
IPMI Configuration Guide

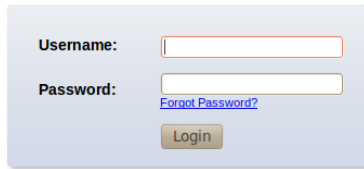
- 1. Introduction of IPMI Server Manager 2
- 2. IPMI Server Manager GUI Overview 3

1. Introduction of IPMI Server Manager

IPMI Server Manager 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 IPMI Server Manager GUI using standard Internet browsers.

2. IPMI Server Manager GUI Overview

2.1 Login page



Username:


Password:

[Forgot Password?](#)

Login

Language:

Required Browser Settings

1. Allow popups from this site ✓
2. Allow file download from this site. (How to )
3. Enable javascript for this site ✓
4. Enable cookies for this site ✓

It is recommended not to use Refresh, Back and Forward options of the browser.

The default username is “root” and password is “changeme”. It is recommended to change the username and password after your first login.
*Choose your preferred language from the language drop-down menu.

2.2 Dashboard

The screenshot shows the IPMI Server Manager interface. At the top, there's a navigation bar with tabs: Dashboard, FRU Information, Server Health, Configuration, Remote Control, Auto Video Recording, Maintenance, and Firmware Update. The main content area is titled "Dashboard" and is divided into several sections:

- Remote Control:** Includes a "Launch" button and a window titled "Capturing..." with a "Refresh" button.
- Location LED Status:** Shows a status indicator (a circle) and a toggle switch set to "ON".
- Device Information:** Displays "Firmware Revision: 0.32.0" and "Firmware Build Time: Aug 6 2013 20:20:03 CST".
- Network Information:** Shows MAC Address (BC:5F:F4:BC:42:38), V4 Network Mode (Static), IPv4 Address (192.168.30.205), and V6 Network Mode (Disable).
- Event Logs:** A pie chart showing the distribution of event types: Unknown (2.2%), +5V (0.16%), SYS_FAN1 (0.05%), CPU_FAN1 (0.11%), VCCM (0.11%), +12V (0.33%), and Free Space (97.04%).
- Sensor Monitoring:** A table listing various sensors and their readings.

Status	Sensor	Reading
●	ATX+5VSB	5.1 Volts
●	+3VSB	3.439 Volts
●	Vcore	1.76 Volts
●	VCCM	1.49 Volts
●	+1.05V	1.06 Volts
●	CPU VCCIO_OUT	1.01 Volts
●	BAT	3.06 Volts
●	+3V	3.34 Volts
●	+5V	5.13 Volts
●	+12V	12 Volts
●	CPU_FAN1	1600 RPM
●	SYS_FAN1	Not Available
●	AUX_FAN1	Not Available
●	HDD_FAN1	Not Available
●	MB Temperature	39 ° C
●	TR1 Temperature	39 ° C
●	CPU Temperature	51 ° C
●	HDD_1	Not Available
●	HDD_2	Not Available
●	HDD_3	OK
●	HDD_4	OK
●	HDD_5	Not Available
●	HDD_6	Not Available
●	HDD_7	Not Available
●	HDD_8	Not Available

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.

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 Server Health

2.3.1 Sensor Readings

The screenshot displays the 'Sensor Readings' section of a web application. The top navigation bar includes 'Dashboard', 'FRU Information', 'Server Health', 'Configuration', 'Remote Control', 'Auto Video Recording', 'Maintenance', and 'Firmware Update'. The 'Sensor Readings' section contains a table of sensors and a detailed view for the selected 'ATX+5VSB' sensor.

Sensor Name	Status	Current Reading
ATX+5VSB	Normal	Not Available
+3VSB	Normal	Not Available
Vcore	Normal	Not Available
VCCM	Normal	Not Available
+1.05	Normal	Not Available
CPU_VTT	Normal	Not Available
BAT	Normal	Not Available
+3V	Normal	Not Available
+5V	Normal	Not Available
+12	Normal	Not Available
CPU_FAN1	Lower Non-Critical	Not Available
REAR_FAN1	Lower Non-Critical	Not Available
FRNT_FAN1	Lower Non-Critical	Not Available
FRNT_FAN2	Lower Non-Critical	Not Available
FRNT_FAN3	Lower Non-Critical	Not Available
CPU_FAN1_2	Normal	Not Available
MB TemperatureZP	Normal	Not Available

ATX+5VSB: Not Available **NORMAL**

Thresholds for this sensor

Lower Non-Recoverable (LNR)	4.049	Upper Non-Recoverable (UNR)	6.029
Lower Critical (LC)	4.259	Upper Critical (UC)	5.759
Lower Non-Critical (LNC)	4.5	Upper Non-Critical (UNC)	5.49

Graphical View of this sensor's events

LNR	LC	LNC	UNR
(0)	(0)	(0)	(0)

A list of sensor readings will be displayed here. Click on a record to show more information about that particular sensor, including thresholds and a graphical representation of all associated events. Double click on a record to toggle (ON / OFF) the live widget for that particular sensor. You can filter the list to view particular sensors only using the drop-down listbox.

NOTE: N/A represents Not Applicable.

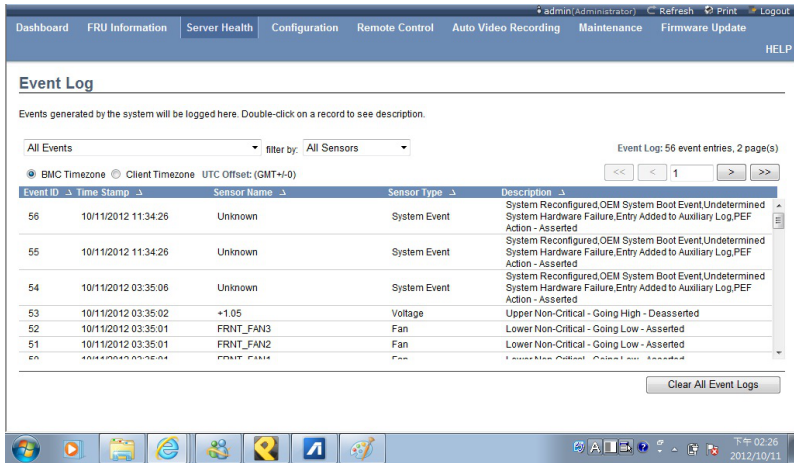
Live Widget

Turn On or Off the live widget for this sensor. This widget gives a dynamic representation of the readings for the sensor.

View this Event Log

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

2.3.2 Event Log



The screenshot shows a web-based Event Log interface. At the top, there are navigation tabs: Dashboard, FRU Information, Server Health (selected), Configuration, Remote Control, Auto Video Recording, Maintenance, and Firmware Update. Below the tabs, the page title is "Event Log". A message states: "Events generated by the system will be logged here. Double-click on a record to see description." Below this, there are filter options: "All Events" (selected), "filter by: All Sensors", and "Event Log: 56 event entries, 2 page(s)". There are also checkboxes for "BMC Timezone", "Client Timezone", and "UTC Offset: (GMT+0)". A table of events is displayed with the following columns: Event ID, Time Stamp, Sensor Name, Sensor Type, and Description. The table contains several entries, including system events and fan status changes. At the bottom of the table, there is a "Clear All Event Logs" button. The browser's taskbar and system tray are visible at the bottom of the screenshot.

Event ID	Time Stamp	Sensor Name	Sensor Type	Description
56	10/11/2012 11:34:26	Unknown	System Event	System Reconfigured.OEM System Boot Event.Undetermined System Hardware Failure.Entry Added to Auxiliary Log.PEF Action - Asserted
55	10/11/2012 11:34:26	Unknown	System Event	System Reconfigured.OEM System Boot Event.Undetermined System Hardware Failure.Entry Added to Auxiliary Log.PEF Action - Asserted
54	10/11/2012 03:35:06	Unknown	System Event	System Reconfigured.OEM System Boot Event.Undetermined System Hardware Failure.Entry Added to Auxiliary Log.PEF Action - Asserted
53	10/11/2012 03:35:02	+1.05	Voltage	Upper Non-Critical - Going High - Deasserted
52	10/11/2012 03:35:01	FRNT_FAN3	Fan	Lower Non-Critical - Going Low - Asserted
51	10/11/2012 03:35:01	FRNT_FAN2	Fan	Lower Non-Critical - Going Low - Asserted
50	10/11/2012 03:35:01	FRNT_FAN1	Fan	Lower Non-Critical - Going Low - Asserted

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.

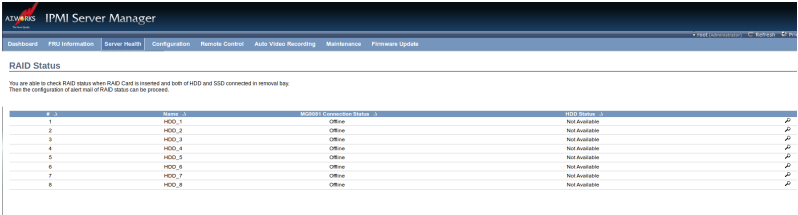
UTC Offset

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.

Clear All Event Logs

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

2.3.3 RAID Status



You are able to check RAID status when RAID Card is inserted and both of HDD and SSD connected in removal bay. Then the configuration of each row of RAID appears on the screen.

ID	Name	Controller	RAID Status	
1	HDD_0	Offline	Not Available	
2	HDD_1	Offline	Not Available	
3	HDD_2	Offline	Not Available	
4	HDD_3	Offline	Not Available	
5	HDD_4	Offline	Not Available	
6	HDD_5	Offline	Not Available	
7	HDD_6	Offline	Not Available	
8	HDD_7	Offline	Not Available	

RAID Status provides information for you to monitor the RAID status.

The magnifying glass allows access to the details page for the selected item.

*Please make sure your RAID Card is inserted and HDD/SSD are well connected.

2.3.4 System and Audit Log

admin(Administrator) Refresh Print Logout

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

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: Alert This Filter: 2 event entries

Event ID ↕	Time Stamp ↕	HostName ↕	Description ↕
1	Oct 11 03:28:19	AMBC5FF45601A4	kernel: Helper Module Driver Version 1.2
2	Oct 11 03:28:19	AMBC5FF45601A4	kernel: Copyright (c) 2006 American Megatrends Inc.

下午 02:27
2012/10/11

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 and Audit 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.

2.4 Configuration

2.4.1 Active Directory Settings

The screenshot shows the 'Active Directory Settings' page. At the top, there is a navigation bar with the following tabs: Dashboard, FRU Information, Server Health, Configuration (selected), Remote Control, Auto Video Recording, Maintenance, and Firmware Update. Below the navigation bar, the page title is 'Active Directory Settings'. A message states: 'The 'Active Directory' is currently disabled. To enable Active Directory and configure its settings, click on 'Advanced Settings' button.' There is an 'Advanced Settings' button. Below this, another message says: '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.' A counter indicates 'Number of configured Role groups: 0'. A table with the following columns is displayed: Role Group ID, Group Name, Group Domain, and Group Privilege. The table contains five rows, each with a role group ID (1-5) and '~' in the other three columns. Below the table are three buttons: 'Add Role Group', 'Modify Role Group', and 'Delete Role Group'. The Windows taskbar is visible at the bottom of the screenshot, showing the system clock as 下午 02:30 on 2012/10/11.

Role Group ID	Group Name	Group Domain	Group Privilege
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.

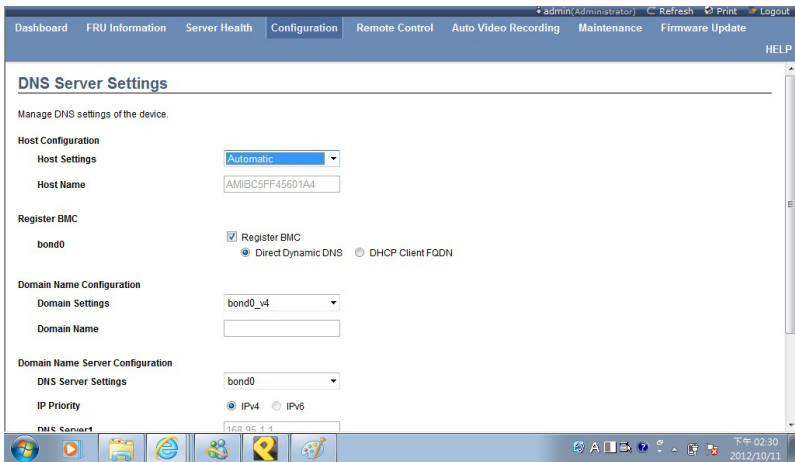
Modify Role Group

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'.

2.4.2 DNS Server Settings



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

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.

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.

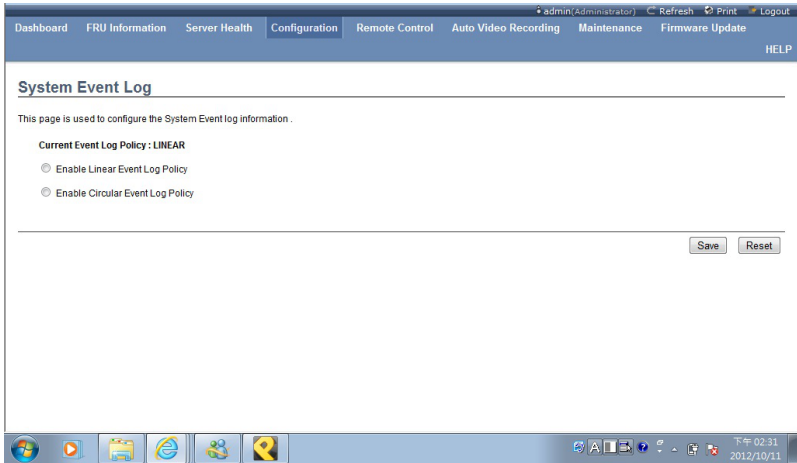
Save

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.

2.4.3 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.

2.4.4 Images Redirection

admin(Administrator) Refresh Print Logout

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

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.

Advanced Settings

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

Windows taskbar: 下午 02:32 2012/10/21

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.

2.4.5 LDAP/E-Directory Settings

admin(administrator) Refresh Print Logout

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

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.

Number of configured Role groups: 0

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

Add Role Group Modify Role Group Delete Role Group

下午 02:34 2012/10/11

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'.

2.4.6 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.

2.4.7 Network Settings

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

Network Settings

Manage network settings of the device.

LAN Interface	IPMI/LAN Port
LAN Settings	<input checked="" type="checkbox"/> Enable
MAC Address	BC:5F:F4:BC:42:38
IPv4 Configuration	
Obtain an IP address automatically	<input type="checkbox"/> Use DHCP
IPv4 Address	192.168.30.205
Subnet Mask	255.255.255.0
Default Gateway	192.168.30.1
IPv6 Configuration	
IPv6 Settings	<input type="checkbox"/> Enable
Obtain an IP address automatically	<input type="checkbox"/> Use DHCP
IPv6 Address	::
Subnet Prefix length	0
Default Gateway	::
VLAN Configuration	
VLAN Settings	<input type="checkbox"/> Enable
VLAN ID	0
VLAN Priority	0

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 IPv4 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.

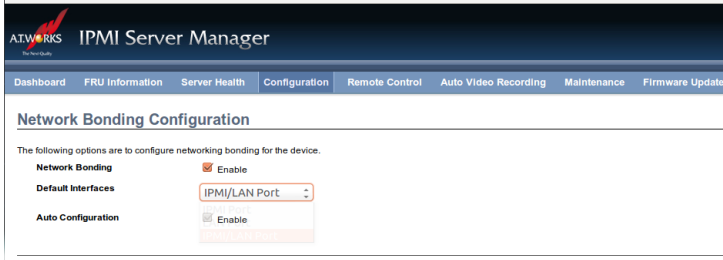
Save

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.

2.4.8 Network Bonding Configuration



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

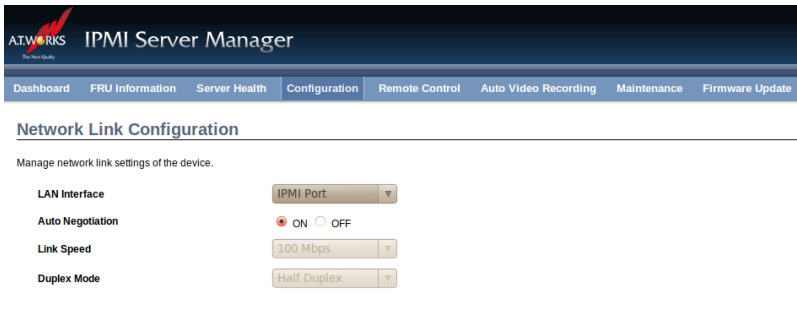
Click "Save" to save the current changes.

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

Reset

Click "Reset" to reset the modified changes.

2.4.9 Network Link Configuration



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.

2.4.10 NTP Settings

admin(Administrator) Refresh Print Logout

Dashboard FRU Information Server Health 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: October 11 2012

Time: (hh:mm:ss) 06 36 50

UTC Timezone: (GMT+/-0) Hour(s)

NTP Server: pool.ntp.org

Automatically synchronize Date & Time with NTP Server

Refresh Save Reset

下午 02:37
2012/10/11

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.

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.

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.

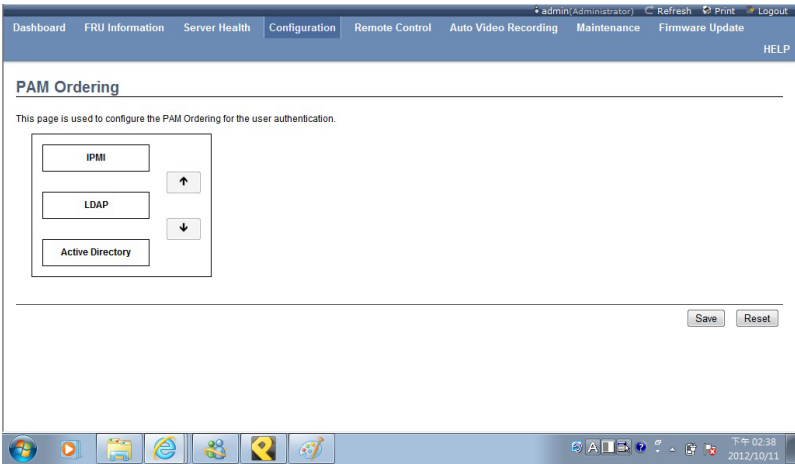
Save

Click 'Save' to save any changes made.

Reset

Click 'Reset' to reset the modified changes.

2.4.11 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.

2.4.12 PEF Management

admin(Administrator) Refresh Print Logout

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

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	~	~	~	~
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	~	~	~	~
12	~	~	~	~
13	~	~	~	~

Add Modify Delete

下午 02:39 2012/10/11

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'.

2.4.13 RADIUS Settings

admin/Administrator Refresh Print Logout

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

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

Time Out seconds

Server Address

Secret

Save Reset

下午 02:40
2012/10/11

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.

Time Out

Specify the Time out value.

- The default Time out value is 3 seconds.
- Time out value ranges from 3 to 300.

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.

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.

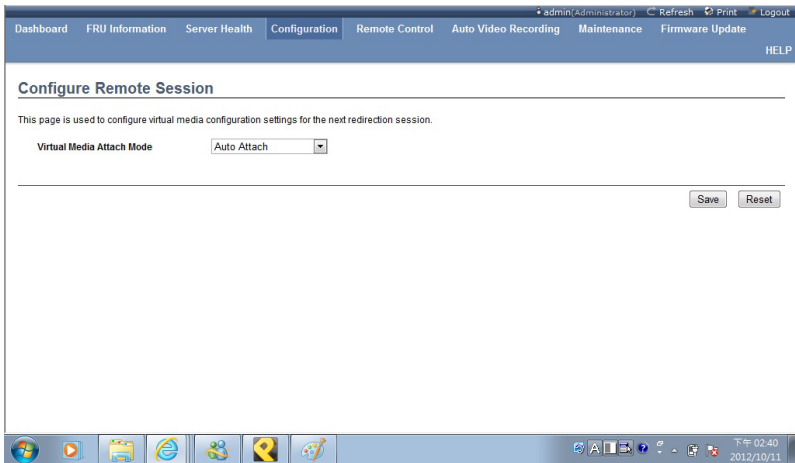
Save

Click 'Save' to save the settings.

Reset

Click 'Reset' to reset the modified changes.

2.4.14 Configure Remote Session



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

Virtual Media Attach Mode

Two types of VM attach modes are available:

- Attach - Immediately attaches Virtual Media to the server upon bootup.
- Auto Attach - Attaches Virtual Media to the server only when a virtual media session is started.

Save

Click 'Save' to save the current changes.

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

Reset

Click 'Reset' to reset the modified changes.

2.4.15 Services

admin(administrator) Refresh Print Logout

Dashboard FRU Information Server Health Configuration Remote Control Auto Video Recording Maintenance Firmware Update 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	Interfaces	Nonsecure Port	Secure Port	Timeout	Maximum Sessions	Active Sessions
1	web	Active	bond0	80	443	1800	20	1
2	lcm	Active	bond0	7578	7582	N/A	2	0
3	cd-media	Active	bond0	5120	5124	N/A	1	0
4	fd-media	Active	bond0	5122	5126	N/A	1	0
5	hd-media	Active	bond0	5123	5127	N/A	1	0
6	ssh	Active	N/A	N/A	22	600	N/A	N/A
7	telnet	Active	N/A	23	N/A	600	N/A	N/A

Modify

下午 02:43
2012/10/11

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.

2.4.16 SMTP Settings

The screenshot shows a web-based configuration interface for SMTP settings. The page title is "SMTP Settings". Below the title, there is a navigation bar with tabs: Dashboard, FRU Information, Server Health, Configuration (selected), Remote Control, Auto Video Recording, Maintenance, Firmware Update, and HELP. The main content area is titled "Manage SMTP settings of the device." and contains the following fields:

- LAN Channel Number:** A dropdown menu with the value "1" selected.
- Sender Address:** A text input field.
- Machine Name:** A text input field.
- Primary SMTP Server:**
 - SMTP Support:** A checked checkbox labeled "Enable".
 - Server Address:** A text input field.
 - SMTP Server requires Authentication:** An unchecked checkbox.
 - User Name:** A text input field.
 - Password:** A text input field.
- Secondary SMTP Server:**
 - SMTP Support:** A checked checkbox labeled "Enable".
 - Server Address:** A text input field.
 - SMTP Server requires Authentication:** An unchecked checkbox.
 - User Name:** A text input field.
 - Password:** A text input field.

The bottom of the screenshot shows a Windows taskbar with various icons and a system tray displaying the time "下午 02:54" and date "2012/10/11".

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.

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.

2.4.17 SSL Certificate Configuration

Dashboard FRU Information Server Health Configuration Remote Control Auto Video Recording Maintenance Firmware Update Refresh Print Logout HELP

SSL Certificate Configuration

This page is used to configure SSL certificate into the BMC. Using this, the device can be accessed in a secured mode. 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.

Upload SSL Generate SSL View SSL

Current Certificate Thu Jan 1 00:00:00 1970

New Certificate 浏览

Current Privacy Key Thu Jan 1 00:00:00 1970

New Privacy Key 浏览

Upload

下午 02:55 2012/10/11

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.

2.4.18 System and Audit Log Settings

The screenshot shows a web browser window displaying the 'System and Audit Log Settings' page. The page has a navigation menu at the top with items: Dashboard, FRU Information, Server Health, Configuration (selected), Remote Control, Auto Video Recording, Maintenance, Firmware Update, and HELP. The main content area is titled 'System and Audit Log Settings' and contains the following settings:

- System Log:** Enable
- Log Type:** Local Log Remote Log
- File Size (in bytes):**
- Rotate Count:**
- Server Address:**
- Audit Log:** Enable

At the bottom right of the settings area are 'Save' and 'Reset' buttons. The Windows taskbar at the bottom shows the system tray with the date and time: 下午 02:57, 2012/10/21.

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.

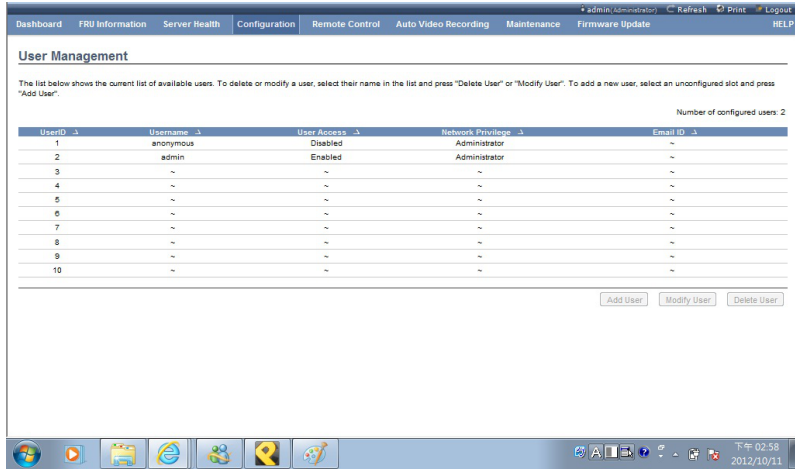
Save

Click 'Save' to save the configured settings.

Reset

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

2.4.19 User Management



Dashboard FRU Information Server Health Configuration Remote Control Auto Video Recording Maintenance Firmware Update admin (Administrator) Refresh Print Logout HELP

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

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

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'.

2.5.20 Virtual Media Devices

The screenshot shows a web browser window displaying the 'Virtual Media Devices' configuration page. The page title is 'Virtual Media Devices'. Below the title, there is a sub-header: 'The following option will allow to configure virtual media devices.' The configuration options are:

- Floppy devices: 1 (dropdown menu)
- CD/DVD devices: 1 (dropdown menu)
- Harddisk devices: 1 (dropdown menu)
- SD Media Support: Enable

At the bottom right of the configuration area, there are two buttons: 'Save' and 'Reset'. The browser's address bar shows 'ADMIN/Administrator', and the system tray at the bottom right shows the time '下午 02:59' and date '2012/10/11'.

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.

SD Media Support

Check this option to enable SD Media support in BMC.

Save

Click 'Save' to save the configured settings.

Reset

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

2.4.21 Network Filter Configuration

The screenshot shows the ATW RKS IPMI Server Manager interface. The top navigation bar includes: Dashboard, FRU Information, Server Health, Configuration, Remote Control, Auto Video Recording, Maintenance, and Firmware Update. The main heading is "Network Filter Configuration". Below the heading, a message states: "The following options are to configure networking ip filter for the device." The configuration area contains three input fields: "Mode" with a dropdown menu showing "WWW", "IP Address" with an empty text box, and "Target" with a dropdown menu showing "ACCEPT" and an "Add" button. Below these fields, a small note reads: "192.168.100.1 or 192.168.50.0/24 for IP" and "82:5F:01:02:03:04 for MAC". At the bottom, there is a table with columns for "#", "Mode", "Address", "Target", and a "Clear All" button.

#	Mode	Address	Target	Clear All
---	------	---------	--------	-----------

The Network Filter Configuration allows the administrator to limit the users within a certain range of IP addresses to access the device.

Mode

Select the Mode.

IP Address

Enter the IP Address.

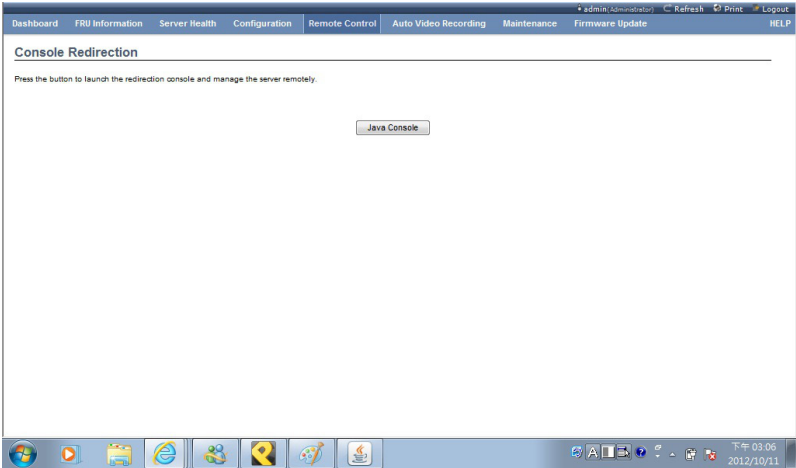
Target

Select the ACCEPT option to assign the range of IP addresses that are allowed to access the device, or select the DENY option to assign the range of IP addresses that are blocked to access the device.

Click on 'Add' to save the setting.

2.5 Remote Control

2.5.1 Console Redirection



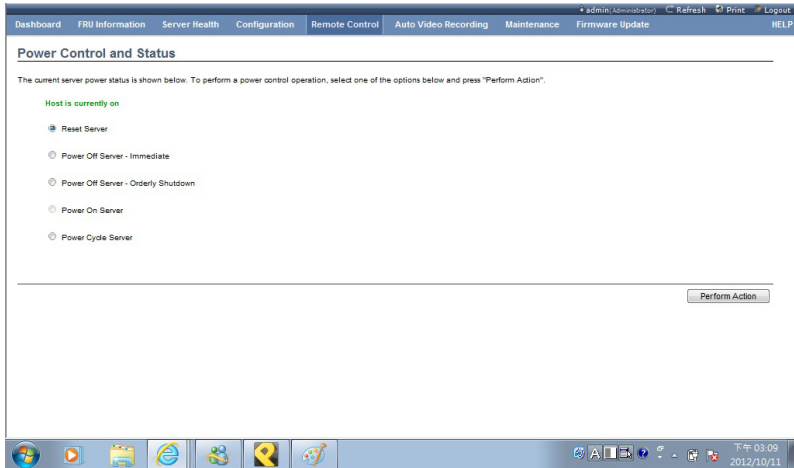
Launch the remote console redirection window from this page. To launch it, you must have Administrator privileges.

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.

2.5.2 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.

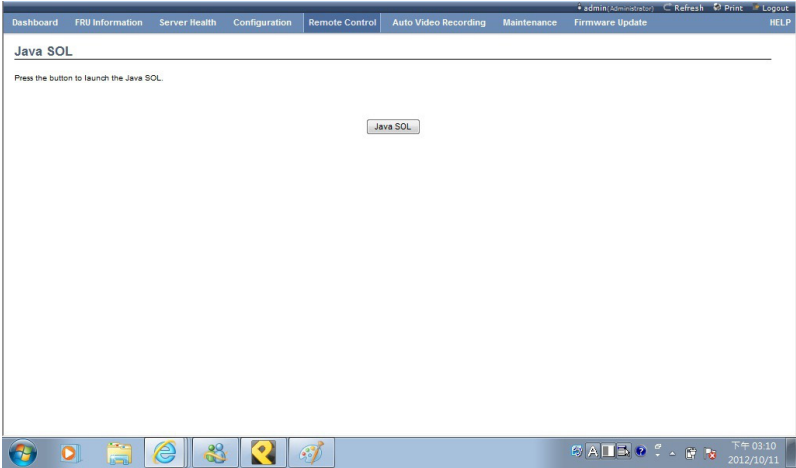
Power Cycle Server

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

Perform Action

Click 'Perform Action' to perform the selected option.

2.5.3 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.

2.6 Auto Video Recording

2.6.1 Triggers Configuration

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

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 Date and Time Event
- Temperature/Voltage Non Critical Events
- Fan state changed Events
- Chassis Power on Event
- Chassis Reset Event
- LPC Reset Event

Date: October 11 2012

Time: (hh:mm:ss) 07 10 10

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

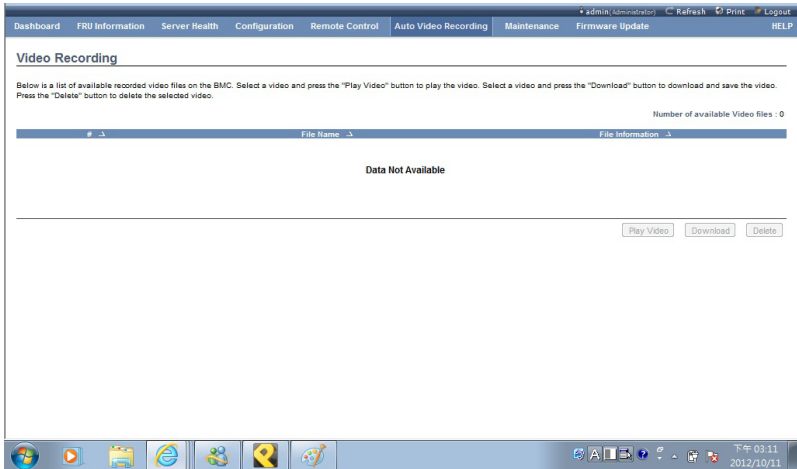
Click 'Save' to save any changes made.

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

Reset

Click 'Reset' to reset the modified changes.

2.6.2 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.

Play Video

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

Download

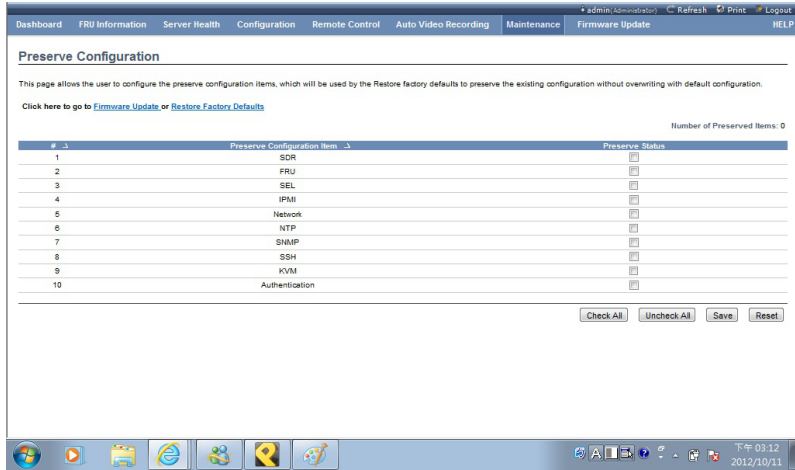
Select a video and click the Download button to download and save the video file in the client machine. The video will be downloaded in (.avi) format.

Delete

Click the Delete button to delete the selected video file.

2.7 Maintenance

2.7.1 Preserve Configuration



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

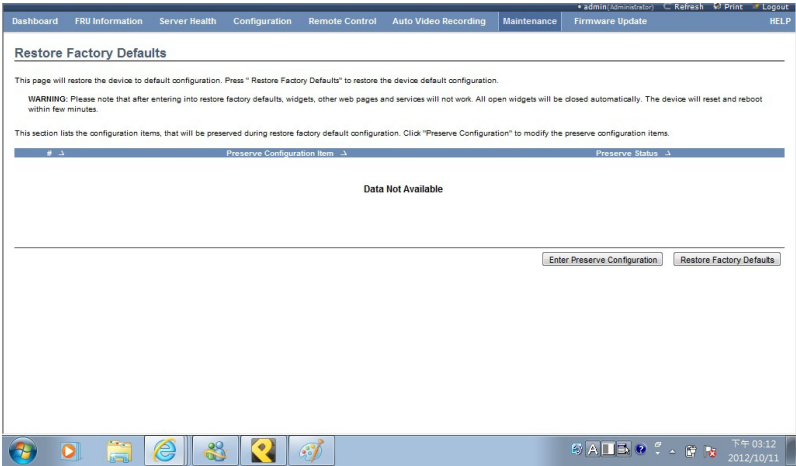
Click 'Save' to save any changes made.

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

Reset

Click 'Reset' to reset the modified changes.

2.7.2 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.

2.7.3 System Administrator

Dashboard FRU Information Server Health Configuration Remote Control Auto Video Recording Maintenance Firmware Update admin/Administrator Refresh Print Logout HELP

System Administrator

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

Username

User Access Enable Change Password

Password

Confirm Password

下午 03:13 2012/10/21

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.

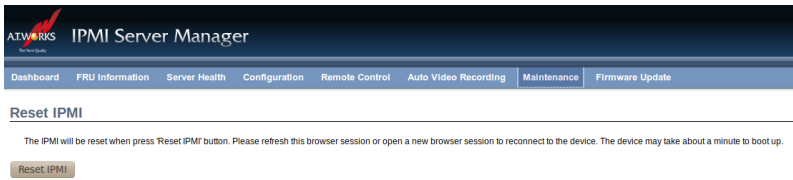
Save

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

Reset

Click 'Reset' to reset the modified changes.

2.7.4 IPMI Reset



Click on 'Reset IPMI' to reset IPMI to the factory default.

2.8 Firmware Update

2.8.1 Firmware Update



This wizard takes you through the process of firmware upgrades. A reset of the box will automatically follow whether the upgrade is completed or cancelled. An option to Preserve configuration will be presented. Enable the option, if you wish to preserve configured settings through the upgrade.

Enter Preserve Configuration

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

Enter Update Mode

Click 'Enter Update Mode' to upgrade the current device firmware.

2.8.2 Image Transfer Protocol

The screenshot shows a web browser window displaying the 'Image Transfer Protocol' configuration page. The page has a navigation bar at the top with links: Dashboard, FRU Information, Server Health, Configuration, Remote Control, Auto Video Recording, Maintenance, Firmware Update, Refresh, Print, and Logout. The main content area is titled 'Image Transfer Protocol' and contains the following text: 'The following option will allow to configure firmware image protocol information.' Below this text are four form 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 text input field with the value '0'). At the bottom right of the form area are two buttons: 'Save' and 'Reset'. The browser's taskbar at the bottom shows various icons and the system clock displaying '下午 03:14 2012/10/11'.

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.