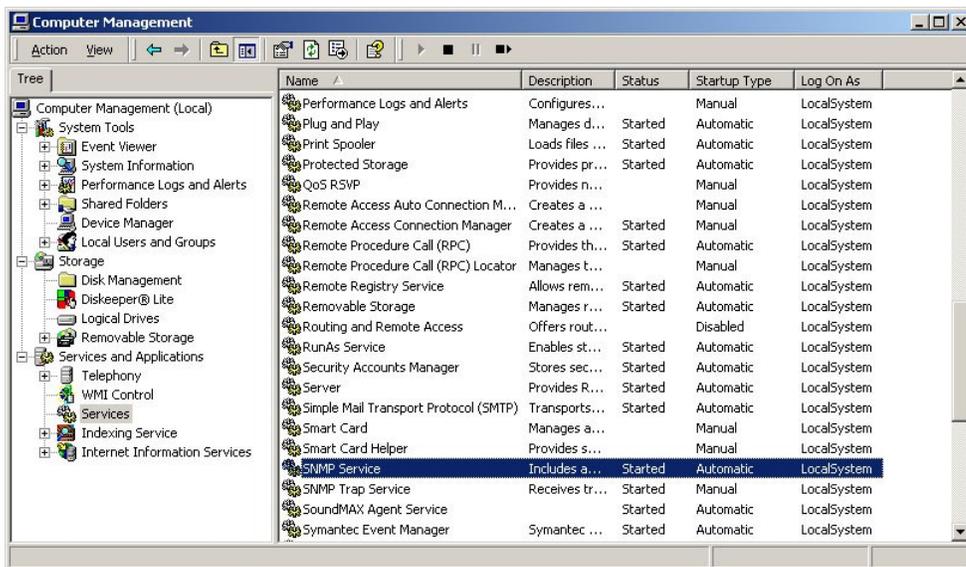
Note: If the PET received is not recognized, the administrator will be notified that an unidentified PET has been received and the Trap detail will be stored in the event log.
For more information on PET 1.0 specification please refer to the DMTF Website.

Configuring Server Monitor Central to Receive Platform Event Traps

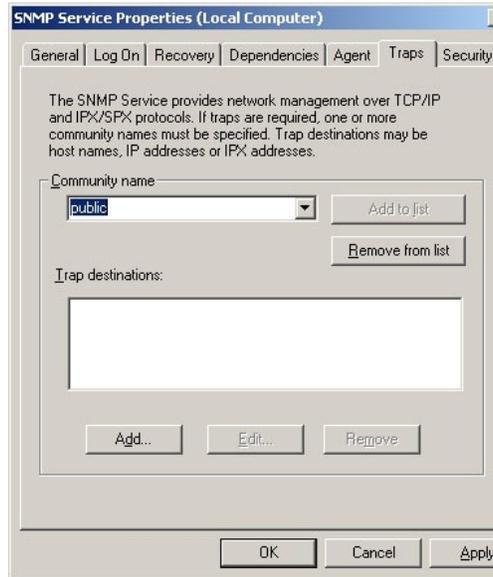
In order for Server Monitor Central to receive and process PETS, the system must have its SNMP service properties changed to include the community name “Public” and that no other SNMP Trap service is running, including the SNMP Trap Service that is automatically installed with the Windows SNMP Option.

To configure the SNMP Service Properties:

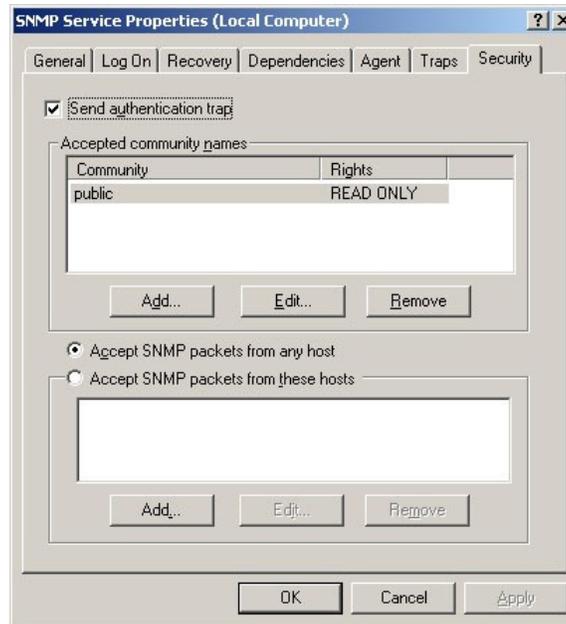
1. Open “Computer Management”
2. Under Services and Applications, select SNMP



3. Under the SNMP Services General Properties, Select Public as the community name and click <Apply>.

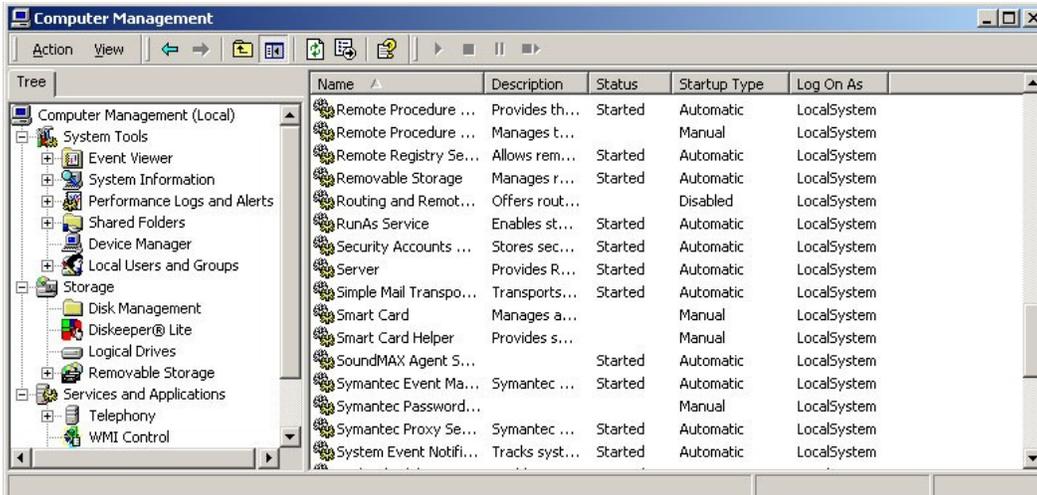


4. Under the SNMP Services Security properties, click the check box to enable Accept SNMP packets from any Host, or enter the IP addresses configured for the BMC on the IPMI-enabled servers.



5. Press the OK button and close the services window.
6. You will need to reboot the system in order for these changes to take effect.

If you cannot find the SNMP service, it means that it is not loaded.



To load the SNMP service:

1. Open up Control Panel, Add/Remove Programs and choose the <Add/Remove Windows Components> button on the left side of the screen.
2. Scroll down the list until you find Management and Monitoring Tools, and double click to display the options.
3. Once the options are shown, click on the check box next to Simple Networking Protocol, and click <OK>.
4. Click on the next button. This will then start to load the windows SNMP component. If the files are not found on the server's disks it will prompt you to insert the Windows Server OS CD's.
5. Once installed you follow the instructions on how to configure the SNMP service.

If another SNMP service is already running then the Server Monitor Central PET trap listener service will not be able to start. You will receive a notification and the event will be recorded in the event log.

Also the Central Alert Matrix will inform you that the Platform Event Trap Listener service is not running.

Chapter 11: Contact Details & Glossary

This chapter contains technical support contact information as well as a glossary.

Contact Details

Contact	product-support@syamssoftware.com
Web	www.syamssoftware.com
Support Information	http://www.syamssoftware.com/
Product Information	http://www.syamssoftware.com/

Glossary

Adding a sensor to the alert matrix

Sensors are automatically monitored, they have their sensor category default notifications applied to them.

Asset-monitoring event

Discrepancy in the systems physical and software inventory.

Central Alert Matrix

Administrators use this screen to define the notifications for all of the managed systems.

Central Alert Notification Settings

Notification and configuration details for the Central Alert matrix.

Central Management Tree

Displays in a tree format all of the managed systems.

Changing Central Management Tree grouping

Click on the <Group By> drop down menu to group systems by Location, Function, or Operating System.

Changing Central Management Tree sorting order

Click on the <Sort By> drop down menu to sort by IP address or Machine Name.

Changing to which Server/Desktop Monitor Central the system reports

Remove the system from the first Server/Desktop Monitor Central tree to stop the system from reporting. Once this is done, add the system to the second Server/Desktop Monitor Central tree by following the instructions "Add Managed System"

Critical Level

The level of the threshold which is operating beyond the normal and warning thresholds.

Current Value

The actual reported sensor reading for the system component on a timed reporting cycle.

Email #1/ #2

Primary and secondary administrator email addresses

Event Log

Record of all of the managed systems events.

From Address

Administrators can define a unique name for the SyAM alerting email address.

Graceful shutdown

Shutdown a managed system remotely if the agent on that system is in a functioning state.

Grouping systems

Group managed system by location, operating system, or function.

Hardware Detail Screen

Information on the system components being monitored, including fans, temperature, voltages, etc.

Hardware Event

When a threshold is met or exceeded by a physical component of the system.

Header Bar

The header bar within this browser contains the **<Logout>** **<Refresh>** **<?>** function buttons

Health colors

Green = Fully Functional
Amber = Warning threshold exceeded
Red = Critical Threshold exceeded
Grey = System update pending
Blue = Agent has been manually stopped
Purple = System is no longer responding
Black = System has been shut down
Cyan = System has expired Central Management License Key

Intervals

Readings on all monitored systems and components are at preset cycles of 20 seconds.

IPMI Event Log

Hardware event log stored within the IPMI based server

Logical Sensor

Storage, network adapters, removable disk drives, and CPU and memory usage.

Login

Administrators must login using a user name and password that has administrative rights to the machine that is running SyAM software

Lower threshold

The lowest threshold to be alerted upon if it is exceeded.

Network Detail Screen

Information on network adapters and their configuration.

Network Event

Network connectivity is lost.

Notification Settings

Email, SMS/pager, SyAM-Server Central, Network Messages and SNMP Traps.

Performance utilization event

CPU or memory utilization threshold is met or exceeded.

Physical Sensors

Physical Security, Fans, Temperature, Voltages and Power Unit sensor monitored

Platform Event Trap (PET)

SNMP formatted trap received from IPMI-enabled server

Remote Management

Shutdown, Reset, Wake on LAN and Remote Console

Remote Console

The Remote Console provides the capability of taking control of a managed systems local screen, keyboard and mouse directly through the web browser from the Central System Management Interface.

Removing a sensor from the System Alert matrix

To remove a sensor it must be in a critical state, then click on the "X" to permanently delete this sensor from the alert matrix.

Removing systems from Central Management Tree

To remove a system from the Central Management Tree, select the system and click on the X.

Reset period

The frequency of notifications sent after the initial alert has been sent and if the sensor has not been corrected.

Restore Physical Sensor Thresholds

This will reset to the original sensor threshold values when you click on this button.

Sample period

Time that is used to take CPU and Memory utilization samples.

Sensor Status Change back to normal

When a sensor returns back to within its operating threshold range.

SyAM Agent

Non-intrusive monitoring agent configured and managed by the SyAM Central Manager

SyAM Central Manager

Provides monitoring and communications with all managed agents

SyAM Local

Non-intrusive monitoring agent that can be browsed to directly or managed and configured from the SyAM Central Manager

SyAM Local Tree

Browsing directly to a system running SyAM Local.

SMS Pager #1/#2

Primary and secondary administrator SMS/Pager addresses.

SMTP address

Mail system address: example: mail.company.com or 192.168.1.100

SNMP Traps

Notification from a system or central manager to an enterprise framework server – Requires System Area Management (SyAM) MIB to be installed on enterprise framework server.

Software Detail Screen

Information on the processes, services, and applications installed.

Storage Detail Screen

Information on physical and logical disks, controllers and removable devices.

Storage Event

Logical disk has reached its utilization threshold, Loss of logical disk, or Loss of Physical disk.

System Absent

When the Server/Desktop Monitor Central is no longer able to communicate with a managed system, it is reported as being absent, unless it was correctly shutdown.

System Alert Matrix

Interface to configure sensor thresholds and notification options.

System Alert Notification Settings

Notification and configuration details for the System Alert matrix.

System Detail Screen

Information on the system's configuration, BIOS, operating system, location, memory, CPU, etc.

Upper Threshold

The highest threshold to be alerted upon if exceeded.

User name and Password for outgoing Authentication

Enter the administrator user name and password (if the outgoing email system requires authentication)

Wake on LAN

Power up a WOL-enabled managed system.

Warning Level

The level of the threshold that is operating between the normal and critical thresholds.

Welcome

Displays the Revision and contact details for the product.