



IPMI Configuration Guide

Published April 2019

Copyright©2019 ASRock Rack INC. All rights reserved.

AST2400 V1.02

1. Introduction of Megarac SP	4
2. Megarac SP GUI Overview	5
2.1 Login page	5
2.2 Dashboard	6
2.3 Field Replaceable Unit (FRU)	8
2.4 Server Health	10
2.4.1 Sensor Readings	10
2.4.2 Event Log	12
2.4.3 System and Audit Log	14
2.4.4 BSOD Screen	15
2.5 Configuration	16
2.5.1 Active Directory Settings	16
2.5.2 DNS Server Settings	17
2.5.3 System Event Log	20
2.5.4 Images Redirection	21
2.5.5 LDAP/E-Directory Settings	22
2.5.6 Mouse Mode Settings	23
2.5.7 Network Settings	24
2.5.8 Network Bonding Configuration (Optional)	27
2.5.9 Network Link Configuration (Optional)	29
2.5.10 NTP Settings	30
2.5.11 PAM Ordering	32
2.5.12 PEF Management	33
2.5.13 RADIUS Settings	35
2.5.14 Configure Remote Session	37
2.5.15 Services	39
2.5.16 SMTP Settings	40
2.5.17 SSL Certificate Configuration	43
2.5.18 System and Audit Log Settings	44
2.5.19 System Firewall	46
2.5.20 User Management	48
2.5.21 Virtual Media Devices	49
2.5.22 Keep NCSI Link Up	50
2.6 Remote Control	51
2.6.1 Console Redirection	51

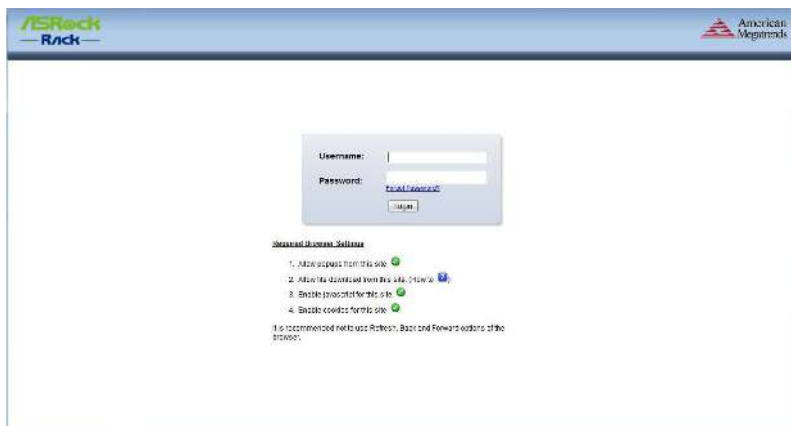
2.6.2 Power Control and Status.....	52
2.6.3 Java SOL	53
2.7 Auto Video Recording.....	54
2.7.1 Triggers Configuration	54
2.7.2 Video Recording	55
2.8 Maintenance	56
2.8.1 Preserve Configuration	56
2.8.2 Restore Factory Defaults	57
2.8.3 System Administrator	58
2.9 Firmware Update	59
2.9.1 Firmware Update	59
2.9.2 BIOS Update.....	60
2.9.3 Image Transfer Protocol	61

1. Introduction of Megarac SP

Megarac SP allows remote access of computers with BMC (Baseboard Management Controllers) and IPMI (Intelligence Platform Management Interface). System administrators may easily monitor system health or manage computer events of remote computers via the web based Megarac SP GUI using standard Internet browsers.

2. Megarac SP GUI Overview

2.1 Login page

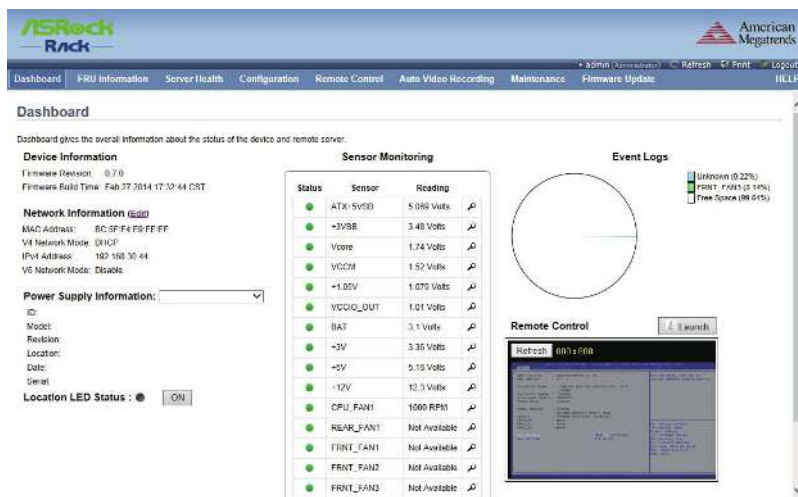


The default username and password are both “admin”. It is recommended to change the username and password after your first login.

Forgot password

If you forget the password, click on “Forgot password?”, and the system will send you a newly generated password.

2.2 Dashboard



The dashboard displays overall information about the status of the device.

Device Information

Displays the Firmware Revision and Firmware Build Time (Date and Time).

Network Information

Shows network settings for the device. Click on the link Edit to view the Network Settings Page.

Remote Control

Start remote redirection of the host by launching the console from this page. Clicking on the 'Launch' button of the 'Remote Control' will cause the `jviewer.jnlp` file to be downloaded. Once the file is downloaded and launched, a Java redirection window will be displayed.

Remote Console Preview Box

It will show the console preview of the remote server by using a java application. Click on the 'Refresh' button to reload the console preview.

Power Supply Information

Choose from the drop-down list to display the selected Power Supply Information.

Location LED Status

Display the current status of the Location LED. Click the ON/OFF button to control the Location LED.

Sensor Monitoring

It lists all available sensors on the device, with information such as status, name, reading, and status icon, as well as a link to that sensor's page.

There are 3 possible states for a Sensor:

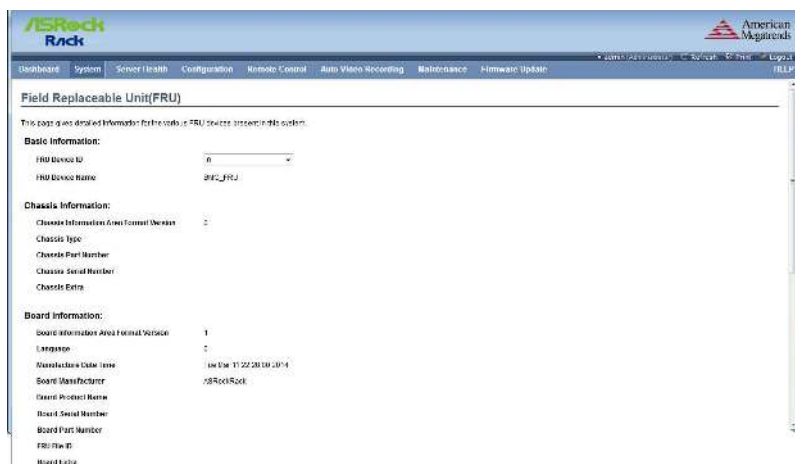
- Green dot denotes a Normal state.
- Yellow exclamation mark denotes a Warning state.
- Red x denotes a Critical state.

The magnifying glass allows access to the Sensor details page for that sensor.

Event Logs

A graphical representation of all events incurred by the various sensors and occupied/available space in logs. If you click on the color-coded rectangle in the Legend for the chart, you can view a list of those specific events only.

2.3 Field Replaceable Unit (FRU)



This page displays the BMC FRU file information. On selecting a particular FRU Device ID its corresponding FRU information will be displayed.

Basic Information

It displays the FRU device ID and device name for the selected FRU device ID.

Chassis Information

It displays the following Chassis information fields.

- Area Format Version
- Chassis Type
- Chassis Part Number
- Chassis Serial Number
- Chassis Extra

Board Information

It displays the following Board information fields.

- Area Format Version
- Language
- Manufacture Date Time
- Board Manufacturer

-
- Board Product Name
 - Board Serial Number
 - Board Part Number
 - FRU File ID
 - Board Extra

Product Information

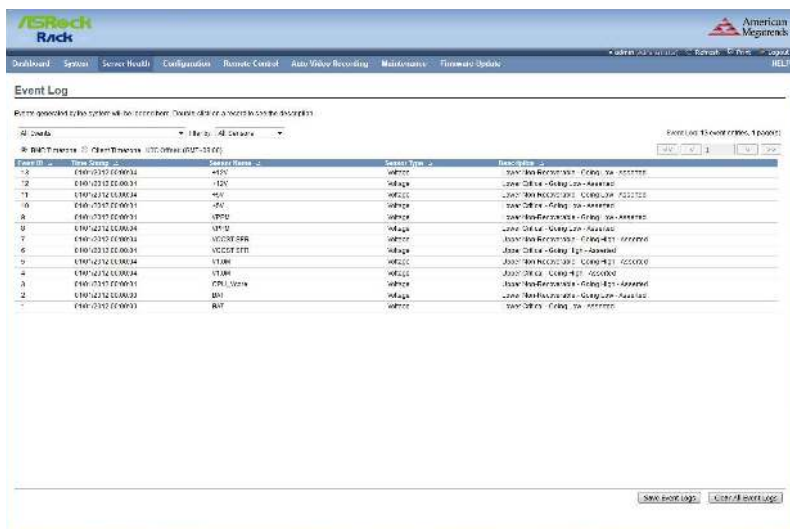
It displays the following Product information fields.

- Area Format Version
- Language
- Manufacturer Name
- Product Name
- Product Part Number
- Product Version
- Product Serial Number
- Asset Tag
- FRU File ID
- Product Extra

View this Event Log

Click this button to go the event log page for the viewed sensor.

2.4.2 Event Log



Event ID	Time	Sensor Name	Sensor Type	Description
10	040-0302-000000	TEMP	TEMP	TEMP Sensor - Gang 1 - Normal
9	040-0302-000000	TEMP	TEMP	TEMP Sensor - Gang 2 - Normal
8	040-0302-000000	TEMP	TEMP	TEMP Sensor - Gang 3 - Normal
7	040-0302-000000	TEMP	TEMP	TEMP Sensor - Gang 4 - Normal
6	040-0302-000000	TEMP	TEMP	TEMP Sensor - Gang 5 - Normal
5	040-0302-000000	TEMP	TEMP	TEMP Sensor - Gang 6 - Normal
4	040-0302-000000	TEMP	TEMP	TEMP Sensor - Gang 7 - Normal
3	040-0302-000000	TEMP	TEMP	TEMP Sensor - Gang 8 - Normal
2	040-0302-000000	TEMP	TEMP	TEMP Sensor - Gang 9 - Normal
1	040-0302-000000	TEMP	TEMP	TEMP Sensor - Gang 10 - Normal

This page displays the list of events incurred by different sensors on this device. Double click on a record to see the details of that entry. You can also sort the list of entries by clicking on any of the column headers. You can use the sensor type or sensor name filter options to view those specific events logged in the device.

BMC Timezone

Check this option to display the event log entries logged with the BMC Timezone value.

Client Timezone

Check this option to display the event log entries logged with the Client (user's) Timezone value.

UTC Offset

Displays the current UTC Offset value based on which event Time Stamps will be updated. Navigational arrows can be used to selectively access different pages of the Event Log.

Event log Category

The group of Sensor type, you can filter event log by sensor type.

All Events, System Event Records, OEM Event Records, BIOS Generated Events, SMI Handler Events, System Management Software Events, System Software - OEM Events, Remote Console software Events, Terminal Mode Remote Console software Events, follow the table below for more information.

Filter By

The group of Sensor name, you can filter event log by sensor name.

Event ID

Displays the ID number of event.

Time Stamp

Displays the timestamp of event.

Sensor Type

Displays the sensor type of event.

Description

Displays more information include which sensor name that generated the event.

Save Event Logs

Clicking this button will pop-up a Save dialog to save all existing records.

Clear All Event Logs

Clear All Event Logs option will delete all existing records for all sensors.

2.4.3 System and Audit Log

System & Audit Logs

This page displays logs of system and audit events for this device (if the options have been configured).

System Log Audit Log UTC Offset: (GMT+0)

Filter by: This Filter: 2 event entries

Event ID	Time Stamp	Host Name	Description
1	Mar 2 03:18:48	AMUC2H14L911L1	Internal Helper Module Driver Version 1.2
2	Mar 2 03:18:48	AMUC2H14L911L1	Internal Copyright (c) 2006 American Megatrends Inc.

If configured, these logs will display all the system and audit events that occurred on this device.

NOTE: Logs have to be configured under 'Configuration -> System Log' in order to display entries.

System Log

Click the System Log tab to view all system events. Entries can be filtered based on their classification levels.

Audit Log

Click the Audit Log tab to view all audit events for this device.

Blue Screen of Death

A problem has been detected and Windows has been shut down to prevent damage to your computer.

If you're having trouble, you can try the following steps to troubleshoot the problem:

- Restart the computer.
- Check for new hardware or software that you've recently installed.
- Check for updates to your operating system and drivers.
- Check for viruses and malware.
- Check for disk space and defragment the hard drive.
- Check for overheating and clean the dust from the fans.
- Check for hardware failure, such as a failing hard drive or RAM.
- Check for software conflicts, such as conflicting antivirus programs.
- Check for system updates and install them.

If the problem continues, you may need to contact technical support or a professional technician.

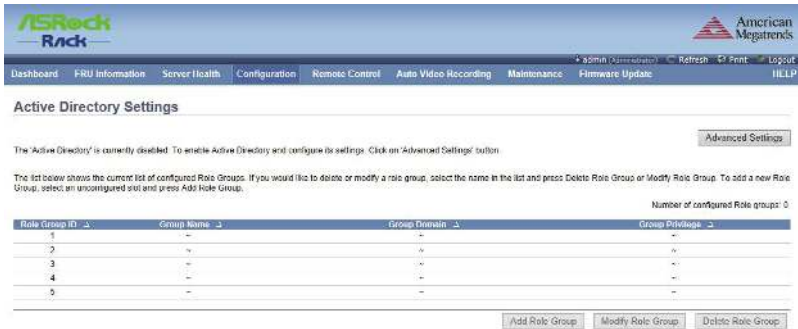
Technical information:
 STOP: 0x00000000, 0x00000000, 0x00000000, 0x00000000

Collecting data for crash dump ...
 Calculating disk for crash dump ...

15

2.5 Configuration

2.5.1 Active Directory Settings



The screenshot shows the 'Active Directory Settings' page in the ASRock Rack BIOS. At the top, there's a navigation bar with links like Dashboard, FRU Information, Server Health, Configuration, Remote Control, Auto Video Recording, Maintenance, Firmware Update, and a user profile section for 'admin (Administrator)' with options for Refresh, Exit, and Logout. The main heading is 'Active Directory Settings'. Below it, a message states: 'The Active Directory is currently disabled. To enable Active Directory and configure its settings, click on 'Advanced Settings' button.' To the right is an 'Advanced Settings' button. Below the message, a text block explains: '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 press Delete Role Group or Modify Role Group. To add a new Role Group, select an unconfigured slot and press Add Role Group.' To the right of this text is 'Number of configured Role groups: 0'. The main part of the page is a table with four columns: 'Role Group ID', 'Group Name', 'Group Domain', and 'Group Sid/Name'. The table has five rows. The first row is filled with '1', '1', '1', and '1'. The second row is filled with '2', '~', '~', and '~'. The third row is filled with '3', '~', '~', and '~'. The fourth row is filled with '4', '~', '~', and '~'. The fifth row is filled with '5', '~', '~', and '~'. Below the table are three buttons: 'Add Role Group', 'Modify Role Group', and 'Delete Role Group'.

Role Group ID	Group Name	Group Domain	Group Sid/Name
1	1	1	1
2	~	~	~
3	~	~	~
4	~	~	~
5	~	~	~

The displayed table shows current configured Role Groups and the available slots. You can modify, add or delete role groups from here. Group domain can be the AD domain or a trusted domain. Group Name should correspond to the name of an actual AD group. To view the page, you must be at least a User. To modify or add a group, you must be an Administrator.

NOTE: Free slots are denoted by “~” in all columns for the slot.

Advanced Settings

Click this option to configure the Active Directory Settings. Options are Enable Active Directory Authentication, User Domain name, Time Out and up to three Domain Controller Server Addresses.

Add Role Group

Select a free slot and click ‘Add Role Group’ to add a new role group to the device. Alternatively, double click on a free slot to add a role group.

Modify Role Group

Select a configured slot and click ‘Modify Role Group’ to modify that role group. Alternatively, double click on the configured slot.

Delete Role Group

Select the desired role group to be deleted and click ‘Delete Role Group’.

2.5.2 DNS Server Settings

DNS Server Settings

Enable DNS settings on this device

DNS Service

☒ Enable

mDNS Settings

☐ Enable

Host Configuration

Host Settings

Automatic

Host Name

AMROCTE0101010

Register DNS

☒ Enable

☒ Dynamic ☐ Static ☐ DHCP Client ☐ None

TFTP Configuration

TFTP Authentication

☐ Enable

TFTP Username

101010101010

Domain Name Configuration

Domain Name

LOCAL_101

Domain Name Server Configuration

DNS Server Settings

LOCAL

DNS Server

1

mDNS Settings

2

This page is used to configure the Host name and Domain Name Server configuration of the device.

Domain Name Service Configuration

DNS Service

Check this box to enable all the DNS Service configurations.

Multicast DNS

mDNS Settings

Check this box to enable/disable the mDNS Support Configurations.

Host configuration

Host Settings

Choose either Automatic or Manual settings.

Host Name

It displays the hostname of the device if Auto is selected. If the Host setting is chosen as Manual, then specify the hostname of the device.

Register BMC

Choose the BMC's network port to register with the DNS settings. Check the option 'Register BMC' to register with the DNS settings. Choose the option 'Direct Dynamic DNS' to register with direct dynamic DNS or choose 'DHCP Client FQDN' to register through a DHCP server.

TSIG Configuration

TSIG Authentication

Check this option to enable TSIG authentication while registering DNS via Nsupdate.

Current TSIG Private File

The information as Current TSIG private and uploaded date/time will be displayed (readonly).

New TSIG Private File

Browse and navigate to the TSIG private file.

- TSIG file should be of private type

Domain Name Configuration

Domain Settings

It lists the options for the domain interface as Manual, v4 or v6 for multi LAN channels.

Domain Name

It displays the domain name of the device if Auto is selected. If the Domain setting is chosen as Manual, then specify the domain name of the device.

Domain Name Server Configuration

DNS Server Settings

It lists the options for the DNS interface, Manual and available LAN interfaces.

IP Priority

If the IP Priority is IPv4, it will have 2 IPv4 DNS servers and 1 IPv6 DNS server. If the IP Priority is IPv6, it will have 2 IPv6 DNS servers and 1 IPv4 DNS server.

NOTE: This is not applicable for Manual configuration.

DNS Server 1, 2 & 3

Specify the DNS (Domain Name System) server address to be configured for the BMC.

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

DNS Server Address will support the following:

- IPv4 Address format.
- IPv6 Address format.

Save

Click 'Save' to save any changes made. You will be logged out of current UI session and will need to log back in.

Reset

Reset the modified changes.

2.5.3 System Event Log



This page is used to configure the System Event log information.

Current Event Log Policy

It will display the configured Event Log Policy.

Linear Event Log Policy

Check this option to enable the Linear System Event Log Policy for the Event Log.

Circular Event Log Policy

Check this option to enable the Circular System Event Log Policy for the Event Log.

Save

Click 'Save' to save the configured settings.

Reset

Click 'Reset' to reset the modified changes.

2.5.4 Images Redirection

Images Redirection

Remote Media is used to mount the images from remote system and perform redirection. Remote Media is currently disabled. To configure Remote Media Settings, click on 'Advanced Settings' button.

Number of available Images: 0

Slot	Image Type	Image Name	Redirection Status
1	Flash	~	~
2	CD/DVD	~	~
3	Harddisk	~	~

Start Redirection Add Image Replace Image Delete Image

The displayed table shows configured images on BMC. You can add or replace the images from here to the remote media. 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.

NOTE: Free slots are denoted by "~".

Start/Stop Redirection

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 the 'Stop Redirection' button to stop the remote media redirection.

Add 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.

Replace Image

Select a configured slot and click 'Replace Image' to replace the existing image. Alternatively, double click on the configured slot.

Delete Image

Select the desired image to be deleted and click 'Delete Image'.

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

2.5.5 LDAP/E-Directory Settings

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 press Delete Role Group or Modify Role Group. To add a new Role Group, select an unconfigured slot and press Add Role Group.

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

Number of configured Role groups: 0

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

The displayed table shows the configured Role Groups and available slots. You can modify or add/delete role groups from here. The Group Search Base can be any path from where a Group is located to the Base DN. The Group Name should correspond to the name of an actual LDAP/E-Directory group. To view the page, the user must at least be a User. To modify or add a group, the user must be an Administrator.

NOTE: Free slots are denoted by “~” in all columns for the slot.

Advanced Settings

Click this option to configure LDAP/E-Directory Advanced Settings. Options are Enable LDAP/E-Directory Authentication, IP Address, Port, Bind DN, Password and Search base.

Add Role Group

Select a free slot and click 'Add Role Group' to add a new role group to the device. Alternatively, double click on a free slot to add a role group.

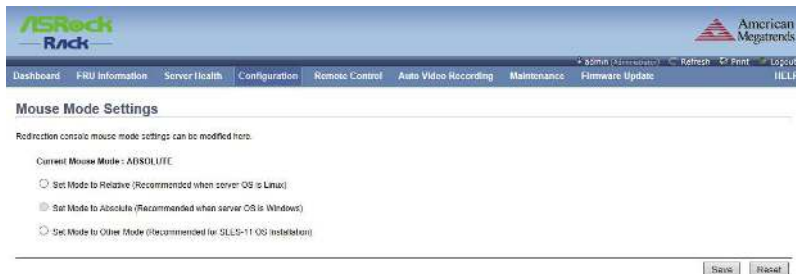
Modify Role Group

Select a configured slot and click 'Modify Role Group' to modify that role group. Alternatively, double click on the configured slot.

Delete Role Group

Select the desired role group to be deleted and click 'Delete Role Group'.

2.5.6 Mouse Mode Settings



The Redirection Console handles mouse emulation from the local window to the remote screen using either of the two methods. Only 'Administrator' has the right to configure these options.

- Relative Mouse mode
- Absolute Mouse mode
- Other Mouse mode

Relative Mouse mode

The Relative mode sends the calculated relative mouse position displacement to the server. To select this mode select the "Set mode to Relative" option.

Absolute Mouse mode

The absolute position of the local mouse is sent to the server. To select this mode select the "Set mode to Absolute" option.

Other Mouse mode

Select Other Mode to have the calculated displacement from the local mouse in the centre position, sent to the server. Use this mode for SLES 11 Linux OS installation.

Save

Click 'Save' to save any changes made.

Reset

Click 'Reset' to reset the modified changes.

2.5.7 Network Settings

Network Settings

Ext. LAN/USB LAN (2 x RJ45/USB)

LAN Interface:

LAN Settings: ☒ Enabled

MAC Address:

IPv4 Configuration:

Obtain an IP address automatically: ☒ Yes / ☐ No

IPv4 Address:

Subnet Mask:

Default Gateway:

IPv6 Configuration:

IPv6 Settings: ☒ Enabled

Obtain an IP address automatically: ☒ Yes / ☐ No

IPv6 Address:

Subnet Prefix length:

Default gateway:

VLAN Configuration:

VLAN Settings: ☒ Enabled

VLAN ID:

VLAN Priority:

This page is used to configure the network settings for available LAN channels.

LAN Interface

Select the LAN interface to be configured.

LAN Settings

Check this option to enable LAN support for the selected interface.

MAC Address

This field displays the MAC address of the selected interface (read only).

IPv4 Configuration

It lists the IPv4 configuration settings.

Obtain an IP address automatically

Enable 'Use DHCP' to dynamically configure the IPv4 address using Dynamic Host Configuration Protocol (DHCP).

IPv4 Address, Subnet Mask, Default Gateway

If DHCP is disabled, specify a static IPv4 address, Subnet Mask and

Default Gateway to be configured for the selected interface.

- An IP Address consists of 4 sets of numbers separated by dots as in "xxx.xxx.xxx.xxx".
- Each set ranges from 0 to 255.
- The first Number must not be 0.

IPv6 Configuration

It lists the IPv6 configuration settings.

IPv6 Settings

Check this option to enable IPv6 support for the selected interface.

Obtain an IP address automatically

Enable 'Use DHCP' to dynamically configure the IPv6 address using Dynamic Host Configuration Protocol (DHCP).

IPv6 Address

Specify a static IPv6 address to be configured for the selected interface.

Subnet Prefix length

Specify the subnet prefix length for the IPv6 settings.

- Value ranges from 0 to 128.

Default Gateway

Specify the v6 default gateway for IPv6 settings.

VLAN Configuration

It lists the VLAN configuration settings.

VLAN Settings

Check this option to enable VLAN support for the selected interface.

VLAN ID

Specify the Identification for VLAN configurations.

- Value ranges from 2 to 4094.

NOTE: VLAN ID cannot be changed without resetting the VLAN configuration. VLAN ID 0, 1, 4095 are reserved VLAN ID's.

VLAN Priority

Specify the priority for VLAN configurations.

- Value ranges from 1 to 7.

NOTE: 7 is the highest priority for VLAN.

Save

Click 'Save' to save any changes made. You will be prompted to log out of the current UI session and log back in at the new IP address.

Reset

Click 'Reset' to reset the modified changes.

2.5.8 Network Bonding Configuration (Optional)

Note: This page may not appear or some of the items cannot be changed if the platform doesn't support this function.

The screenshot shows a web interface for 'Network Bonding Configuration'. At the top, there's a navigation bar with links: Dashboard, System, Server Health, Configuration (selected), Remote Control, Auto Video Recording, Maintenance, and Firmware Update. The main title is 'Network Bonding Configuration'. Below it, a message states: 'The following options are for configuring the networking bonding for the device.' The configuration options are: 'Network Bonding' with a checked 'Enable' checkbox; 'Bonding Mode' with a dropdown menu set to 'active-backup'; 'Default Interfaces' with a dropdown menu set to 'Dedicate'; and 'Auto Configuration' with an unchecked 'Enable' checkbox. At the bottom right, there are 'Save' and 'Reset' buttons.

This page is used to configure the network bonding configuration for network interfaces.

NOTE: A minimum of 2 network interfaces are required to enable Network bonding for the device.

Network Bonding

Check this option to enable network bonding for network interfaces.

NOTE: If VLAN is enabled for slave interfaces, then Bonding cannot be enabled. VLAN can be disabled under Configuration -> Network -> VLAN.

Default Interfaces

Choose any one of the bonding interfaces for configuring active slave(s).

Auto Configuration

Enable this option to configure the interfaces in service configuration automatically.

NOTE: If Auto configuration is disabled, then interfaces in services can be configured via IPMI command. If Auto configuration is enabled, then all the services will be restarted automatically.

Save

Click "Save" to save the current changes.

NOTE: Disabling bonding will disable the Bonding-VLAN configuration.

Reset

Click “Reset” to reset the modified changes.

2.5.9 Network Link Configuration (Optional)

This page may not appear or some of the items cannot be changed if the platform doesn't support this function.



This page is used to configure the network link configuration for available network interfaces.

LAN Interface

Select the required network interface from the list to which the Link speed and duplex mode is 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

Select any one of the following Duplex Modes.

- Half Duplex
- Full Duplex

Save

Click 'Save' to save the settings.

Reset

Click 'Reset' to reset the modified changes.

2.5.10 NTP Settings

ASRock Rack American Megatrends

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

NTP Settings

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

Date: March 3 2016

Time: 11 52 AM

UTC Timezone: GMT+0 Hour(s)

NTP Server: pool.ntp.org

☒ Automatically synchronize Date & Time with NTP Server

Refresh Save Reset

This page displays the device's current Date & Time Settings. It can be used to configure either Date & Time or NTP (Network Time Protocol) server settings for the device.

Date

Specify the current Date for the device.

Time

Specify the current Time for the device.

NOTE: As a year 2038 problem exists, the acceptable date range is from 01-01-2005 to 01-18-2038.

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.

NTP Server

Specify the NTP Server for the device. Check the 'Automatically synchronize' option to configure the NTP Server. The NTP Server will support the following:

- IP Address (Both IPv4 and IPv6 format).
- FQDN (Fully qualified domain name) format.

Primary NTP Server & Secondary NTP Server

Specify the NTP Servers for the device. 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.

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

UTC Offset

UTC Offset list contains the UTC offset values for the NTP server, which can be used to display the exact local time.

NOTE: Use the correct UTC offset after adjusting for DST.

Automatically synchronize

Check this option to automatically synchronize Date and Time with the NTP Server.

Refresh

Click 'Refresh' to reload the current date & time settings.

Save

Click 'Save' to save any changes made.

Reset

Click 'Reset' to reset the modified changes.

2.5.11 PAM Ordering



This page is used to configure the PAM order for user authentication into the BMC.

PAM Module

It shows the list of available PAM modules supported in BMC.

Move Up

Click on the required PAM module, it will be selected. Click on the 'Move Up' option to move the selected PAM module one step before the existing PAM module.

Move Down

Click on the required PAM module, it will be selected. Click on the 'Move Down' option to move the selected PAM module one step after the existing PAM module.

Save

Click 'Save' to save any changes made.

NOTE: Whenever the configuration is modified, the web server will be restarted automatically. The logged session will be logged out.

Reset

Click 'Reset' to reset the modified changes.

2.5.12 PEF Management

ASRock Rack American Megatrends

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

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 press "Delete" or "Modify". To add a new entry, select an unconfigured slot and press "Add".

Event Filter Alert Policy LAN Destination

Configured Event Filter count: 13

PEF ID	Filter Configuration	Event Filter Action	Event Severity	Sensor Name
1	~	~	~	~
2	~	~	~	~
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	~	~	~	~

Add Modify Delete

This page is used to configure the Event Filter, Alert Policy and LAN Destination. To view the page, the user must at least be an Operator. To modify or add a PEF, the user must be an Administrator.

NOTE: Free slots are denoted by '~' in all columns for the slot. For more information, refer the Platform Event Filtering (PEF) section in IPMI Specification.

Event Filter

Click the Event Filter tab to show configured Event filters and available slots. You can modify or add new event filter entries here. A maximum of 40 slots are available and include the default of 15 event filter configurations.

Alert Policy

Click the Alert policy tab to show configured Alert policies and available slots. You can modify or add new alert policy entries here. A maximum of 60 slots are available.

LAN Destination

Click the LAN Destination tab to show configured LAN destinations and available slots. You can modify or add new LAN destination entries here. A maximum of 15 slots are available.

Send Test Alert

Select a configured slot in the LAN Destination tab and click 'Send Test Alert' to send a sample alert to the configured destination.

NOTE: Test alerts can be sent only with SMTP configurations set to enabled. SMTP support can be enabled under Configuration->SMTP.

Add

Select a free slot and click 'Add' to add a new entry to the device. Alternatively, double click on a free slot.

Modify

Select a configured slot and click 'Modify' to modify that entry. Alternatively, double click on the configured slot.

Delete

Select the desired configured slot to be deleted and click 'Delete'.

2.5.13 RADIUS Settings

RADIUS Settings

The RADIUS Authentication is currently disabled. To enable RADIUS Authentication and enter the required information to access the RADIUS server, Press the Save button to save your changes. To configure the Advanced settings, RADIUS Server authentication should be enabled.

RADIUS Authentication: ☒ Enable

Port:

Server Address:

Secret:

Extended privileges: ☐ kuli ☐ libradius

[Advanced Settings](#)

[Save](#) [Reset](#)

To enable/disable RADIUS, check or uncheck the “RADIUS Authentication” Enable checkbox respectively.

NOTE: Generic FreeRADIUS alone is supported.

RADIUS Authentication

Check the option ‘Enable’ to enable RADIUS authentication.

Port

Specify the RADIUS Port.

- The default Port is 1812.
- Port value ranges from 1 to 65535.

Server Address

Enter the ‘IP address’ of the RADIUS server

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

Advanced Settings

Click 'Advanced Settings' to Radius User Authorization.

The server address will support the following:

- IPv4 Address format.
- IPv6 Address format.

Secret

Enter the 'Authentication Secret' for RADIUS server

- Secret must be at least 4 characters long.
- Space is not allowed.

NOTE: This field will not allow more than 31 characters.

Save

Click 'Save' to save the settings.

Reset

Click 'Reset' to reset the modified changes.

2.5.14 Configure Remote Session



This page is used to configure virtual media configuration settings for the next redirection session.

Single Port Application

This select box is used to enable the single port application support at runtime.

KVM Encryption

Enable/Disable encryption on KVM data for the next redirection session.

Media Encryption

Enable/Disable encryption on Media data for the next redirection session.

NOTE: It will automatically close existing remote redirection either KVM or Virtual media sessions, if any.

Keyboard Languages

This select box is used to select the keyboard supported languages.

Local Monitor OFF

Check this box to enable Local Monitor ON/OFF command can be enabled at runtime.

Automatically OFF Local Monitor, When JViewer Launches

Check this box to automatically Lock the local monitor, When JViewer launches.

Save

Click 'Save' to save the current changes.

Reset

Click 'Reset' to reset the modified changes.

2.5.15 Services



Dashboard | FRU Information | Server Health | Configuration | Remote Control | Auto Video Recording | Maintenance | Firmware Update | ADMIN (Administrator) | Refresh | Print | Logout | [HELP](#)

Services

Below is a list of services running on the BMC. It shows current status and other basic information about the services. Select a slot and press "Modify" button to modify the services configuration.

Number of Services: 7

#	Service Name	Current State	Interface	Nonsecure Port	Secure Port	Timeout	Maximum Sessions	Active Sessions
1	web	Active	bond0	80	443	1800	20	5
2	kvm	Active	bond0	7578	7582	N/A	2	0
3	ok-medi	Active	bond0	5128	5124	N/A	1	0
4	st-media	Active	bond0	5122	5126	N/A	1	0
5	hy-media	Active	bond0	5123	5127	N/A	1	0
6	ssh	Active	N/A	N/A	22	600	N/A	N/A
7	lanef	Active	N/A	23	N/A	600	N/A	N/A

Modify

This page is used to display the basic information about services running in the BMC. To modify a service, the user must be an Administrator.

Modify

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. Users have to close the existing opened session for the service if needed.

2.5.16 SMTP Settings

The screenshot shows the ASRock BIOS Setup Utility interface. The top navigation bar includes links for Mainboard, System, Server Health, Configuration, Hardware Control, Audio Video Overclocking, Maintenance, and Firmware Update. The 'SMTP Settings' page is active, displaying the following configuration options:

- LAN Channel Number:** A dropdown menu set to '1'.
- Primary SMTP Server:**
 - SMTP Support:** ☒ Enable
 - Port:** 25
 - Sender Address:** [Empty text field]
 - SMTP Server requires authentication:** ☐ No
 - User Name:** [Empty text field]
 - Password:** [Empty text field]
- Secondary SMTP Server:**
 - SMTP Support:** ☐ Enable
 - Port:** 25
 - Sender Address:** [Empty text field]
 - SMTP Server requires authentication:** ☐ No
 - User Name:** [Empty text field]
 - Password:** [Empty text field]

Navigation buttons 'Back' and 'Exit' are located at the bottom right of the page.

This page is used to configure the SMTP settings.

LAN Channel Number

Select the LAN channel to which the SMTP information needs to be configured.

Sender Address

Enter the 'Sender Address' valid on the SMTP Server.

Machine Name

Enter the 'Machine Name' of the SMTP Server.

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

Primary SMTP Server

It lists the Primary SMTP Server configuration.

SMTP Support

Check this option to enable SMTP support for the BMC.

Port

Specify the SMTP Port.

-
- Default Port is 25.
 - Port value ranges from 1 to 65535.

Server Address

Enter the 'IP address' of the SMTP Server. It is a mandatory field.

- An IP Address is made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx".
- Each Number ranges from 0 to 255.
- The first Number must not be 0.

The server address will support the following:

- IPv4 Address format.
- IPv6 Address format.

SMTP Server requires Authentication

Check the option 'Enable' to enable SMTP Authentication.

Note: SMTP 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

Enter the username to access SMTP Accounts.

- The User Name can be 4 to 64 alpha-numeric characters.
- It must start with an alphabet.
- Special characters ',' (comma), ':' (colon), ';' (semicolon), ' ' (space) and '\' (backslash) are not allowed.

Password

Enter the password for the SMTP User Account.

- Passwords must be at least 4 characters long.
- Space is not allowed.

NOTE: This field will not allow more than 64 characters.

Secondary SMTP Server

It lists the Secondary SMTP Server configuration. It is an optional field. If the Primary SMTP server is not working, then it tries the Secondary SMTP Server configuration.

Save

Click 'Save' to save the new SMTP server configuration.

Reset

Click 'Reset' to reset the modified changes.

2.5.17 SSL Certificate Configuration

ASRock Rack American Megatrends

Dashboard Status Service Health Configuration Remote Control Auto Video Recording Maintenance Firmware Update

SSL Certificate Configuration

This page is used to configure the SSL certificate for the BMC. The SSL certificate is used to secure the BMC's communication with the web browser. The SSL certificate is generated by the BMC's internal SSL engine. The SSL certificate is used to secure the BMC's communication with the web browser. The SSL certificate is generated by the BMC's internal SSL engine. The SSL certificate is used to secure the BMC's communication with the web browser. The SSL certificate is generated by the BMC's internal SSL engine.

Upload SSL Generate SSL View SSL

Common Name (CN)
Organization (O)
Organizational Unit (OU)
City or Locality (L)
State or Province (ST)
Country (C)
Email Address
Valid For: days months
Key Length: bits key size

Generate

This page is used to upload a new SSL certificate and privacy key.

NOTE: Please check the current BMC time in NTP under the Configuration menu while uploading the SSL certificate.

Current Certificate

The current certificate, uploaded date/time information will be displayed (read only).

New Certificate

Browse and navigate the certificate file.

- The certificate file should be of pem type

Current Privacy Key

The current privacy key, uploaded date/time information will be displayed (read only).

New Privacy Key

Browse and navigate the privacy key file.

- The privacy key file should be of pem type

Upload

Click 'upload' to upload the SSL certificate and privacy key into the BMC.

NOTE: Upon successful upload, HTTPs service will be restarted to use the newly uploaded SSL certificate.

2.5.18 System and Audit Log Settings

System and Audit Log Settings

Enable and configure logging of system events below. Or you can enable/disable logging of audit events. Press the Save button to save your changes.

System Log

Log Type: ☒ Local Log ☐ Remote Log

File Size (in bytes):

Rotate Count:

Server Address:

Audit Log

☒ Enable

This page is used to configure the System and Audit log settings.

System Log

Check the option 'Enable' to enable system logs.

Log Type

Select the Log type for system logs, whether it should be preserved in a local file or on a remote server. Local file resides at `/var/log/`.

File Size

If Local log is selected, specify the size of the file in bytes.

- Size ranges from 3 to 65535.

Rotate Count

When logged information exceeds the specified file size, the old log information automatically gets moved to backup files based on the rotate count value. If the rotate count is zero, the old log information gets cleared permanently each time.

- Value ranges from 0 to 255.

Server Address

Specify the remote server address to log system events. The server address will support the following:

- IP Address (Both IPv4 and IPv6 format).
- FQDN (Fully qualified domain name) format.

Audit Log

Check the option 'Enable' to enable audit log.

Save

Click 'Save' to save the configured settings.

Reset

Click 'Reset' to reset to the previously saved values.

2.5.19 System Firewall



This page is used to configure System Firewall settings. The firewall rule can be set for an IP or range of IP Addresses or Port numbers.

Advanced Setting

Click 'Advanced Setting' to set Block All and Flush All options.

Block All

This option will block all incoming IPs and Ports.

Flush All

This is used to flush all the system firewall rules.

Save

Click "Save" to save the current changes.

IP address page

This is used to add a new IP Address or Range of IP Address rule settings.

Add

Click 'Add' to configure IP/IP range & IP settings.

IP/IP range

This field is used to set the IP Address or Range of IP Addresses manually. IP Address will support IPv4 and IPv6 Address formats:

- 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 groups of 4 Hexadecimal digits separated by colon as in xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx.
 - Hexadecimal digits are expressed as lower-case letters.

IP setting

IP Settings are used to determine the rule whether block or allow from the configured IP or IP Range.

Save

Click “Save” to save the current changes.

Port page

This is used to configure the Port/ Port range & Port settings.

Add

Click ‘Add’ to configure Port/ Port range & Port settings.

Port/Port range

This field is used to set the Port Address or Range of Ports manually.

Port setting

This column indicates the current setting of the listed Port or Range of Port rules (Allow or Block).

Save

Click “Save” to save the current changes.

2.5.20 User Management

User Management

The list below shows the current list of available users. To delete or modify a user, select their name in the list and press 'Delete User' or 'Modify User'. To add a new user, select an unconfigured slot and press 'Add User'.

Number of configured users: 2

Slot#	Username	User Access	Network Privilege	Email ID
1	anonymous	Disabled	Administrator	
2	admin	Enabled	Administrator	
3	~	~	~	~
4	~	~	~	~
5	~	~	~	~
6	~	~	~	~
7	~	~	~	~
8	~	~	~	~
9	~	~	~	~
10	~	~	~	~

[Add User](#) [Modify User](#) [Delete User](#)

The displayed table shows any configured Users and available slots. You can modify or add new users from here. A maximum of 10 slots are available, including the default admin and anonymous. It is advised that the anonymous user's privilege and password should be modified as a security measure. To view the page, you must have Operator privileges. To modify or add a user, You must have Administrator privileges.

NOTE: Free slots are denoted by “~” in all columns for the slot.

Add User

Select a free slot and click 'Add User' to add a new user to the device. Alternatively, double click on a free slot to add a user.

Modify User

Select a configured slot and click 'Modify User' to modify that user. Alternatively, double click on the configured slot.

Delete User

Select the desired user to be deleted and click 'Delete User'.

2.5.21 Virtual Media Devices

The screenshot shows the ASRock Rack BIOS interface. At the top, there's a header with the ASRock Rack logo on the left and the American Megatrends logo on the right. Below the header is a navigation bar with tabs: Dashboard, System, Server Health, Configuration (selected), Remote Control, Auto Video Recording, and Maintenance. A sub-header 'Firmware Update' is visible on the left, and a 'HELP' link is on the right. The main content area is titled 'Virtual Media Devices'. It contains a paragraph: 'The following option will allow to configure virtual media devices. Below, you can select the number of instances that are supported for each type of virtual media devices.' Below this, there are four settings: 'Floppy devices' with a dropdown menu set to '1', 'CD/DVD devices' with a dropdown menu set to '1', 'Hard disk devices' with a dropdown menu set to '1', and 'Power Save Mode' with a checked checkbox and the label 'Enable'. At the bottom right of the configuration area are 'Save' and 'Reset' buttons.

Use this page to configure Virtual Media device settings.

Floppy devices

Select the number of floppy devices that support Virtual Media redirection.

CD/DVD devices

Select the number of CD/DVD devices that support Virtual Media redirection.

Hard disk devices

Select the number of hard disk devices that support Virtual Media redirection.

Power Save Mode

Enable/Disable virtual USB devices visibility in the host.

Save

Click 'Save' to save the configured settings.

Reset

Click 'Reset' to reset the previously-saved values.

2.5.22 Keep NCSI Link Up



This page is used to configure the share NIC (NCSI) PHY link up setting. If it is enabled, share NIC PHY will keep link up, which can avoid share NIC disconnection while system is resetting.

VetoBit

Check this option to enable/disable the VetoBit.

Save

Click 'Save' to save the configured setting.

Reset

Click 'Reset' to reset the modified changes.

2.6 Remote Control

2.6.1 Console Redirection



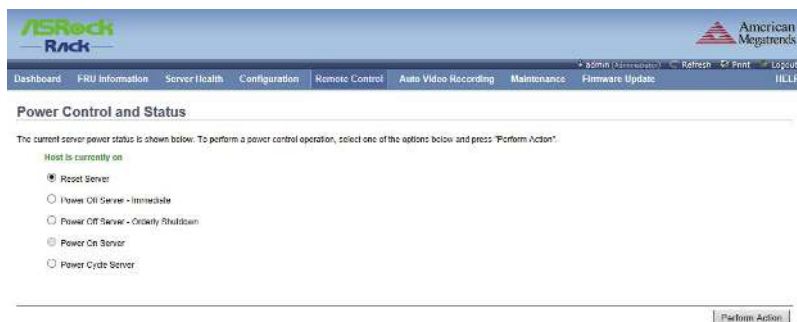
Launch the remote console redirection window from this page. To launch it, you must have Administrator privileges.

NOTE: A compatible JRE must be installed in the system prior to the launch of the JNLP file.

Java Console

Click 'Java Console' which will cause the `jviewer.jnlp` file to be downloaded. Once the file is downloaded and launched, a Java redirection window will be displayed.

2.6.2 Power Control and Status



This page helps you to view or perform any host power cycle operations.

Reset Server

Select this option to reboot the system without powering off (warm boot).

Power Off Server - Immediate

Select this option to immediately power off the server.

Power Off Server - Orderly Shutdown

Select this option to initiate operating system shutdown prior to the shutdown.

Power On Server

Select this option to power on the server.

Power Cycle Server

Select this option to first power off, and then reboot the system (cold boot).

2.6.3 Java SOL



Launch the Java SOL, you must have Administrator privileges.

NOTE: A compatible JRE must be installed in the system prior to the launch of the JNLP file.

2.7 Auto Video Recording

2.7.1 Triggers Configuration

The screenshot shows the 'Triggers Configuration' page in the iBMC web interface. The page has a blue header with the 'iBMC Rack' logo and 'American Megatrends' logo. Below the header is a navigation bar with links: Dashboard, FRU Information, Server Health, Configuration, Remote Control, Auto Video Recording, Maintenance, Firmware Update, and iLLP. The main content area is titled 'Triggers Configuration' and contains a description: 'This page allows the user to configure which events will trigger the auto video recording function of the KVM server'. There are two columns of checkboxes for selecting events to trigger recording. The left column includes: Temperature/Voltage Critical Events, Temperature/Voltage Non Recoverable Events, Watchdog Timer Events, Chassis Power off Event, and Particular User and Time Event. The right column includes: Temperature/Voltage Non Critical Events, Fan state changed Events, Chassis Power on Event, Chassis Reset Event, and LPC Reset Event. Below the checkboxes, there is a 'Date' field with a dropdown menu showing 'March', a day selector showing '3', and a year selector showing '2014'. There is also a 'Time' field with a dropdown menu showing '00:00:00' and a time selector showing '12:00:32'. At the bottom right of the page, there are 'Save' and 'Reset' buttons.

Triggers Configuration

This page allows the user to configure which events 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 User and Time Event

Date: March 3 2014

Time: 00:00:00 12 00 32

☐ Temperature/Voltage Non Critical Events

☐ Fan state changed Events

☐ Chassis Power on Event

☐ Chassis Reset Event

☐ LPC Reset Event

Save Reset

Configure which events on the page will trigger the auto-video recording option to start.

NOTE: Maximum of 2 video files can be recorded in BMC.

Event List

You can check/uncheck a box to add/remove that trigger for your system.

Save

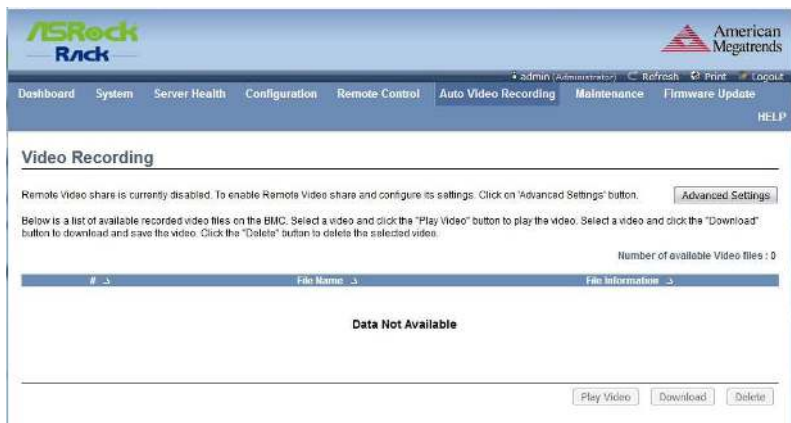
Click 'Save' to save any changes made.

NOTE: KVM service should be enabled (under 'Configuration -> Services') to perform auto-video recording.

Reset

Click 'Reset' to reset the modified changes.

2.7.2 Video Recording



This page displays the list of available recorded video files on the BMC. 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.

NOTE: A maximum of 2 video files can be recorded in BMC.

Advanced Settings

Click this option to configure the Remote Video Settings. Options are Enable/Disable Remote Video Support, Server Address, Source Path, Share Type, Username, Password and Domain Name.

Play Video

Select a video and click the Play Video button to play the video file in the Java Application.

Download

Select a video and click the Download button to download and save the video file in the client machine. The video will be downloaded in (.avi) format.

Delete

Click the Delete button to delete the selected video file.

2.8 Maintenance

2.8.1 Preserve Configuration

ASRock Rack American Megatrends

Dashboard System Server Health Configuration Remote Control Audio Video Recording Maintenance Firmware Update

Preserve Configuration

This page allows you to select the specific configuration items to be preserved in the cases of "Restore Configuration", and "Firmware Update without Preserve Configuration option".

[Click here to go to Firmware Update or Restore Configuration](#)

Number of Preserved Items: 0

#	Preserve Configuration Item	Preserve Status
1	SDR	☐
2	FRU	☐
3	SBL	☐
4	IPMB	☐
5	Hibernation	☐
6	nTPT	☐
7	SSH	☐
8	VBIOS	☐
9	Authentication	☐
10	Bypass	☐

Check which configurations need to be preserved, while Restore Factory Defaults is done.

Configuration list

You can either check/uncheck a check box to preserve/overwrite the configurations for your system.

Check All

Click this button to check the whole configuration list.

Uncheck All

Click this button to uncheck the whole configuration list.

Save

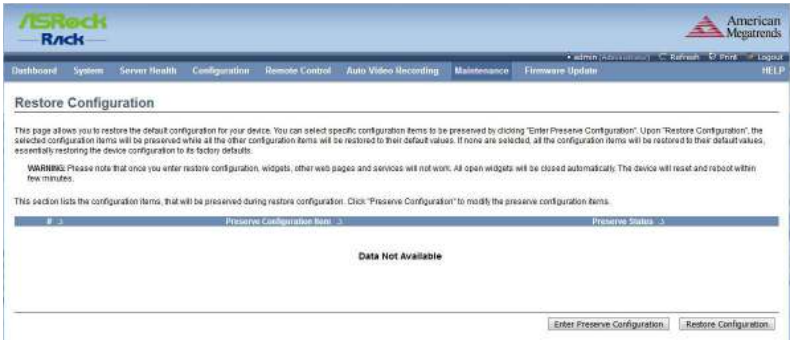
Click 'Save' to save any changes made.

NOTE: This configuration is used by the Restore Factory Defaults process.

Reset

Click 'Reset' to reset the modified changes.

2.8.2 Restore Factory Defaults



This page helps to restore the factory defaults of the device. 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 a few minutes.

Preserve Configuration

Click this to redirect to Preserve configuration page, which is used to preserve the particular configurations not to be overwritten by the default configuration.

Restore Factory Defaults

Click this to restore the firmware with default configurations.

2.8.3 System Administrator

System Administrator

This page allows the user to enable/disable access and change the password for the System Administrator account.

Username: sysadmin

User Access: ☒ Enable ☐ Change Password

Password:

Confirm Password:

Save Reset

This page is used to configure the System Administrator configurations.

Username

Username of the System Administrator is displayed (read only).

User Access

Check this option to enable user access for the system administrator.

Change Password

To change the user's password, check the 'Change Password' option. This will enable the password fields.

Password, Confirm Password

Enter and confirm the new password here.

- Passwords must be at least 8 characters long.
- Space is not allowed.

NOTE: This field will not allow more than 64 characters.

Save

Click 'Save' to save the new configuration for the system administrator.

Reset

Click 'Reset' to reset the modified changes.

2.9.2 BIOS Update



This page is used to update BIOS of the host.

WARNING: Please note that after entering update mode widgets, all open widgets will be closed automatically.

Start Updating BIOS

1. Click "Start Updating BIOS" to start the BIOS update procedure.
2. Click "OK" on the prompt window.
3. Upload the BIOS image.
4. Click "Proceed" when [BIOS update confirmation] windows prompts out.
5. Flashing BIOS image.
6. Wait for about one minute to reset BIOS.

2.9.3 Image Transfer Protocol

The screenshot shows the ASRock Rack BIOS/UEFI interface. At the top, there is a navigation bar with links: Dashboard, FRU Information, Server Health, Configuration, Remote Control, Auto Video Recording, Maintenance, Firmware Update, Refresh, Print, Logout, and HELP. The 'Firmware Update' link is highlighted. Below the navigation bar, the title 'Image Transfer Protocol' is displayed. A sub-header states: 'The following option will allow to configure firmware image protocol information.' The configuration area contains four fields: 'Protocol Type' (a dropdown menu with 'HTTP/HTTPS' selected), 'Server Address' (a text input field), 'Source Path' (a text input field), and 'Retry Count' (a numeric input field with '0' entered). At the bottom right of the configuration area, there are two buttons: 'Save' and 'Reset'.

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

Protocol Type

Protocol type to transfer the firmware image into the BMC.

Server Address

The Server IP address of the firmware image is stored.

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

Source Path

Full Source path with filename of where 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

Click 'Save' to save the configured settings.

Reset

Click 'Reset' to reset the modified changes.