



GSMT USER'S MANUAL

Table of Content

Preface	3
Technical Support	3
Packing contents	3
Chapter 1 Introduction	4
Overview	4
Operating System	4
Summary of Features	5
Intrusive and Non Intrusive Methods	7
Chapter 2 Quick Installation	8
Getting Started	8
Installation	10
Installing Java Development Kit	10
Installing GSMT	16
Running the GSMT server from Windows	20
Connecting	21
Uninstalling UMS	23
Chapter 3 Configuration GSMT	24
Overview	24
Section Icons and Functions	25
Default User Name and Password	28
UMS Discovery	29
UMS Device	41
UMS Monitoring	49
UMS Configuration	56
UMS Service	60
UMS Events	65
UMS User	69
UMS Reports	80
Appendix Reference	82

Preface

Packing contents

- The GSMT User's Manual
- GSMT (Version 1.0) on CD
- GSMT (Version 1.0) Quick Installation Guide
- Warranty and Registration Software

Technical Support

Gigabyte provides technical support for Gigabyte products purchased directly from Gigabyte or from Gigabyte authorized reseller only.

IF	Then
You purchased this product from Gigabyte or from a authorized reseller,	Call Gigabytes' technical support at 886-2-89124888, ext.2222. Please be prepared to specify the serial number or CD Key of the product (if applicable)
This Gigabyte product was installed as part of system manufactured by a company other than Gigabyte or you purchased a Gigabyte product from an unauthorized reseller,	Call the technical support department of the computer manufactured or the unauthorized reseller. Gigabyte does not provide direct technical support in this case

Website

We invite you to access the Gigabytes' World Wide Web site via:

<http://www.giga-byte.com>

Chapter 1 Introduction

Overview

Gigabyte Server Management Tool is the solution for centralized management (From a Single Station) of various devices that are connected in the network environments. GSMT provides powerful features under the UMS utility. It is also a powerful server application that allows system administrators to simplify hardware management because GSMT is a J2ee (Java 2 Platform Enterprise Edition) server application. GSMT is portable to any operating system. GSMT console is web enabled where the user interacts with the application using a web browser.

Note: A smart JMX (Java Management Extension) agent enables the system administrator to perform complex management operations.

Supported Protocols

Standard Protocols

- SNMP (Simple Network Management Protocol)
- IPMI (Intelligent Platform Management Interface)

Operating System

GSMT is supported by the following operating systems:

- Windows® 2K
- Windows® XP

The Following table shows browsers that are compatible with GSMT:

OS Name	IE version	Netscape version	Opera version
Windows	6.0 and above	6.0 and above	6.0 and above

Summary of Features

Features	Description
Discovery	<ul style="list-style-type: none"> • Network Model definition • Defining Discovery Scheduling • Start Discovery • Stop Discovery • Support multiple protocols to discover and manage devices
System Monitoring	<ul style="list-style-type: none"> • Hardware health monitoring • Gauge Monitoring • Counter Monitoring • String Monitoring • Configure Poll Interval • Global Stop Monitoring • Global Start Monitoring • Start/Stop Monitoring • Event Management • Automated corrective actions to reduce downtime of the system
Configuration Management	<ul style="list-style-type: none"> • Configuring device
Advanced IPMI Features	<ul style="list-style-type: none"> • Serial Flashing • Console Redirection
Security	<ul style="list-style-type: none"> • Role <ul style="list-style-type: none"> • Execution • Configuration • Organization • General

Cont'd

Features	Description
Security (Contd)	<ul style="list-style-type: none">• Signup• Login• Start Discovery• User rights based on node• User profile
Report	<ul style="list-style-type: none">• Graphic format• File• View Event Log• View Configuration of a node• View Monitoring of an attribute• View Discovered nodes• Global Start Monitoring• View Network model• View Historical Data collection of an attribute• View Discovery Progress

Intrusive and Non Intrusive Methods

The GSMT uses two different methods to instrument managed nodes. These two methods are explained in the table below:

Method	Description
Intrusive	<p>A node management method is classified as intrusive when the agent used to instrument the node and communicate with the server application resides on the node.</p> <p>For instance:</p> <p>The smart JMX agent would reside on all the IPMI in-band managed nodes. GSMT will communicate to the BMC on the managed node via the smart agent. The smart agent communicates to the BMC using a device driver, which in turn communicates using KCS or SMIC interface.</p>
Non-Intrusive	<p>A node management method is classified as non-intrusive when the agent resides remotely on the GSMT and the communication with the node is implemented through a standard communication protocol already supported by the OS of the managed node.</p> <p>For instance:</p> <p>In case of IPMI, GSMT can communicate side-band with the BMC on the managed node. In this type of management, GSMT manages the node using RMCP (Remote Management Control Protocol) over UDP (User Datagram Protocol) and send request data according to the IPMI specification.</p>

Chapter 2 Quick Installation

Getting Started

Prerequisites

Before you can install the GSMT utility into your host system, you must meet the minimum system requirements. See the table below:

Requirement	Description
Processor/speed	You need at least an 800 MHz processor installed (Intel® Pentium® III processor, Intel® Pentium® 4 processor, AMD Athlon™ XP processor, or equivalent).
System memory	You need to install at least 256 MB of system memory.
Hard disk drive space	You need at least 28 MB of space on the Primary Master IDE hard disk drive dedicated to the GSMT utility.
Network card	You must have a 10/100 Ethernet adapter card installed (onboard or installed in an expansion slot). You must have a 10/100 Ethernet adapter card installed (onboard or installed in an expansion slot). Note: The GSMT utility supports one network controller.

Required Plugin

The following UMS components require Java plugin:

- Discovery Status
- Graphical View of Historic Data Collection
- Console Redirection

If any of the UMS components above failed to function, you must download the Java plugins as described below:

For Microsoft Windows operating system:

- Step1. Go to <http://java.sun.com> website.
- Step2. Go to download of J2SE v1.4.2
- Step3. Select the 'Windows Installation' and 'JRE' version.

Step4. Install the JRE.

Step5. Exit the internet browser running the UMS utility and login to UMS.

For Linux operating system:

Step1. Go to <http://java.sun.com> website.

Step2. Select the 'Linux RPM in self-exacting file' and 'JRE' version.

Step3. Install the JRE.

Step4. Exit the internet browser running the UMS utility and login to UMS.

Macromedia Plugin

The following UMS components require macromedia plugin:

- Discovery Nodes

If the UMS components above failed to function, you must download the macromedia plugins as described below:

Step1. Go to <http://www.macromedia.com> website.

Step2. Select download and then install the latest version of the 'Macromedia Flash player.

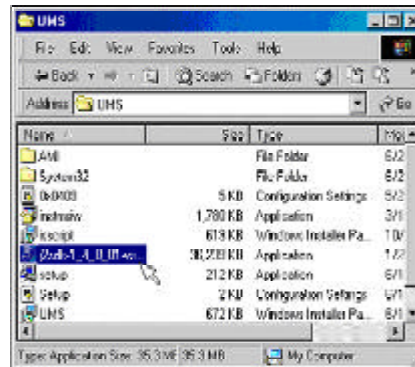
Installation



Installing Java Development Kit

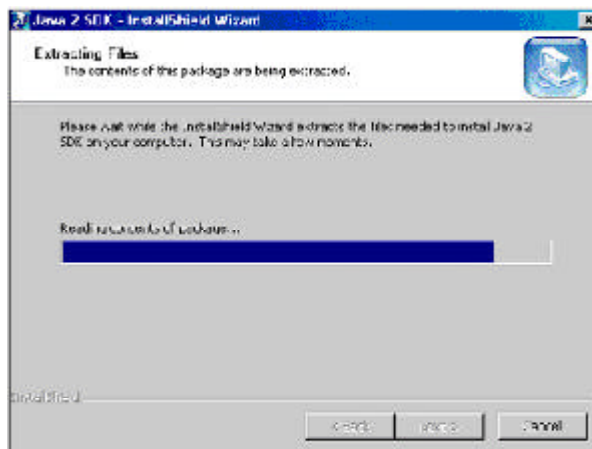
Use the following steps to install the Java Development Kit into the host system.

Step1. Insert the UMS CD into the host system. Double left click on the j2sdk-x_x_x_xx-windows-xxxx.exe executable file to begin the Java Development Kit installation procedure.

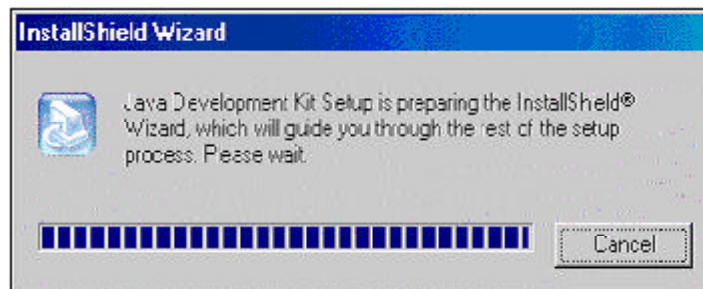


Note: It is recommended to install an Internet browser first before installing the Java 2 SDK. By following this sequence, you ensure that all necessary plug-ins required by GSMT are loaded.

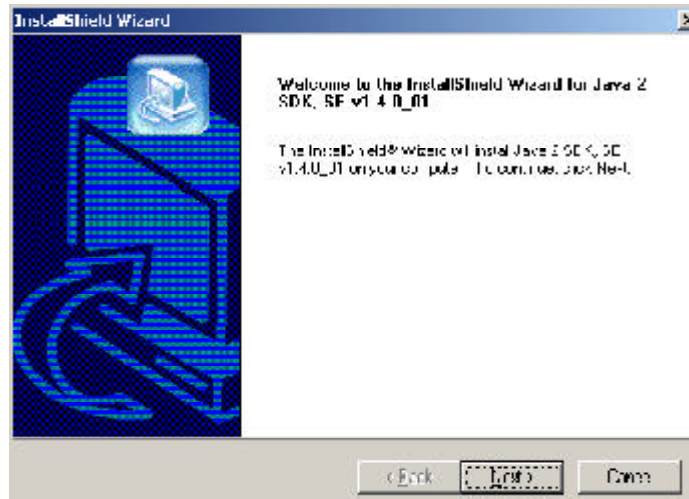
Step2. The Java DevelopmentKit InstallShield Wizard automatically starts to extract the files needed for the installation. After the extraction is complete, the Java Development Kit InstallShield Wizard automatically begins to load.



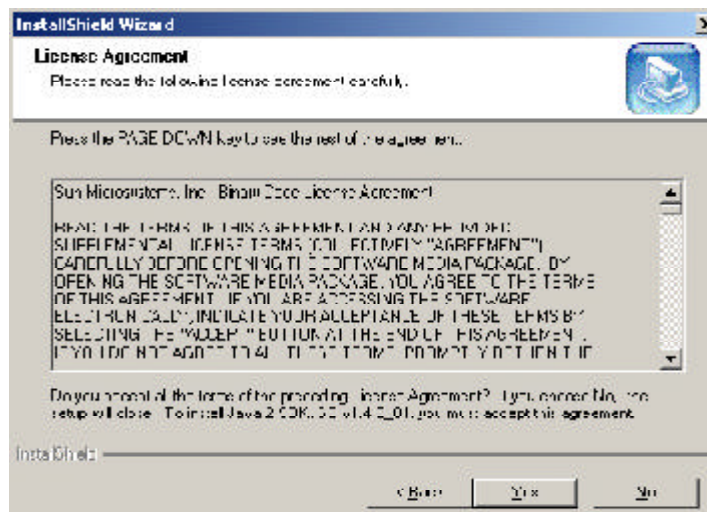
Step3. Java DevelopmentKit InstallShield Wizard dialog box opens. It states that the Java Development Kit Setup is being prepared.



Step4. Click on the Next button when you see the Welcome to the InstallShield Wizard Java 2 SDK screen.



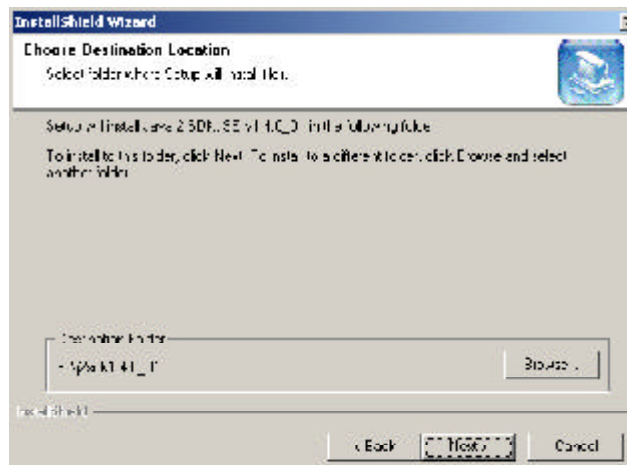
Step5. Click the Yes button to accept all terms of the Sun Microsystems, Inc. Binary Code License Agreement to proceed with the Java DevelopmentKit installation procedure.



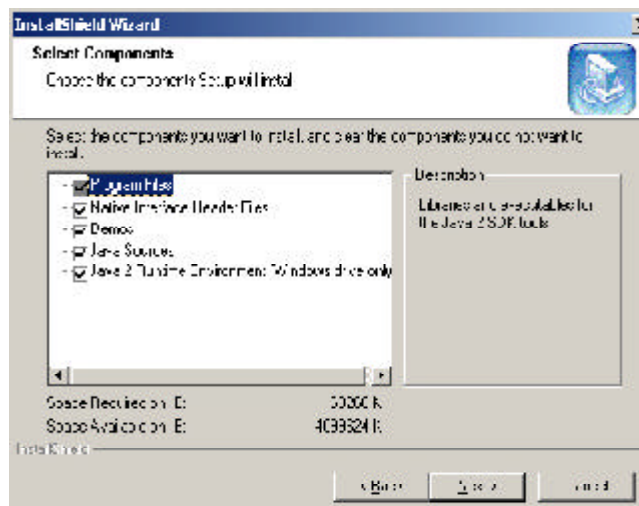
Step6. Click on the Next button to install the Java 2 SDK into the default location.

Note: You can also select another location by left clicking on the Browse button.

Note: If another location is selected, do not use spaces in the path or file name.



Step7. Select the components you want to install and uncheck the components you do not want to install. Left click on the Next button to continue.

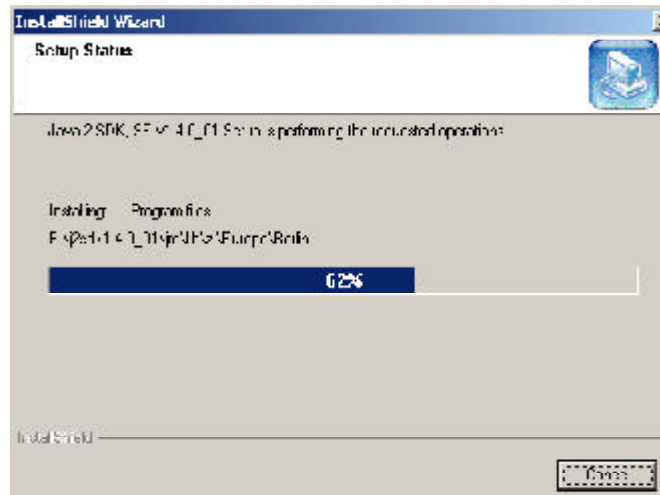


Step8. Select the Internet browser(s) you want to use to access the UMS server and click on the Next button.

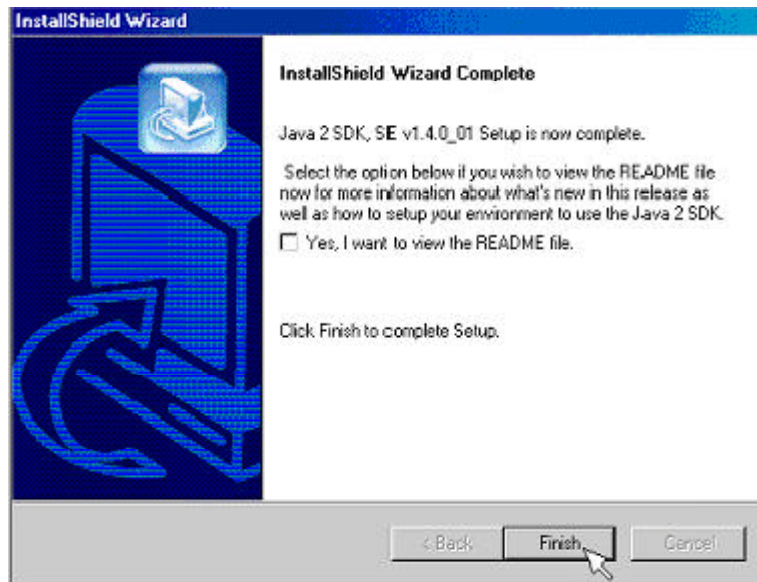
Note: You can enable or disable the Java(TM) Plug-in Control Panel.



Step9. The Setup Status screen appears giving you a graphical representation of the installation progress.



Step10. Click on the Finish button to complete the InstallShield Wizard.



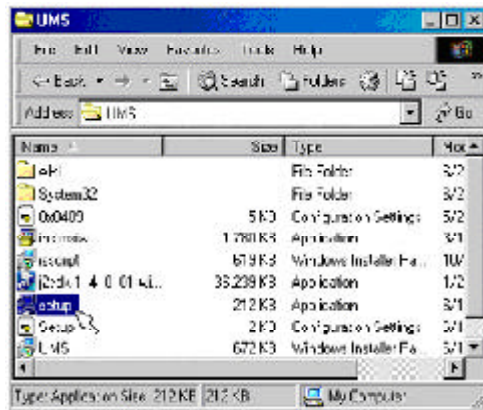
Step11. Congratulations! You have successfully installed the Java 2 SDK on your host system.

Note: The Java 2 Development Kit is now available from your Programs menu accessible from the Start button.

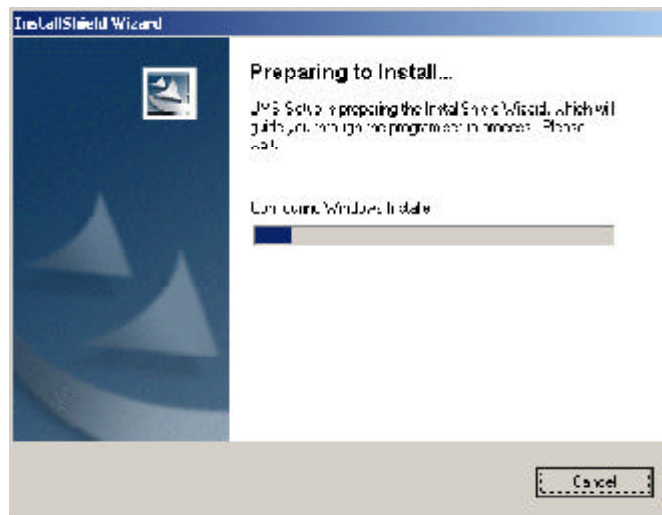
Installing GSMT

Use the following steps to install the UMS utility into the host system.

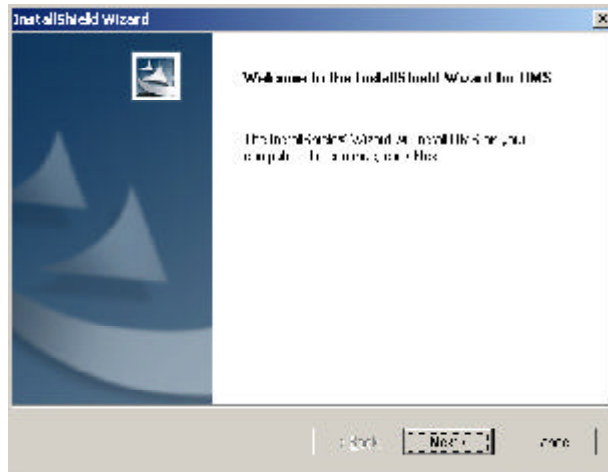
Step1. Insert the GSMT CD. Double click on the Setup.exe executable file to initiate the GSMT installation procedure.



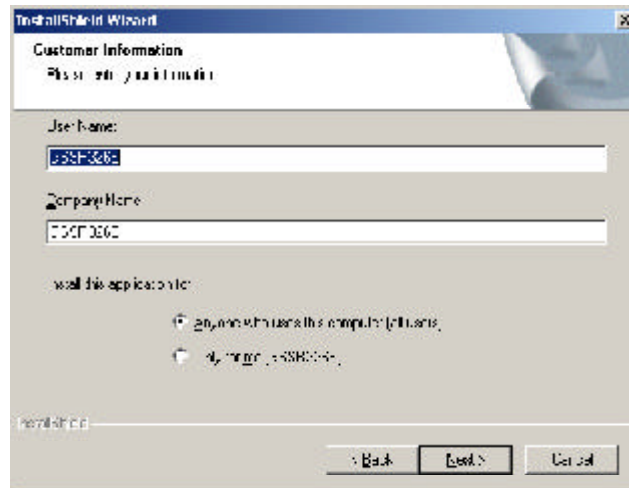
Step 2. GSMT automatically starts to extract files needed for the installation. After the extraction is complete, the InstallShield Wizard automatically begins to load.



Step 3. Click on the Next button when you see the Welcome to the InstallShield Wizard for GSMT screen.



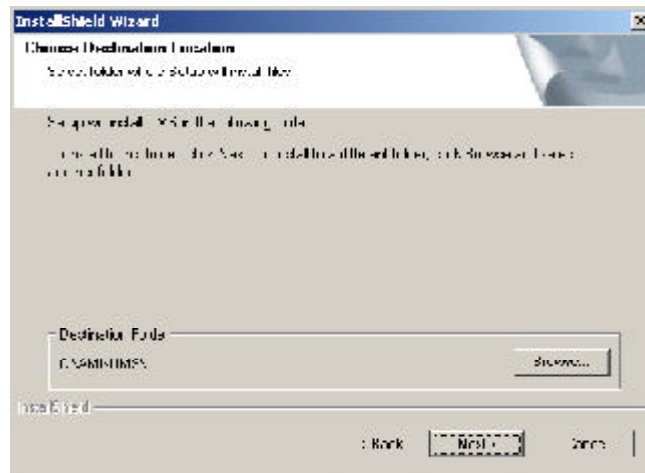
Step 4. Type your User Name and Company Name into the appropriate fields. Select all users or self-accessible rights by left clicking on one of the two radio buttons, (Anyone who uses this computer [all users] or, Only for me). Left click on the Next button to continue.



Step 5. Click on the Next button to install the GSMT utility into the default location.

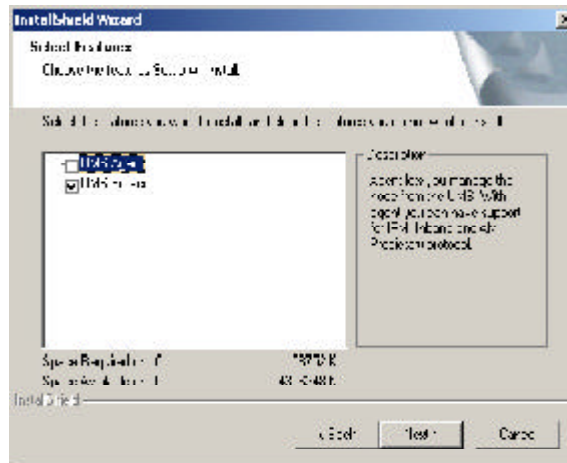
Note: You can also select another location by left clicking on the Browse button.

Note: If another location is selected, do not use spaces in the path or file name.

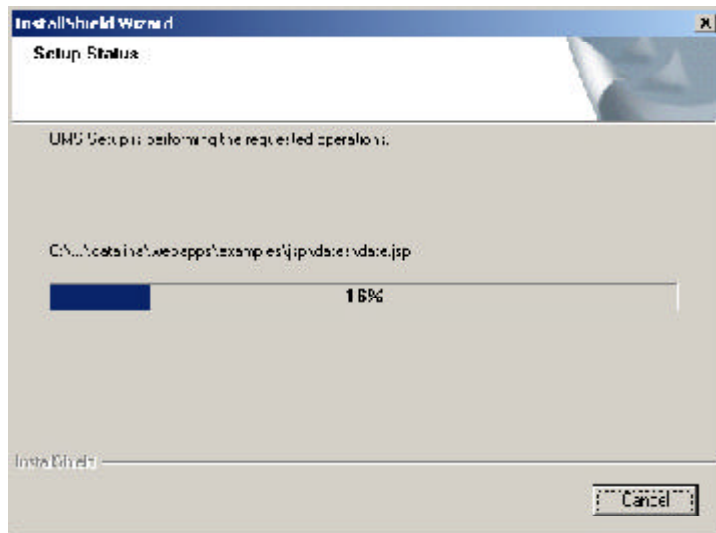


Step 6. Select the feature you want to install. Left click on the Next button to continue.

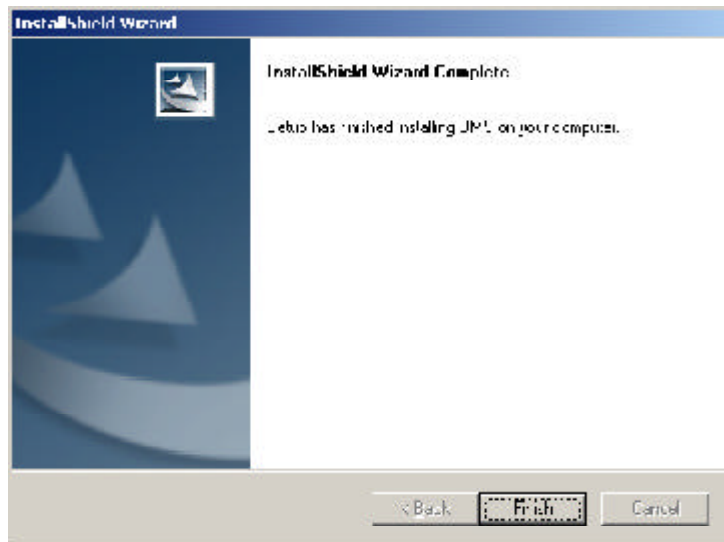
Note: If UMS Server is selected, you can manage any nodes connected on the network. Also, if UMS Agent is selected, you can have support for IPMI Inband and AMI proprietary protocol.



Step 7. The Setup Status screen appears giving you a graphical representation of the installation progress.



Step 8. Click on the Finish button to complete the InstallShield Wizard.



Step 9. Congratulations! You have successfully installed the GSMT utility on your system. It is now a UMS server.

Note: The GSMT utility is now available from your Programs menu accessible from the Start Window button.

Running the GSMT server from Windows

Use the following steps to start UMS through the Start window button.

Step 1. From the Programs menu item, select UMS and click on Start UMS menu item.

Note: This will take 4 minutes to complete the application running appropriately.



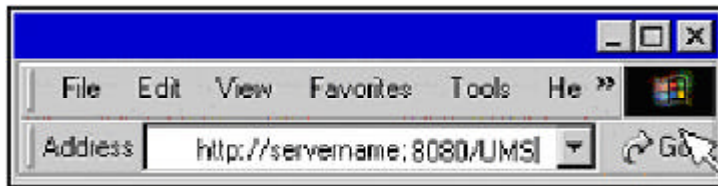
Step 2. You can stop UMS by left clicking the Stop GSMT menu item.



Connecting

Use the following steps to connect to your UMS server.

Step 1. Type the IP address of the UMS server



Step 2. Once you press the <ENTER> key or left click the Go button, you are immediately prompted for a username and password.

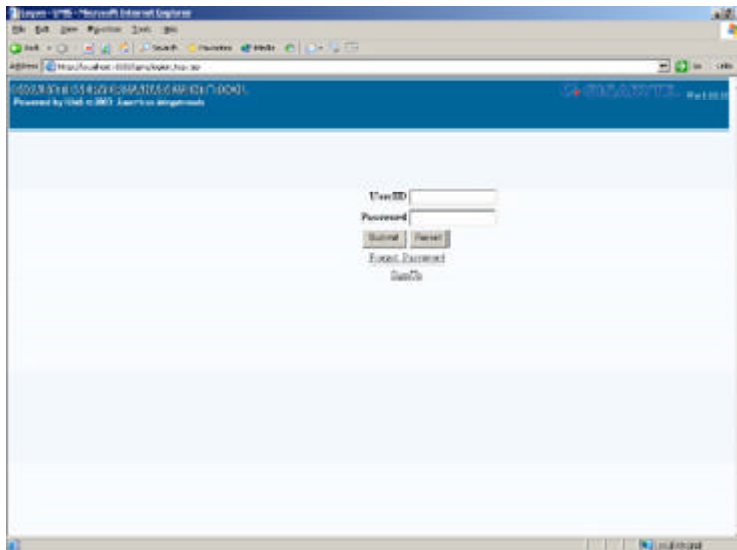
The default username and password is as follows:

Default username: **Admin**

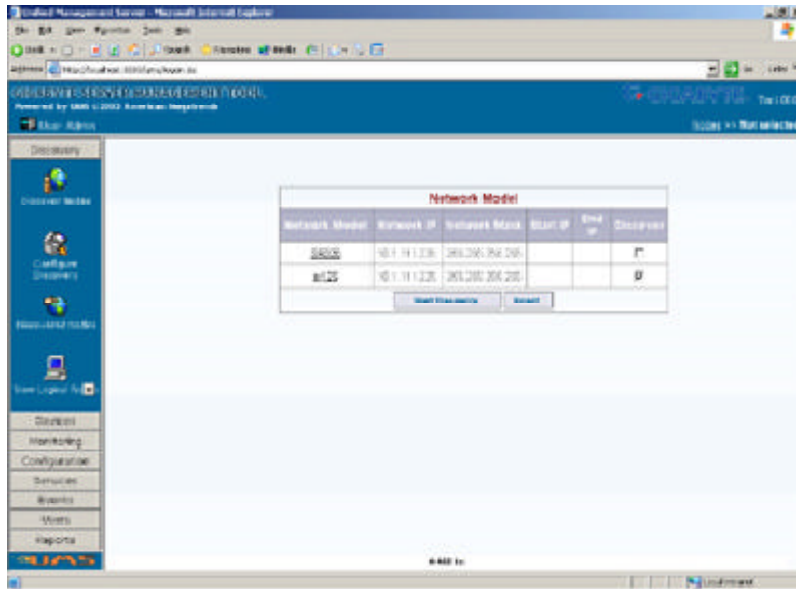
Default password: **Admin**

Note: If this is your first time using UMS, then enter the following IP address:

Http:<Servername>:8080/UMS/first_time_only.jsp



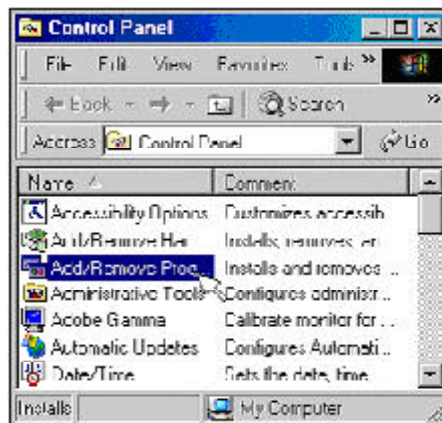
Step 3. The UMS startup screen appears. You are now connected to the UMS server.



Uninstalling UMS

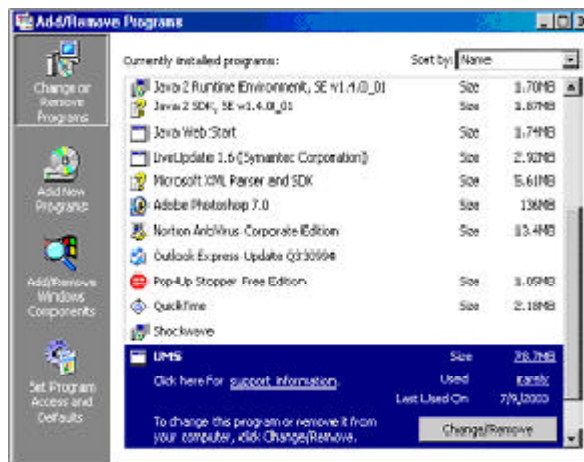
Use the following steps to uninstall UMS (server/agent).

Step 1. From the Settings menu item, select Control Panel and double click on Add/Remove Programs.



Step 2. Click on the UMS component you want to remove and then left click on the Change/Remove button.

Note: GSMT must be uninstalled first before the Java SDK is uninstalled.



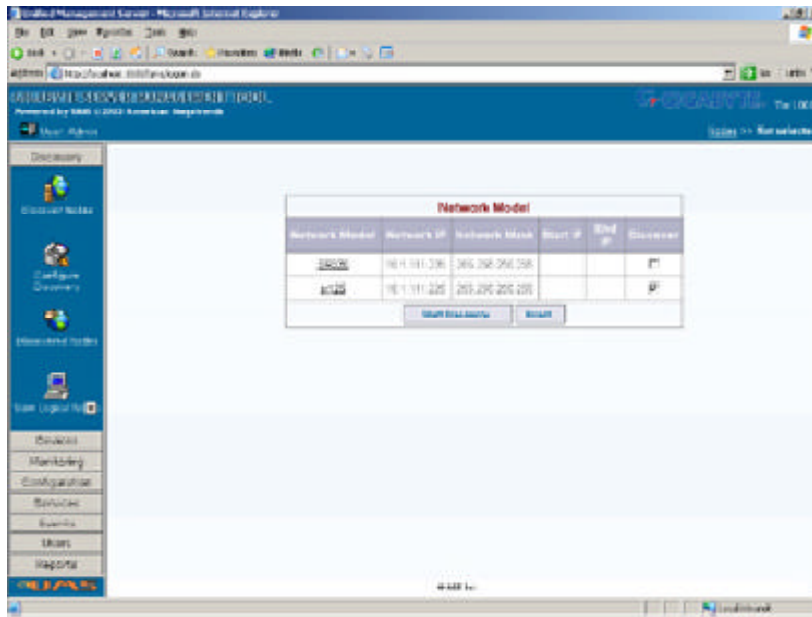
Chapter 3 Configuration GSMT

Overview









Gigabyte Server Management Tool (GSMT) provides powerful features under the UMS utility. Through the user-friendly Web-based interface, you can define and manage Network Models are located in the same or connecting network. The UMS utility provides you with powerful tools that allow you to manage multiple Network Models from a single station.











Note: A network model is the domain where the UMS utility performs the discovery process on the nodes to be managed. You can specify a network model by defining the network address, the network mask and the start/end IP addresses.
















The following sections will guide you the procedures to configure UMS utilities.



Section Icons and Functions

SECTION	ICON	NAME	DESCRIPTION
Discovery		Device Nodes	This section can be started any time using start discovery process. Discovery can also be started for a single network model or a set of network models. When discovery is started, UMS will present a discovery progress screen to the user. If discovery is already in progress, then a new discovery process can not be started.
		Configure Discovery	This section allows you to configure the network model and the discovery cycle.
		Discovered Nodes	This section allows you to view list of discovered nodes in UMS.
		View Logical Nodes	This section displays the <i>Nodes Identifier, Device Type</i> and <i>Protocol Name</i> .
		Stop Discovery	This section allows you to stop discovery at any time through stop discovery process. When stop discovery is clicked, the discovery that was started previously will be stopped.
Devices		Select Device	This section allows you to select a device. A list of discovered device will be displayed. After selecting the device and clicking on [Enter], the selected device will be the current device.
		Method Invocation	This section allows you to invoke a method on a selected device remotely.
		View SEL	This section allows you to view and clear the BMC event log. The event log is a repository system events and certain system configuration information. The event log displays information such as attribute values going out of range, BIOS post messages, and so on.

SECTION	ICON	NAME	DESCRIPTION
Device (Cont'd)		View FRU	This section provides support for accessing multiple sets of non-volatile FRU information. User will typically access information for each major system board (for example: Processorboard, memory board, I/O board and etc.) The FRU data includes information such as serial number, part number, model and asset tag. This information is available even when the system is powered down.
		Unmanaged Nodes	This section allows you to delete template nodes.
		Unmanaged Template Nodes	This section allows you to delete a template nodes.
		Select Device	This section allows you to select a template nodes.
Monitoring		System Health Information	This section allows you to view the list of attributes that are marked as candidate for monitoring for a given node or template.
		Select Monitorable Attributes	This section allows you to select attributes to be monitored of the selected node.
		Global Start Monitoring	This section facilitates restart of the monitoring in case its globally stopped. Monitoring of any of the attribute on any node could be done only if monitoring is globally started.
		Global Stop Monitoring	This page facilitates you to globally stop monitoring. None of the attributes of any node will be monitored if the monitoring is globally stopped.
		Configure Poll Interval	This section shows you how frequently the attributes should be polled. You are allowed to configure this interval. Note: This sampling time is always the multiple of this poll interval.
		View Historical Data	This section allows you to view historical data collected for a particular attribute for particular node.

SECTION	ICON	NAME	DESCRIPTION
Configuration		Configure Monitoring	This section allows you to configure the monitoring definition of a certain attribute that belongs to the current device (node) in the session.
		Configure	This section allows you to configure the parameter attributes of IPMI Commands that are configurable. Currently implemented for LAN and PEF.
		Configure Mail Server	This section allows you to configure mail server details.
Services		Load Services	This section allows you to load services
		Compile Files	This section allows you to compile the loaded files and associate device type with it.
		IPMI Conformance Tool	This section provides a means to send IPMI commands to BMC. You can send commands using an in band interface. UMS also provides screens for giving input parameters for each command. UMS constructs a request packet with the input given by the BMC forwarding it back to the client.
Events		View Events	This section allows you to view the event occurred in UMS.
		Modify Action	This section allows you to modify actions associated with events.
		Event Config.	This section allows you to configure events.
Users		Modify Rights	This section allows you to modify rights associated to a user.
		View Rights	This section allows you to view rights associated to users.
		Node Rights	This section allows you to associated node to users.
		User Profile	User section allows you to view or modify your profile but not access permission using user profile option.
		User Accept	This section allows you to accept users.
Reports		Historical Data Files	This section allows you to download the historical data as reports.

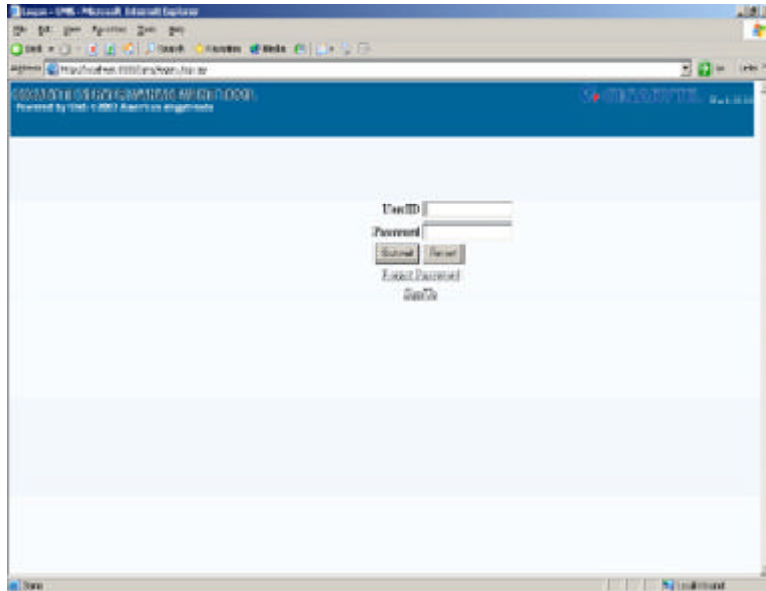
Default User Name and Password

When you first try to access your UMS server, you will be prompted to enter a user name and password.

The default user name and password is as below:

Filed	Default
Default user name	Admin
Default password	Admin






Note: User name and password are both case sensitive.



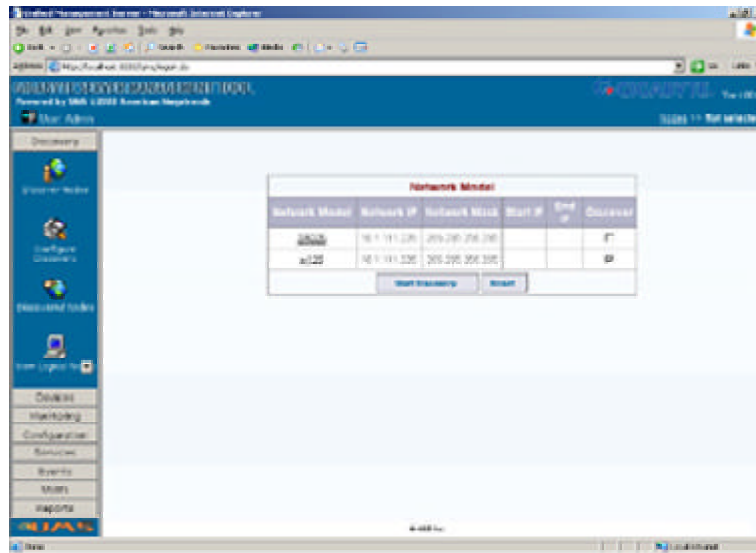
UMS Discovery

The *UMS discovery* feature allows you to start discovery process for a single network or a set of network models. By using this feature, you can use the following subsection: *Discover Nodes*, *Configure Discovery*, view *Discovered Nodes* and *View Logical Nodes*. Each subsection is explained in more detail further in this section:

- Discover Nodes
- Configure Discovery
- Discovered Nodes
- View Logical Nodes
- Stop Discovery

SECTION	ICON	NAME	DESCRIPTION
Discovery		Device Nodes	This section can be started any time using start discovery process. Discovery can also be started for a single network model or a set of network models. When discovery is started, UMS will present a discovery progress screen to the user. If discovery is already in progress, then a new discovery process can not be started.
		Configure Discovery	This section allows you to configure the network model and the discovery cycle.
		Discovered Nodes	This section allows you to view list of discovered nodes in UMS.
		View Logical Nodes	This section displays the <i>Nodes Identifier</i> , <i>Device Type</i> and <i>Protocol Name</i> .
		Stop Discovery	This section allows you to stop discovery at any time through stop discovery process. When stop discovery is clicked, the discovery that was started previously will be stopped.

Discover Node



Discovery can be started any time using start discovery process. Discovery can also be started for a single network model or a set of network models. When discovery is started, UMS will present a discovery progress screen to the user.

Note: If discovery is already in progress, then a new discovery process can not be started.

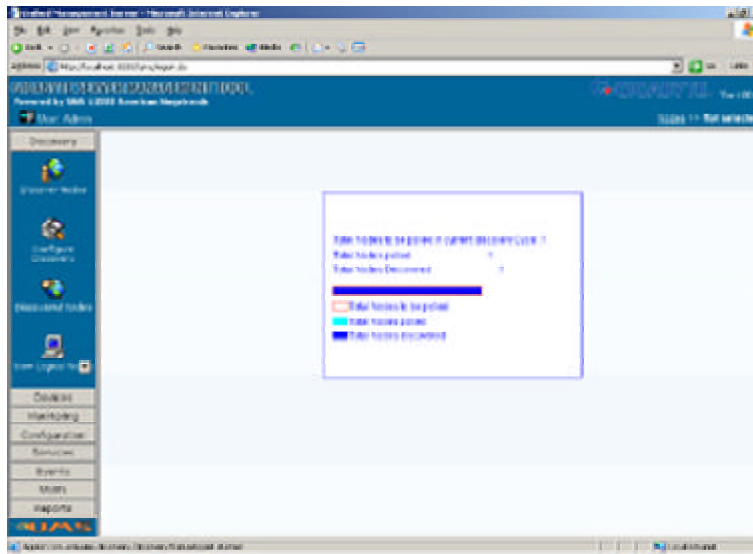
Fields	Description
Network Model	This field displays the name of the network Model.
Network IP	This field displays the IP address of the Network.
Network Mask	This field displays the Network Mask of the Network.
Start IP	This field displays the address to start discovery in the given Network.
End IP	This field displays the address to end discovery in the given Network.
Discover	This field includes the given Network Model in discovery by default.

Start Discovery

The Start Discovery button allows you to start discovery process.

Click on the **Start Discovery** button to start discovery process.

When you click on the Start Discovery button, the following screen appears:



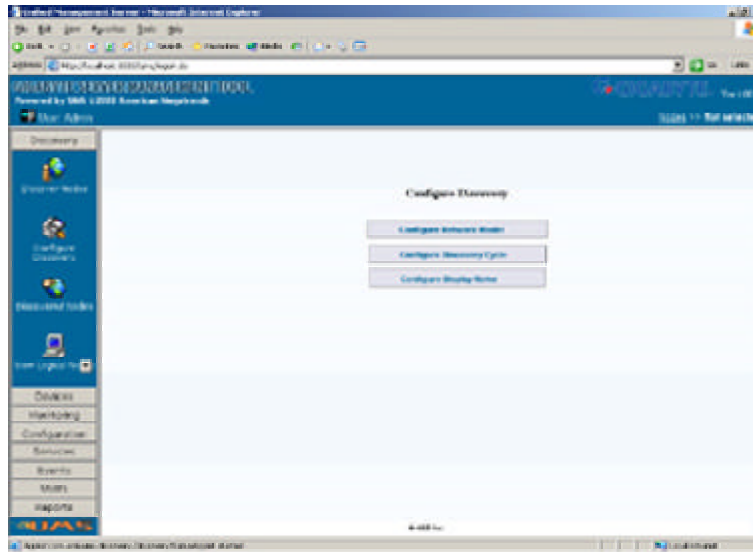
Click on the **Reset** button to reset the discovery process of a network model.

Reset

Name	Description
Total Nodes to be Pulled	Count for total number of nodes to be polled.
Total Nodes Pulled	Count of number of nodes polled.
Total Nodes Discovered	Count of number of nodes discovered currently

Configure Discovery

This feature allows you to configure the network model and the discovery cycle.



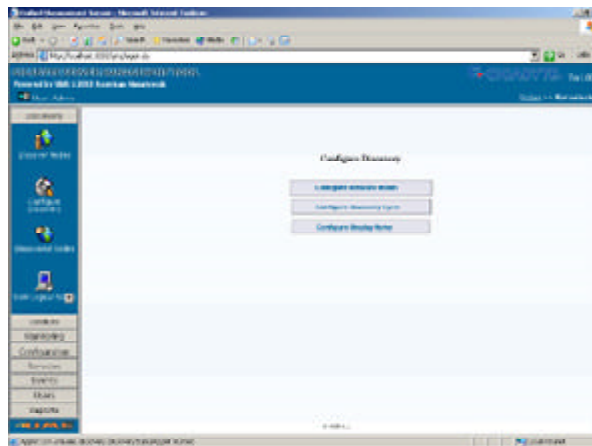
Name	Button	Description
Configure Network Model	Configure Network Model	Click on the Configure Network Model button to add and configure a network model.
Configure Discovery Cycle	Configure Discovery Cycle	Click on the Configure Discovery Cycle button to enable the discovery configuration, rediscover already discovered nodes to set discovery cycle periods, days, hours and dates.

Note: These buttons are explained in more detail further in this section.

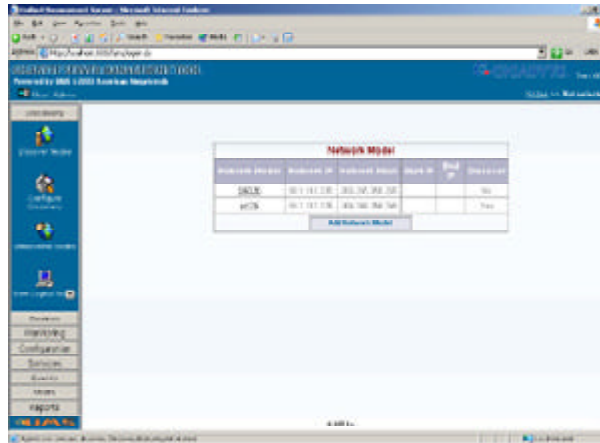
Configure Network Model

The following pictorial description shows the procedures to add and configure a network model:

Step1. Click on the **Configure Network Model** button.

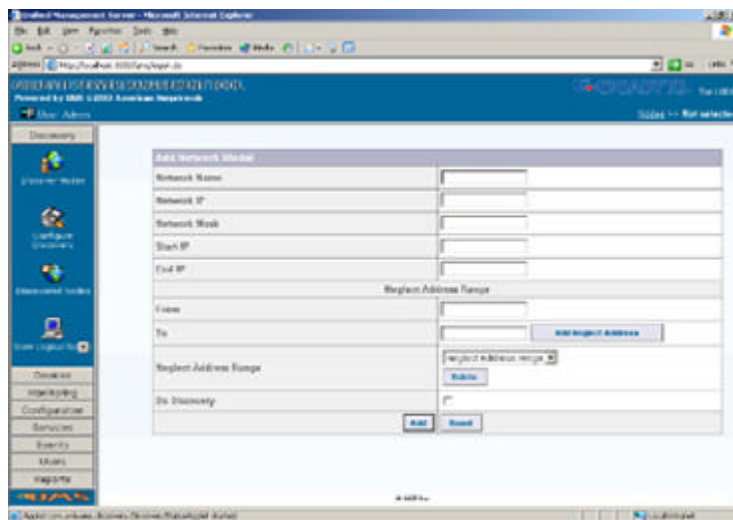


Step 2. Click on the **Add Network Model** to create a new network model.


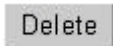

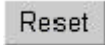


Field	Description
Network Model	This field displays the name of Network Model.
Network IP	This field displays the IP address of the Network Model.
Network Mask	This field displays the Network Mask of the Network Model.
Start IP	This field displays the IP address where the discovery process start in the Network Model.
End IP	This field displays the IP address where the discovery process ends in the Network Model.
Discover	This field reports the Network Model discovery status.

Step 3. To create Network Model needs. You must fill Network Model information such as: network IP, network mask, start IP, end IP. After filling the required network model details, click on the Add button to display the default screen.

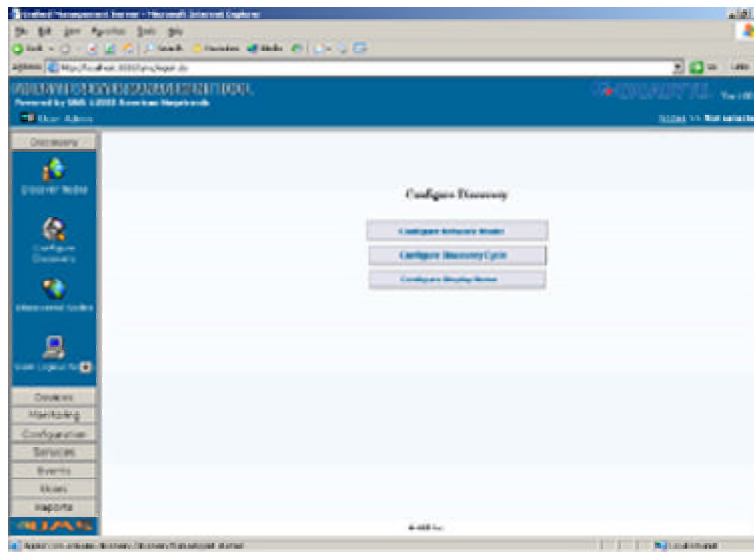


Field	Description	
Network Name	Enter the name of the Network Model	
Network IP	Enter the IP of the Network.	
Network MASK	Enter the Network MASK of the Network.	
Start IP	Enter the address to start discovery in the given Network.	
End IP	Enter the address to end discovery in the given Network.	
Neglect Address Range	From	Enter the start address to neglect in a given address range.
	To	Enter the end address to neglect in a given address range.
	Neglect Address Range	Select address range from the drop down box.
Do Discovery	Click on the Do Discovery check box.	

Field	Button	Description
Add Neglect Address		Click on Add Neglect Address button to add range of neglect addresses
Delete		Click on Delete button to remove specific neglect address range.
Add		Click on Add button to create network model.
Reset		ClickReset button allows you to clear values entered.

Configure Discovery Cycle

Step1. Click on the Configure Discovery Cycle button.

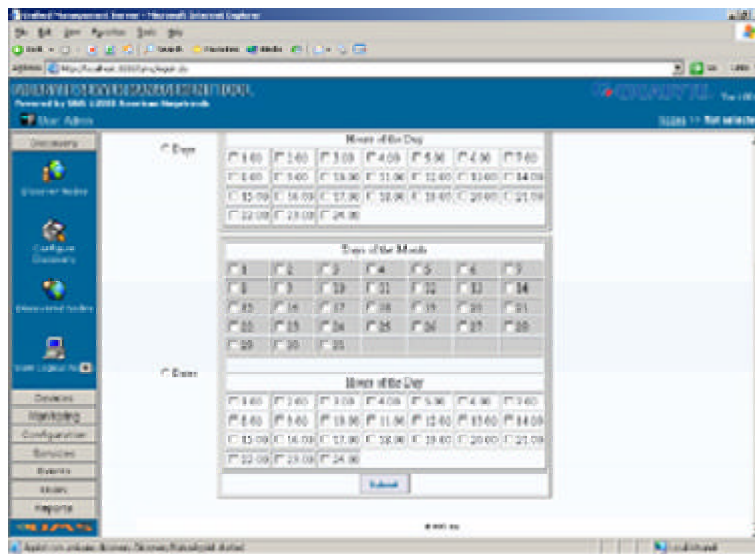


This subsection allows you to enable the discovery configuration, rediscover already discovered nodes and to set discovery cycle periods, days, hours, and dates.

Step 2. Using the discovery schedule, you can specify when to start the discovery process.

For instance:

You can select the day of the week, specified time and a periodic interval to start a discovery process.

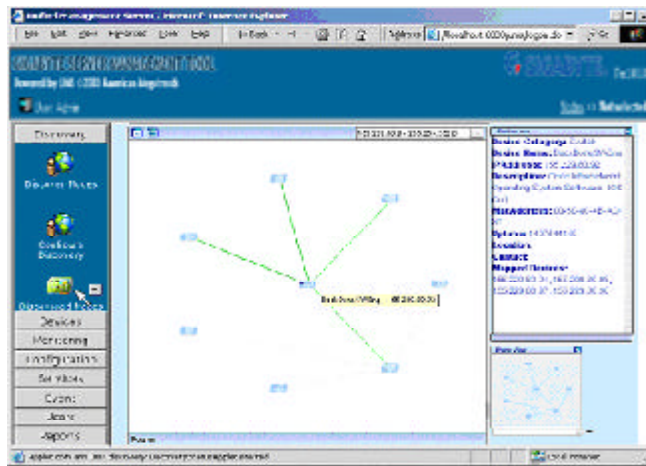


Options	Description
Enabled	This option allows you to enable the auto discovery. Notes: The Enable option allows you to enable network models auto discovery based on the selected time interval.
Rediscovered	This option allows you to enable the auto discovery to discover already discovered nodes. Note: The Rediscovered option allows you to enable network models auto discovery for the discovered nodes.
Periodic (hourly)	Select this option to specify discovery in time interval of hours.
Days (weekly)	Select this option to specify discovery in time interval of days and hours.
Dates (monthly)	Select this option to specify discovery in time interval of dates and hours.

Step2-1. Click on **Submit** button to add a new discovery cycle changes.

Discover Nodes

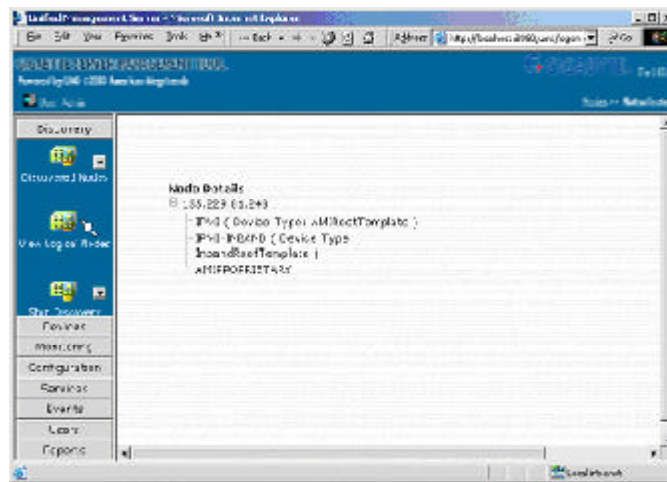
The feature allows you to view list of discovered nodes in GSMT and information on each specific node.



View Logical Nodes

The feature allows you to view the various protocols that are supported by a single node.

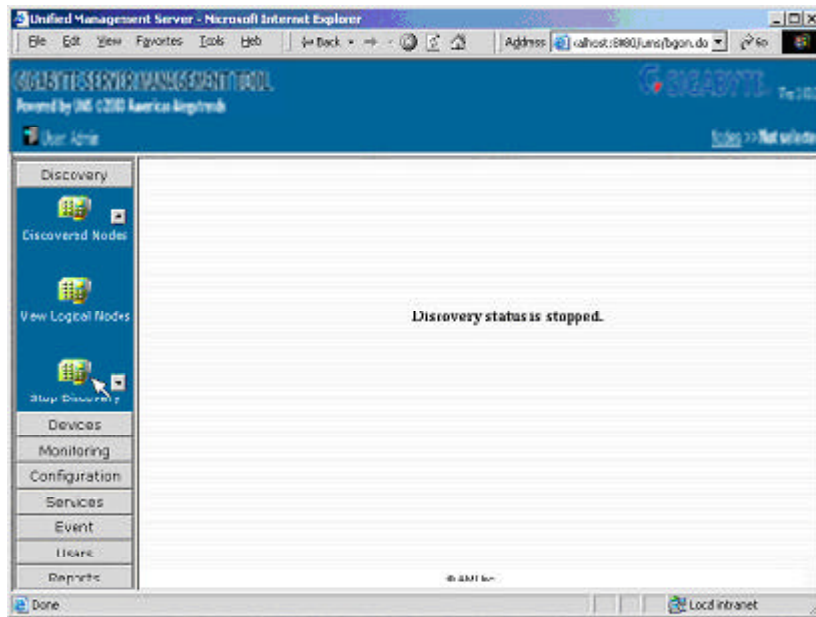
Note: A node is considered logical node if it supports more than one protocol.



Field	Description
Node Details	This field displays details of the managed nodes. Note: Node Details include supported protocols (SNMP, IPMI-INBAND) as well as device type.

Stop Discovery

The privileged allows you to stop discovery at any time through stop discovery process. When you click on the Stop Discovery icon, the discovery that was started previously will be stopped.










UMS Device

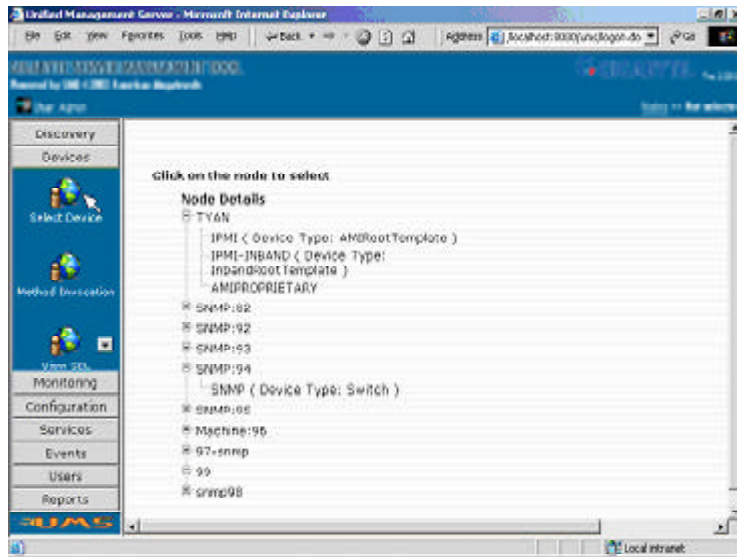
The UMS Devices feature allows you to set any managed device to be the current one. Also, you can use the following subsections:

- Select Device
- Method Invocation
- View SEL
- View FRU
- Unmanage Node
- Unmanage Template Node
- Select Device Type

Each subsection is explained in more detail further in this section.

Section	Icon	Name	Description
Devices		Select Device	This section allows you to select a device. A list of discovered device will be displayed. After selecting the device and clicking on [Enter], the selected device will be the current device.
		Method Invocation	This section allows you to invoke a method on a selected device remotely.
		View SEL	This section allows you to view and clear the BMC event log. The event log is a repository system events and certain system configuration information. The event log displays information such as attribute values going out of range, BIOS post messages, and so on.
		View FRU	This section provides support for accessing multiple sets of non-volatile FRU information. User will typically access information for each major system board (for example: Processor board, memory board, I/O board and etc.) The FRU data includes information such as serial number, part number, model and asset tag. This information is available even when the system is powered down.
		Unmanage Nodes	This section allows you to delete template nodes.
		Unmanaged Template Nodes	This section allows you to delete a template nodes.
		Select Device	This section allows you to select a template nodes.

Select Device



This feature allows you to select a device, under device, left click on the SelectDevice icon. A list of discovered device will be displayed. After selecting the device and clicking on enter, the selected device will be the current device.

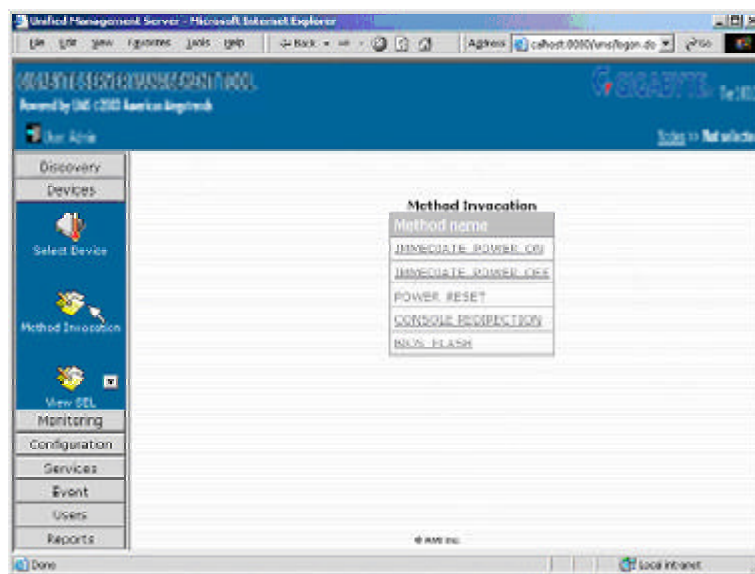
Field	Description
Nodes Details	This field displays the manage node IP that supports protocol (SNMP, IPMI, IPMI-INBAND) using device type.

Method Invocation

This feature allows you to monitor and remotely manage network servers and systems. By using this features, you can perform many recovery and diagnostic actions such as power on/off/reset, BIOS flashing and running the remote diagnostic programs.

Note: Invoked methods depend on the selected protocol as explained below:

Method Invocation (IPMI-Protocol)

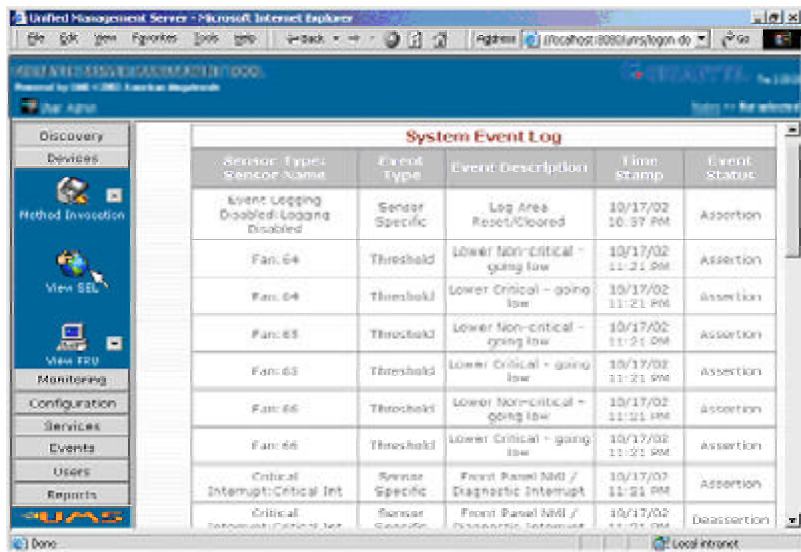


Field	Description
Method Name	This field displays the name of the method to invoke.
Immediate Power On	This field allows you to power on the selected node.
Immediate Power Off	This field allows you to power off the selected node.
Power Reset	This field allows you to reset power on the selected node.
Console Redirection	This field allows you to start console redirection.
BIOS Flash	This field allows you to flash the firmware on the selected node.

View SEL

This feature allows you to view the BMC event log. Left click on the View SEL to display list of all logged events.

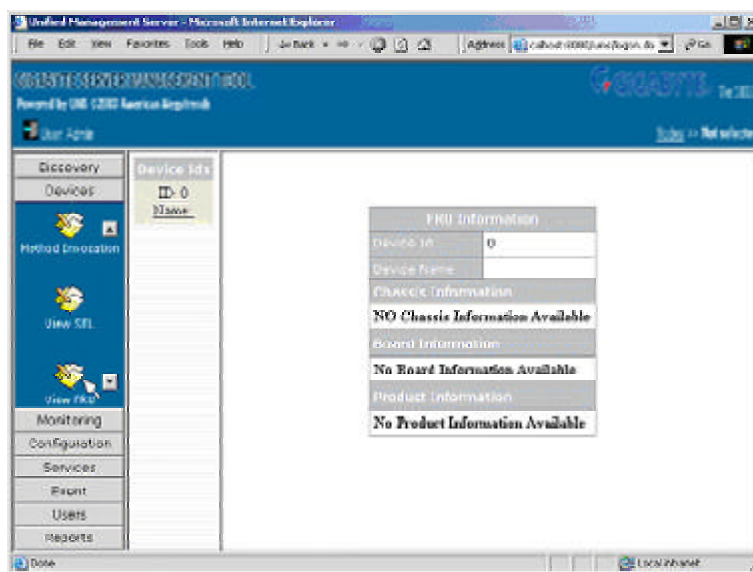
Note: The event log is a repository for system events and certain system configuration information. The event log displays information such as attribute values going out of range, BIOS post messages, and so on.



View FRU

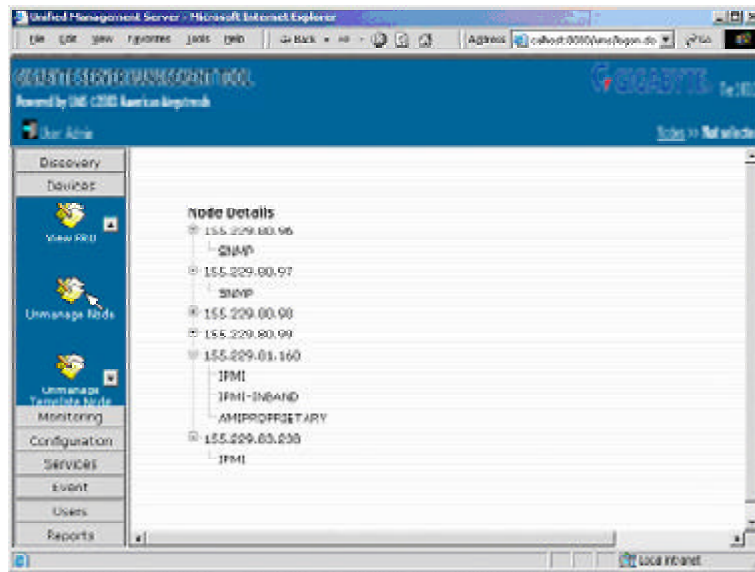
This feature provides support for accessing multiple sets of non-volatile FRU information. You can access information for each major system board (for example: Processor board and Memory board, I/O board). Left click on View FRU icon to view available FRU information.

Note: The FRU data includes information such as serial number, part number, model and asset tag. This information is available even when the system is powered down.



Unmanaged Node

This feature allows you to delete nodes that you do not want to monitor from the managed group. To delete a node, simply left click on the node to be deleted.

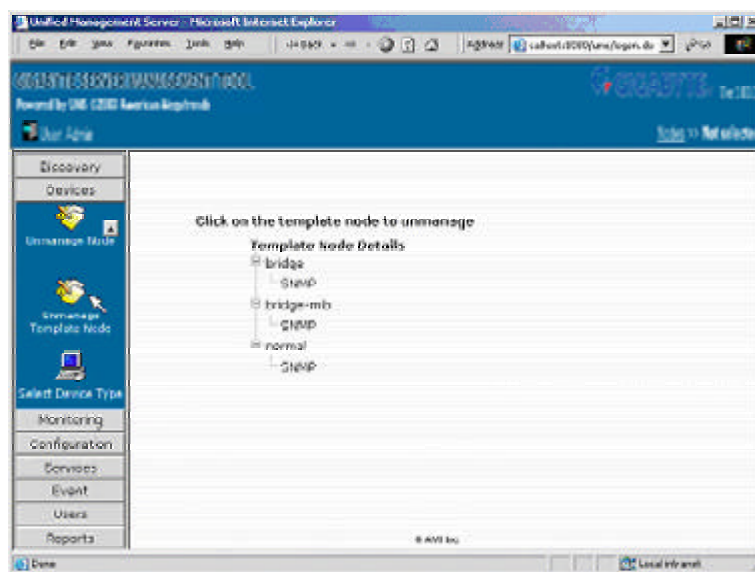


Field	Description
Nodes Details	This field displays the manage node IP that supports protocol (SNMP, IPMI, IPMI-INBAND) using device type.

Unmanaged Template Node

This feature allows you to delete template nodes that you do not want to monitor from the managed group. It displays a list of all available template nodes. To delete a template node, simply left click on the node to be deleted.

Note: Currently, the UMS utility supports four types of templates: (In-band Root Template, AMI Root Template, Root Template and Switch).

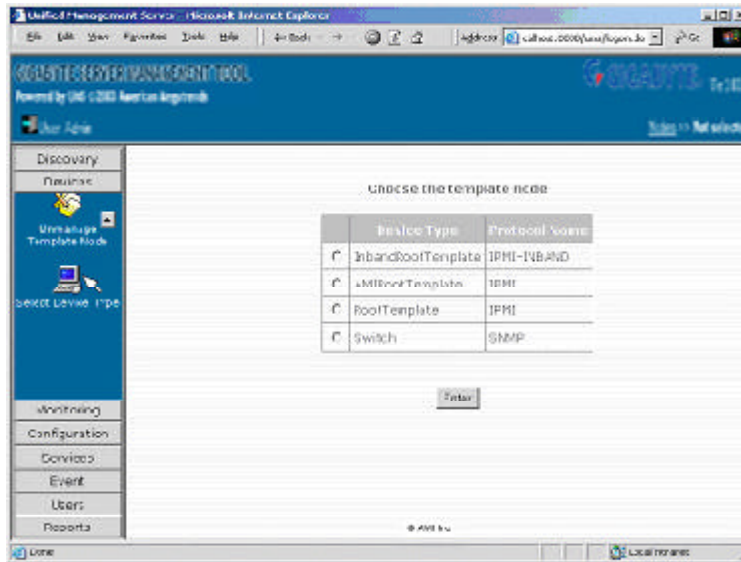


Select Device Type


After a node is created, it is associated with one of three different default root templates. The three templates are defined in the table below:

Template	Description
AMI Root Template	The AMI Root Template means the discovered node is an AMI BMC. Note: AMI BMC will support features such as console redirection and BIOS flashing.
Root Template	The Root Template means that the discovered node is BMC node.
Inband Root Template	The Inband Root Template means the discovered node is in an AMI BMC (Inband).
Switch	The Switch means the discovered node is an SNMP node.

This feature allows you to select a template node.



Field	Description
Device Type	This feature displays device type.
Protocol Name	This field displays the protocol name used to manage the selected node.







Name	Button	Description
Device Type		Click on the Enter button to select the template node.

UMS Monitoring

The UMS Monitoring feature allows you to view and configure a list of attributes of monitored node. By using this feature, you can use the following subsections:

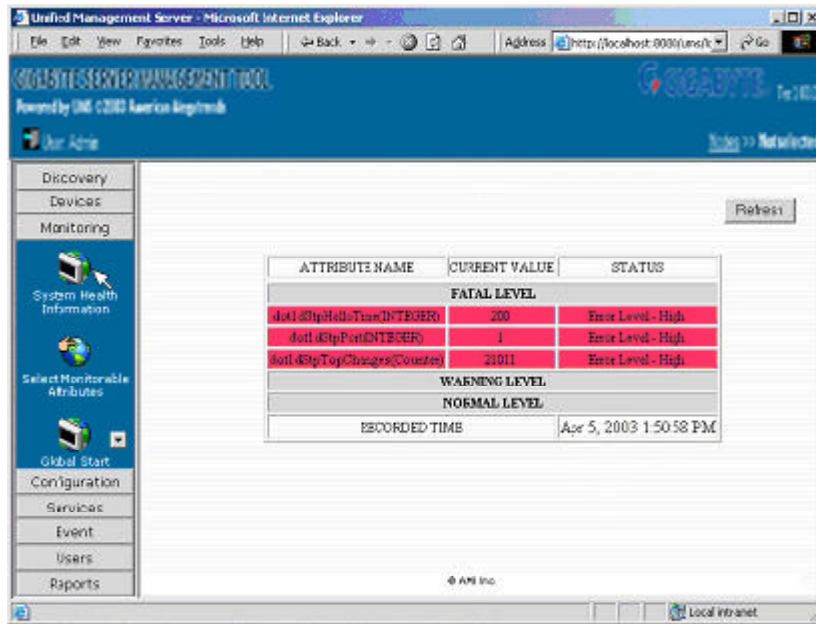
- System Health Information
- Select Monitorable Attributes
- Global Start Monitoring
- Global Stop Monitoring
- Configure Poll Interval
- View Historic Data

Each subsection is explained in more detail further in this section.


Section	Icon	Name	Description
Monitoring		System Health Information	This section allows you to view the list of attributes that are marked as candidate for monitoring for a given node or template.
		Select Monitorable Attributes	This section allows you to select attributes to be monitored of the selected node.
		Global Started Monitoring	This section facilitates restart of the monitoring in case its globally stopped. Monitoring of any of the attribute on any node could be done only if monitoring is globally started.
		Global Stopped Monitoring	This page facilitates you to globally stop monitoring. None of the attributes of any node will be monitored if the monitoring is globally stopped.
		Configure Poll Interval	This section shows you how frequently the attributes should be polled. You are allowed to configure this interval. Note: This sampling time is always the multiple of this poll interval.
		View Historical Data	This section allows you to view historical data collected for a particular attribute for particular node.

System Health Information

This feature allows you to view the list of attributes that are marked as candidate for monitoring for a given node or template.

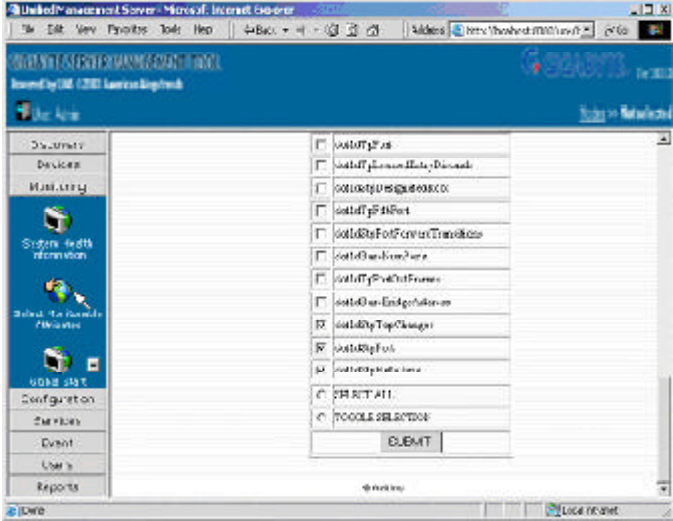


Field	Description
Attribute Name	This field displays the attribute name.
Current Value	This field displays the attribute current value.
Status	This field displays the attribute status.
Fatal , Warning, Normal Levels	These fields display severity levels based on attribute values.
Recorded Time	This field displays the time of attribute value collection.

Name	Button	Description
Refresh		Click on the Refresh button to get the latest attribute values.

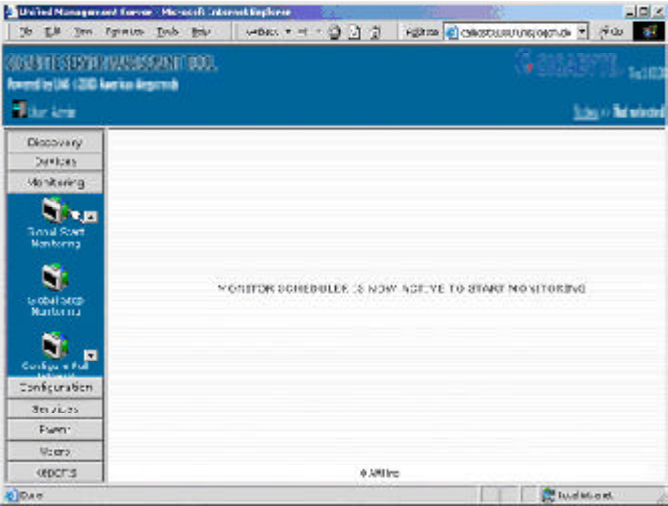
Select Monitorable Attributes

This feature allows you to select attributes to be monitored of the selected node.



Global Start Monitoring

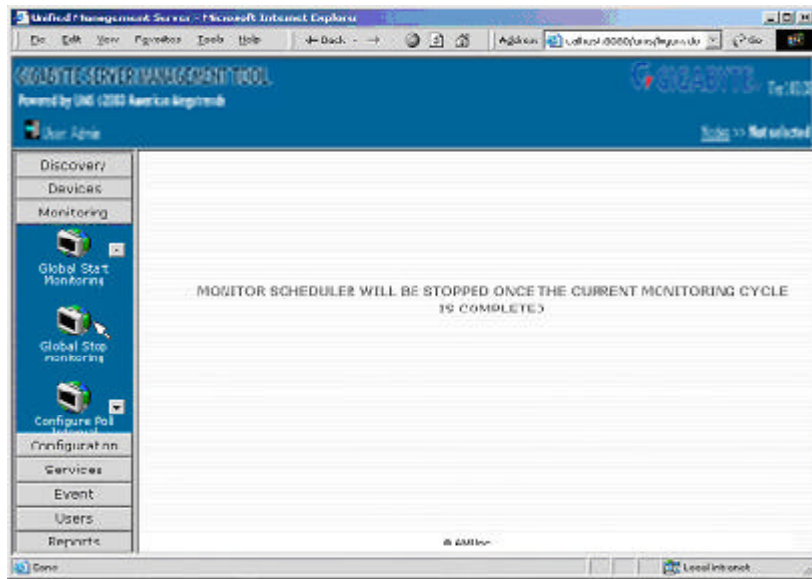
This feature facilitates restart of the monitoring incase it is globally stopped. Monitoring of any of the attribute on any node could be done only if monitoring is globally started.



Global StopMonitoring

This feature allows you to globally stop monitoring. None of the attributes of any node will be monitored if the monitoring is globally stopped.

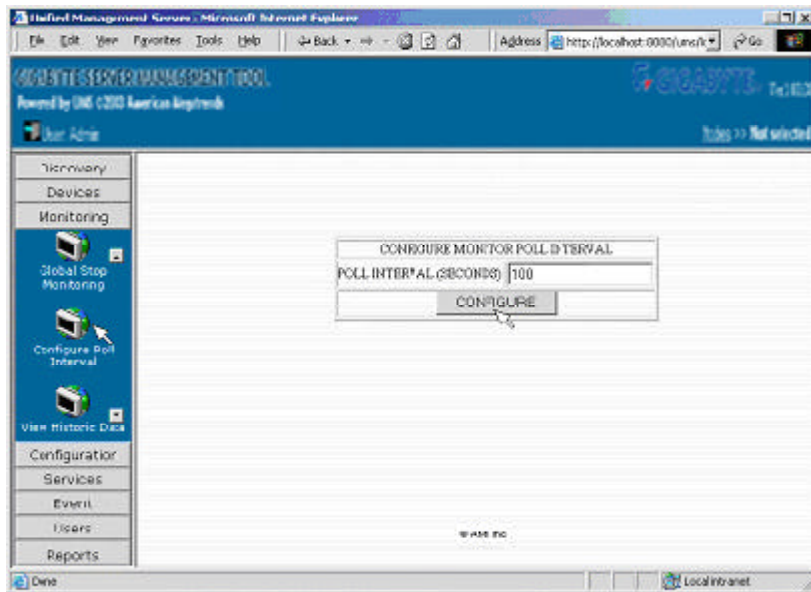
Note: Node attributes are not monitored if global monitoring is stopped.




Configure Poll Interval

This feature shows you how frequently the attributes should be polled. You are allowed to configure this interval.

Note: The sampling time is always the multiple of this poll interval.



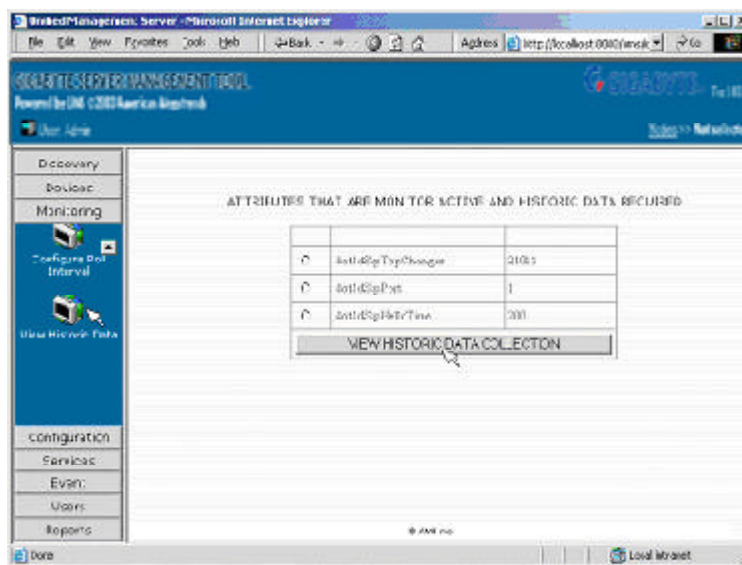
Field	Description
Poll Interval (Seconds)	This field allows you to enter poll interval number.

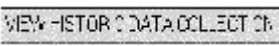
Name	Button	Description
Configure		Click on the Configure button to configure monitor poll interval.

View Historical Data

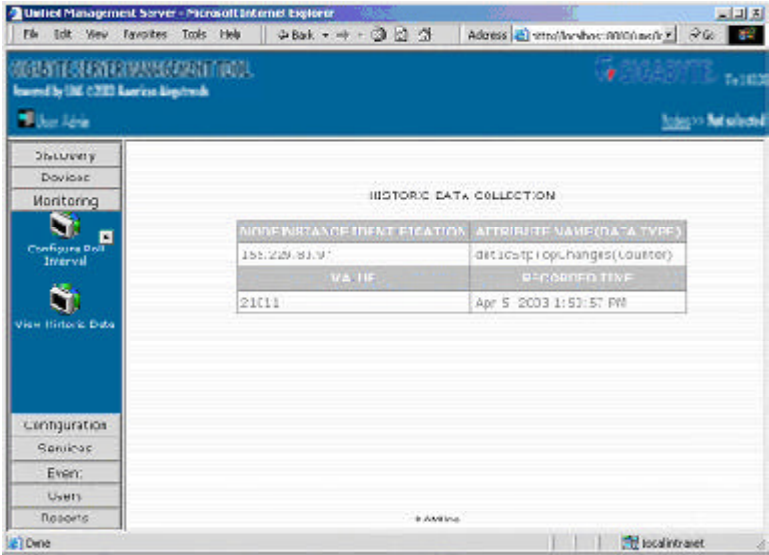
This feature allows you to view historical data collected for a particular attribute for particular node.

Note: You can view all attributes of the current node that have been selected for historical data collection.



Name	Button	Description
View Historic Data Collection		Click on the View Historic Data Collection button to view historic data collection for the selected attribute.

After you click on the View Historic Data Collection button, the following screen appears:






Field	Description
Node Instance Identification	This field displays node instance identification.
Attribute Name (Data Type)	This field displays name and data type.
Value	This field displays attribute value.
Recorded Time	This field displays time of collected attribute value.

UMS Configuration

The UMS Configuration feature allows you to configure monitoring definitions, IPMI commands and the mail server. By using this feature, you can use the following subsections:

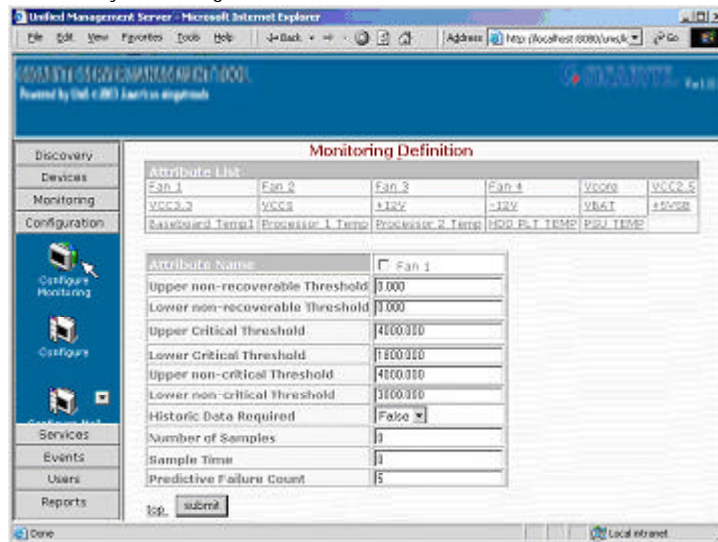
- Configure Monitoring
- Configure
- Configure Mail Server

Each subsection is explained in more detail further in this section.


Section	Icon	Name	Description
Configuration		Configure Monitoring	This section allows you to configure the monitoring definition of a certain attribute that belongs to the current device (node) in the session.
		Configure	This section allows you to configure the parameter attributes of IPMI Commands that are configurable. Currently implemented for LAN and PEF.
		Configure Mail Server	This section allows you to configure mail server details.

Configure Monitoring

This feature allows you to configure certain attributes definitions of the current selected device.



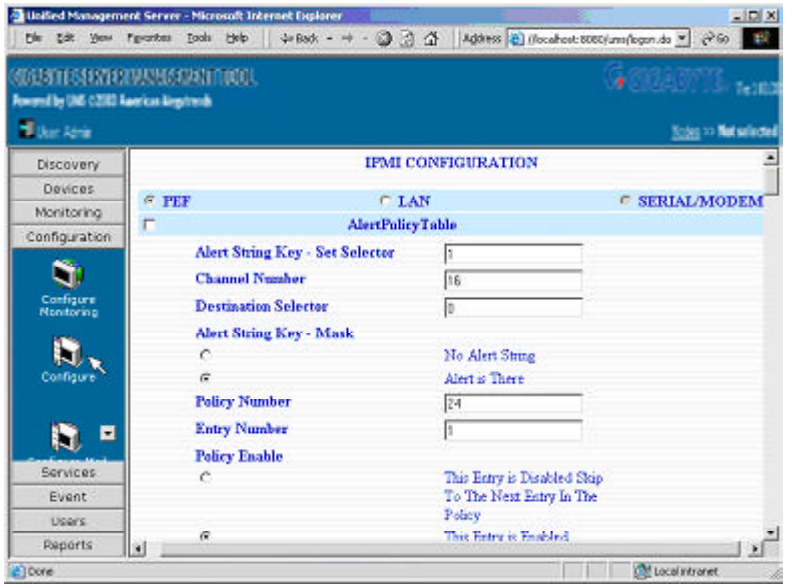
Field	Description
Attribute Name	This field displays the attribute name.
Upper non-recoverable Threshold	This field allows you to configure monitoring of the attribute for Upper non-recoverable Threshold.
Lower non-recoverable Threshold	This field allows you to configure monitoring of the attribute for Lower non-recoverable Threshold.
Upper Critical Threshold	This field allows you to configure monitoring of the attribute for Upper Critical Threshold.
Lower Critical Threshold	This field allows you to configure monitoring of the attribute for Lower Critical Threshold.
Upper non-critical Threshold	This field allows you to configure monitoring of the attribute for Upper non-critical Threshold.
Lower non-critical Threshold	This field allows you to set the lower non-critical threshold value for the selected attribute.
Historical Data Required	This field displays whether historical data collection is required.
Number of Samples	This field displays the number of samples to be collected.
Sample Time	This field displays the time interval to collect samples for the selected attribute.
Predictive Failure Count	This field allows you to specify number of monitoring cycles that can be used to predict an attribute failure.

Name	Button	Description
Submit		The Submit button allows you to update new sensor values for the selected attribute.

Configure

This feature allows you to configure parameter attributes of the IPMI commands.

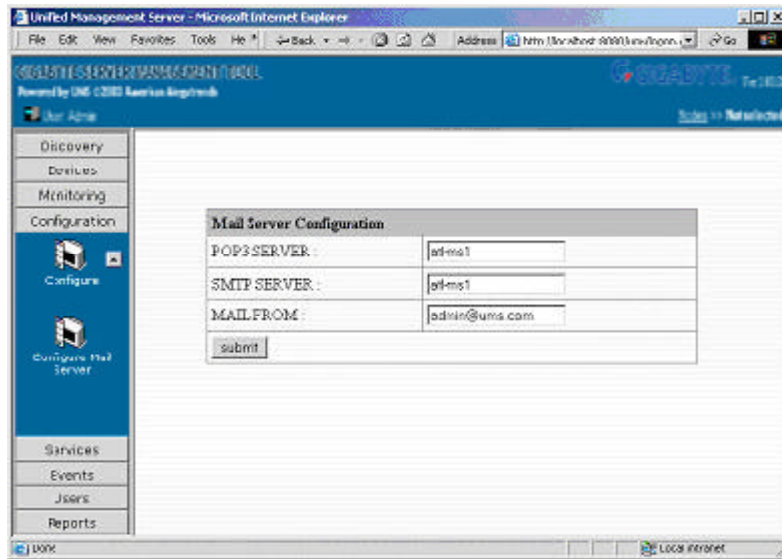
Note: Currently, the UMS utility supports configuring LAN, PEF and Serial/Modem parameters attributes.



Field	Description
PEF	This option allows you to configure IPMI PEF related parameters.
LAN	This option allows you to configure IPMI LAN related parameters.
Serial/Modem	This option allows you to configure IPMI Serial/Modem related parameters.

Configure Mail Server

This feature allows you to configure mail server details. Left click on the Submit button to configure the mail server.



Field	Description
POP Server	This field allows you to enter the name of POP3 server.
SMTP Server	This field allows you to enter the name of SMTP server.
Mail From	This field allows you to enter the administrator mail Id.




Name	Button	Description
Submit	<input type="button" value="Submit"/>	Click on the Submit button to update configure mail server.

UMS Service

The UMS Services feature allows you to load services, compile loaded files and send IPMI commands. By using this feature, you can use the following subsections:

- Load Services
- Compile Files
- IPMI Conformance Tool

Each subsection is explained in more detail further in this section.

Section	Icon	Name	Description
Service		Load Services	This section allows you to load services
		Compile Files	This section allows you to compile the loaded files and associate device type with it.
		IPMI Conformance Tool	This section provides a means to send IPMI commands to BMC. You can send commands using an in band interface. GSMT also provides screens for giving input parameters for each command. GSMT contrasts a request packet with the input given by the BMC forwarding it back to the client.

Load Service

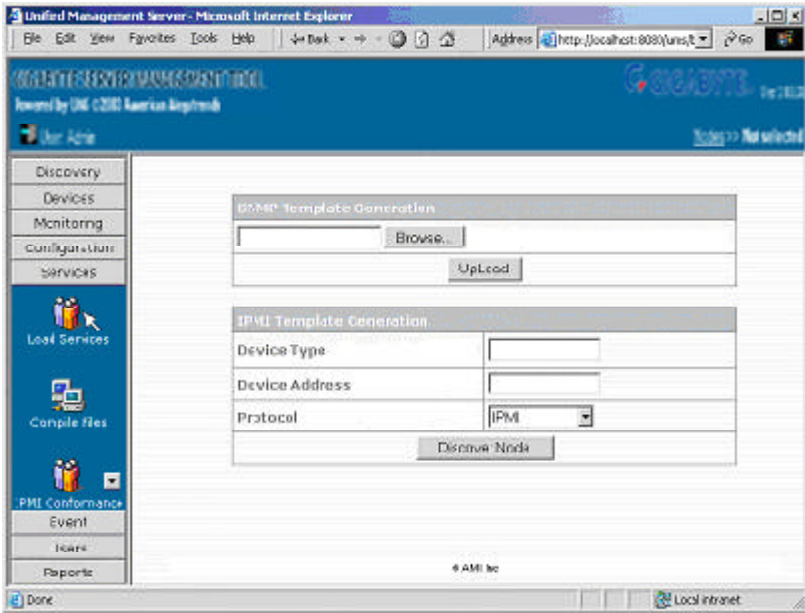
This feature allows you to load service and create IPMI template.

To generation an IPMI template, follow the steps outlined below:




Step1. Specify the device type name, IP address and the protocol type (IPMI or INband) to create the template node.

Step2. UMS will discover the node and create the template.

Note: You can change the threshold values of the attribute by going to Configuration \ Configure Monitoring page. Also the attributes to be started for monitoring can be set.

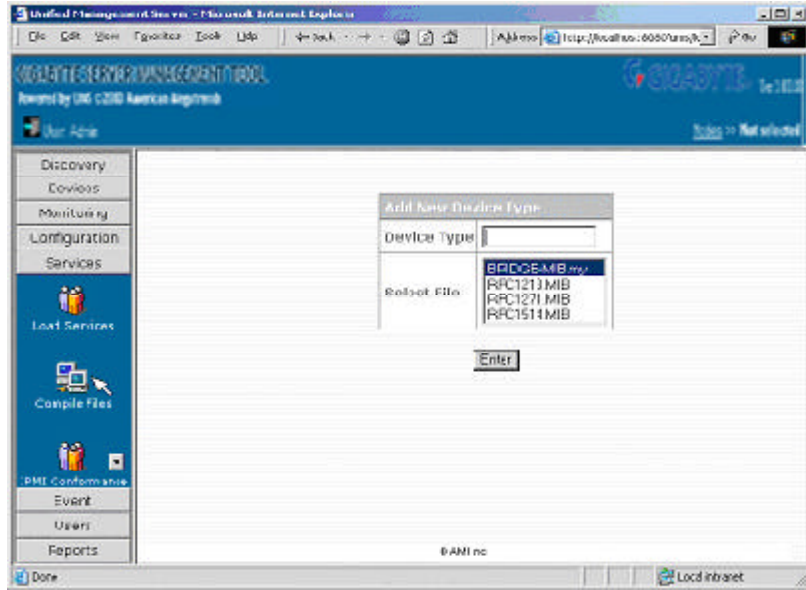


Field	Description	
SNMP Template Generation	This field allows you to enter the file name or left click on the Browse button to select the file to be loaded.	
IPMI Discovery	Device Type	This field allows you to enter the Device Type name.
	Device Address	This field allows you to enter the Device Address.
Protocol	This field displays the protocol name used to manage the selected node.	


Name	Button	Description
Browse		Click on the Browse button to select the file to upload.
Upload		Click on the Upload button to upload the selected file.
Discover Nodes		Click on the Discover Node button to discover IPMI node.

Compile Files

This feature allows you to compile the loaded files and associate device type with it.



Field	Description	
Add New Device Type	Device Type	This field allows you to enter a Device Type name.
	Select File	This field allows you to select a File to be used by this Device Type.

Name	Button	Description
Enter		Click on the Enter button to compile files.

Compile Files, Continued

To edit the correct path where files are to be compiled, follow the steps outlined below:

Step1. Stop the UMS server (if it is currently running).

Step2. Open the file named 'ums-service.xml' located under <JBoss>/server/default/deploy

Step3. Edit the Directory Path

```
<mbeancode="com.ami.ums.mib.MibCompiler" name="ums:service=MIBCompiler">
<attribute name="DirectoryPath">[Path where the mib files are located]</attribute></mbean>
```

Example:

```
<mbeancode="com.ami.ums.mib.MibCompiler" name="ums:service=MIBCompiler"> <attribute
name="DirectoryPath">C:/AMI/UMS/jboss-3.0.0_tomcat-4.0.3/bin</attribute></mbean>
```

Step10. Save the new changes that you have made, and restart the UMS server.

IPMI Conformance Tool

This feature allows you to send IPMI commands to the BMC. You can send commands using an in-band or out-of-band interface.

Note: The USM utility prompts you to enter input parameters for each IPMI command to be executed. After the input is correctly entered, then the UMS utility sends the IPMI command to the BMC of the managed node.

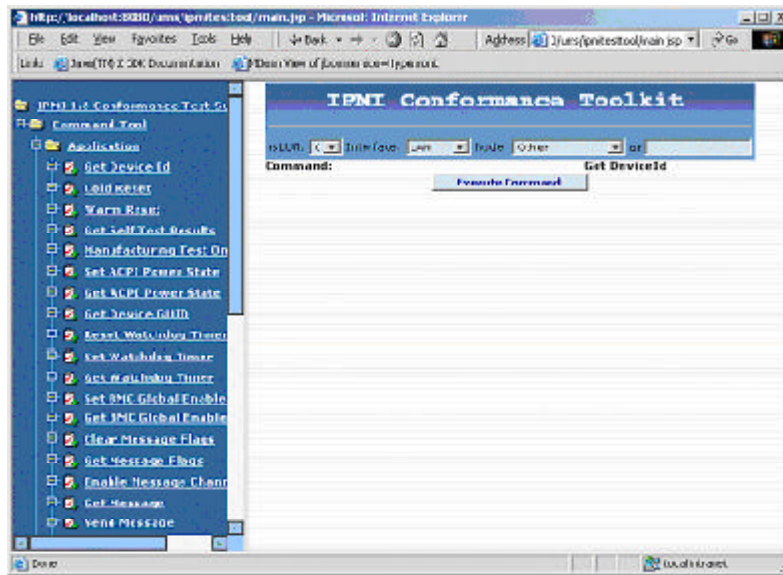
To run IPMI Command Tool, follow the steps outlined below:

Step1. Click on any one of the IPMI commands from the left frame.

Step2. On the main page, select the interface type as (LAN or in-band) and the node address (from the drop down box).

To select a node that is not present in the nodes drop down box, select Other and then enter the designed IP address in the edit box.

Step3. Click on the execute command to execute the selected IPMI command.






UMS Events

The UMS Events feature allows you to view and modify actions associated with events. By using this feature, you can use the following subsections:

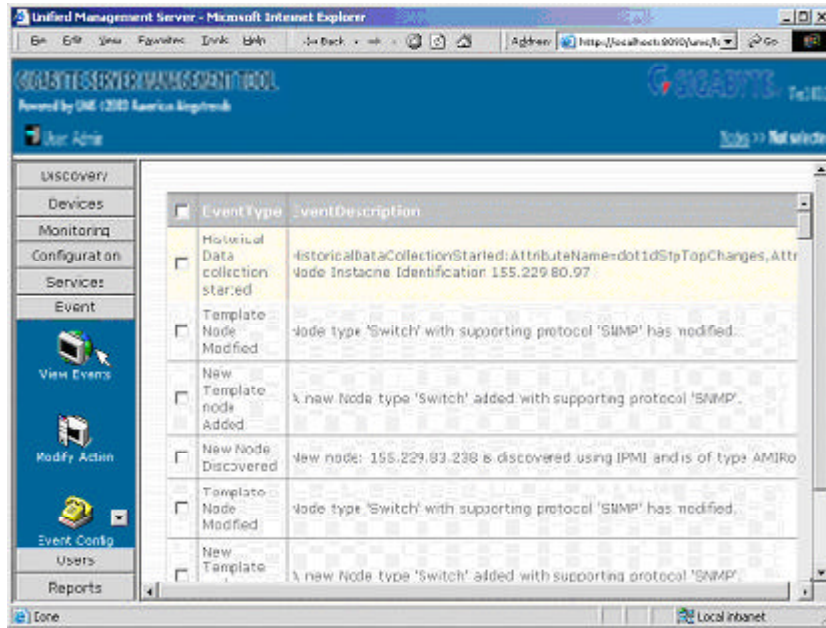
- View Events
- Modify Action
- Event Config

Each subsection is explained in more detail further in this section.

Section	Icon	Name	Description
Events		View Events	This section allows you to view the event occurred in UMS.
		Modify Action	This section allows you to modify actions associated with events.
		Event Config.	This section allows you to configure events.

View Events

This feature allows you to view the events occurred in UMS.

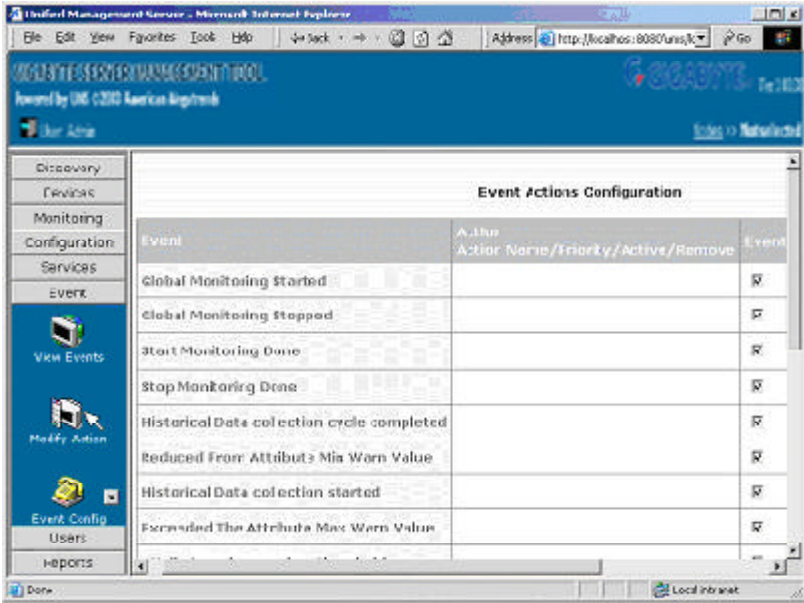


Field	Description
Event Type	This field displays the event type.
Event Description	This field describes the event that is generated.
Event Generator	This field gives the details of the origin of the event.
Event Severity	This field displays the severity of the event.
Event Generated Time	This field displays the time of generation of the event.

Note: You can click on the check box to knowledge, clear acknowledges or clear all events.


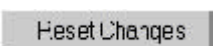
Modify Action

This feature allows you to modify actions associated with events.

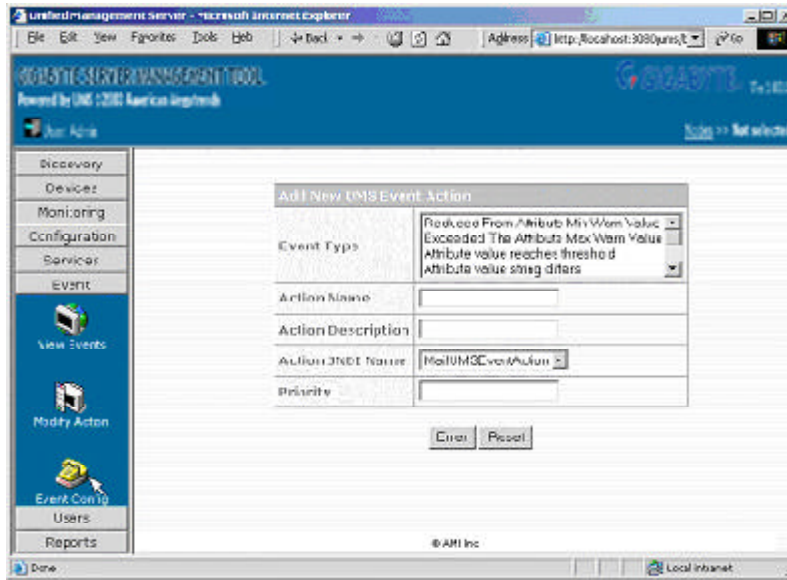


Event Actions Configuration

Field	Description
Event	This field displays the event name.
Action/Action Name/Priority/Active	This field displays the action name associated with the event.
Event	Click on the check box to select the event action.

Name	Button	Description
Save Changes		Click on the Save Changes button to save the changes you have made.
Reset Changes		Click on the Reset Changes button to uncheck all check boxes.



Event Config



Add New UMS Event Action

This feature allows you to add and action for particular UMS event.

Field	Description
Event Type	This field allows you to select event type.
Action Name	This field allows you to enter an action name to be associated with this event.
Action Description	This field allows you to enter a description of the action.
Action JNDI Name	This drop down box allows you to select JNDI name to be associated with the action.
Priority	This field allows you to enter a priority of the event.






Name	Button	Description
Enter		Click on the Enter button to save the event action.
Reset		Click on the Reset button to clear all input values.

UMS User

The UMS Users feature allows you to view and modify users access rights. By using this feature, you can use the following subsections:

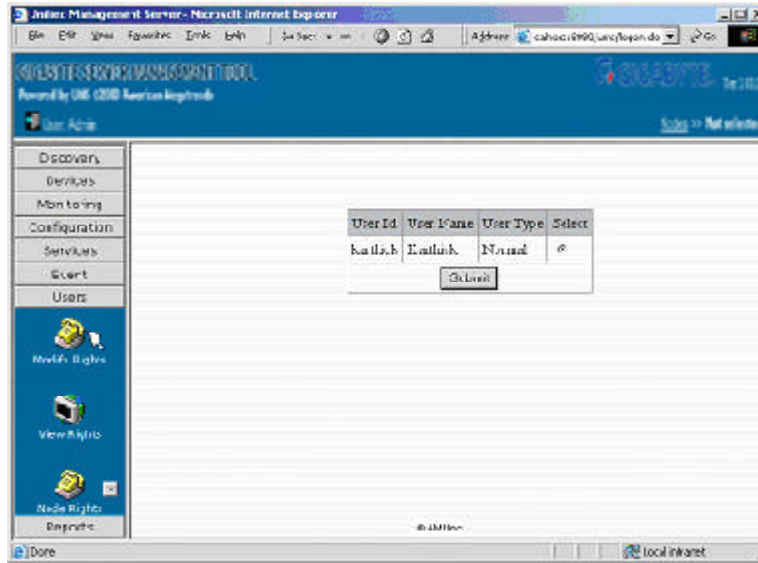
- Modify Rights
- View Rights
- Node Rights
- User Profile
- User Accept

Each subsection is explained in more detail further in this section.


Section	Icon	Name	Description
User		Modify Rights	This section allows you to modify rights associated to a user.
		View Rights	This section allows you to view rights associated to users.
		Node Rights	This section allows you to associated node to users.
		User Profile	User section allows you to view or modify your profile but not access permission using user profile option.
		User Accept	This section allows you to accept users.

Modify Rights

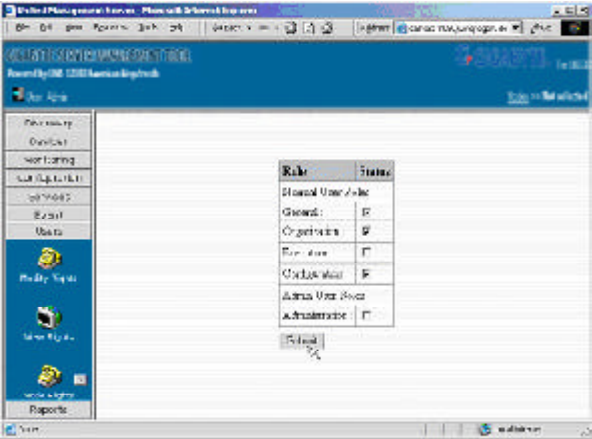
This feature allows you to modify rights associated to a user.



Field	Description
User Id	This field displays the user identification.
User Name	This field displays the user name.
User Type	This field displays the user type (Normal /Admin).
Select	This option allows you to select the user. Note: Only one user can be selected.

Name	Button	Description
Submit		Click on the Submit button to select the user.

The following screen appears when you click on the Submit button.



The system administrator assigns roles to the UMS users. The UMS utility supports five roles. To select a role, click on any of the check boxes. The access permissions for each role is defined as below:


Role	Description	
General	The General role allows you to access UMS general features such as viewing data. The following shows UMS features that are available by assigning the general role to a user.	
	UMS Features	
	Module	
	Discovered Nodes	Discovery Module
	Select Devices	Devices Module
	User Profile	User Module
	View Events	Event Module
	System Health Information	Monitoring Module
	View SEL	Device Module
	View FRU	Device Module
	Modify Action	Events Module
	Event Config	Events Module
View Logical Nodes	Discovery Module	

Continued...

Role	Description
Organization	The Organization role allows you to control UMS node independent tasks. The following shows UMS features that are available by assigning the organization role to a user.
	UMS Features
	Load Services
	Compile Files
Execution	The Execution role allows you to perform UMS execution operations. The following shows UMS features that are available by assigning the execution role to a user.
	UMS Features
	Start Discovery
	Stop Discovery
	Configure Discovery
	Method Invocation
Configuration	The Configuration role allows you to perform any of the UMS configuration operations. The following shows UMS features that are available by assigning the configuration role to a user.
	UMS Features
	Configure Monitoring
	Configure
	Configure Mail Server
	Select Device Type
	Select Monitorable Attribute
	View Historic Data
	Conformance Tool
	Historic Data Files

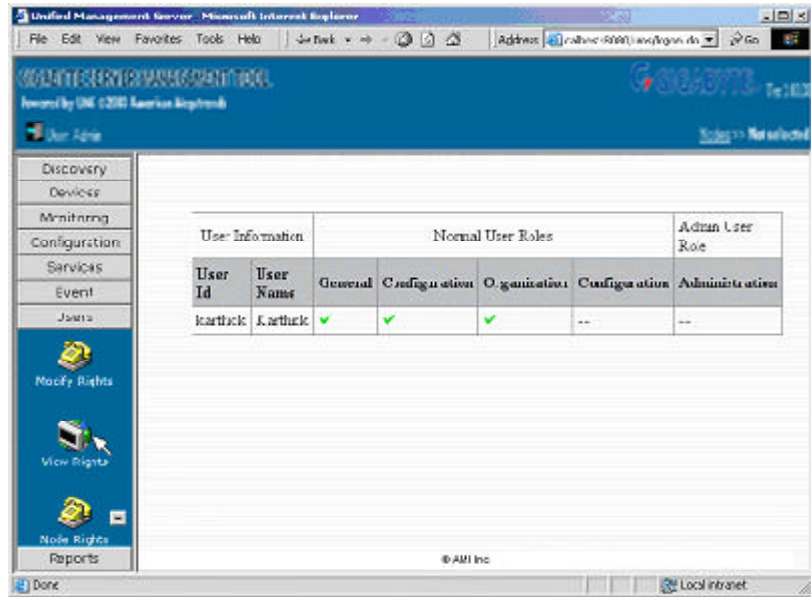
Continued...

Role	Description	
Administration	The Administration role provides you with full access to the UMS features. The following shows UMS features that are available by assigning the administration role	
	UMS Features Module	
	Unmanage Node	Devices Module
	Unmanage Template Node	Devices Module
	Global Start Monitoring	Monitoring Module
	Global Stop Monitoring	Monitoring Module
	Config Poll Interval	Monitoring Module
	Modify Rights	User Module
	View Rights	User Module
	User node Rights	User Module
	User Accept	User Module
	IPMI User Update	User Module
	Delete User	User Module

Name	Button	Description
Sumit		Click on the Submit button to assign role to a user.

View Rights

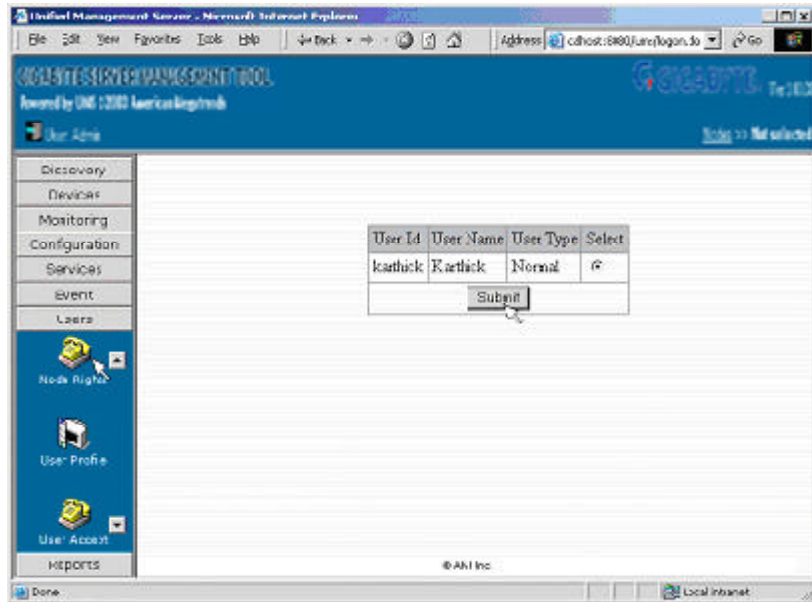
This feature allows you to view rights associated to users.




Field	Description
User Information	This field displays user information, such as user ID, username, normal user roles and administration if available.
Normal User Roles	This field displays the roles that can be assigned to a normal user such as General, Configuration and Organization.
Admin User Role	This field displays roles that can be assigned to an administrator user such as administration.

Node Rights

This feature allows you to associated node to users.

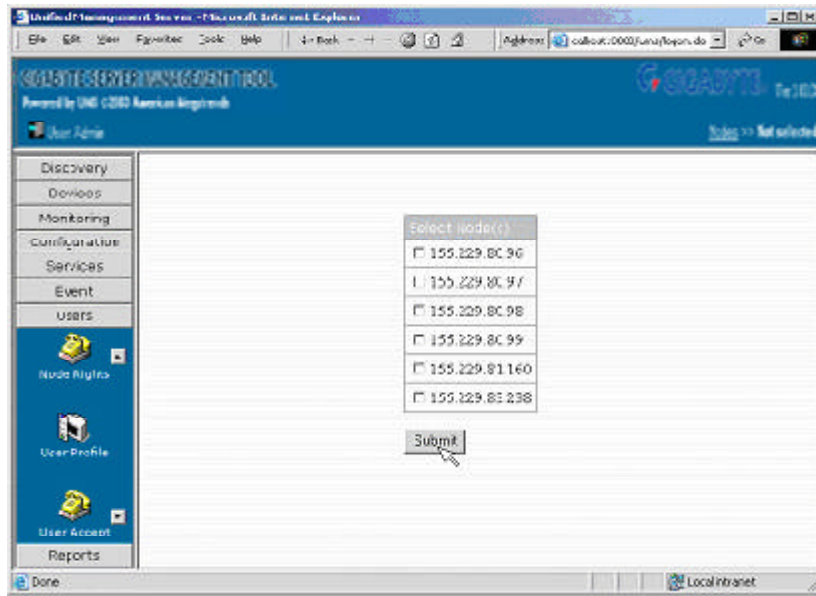


Name	Description
User Id	This field displays the user identification.
User Name	This field displays the user name.
User Type	This field displays the user type (Normal /Admin).
Select	This option allows you to select the user.

Name	Button	Description
Submit		Click on the Submit button to select the user.

The following screen appears when you left click on the Submit button.

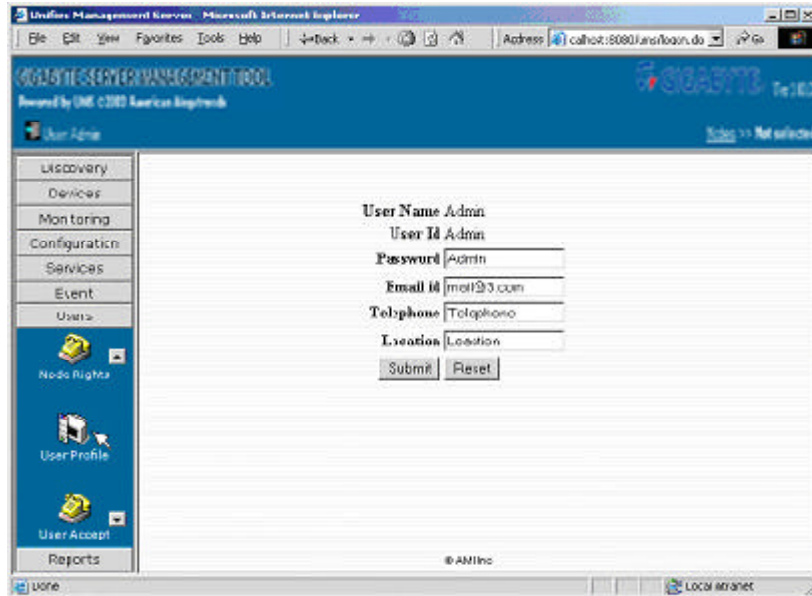
Click on any of the check boxes to select the node(s) and then, click on the Submit button to save any changes you have made.




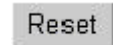
Note: You can assign more than one node to a user.

User Profile

User can view or modify your profile but not access permission using user profile option.

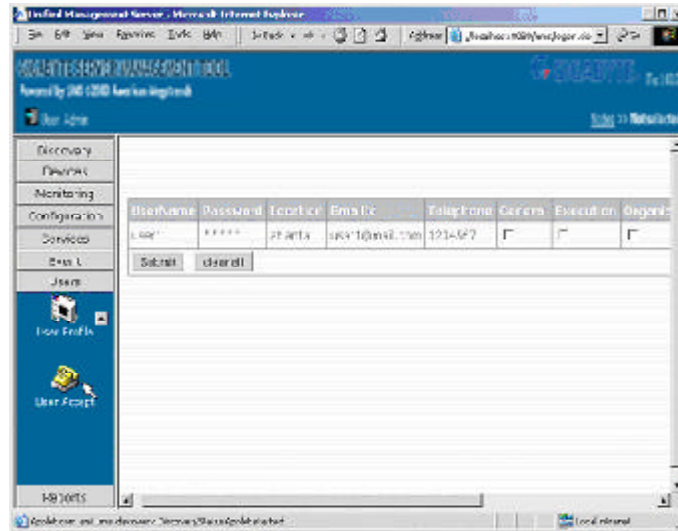


Name	Description
User Name	This field displays the your name.
User Id	This field displays the your identification.
Password	This field allows you to enter the password to login.
E-mail Id	This filed allows you to enter the Email Id.
Telephone	This field allows you to enter the telephone number.
Location	This filed allows you to enter the location.


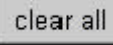
Name	Button	Description
Sumit		Click on the Submit button to select the user.
Reset		Click on the Reset Button to clear values

User Accept

This feature allows administrator to accept users.

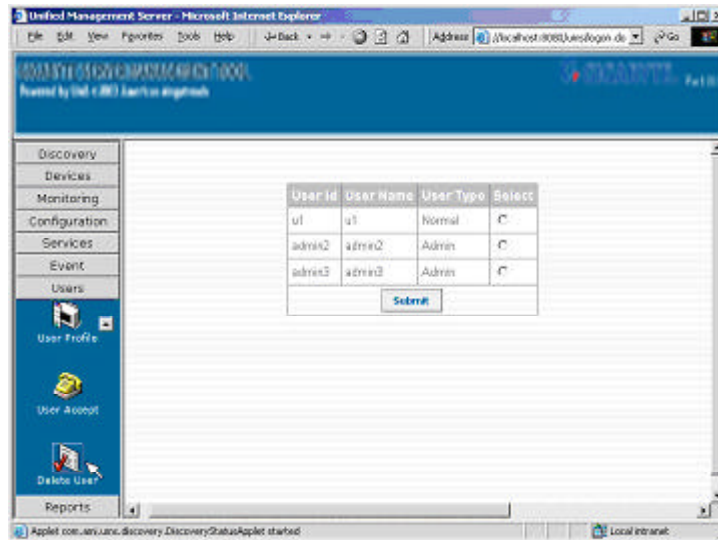


Name	Description
User Name	This field displays the user name.
Password	This field displays the password.
Location	This field displays the location.
E-mail Id	This field displays the Email Id.
Telephone	This field displays the telephone number.
General	This option allows you to accept user in general role.
Execution	This option allows you to accept user in execution role.
Organization	This option allows you to accept user in organization role.
Configuration	This option allows you to accept user in configuration role.
Administration	This option allows you to accept user in Administration role.
Reject	This option allows you to reject the user.

Name	Button	Description
Sumit		Click on the Submit button to accept the user.
Clear All		Click on the Clear All button to uncheck all checked boxes.

Delete User


This feature allows you to delete users. The following table shows types of users that are supported by the UMS utility:



User Type	Description
Super Administrator User	As a Super Administrator User, you can add or delete any administrator or normal users.
Administrator User	As Administrator User, you can add or delete normal users.
Normal User	As a normal user, you cannot delete any user.


Note: When you first login as Admin user, you have super administrator access rights.

Field/Option	Description
User Id	This field displays the user identification.
Username	This field displays the username.
User Type	This field displays the access rights that are assigned to the user.
Select	This option allows you to select the user you want to delete.

Name	Button	Description
Submit		The Submit button allows you to delete the user.

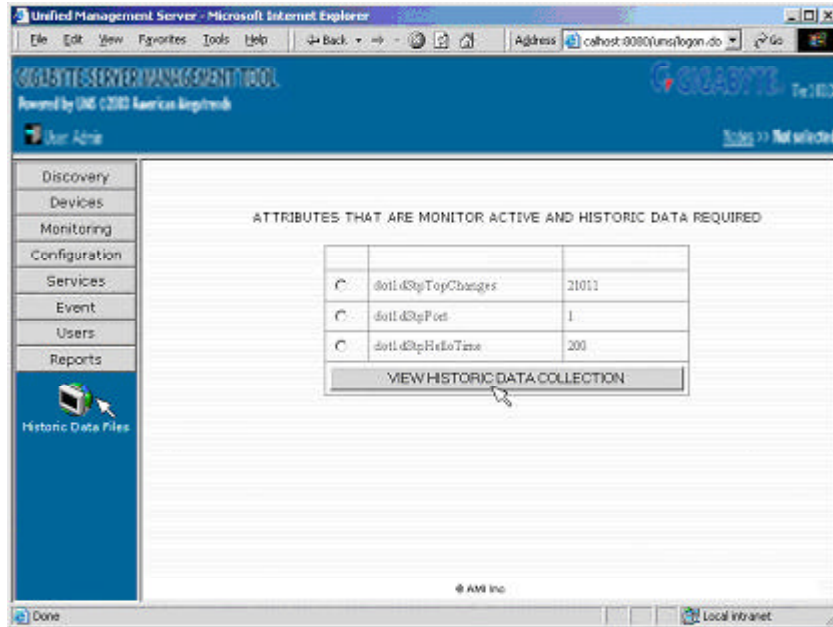
UMS Reports

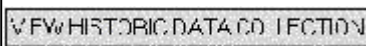
The UMS Reports feature allows you to download reports for a particular attribute.

Section	Icon	Name	Description
Reports		Historical Data Files	This section allows you to download the historical data as reports.

Historic Data Files

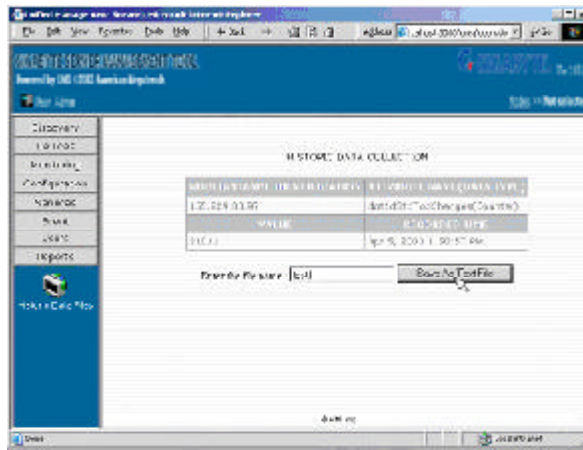
Note: You can view all attributes of the current selected node for the historical data collection.




Name	Button	Description
View Historic Data Collection		Click on the View Historic Data Collection button to select attribute.

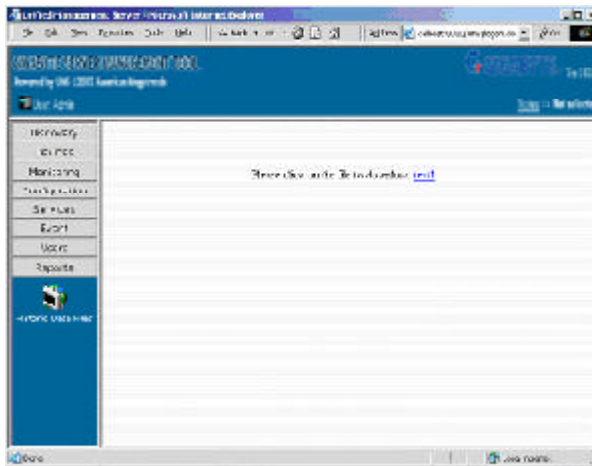
Historic Data Files (Cont'd)

Click on the View Historic Data Collection The following screen appears when you click on the View Historic Data Collection button.



Name	Button	Description
Save As Text Files		The Save As Text File button allows you to enter the report name to be saved.

The following screen appears when you click on the Save As Text File button.



Appendix Reference

Word	Description
AMI	American Megatrends, Inc
GSMT	Gigabyte Server Management Tools
UMS	Unified Management Server
SEL	System Event Log
FRU	Field Replaceable Unit
IPMI	Intelligent Platform Management Interface
SNMP	Simple Network Management Protocol
RMCP	Remote Management Control Protocol
UDP	User Datagram Protocol
BMC	Base Management Controller
JMX	Java Management Extensions
KCS	Keyboard Controller Style
SMIC	Server Management Interface Chip
SDK	Software Development Kit
LAN	Local Area Network
PEF	Platform Event Filtering
SMTP	Simple Mail Transfer Protocol
POP	Post Office Protocol
JNDI	Java Naming and Directory Interface