



**Intel® Active System Console v8.0**

**User Guide**

**October 2015**

## Legal Statements

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS FOR THE PURPOSE OF SUPPORTING INTEL DEVELOPED SERVER BOARDS AND SYSTEMS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Intel is a trademark of Intel Corporation in the U.S. and other countries.

Microsoft, Windows, Windows Server, Active Directory, and Vista are trademarks, or registered trademarks of Microsoft Corporation in the United States and/or other countries.

\* Other names and brands may be claimed as the property of others.

Copyright © 2015 Intel Corporation. All rights reserved.

## Revision History

Description	Revision Date
<ul style="list-style-type: none"> <li>Support for Intel® Server based Greenlow Platforms</li> </ul>	April 2015
<ul style="list-style-type: none"> <li>Cache River update to 7.0 to support UEFI</li> </ul>	April 2015
Trackers EPSD100247844 ,EPSD100247850, EPSD100248104, EPSD100247843 and EPSD100028503 are fixed	May 2015
<ul style="list-style-type: none"> <li>Tracker EPSD100247847 has been fixed</li> </ul>	May 2015
<ul style="list-style-type: none"> <li>New CR 7.0 Build 4 is integrated</li> </ul>	Jun 2015
<ul style="list-style-type: none"> <li>New CR 7.0 Build 6 is integrated</li> <li>User authentication for User Id in Email Setting is fixed(hyphen “-“ issue)</li> <li>RHEL 7.1 support</li> <li>Improved First Login Time to be less than/within 1 minute 15 seconds</li> </ul>	July 2015
<ul style="list-style-type: none"> <li>Integrated CR 7.0 Build 7</li> <li>Integrated the KW fixes for Linux and Windows</li> <li>Integrated CR 7.0 Build 8</li> <li>Fixed Sol Tracker</li> </ul>	August 2015
<ul style="list-style-type: none"> <li>Redhat all versions supports</li> <li>CentOS all versions supports</li> <li>New CR Build 9 with <b>sysfwupdt</b> module added</li> </ul>	September 2015
<ul style="list-style-type: none"> <li>Code defense flags are enabled for windows</li> <li>Code defense flags are enabled for linux</li> <li>Integrated with CR build 10</li> </ul>	October 2015

# Contents

<a href="#">Legal Statements</a>	2
<b><a href="#">Contents</a></b>	<b>4</b>
<b><a href="#">1 Introduction</a></b>	<b>7</b>
<a href="#">1.1 Target Audience</a>	7
<a href="#">1.2 Overview</a>	7
<a href="#">1.3 Features and Benefits</a>	8
<a href="#">1.4 System Requirements</a>	10
<a href="#">1.4.1 Supported Operating Systems</a>	10
<a href="#">1.4.2 Browser Requirements</a>	11
<a href="#">1.4.3 Supported Platforms</a>	11
<a href="#">1.5 Supported Languages</a>	11
<a href="#">1.6 Additional Information</a>	11
<a href="#">1.6.1 Third Party Source Code/Binaries</a>	11
<a href="#">1.6.2 Support Information</a>	11
<a href="#">1.6.3 Related Documentation</a>	12
<a href="#">1.7 Terminology</a>	13
<b><a href="#">2 Getting Started</a></b>	<b>14</b>
<a href="#">2.1 Installing Intel® Active System Console</a>	14
<a href="#">2.2 TCP Information</a>	15
<a href="#">2.3 Uninstalling Intel® Active System Console</a>	15
<b><a href="#">3 Navigating Intel® Active System Console</a></b>	<b>17</b>
<a href="#">3.1 System Information</a>	19
<a href="#">3.1.1 Viewing System Health</a>	20
<a href="#">3.1.2 Viewing System Summary</a>	20
<a href="#">3.1.3 Viewing Processor Summary Readings</a>	21
<a href="#">3.1.4 Viewing Memory Device Readings</a>	22
<a href="#">3.1.5 Viewing Temperature and Fan Readings (Cooling Sensors)</a>	23
<a href="#">3.1.6 Viewing Voltage and Current Sensors Readings</a>	24

3.1.7	<a href="#">Viewing Chassis Information</a>	24
3.1.8	<a href="#">Viewing Storage Readings</a>	25
3.1.9	<a href="#">Viewing Miscellaneous Readings</a>	26
3.1.10	<a href="#">Viewing System Events</a>	26
<b>4</b>	<b><a href="#">Configuring Server Hardware and Reports Generation</a></b>	<b>29</b>
4.1	<a href="#">Configuring BMC</a>	29
4.1.1	<a href="#">Configuring BMC Users</a>	29
4.1.2	<a href="#">Configuring Network</a>	31
4.1.3	<a href="#">Configuring Serial Over Lan (SOL) Settings</a>	32
4.1.4	<a href="#">Configuring SNMP Alerts</a>	33
4.1.5	<a href="#">Configuring BIOS</a>	33
4.1.6	<a href="#">Configuring Basic Email: Use Default Email Profile</a>	34
4.1.7	<a href="#">Configuring Advanced Email: Create and Apply Email Profiles</a>	36
4.2	<a href="#">Generating Reports</a>	37
4.3	<a href="#">User Settings</a>	37
4.4	<a href="#">Viewing Software Updates</a>	37
<b>5</b>	<b><a href="#">Security Features</a></b>	<b>38</b>
5.1	<a href="#">Security Recommendations</a>	40
<b>6</b>	<b><a href="#">Troubleshooting Guidelines</a></b>	<b>41</b>

**<This page is intentionally left blank.>**

# 1.0 Introduction

The Intel® Active System Console is a simple, lightweight web application console that gives you a dashboard view of the Server hardware on which it is running. It helps you proactively monitor the health of your Server, allows remote configuration of Server, tracking of assets, alerting of any issues and generation of asset reports.

The Intel® Active System Console is a product offering from the Intel® System Management Software - a suite of software products designed to reduce the cost and time of managing servers and keep businesses running 24/7.

IASC is included with almost all Intel® Server Products at no additional charge giving your customer “peace of mind” that servers are healthy.

IASC offers the following:

- **Proactive alerting** allows the server administrator to plan routine maintenance activities and avoid unplanned downtime
- **Asset Inventory** tells you what components are installed in the server without having to shut down and open the system
- **Remote debug** isolates problems quickly saving hours and even days in the time it takes to debug and fix the issue.

## 1.1 Target Audience

The purpose of this document is to help system/server administrators install and use the Intel® Active System Console. It provides you detailed information on the features and benefits of Intel® Active System Console and how to use them. It describes the software requirements, supported operating systems, and the supported platforms. It also explains the installation and un-installation process.

## 1.2 Overview

The Intel® Active System Console helps you in proactive monitoring of the health of your Server, allows remote configuration of Server, tracking of assets, alerting of any issues and generation of asset reports. It gives you an overall view of the server hardware. This comprises information on hardware components of the system - overall health of the server and component health, sensors, System Event Log (SEL), storage (Logical Drives, Hard Drives), processors, memory, Field Replaceable Unit(FRU)s as well as BMC configuration.

## Get Peace of Mind

It improves security, reduces costs, and helps businesses move from reactive to proactive system management. The software enables secure remote management and monitoring of servers, clients, and applications from virtually any location—in a way that IT generalists can understand without attending weeks of training. It's all about IT made easy:

### Simple

- Makes it easy to set up and maintain a reliable and secure IT infrastructure
- Streamlines tasks throughout server life cycle with remote management
- Manages IT functions with a single suite of tools

### Secure

- Keeps IT informed with automated daily health reports and alerts
- Improves reliability and stability with application and patch deployment

### Smart

- Designed specifically for small to midsize business
- Reduces travel time and costs
- Provides a proactive solution to server management with reports and alerts

IASC displays the hardware sensors, Field Replaceable Unit (FRU) data, and System Event Log (SEL) for any system.

To launch the Intel® Active System Console, go to **Start> Programs> Intel® Server Management Software > Intel® Active System Console**.

You can also launch IASC from any client using the URL: <https://<ipaddressofserver>:9393/asc>

## 1.3 Features and Benefits

This section discusses the features and benefits of Intel® System Management Software suite of Products in general and the IASC in particular.

### Intel® System Management Software

The following table lists the comparative features and benefits of Intel® System Management Software suite of Products:



Features	Intel® Active System Console	Intel® SNMP-SA
Server Environment	Enterprise	Enterprise
User Interface	Web Based	Integrates into enterprise tools such as HP* OpenView
Operating System Support	Windows, Linux	Windows, Linux
Single, easy to use console	X	
Hardware Predictive Failure Analysis	X	X
Sensor readings	X	X
Hardware Event Log	X	
Hardware and Software Inventory	X (Hardware and Operating System)	
OS and Application Monitoring		
Software Patch Deployment		
Application Deployment		
Alerting	X (Email and BMC SNMP)	X (SNMP)
Reporting	X	
BMC Configuration	X	
Power Management		
Performance Views		
Remote Management	X	X
Multi Server Management		
Remote Power On/Off/Reboot		
Serial Over LAN (Console Redirection)		
OEM Customization		

### Intel® Active System Console

The Intel® Active System Console has the following features:

- Viewing System Health in the Dashboard
- Viewing Other System Information as follows:
  - Viewing System Summary
  - Viewing Processor Summary Readings
  - Viewing Memory Device Readings

- Viewing Temperature and Fan Readings (Cooling Sensors)
- Viewing Voltage and Current Sensors Readings
- Viewing Chassis Information
- Viewing Storage Readings
- Viewing Miscellaneous Readings
- Viewing System Events
- Generating Reports
- Checking for software updates

## 1.4 System Requirements

This section details the software requirements, supported operating systems and the supported platforms for the Intel® Active System Console.

### 1.4.1 Supported Operating Systems

- **Microsoft Windows Server**
  - Microsoft Windows\* Server 2012 R2 EM64T
  - Microsoft Windows\* Server 2012 Enterprise
- **Red Hat\* Enterprise Linux (RHEL)**
  - Red Hat\* Enterprise Linux 6.5 32-bit & EM64T
  - Red Hat\* Enterprise Linux 7.0 EM64T
  - Red Hat\* Enterprise Linux 7.1 EM64T
- **SUSE\* Linux Enterprise Server (SLES)**
  - SUSE\* Linux Enterprise Server 11 SP4 (x86/x64)
  - SUSE\* Linux Enterprise Server 12 SP0 (x64)

**Important Note:**

- a) OS without GUI (Graphical User Interface) is not supported.
- b) For Red Hat OS version, before installing the IASC execute RHELx86\_64AUTO.sh script (> sh RHELx86\_64AUTO.sh) with OS DVD in the DVD for installing the dependent package for IASC.

## 1.4.2 Browser Requirements

The application has been tested to run on Microsoft\* Internet Explorer 7.x or later and Mozilla Firefox\* 3.6 or later versions. It is best viewed in screen resolution from 1024 X 768 to 1440 X 900.

## 1.4.3 Supported Platforms

Intel® Server Board S1200SP

For the latest and up-to-date list of supported operating systems, system requirements and platforms supported refer to the release notes available with the product.

## 1.5 Supported Languages

English only

## 1.6 Additional Information

This section lists additional IASC related information that will help you use it appropriately.

### 1.6.1 Third Party Source Code/Binaries

Link to third party source code/binaries:

<http://support.intel.com/support/motherboards/server/sysmgmt/sb/CS-031025.htm>

### 1.6.2 Support Information

If you encounter an issue with your server platform or management software, please follow these steps to obtain support on your product.

1. Get connected to our [support web page](#) for 24x7 support when you need it to get the latest and most complete technical support information on all Intel® Enterprise Server, Storage Platforms and Management Software. Information available at the support site includes:

- [Latest BIOS, firmware, drivers and utilities](#) available through Intel's download center.
- Product documentation and flash demos, installation and quick start guides
- Full product specifications, technical advisories and errata
- Compatibility documentation for memory, hardware add-in cards, chassis support matrix, and operating systems
- [Server and chassis accessory parts list](#) for ordering upgrades or spare parts

- A searchable knowledgebase to search for product information throughout the support site

2. Utilize the [community forums](#) or [chat with a live person](#).

3. You can also contact an Intel support representative using one of the [following support phone numbers](#). Charges may apply. Intel customer support suggests running the Intel® System Information Tool (depending on the operating system being used) for [Microsoft Windows\\*](#), [Linux\\*](#) or [EFI\\*](#) to extract relevant data that pertains to the issue being encountered and provide the information when asked by a support agent.

Intel now offers Channel Program members round-the-clock [24x7 technical phone support](#) on Intel® server boards, server chassis, server RAID controller cards, and Intel® Server Management.

### Warranty Information

Connect to Intel's website to obtain [warranty information](#).

*NOTE: Requires Login to the Reseller Site to obtain the 24x7 Number.*

## 1.6.3 Related Documentation

The following table lists the related documentation:

Document/ Information	Source
Intel® Active system Console Release Notes	Available at the same package

## 1.7 Terminology

The following table lists the terminology used in this document and the description:

<b>Term</b>	<b>Description</b>
BMC	Baseboard Management Controller
CIM	DMTFs Common Information Model - CIM provides a common definition of management information for systems, networks, applications and services, and allows for vendor extensions
GUI	Graphical User Interface
Intel® SMS	Intel® System Management Software
IPMI	Intelligent Platform Management Interface. Operates independent of the operating system (OS) and allows you to manage a system remotely even in the absence of the OS
RMCP	Remote Management Control Protocol – Protocol used by IPMI for communicating over LAN
SEL	System Event Log
SMBIOS	System Management BIOS (SMBIOS) is specification to lay out data structures (and access methods) in a <a href="#">BIOS</a> which allows a user or application to store and retrieve information specifically about the Server
SNMP	Simple Network Management Protocol
SOL	Serial Over LAN
Upgrade	Enhanced versions of Intel® SMS with new platform support or new features are uploaded to Intel Website. Users installing Intel® SMS from a CD can upgrade to a new version using multiple ways. Intel recommends all users to upgrade to a new versions

## 2.0 Getting Started

This section provides information on how to install and use the Intel® Active System Console.

### 2.1 Installing Intel® Active System Console

#### For Linux\*

To install the software, run with root privilege.

- Get the zip package and unzip to a folder

```
cd Linux/<OS_NAME> [RHEL5 | RHEL6 | RHEL7 | SUSE10 | SUSE11 | SUSE12]
```

- Run the following command to untar the package

```
tar -xvf [ASC package name]
```

- After untar ASC package following folder will appear

```
/ASC and /common
```

- Then run the following commands.

```
*cd ASC  
*./install
```

#### For Microsoft Windows\*

- Insert Intel® Server Deployment and Management media, go to System Management Software Tab or user can browse ASC package folder and start the ASC installation main interface manually.
- Click on the “Click to Install” button for Intel® Active System Console Install. This will take you to the prerequisite Page, choose “Install Software” if enabled. Then, once the prerequisite software is installed click the “Continue Installation” button.

#### Notes:

- *While installing, user will be asked to change the default password of “admin”.*

*We recommend you set a strong password for “admin” (for example, use a combination of letters, numbers, or keyboard characters not defined as letters or numerals such as ` - \_ = + ! ~ # @ \$ \* : ; . , ? & ^ )*

- *The IASC installed in the server also serves as an MSM agent monitoring this server.*

## 2.2 TCP Information

The following TCP ports are used by Intel® Active System Console.

Port #	Description	Firewall Exception Required
7777	Use for discovery and management by Intel® Multi Server Manager (MSM).	Yes **
9393	Use for web server hosting	Yes ***
4369	Use for socket based IPC on the software backend.	No
9191	Use for lighttpd web service.	No
521	Use for lighttpd web service / PHP CGI.	No

### Notes:

\*\* 7777 is required to add on the firewall approval list only when used to manage IASC with Intel® Multi-Server Manager.

\*\*\* 9393 is required to add on the firewall approval list if accessing IASC remotely over the network with a supported web browser.

Refer to **Chapter 5** for more security features.

## 2.3 Uninstalling Intel® Active System Console

To uninstall, run the following:

### Linux\* -

```
cd /usr/local/asc/bin/
```

```
“sh uninstall”
```

**Windows\*** - You can uninstall ASC from Windows either

- from Add/Remove Program options
- from Start Menu->All Programs->Intel->Uninstall Intel® Active System Console

You will be asked to reboot the server to complete installation. You can either reboot immediately or postpone it. All files and registry entries will be completely removed only on reboot.

**Note:** The database will also be removed on uninstallation. If you want the database for any further storage make sure you copy the database SMS.db to appropriate location before uninstall.

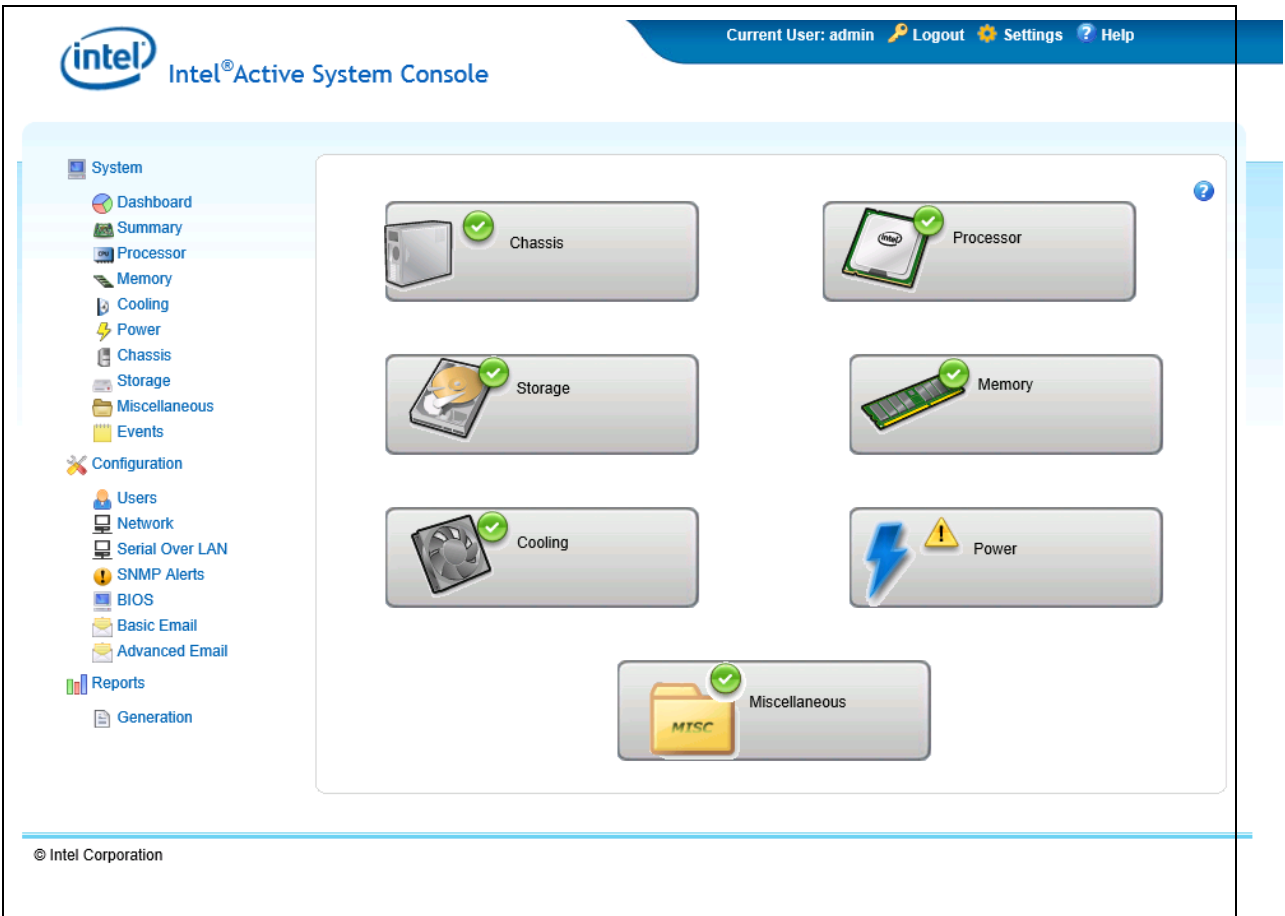
- /usr/local/asc/bin/SMS.db (in Linux\*)

- *C:\Program Files\Intel\ASC\SMS.db (in Windows\* 32 bit)*
- *C:\Program Files (x86)\Intel\ASC\SMS.db (in Windows\* 64 bit)*



# 3.0 Navigating Intel® Active System Console

This section details how you can navigate the Intel® Active System Console to use its features. By default, the Intel® Active System Console opens in the **System>Dashboard** view displaying overall server health as shown in Figure 1.



**Figure 1. Intel® Active System Console Login page (By default, IASC opens in Dashboard page)**

The left side Navigation menu comprises buttons that have submenu items.

For a quick overview of the tasks performed by these buttons and their sub menu items see following Table:

Menu Button	Submenu	Task
<b>System</b>		
	Dashboard	Displays aggregate of the system health in the Dashboard (chassis, storage, cooling, processor, memory, and power).
	Summary	Displays a table of all hardware sensors and the threshold settings.
	Processor	Displays processor details and speed information.
	Memory	Displays memory size and type information.
	Cooling	Displays all System/Processor fans. It shows the current health status of the fan and the current reading of the fan in RPM.
	Power	Displays all Voltage and Current sensors. It shows the current health status and the current reading of the Voltage and Current sensors.
	Chassis	Displays the state of the chassis intrusion sensor and enables identifying the system by turning on/off the Chassis ID LED
	Storage	Displays information about the hard disk drives, logical disk drives, and media or DVD drives.
	Miscellaneous	Lists out all the Sensors which are not categorized under any of the main sensors.  These include some BIOS and other discrete sensors.
	Events	Lists all the server event logs.
<b>Configuration</b>		
<b>BMC</b>	Baseboard Management Controller. Has the following submenu buttons: Manages the interface between system management software and platform hardware.	
	Users	Helps you add/delete/edit a BMC User.
	Network	Lists all the Network present on the motherboard.
	Serial Over Lan	SOL. Settings help change the Baud rate of the system.
	SNMP Alerts	Help send SNMP based alerts to the target server ( fan failure, memory error, etc.

	BIOS	BIOS settings.
<b>Basic Email</b>		Simple mail configuration that sends all server alerts to mail server.
<b>Advanced Email</b>		Helps configure user specific Email alerts. Feature-rich customized user settings available.
<b>Reports</b>		
<b>Generation</b>		Helps generate reports on many categories. For example, Asset Information, All System Events, Critical Events, Sensor Values ,and BMC Settings. The file can be exported either in XML, HTML, or CSV format.

## 3.1 System Information

This section lists the Hardware choices available shown in Figure 1.

The Hardware choices and their functions are listed in the following Table:

Hardware choice	Function
<b>System</b> - Displays system health information.	
Dashboard	Default IASC view. Displays chassis, Processor, Storage, Memory, Cooling, Power, and other Miscellaneous information in a convenient dashboard view.
Summary	Displays a table of all hardware sensors and the threshold settings.
Processor	Displays processor details and speed information.
Memory	Displays memory size and type information.
Cooling	Displays all System/Processor fans. It shows the current health status of the fan and the current reading of the fan in RPM.
Power	Displays all Voltage and Current sensors. It shows the current health status and the current reading of the Voltage and Current sensors.
Chassis	Displays the state of the chassis intrusion sensor and enables identifying the system by turning on/off the Chassis ID LED.
Storage	Displays information about the hard disk drives, logical disk drives, and media or DVD drives.
Miscellaneous	Lists out all the Sensors which are not categorized under any of the main sensors. These include some BIOS and other discrete sensors
Events	Lists all the server event logs.

### 3.1.1 Viewing System Health

The **System** page as shown in Figure 1 displays the health of the system and its components. The UI gets refreshed every 10 minutes.

### 3.1.2 Viewing System Summary

To view information on the board, BIOS, and Firmware, in the **System** page, click the **Summary** button to display System Summary, FRU data, and Power Supply as shown in Figure 2.

System Summary	
Property	Value
System Name	WIN-4QPQRIBE804
Asset Tag	.....
BIOS Version	SE5C610.86B.01.01.0533
System GUID	FFFFFFFFFFFFFFFF FFFF
Manufacturer	Intel Corporation
Platform ID	S2600WTT
SDR Version	SDR Package 0.11
BMC Version	0.22.6105
HSC Version	1.09
Serial Number	.....
Operating System Name	Microsoft (build 9200), 64-bit
Operating System / Kernel Version	6.2.9200
Operating System Build	9200

FRU Data						
Device Name	Model Number	ID	Manufacturer	Part Number	Serial	Version
Baseboard	S2600WTT	0	Intel Corporation	.....	.....	.....
Front Panel	NOT_AVAILABLE	4	Intel Corporation	G10279-402	QSBT32406558	NOT_AVAILABLE
HS Backplane 1	NOT_AVAILABLE	5	Intel Corporation	G43186-150	QSRU22002945	NOT_AVAILABLE
Pwr Supply 1 FRU	DPS-750XB A	2	DELTA	E98791-007	E98791D1227...	02
Pwr Supply 2 FRU	DPS-750XB A	3	DELTA	E98791-007	E98791D1311...	02

Power Supply			
Health	Name	Current Reading (Watts)	Upper Critical (Watts)
✔	PS1 Input Power	80.000000	920.000000
✔	PS2 Input Power	0.000000	920.000000
✔	System Airflow	14.000000	NOT SUPPORTED

**Figure 2. System Summary page**

**System Summary:**

- System Name: Computer name given to a server.
- Asset Tag: Name given to a server for easy server asset tracking such as hardware and software configuration information during server deployment.
- BIOS version details: Current values obtained from server.
- System GUID value: Global Unique Identifier for each system on the network.

- Manufacture, Platform ID and Serial Number: Details of server baseboard manufacture, product name and serial number.
- SDR (Sensor Data Recorded) Package version, BMC (Baseboard Management Controller) and HSC (Hot Swap Backplane) version.
- Operating System Name, Kernal Version and Version Build.

**FRU Data:**

Display entire FRU for server baseboard, chassis board, PDB (Power Distribution Board) and Power Supply unit.

**Power Supply:**

Display system sensor type code for “Other Units Based” threshold sensors.

### 3.1.3 Viewing Processor Summary Readings

To view the processor summary readings, click **System** -> **Processor** to display processor summary, processor configuration, and discrete sensor readings shown as follows:

Processor Summary									
Description	Current Speed(MHz)	Socket	Cores						
[-] Genuine Intel(R) CPU @ 2.20GHz	2200	CPU1	14						
<table border="1"> <thead> <tr> <th>L1 Cache</th> <th>L2 Cache</th> <th>L3 Cache</th> </tr> </thead> <tbody> <tr> <td>896 KB</td> <td>3584 KB</td> <td>35840 KB</td> </tr> </tbody> </table>				L1 Cache	L2 Cache	L3 Cache	896 KB	3584 KB	35840 KB
L1 Cache	L2 Cache	L3 Cache							
896 KB	3584 KB	35840 KB							
[+] Not Populated	-	CPU2	-						

Processor Configuration	Value
MLC Spatial Prefetcher	Enabled
Active Processor Cores	All
Intel(R) TXT	Disabled
DCU Data Prefetcher	Enabled
DCU Instruction Prefetcher	Enabled
Direct Cache Access DCA	Enable
Execute Disable Bit	Enabled
MLC Streamer	Enabled
Intel(R) Virtualization Technology	Disabled
Intel(R) Hyper Threading Tech	Enabled

Discrete Sensor		
Health	Name	VALUE
	CPU Missing	STATE_DEASSERTED
	CATERR	STATE_DEASSERTED
	CPU ERR2	STATE_DEASSERTED
	P1 Status	PROCESSOR_PRESENCE_DETECTED

**Figure 3 – Processor Summary Readings**

**NOTE:**

IASC get the L1, L2 & L3 Cache from SMBIOS table Type 7. In this case, by pressing "F2" BIOS

show L1, L2 & L3 Cache difference from IASC. Because in BIOS setup, the cache size is for per core instead of socket, but in SMBIOS Type 7, the cache size is for socket instead of per core. Example show in above picture:

IASC:

L1 = 896KB (64KB X 14 (cores))

L2 = 3584KB (256KB X 14 (cores))

L3 = 35840KB

BIOS:

L1 = 64KB

L2 = 256KB

L3 = 35840KB

### 3.1.4 Viewing Memory Device Readings

To view the processor memory device readings, click **System** -> **Memory** to display memory device details and discrete sensor readings shown as follows:

Memory Device				
Health	Slot Name	Size(MB)	Speed(MHz)	Type
✔	DIMM_A1	1024	1067	DDR3
-	DIMM_A2	-	-	-
-	DIMM_A3	-	-	-
✔	DIMM_B1	1024	1067	DDR3
-	DIMM_B2	-	-	-
-	DIMM_B3	-	-	-

Discrete Sensor	
Health	Name
-	Mmry ECC Sensor

**Figure 4 – Memory Device Readings**

Displays the health of each populate memory module. It lists the entire memory bank supported in the Server. If a memory module is populated in the memory slot, it will list the corresponding size, speed, and type of module. If the slot is not populated, then it will list as not populated.

### 3.1.5 Viewing Temperature and Fan Readings (Cooling Sensors)

To view the temperature and fan readings, click **System** -> **Cooling** to display the Cooling Sensors page shown as follows:

Temperature			
	Health	Name	Current Reading(Deg Celsius)
		P1 Therm Margin	-71
		P1 Therm Ctrl %	0
		Baseboard Temp	30
		P1 Mem Margin	0

Fan			
	Health	Name	Current Reading(RPM)
		System Fan 2	1,620
		System Fan 3	1,566

Discrete Sensor		
Health	Name	Current Reading
	CPU Therm Trip	STATE_DEASSERTED

**Figure 5 - Cooling Sensors**

Display all System threshold temperature and fans, display discrete temperature sensors. It shows the current health status of the fan and the current reading of the fan in RPM. Click on any of the System threshold temperature and fans to view the upper and lower threshold details.

### 3.1.6 Viewing Voltage and Current Sensors Readings

To view the voltage and current readings, click **System** -> **Power** to display the Voltage and Current Sensors page shown as follows:

Voltage			
Health	Name	Current Reading(Volts)	
[-]	BB +12.0V	12.10	
		Lower Critical	Lower Warning
		10.616000	11.001000
		Upper Warning	Upper Critical
		13.311000	13.696000
[+]	BB +3.3V Vbat	3.10	

Current			
Health	Name	Current Reading(Amps)	
[-]	PS1 Curr Out %	8.00	
		Lower Critical	Lower Warning
		NOT SUPPORTED	NOT SUPPORTED
		Upper Warning	Upper Critical
		100.000000	112.000000

Discrete Sensor		
Health	Name	Current Reading
	Voltage Fault	STATE_ASSERTED
	VR Watchdog	STATE_DEASSERTED
	Pwr Unit Status	ALL_DEASSERTED
	PS1 Status	PRESENCE_DETECTED

**Figure 6. Power Sensors**

Lists all the current reading of the voltage sensors present on the base board. The details of each voltage sensor list the upper/lower critical and warning values.

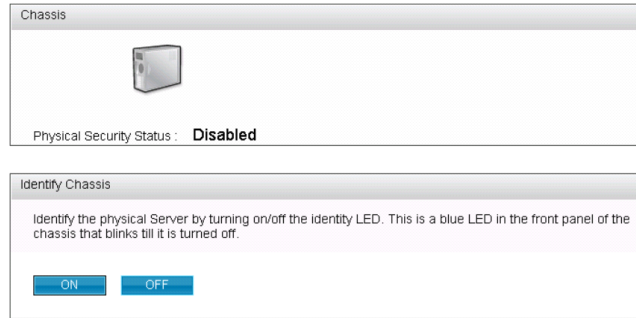
### 3.1.7 Viewing Chassis Information

To view chassis status, click **System** -> **Chassis** to display shown in following figure. The user can also identify the server by turning the LED on or off. To do this, click the 'ON' / 'Off' button.



**Notes:**

- For systems that do not support the chassis sensor, **The system LED is currently Not Supported** status is displayed.
- For some platforms, the status of LED is not supported, but the user will still be able to turn the LED on and off as shown in Figure 7.



**Figure 7 – Chassis Information page/ Identify Chassis On/Off Dialog**

Display physical security status of the chassis. Also helps identify chassis (physical Server) by turning the blue LED in the front panel of the chassis on/off (LED blinks till it is turned off).

### 3.1.8 Viewing Storage Readings

To view the temperature and fan readings, click **System** -> **Storage** to display the Storage Sensors page as shown in following figure.

Storage device			
Model	Name	Serial Number	Total Space
BT380815A8	/dev/sda	9QZ39VQW	80.00 GB

Logical Drives		
Name	Total Space	Free Space
/	72.39 GB	65.01 GB
/dev	0.96 GB	0.96 GB
/boot	0.47 GB	0.42 GB

Drive Sensor		
Health	Name	VALUE
No sensors found.		

**Figure 8 – Storage Device, Logical Drives, Drive Sensor Information page**

- **Storage Device.** The Storage page lists out all the Storage drives present in the server. Each drive name includes the Model Number, device name serial number and the total Hard Disk capacity.
- **Logical Drive.** Each correctly mounted logical drive is listed including it total and free space.

- **Drive Sensor.** The Drive Status and the Drive Presence sensors are displayed for each drive slot. These indicate the corresponding Hard drive presence or absence status.

*A warning alert gets generated in the Events page if the Hard disk space crosses the threshold of 75% and a Critical alert is generated if it crosses the 90% margin.*

### 3.1.9 Viewing Miscellaneous Readings

This section lists out all the Sensors which are not categorized under any of the main pages. These include some BIOS and other discrete sensors. It lists the name of the Bus Sensors and shows the corresponding health along with the values.

Bus Sensor		
Health	Name	VALUE

**Figure 9. Miscellaneous Information page (Bus Sensors, BIOS and other discrete sensors)**

### 3.1.10 Viewing System Events

This page lists all the server events as follows:

State	Date:time	Description	Severity	State	Sensor Type
<input type="checkbox"/>	2010-03-29 12:44:25	User "admin" logged in from 10...	Informational	Open	Security
<input type="checkbox"/>	2010-03-29 12:41:49	System Event sensor 131 repor... occurred.	Informational	Open	System Event
<input type="checkbox"/>	2010-03-29 12:41:49	System Event sensor 255 repor... alert.	Informational	Open	System Event
<input type="checkbox"/>	2010-03-29 12:40:35	System Event sensor 131 reports Timestamp Clock Sync. Event is second of two expected events from BIOS on every power on.	Informational	Open	System Event
<input type="checkbox"/>	2010-03-29 12:40:11	System Event sensor 131 reports Timestamp Clock Sync. Event is first of two expected events from BIOS on every power on.	Informational	Open	System Event
<input type="checkbox"/>	2010-03-29 11:30:06	User "admin" logged in from 10.223.52.3	Informational	Open	Security
<input type="checkbox"/>	2010-03-29 11:03:45	User "admin" logged in from 10.223.52.3	Informational	Open	Security
<input type="checkbox"/>	2010-03-25 13:58:18	User "admin" logged in from 127.0.0.1	Informational	Open	Security
<input type="checkbox"/>	2010-03-25 13:56:55	User "admin" logged in from unknown client	Informational	Open	Security
<input type="checkbox"/>	2010-03-25 13:56:55	User admin logged off	Informational	Open	Security
<input type="checkbox"/>	2010-03-25	System Event sensor 131 reports a system boot event has	Informational	Open	System Event

**Figure 10 – System Events Information page**

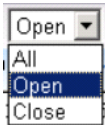
The description, severity, status of events (open or closed) and time stamp for each of the events is listed.

The top row heading shows a list of filters and actions that can be taken on the table. There are filters for State, Severity and Module Type. If a particular value in filter is selected, only events belonging to that filter value appears in the table.



- **Severity filter.** Use for viewing only critical/warning/informational events. The column headings follow the filters and actions. The entire table can be sorted based on each column.

To sort the table based on a column click on column heading. First click on the column sorts it in ascending (lexicographic) order. Any further clicks, the order toggles between ascending and descending.



- **Open Status.** If in open state, check for event description. If critical event, take immediate corrective action.

## Actions

Two sets of actions can be performed on events.

- **Delete Events.** All the events listed in the table can be deleted from database. Here again, two options are available:

Delete all events from Database. Here the events are deleted from ASC database. This include all open and closed Server Events as well as Application Events.

Delete all events from Baseboard Management Controller (BMC). Here the Server Events are deleted from BMC SEL store.

### **Notes:**

You cannot selectively delete events from either database or BMC. Either all events or none are deleted.

If you delete from database, it cannot be recovered. So, backup event logs by exporting Reports. Also a refresh for new events information will not display anything until after ~5-6 mins.

- **Close Selected.** Update the status of events to close. Based on the type of events two results are observed. If the event is regular events, close will just update the status to close. If any active events are appearing in bottom scroll log, that will be gone. If the event

contributes to Server health, displayed as "Open \*" in the Status column, closing the event causes the IASC to ignore the event and re-compute the health of the component. This may cause the health of the Server from being critical to go to healthy state in IASC (if the event that closed is the only one causing the critical state).

For instance "memory ...."

## 4.0 Configuring Server Hardware and Reports Generation

This section explains configuring the server hardware using IASC. It details the options available in the Configuration feature of the Intel® Active System Console. Click **Configuration** button to access the menu with the configuration options on Baseboard Management Controller as follows:

**Note:** Only users with ADMIN privilege can configure a Server using ASC.

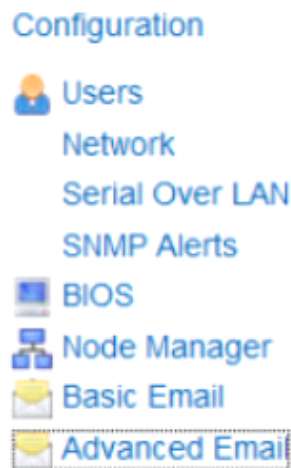


Figure 11 – Configuration Menu

### 4.1 Configuring BMC

This section explains configuring the BMC. It details the options available in the BMC Configuration feature of the Intel® Active System Console. The BMC Configuration window has the choices listed in Figure 11.

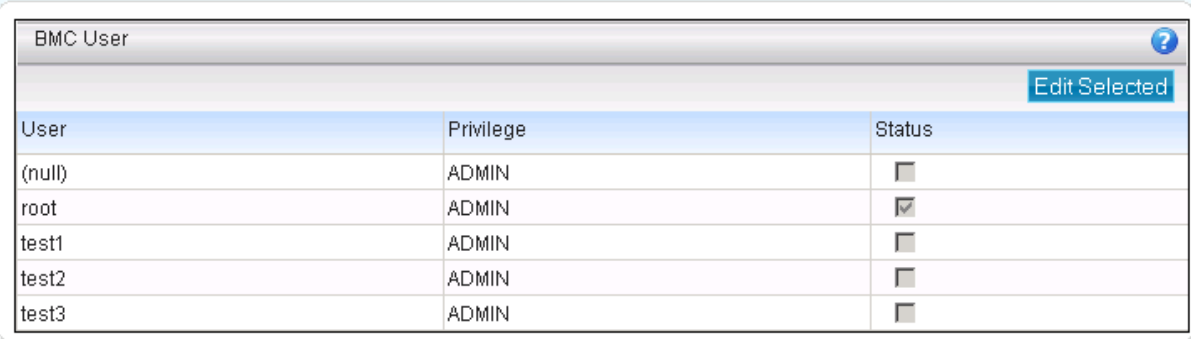
#### 4.1.1 Configuring BMC Users

The BMC User Configuration section helps you edit a BMC User. While doing so, you can set the privilege level as Administrator, Operator, or User.

Baseboard Management Controller supports authentication and authorization for remote access (out-of-band access). Users have to configure a BMC Username and password to access BMC in out-of-band fashion

You can also enable or disable the User.

In the left navigation pane, click the **Configuration>Users** button to view the BMC User window as shown in Figure 12.

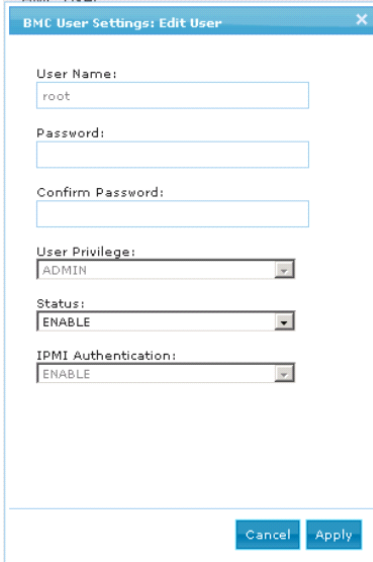


The screenshot shows a window titled "BMC User" with a table of users. The table has three columns: "User", "Privilege", and "Status". The "Status" column contains checkboxes. A blue button labeled "Edit Selected" is located in the top right corner of the table area.

User	Privilege	Status
(null)	ADMIN	<input type="checkbox"/>
root	ADMIN	<input checked="" type="checkbox"/>
test1	ADMIN	<input type="checkbox"/>
test2	ADMIN	<input type="checkbox"/>
test3	ADMIN	<input type="checkbox"/>

**Figure 12. Intel® Active System Console BMC User Configuration window**

You can enable or disable the User by clicking **Edit Selected** to display the following dialog:



The dialog box is titled "BMC User Settings: Edit User". It contains the following fields and controls:


- User Name:
- Password:
- Confirm Password:
- User Privilege:  (dropdown menu)
- Status:  (dropdown menu)
- IPMI Authentication:  (dropdown menu)

At the bottom right, there are two buttons: "Cancel" and "Apply".

**Figure 13. Configuring BMC User Settings: Edit User dialog**

## 4.1.2 Configuring Network

Click the **Configuration>Network**.



Network	Enable	IP Address	Gateway
1	<input checked="" type="checkbox"/>	10.223.132.53	10.223.132.62
3	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0

**Figure 14. Configuring BMC Network Window**

This page lists all the networks present on the motherboard. This indicates the LAN channels over which a baseboard controller (BMC) can be reached out-of-band.

To enable, check the enable box.

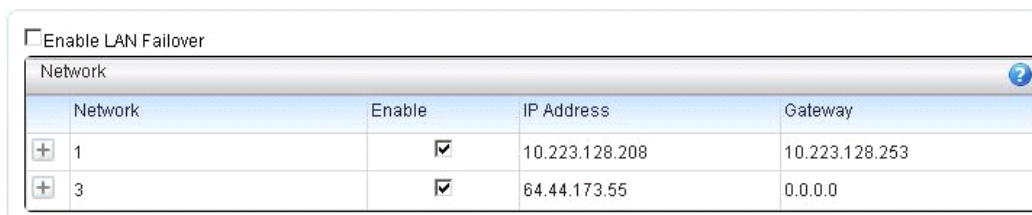
- To edit the settings, select the network channel and then choose either static or DHCP IP address.
- If you are choosing the option "IP address from a DHCP server" then you must have a DHCP Server present in your network environment for the server to obtain an IP address automatically.
  - User Privilege can be either set to Admin, User, or Operator.
  - Admin user privilege configuration is needed for read, execute, and write privileges.

**Note:** These are not Operating System IP Addresses.

### LAN Failover

BMC FW provides the LAN Failover capability such that the failure of the system HW associated with one LAN link will result in traffic being routed to an alternate link.

Intel<sup>®</sup> Active System Console enables LAN FAILOVER feature dynamically on the supported platform. On enabling LAN FAILOVER, only LAN Channel No. 1 will be allowed for configuration. Other active LAN channel shares the same configuration when the network connection of LAN channel 1 is broken.



Network	Enable	IP Address	Gateway
1	<input checked="" type="checkbox"/>	10.223.128.208	10.223.128.253
3	<input checked="" type="checkbox"/>	64.44.173.55	0.0.0.0

**Figure 155. Configuring LAN FAIL Over**

**Note:**

This feature is supported only on Intel<sup>®</sup> Xeon<sup>®</sup> Process E5 family based platforms. For more details on LAN Failover feature, refer Motherboard TPS.

### 4.1.3 Configuring Serial Over Lan (SOL) Settings

Base-board controller supports re-direction of Server boot sequence video console over LAN channel. Users can see the entire screen output of boot sequence and control it using keyboard simulating actual Server control. This console is lost once the operating system boots up. This feature is known as Serial-over-LAN.

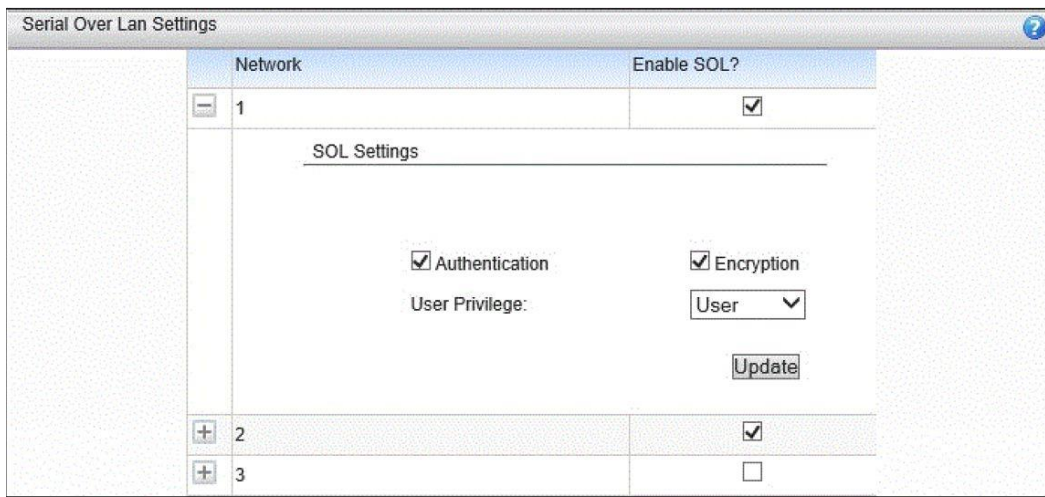
Using ASC you can enable/disable or edit Serial-Over-LAN settings in base-board controller.

To change SOL settings, select LAN channel -> select baud rate -> select privilege level -> click **Update**.

You can enable authentication in which case only users with valid username and password can do SOL console redirection.

You can enable encryption in which case the entire SOL traffic will be encrypted and protected from network snooping.

Click **Configuration>Serial Over Lan** to display the **Serial Over Lan** window as shown in following figure:



**Figure16. Configuring SOL Settings Window**

**Note:**

Configuring Baud Rate will not be supported on Intel® Xeon® E5, E5 V2, E5 V3 Process based platforms and the Baud Rate will be shown as “NOT\_AVAILABLE”. For more details, refer Motherboard TPS.



## 4.1.4 Configuring SNMP Alerts

SNMP Alerts help send SNMP -based alerts to the target server. Alerts include fan failure, memory error, and so on.

If you want base-board controller to send alerts about any change in Server hardware in the form of SNMP Traps to any SNMP Manager you can set it up using Active System Console.

SNMP Alerts help send SNMP Traps to the target server. Alerts include fan failure, memory error, and so on. Click **Configuration>SNMP Alerts** to display the SNMP Alerts settings window as shown in following figure:

Events for which SNMP Traps are generated:	
Temperature Sensor Out of Range	Voltage Sensor Out of Range
Chassis intrusion (security violation)	Fan Failure
Power Supply Failure	BIOS: Post Error Code
System restart (reboot)	Watchdog Timer
Fatal NMI	Memory Error
FRB Failure	Node Manager

Traps are sent to:
IP Address: <input type="text" value="10"/> . <input type="text" value="223"/> . <input type="text" value="132"/> . <input type="text" value="39"/>

**Figure17. Configuring SNMP Alerts Settings Window**

To set an alert, enter the IP address of target SNMP Manager or trap receiver -> click **Apply**.

## 4.1.5 Configuring BIOS

Click **Configuration>BIOS** to display the BIOS settings window as shown in the following figure:

Boot Order
1 IBA GE Slot 00C8 v1335
2 Internal EFI Shell
3 SATA Port 0 Hard Disk

---

Power Action

When power is restored after a power failure

Stay Powered Off

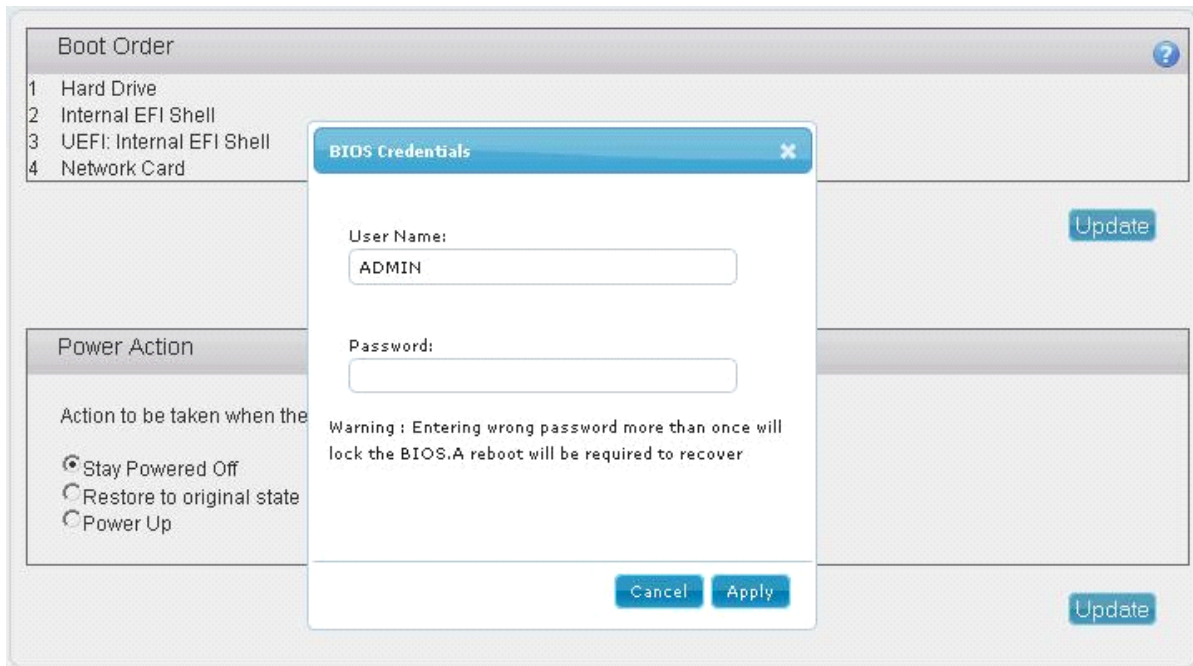
Restore previous power state

Power Up

**Figure 18. Configuring BIOS Window**

**Set Boot Order.** Helps select system boot order - Hard Disk, DVD, Network, and so on - for the next reboot cycle. Select desired boot order -> click **Update**.

When Admin Password is set on the BIOS, user will be prompted as shown in the below image to enter the BIOS Admin password to update the boot order change. This feature is supported only on Romley.



**Figure 169. BIOS Admin Credentials for Boot Order**

**Power Action.** Helps set power action in case of power breakdown. You have the option to choose one of the following:

- Stay powered off. Server remains in a powered off state even if the power is restored back.
- Restore to Original State. Server will either get powered up or it will remain in an Off state depending on previous power state during the power breakdown.
- Power Up. Server powers up when the power is restored back.

### 4.1.6 Configuring Basic Email: Use Default Email Profile

Email Alerting helps you receive Server Health Alert messages. For this, you must first configure your mail settings either through Basic Email settings or through Advanced Email settings.

Click **Configuration>Basic Email** to display the Email Alerts Settings window as shown in following figure:

Email Alert Settings

Select Email Policy:  All Events (Default - 1)  Critical Events Only (Default - 2)

Mail Server Address:

User ID:

Password:

Receipient Email ID:

Apply

**Figure 21. Basic Email Alerts Settings Window**

Email Alerting helps you receive Server Health Alert messages. For this, you must first configure your mail settings either through Basic Email page or through Advanced Email.

For configuring Basic Email settings, you must have a mail server in your network environment. If not present, you must setup a mail server to use this feature.

- Select Default -1 profile to receive all Hardware alerts that include critical, warning, and informational.

OR

- Select Default-2 profile to get only the critical Hardware events alert.

Enter the mail server IP address, its hostname and then enter the **To** Email address to which the alert has to be sent. Click **Apply** to set the basic Email alert setting.

## 4.1.7 Configuring Advanced Email: Create and Apply Email Profiles

Click **Configuration>Advanced Email** to display the advanced **Email Alerts Settings** window as shown in following figure:

The screenshot shows the 'Email Alert Settings: Create New Policy' window. It features a blue header bar with the title. Below the header, there are several input fields for configuration: 'Email Alert Policy', 'Mail Server Address', 'User ID', 'Password', 'Status' (a dropdown menu currently set to 'ENABLE'), 'From Address', 'Receipient Email ID', and 'Subject'. At the bottom right of the form area, there are 'Apply' and 'Cancel' buttons. Below the form fields is an 'Alerts' section with 'Select All' and 'Clear All' buttons. The 'Alerts' section contains a list of alert categories with checkboxes: Application, Memory, Peripheral Components, Processor, Configuration Alerts, Misc, Power, Security, Cooling, OS Boot Events, and Power State. All checkboxes are checked.

**Figure 22. Advanced Email Alerts Settings Window**

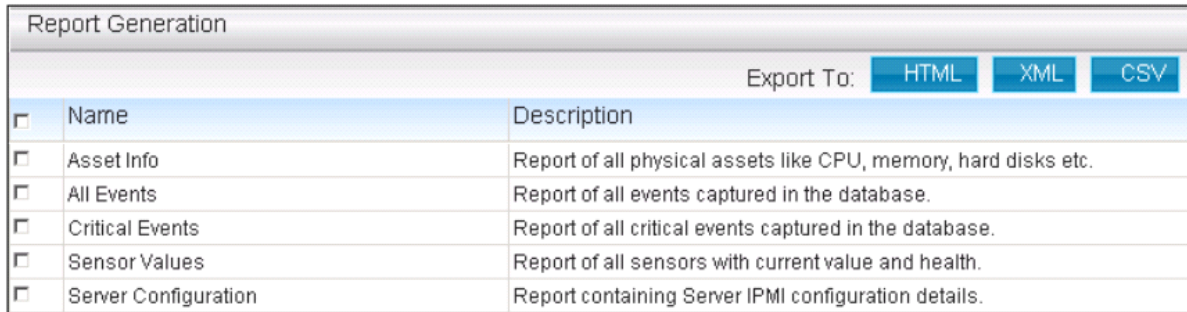
Advanced Email Settings is rich in customized user settings. To create an advanced Email, do the following:

- Enter the following:
    - Profile name
    - Mail server IP address. If a mail server is not present, then you need to set one up to use this feature.
    - From address of the Email
    - One/multiple "To" address/s
    - Subject line. For example, Chassis Intrusion Detected
    - Specific comments
  - Next, in the Alerts pane
    - Click **Select** all to select all the alerts (Select **Clear All** to deselect all as needed)
- OR
- Select only specific alerts based on your need.
- Next, click **Apply** to apply the settings.

To create another advanced Email, create a separate profile in step1 and then follow the same procedure.

## 4.2 Generating Reports

This option helps you generate reports on categories such as Asset Information, All System Events, Critical Events, Sensor Values, and BMC Settings. Click **Reports>Generation** to display the **Report Generation** window as shown in following figure:



Report Generation	
Export To: <span>HTML</span> <span>XML</span> <span>CSV</span>	
<input type="checkbox"/> Name	Description
<input type="checkbox"/> Asset Info	Report of all physical assets like CPU, memory, hard disks etc.
<input type="checkbox"/> All Events	Report of all events captured in the database.
<input type="checkbox"/> Critical Events	Report of all critical events captured in the database.
<input type="checkbox"/> Sensor Values	Report of all sensors with current value and health.
<input type="checkbox"/> Server Configuration	Report containing Server IPMI configuration details.

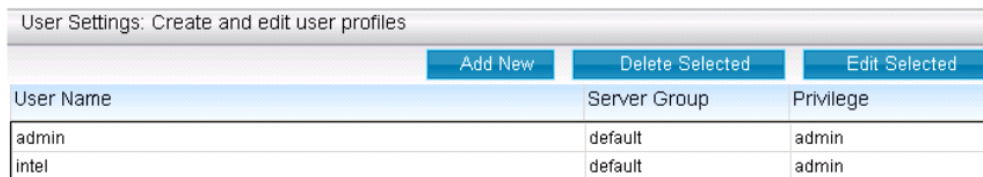
**Figure 23. Generating Reports Window**

The file can be exported either in HTML, XML, or CSV format.

## 4.3 User Settings

A User setting icon is provided on the main IASC page on the top corner right hand side.

Clicking on the setting icon will open the user setting page. Here, new users can be added or existing user privilege can be edited or users can be deleted.



User Settings: Create and edit user profiles		
Add New <span>Delete Selected</span> <span>Edit Selected</span>		
User Name	Server Group	Privilege
admin	default	admin
intel	default	admin

**Figure 24. User Settings Window**

## 4.4 Viewing Software Updates

This feature is no longer supported.

## 5.0 Security Features

The Intel® Active System Console offers multiple security features as protection against unauthorized access to the application.

- It supports role-based multiple user authentication as follows:
  - ADMIN. Users with administrator privileges. Default Administrator user is admin. Only admin can create new users and assign privileges. Any user can, however, change password.
  - USER. Users with read-only privileges. Configuration changes using the application not permitted.
- IASC supports SSL based data encryption to securely communicate between client and application
- Secure Socket Layer allows two communicating devices to encrypt data using a public certificate and private key.
- The certificate used in IASC is a self-signed one to reduce the cost of deployment. All modern browsers will detect self-signed certificate and give a warning that the “certificate is invalid” since the authority that signed the certificate is not a publicly acknowledged authority. However, Users can override the warning and accept the certificate. You should do this only if you are sure that the certificate is originated from the application itself (by making sure you first launch the application from a trusted network and add the certificate to the trusted list). Once a certificate is accepted, the warning goes away as long as you launch the application from the same client.

Customers having a valid certificate from a public CA can use that certificate instead of auto-generated one.

### Replacing Certificate in a Windows\* Installation

To replace certificate in a Windows\* installation, do the following:

- After installation, shut down the web-server for Certificate replacement.
  - Run services.msc from Run command in Windows. This will launch Services window.
  - Search for LightTPDService and stop the service.
- Go to application installation directory (C:\Program Files\Intel\ASC\ in default case) and go inside conf folder.
- Replace lighttpd.crt with your valid certificate. If the name is different rename it to lighttpd.crt.
- Replace the private key file, lighttpd.pem with your private key file.
- Set all the permissions of the key file to only Administrator. No other users should be able to read or write this file.

- Set the permissions of the `lighttpd.pem` to read-write for Administrator and read-only for other users.
- If you do not want to change the file names of your certificate/key file pair, make appropriate changes in the `lighttpd-inc.conf` in the same folder.
- Restart the web-service `LightTPDService` from the Service window.

### Replacing Certificate in Linux\* Installation

To replace certificate in a Linux installation, do the following:

- After installation, shut down the web-server for Certificate replacement.  
`/etc/init.d/lighttpd stop.`
- Go to the folder `/etc/lighttpd/` and replace `lighttpd.crt` with your valid certificate. If the name is different rename it to `lighttpd.crt`.
- Replace the private key file, `lighttpd.pem` with your private key file.
- Set the permissions of the files as below:  

```
-rw-r--r--  1 root root  1326 Mar 28 12:11 lighttpd.crt
-rw-----  1 root root  3005 Mar 28 12:11 lighttpd.pem
```

Only root is allowed to read the private key file and write the public certificate file

- If you do not want to change the file names of your certificate/key file pair, make appropriate changes in the `lighttpd.conf` in the same folder.
  - Restart the web-server  
`/etc/init.d/lighttpd start`
- IASC uses a custom http TCP port (9393) so it does not conflict with site's access control lists or firewall rules  
For proper access to the application, appropriate changes should be done in firewall rules to exclude this port from blocking.  
Customers can modify the port if they want by editing the `/etc/lighttpd/lighttpd.conf` (in Windows, `%ProgramFiles%\Intel\ASC\conf\lighttpd-inc.conf`) and restarting the web-service.
  - IASC uses TCP port 7777 for the communication between IASC and Intel® Multi-Server Manager (MSM). The port can be blocked by customer firewall if you don't have MSM.
  - IASC may use TCP port 9191, 4369, 521 for internal only, those ports all can be blocked by firewall for security purpose.

### Traceability and Security Audit

- IASC keeps track of who all logged-in and logged out and from which client. Any unauthorized attempts to login are also kept track of. This is recorded in the form of events in the Event Table.

Administrators of the tool should periodically do an audit on the events table to find out if there is any misuse of the application or any unauthorized attempts to access the tool.

## 5.1 Security Recommendations

No security feature is fool proof unless you follow certain standard security procedures and controls.

- **Security controls.** Implement, update and monitor industry security products for servers, such as but not limited to: anti-virus, anti-spyware, host based firewall, intrusion prevention, and so on.
- **Remote access.** The platform should be managed by those familiar with securing remote access functions as well as managing systems that are exposed to the Internet.
- When assigning passwords for the ASC and BMC user accounts, make them strong enough to minimize your risk that someone could guess the passwords and thus use the ASC to change the server configuration or interrupt its power/temperature controls. ASC warns the user if the password is weak, so follow the warning and guide-lines.
- **Network controls.** If the management console is being established to allow internet based access it is recommended to be placed within a network enclave that is consistent with many companies' internal policy of maintaining a "DMZ" or zone of networks that is more closely monitored than internal networks.
- **Firewall.** Enable firewall software/services on Server where you install ASC or to the network, and only enable exceptions to allow access to the web server on each server. Where possible, limit which remote clients (e.g. using IP address ranges) can connect to the web server.
- To prevent successful Cross-Site Scripting and Forgery attack (XSS/CSRF) the users should follow certain security guidelines:
  - Make sure you access the application only from trusted clients.
  - Do not leave the application logged-in for a prolonged time and close the browser as soon as you finish the usage.
  - Do not visit any suspicious site or click on any public links in any other tabs in the browser while you are accessing the application.
  - Change the passwords frequently to prevent unauthorized access by any internal user and to reduce social engineering attacks.
  - Delete and create new application user accounts to reduce the risk of unauthorized access from internal users or ex-users.



## 6.0 Troubleshooting Guidelines

If you face any issues or doubts while using IASC, you may refer to the **Help** section available in each page of IASC. If the issue persists, read the following sections for known issues and troubleshooting tips.

### INSTALLATION ISSUES AND ENVIRONMENT REQUIREMENTS

- If you are not able to access the IASC installed in a server from a remote location but you are able to ping the server or connect remotely to the server, then it could be a firewall issue. Troubleshoot this by disabling the firewall temporarily and try connecting to the IASC URL remotely again. If it works by disabling the firewall, then try adding the ports **9393, 9191, and 7777** to the exception list of firewalls to the server.

IASC uses ports **9393, 9191, and 7777** which should be excluded from system's firewall if you have to reach the tool from other systems remotely or from outside of your private network.

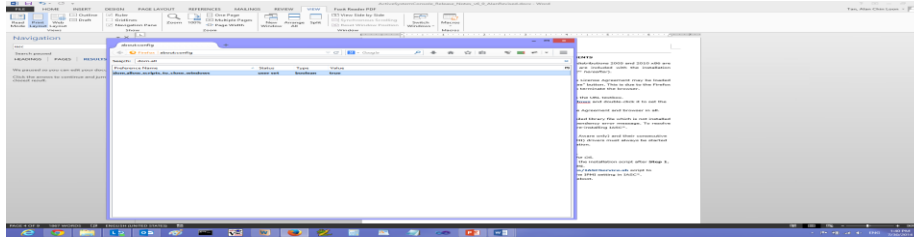
- System runtime components such as Microsoft Visual C++ Redistributions 2005 and 2010 x86 are pre-requisites for IASC installation, the IASC installer will install those components automatically.
- During installation of IASC on Linux\* Operating Systems, the License Agreement may be loaded with Firefox\* browser and cannot be closed by clicking the "Close" button. This is due to the Firefox\* browser's default setting which disabled any external script to terminate the browser.

To enable the button,

**Step 1:** In Mozilla Firefox browser, type **about:config** in the URL textbox.

**Step 2:** Search for **dom.allow\_scripts\_to\_close\_windows** and double-click it to set the value to "true".

**Step 3:** Click the "Close" button, it shall close the License Agreement and browser in all.



4. Installation of IASC on RHEL\* 5.x requires **libxslt.so**, a compiled library file which is not installed by default OS setting. This may halt the installation with dependency error message. To resolve the issue, install compatible **libxslt.<os\_arch>.rpm** before re-installing IASC.
  
5. For RHEL\* 6.4 (Legacy Boot and UEFI Optimized Boot), SLES 11 (UEFI Optimized Boot only) and their consecutive releases. The Intelligent Platform Management Interface (IPMI) drivers must always be started manually before starting IASC service, including the installation. To start the IPMI service,  
**Step 1:** Enter **modprobe ipmi\_devintf\*** in a Linux Terminal.  
*\* This command works only if the openIPMI package has been installed in the OS.*  
**Step 2:** (i) For first-time installation of IASC, re-launch the installation script after **Step 1**, IASC service will use the latest setting of IPMI.  
(ii) For post-installation, run **/usr/local/asc/bin/IASCService.sh** script to restart IASC after **Step 1**, this will update the IPMI setting in IASC.  
**Note:** Both steps have to be performed for each System reboot.
  
6. (i) Installation of IASC on RHEL\* 6.x (x64 architecture only) requires the following 32-bit shared library files which are not installed with the OS by default setting. The shared libraries could be installed from the RHEL\* OS installation image disc (ISO) containing their respective RPMs.

**Table 2: Required RPMs for IASC Installation**

<ul style="list-style-type: none"><li>• zlib-1.2.3*i686*</li><li>• libxml2-2.7.6*i686*</li><li>• libgpg-error-1.7*i686*</li><li>• libgcrypt-1.4.5*i686*</li><li>• libxslt-1.1.26*i686*</li><li>• libstdc++-4.4.7*i686*</li><li>• compat-libstdc++-33-3*i686*</li><li>• ncurses-libs-5.7-3*i686*</li><li>• ncurses-devel-5.7-3*i686*</li><li>• db4-4.7*i686*</li><li>• nspr-4.9*i686*</li><li>• nss-util-3.14.0*i686*</li><li>• readline-6.0*i686*</li></ul>	<ul style="list-style-type: none"><li>• sqlite-3.6.20*i686*</li><li>• nss-softokn-3.12.9*i686*</li><li>• nss-3.14.0.0*i686*</li><li>• cyrus-sasl-lib-2.1.23*i686*</li><li>• libidn-1.18-2*i686*</li><li>• libcom_err-1.41.12*i686*</li><li>• openldap-2.4.23*i686*</li><li>• keyutils-1.4-4*x86_64*</li><li>• keyutils-libs-1.4-4*i686*</li><li>• libsasl-2.0.94*i686*</li><li>• krb5-libs-1.10.3*i686*</li><li>• openssl-1.0.0-27*i686*</li><li>• libssh2-1.4.2*i686*</li></ul>
---	--

**Note:** The RPMs have inter-dependency which requires them to be installed in sequence as numbered as in **Table 2**.

(ii) The IASC installation package has included a shell script **RHELx86\_64AUTO.sh** for the convenience of installing the 26 RPMs all in once.

To use the script,

**Step 1:** Insert a RHEL\* 6.x OS installation image disc containing the 32-bit shared library RPMs to the system.

**Step 2:** Unzip the shell script and run **sh RHELx86\_64AUTO.sh** in a Linux Terminal.

**Disclaimer:** The **RHELx86\_64AUTO.sh** script is intended to be used as an installation auxiliary, and it is not maintained as an Intel product, thus its content may be outdated and rendered the script erroneous. However, user may install each of the RPMs directly from the RHEL\* OS ISO Disc or download using **yum install**.

7. User may see the following warnings during installation of IASC on SLES\*:

*Insserv: warning: script 'K01Appcore' missing LSB tags and overrides*

*Insserv: warning: script 'S01Appcore' missing LSB tags and overrides*

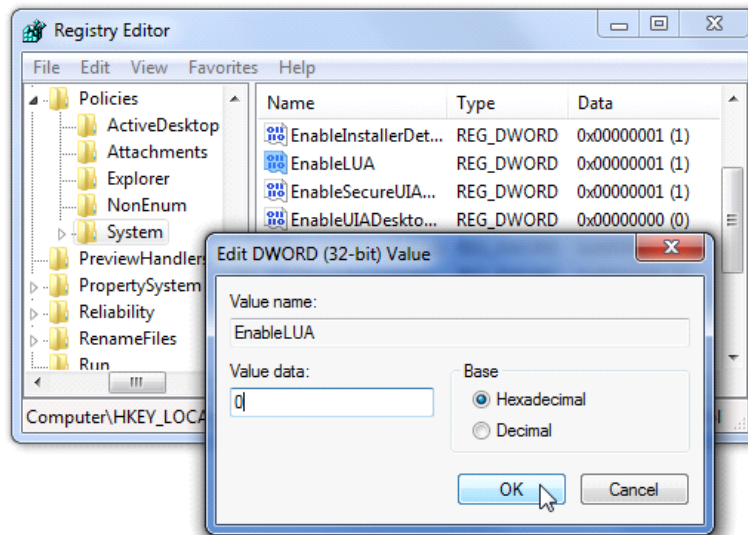
Insserv warning are bootscript comment header warning. User may ignore these warnings as they do not affect the installation.

- Installation of IASC on Microsoft Windows 8\* and Windows 2012\* R2 requires UAC to be disabled using direct registry modification.

**Step 1:** Launch regedit.exe, look through directories for **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**

**Step 2:** Look for entry EnableLUA, and alter the values as followed  
 UAC Enabled: 1  
 UAC Disabled: 0

**Step 3:** Save the setting and reboot the system if required.



9. If at any time, any of the following essential services of IASC are down, IASC will not work properly. If you are facing some issues in accessing the tool, you should check if the following services are running.

In Windows\*, start the following services and verify,

- IASCServiceManager
- Appcore

In Linux\*, run the following commands and verify,

- `/etc/init.d/lighttpd status`
- `/etc/init.d/ascpolicy status`
- `/etc/init.d/Appcore status`

10. If web-server seems to be non-responsive on Linux\* OS, run the following command:

`/etc/init.d/lighttpd restart`

11. User must make sure two Windows\* services, **IASCServiceManager** and **Appcore**, are always running on Windows\* OS. To run the services, execute the batch file "**IASCService.bat**" in the

installed path, user may run “services.msc” from command line and search for the service names.

Manually start these services if they are stopped. If the problem persists due to Baseboard Management Controller (BMC) interface being non-responsive, a power cycle may resolve the problem.

12. User must make sure that the system installed with IASC is **NOT** installed with SNMP-SA or equivalent applications. IASC may provide incorrect and incomplete information or even ceased from running as it would conflict with SNMP-SA on using the same system resources.
13. Installation of IASC in Linux\* Operating Systems will show warning message (shown below message) at the end of the installation process. This warning is to let user know user may experience IASC login failure if the system network configuration not working properly. For more details refer section 10.

“!!! Warning.....!!!!

Please check the DNS server setting or add the hostname into system file /etc/hosts in order for the Active System Console to do name resolution for the system name to avoid login fail issue, refer to the software Release Notes for details.”

## **USER LOGIN ISSUES AND BROWSER SETTINGS**

- IASC supports secure transport using SSL/TLS authentication process with self-signed certification. But as the certification is not signed by publicly acknowledged authority, default security settings of web browsers may blocked IASC Login Page from loading and prompt warning messages of “Untrusted Connection” (Firefox) or “Invalid Security Certification” (Internet Explorer)

To resolve this,

**Method 1:** Override the warnings and accept the certificate, proceed to login page. User must ensure the certificate is originated from the application on a trusted secure network.

**Method 2:** Add your own certificate, please refer to User Guide for further instructions.

- When user logged into IASC webpage [https://system\\_IP:9393/asc/](https://system_IP:9393/asc/) for the first time, IASC may appear unresponsive for a few minutes as it is updating its system health data enquiries with latest information.

- When using Internet Explorer to launch IASC, users may clicked button with no response, or not able to launch pop-up active windows upon clicking button.

To resolve this, user must edit setting of Internet Explorer:

**Step 1:** Go to **Menu -> Tools -> Options -> Security -> Select Internet Zone -> Custom Level -> Scripting**

**Step 2:** Under Scripting, enable all Active Scripting and Scripting options.

**Step 3:** Save the new setting, then restart Internet Explorer and load IASC page.

- User may not able to save the reports generated by Report feature of IASC in Internet Explorer\* due to browser setting.

To change this,

**Step 1:** Go to **Tools -> Internet Options -> Advanced -> Security**, and uncheck the 'Do not save encrypted pages to disk'.

**Step 2:** Retry generating the reports and save.

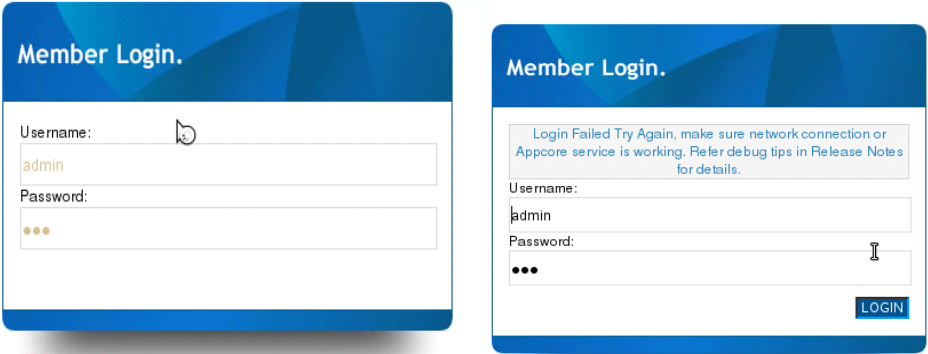
- The "waiting" icon (spinning wheel, flashing dots) and Critical Event scrolling may not work if the browser does not allow animation to play.

To enable the feature in Internet Explorer,

**Step 1:** Go to **Tools -> Internet Options -> Advanced -> Multimedia**, and check the 'Play animations' option.

**Step 2:** Refresh browser or re-launch IASC.

- When IASC login shows “Login Failed Try Again” or no activity, user should follow the methods below to debug the issue.

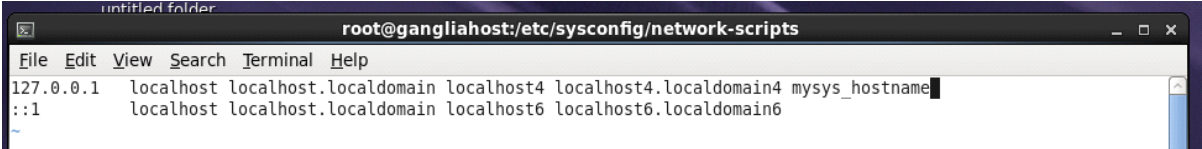


To resolve this,

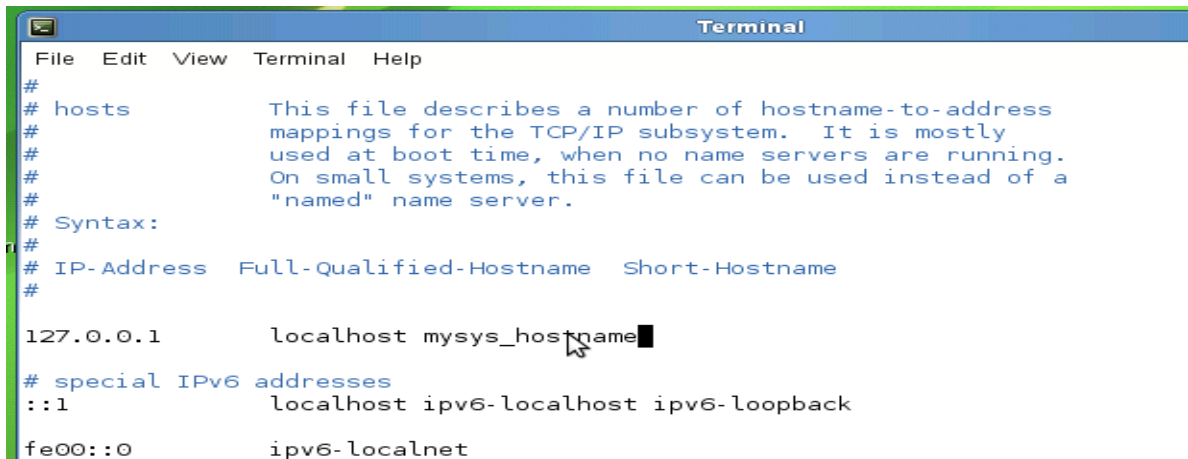
**Method 1:** If Appcore service is stop, restart the service by running shell script file `/usr/local/asc/bin/IASCService.sh`.

**Method 2:** Check the network connection. If DNS network connection is disconnected, IASC will keep looping until time-out. If user decides not to use DNS network anymore, user can set the system hostname into the `/etc/hosts` refer below example (mysys\_hostname added into hosts file). Restart IASC service after setting the system hostname.

Rhat OS:



SuSE OS:



```
Terminal
File Edit View Terminal Help
#
# hosts          This file describes a number of hostname-to-address
#                mappings for the TCP/IP subsystem.  It is mostly
#                used at boot time, when no name servers are running.
#                On small systems, this file can be used instead of a
#                "named" name server.
# Syntax:
#
# IP-Address    Full-Qualified-Hostname  Short-Hostname
#
127.0.0.1      localhost msys_hostname
# special IPv6 addresses
::1           localhost ipv6-localhost ipv6-loopback
fe00::0       ipv6-localnet
```

### KNOWN INFORMATIONAL IRREGULARITIES AND ISSUES

- Part of system sensor information, such as on Memory and Processor, are not available in IASC that installed on system with GPT volume.
- Sensor Events are generated by IASC only if the sensor is functional and providing analyzable reading; sensors which are showing *NOT\_AVAILABLE* state are not used in system health calculation, e.g. PCIe Corr sensor.
- When a CD/DVD is inserted to the system, IASC® would show “OMB space left” and generates a Critical warning. Once the CD/DVD is removed from system, IASC® returns to Healthy state.
- IASC may not able to comprehend FRUSDR details which have special characters such as “&”, “\*”, “#”, thus blank values may be shown.
- IASC is not supported on Virtual Environment and Non-BMC Server Board.
- SOL BAUD Rate configuration is not available for Intel® Server S1200RP product family.



- HSC FW version for Intel® Server S1200RP product family is shown in unseparated format on screen.
- Boot order changes might not be successful if “syscfg /bbo” command is being used before using IASC to change the boot order. Use bios F2 setup page, press F9 to load bios default & reconfigure the boot order if this issue happen.
- IASC may not display the Serial number and Model number of the configured RAID volumes and it may display NOT\_AVAILABLE in Model number and Serial Number columns of Storage information.
- IASC may not display the Serial number and Model number of the USB drives if the firmware is not available for the devices and it may display NOT\_AVAILABLE in Model number and Serial number columns for storage information.