



AST2400 iBMC Configuration Guide

Version 1.0

Copyright

Copyright © 2014 MiTAC International Corporation. All rights reserved. No part of this manual may be reproduced or translated without prior written consent from MiTAC International Corporation.

Notice

Information contained in this document is furnished by MiTAC International Corporation and has been reviewed for accuracy and reliability prior to printing. MiTAC assumes no liability whatsoever, and disclaims any express or implied warranty, relating to sale and/or use of TYAN[®] products including liability or warranties relating to fitness for a particular purpose or merchantability. MiTAC retains the right to make changes to product descriptions and/or specifications at any time, without notice. In no event will MiTAC be held liable for any direct or indirect, incidental or consequential damage, loss of use, loss of data or other malady resulting from errors or inaccuracies of information contained in this document.

Contents

1. IPMI OS Drivers and Open Source Software.....	4
1.1 Windows IPMI Driver	4
1.2 Open IPMI Driver on Linux	4
1.3 IPMI Tool and Other Open Source Software	4
2. SP-X WEB GUI.....	6
2.1 MegaRAC® GUI Overview	6
2.2 User Name and Password	6
2.3 Dashboard	7
2.4 FRU Information.....	8
2.5 Server Health Group.....	9
2.5.1 Sensor Readings	10
2.5.2 Event Log.....	11
2.5.3 Audio Logs	12
2.5.4 BSOD Screen	13
2.6 Configuration Group.....	14
2.6.1 Active Directory.....	15
2.6.2 DNS.....	16
2.6.3 Event Log.....	17
2.6.4 Image Redirection.....	18
2.6.5 LDAP.....	23
2.6.6 License.....	24
2.6.7 Mouse Mode	26
2.6.8 NCSI	27
2.6.9 Network.....	28
2.6.10 Network Link	31
2.6.11 NTP Settings.....	33
2.6.12 PAM Ordering Settings.....	35
2.6.13 PEF	36
2.6.14 RADIUS	48
2.6.15 Remote Session.....	50
2.6.16 Services	51
2.6.17 SMTP	53

2.6.18	SSL	55
2.6.19	System Firewall.....	56
2.6.20	User Management	58
2.6.21	Virtual Media	62
2.7	Remote Control.....	64
2.7.1	Console Redirection.....	65
2.7.1.1	Video	69
2.7.2	Server Power Control.....	84
2.7.3	Other Control	85
2.7.4	JAVA SOL.....	86
2.8	Auto Video Recording.....	87
2.8.1	Trigger Configuration	88
2.8.2	Video Recording	90
2.9	Maintenance Group	92
2.9.1	Preserve Configuration	93
2.9.2	Restore Configuration	94
2.10	Firmware Update	95
2.10.1	Firmware Update	96
2.10.2	BIOS Update.....	97
2.10.3	Protocol Configuration	98
2.11	Log Out	100
3.	BMC Port Number	101

1. IPMI OS Drivers and Open Source Software

AST2400 firmware is full compliant with IPMI 2.0 specification. So users could use standard IPMI driver comes from operation system distribution.

1.1 Windows IPMI Driver

AST2400 supports Intel reference driver, you can get it from

<http://www.intel.com/design/servers/ipmi/tools.htm>

From Windows Server 2003 R2, Microsoft also provide in box IPMI driver. You can use it also.

1.2 Open IPMI Driver on Linux

AST2400 supports the Open IPMI driver in Linux Kernel. Use the following commands to load IPMI drivers.

```
“modprobe ipmi_devintf”
```

```
“modprobe ipmi_si”
```

If you use old version Linux Kernel, you need to replace module “ipmi_si” with “ipmi_kcs”

Note that TYAN motherboard BIOS encodes IPMI Base IO address at 0xCA2 in its DMI table IPMI entry, any generic OS IPMI drivers should have no problem to support it.

1.3 IPMI Tool and Other Open Source Software

AST2400 supports open source software IPMI Tool, you can also use other ones like Open IPMI, IPMI Utility. Note that for IPMI Tool SOL session, user needs to use BIOS setup menu to configure “Remote Serial Console Redirect” to use COMA, and set baud rate to 38.4K, 8 bits, no parity, and Xon/Xoff handshaking.

NOTE

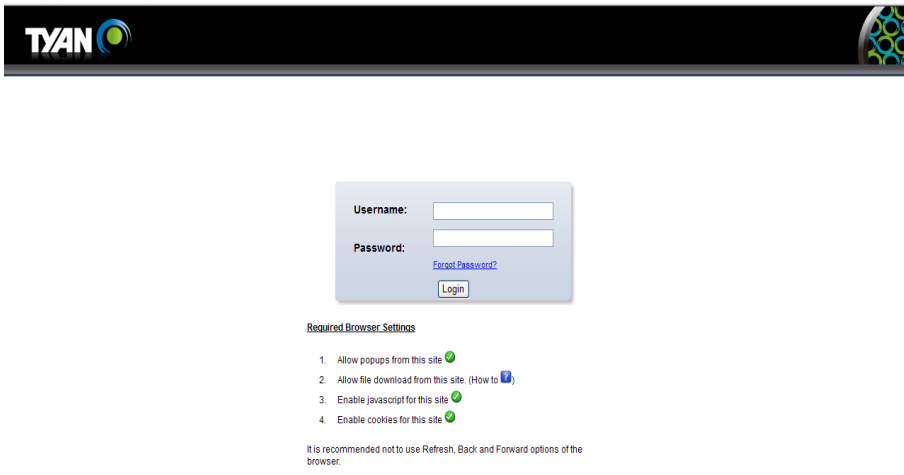
2. SP-X WEB GUI

2.1 MegaRAC® GUI Overview

The MegaRAC® SP-X SoC (System-on-Chips) has an AMI generic, user-friendly Graphics User Interface (GUI) called the **MegaRAC® GUI**. It is designed to be easy to use. It has a low learning curve because it uses a standard Internet browser. You can expect to be up and running in less than five minutes.

2.2 User Name and Password

Initial access of MegaRAC SP-X prompts you to enter the User Name and Password. A screenshot of the login screen is given below.



Default User Name and Password

The default user name and password are as follows:

Username: root

Password: superuser

NOTE:

- The default user name and password are in lower-case characters.
- When you log in using the user name and password, you get full administrative rights. It is advised to change your password once you login.

2.3 Dashboard

In MegaRAC GUI, the Dashboard page gives the overall information about the status of a device. To open the Dashboard page, click **Dashboard** from the main menu. A sample screenshot of the Dashboard page is shown below.

Dashboard

Dashboard gives the overall information about the status of the device and remote server.

Device Information

Device Power Status: On
 Firmware Revision: FT77A-B7059 R1.08
 Firmware Build Time: May 6 2014 15:48:39

System Information

BIOS Revision:
 BIOS Build Time:

Network Information (Edit)

MAC Address: 00:E0:81:E9:F5:51
 V4 Network Mode: DHCP
 IPv4 Address: 10.60.254.75
 V6 Network Mode: DHCP
 IPv6 Address:

Remote Control

800 x 600

Sensor Monitoring

Status	Sensor	Reading	
●	PCH_E_Air_Inlet	Not Available	↗
●	PCH_Area_Temp	Not Available	↗
●	LSI_SAS2008_Temp	Not Available	↗
●	ME PCH Temp.	0 ° C	↗
●	CPU0_DTS_Temp	91 ° C	↗
●	CPU1_DTS_Temp	Not Available	↗
●	CPU0_PECCL_Value	-1 ° C	↗
●	CPU1_PECCL_Value	Not Available	↗
●	CPU0_VCore	0.52 Volts	↗
●	CPU1_VCore	Not Available	↗
●	CPU0_Memory	0.41 Volts	↗
●	CPU1_Memory	Not Available	↗
●	VBAT	0.754 Volts	↗
●	3.3V	0.81 Volts	↗
●	5V	1.295 Volts	↗
●	12V	2.99 Volts	↗
●	CPU0_DIMM_A0	Not Available	↗
●	CPU0_DIMM_A1	Not Available	↗
●	CPU0_DIMM_A2	Not Available	↗
●	CPU0_DIMM_B0	Not Available	↗
●	CPU0_DIMM_B1	Not Available	↗
●	CPU0_DIMM_B2	Not Available	↗
●	CPU0_DIMM_C0	Not Available	↗
●	CPU0_DIMM_C1	Not Available	↗
●	CPU0_DIMM_C2	Not Available	↗
●	CPU0_DIMM_D0	Not Available	↗
●	CPU0_DIMM_D1	Not Available	↗
●	CPU0_DIMM_D2	Not Available	↗
●	CPU_FAN	Not Available	↗
●	SYS_FAN_1	Not Available	↗
●	SYS_FAN_2	4300 RPM	↗
●	SYS_FAN_3	Not Available	↗
●	SYS_FAN_4	Not Available	↗
●	SYS_FAN_5	Not Available	↗
●	SYS_FAN_6	Not Available	↗
●	SYS_FAN_7	Not Available	↗
●	SYS_FAN_8	Not Available	↗
●	SYS_FAN_9	Not Available	↗
●	SYS_FAN_10	Not Available	↗
●	SYS_FAN_11	Not Available	↗
●	SYS_FAN_12	Not Available	↗
●	PSU1 Status	Not Available	↗
●	PSU2 Status	Not Available	↗
●	PSU1 Power	Not Available	↗
●	PSU2 Power	Not Available	↗

Event Logs

● CPU0 Thermal Status (100%)
 □ Free Space (0%)

2.4 FRU Information

In MegaRAC GUI, the FRU Information Page displays the BMC FRU file information. The information displayed in this page is Basic Information, Common Header Information, Chassis Information, Board Information and Product Information of the FRU device.

To open the FRU Information, click **FRU Information** from the top menu. Select a FRU Device ID from the Basic Information section to view the details of the selected device. A screenshot of FRU Information Page is given below.

TYAN

Dashboard | **FRU Information** | Server Health | Component | Configuration | Remote Control | Auto Video Recording | Maintenance | Firmware Update | HELP

root/Administrator Refresh Print Logout

Field Replaceable Unit(FRU)

This page gives detailed information for the various FRU devices present in this system.

Basic Information:

FRU Device ID: 0

FRU Device Name:

Chassis Information:

Chassis Information Area Format Version: 0

Chassis Type:

Chassis Part Number:

Chassis Serial Number:

Chassis Extra:

Board Information:

Board Information Area Format Version: 1

Language: 0

Manufacture Date Time: Mon Oct 7 15:22:00 2013

Board Manufacturer: TYAN

Board Product Name:

Board Serial Number:

Board Part Number:

FRU File ID:

Board Extra:

Product Information:

Product Information Area Format Version: 0

Language: 0

Manufacturer Name:

Product Name:

Product Part Number:

Product Version:

Product Serial Number:

Asset Tag:

FRU File ID:

Product Extra:

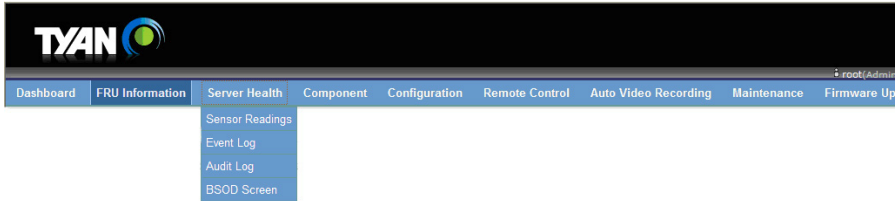
Internet 100%

2.5 Server Health Group

The Server Health Group consists of two items.

- Sensor Readings
- Event Log
- Audio Log
- BSOD Screen

A screenshot displaying the menu items under the Server Health is shown below.



2.5.1 Sensor Readings

In MegaRAC GUI, the Sensor Readings Page displays all the sensor related information.

To open the Sensor Readings Page, click **Server Health** → **Sensor Readings** from the top menu. Click on a record to show more information about that particular sensor, including thresholds and a graphical representation of all associated events. A screenshot of Sensor Readings Page is given below.

TYAN

root/Administrator Refresh Print Logout

Dashboard FRU Information **Server Health** Component Configuration Remote Control Auto Video Recording Maintenance Firmware Update HELP

Sensor Readings

All sensor related information will be displayed here. Double click on a record to toggle (ON / OFF) the live widget for that particular sensor.

All Sensors Sensor Count: 81 sensors

Sensor Name	Status	Current Reading
PCI-E_Air_Inlet	All deasserted	Not Available
PCH_Area_Temp	All deasserted	Not Available
LSI_SAS2008_Temp	All deasserted	Not Available
ME PCH Temp	Normal	0 ° C
CPU0_DTS_Temp	Upper Critical	91 ° C
CPU1_DTS_Temp	All deasserted	Not Available
CPU0_PECL_Value	Upper Critical	-1 ° C
CPU1_PECL_Value	All deasserted	Not Available
CPU0_VCore	Lower Critical	0.52 Volts
CPU1_VCore	All deasserted	Not Available
CPU0_Memory	Lower Critical	0.41 Volts
CPU1_Memory	All deasserted	Not Available
VBAT	Lower Critical	0.783 Volts
3.3V	Lower Critical	0.756 Volts
5V	Lower Critical	1.242 Volts
12V	Lower Critical	2.925 Volts
CPU0_DIMM_A0	All deasserted	Not Available
CPU0_DIMM_A1	All deasserted	Not Available
CPU0_DIMM_A2	All deasserted	Not Available
CPU0_DIMM_B0	All deasserted	Not Available
CPU0_DIMM_B1	All deasserted	Not Available
CPU0_DIMM_B2	All deasserted	Not Available
CPU0_DIMM_C0	All deasserted	Not Available
CPU0_DIMM_C1	All deasserted	Not Available
CPU0_DIMM_C2	All deasserted	Not Available
CPU0_DIMM_D0	All deasserted	Not Available
CPU0_DIMM_D1	All deasserted	Not Available
CPU0_DIMM_D2	All deasserted	Not Available
CPU1_DIMM_A0	All deasserted	Not Available
CPU1_DIMM_A1	All deasserted	Not Available
CPU1_DIMM_A2	All deasserted	Not Available
CPU1_DIMM_B0	All deasserted	Not Available
CPU1_DIMM_B1	All deasserted	Not Available
CPU1_DIMM_B2	All deasserted	Not Available
CPU1_DIMM_C0	All deasserted	Not Available
CPU1_DIMM_C1	All deasserted	Not Available
CPU1_DIMM_C2	All deasserted	Not Available
CPU1_DIMM_D0	All deasserted	Not Available
CPU1_DIMM_D1	All deasserted	Not Available
CPU1_DIMM_D2	All deasserted	Not Available
DIMM1	All deasserted	Not Available
DIMM2	All deasserted	Not Available
DIMM3	Normal	30 ° C
DIMM4	All deasserted	Not Available
CPU_FAN	All deasserted	Not Available
SYS_FAN_1	All deasserted	Not Available
SYS_FAN_2	Normal	4300 RPM
SYS_FAN_3	All deasserted	Not Available
SYS_FAN_4	All deasserted	Not Available
SYS_FAN_5	All deasserted	Not Available
SYS_FAN_6	All deasserted	Not Available
SYS_FAN_7	All deasserted	Not Available
SYS_FAN_8	All deasserted	Not Available
SYS_FAN_9	All deasserted	Not Available
SYS_FAN_10	All deasserted	Not Available
SYS_FAN_11	All deasserted	Not Available
SYS_FAN_12	All deasserted	Not Available
PSU1 Status	All deasserted	Not Available
PSU2 Status	All deasserted	Not Available
PSU1 Power	All deasserted	Not Available
PSU2 Power	All deasserted	Not Available

PCI-E_Air_Inlet: Not Available **ALL DEASSERTED**

Thresholds for this sensor LIVE WIDGET N/A |

Lower Non-Recoverable (LNR): N/A Upper Non-Recoverable (UNR): N/A
 Lower Critical (LC): N/A Upper Critical (UC): N/A
 Lower Non-Critical (LNC): N/A Upper Non-Critical (UNC): N/A

[Threshold Settings](#)

Graphical View of this sensor's events

[View this Event Log](#)

2.5.2 Event Log

In MegaRAC GUI, this page displays the list of event logs occurred by the different sensors on this device. Double click on a record to see the details of that entry. You can use the sensor type or sensor name filter options to view those specific events or you can also sort the list of entries by clicking on any of the column headers.

To open the Event Log page, click **Server Health** → **Event Log** from the top menu. A sample screenshot of Event Log Page is shown below.

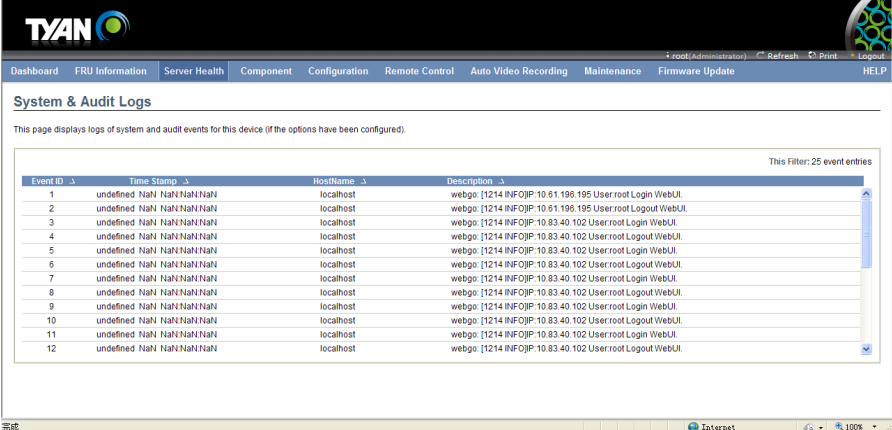
The screenshot displays the MegaRAC GUI interface. At the top, there is a navigation bar with the TYAN logo and several menu items: Dashboard, FRU Information, Server Health, Component, Configuration, Remote Control, Auto Video Recording, Maintenance, Firmware Update, and HELP. The 'Server Health' menu is currently selected.

Below the navigation bar, the 'Event Log' page is shown. It features a header with the text: 'Events generated by the system will be logged here. Double-click on a record to see the description.' Below this, there are filter options: 'All Events' (selected) and 'filter by: All Sensors'. A status indicator shows 'Event Log: 3639 event entries, 73 page(s)'. There are also time zone options: 'BMC Timezone' (selected), 'Client Timezone', and 'UTC Offset: (GMT+/-0)'. Navigation buttons include '<<', '<', '1', '>', and '>>'. The main content is a table with the following columns: Event ID, Time Stamp, Sensor Name, Sensor Type, and Description. The table contains 10 rows of data, all related to OEM CPU0 Thermal Status events. At the bottom of the table, there are two buttons: 'Save Event Logs' and 'Clear All Event Logs'.

Event ID	Time Stamp	Sensor Name	Sensor Type	Description
3639	05/09/2014 16:43:45	OEM: CPU0 Thermal Status	Processor	OEM Discrete - Asserted
3638	05/09/2014 16:43:46	OEM: CPU0 Thermal Status	Processor	OEM Discrete - Asserted
3637	05/09/2014 16:43:46	OEM: CPU0 Thermal Status	Processor	OEM Discrete - Asserted
3636	05/09/2014 16:43:45	OEM: CPU0 Thermal Status	Processor	OEM Discrete - Deasserted
3635	05/09/2014 16:43:45	OEM: CPU0 Thermal Status	Processor	OEM Discrete - Asserted
3634	05/09/2014 16:43:44	OEM: CPU0 Thermal Status	Processor	OEM Discrete - Deasserted
3633	05/09/2014 16:43:44	OEM: CPU0 Thermal Status	Processor	OEM Discrete - Asserted
3632	05/09/2014 16:43:44	OEM: CPU0 Thermal Status	Processor	OEM Discrete - Deasserted
3631	05/09/2014 16:43:44	OEM: CPU0 Thermal Status	Processor	OEM Discrete - Deasserted
3630	05/09/2014 16:43:44	OEM: CPU0 Thermal Status	Processor	OEM Discrete - Deasserted

2.5.3 Audio Logs

To open the Event Log page, click **Server Health** → **Audio Logs** from the top menu. A sample screenshot of Audio Logs Page is shown below.

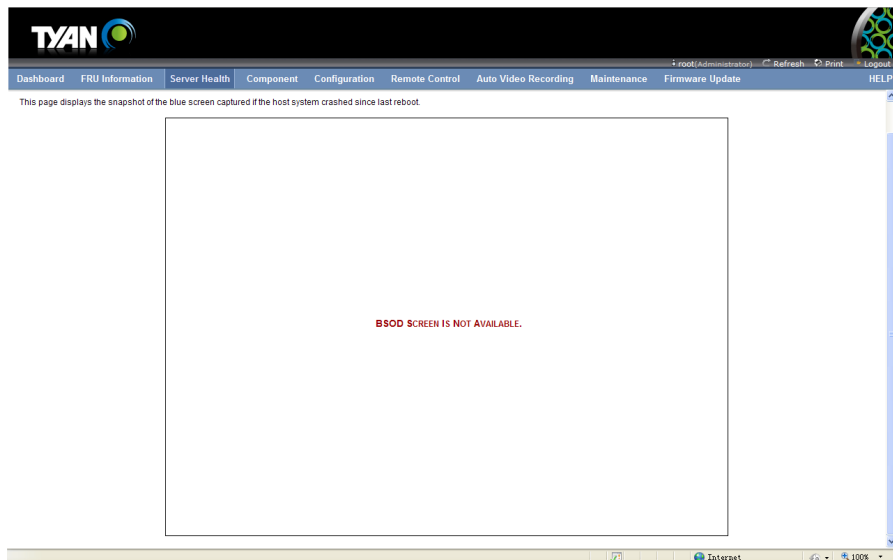


The screenshot displays the 'System & Audit Logs' page in a web browser. The page title is 'System & Audit Logs' and it includes a sub-header: 'This page displays logs of system and audit events for this device (if the options have been configured)'. A filter is applied, showing '25 event entries'. The main content is a table with the following data:

Event ID	Time Stamp	Host Name	Description
1	undefined NaN NaNNaNNaN	localhost	webgo: [1214 INFO]IP: 10.61.196.195 Userroot Login WebUI
2	undefined NaN NaNNaNNaN	localhost	webgo: [1214 INFO]IP: 10.61.196.195 Userroot Logout WebUI
3	undefined NaN NaNNaNNaN	localhost	webgo: [1214 INFO]IP: 10.83.40.102 Userroot Login WebUI
4	undefined NaN NaNNaNNaN	localhost	webgo: [1214 INFO]IP: 10.83.40.102 Userroot Logout WebUI
5	undefined NaN NaNNaNNaN	localhost	webgo: [1214 INFO]IP: 10.83.40.102 Userroot Login WebUI
6	undefined NaN NaNNaNNaN	localhost	webgo: [1214 INFO]IP: 10.83.40.102 Userroot Logout WebUI
7	undefined NaN NaNNaNNaN	localhost	webgo: [1214 INFO]IP: 10.83.40.102 Userroot Login WebUI
8	undefined NaN NaNNaNNaN	localhost	webgo: [1214 INFO]IP: 10.83.40.102 Userroot Logout WebUI
9	undefined NaN NaNNaNNaN	localhost	webgo: [1214 INFO]IP: 10.83.40.102 Userroot Login WebUI
10	undefined NaN NaNNaNNaN	localhost	webgo: [1214 INFO]IP: 10.83.40.102 Userroot Logout WebUI
11	undefined NaN NaNNaNNaN	localhost	webgo: [1214 INFO]IP: 10.83.40.102 Userroot Login WebUI
12	undefined NaN NaNNaNNaN	localhost	webgo: [1214 INFO]IP: 10.83.40.102 Userroot Logout WebUI

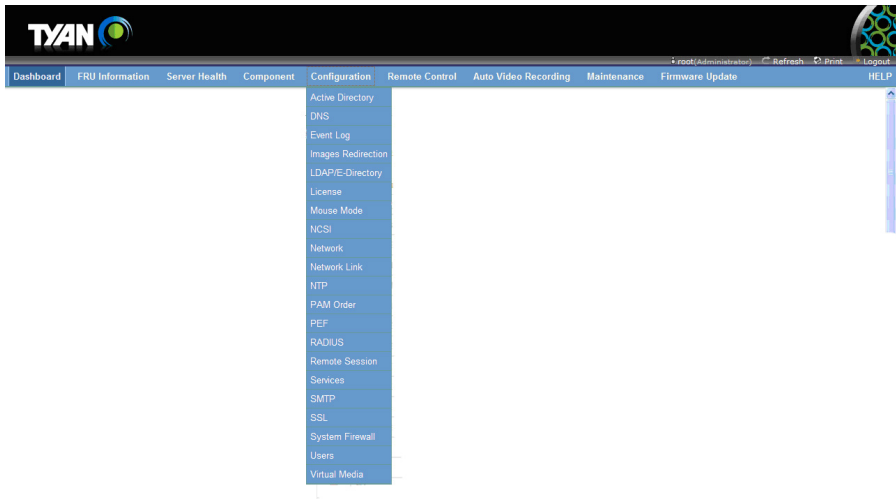
2.5.4 BSOD Screen

If system into blue screen state, the BSOD screen show the last screen. If the system is in normal state, the BSOD screen is not available.



2.6 Configuration Group

This group of pages allows you to access various configuration settings. A detailed description of each configuration group is given ahead. A screenshot of Configuration Group Page is shown below.



2.6.1 Active Directory

An active directory is a directory structure used on Microsoft Windows based computers and servers to store information and data about networks and domains. An active directory (sometimes referred to as an AD) does a variety of functions including the ability to provide information on objects, helps organize these objects for easy retrieval and access, allows access by end users and administrators and allows the administrator to set security up for the directory.

This page allows you to configure Active Directory Server Settings.

To open the Active Directory Settings Page, click **Configuration** → **Active Directory** from the main menu. A sample screenshot of Active Directory Settings Page is shown in the screenshot below.

Active Directory Settings

The "Active Directory" is currently disabled. To enable Active Directory and configure its settings, click on "Advanced Settings" button.

The list below shows the current list of configured Role Groups. If you would like to delete or modify a role group, select the name in the list and click Delete Role Group or Modify Role Group. To add a new Role Group, select an unconfigured slot and click Add Role Group.

Number of configured Role groups: 0

Role Group ID	Group Name	Group Domain	Group Privilege
1	~	~	~
2	~	~	~
3	~	~	~
4	~	~	~
5	~	~	~

[Add Role Group](#) [Modify Role Group](#) [Delete Role Group](#)

2.6.2 DNS

The **Domain Name System (DNS)** is a distributed hierarchical naming system for computers, services, or any resource connected to the internet or a private network. It associates the information with domain names assigned to each of the participants. Most importantly, it translates domain names meaningful to humans into the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

In MegaRAC GUI, the DNS Server Settings page is used to manage the DNS settings of a device.

To open the DNS Server Settings Page, click **Configuration** → **DNS** from the main menu. A sample screenshot of DNS Server Settings Page is shown in the screenshot below.

TYAN

Dashboard FRU Information Server Health Component Configuration Remote Control Auto Video Recording Maintenance Firmware Update HELP

DNS Server Settings

Manage DNS settings of the device.

Host Configuration

Host Settings: Automatic

Host Name: AMI00E081E9F551

Register BMC

eth0: Register BMC
 Direct Dynamic DNS DHCP Client FQDN

TSIG Configuration

TSIG Authentication: Enable

Current TSIG Private File: Not Available

New TSIG Private File: 浏览...

Domain Name Configuration

Domain Settings: eth0_v4

Domain Name:

Domain Name Server Configuration

DNS Server Settings: eth0

IP Priority: IPv4 IPv6

DNS Server1: 10.60.0.20

DNS Server2: 10.88.1.86

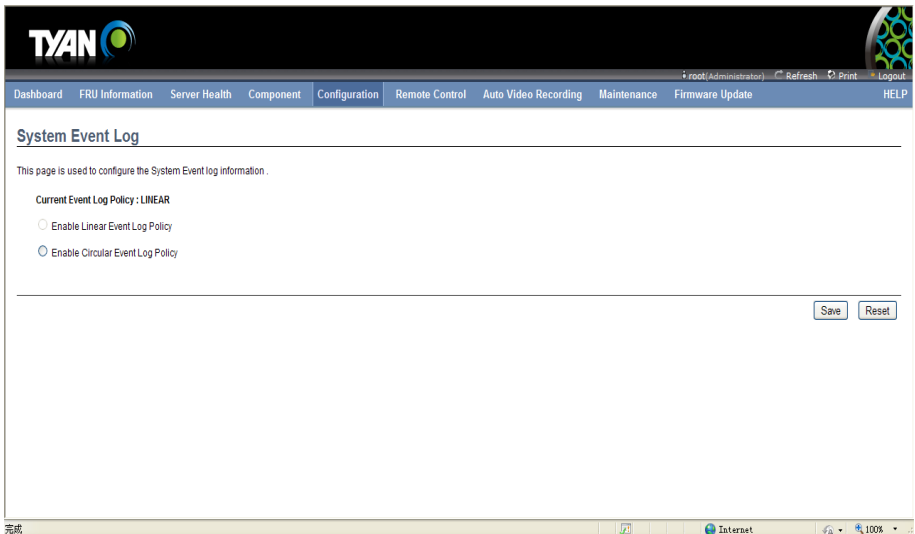
DNS Server3:

Save Reset

2.6.3 Event Log

This page is used to configure the SEL type, that is Linear SEL or Circular SEL. Linear SEL type will store the System Event log linearly up to its SEL Repository size and SEL will be discarded if the SEL Repository is full. Circular SEL type will store the System Event log linearly up to its SEL Repository size and override the SEL entry if the SEL Repository is full.

To open System Event log page, click Configuration > Event Log from the menu bar. A sample screenshot of System Event log page is shown below.



System Event Log Page

The fields of System Event Log page are explained below.

Current Event Log Policy: Displays the configured Event Log Policy.

- **Enable Linear Event Log Policy:** To enable the Linear System Event Log Policy for Event Log.
- **Enable Circular Event Log Policy:** To enable the Circular System Event Log Policy for Event Log.

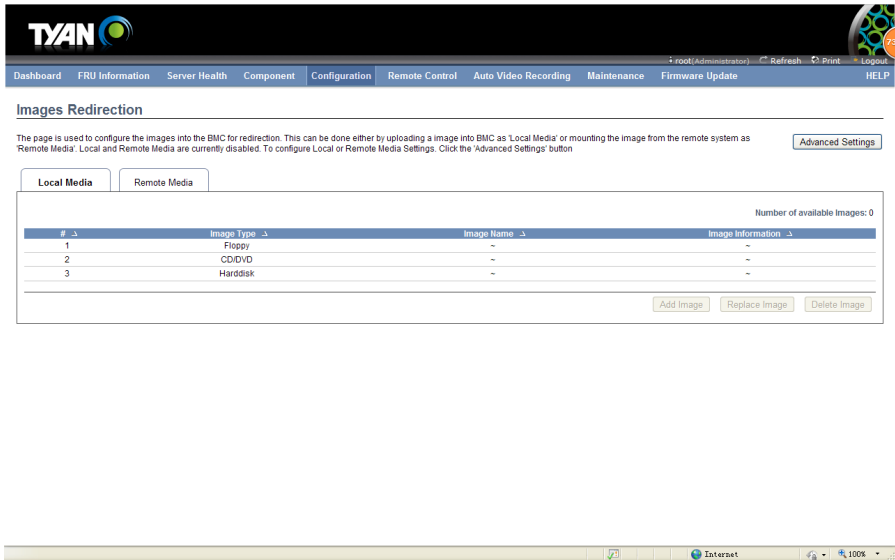
Save: To save the configured settings.

Reset: To reset the modified changes.

2.6.4 Image Redirection

This page is used to configure the images into BMC for redirection. This can be done either by uploading an image into BMC say, Local Media or by mounting the image from the remote system, Remote Media.

To open Images Redirection page, click Configuration > Images Redirection from the menu bar. A sample screenshot of Images Redirection page is shown below.

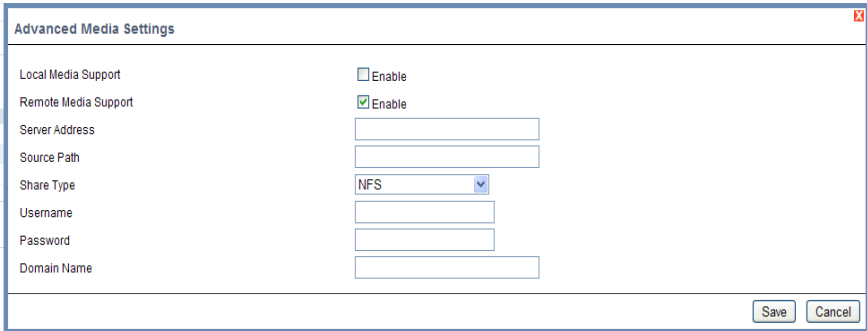


The fields of Images Redirection page are explained below.

- Local Media
- Remote Media

Advanced Setting for Media Redirection

Enter the Advanced Media Settings for media redirection.



Local Media Support	<input type="checkbox"/> Enable
Remote Media Support	<input checked="" type="checkbox"/> Enable
Server Address	<input type="text"/>
Source Path	<input type="text"/>
Share Type	NFS
Username	<input type="text"/>
Password	<input type="text"/>
Domain Name	<input type="text"/>

Save Cancel

Local Media Support: To enable or disable Local Media support, check or uncheck the 'Enable' checkbox respectively.

Remote Media Support: To enable or disable Remote Media support, check or uncheck the 'Enable' checkbox respectively.

Note: Both local and remote media support can be enabled at a time

Server Address: Server address of the remote media images are stored.

Source Path: Source path of the remote media images are stored.

Share Type: Share Type of the remote media server either NFS or Samba(CIFS).
Username, Password and Domain Name: If share Type is Samba(CIFS), then user credentials to authenticate the server.

Save: To save the settings.

Cancel: To cancel the modifications and return to Image list.

Local Media

This tab displays the list of available images in the local media on BMC. You can replace or add new images from here. To configure the image, you need to enable Local Media support under **Images Redirection -> Advanced Settings**. Once you enable this option, the user can add the images and the added images will be redirected to the host machine

Note: To replace or add an image, you must have Administrator Privileges. Only one image can be uploaded for each image type. If the existing image and uploading image name is same, then a message is shown “Image already exists”. In Local Media redirection, the maximum upload size is 8MB. The fields of Local Media tab is as follows:

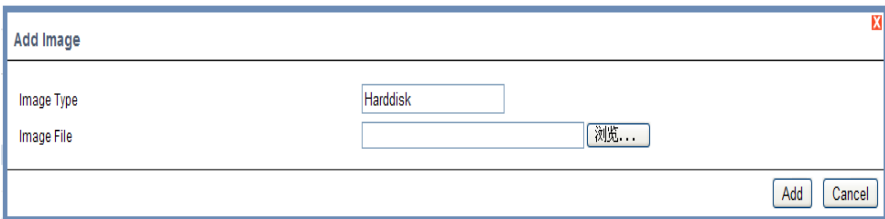
Add Image: To upload a new image to the device.

Replace Image: To replace the existing image.

Delete Image: To delete the desired image.

Procedure:

1. To add, remove or modify images, click Advanced Settings and make sure Local Media Support option is enabled. If not, disable Remote Media Redirection and then enable Local Media Redirection.
2. Click on the Local Media Tab.
3. To add an image, select a free slot and click Add Image to upload a new image to the device. Alternatively, double click on a free slot to add an image. A sample screenshot of Add Image screen is given below.



The screenshot shows a dialog box titled "Add Image". It has a title bar with a close button (X). The dialog contains two input fields: "Image Type" with a dropdown menu showing "Harddisk", and "Image File" with a text input field and a "浏览..." (Browse...) button. At the bottom right, there are "Add" and "Cancel" buttons.

4. To replace an image, select a configured slot and click Replace Image to replace the existing image. Alternatively, double click on the configured slot.
5. Browse the image File and click Replace
6. To delete an image, select a record and click Delete Image to delete the selected image.

Remote Media

The displayed table shows configured images on BMC. You can configure images of the remote media server.

Number of available Images: 0

#	Image Type	Image Name	Redirection Status
1	Floppy	~	~
2	CD/DVD	~	~
3	Harddisk	~	~

Start Redirection Add Image Replace Image Delete Image

Note: Only one image can be configured for each image type. To configure the image, you need to enable Remote Media support using 'Advanced Settings'. To add or replace an image, you must have Administrator Privileges. Free slots are denoted by "~". The fields of Remote Media tab are as follows:

Start/Stop Redirection: To start or stop Media redirection.

Add Image: To upload a new image to the device.

Replace Image: To replace the existing image.

Delete Image: To delete the desired image.

Procedure:

1. To Start/Stop Redirection and configure remote media images, click Advanced Settings and make sure Remote Media Support option is enabled. If not, disable Local Media Redirection and then enable Remote Media Redirection.

Note: The Start Redirection button is active only for VMedia enabled users.

2. Select a configured slot and click Start Redirection to start the remote media redirection. It is a toggle button, if the image is successfully redirected, then click Stop Redirection to stop the remote media redirection.
3. To add an image, select a free slot and click Add Image to configure a new image to the device. Alternatively, double click on a free slot to add an image.
4. To replace an image, select a configured slot and click Replace Image to replace the existing image. Alternatively, double click on the configured slot.
5. To delete an image, select the desired image to be deleted and click Delete Image.

Note: Redirection needs to be stopped to replace or delete the image.

2.6.5 LDAP

The **Lightweight Directory Access Protocol (LDAP)** is an application protocol for querying and modifying data of directory services implemented in internet Protocol (IP) networks.

To open the LDAP Settings Page, click **Configuration** → **LDAP** from the main menu. A sample screenshot of LDAP Settings Page is shown in the screenshot below.

The screenshot shows the TYAN web interface. The navigation menu includes: Dashboard, FRU Information, Server Health, Component, Configuration, Remote Control, Auto Video Recording, Maintenance, Firmware Update, and HELP. The user is logged in as root/Administrator.

LDAP/E-Directory Settings

LDAP/E-Directory is currently disabled. To enable LDAP/E-Directory and configure its settings, click on 'Advanced Settings' button.

The list below shows the current list of configured Role Groups. If you would like to delete or modify a role group, select the name in the list and click Delete Role Group or Modify Role Group. To add a new Role Group, select an unconfigured slot and click Add Role Group.

Number of configured Role groups: 0

Role Group ID	Group Name	Group Search Base	Group Privilege
1	-	-	-
2	-	-	-
3	-	-	-
4	-	-	-
5	-	-	-

Buttons: Add Role Group, Modify Role Group, Delete Role Group

Bottom status bar: 完成, Internet, 100%

2.6.6 License

The License page is used to display the available services and its validity period. To open License page, click Configuration > License from the menu bar. A sample screenshot of License Page is shown below.

License

Below is a list of available Features and its License validity. Click the "Upload License Key" button to upload a new Key to activate the particular feature.

Number of Licensed Features: 3

#	Feature Name	Validity
1	CIM	Full
2	KVM	Full
3	MEDIA	Full

Upload License Key

The fields of License page are explained below. Upload License Key: This button is used to add a license key to activate the particular service.


Feature Name: This field is used to list all the available services.

Validity: This field is used to show the validity of the particular service.

NOTE: Validity period mentioned in days.

Procedure

1. To add a license key, click Upload License Key button. This opens the Upload license Key window as shown below.



Upload License Key

License Key

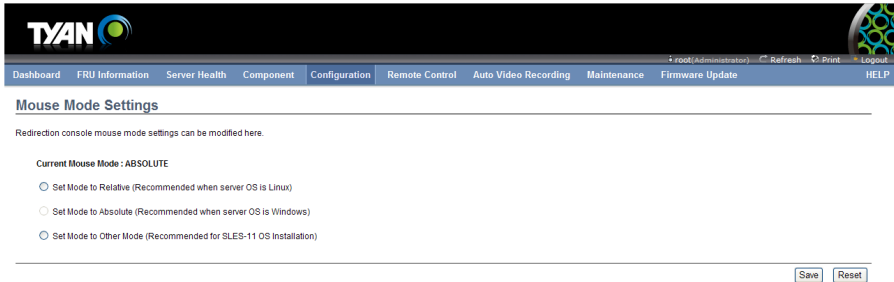
Upload Cancel

2. Enter the License Key.
3. Click Add to add the license key.
4. Click Cancel to go back to the License page.
5. The added license can be seen in the grid.

2.6.7 Mouse Mode

In MegaRAC GUI, Redirection Console handles mouse emulation from local window to remote screen in either of two methods. User has to be an Administrator to configure this option.

To open the Mouse Mode Page, click **Configuration** → **Mouse Mode** from the main menu. A sample screenshot of Mouse Mode Settings page is shown in the screenshot below.

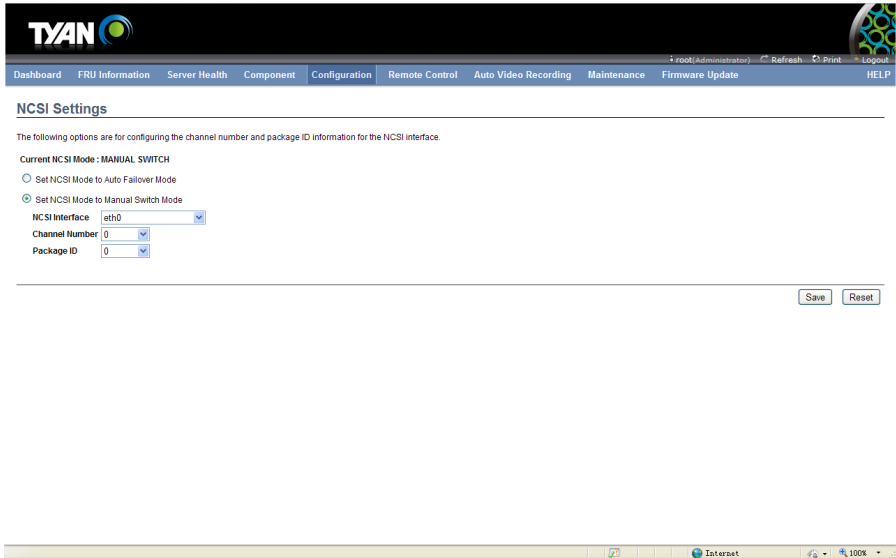


Note: When server OS is Redhat 6.x, please select the absolute mouse mode

2.6.8 NCSI

In MegaRAC GUI, this page is used to configure Network Controller Sideband Interface (NCSI) configuration settings.

To open the NCSI Page, click **Configuration** → **NCSI** from the main menu. A sample screenshot of NCSI Settings Page is shown in the screenshot below.



NCSI Interface: It lists the interface name in list box.

Channel Number: Lists the channel number of the selected interface.

Package ID: Lists the package id of the selected interface.

Save: To save the current changes.

Reset: To reset the modified changes.

Procedure

1. Choose the particular **NCSI Interface** to which you need to configure NCSI settings.
2. Choose the **Channel Number** to be configured for the selected Interface name.
3. Choose the **Package ID** to be configured for the selected Interface name.
4. Click **Save** to save the current changes.
5. Click **Reset** to reset the modified changes.

2.6.9 Network

In MegaRAC GUI, the Network Settings Page is used to configure the network settings for the available LAN channels.

To open the Network Settings Page, click **Configuration** → **Network** from the main menu. A sample screenshot of Network Settings Page is shown in the screenshot below.

Manage network settings of the device.

LAN Interface

LAN Settings Enable

MAC Address

IPv4 Configuration

Obtain an IP address automatically Use DHCP

IPv4 Address

Subnet Mask

Default Gateway

IPv6 Configuration

IPv6 Settings Enable

Obtain an IP address automatically Use DHCP

IPv6 Address

Subnet Prefix length

Default Gateway

VLAN Configuration

VLAN Settings Enable

VLAN ID

VLAN Priority

The fields of Network Settings page are explained below.

LAN Interface: Lists the LAN interfaces.

LAN Settings: To enable or disable the LAN Settings.

MAC Address: This field displays the MAC Address of the device. This is a read only field.

IPv4 Settings: This option lists the IPv4 configuration settings.

Obtain IP Address automatically: This option is to dynamically configure IPv4 address using DHCP (Dynamic Host Configuration Protocol).

IPv4 Address, Subnet Mask, and Default Gateway: These fields are for specifying

the static IPv4 address, Subnet Mask and Default Gateway to be configured to the device. MEGARAC SP-X USER GUIDE Configuration Group 68

Note:

- IP Address made of 4 numbers separated by dots as in “xxx.xxx.xxx.xxx”.
- Each Number ranges from 0 to 255.
- First Number must not be 0.

IPv6 Configuration: This option lists the following IPv6 configuration settings.

IPv6 Settings: This option is to enable/disable the IPv6 settings in the device.

Obtain an IPv6 address automatically: This option is to dynamically configure IPv6 address using DHCP (Dynamic Host Configuration Protocol).

IPv6 Address: To specify a static IPv6 address to be configured to the device. Eg: 2004::2010

Subnet Prefix length: To specify the subnet prefix length for the IPv6 settings.

Note:

- Value ranges from 0 to 128.

Default Gateway: Specify v6 default gateway for the IPv6 settings.

VLAN Configuration: It lists the VLAN configuration settings.

VLAN Settings: To enable/disable the VLAN support for selected interface.

VLAN ID: The Identification for VLAN configuration.

Note:

- Value ranges from 1 to 4095.

VLAN Priority: The priority for VLAN configuration.

Note:

- Value ranges from 1 to 7.
- 7 is the highest priority for VLAN.

Save: To save the entries.

Reset: To Reset the modified changes.

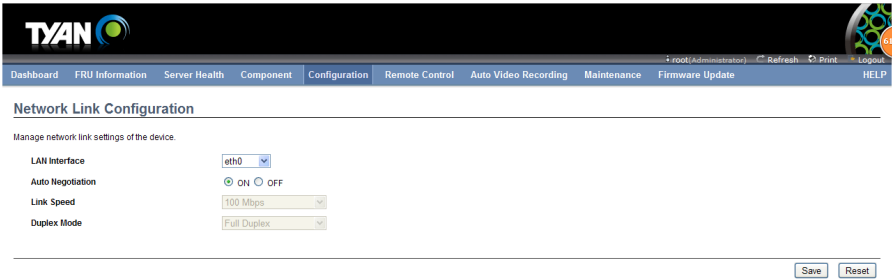
Procedure

1. Select the LAN Interface from the drop down list.
2. Check Enable to enable the LAN Settings.
3. In IPv4 Configuration, enable Use DHCP to Obtain an IP address automatically to dynamically configure IPv4 address using DHCP.
4. If the field is disabled, enter the IPv4 Address, **Subnet Mask** and **Default Gateway** in the respective fields.
5. In IPv6 Configuration, if you wish to enable the IPv6 settings, check Enable.
6. If the IPv6 setting is enabled, enable or disable the option **Use DHCP for obtaining the IP address automatically**.
7. If the field is disabled, enter the IPv6 Address, Subnet Prefix length and Default Gateway in the given field.
8. In VLAN Configuration, if you wish to enable the VLAN settings, check Enable.
9. Enter the **VLAN ID** in the specified field.
10. Enter the **VLAN Priority** in the specified field.
11. Click **Save** to save the entries.
12. Click **Reset** if you want to reset the modified changes

2.6.10 Network Link

In MegaRAC GUI, this page is used to configure network link configuration for available network interfaces.

To open the Network Link Page, click **Configuration** → **Network Link** from the main menu. A sample screenshot of Network Link Configuration Page is shown in the screenshot below.



The fields of Network Link page are explained below.

LAN Interface: Select the required network interface from the list to which the Link speed and duplex mode to be configured.

Auto Negotiation: This option is enabled to allow the device to perform automatic configuration to achieve the best possible mode of operation (speed and duplex) over a link.

Link Speed: Link speed will list all the supported capabilities of the network interface. It can be 10/100/1000 Mbps.

Duplex Mode: Duplex Mode could be either Half Duplex or Full Duplex.

Save: To save the settings.

Reset: To reset the modified changes.

Procedure

1. Select the LAN Interface from the drop down list.
2. Select either ON or OFF for Auto Negotiation.

Note: The Link Speed and Duplex Mode will be active only when Auto Negotiation is OFF.

3. Select the Link Speed from the drop-down list.
4. Select the Duplex Mode from the drop-down list.
5. Click Save to save the configuration.
6. Click Reset to reset the configuration.

2.6.11 NTP Settings

The **Network Time Protocol (NTP)** is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. It is designed particularly to resist the effects of variable latency by using a jitter buffer.

In MegaRAC GUI, this page displays the device current date and time settings. It can be used to configure either Data & Time or NTP server settings for the device.

To open the NTP Settings Page, click **Configuration** → **NTP** from the main menu. A sample screenshot of NTP Settings Page is shown in the screenshot below.

TYAN

Dashboard FRU Information Server Health Component Configuration Remote Control Auto Video Recording Maintenance Firmware Update HELP

NTP Settings

Here you can either configure the NTP server or view and modify the device's Date & Time settings.

Date: May 12 2014

Time: (hh:mm:ss) 11 36 40

Timezone:

Primary NTP Server: pool.ntp.org

Secondary NTP Server: time.nist.gov

Automatically synchronize Date & Time with NTP Server

Refresh Save Reset

The fields of Configuration – NTP are explained below.

Date: To specify the current date of the device

Time: To specify the current Time for the device.

Note: As Year 2038 Problem exists, Date and Time should be configured within the range.

TimeZone: Timezone list contains the UTC offset along with the locations and Manual UTC offset for NTP server, which can be used to display the exact local time.

Primary NTP Server & Secondary NTP Server: NTP Server fields will support the following:

- IP Address (Both IPv4 and IPv6 format).
- FQDN (Fully qualified domain name) format.
- FQDN Value ranges from 1 to 128 alpha-numeric characters.

Automatically synchronize Date & Time with NTP Server: To automatically synchronize Date and Time with the NTP Server.

Refresh: To reload the current date and time settings.

Save: To save the settings.

Reset: To reset the modified changes.

Procedure

1. Enter the Date and Time in the given fields.

Note: These fields are enabled only when the option Automatically synchronizes Date & Time with NTP Server is disabled.

2. Select the Timezone from the drop-down list.

3. In the Primary NTP Server / Secondary NTP Server field, specify the NTP server for the device.

Note: Secondary NTP server is optional field. If the Primary NTP server is not working fine, then the Secondary NTP Server will be tried.

4. To Automatically synchronize Date & Time with NTP Server, enable the option.

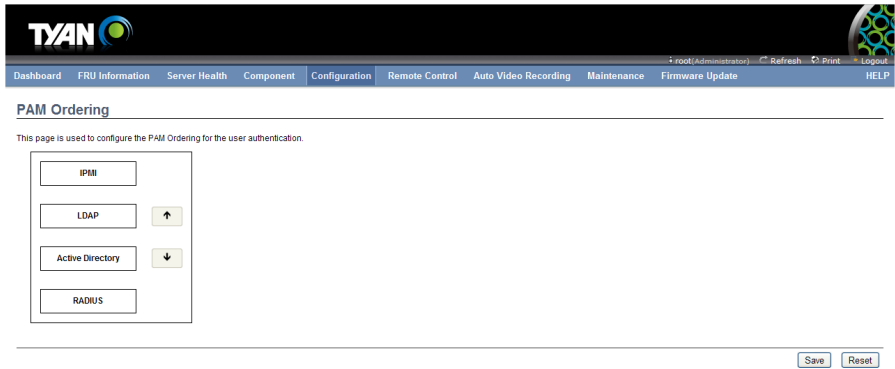
5. Click **Refresh** button to reload the date and time settings

6. Click **Save** button to save the entries.

7. Click **Reset** button to reset the entries.

2.6.12 PAM Ordering Settings

This page is used to configure the PAM ordering for user authentication in to the BMC. Opening PAM Ordering page, click Configuration > PAM Order of the menu bar. A sample screenshot of PAM Ordering Page is shown below.



The fields of Configuration > PAM Ordering page are explained below.

Procedure

1. Select the required PAM module and click ↑ button to move the module one step before the existing module.
2. Select the required PAM module and click ↓ button to move the module one step after the existing module.
3. Click **Save** to save any changes made.
4. Click **Reset** to reset the modified changes.

2.6.13 PEF

Platform Event Filtering (PEF) provides a mechanism for configuring the BMC to take selected actions on event messages that it receives or has internally generated. These actions include operations such as system power-off, system reset, as well as triggering the generation of an alert.

In MegaRAC GUI, the PEF Management is used to configure the following:

- Event Filter
- Alert Policy
- LAN Destination

To open the PEF Management Settings Page, click **Configuration** → **PEF** from the main menu. A sample screenshot of PEF Management Page is shown in the screenshot below.

Event Filter Table

A PEF implementation is recommended to provide at least 16 entries in the event filter table. A subset of these entries should be pre-configured for common system failure events, such as over-temperature, power system failure, fan failure events, etc. Remaining entries can be made available for 'OEM' or System Management Software configured events. Note that individual entries can be tagged as being reserved for system use - so this ratio of pre-configured entries to run-time configurable entries can be reallocated if necessary.

PEF Management

Use this page to configure Event Filter, Alert Policy and LAN Destination. To delete or modify an entry, select it in the list and click "Delete" or "Modify". To add a new entry, select an unconfigured slot and click "Add".

Event Filter
Alert Policy
LAN Destination

Configured Event Filter count: 15

PEF ID	Filter Configuration	Event Filter Action	Event Severity	Sensor Name
1	Enabled	[Alert]	Unspecified	Any
2	Enabled	[Alert]	Unspecified	Any
3	Enabled	[Alert]	Unspecified	Any
4	Enabled	[Alert]	Unspecified	Any
5	Enabled	[Alert]	Unspecified	Any
6	Enabled	[Alert]	Unspecified	Any
7	Enabled	[Alert]	Unspecified	Any
8	Enabled	[Alert]	Unspecified	Any
9	Enabled	[Alert]	Unspecified	Any
10	Enabled	[Alert]	Unspecified	Any
11	Enabled	[Alert]	Unspecified	Any
12	Enabled	[Alert]	Unspecified	Any
13	Enabled	[Alert]	Unspecified	Any
14	Enabled	[Alert]	Unspecified	Any
15	Enabled	[Alert]	Unspecified	Any
16	~	~	~	~
17	~	~	~	~
18	~	~	~	~
19	~	~	~	~
20	~	~	~	~
21	~	~	~	~
22	~	~	~	~
23	~	~	~	~
24	~	~	~	~
25	~	~	~	~
26	~	~	~	~
27	~	~	~	~
28	~	~	~	~
29	~	~	~	~
30	~	~	~	~
31	~	~	~	~
32	~	~	~	~
33	~	~	~	~
34	~	~	~	~
35	~	~	~	~
36	~	~	~	~
37	~	~	~	~
38	~	~	~	~
39	~	~	~	~
40	~	~	~	~

PEF Management

Use this page to configure Event Filter, Alert Policy and LAN Destination. To delete or modify a entry, select it in the list and click "Delete" or "Modify". To add a new entry, select an unconfigured slot and click "Add".

Event Filter Alert Policy LAN Destination

Configured Event Filter count: 15

PEF ID	Filter Configuration	Event Filter Action	Event Severity	Sensor Name
22	--	--	--	--
23	--	--	--	--
24	--	--	--	--
25	--	--	--	--
26	--	--	--	--
27	--	--	--	--
28	--	--	--	--
29	--	--	--	--
30	--	--	--	--
31	--	--	--	--
32	--	--	--	--
33	--	--	--	--
34	--	--	--	--
35	--	--	--	--
36	--	--	--	--
37	--	--	--	--
38	--	--	--	--
39	--	--	--	--
40	--	--	--	--

Add Modify Delete

The fields of PEF Management – Event Filter Tab are explained below.

This page contains the list of configured PEF's.

PEF ID: This field displays the ID for the newly configured PEF entry (read only).

Filter configuration: Check box to enable the PEF settings.

Event Filter Action: Check box to enable PEF Alert action. This is a mandatory field.

Event Severity: To choose any one of the Event severity from the list.

Sensor Name: To choose the particular sensor from the sensor list.

Add: To add the new event filter entry and return to Event filter list.

Modify: To modify the existing entries.

Cancel: To cancel the modification and return to Event filter list.

Procedure

1. Click the **Event Filter** Tab to configure the event filters in the available slots
2. To Add an Event Filter entry, select a free slot and click **Add** to open the Add event Filter entry Page. A sample screenshot of Add Event Filter Page is seen in the screenshot below.

PEF Management

Use this page to configure Event Filter, Alert Policy and LAN Destination. To delete or modify a entry, select it in the list and click "Delete" or "Modify". To add a new entry, select an unconfigured slot and click "Add".

Event Filter

PEF ID
14
15
16
17
18
19
20
21
22
23
24

Add Event Filter entry

Event Filter Configuration

PEF ID:

Filter Configuration: Enable

Event Severity:

Filter Action configuration

Event Filter Action: Alert

Power Action:

Alert Policy Number:

Generator ID configuration

Generator ID Data: Raw Data

Generator ID 1:

Generator ID 2:

Event Generator: Slave type Software type

Slave Address/Software ID:

Channel Number:

IPMB Device LUN:

Sensor configuration

Sensor Type:

Sensor Name:

Event Options:

Event Data configuration

Event Trigger:

Event Data 1 AND Mask:

Event Data 1 Compare 1:

Event Data 1 Compare 2:

Event Data 2 configuration

Event Data 2 AND Mask:

Event Data 2 Compare 1:

Event Data 2 Compare 2:

Event Data 3 configuration

Event Data 3 AND Mask:

Event Data 3 Compare 1:

Event Data 3 Compare 2:

3. In the Event Filter Configuration section,
 - PEF ID displays the ID for configured PEF entry (read-only).
 - In filter configuration, check the box to enable the PEF settings.
 - In Event Severity, select any one of the Event severity from the list.

4. In the Filter Action configuration section,
 - Event Filter Action is a mandatory field and checked by default, which enable PEF Alert action (read-only).
 - Select any one of the Power action either Power down, Power reset or Power cycle from the drop down list
 - Choose any one of the configured alert policy number from the drop down list.

NOTE: Alert Policy has to be configured - under Configuration → PEF → Alert Policy.

5. In the Generator ID configuration section,
 - Check Generator ID Data option to fill the Generator ID with raw data.
 - Generator ID 1 field is used to give raw generator ID1 data value.
 - Generator ID 2 field is used to give raw generator ID2 data value.

NOTE: In RAW data field, to specify hexadecimal value prefix with '0x'.

- In the Event Generator section, choose the event generator as Slave Address - if event was generated from IPMB. Otherwise as System Software ID - if event was generated from system software.
- In the Slave Address/Software ID field, specify corresponding I²C Slave Address or System Software ID.
- Choose the particular channel number that event message was received over. Or choose '0' if the event message was received via the system interface, primary IPMB, or internally generated by the BMC.
- Choose the corresponding IPMB device LUN if event generated by IPMB.

6. In the Sensor configuration section,
 - Select the s type of sensor that will trigger the event filter action.
 - In the sensor name field, choose the particular sensor from the sensor list.
 - Choose event option to be either All Events or Sensor Specific Events.

7. In the Event Data configuration section,
 - Event Trigger field is used to give Event/Reading type value.

NOTE: Value ranges from 1 to 255.

- Event Data 1 AND Mask field is used to indicate wildcarded or compared bits.

NOTE: Value ranges from 0 to 255.

- Event Data 1 Compare 1 & Event Data 1 Compare 2 field is used to indicate whether each bit position's comparison is an exact comparison or not.

NOTE: Value ranges from 0 to 255.

8. In the Event Data 2 configuration section,
 - Event Data 2 AND Mask field is similar to Event Data 1 AND Mask.
 - Event Data 2 Compare 1 & Event Data 2 Compare 2 fields are similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.
9. In the Event Data 3 configuration section,
 - Event Data 3 AND Mask field is similar to Event Data 1 AND Mask.
 - Event Data 3 Compare 1 & Event Data 3 Compare 2 fields are similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.
10. Click **Modify** to accept the modification and return to Event filter list.
11. Click **Reset** to reset the modification done.
12. Click on **Cancel** to cancel the modification and return to Event filter list.
13. In the Event filter list, click **Modify** to modify the existing filter.
14. In the Event filter list, click **Delete** to delete the existing filter.

Alert Policy Tab

This page is used to configure the Alert Policy and LAN destination. You can add, delete or modify an entry in this page.

Configured Alert Policy count: 0

Policy Entry #	Policy Number	Policy Configuration	Policy Set	Channel Number	Destination Selector
1	~	~	~	~	~
2	~	~	~	~	~
3	~	~	~	~	~
4	~	~	~	~	~
5	~	~	~	~	~
6	~	~	~	~	~
7	~	~	~	~	~
8	~	~	~	~	~
9	~	~	~	~	~
10	~	~	~	~	~
11	~	~	~	~	~

Add Modify Delete

PEF Management – Alert Policy

The fields of PEF Management – Alert Policy Tab are explained below.

Policy Entry #: Displays Policy entry number for the newly configured entry (read-only).

Policy Number: Displays the Policy number of the configuration.

Policy Configuration: To enable or disable the policy settings.

Policy Set: To choose any one of the Policy set values from the list.

0 - Always send alert to this destination.

1 - If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set.

2 - If alert to previous destination was successful, do not send alert to this destination. Do not process any more entries in this policy set.

3 - If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different channel.

4 - If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different destination type.

Channel Number: To choose a particular channel from the available channel list.

Destination Selector: To choose a particular destination from the configured destination list.

NOTE: LAN Destination has to be configured - under **Configuration → PEF → LAN Destination**.

Add: To save the new alert policy and return to Alert Policy list.

Modify: To modify the existing entries.

Cancel: To cancel the modification and return to Alert Policy list.

Procedure:

1. In the Alert Policy Tab, select the slot for which you have to configure the Alert policy. That is, In the **Event Filter Entry Page**, if you have chosen Alert Policy number as 4, you have to configure the 4th slot (the slot with Policy Number 4) in the Alert Policy Tab.
2. Select the slot and click **Add** to open the **Add Alert Policy Entry Page** as shown in the screenshot below.



Policy Entry #	3
Policy Number	1
Policy Configuration	<input type="checkbox"/> Enable
Policy Set	0
Channel Number	1
Destination Selector	1
Alert String	<input type="checkbox"/> Event Specific
Alert String Key	0

3. **Policy Entry #** is a read only field.
4. Select the **Policy Number** from the list.
5. In the **Policy Configuration** field, check **Enable** if you wish to enable the policy settings.
6. In the **Policy Set** field, choose any of the Policy set from the list.
7. In the **Channel Number** field, choose particular channel from the available channel list.

8. In the **Destination Selector field**, choose particular destination from the configured destination list.

NOTE: LAN Destination has to be configured under **Configuration → PEF → LAN Destination**. That is if you select the number 4 for destination selector in Alert Policy Entry page, then you have to configure the 4th slot (LAN Destination Number 4) in the LAN Destination tab.

9. In the **Alert String** field, enable the check box if the Alert policy entry is Event Specific.
10. In the **Alert String Key** field, choose any one value that is used to look up the Alert String to send for this Alert Policy entry.
11. Click **Add** to save the new alert policy and return to Alert Policy list.
12. Click **Cancel** to cancel the modification and return to Alert Policy list.
13. In the Alert Policy list, to modify a configuration, select the slot to be modified and click **Modify**.
14. In the **Modify Alert Policy Entry Page**, make the necessary changes and click **Modify**.
15. In the Alert Policy list, to delete a configuration, select the slot and click **Delete**.

PEF Management LAN Destination Page

This page is used to configure the Event filter, Alert Policy and LAN destination. A sample screenshot of PEF Management LAN Destination Page is given below.

PEF Management

Use this page to configure Event Filter, Alert Policy and LAN Destination. To delete or modify an entry, select it in the list and click "Delete" or "Modify". To add a new entry, select an unconfigured slot and click "Add".

Event Filter | Alert Policy | **LAN Destination**

LAN Channel: 1

Configured LAN Destination count: 0

LAN Destination	Destination Type	Destination Address
1	~	~
2	~	~
3	~	~
4	~	~
5	~	~
6	~	~
7	~	~
8	~	~
9	~	~
10	~	~
11	~	~
12	~	~
13	~	~
14	~	~
15	~	~

Send Test Alert | Add | Modify | Delete

PEF Management LAN Destination

The fields of PEF Management – LAN Destination Tab are explained below.

LAN Destination: Displays Destination number for the newly configured entry (read only).

Destination Type: Destination type can be either an SNMP Trap or an Email alert. For Email alerts, the 3 fields - destination Email address, subject and body of the message needs to be filled. The SMTP server information also has to be added - under Configuration->SMTP. For SNMP Trap, only the destination IP address has to be filled.

Destination Address: If Destination type is SNMP Trap, then enter the IP address of the system that will receive the alert. Destination address will support the following:

- IPv4 address format
- IPv6 address format

If Destination type is Email Alert, then give the email address that will receive the email.

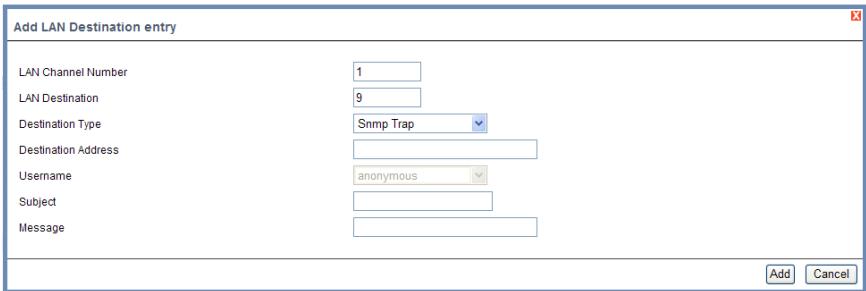
Subject & Message: These fields must be configured if email alert is chosen as destination type. An email will be sent to the configured email address in case of any severity events with a subject specified in subject field and will contain the message field's content as the email body.

Add: To save the new LAN destination and return to LAN destination list.

Cancel: To cancel the modification and return to LAN destination list.

Procedure

1. In the **LAN Destination Tab**, choose the slot to be configured. This should be the same slot that you have selected in the Alert Policy Entry- Destination Selector field. That is if you have chosen the Destination Selector as 4 in the Alert Policy Entry page of Alert Policy Tab, then you have to configure the 4th slot of LAN Destination Page.
2. Select the slot and click **Add**. This opens the **Add LAN Destination entry**.



The screenshot shows a dialog box titled "Add LAN Destination entry". It contains the following fields and values:

- LAN Channel Number: 1
- LAN Destination: 9
- Destination Type: Snmp Trap (dropdown menu)
- Destination Address: (empty text box)
- Username: anonymous (dropdown menu)
- Subject: (empty text box)
- Message: (empty text box)

At the bottom right of the dialog, there are two buttons: "Add" and "Cancel".

Add LAN Destination Entry Page

3. In the **LAN Destination** field, the destination for the newly configured entry is displayed and this is a read only field.
4. In the **Destination Type** field, select the one of the types.
5. In the **Destination Address** field, enter the destination address.
NOTE: If Destination type is Email Alert, then give the email address that will receive the email.
6. Select the **User Name** from the list of users.
7. In the **Subject** field, enter the subject.
8. In the **Message** field, enter the message.
9. Click **Add** to save the new LAN destination and return to LAN destination list.
10. Click **Cancel** to cancel the modification and return to LAN destination list.
11. In the LAN Destination Tab, to modify a configuration, select the row to be

modified and click **Modify**.

12. In the **Modify LAN Destination Entry** page, make the necessary changes and click **Modify**.
13. In the LAN Destination Tab, to delete a configuration, select the slot and click **Delete**.

2.6.14 RADIUS

RADIUS is a modular, high performance and feature-rich RADIUS suite including server, clients, development libraries and numerous additional RADIUS related utilities.

In MegaRAC GUI, this page is used to set the RADIUS Authentication.

To open the RADIUS Settings Page, click **Configuration** → **RADIUS** from the main menu. A sample screenshot of RADIUS Settings Page is shown in the screenshot below.

RADIUS Settings

Check the box below to enable RADIUS authentication and enter the required information to access the RADIUS server. Press the Save button to save your changes.

RADIUS Authentication Enable

Port

Server Address

Secret

Extended privileges KVM VMedia

Save Reset Advanced Setting

RADIUS Settings Page

The fields of RADIUS Settings Page are explained below.

RADIUS Authentication: Option to enable RADIUS authentication.

Port: The RADIUS Port number.

Note:

- Default Port is 1812.

Time Out: The Time out value in seconds.

Note:

- Default Timeout value is 3seconds.
- Timeout value ranges from 3 to 300.

Server Address: The IP address of RADIUS server.

Note:

- IP Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx".

- Each Number ranges from 0 to 255.
- First Number must not be 0.

Secret: The Authentication Secret for RADIUS server.

Note:

- This field will not allow more than 31 characters.
- Secret must be at least 4 characters long.
- White space is not allowed.

Save: To save the settings.

Reset: To reset the modified changes.

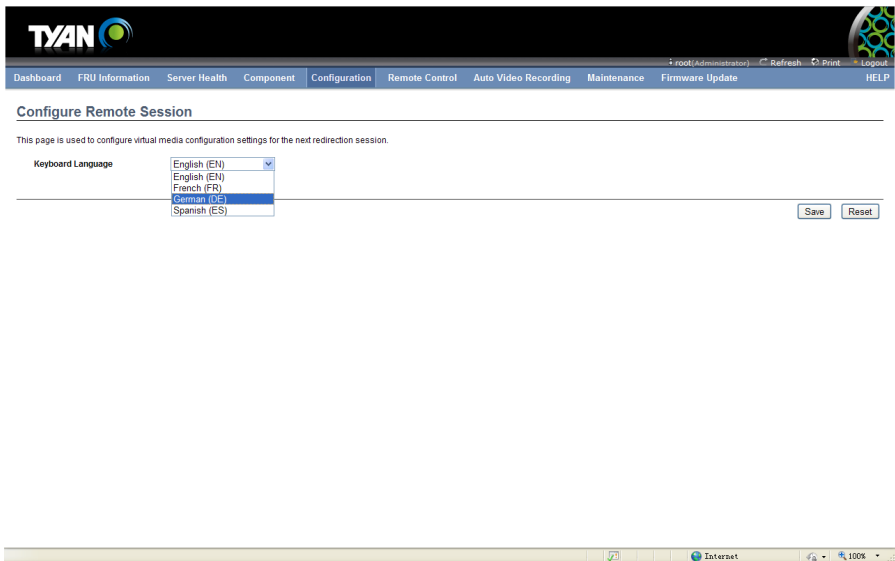
Procedure

1. Enable the **RADIUS Authentication** checkbox to authenticate the RADIUS.
2. Enter the port number in the **Port Number** field.
3. Enter the time out value in seconds in the **Time out** field.
4. Enter the address of the server in the **Server Address** field.
5. Enter the authentication secret for RADIUS Server in the **Secret** field.
6. Click **Save** to save the entered details.
7. Click **Reset** to reset the entered details.

2.6.15 Remote Session

In MegaRAC GUI, use this page to configure virtual media configuration settings for the next redirection session. Encryption is disabled by default.

To open the Configure Remote Session Page, click **Configuration** → **Remote Session** from the main menu. A sample screenshot of Configure Remote Session Page is shown in the screenshot below.



2.6.16 Services

This page displays the basic information about services running in the BMC. Only Administrator can modify the service.

To open Services page, click Configuration > Services from the menu bar. A sample screenshot of Services Page is shown below.

The screenshot shows the BMC web interface. At the top is the TYAN logo and a navigation menu with items: Dashboard, FRU Information, Server Health, Component, Configuration, Remote Control, Auto Video Recording, Maintenance, Firmware Update, and HELP. The main content area is titled "Services" and contains a table of services. Below the table is a "Modify" button. At the bottom of the screenshot is a Windows taskbar showing the system tray with a volume icon, network status (Internet), and a zoom level of 100%.

#	Service Name	Current State	Interfaces	Nonsecure Port	Secure Port	Timeout	Maximum Sessions	Active Sessions
1	web	Active	eth0	80	443	300	20	1
2	kvm	Active	eth0	7578	7582	N/A	4	0
3	cd-media	Active	eth0	5120	5124	N/A	1	0
4	fd-media	Active	eth0	5122	5126	N/A	1	0
5	hd-media	Active	eth0	5123	5127	N/A	1	0
6	ssh	Active	N/A	N/A	22	600	N/A	N/A
7	telnet	Inactive	N/A	23	N/A	600	N/A	N/A

The fields of Services Page are explained below.

Service Name: Displays service name of the selected slot (read-only).

Current State: Displays the current status of the service, either active or inactive state.

Interfaces: It shows the interface in which service is running.

Nonsecure Port: This port is used to configure non secure port number for the service.

- Web default port is 80
- KVM default port is 7578
- CD Media default port is 5120
- FD Media default port is 5122
- HD Media default port is 5123
- Telnet default port is 23

Note: SSH service will not support non secure port. If single port feature is enabled, KVM, CD Media, FD Media and HD Media ports cannot be edited.

Secure Port: Used to configure secure port number for the service.

- Web default port is 443
- KVM default port is 7582
- CD Media default port is 5124
- FD Media default port is 5126
- HD Media default port is 5127
- SSH default port is 22

Note: Telnet service will not support secure port. If single port feature is enabled, KVM, CD Media, FD Media and HD Media ports cannot be edited.

Timeout: Displays the session timeout value of the service. For web, SSH and telnet service, user can configure the session timeout value.

Note:

- Web timeout value ranges from 300 to 1800 seconds.
- SSH and Telnet timeout value ranges from 30 to 1800 seconds.
- SSH and telnet service will be using the shared timeout value. If the user configures SSH timeout value, it will be applied to telnet service also and vice versa.

Maximum Sessions: Displays the maximum number of allowed sessions for the service.

Modify: To modify the existing services.

Procedure

1. Select a slot and click Modify to modify the configuration of the service. Alternatively, double click on the slot.

Note: Whenever the configuration is modified, the service will be restarted automatically. User has to close the existing opened session for the service if needed.

2. This opens the Modify Service screen as shown in the screenshot below.
3. Modify Service
4. Service Name is a read only field
5. Activate the Current State by enabling the Activate check box.

Note: The Interface, Nonsecure port, Secure port, Time out and Maximum Sessions will not be active unless the current state is active.

6. Choose any one of the available interfaces from the Interface drop-down list.
7. Enter the Nonsecure port number in the Nonsecure Port field.
8. Enter the Secure Port Number in the Secure Port field.
9. Enter the timeout value in the Timeout field.

Note: The values in the Maximum Sessions field cannot be modified.

10. Click Modify to save the entered changes and return to the Services Page.
11. Click Cancel to exit.

2.6.17 SMTP

Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

Using the MegaRAC GUI, you can configure the SMTP settings of the device.

To open the SMTP Settings Page, click **Configuration** → **SMTP** from the main menu. A sample screenshot of SMTP Settings Page is shown in the screenshot below.

The screenshot shows the 'SMTP Settings' page in the MegaRAC GUI. The page has a navigation bar at the top with the following items: Dashboard, FRU Information, Server Health, Component, Configuration, Remote Control, Auto Video Recording, Maintenance, Firmware Update, and HELP. The main content area is titled 'SMTP Settings' and contains the following sections:

- LAN Channel Number:** A dropdown menu with '1' selected.
- Sender Address:** A text input field.
- Machine Name:** A text input field.
- Primary SMTP Server:**
 - SMTP Support
 - Server Address: A text input field.
 - SMTP Server requires Authentication
 - User Name: A text input field.
 - Password: A text input field.
- Secondary SMTP Server:**
 - SMTP Support
 - Server Address: A text input field.
 - SMTP Server requires Authentication
 - User Name: A text input field.
 - Password: A text input field.

At the bottom right of the page, there are 'Save' and 'Reset' buttons.

SMTP Settings Page

SMTP Server IP: The IP address of the SMTP Server.

Note:

- IPv4 Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx".
 - Each Number ranges from 0 to 255.
 - First Number must not be 0.
 - IPv6 Address made of 8 numbers separated by IP colon ":" or double colon "::".
- Eg: 2004::2010
- Each field ranges from 0 to FFFF.

Sender Address: The email address of the sender valid on the SMTP Server.

Machine Name: Name of the SMTP Server.

- Machine Name is a string of maximum 15 alpha-numeric characters.
- Space and special characters are not allowed.

SMTP Server requires Authentication: Option to enable SMTP Authentication.

Note: Server Authentication Types supported are:

- CRAM-MD5
- LOGIN
- PLAIN

If the SMTP server does not support any one of the above authentication types, the user will get an error message stating, "Authentication type is not supported by SMTP Server"

Username: Username using which you wish to access SMTP Accounts.

Note:

- User Name can be of length 4 to 15 alpha-numeric characters.
- It must start with an alphabet.
- Special characters ','(comma), ':'(colon), ';' (semicolon), ' '(space) and '\\(backslash) are not allowed.

Password: Password for the SMTP User Account.

Note: This field will not allow more than 19 characters.

- Password must be at least 4 characters long.
- White space is not allowed.

Save: To save the entries.

Reset: To reset the entries.

Procedure

1. Enter the SMTP Server IP in the field given.
2. Enter your email address in the Sender Address field.
3. Enter the IPMI machine name in the Machine Name field.
4. Enable the check box SMTP Server requires Authentication if you want to authenticate SMTP Server.
5. Enter your User name in the given field.
6. Enter your Password in the given field.
7. Click Save to save the entered details.
8. Click Reset to update the entered details.

2.6.18 SSL

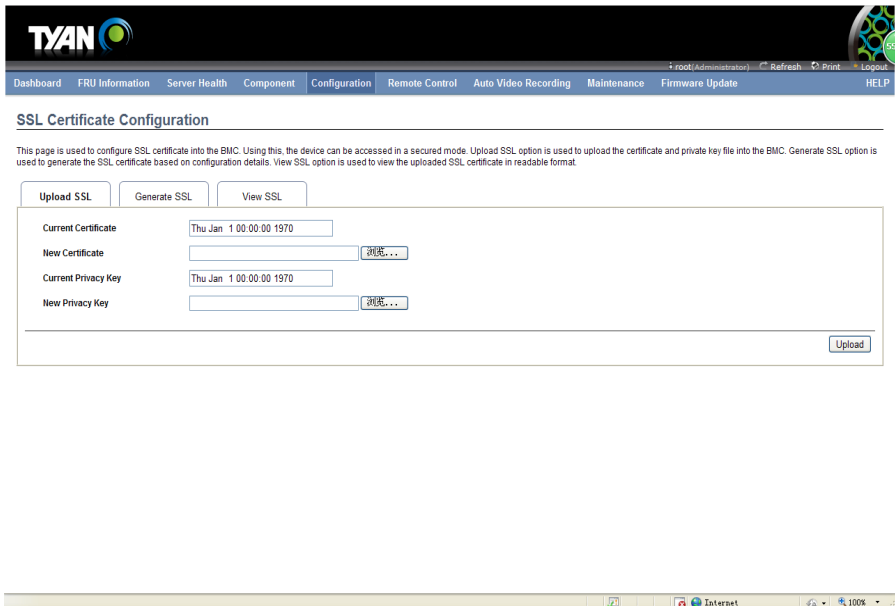
The **Secure Socket Layer (SSL)** protocol was created by Netscape to ensure secure transactions between web servers and browsers. The protocol uses a third party, a **Certificate Authority (CA)**, to identify one end or both end of the transactions.

Using the MegaRAC GUI, configure SSL certificate into the BMC. Using this, the device can be accessed in a secured mode.

To open the SSL Certificate Configuration Page, click **Configuration** → **SSL** from the main menu. There are three tabs in this page.

- **Upload SSL** option is used to upload the certificate and private key file into the BMC.
- **Generate SSL** option is used to generate the SSL certificate based on configuration details.
- **View SSL** option is used to view the uploaded SSL certificate in readable format.

A sample screenshot of SSL Certificate Configuration Page is shown in the screenshot below.



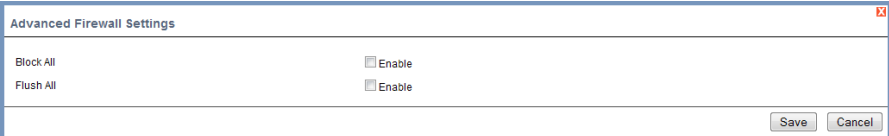
2.6.19 System Firewall

In MegaRAC GUI, the System Firewall page allows you to configure the firewall settings. The firewall can be set for a range or IP Addresses or Port Addresses. To view this page, you must at least be an operator. Only administrators can add or delete a firewall.

To open System Firewall page, click Configuration > System Firewall from the menu bar.

Advanced Settings

1. Click on the Advanced Settings button. This opens the Advanced Firewall Settings window as shown below.



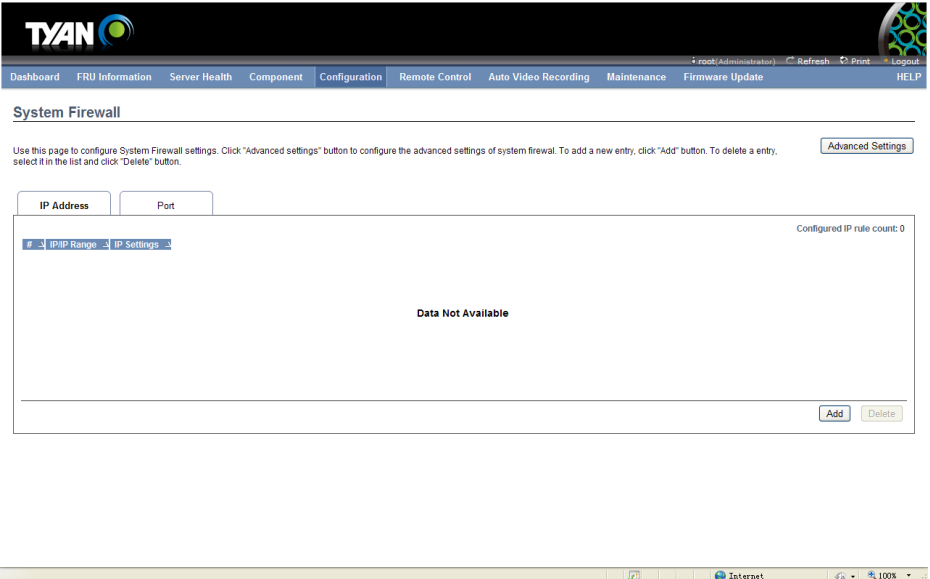
Advanced Firewall Settings

Block All Enable

Flush All Enable

Save Cancel

2. Block All blocks all the incoming IP's and Port's. Check this option to enable this feature.
3. Flush All is to flush all the system firewall rules. Check this option to enable this feature.
4. Click Save to save the changes made else click Cancel to go back to the previous screen.



TYAN

root/Administrator Refresh Print Logout HELP

Dashboard FRU Information Server Health Component Configuration Remote Control Auto Video Recording Maintenance Firmware Update

System Firewall

Use this page to configure System Firewall settings. Click "Advanced settings" button to configure the advanced settings of system firewall. To add a new entry, click "Add" button. To delete an entry, select it in the list and click "Delete" button. [Advanced Settings](#)

IP Address	Port
Data Not Available	

Configured IP rule count: 0

Add Delete

Internet 100%

The fields of System Firewall - IP Address tab are explained below.

IP/IP Address Range: Lists all the IP Address or Range of IP Addresses that are already configured.

IP Settings: To indicate the corresponding IP Address or range of IP Addresses rules that Allow or Block.

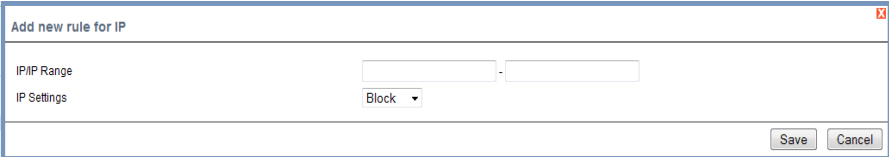
Add: To add a new entry to the firewall entry either IP or Sections

Delete: To delete the selected slot.

Procedure

To block or allow an IP address or range of IP addresses,

1. Click Add button to add a new rage of IP address.



The screenshot shows a dialog box titled "Add new rule for IP". It has a close button in the top right corner. The dialog contains two main sections: "IP/IP Range" and "IP Settings". The "IP/IP Range" section has two text input fields separated by a dot, and a dropdown menu below them currently set to "Block". The "IP Settings" section has a single text input field. At the bottom right of the dialog, there are two buttons: "Save" and "Cancel".

2. In the Add new rule for IP window, Enter the IP address or a range of IP addresses in the IP/ IP range field.

Note: IP Address will support IPv4 Address format only:

- IPv4 Address made of 4 numbers separated by dots as in xxx.xxx.xxx.xxx.
- Each number ranges from 0 to 255.
- First number must not be 0.

3. Enter the IP settings to be either Block or Allow. IP Settings are used to determine the rule whether block or allow from the configured IP or IP Range.

4. Click Save to save the changes made else click Cancel to go back to the previous screen.

5. To delete an IP address or a range of IP addresses, select the slot and click Delete.

2.6.20 User Management

In MegaRAC GUI, the User Management Page allows you to view the current list of user slots for the server. You can add a new user and modify or delete the existing users.

To open the User Management Page, click **Configuration** → **Users** from the main menu. A sample screenshot of User Management Page is shown in the screenshot below.

The screenshot displays the 'User Management' page in the TYAN MegaRAC GUI. The page title is 'User Management' and it indicates 'Number of configured users: 2'. Below the title is a descriptive text: 'The list below shows the current list of available users. To delete or modify a user, select the user name from the list and click "Delete User" or "Modify User". To add a new user, select an unconfigured slot and click "Add User"'. The main content is a table with the following data:

UserID ↘	Username ↘	User Access ↘	Network Privilege ↘	SNMP Status ↘	Email ID ↘
1	anonymous	Enabled	Administrator	Disabled	~
2	root	Enabled	Administrator	Enabled	~
3	~	~	~	~	~
4	~	~	~	~	~
5	~	~	~	~	~
6	~	~	~	~	~
7	~	~	~	~	~
8	~	~	~	~	~
9	~	~	~	~	~
10	~	~	~	~	~

At the bottom right of the table, there are three buttons: 'Add User', 'Modify User', and 'Delete User'.

User Management

The fields of User Management Page are explained below.

User ID: Displays the ID number of the user.

Note: The list contains a maximum of ten users only.

User Name: Displays the name of the user.

Email ID: Displays email address of the user.

Network Privilege: Displays the network access privilege of the user.

Add User: To add a new user.

Modify User: To modify an existing user.

Delete User: To delete an existing user

Note: The Free slots are denoted by "~" in all columns for the slot.

Procedure

Add a new user:

1. To add a new user, select a free slot and click **Add User**. This opens the Add User screen as shown in the screenshot below.

The screenshot shows the 'Add User' configuration window. The left sidebar lists the following fields: Username, Password Size, Password, Confirm Password, User Access, Network Privilege, Extended Privileges, SNMP Status, SNMP Access, Authentication Protocol, Privacy Protocol, Email ID, Email Format, and New SSH Key. The main area contains the following controls: Username (text input), Password Size (radio buttons for 16 Bytes and 20 Bytes), Password (text input), Confirm Password (text input), User Access (checkbox for Enable), Network Privilege (dropdown menu set to Administrator), Extended Privileges (checkboxes for KVM and VMedia), SNMP Status (checkbox for Enable), SNMP Access (dropdown menu set to Read Only), Authentication Protocol (dropdown menu set to SHA), Privacy Protocol (dropdown menu set to DES), Email ID (text input), Email Format (dropdown menu set to AMI-Format), and New SSH Key (text input with a '浏览...' button). At the bottom right are 'Add' and 'Cancel' buttons.

Add User Page

2. Enter the name of the user in the **User Name** field.
Note:
 - User Name is a string of 4 to 16 alpha-numeric characters.
 - It must start with an alphabetical character.
 - It is case-sensitive.
 - Special characters ','(comma), '.'(period), ':'(colon), ';' (semicolon), ' '(space), '/'(slash), '\'(backslash), '('(left bracket) and ')' (right bracket) are not allowed.
3. In the **Password** and **Confirm Password** fields, enter and confirm your new password.
4. **Note:**
 - Password must be at least 8 characters long.
 - White space is not allowed.
 - This field will not allow more than 20 characters.
5. In the **Network Privilege** field, enter the network privilege assigned to the user which could be Administrator, Operator, User or No Access.
6. In the **Email ID** field, enter the email ID of the user. If the user forgets the password, the new password will be mailed to the configured email address.
Note: SMTP Server must be configured to send emails.
7. In the **New SSK Key** field, click Browse and select the SSH key file
Note: SSH key file should be of pub type.

8. Click **Add** to save the new user and return to the users list.
9. Click **Cancel** to cancel the modification and return to the users list.

Modify an existing User

1. Select an existing user from the list and click **Modify User**. This opens the Add User screen as shown in the screenshot below.

The screenshot shows a 'Modify User' window with the following fields and values:

- Username: root
- Change Password:
- Password Size: 16 Bytes 20 Bytes
- Password: [Empty]
- Confirm Password: [Empty]
- User Access: Enable
- Network Privilege: Administrator
- Extended Privileges: KVM VMedia
- SNMP Status: Enable
- SNMP Access: Read Only
- Authentication Protocol: SHA
- Privacy Protocol: DES
- Email ID: [Empty]
- Email Format: AMI-Format
- Uploaded SSH Key: Not Available
- New SSH Key: [Empty] 浏览...

Buttons: Modify, Cancel

Modify User Page

2. Edit the required fields.
3. To change the password, enable the **Change Password** option.
4. After editing the changes, click **Modify** to return to the users list page.

Delete an existing User

To delete an existing user, select the user from the list and click **Delete User**.

Note: There is a list of reserved users which cannot be added / modified as BMC users. Please Refer “MEGARAC SP-X Platform Porting Guide” section “Changing the Configurations in PMC File-> User Configurations in PMC File” for the list of reserved users.

Important:

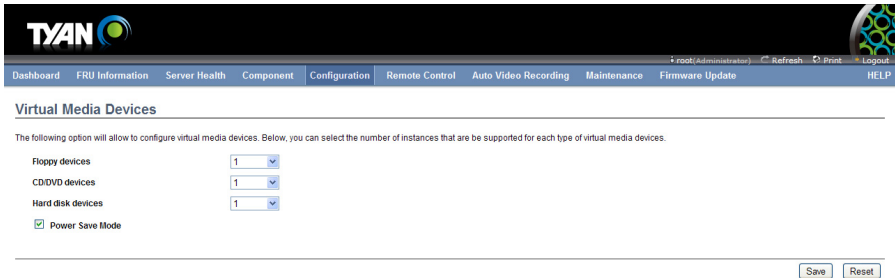
Reserved Users: There are certain reserved users which cannot be added as BMC Users. The list of reserved users are given below,

- sysadmin
- daemon
- sshd
- ntp
- stunnel4

2.6.21 Virtual Media

In MegaRAC GUI, this page is used to configure Virtual Media Devices settings. If you change the configuration of the Virtual Media Devices in this page, it show the appropriate device in the JViewer Vmedia dialog. For example, if you select two floppy devices in Configure Virtual Media Page, then in JViewer Vmedia, you can view two floppy device panel.

To open the Virtual Media Devices Page, click **Configuration** → **Virtual Media** from the main menu. A sample screenshot of Virtual Media Devices Page is shown in the screenshot below.



The following fields are displayed in this page.

Floppy devices: The number of floppy devices that support for Virtual Media redirection.

CD/DVD devices: The number of CD/DVD devices that support for Virtual Media redirection.

Harddisk devices: The number of harddisk devices that support for Virtual Media redirection.

Disable Power Save Mode: To enable or disable the virtual USB devices visibility in the host.

Save: To save the configured settings.

Reset: To reset the previously-saved values.

Procedure

1. Select the number of Floppy devices, CD/DVD devices and Harddisk devices from the drop-down list

Note: Maximum of two devices can be added in Floppy, CD/DVD and Harddisk drives.

2. Check the option Disable Power Save Mode to disable the virtual USB devices visibility in the host machine.

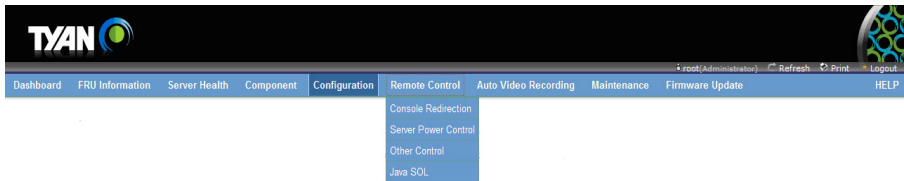
3. Click **Save** to save the changes made else click Reset to reset the previously saved values.

2.7 Remote Control

The Remote Control consists of the following menu items.

- Console Redirection
- Server Power Control
- Other Control
- JAVA SOL

A sample screenshot of the Remote Control menu is given below.



2.7.1 Console Redirection

The remote console application, which is started using the WebGUI, allows you to control your server's operating system remotely, using the screen, mouse, and keyboard, and to redirect local CD/DVD, Floppy diskette and hard disk/USB thumb drives as if they were connected directly to the server.

List of Supported Client Operating System

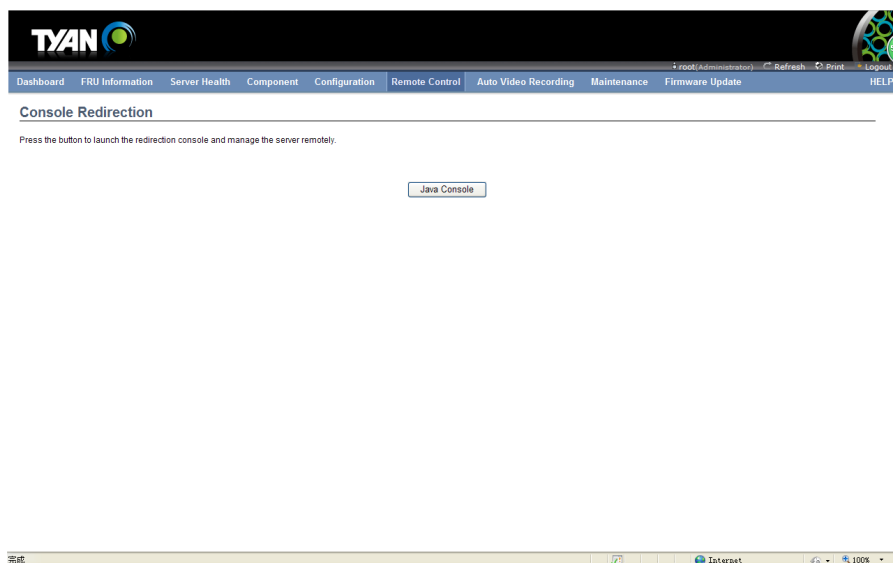
- winxp
- w2k3 - 32 bit
- w2k3 - 64 bit
- Windows 7 – 32 bit
- Windows 7 – 64 bit
- RHEL 4 - 32 bit
- RHEL 4 - 64 bit
- RHEL 5.4 - 32 bit
- RHEL 5.4 - 64 bit
- RHEL 6.0 - 64 bit
- RHEL 6.0 - 32 bit
- Ubuntu 9.10 LTS - 32
- Ubuntu 9.10 LTS - 64
- Ubuntu 10.04 LTS - 32 bit
- Ubuntu 10.04 LTS - 64 bit
- Ubuntu 8.10 -32
- Ubuntu 8.10 -64
- Ubuntu 11.10 Server - 32 bit
- Ubuntu 11.10 Server - 64 bit
- OpenSuse 11.2 -32

- OpenSuse 11.2 -64
- FC 9 - 32
- FC 9 - 64
- FC 10 - 32
- FC 10 - 64
- FC 12 - 32
- FC 12 - 64
- FC 13 - 32
- FC 13 - 64
- FC 14 - 32
- FC 14 - 64
- FC 15
- FC 16
- MAC -32
- MAC-64

List of Supported Host OS

- RHEL 5
- RHEL 5.3
- RHEL 5.4
- RHEL 6
- w2k3
- w2k8
- Windows 2008 R2
- Windows 2008 SP 2

- Win 2012 (64 bit)
- RHEL 4
- OpenSuse 11.2
- OpenSuse 10.x
- Ubuntu 8.10
- Ubuntu 9.10
- Ubuntu 11.04
- Ubuntu 11.10 Server
- Ubuntu Server 12.04 (64)
- SLES 11
- Debian 6
- CentOS 6.0



Browser Settings

For launching the KVM, pop-up block should be disabled. For Internet Explorer, enable the download file options from the settings.

Java Console

This is an OS independent plug-in which can be used in Windows as well as Linux with the help of JRE. JRE should be installed in the client's system. You can install JRE from the following link.

<http://www.java.com/en/download/manual.jsp>

The Console Redirection main menu consists of the following menu items.

- Video
- Keyboard
- Mouse
- Options
- Media
- Keyboard Layout
- Video Record
- Power
- Active Users
- Help

A detailed explanation of these menu items are given below.

2.7.1.1 Video

This menu contains the following sub menu items.

Pause redirection: This option is used for pausing Console Redirection.

Resume Redirection: This option is used to resume the Console Redirection when the session is paused.

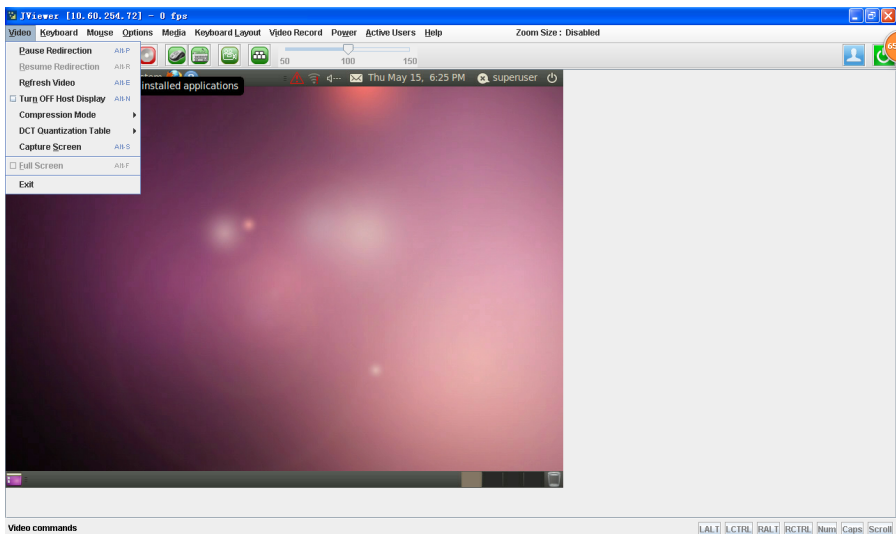
Refresh Video: This option can be used to update the display shown in the Console Redirection window.

Turn Off Host display: If you enable this option, the server display will be blank but you can view the screen in Console Redirection. If you disable this option, the display will be back in the server screen.

Capture Screen: This option is used to seize the picture of console redirection.

Full Screen: This option is used to view the Console Redirection in full screen mode (Maximize). This menu is enabled only when both the client and host resolution are same.

Exit: This option is used to exit the console redirection screen



2.7.1.2 Keyboard

This menu contains the following sub menu items.

Hold Right Ctrl Key: This menu item can be used to act as the right-side <CTRL> key when in Console Redirection.

Hold Right Alt Key: This menu item can be used to act as the right-side <ALT> key when in Console Redirection.

Hold Left Ctrl Key: This menu item can be used to act as the left-side <CTRL> key when in Console Redirection.

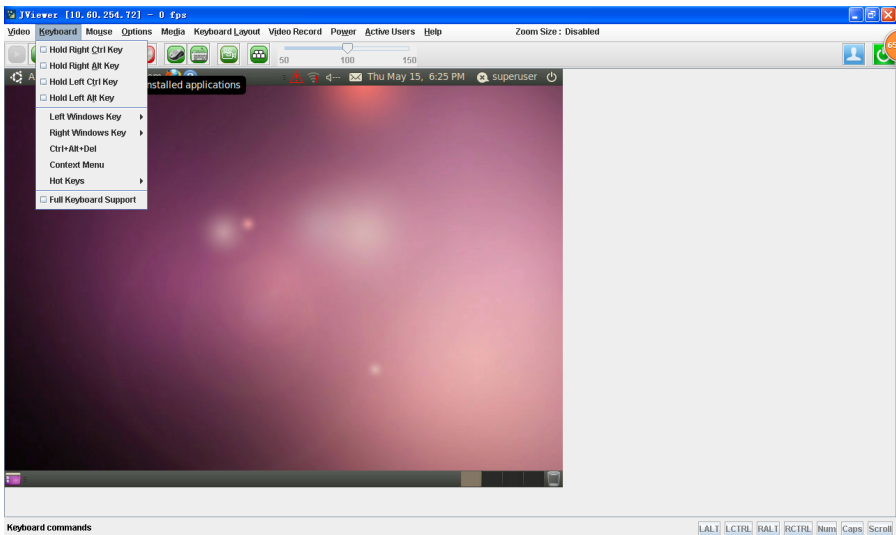
Hold Left Alt Key: This menu item can be used to act as the left-side <ALT> key when in Console Redirection.

Left Windows Key: This menu item can be used to act as the left-side <WIN> key when in Console Redirection. You can also decide how the key should be pressed: Hold Down or Press and Release.

Right Windows Key: This menu item can be used to act as the right-side <WIN> key when in Console Redirection. You can also decide how the key should be pressed: Hold Down or Press and Release.

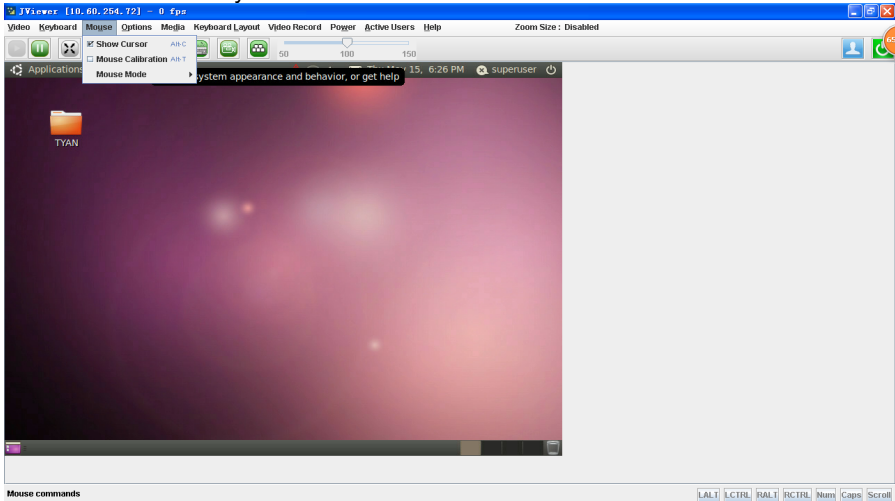
Alt+Ctrl+Del: This menu item can be used to act as if you depressed the <CTRL>, <ALT> and keys down simultaneously on the server that you are redirecting.

Context menu: This menu item can be used to act as the context menu key, when in Console Redirection.



2.7.1.3 Mouse

Show Cursor: This menu item can be used to show or hide the local mouse cursor on the remote client system.



Mouse Calibration: This menu item can be used only if the mouse mode is relative. In this step, the mouse threshold settings on the remote server will be discovered. The local mouse cursor is displayed in RED color and the remote cursor is part of the remote video screen. Both the cursors will be synchronized in the beginning. Please use '+' or '-' keys to change the threshold settings until both the cursors go out of synch. Please detect the first reading on which cursors go out of synch. Once this is detected, use 'ALT-T' to save the threshold value.

****Show Host Cursor:** This option is used to enable or disable the visibility of the host cursor.

Mouse Mode: This option handles mouse emulation from local window to remote screen using either of the two methods. Only 'Administrator' has the right to configure this option.

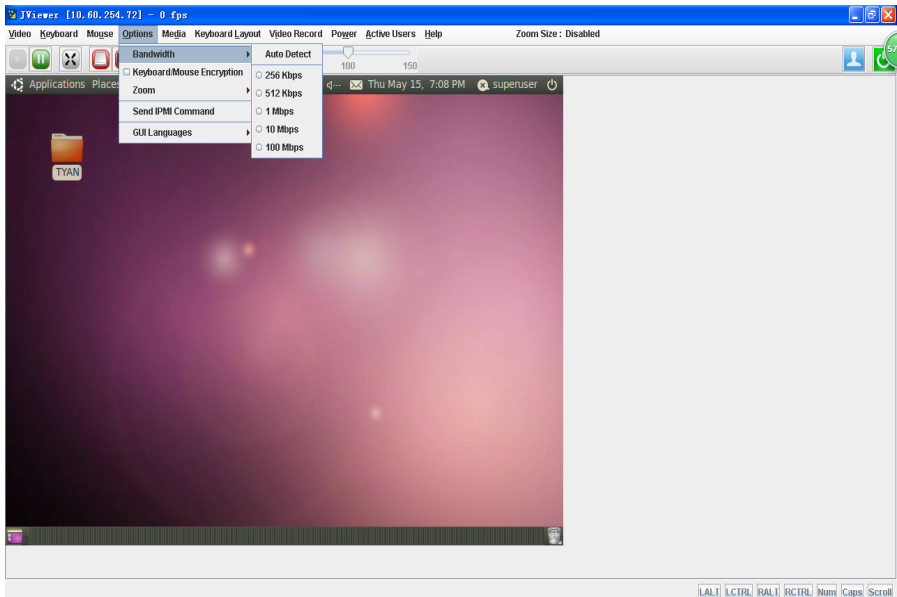
- **Absolute mouse mode:** The absolute position of the local mouse is sent to the server if this option is selected.
- **Relative mouse mode:** The Relative mode sends the calculated relative mouse position displacement to the server if this option is selected.
- **Other mouse mode:** This mouse mode sets the client cursor in the middle of the client system and will send the deviation to the host. This mouse mode is specific for SUSE Linux installation.

Note: Client cursor will be hidden always. If you want to enable, use Alt + C to access the menu. To view the Supported Operating Systems for Mouse Mode, click here.

2.7.1.4 Options

Band width: The Bandwidth Usage option allows you to adjust the bandwidth. You can select one of the following:

- Auto Detect - This option is used to detect client system keyboard layout automatically and send the key event to the host based on the Layout detected.
- 256 Kbps
- 512 Kbps
- 1 Mbps
- 10 Mbps
- 100Mbps



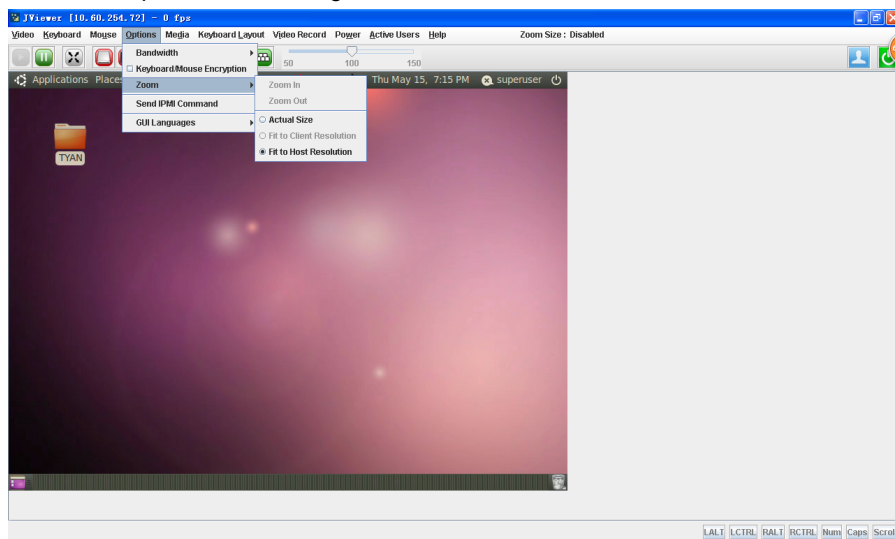
Keyboard/Mouse Encryption: This option allows you to encrypt keyboard inputs and mouse movements sent between the connections.

Zoom:

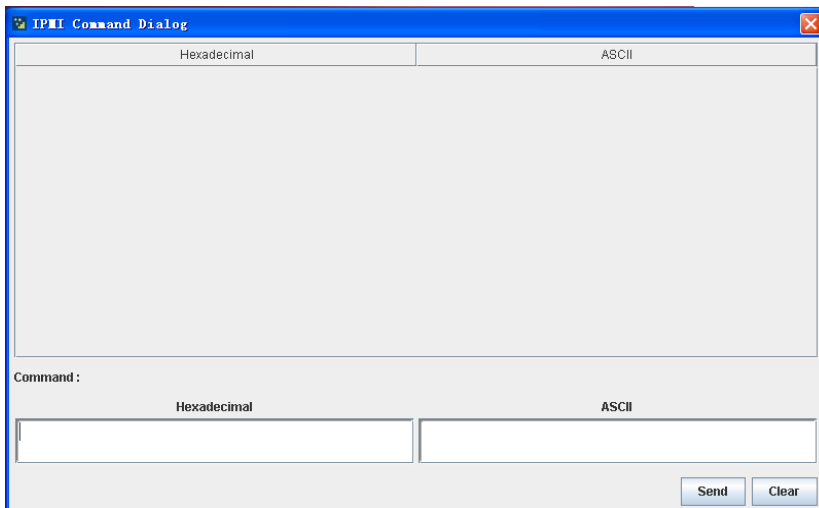
Note: When the mouse is relative, the mouse synchronization will be executed if the zoom size reaches 100%.

- **Zoom In** – For increasing the screen size. This zoom varies from 100% to 150% with an interval of 10%
- **Zoom Out** – For decreasing the screen size. This zoom varies from 100% to 50% with an interval of 10%
- **Actual Size** - By default this option is selected
- **Fit to Client Resolution** - If the host screen resolution is greater than the client screen resolution, choose this option to fit the host screen to client screen.
- **Fit to Host Resolution** - If the host screen resolution is lesser than the client screen resolution, choose this option to resize the JViewer frame to the host resolution.

Note: This option can be configured from PRJ in MDS.



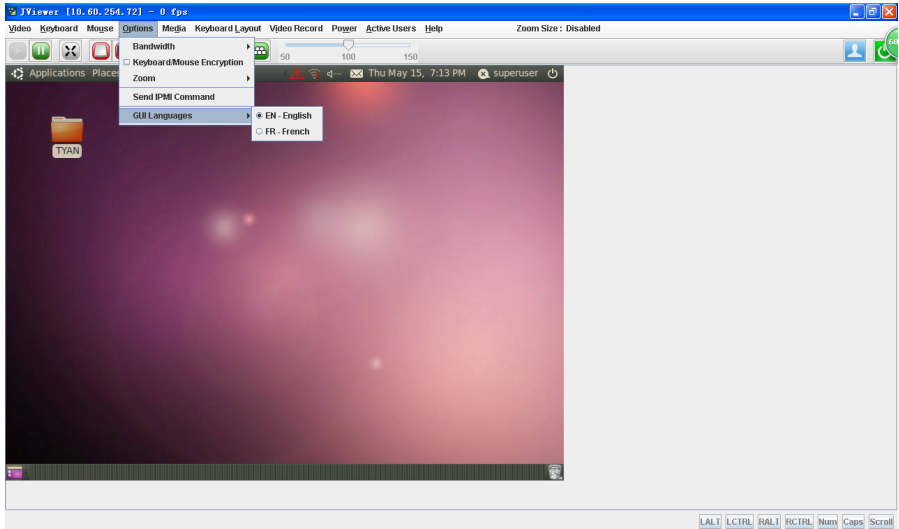
Send IPMI Command: This option opens the IPMI Command dialog. Enter the raw IPMI command in Hexadecimal field as Hexadecimal value and click **Send**. The Response will be displayed as shown in the screenshot below.



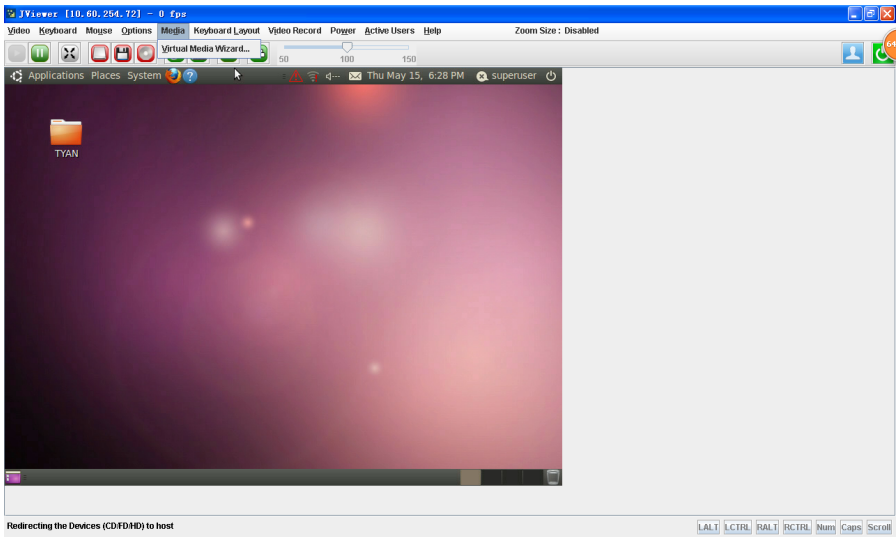
GUI Languages - Choose the desired GUI language.

Request Full Permission - Partially Permitted sessions can use this option to request the Full permission from the existing full permitted session.

Note: This menu option is available only for partially privileged session and Full permission sessions will not have this option in the menu.

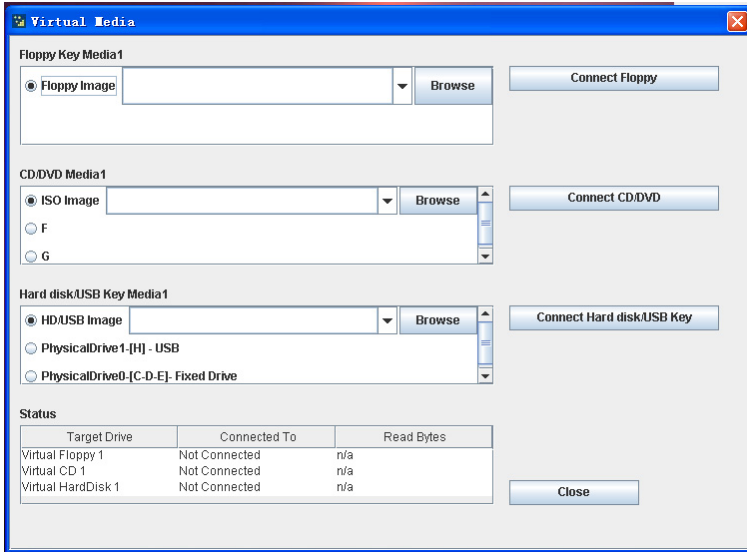


2.7.1.5 Media



Virtual Media Wizard

To add or modify a media, select and click **Virtual Media Wizard**, which pops out a box named “Virtual Media” where you can configure the media. A sample screenshot of Virtual Media Page is given below.



Floppy Key Media: This menu item can be used to start or stop the redirection of a physical floppy drive and floppy image types such as img.

Note: Floppy Redirection is not an available feature on all versions of the MegaRAC® SPs.

CD/DVD Media: This menu item can be used to start or stop the redirection of a physical DVD/ CD-ROM drive and cd image types such as iso.

Hard disc/USB Key Media: This menu item can be used to start or stop the redirection of a Hard Disk/USB key image and USB key image such as img.

Note: For windows client, if the logical drive of the physical drive is dismount then the logical device is redirected with Read/Write Permission else it is redirected with Read permission only.

For MAC client, External USB Hard disk redirection is only supported.

For Linux client, fixed hard drive is redirected only as Read Mode. It is not Write mode supported.

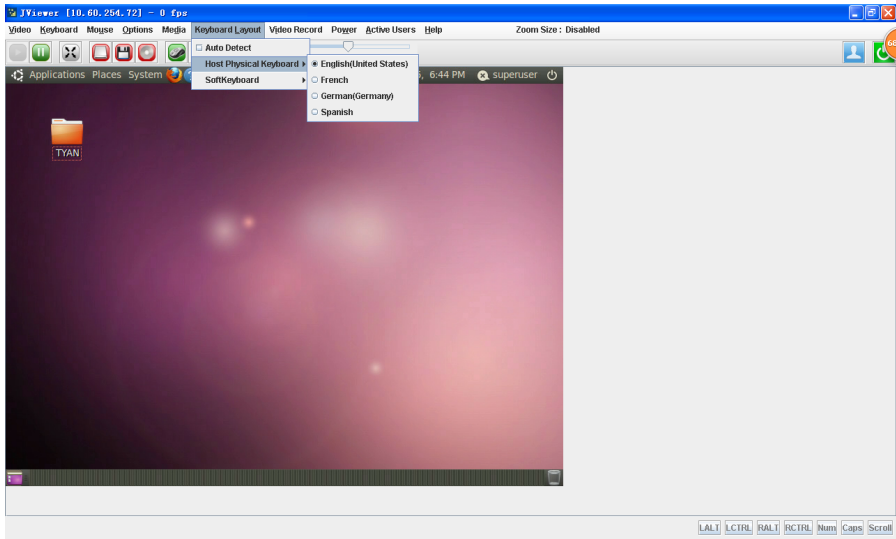
For USB key image redirection, support FAT 16, FAT 32 and NTFS.

SPX Stack Media redirection supports only Basic Hard disk Redirection.

2.7.1.6 Keyboard Layout

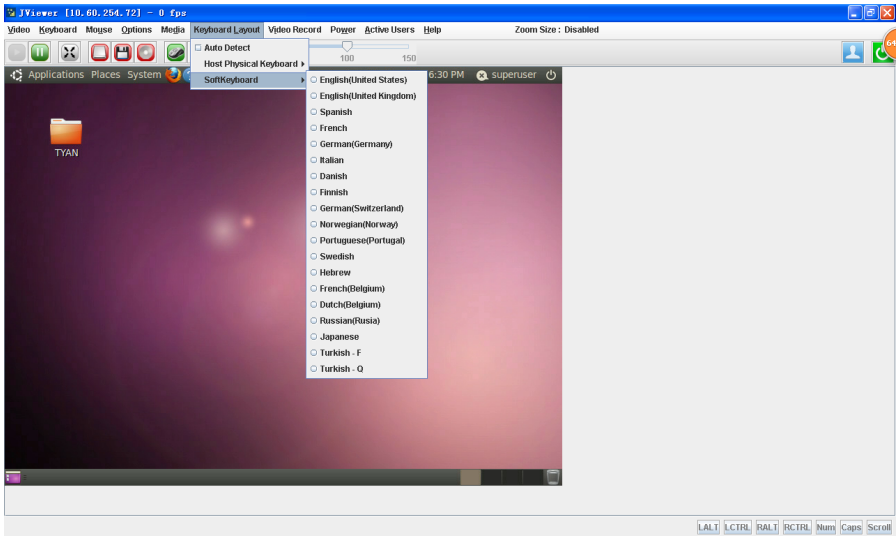
Auto Detect: This option is used to detect keyboard layout automatically. The languages supported automatically are English-US, French-France, Spanish-Spain, German-Germany, Japanese-Japan. If the client and host languages are same, then for all the languages other than English mentioned above, you must select this option to avoid typo errors.

Host Physical Keyboard: This option is to choose the host physical keyboard, languages supported English, French, German, Spanish,

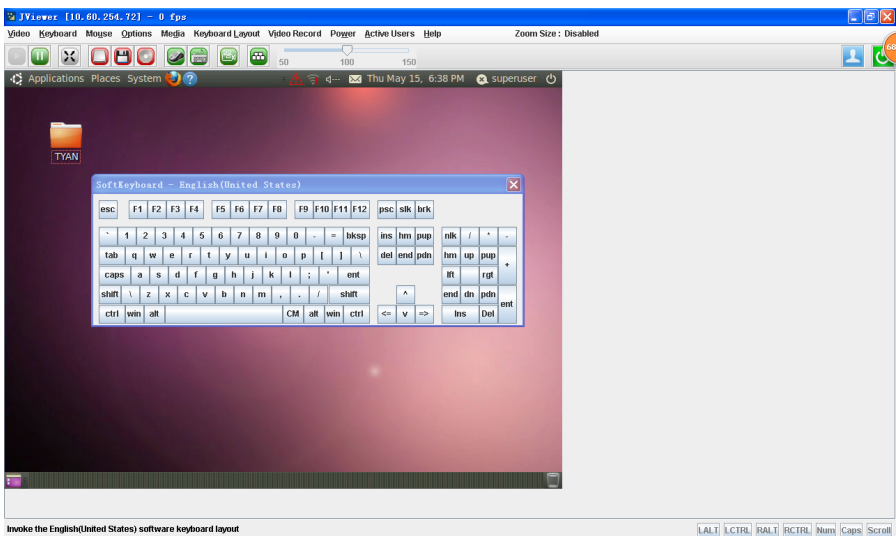


Soft Keyboard: This option allows you to select the keyboard layout. It will show the dialog as similar to onscreen keyboard. If the client and host languages are different, then for all the languages other than English mentioned above, you must select the appropriate language in the list shown in JViewer and use the softkeyboard to avoid typo errors.

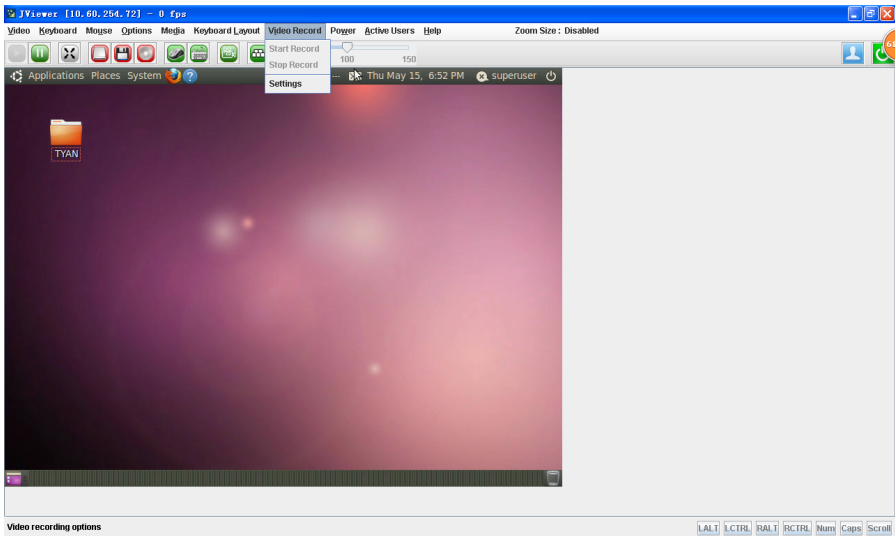
Note: Soft keyboard is applicable only for JViewer Application not for other application in the client system.



A sample screenshot of the US Keyboard is given below.



2.7.1.7 Video Record



Start Record: This option is to start recording the screen.

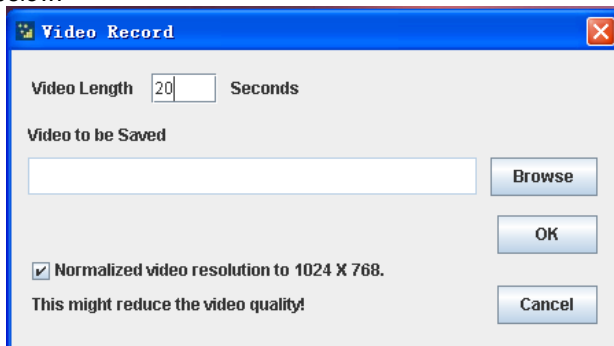
Stop Record: This option is used to stop the recording.

Settings: To set the settings for video recording.

Procedure

Note: Before you start recording, you have to enter the settings.

1. Click Video Record > Settings to open the settings page as shown in the screenshot below.



2. Enter the Video Length in seconds.
3. Browse and enter the location where you want the video to be saved.
4. Enable the option Normalized video resolution to 1024X768.
5. Click OK to save the entries and return to the Console Redirection screen.
6. Click Cancel if you don't wish to save the entries.
7. In the Console Redirection window, click Video Record > Start Record.
8. Record the process.
9. To stop the recording, click Video Record > Stop Record.

2.7.1.8 Power

The power option is to perform any power cycle operation. Click on the required option to perform the following operation.

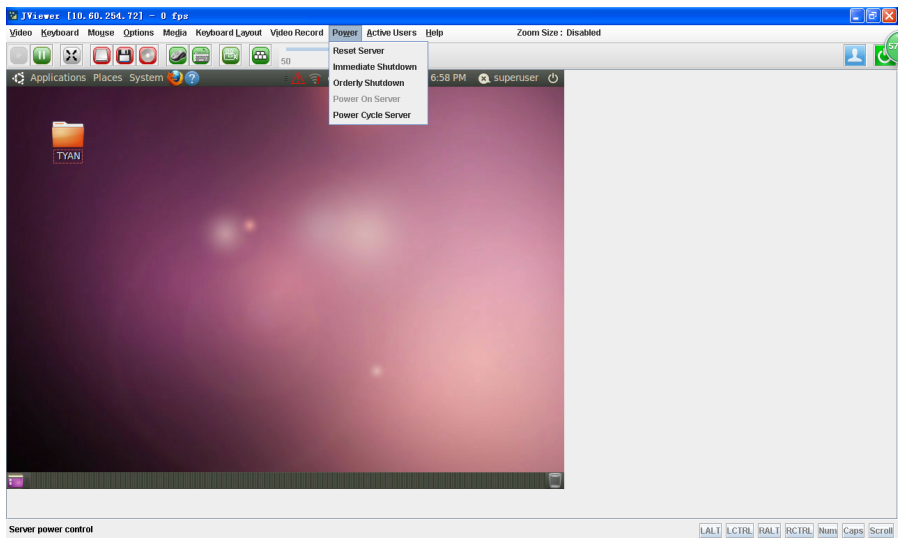
Reset Server: To reboot the system without powering off (warm boot).

Immediate Shutdown: To immediately power off the server.

Orderly Shutdown: To initiate operating system shutdown prior to the shutdown.

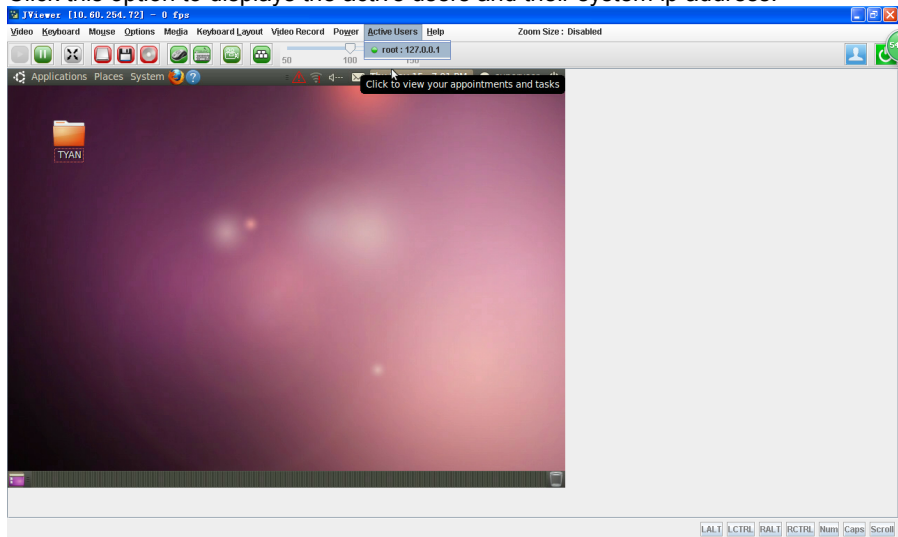
Power On Server: To power on the server.

Power Cycle Server: To first power off, and then reboot the system (cold boot).



2.7.1.9 Active Users

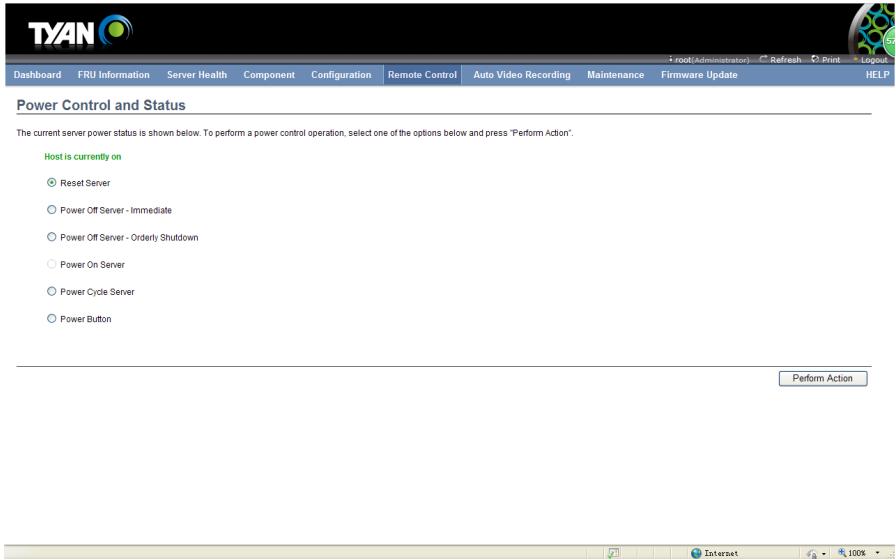
Click this option to displays the active users and their system ip address.



2.7.2 Server Power Control

This page allows you to view and control the power of your server.

To open the Power Control and Status Page, click **Remote Control** → **Server Power Control** from the main menu. A sample screenshot of Power Control and Status Page is shown in the screenshot below.



The various options of Power Control are given below.

Reset Server: This option will reboot the system without powering off (warm boot).

Power Off Server – Immediate: This option will immediately power off the server.

Power Off Server – Orderly Shutdown: This option will initiate operating system shutdown prior to the shutdown.

Power On Server: This option will power on the server.

Power Cycle Server: This option will first power off, and then reboot the system (cold boot).

Perform Action: Click this option to perform the selected operation.

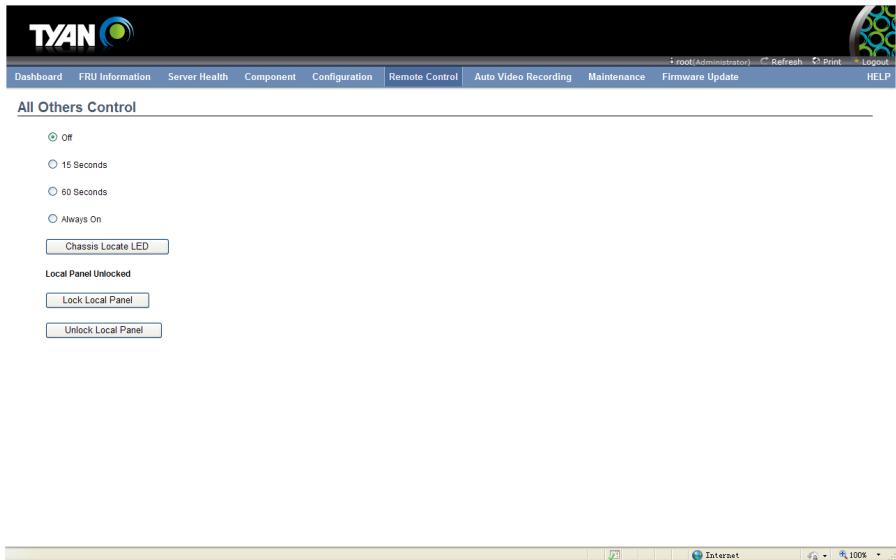
Procedure

Select an action and click Perform Action to proceed with the selected action.

Note: You will be asked to confirm your choice. Upon confirmation, the command will be executed and you will be informed of the status.

2.7.3 Other Control

Select options in the All Others Control Page to Chassis Locate LED, Clear CMOS and Local Panel Lock control.



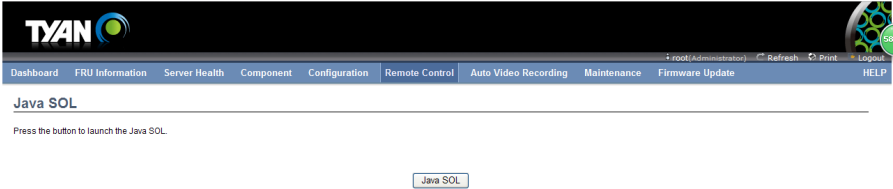
The screenshot shows a web browser window displaying the 'All Others Control' page. The browser's address bar shows 'root/Administrator' and navigation buttons for Refresh, Print, and Logout. The page header includes the TYAN logo and a navigation menu with items: Dashboard, FRU Information, Server Health, Component, Configuration, Remote Control, Auto Video Recording, Maintenance, and Firmware Update. The main content area is titled 'All Others Control' and contains the following controls:

- Radio buttons for LED settings: Off (selected), 15 Seconds, 60 Seconds, and Always On.
- A button labeled 'Chassis Locate LED'.
- A section titled 'Local Panel Unlocked' containing two buttons: 'Lock Local Panel' and 'Unlock Local Panel'.

The browser's status bar at the bottom shows 'Internet' and a zoom level of 100%.

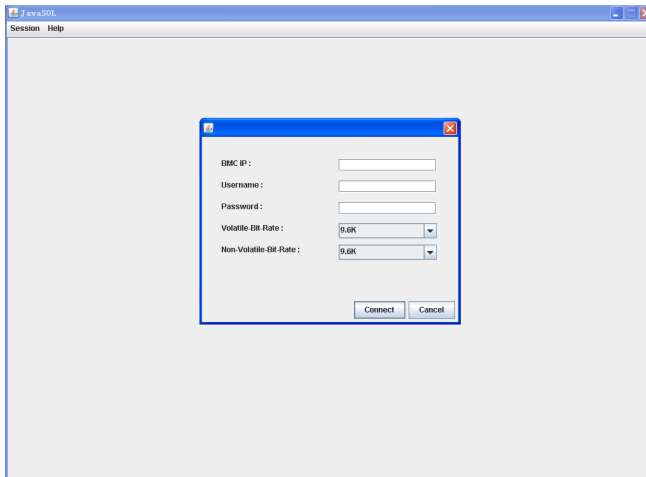
2.7.4 JAVA SOL

This page allows you to launch the Java SOL. The Java SOL is used to view the host screen using the SOL Redirection. For more details on SOL, click SOL. To open Java SOL page, click Remote Control > Java SOL from the menu bar. A sample screenshot of Java SOL page is shown below.



Procedure

1. Click the Java SOL button to open the Java SOL window.



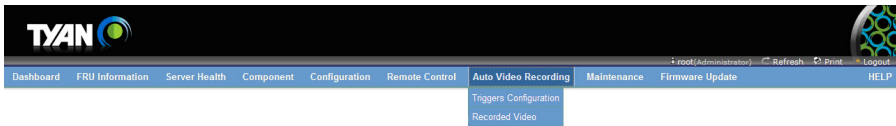
2. Enter the BMC IP address, User Name and Password in the respective fields.
3. Select the Volatile-Bit-Rate and Non-Volatile-Bit-Rate from the drop down lists.
4. Click Connect to open the SOL redirection window as shown in the screenshot below.

2.8 Auto Video Recording

The Auto Video Recording consists of the following menu items.

- Triggers Configuration
- Recorded Video

A sample screenshot of the Remote Control menu is given below.



2.8.1 Trigger Configuration

This page is used to configure the triggers for various events, which can be used by the KVM server to perform auto video recording feature.

To triggers for Auto Video Recording, click Auto Video Recording > Triggers Configuration from the menu bar. A sample screenshot of Triggers Configuration page is shown below.

Triggers Configuration

This page allows the user to configure the events that will trigger the auto video recording function of the KVM server

Temperature/Voltage Critical Events

Temperature/Voltage Non Recoverable Events

Watchdog Timer Events

Chassis Power off Event

Particular Date and Time Event

Date:

Time: (hh:mm:ss)

Temperature/Voltage Non Critical Events

Fan state changed Events

Chassis Power on Event

Chassis Reset Event

LPC Reset Event

The various fields of Triggers Configuration are as follows.

Event List: It shows the list of available events to be configured. The events are mentioned below.

- Temperature/Voltage Critical Events
- Temperature/Voltage Non Critical Events
- Temperature/Voltage Non Recoverable Events
- Fan state changed Events
- Watchdog Timer Events
- Chassis Power on Event
- Chassis Power off Event
- Chassis Reset Event
- Particular Date and Time Event

- LPC Reset Event

Save: To save any changes made.

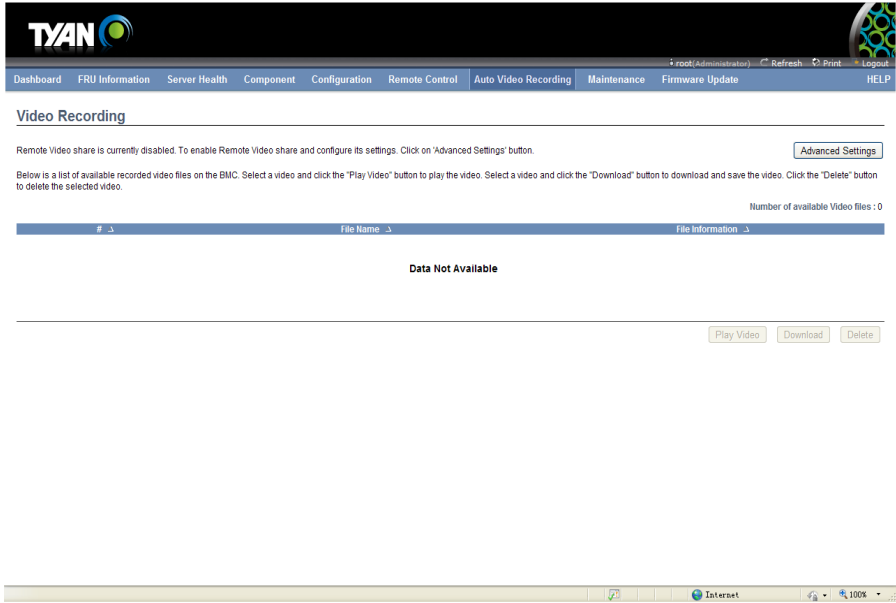
Reset: To reset the modified changes.

Procedure

1. Check the events to be enabled.
2. To set particular Date and Time Event, check the option Particular Date and Time Event.
 - Choose the month, day and year from the Date field
 - Enter the Time in hh:mm:ss format in the respective fields.
3. Click **Save** to save the changes.
4. Click **Reset** to reset the changes made

2.8.2 Video Recording

This page displays the list of available recorded video files on the BMC. Open Video Recording page, click Auto Video Recording > Recorded Video from the menu bar. A sample screenshot of Video Recording page is shown below.



The various fields of Recorded Video are given below.

- The serial number

File Name – The video filename

File Information – Day, date and time of video upload

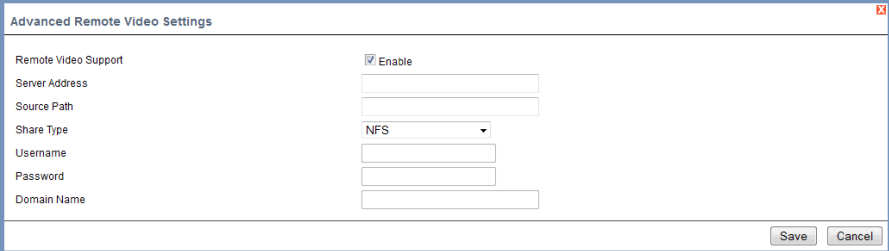
Play Video – To play the selected video

Download – To download the selected video

Delete – To delete the selected video.

Procedure

1. Click Advanced Settings.



Advanced Remote Video Settings

Remote Video Support Enable

Server Address

Source Path

Share Type

Username

Password

Domain Name

Save Cancel

a. Click Enable to enable the Remote Video Support.

Note: The Server Address, Source Path and Share Type will be enabled only if the Remote Video Support option is enabled.

b. Enter the Server Address.

c. Enter the Source Path.

d. Select the Share Type from the drop-down list.

e. Enter the User Name, Password and Domain Name in the respective fields.

f. Click Save to save the settings.

2. Select a video and click the Play Video button to play the video.

3. Select a video and click the Download button to download and save the video.

4. Click the Delete button to delete the selected video.

Note:

A maximum of only 2 Video Files can be recorded and available for access, with each recording limited to 5 minutes (300 Seconds) if Remote Video Support is enabled else 5.5MB or 20 seconds whichever is earlier.

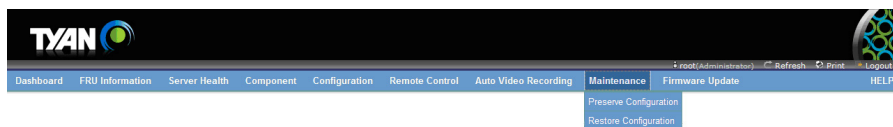
If the Recorded Video Files are stored in RAM(Remote Video Support is not enabled), then those video recordings will not be persistent upon BMC Reboot. If Remote video Support is enabled recorded video files can be accessible after BMC reboot. The Play Video and Download video buttons are active only for the KVM enabled users.

If the Recorded Video Files are stored in RAM, then those video recordings will not be persistent upon BMC Reboot.

2.9 Maintenance Group

This group of pages allows you to do maintenance tasks on the device. The menu contains of the following items:

- Preserve Configuration
- Restore Configuration



A detailed description is give below.

2.9.1 Preserve Configuration

This page allows the user to configure the preserve configuration items, which will be used by the Restore factory defaults to preserve the existing configuration without overwriting with defaults/ Firmware Upgrade configuration.

To open Preserve Configuration page,click Maintenance Group > Preserve Configuration from the menu bar. A sample screenshot of Preserve Configuration page is shown below.

Note: You can navigate to the Firmware Update Page and Restore Factory Defaults by clicking the respective links.

Number of Preserved Items: 1

#	Preserve Configuration Item	Preserve Status
1	Authentication	<input type="checkbox"/>
2	KVM	<input type="checkbox"/>
3	SNMP	<input type="checkbox"/>
4	SEL	<input type="checkbox"/>
5	FRU	<input type="checkbox"/>
6	Network	<input type="checkbox"/>
7	NTP	<input type="checkbox"/>
8	IPMI	<input type="checkbox"/>
9	SSH	<input type="checkbox"/>
10	SDR	<input type="checkbox"/>
11	biosdsg.conf	<input checked="" type="checkbox"/>

Check All Uncheck All Save Reset

The various fields of Preserve Configuration are as follows.

Preserve Status: To check/uncheck a check box to preserve/overwrite the configuration for your system.

Check All: To check the entire configuration list.

Uncheck All: To uncheck the entire configuration list.

Save: To save any changes made.

Note: This configuration is used by Restore Factory Defaults process.

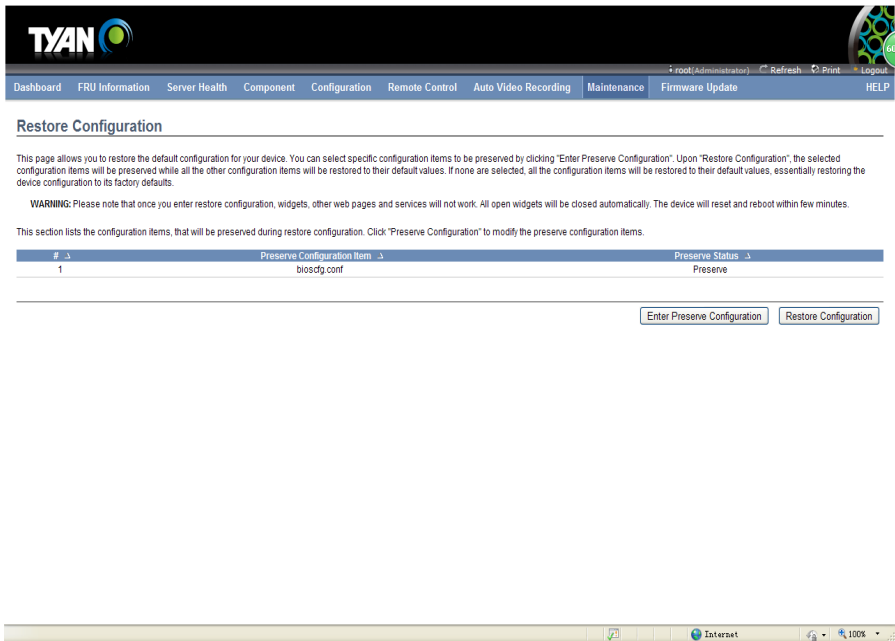
Reset: To reset the modified changes.

2.9.2 Restore Configuration

In MegaRAC GUI, this option is used to restore the factory defaults of the device firmware. This section lists the configuration items that will be preserved during restore factory default configuration.

Warning: Please note that after entering restore factory widgets, other web pages and services will not work. All open widgets will be closed automatically. The device will reset and reboot within few minutes.

To open Restore Factory Defaults page, click Maintenance > Restore Factory Defaults from the menu bar. A sample screenshot of Restore Factory Defaults Page is shown below.



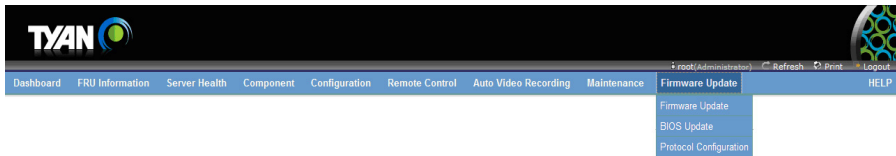
Procedure

1. Click Enter Preserve Configuration to redirect to Preserve Configuration page, which is used to preserve the particular configuration not to be overwritten by the default configuration.
2. Click Restore Configuration to restore the factory defaults of the device firmware.

2.10 Firmware Update

This group of pages allows you to do update tasks on the device. The menu contains of the following items:

- Firmware Update
- BIOS Update
- Protocol Configuration



2.10.1 Firmware Update

In MegaRAC GUI, this wizard takes you through the process of firmware upgrade. A reset of the box will automatically follow if the upgrade is completed or cancelled. An option to preserve configuration will be presented. Enable it, if you wish to preserve configured settings through the upgrade.

WARNING: Please note that after entering update mode widgets, other web pages and services will not work. All open widgets will be closed automatically, if upgrade process is cancelled in the middle of the wizard, the device will be reset.

NOTE:

The firmware upgrade process is a crucial operation. Make sure that the chances of a power or connectivity loss are minimal when performing this operation.

Once you enter into Update Mode and choose to cancel the firmware flash operation, the MegaRAC card must be reset. This means that you must close the Internet browser and log back onto the MegaRAC card before you can perform any other types of operations.

To open the Firmware Update Page, click **Maintenance** → **Firmware Update** from the main menu. A sample screenshot of Firmware Update Page is shown in the screenshot below.

Firmware Update

Upgrade firmware of the device. Press "Enter Update Mode" to put the device in update mode.

The protocol information to be used for firmware image transfer during this update is as follows. To configure, choose "Protocol Configuration" under Firmware Update menu.
Protocol Type : HTTP/HTTPS

WARNING: Please note that after entering the update mode, the widgets, other web pages and services will not work: All the open widgets will be automatically closed. If the upgradation is cancelled in the middle of the wizard, the device will be reset.

Preserve all Configuration. This will preserve all the configuration settings during the firmware update – irrespective of the individual items marked as preserve/overwrite in the table below. All configuration items below will be preserved as default during the restore configuration operation. Click "Enter Preserve Configuration" to modify the Preserve status settings.

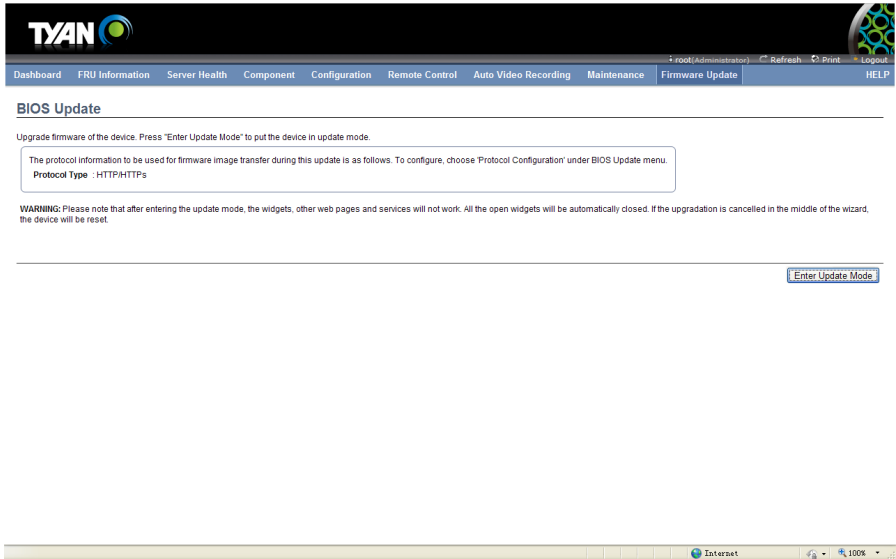
#	Preserve Configuration Item	Preserve Status
1	Authentication	Overwrite
2	KVM	Overwrite
3	SNMP	Overwrite
4	SEL	Overwrite
5	FRU	Overwrite
6	Network	Overwrite
7	NTP	Overwrite
8	IPMI	Overwrite
9	SSH	Overwrite
10	SDR	Overwrite
11	bioscdp.conf	Preserve

Enter Preserve Configuration Enter Update Mode

2.10.2 BIOS Update

This page allows you to upgrade BIOS of the device.

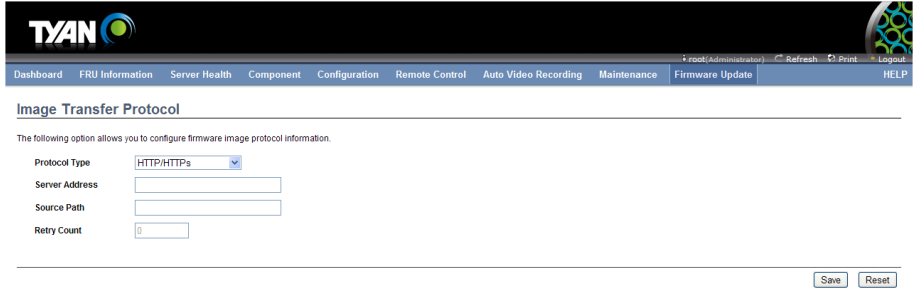
To open the BIOS Update Page, click **Maintenance** → **BIOS Update** from the main menu. A sample screenshot of BIOS Update Page is shown in the screenshot below.



2.10.3 Protocol Configuration

This page is used to configure the firmware image protocol information.

To open Image Transfer Protocol page, click Firmware Update > Protocol Configuration from the menu bar. A sample screenshot of Image Transfer Protocol page is shown below.



The various options of Image Transfer Protocol are given below.

Protocol Type: To transfer the firmware image into the BMC.

Server Address: Server IP address of the firmware image is stored.

Note:

- IP Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx".
- Each number ranges from 0 to 255.
- First number must not be 0.

Source Path: Full Source path with filename of the firmware image is stored.

Retry Count: Number of time(s) to be retried when transfer failure occurs. Retry count ranges from 0 to 255.

Save: To save the configured settings.

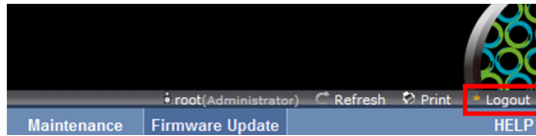
Reset: To reset the modified changes.

Procedure

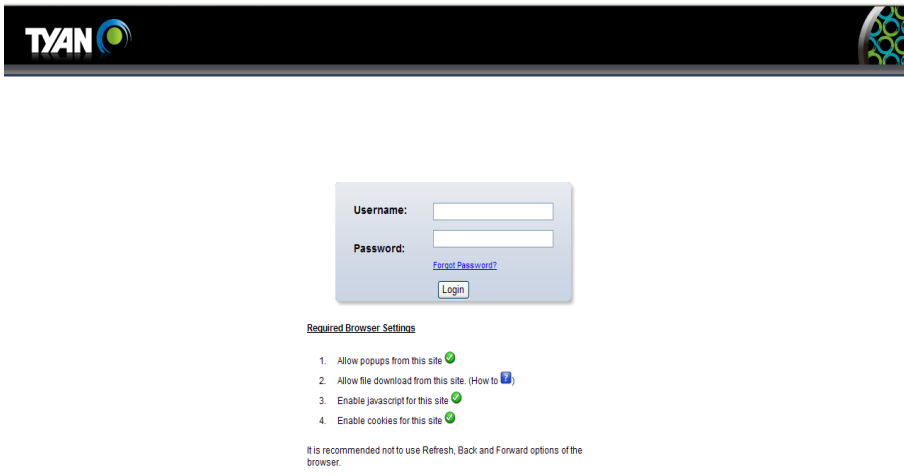
1. Select the Protocol Type from the drop-down list.
2. If the protocol selected is TFTP, enter the IP address of the server in the Server Address field.
3. Enter the Source Path in the given field.
4. Enter the Retry Count value.
5. Click Save to save the changes.
6. Click Reset to reset the entered values.

2.11 Log Out

To log out of the MegaRAC GUI, click the logout link on the top right corner of the screen.



The Log in screen will pop out.



3. BMC Port Number

This section will list a table of the BMC Port numbers.

BMC Port Number	Web Server: 80, 443
	KVM: 7578, 7582
	CD Media: 5120, 5124
	FD Media: 5123, 5127
	HD Media: 5122, 5126
	IPMI: 623
	UPnP Discovery: 1900, 50000

Document NO. D2283 - 100