



Intel® Multi-Server Manager

User Guide

February 2012

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 © 2012 Intel Corporation. All rights reserved.

Revision History

Description	Revision Date
Initial release.	March 2011
Updated TCP ports information	June 2011
Support for Intel® Xeon® E5 Processor based platforms	December 2011
Updated Supported Operating Systems	February 2012

Contents

Legal Statements	2
Contents	4
List of Figures.....	6
1 Introduction	8
1.1 Document Scope.....	8
1.2 Overview	8
1.3 Features and Benefits.....	9
1.4 System Requirements	11
1.4.1 Supported Operating Systems.....	12
1.4.2 Browser Requirements	12
1.4.3 Supported Platforms	12
1.5 Supported Languages.....	12
1.6 Additional Information	12
1.6.1 Third Party Source Code/Binaries	12
1.6.2 Support Information	13
1.6.3 Related Documentation	13
1.7 Terminology	14
2 Getting Started.....	15
2.1 Installing Intel® Multi-Server Manager	15
2.2 TCP Information	17
2.3 Launch Intel® Multi-Server Manager	17
2.4 Uninstalling Intel® Multi-Server Manager.....	20
3 Navigating Intel® Multi-Server Manager.....	21
3.1 Home (Dashboard).....	23
3.1.1 Summary	23
3.1.2 Open Events	24
3.1.3 Actions.....	24
3.1.4 Groups.....	26
3.1.5 Creating a New Group.....	26
3.1.6 Deleting Groups	26
3.1.7 Deleting Servers.....	27
3.1.8 Move To (Moving servers from one group to another)	27
3.2 Discovery.....	27
3.2.1 Discovery Operation	28
3.3 Remote Console.....	29
4 Configuring Intel® Multi-Server Manager	30

4.1	Users	30
4.1.1	Creating a new User	30
4.1.2	Deleting a User	31
4.1.3	Editing a User	31
4.2	Email Server	31
4.2.1	Creating a New Mail Server.....	31
4.2.2	Deleting an already created mail server	32
4.2.3	Editing a mail server	32
4.3	Email Policies	32
4.3.1	Editing Email Alert Policy	32
4.3.2	Configuring New Email Alert Policy.....	33
4.3.3	Configuring Advanced Email Alert Policy	33
4.3.4	Data Archive.....	33
5	Reports	35
6	Security Features	36
6.1	Security Recommendations	38

List of Figures

- Figure 1. Windows version MSM installation main interface..... 15
- Figure 2. Set password for MSM default administrator account "admin"..... 16
- Figure 3. MSM self-signed certificate alert in IE* and Firefox*..... 18
- Figure 4. MSM login window 21
- Figure 5. MSM Home page..... 22
- Figure 6. Tool-bar of MSM 22
- Figure 7. MSM Discover page..... 27
- Figure 8. MSM Discovery operation..... 28
- Figure 9. MSM User Settings..... 30
- Figure 10. MSM Email Server configuration..... 31
- Figure 11. MSM Report generation..... 35

<This page is intentionally left blank.>

1 Introduction

Intel® Multi-Server Manager (MSM) is a simple, easy-to-use web-application that allows users to discover and manage multiple Servers in their network from a single console. It can manage any Server hardware that is IPMI compatible.

1.1 Document Scope

The purpose of this document is to help system/server administrators install and use the Intel® Multi-Server Manager (MSM). It provides you detailed information on the features and benefits of MSM 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® Multi-Server Manager 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.

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

1.3 Features and Benefits

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

Intel® System Management Software

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

Features	Intel® Multi-Server Manager	Intel® Active System Console	Intel Management packs for the Microsoft* System Center	Intel® SNMP-SA
Server Environment	1-100 servers	1-10 servers	10-50 servers (Use Operations Manager for Enterprise)	Enterprise
User Interface	Web Based	Web Based	Windows Management Application	Integrates into enterprise tools such as HP* OpenView
Operating System Support	Windows, Linux	Windows, Linux	Windows, Linux	Windows, Linux
Single, easy to use console	X	X	X	
Hardware Predictive Failure Analysis	X	X	X	X
Sensor readings	X	X	X	X
Hardware Event Log	X	X	X	
Hardware and Software Inventory	X (Hardware and Operating System)	X (Hardware and Operating System)	X	
OS and Application Monitoring			X	
Software Patch Deployment			X	
Application Deployment			X	
Alerting	X (Email or BMC SNMP)	X (Email and BMC SNMP)	X (Email, SNMP, SMS)	X (SNMP)
Reporting	X	X	X (80 powerful software and hardware reports)	
BMC Configuration	X	X	X	

Features	Intel® Multi-Server Manager	Intel® Active System Console	Intel Management packs for the Microsoft* System Center	Intel® SNMP-SA
Power Management	X	X	X	
Performance Views			X	
Remote Management	X	X	X	X
Multi Server Management	X		x	
Remote Power On/Off/Reboot	X		X	
Serial Over LAN (Console Redirection)			X	
OEM Customization	X	X	X	

Intel® Multi-Server Manager

The Intel® Multi-Server Manager has all the features of the Intel® Active System Console and combines it in one easy to use console to manage the entire network.

Intel® Multi-Server Manager is included with almost all Intel Server Products at no additional charge giving user "peace of mind" that servers are healthy.

Prime benefits include:

- 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.

Additional features bring in benefits including:

- Simple discovery and grouping capabilities. Discovery of the system regardless of the operating system and organize them exactly how you want to.
- Power on, off, or reset the servers from a remote location.

- Single point alert configuration. Set up email alerting for all the systems in your environment from one location.
- Powerful reporting. Select from many reports to run against a single system or an entire group. Compare two or more servers to see systems differences.

The Intel® Multi-Server Manager (MSM) provides broad spectrum server management options ranging from Power actions and group server health monitoring to sending software level Email alert and BMC SNMP alert. The Remote console launch point is a convenient way to monitor minute details of the health of your Server enabling Server settings configuration both for *In-Band* and *Out-of-Band* conditions.

- **In-Band.** In an In-Band condition, the Remote console provides Operating system along with the Intel agent and helps obtain relevant additional details.
- **Out-of-Band.** In an Out-of-Band condition, the console provides concise information obtained from the Baseboard Management controller (BMC).

1.4 System Requirements

This section details the software requirements, supported operating systems and the supported platforms for the Intel® Multi-Server Manager. The following table lists the system requirements:

System Requirements					
Number of Servers		Minimum CPU Requirement**	Minimum Memory Requirement	Minimum Network Requirement	Minimum Hard Disk free space for MSM Logs
In-Band	Out of Band				
10	0	1 Core	1 GB	Shared NIC	200MB
20	10	2 Cores	2 GB	1 Dedicated NIC	400 MB
20	15	2 Cores	2 GB	1 Dedicated NIC	450MB
30	20	4 Cores	4 GB	1 Dedicated NIC	600MB
40	25	4 Cores	4 GB	1 Dedicated NIC	750MB
50	30	6 Cores	4 GB	2 Dedicated NIC	900MB
60	30	6 Cores	4 GB	2 Dedicated NIC	1GB
70	30	8 Cores	4 GB	2 Dedicated NIC	1.5 GB

Note: ** Please refer to the *processor specifications* for the number of cores supported.

1.4.1 Supported Operating Systems

Intel® Multi-Server Manager Server and Agent

- Microsoft Windows* Server 2003 SP2 Standard/Enterprise Edition – (x86 & EM64T)
- Microsoft Windows* Server 2003 R2 Standard/Enterprise – (x86 & EM64T)
- Microsoft Windows* Server 2008 Standard/Enterprise/Datacenter (x86/x64)
- Microsoft Windows* Server 2008 R2 Standard/Enterprise/Datacenter
- Red Hat* Linux* Enterprise 5.7/6.x (x86/x64)
- SuSE* Linux Enterprise Server 10 SP3 (x86/x64)
- SuSE* Linux Enterprise Server 11 SP1 (x86/x64)

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

- Multi-Core Intel® Xeon® Processor E5 Sequence-based Servers
- Multi-Core Intel® Xeon® Processor 5500 Sequence-based Servers
- Multi-Core Intel® Xeon® Processor 3000 Sequence-based Servers

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 MSM 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® Multi-Server Manager Release Notes	Available at the root of the CD.
Intel® Active System Console User Guide	Available at CD\documents\User Guide\ENU
Intel® Active system Console Release Notes	Available at the root of the CD.
Intel® Intelligent Power Node Manager – White Paper	Available at CD\documents\User Guide\ENU

1.7 Terminology

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

Term	Description
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(ISMS)	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 BIOS 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
MSM	Intel® Multi-Server Manager
IASC	Intel® Active System Console

2 Getting Started

This section provides some basic steps on how to install and use the Intel® Multi-Server Manager.

2.1 Installing Intel® Multi-Server Manager

Intel® Multi-Server Manager (MSM) installation includes MSM itself and MSM agent. MSM agent needs to be installed on all managed server manually, MSM can be installed on one of server and user can monitor other managed server from it.

- **Install MSM and agent on Microsoft Windows* OS**
 1. Insert Intel® Server Deployment and Management media, go to System Management Software Tab or user can browse MSM package folder and start the MSM installation main interface manually.

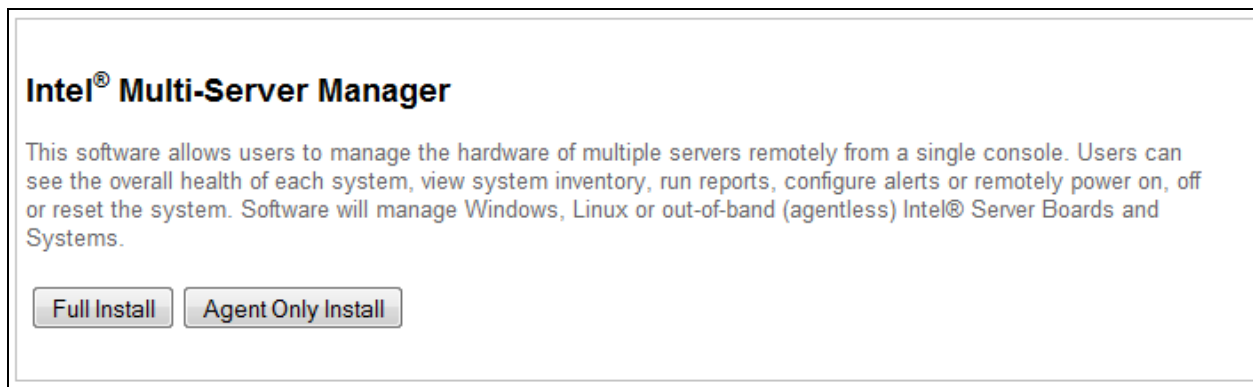


Figure 1. Windows version MSM installation main interface

2. Click "Full Install" button to install MSM or Click "Agent only Install" button to install MSM agent only
3. Following the screen indicators to start MSM installation, accept MSM end user license, and confirm the installation folder for MSM.
4. The MSM installer prompts you to password for Intel® MSM default administrator account "admin" during installation. 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 ` - _ = + ! ~ # @ \$ * ; : , . ? & ^) **Note:** If you forget the password, you need to reinstall MSM.

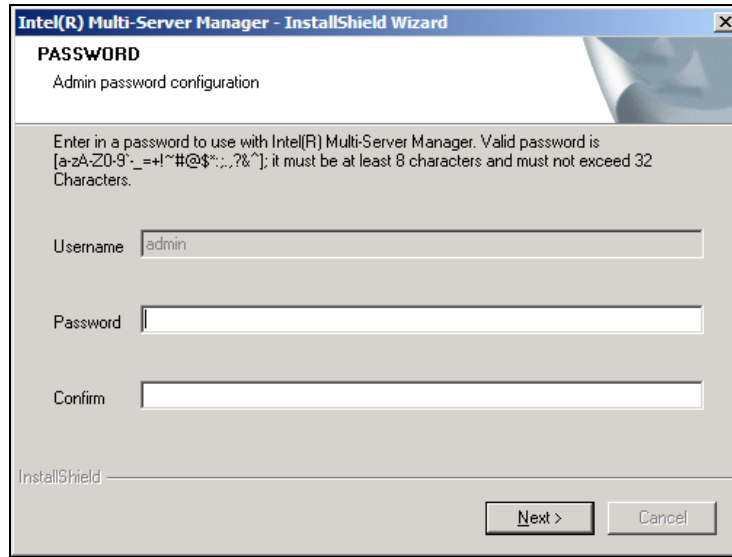


Figure 2. Set password for MSM default administrator account "admin"

- **Install MSM and agent on Linux* OS**

1. User should have root privilege to install MSM or agent on Linux* OS. Intel ISMS CD provide **different SMS version for RHEL* Linux 5 and SuSE* Linux 10, 11**. Copy relative Multi Server Manager-*.tar.gz from ISMS CD\Software folder to a temporary folder in Linux OS
2. Change folder to the temporary folder
3. Run command " tar -xzvf ./Multi-ServerManager-*.tar.gz " to unzip this file
4. Change folder to "./MSM" if you want to install MSM, or "./MSMAGENT" if you just need to install MSM agent.
5. Run command "./install" to start the MSM installation. The installer shows the MSM end user license in a browser first, click the "Close" button or close the browser window directly after reading MSM end user license.

Note: License page cannot be closed by clicking "Close" button on some Linux* systems. To resolve, do the following:

1. Launch Mozilla Firefox* and type about:config in the URL window.
2. Search for " dom.allow_scripts_to_close_windows ", double click it and set it to "true".
3. After you close the end user license, the installer will ask you "Do you agree to the terms of license? Answer "Y" if you agree to it or "N" to stop the MSM installation. The installer will continue to install all software packages after you answer "Y"
4. The installer will ask user set password for default MSM administrator account "admin", we recommend you set "admin" with strong password.

2.2 TCP Information

The following TCP ports are used by Intel® Multi-Server Manager and Agent.

Port #	Description	Firewall Exception Required
7777	Use for discovery and manage Intel® Multi Server Manager Agent and Intel® Active System Console	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 and 9393 is required to add on the firewall approval list.

Refer **Chapter 6** for more security features.

2.3 Launch Intel® Multi-Server Manager

The installer will create a shortcut of "Intel® Multi-Server Manager" on Microsoft Windows* or Linux* desktop after MSM is installed successfully. User can double click this shortcut icon to launch MSM or go to **Start > Programs > Intel > Intel® Multi-Server Manager** to launch it on Microsoft Windows* OS.

User can also launch MSM from local browser with URL <https://localhost:9393/iscc/> or from any client with browser using the URL:
`https://<ipaddressofMSMserver>:9393/iscc/`

MSM supports secure transport using SSL/TLS. SSL/TLS uses a self-signed certificate because of which the browsers will throw an "Untrusted Connection" warning. The following are screen shoot of this warning on Microsoft Windows* and Linux* OS

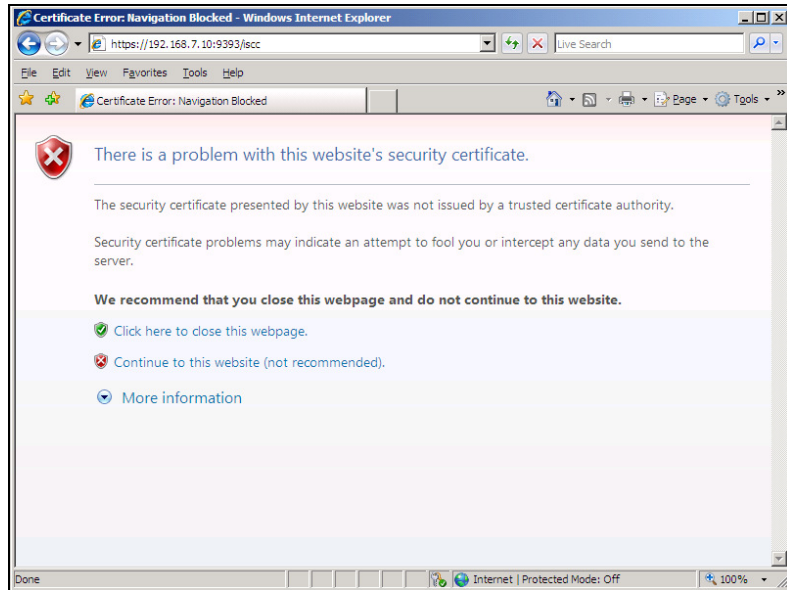


Figure 3. MSM self-signed certificate alert in IE* and Firefox*

The certificate used in MSM 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 the auto-generated one.

- **Replacing Certificate in a Microsoft Windows* Installation**

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

1. 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.
2. Go to application installation directory (C:\Program Files\Intel\ASC\ in default case) and go inside conf folder.
3. Replace lighttp.crt with your valid certificate. If the name is different rename it to lighttp.crt.
4. Replace the private key file, lighttp.pem with your private key file.
5. Set all the permissions of the key file to only Administrator. No other users should be able to read or write this file.
6. Set the permissions of the lighttp.pem to read-write for Administrator and read-only for other users.
7. 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.
8. Restart the web-service LightTPDService from the Service window.

- **Replacing Certificate in Linux* Installation**

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

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

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

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

5. 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.
6. Restart the web-server
/etc/init.d/lighttpd start

2.4 Uninstalling Intel® Multi-Server Manager

User can uninstall MSM from Microsoft Windows* OS from Menu **Start ->All Programs->Intel->Uninstall Intel® Active System Console**

And run command " `/usr/local/asc/bin/uninstall` " to uninstall MSM from Linux* OS.

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 (`/usr/local/asc/bin/SMS.db`) to appropriate location before uninstall.

3 Navigating Intel® Multi-Server Manager

This section details how you can navigate the Intel® Multi-Server Manager to use its features.

During MSM launch, you are required to enter your user login. The default MSM administrator username is "admin". You can set the password during the MSM installation process.

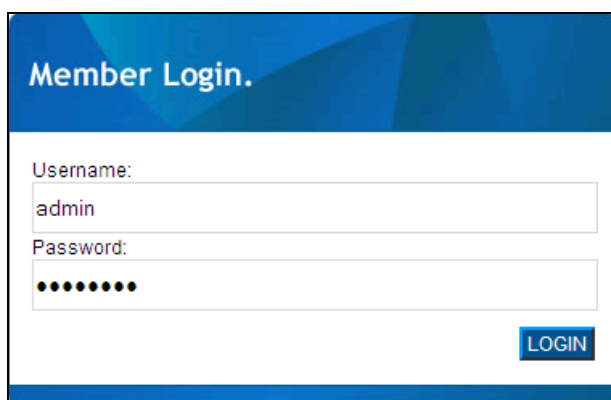


Figure 4. MSM login window

By default, Intel® Multi-Server Manager opens the home page after successful login. The MSM home page comprises three sections.

- **Groups.** The first section on the left is Groups. Use this to perform actions on groups. See Groups for details.
- **Dashboard.** This central page gives dashboard view of all Servers within a group in the Home page and comprises:
 - A tool-bar access to the main pages
 - Listing of all Servers in a group you selected from the Groups section, with the selected group name shown on its top left.
- **Actions.** Listed at the right hand side are a set of actions that can be performed on Servers.

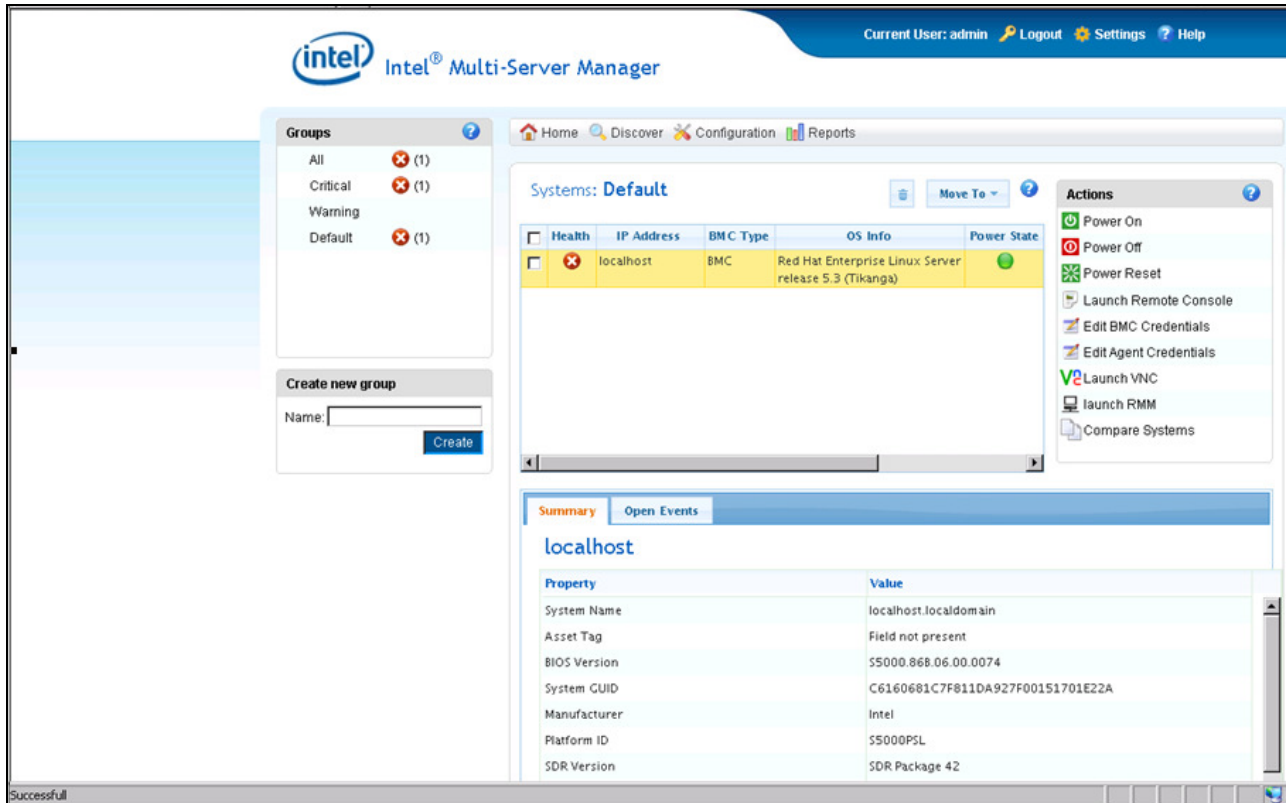


Figure 5. MSM Home page

The Intel® Multi-Server Manager has the following four pages:

- Home(Dashboard)
- Discovery
- Configuration
- Reports

These pages can be quickly accessed from any other Page using a tool-bar at the top of the middle section of MSM Home page as shown in Figure 6.

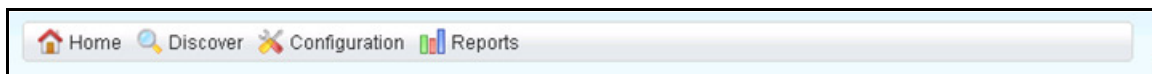


Figure 6. Tool-bar of MSM

3.1 Home (Dashboard)

The Home page of Intel® Multi-Server Manager (MSM) shows the local host server in which the MSM has been installed by default. This provides a dashboard view of the Servers in the network. The Servers are organized into user-defined Server Groups.

The center section lists the Servers in the Group selected on the left menu. For each Server, its overall hardware health status, the IP address/hostname and the operating system information and power state are listed. It also shows how the Server was discovered (whether discovered using SMS Agent (In-Band) or in an agent-less fashion (Out-of-Band)).

The field BMC Type indicates what management controller is available in the Server. It can take values such as

- BMC - only basic management controller available,
- RMMlite - intermediate management controller available
- RMM[2|3|4] - advanced Server management controller available

Click on the IP Address of each Server in the list to see more details (Summary and Open Events) of the Servers in the main page.

3.1.1 Summary

The Summary section displays the following system summary properties and corresponding values:

Property	Value
System Name	Host name of the Server
Asset Tag	Asset name in server board FRU
BIOS version	The BIOS, Firmware version details are mentioned based on the current values obtained from the server.
System GUID	The system GUID is a Global Unique Identifier which is usually unique for each and every system on the network.
Manufacturer	The manufacturer details
Platform ID	Corresponding Motherboard platform identification value.
SDR Version	Sensor Data Recorded Package version
BMC Version	Baseboard Management Controller version
HSC Version	Hot Swap Backplane Controller version

Property	Value
Serial Number	Serial number of the server
Operating System Name/ Kernel VersionName/ Kernel Version	In Band: The server OS name and version information OOB: Display a string called Out of Band
Operating System Build	The server OS Build version





3.1.2 Open Events





This tab displays all open Critical and Warning events of the Server. This provides an easy access to latest events without launching remote console.


The table of Events lists the date and time of occurrence of an event, its description, severity, and status

3.1.3 Actions

The right pane on the Home page of Multi Server Manager provides the Actions menu of any selected servers. Key actions include the following:

Action	Meaning
 Power On	The action can turn on all selected server.
 Power Off	The action can turn off all selected server.
 Power Reset	The action can reset all selected server.
 launch remote Console	<p>The Remote console helps user in fine grain monitoring and trouble-shooting of the selected Server and also to configure the Server settings. It can be accessed in both in-band and out-of-band conditions. During in-band condition the Remote console provides more information as Operating system along with the Intel agent helps in obtaining the additional information. During Out of Band condition the console provides minimal necessary information which it gets from the Baseboard Management Controller (BMC).</p> <p>Note: This action is only for one selected server a time.</p>

Action	Meaning
 Edit BMC Credentials	<p>The BMC Credentials allow user to edit the BMC credentials that user had given during the discovery of the server. If user had given incorrect credentials during discovery or if the BMC credentials have been changed then the new credentials can be entered into database using this option.</p> <p>Edits only the SMS database, it doesn't change the credentials in the base-board controller. The credentials are stored in the SMS database for remote access to the Server for health calculation.</p> <p>For editing the actual Motherboard BMC Credentials, user must launch Remote console and then edit the setting from the BMC User configuration</p> <p>Edit Agent Credentials. This option helps in editing the In-Band agent credentials. In case you had given incorrect credentials during discovery, then the new credentials can be entered into database using this option.</p> <p>Note: This action is only for one selected server a time.</p>
 Edit Agent Credentials	<p>This option helps in editing the In Band agent credentials. If you had given incorrect credentials during discovery, then the new credentials can be entered into database using this option.</p> <p>Edits only the SMS database. It does not change the credentials in the Agent. The credentials are stored in the SMS database for remote access to the Server for health calculation.</p>
 Launch VNC*	<p>Launches Virtual Network Computing*</p> <p>Note: This action is only for one selected server a time, and only Linux* OS is supported by this action. User can refer http://www.vnc.com for more details of VNC configuration</p>
 Launch RMM	<p>Launches Remote Management Module embedded web console or Integrated BMC web console. This option is dynamically enabled based on type of the server selection. Launch RMM will launch the Embedded Web Server on new generation</p>

Action	Meaning
	platforms.
 Compare Systems	User can select more than two servers and compare their summary information





3.1.4 Groups

Servers can be organized into user-defined groups. By default four groups are created – All, Critical, Warning and Default.

- All. Lists all Servers discovered and managed.
- Critical. Lists only Servers that are in Critical status.
- Warning. Lists Servers that are in Warning status of health.
- Default. This is the default group. All Servers that are discovered and added for management are added to this group. Users can move Servers from here to user-defined groups.

Additional groups can be created using the action Create new group be organized into user-defined groups. By default, four groups are created - *All, Critical, Warning* and *Default*.


The aggregate of the system health is shown as icons in the Dashboard as follows:

 Healthy	You need not check on that component
 Critical	Component needs your immediate attention
 Warning	Component is on the path towards criticality and needs your attention. Unavailable.
	The Server, though discovered is not reachable. It could be network connection issue or credentials issue. The reason can be seen in Remarks column


3.1.5 Creating a New Group

1. Enter a group name in the section of "Create new group" at MSM Home page, for example "Rack1", "Core Group", etc.
2. Click on **Create** button. The message Group created successfully will appear. Click on **OK**.
3. The new group will now appear in the list of groups.

3.1.6 Deleting Groups

The default 4 groups: All; Critical; Warning and Default cannot be deleted. Only user created groups can be deleted. All user created groups has icon as  in front of group name, click this icon and select menu "Delete". The message Group deleted successfully will appear. Click **OK**.

3.1.7 Deleting Servers

There is an option for deleting servers from the management console. Select Server to be deleted using the check box and then click the  (Delete icon). This will permanently delete the Server from the management database. User still can manage the server again by discovery operation.

Note: As a precautionary means of self protection of the installed software, the Localhost server cannot be deleted.

3.1.8 Move To (Moving servers from one group to another)

For ease of use, managing servers in multiple locations or in different racks, specific servers can be selected from the Default group by checking on the corresponding check boxes and from the Move To task bar the group can be selected. User created group name is shown in the menu of **Move To**.

3.2 Discovery

The **Discover** tab helps user to discover the Servers in the network that can be managed using MSM. Click **Discover** at the MSM home page tool-bar to open the **Discover** tab.

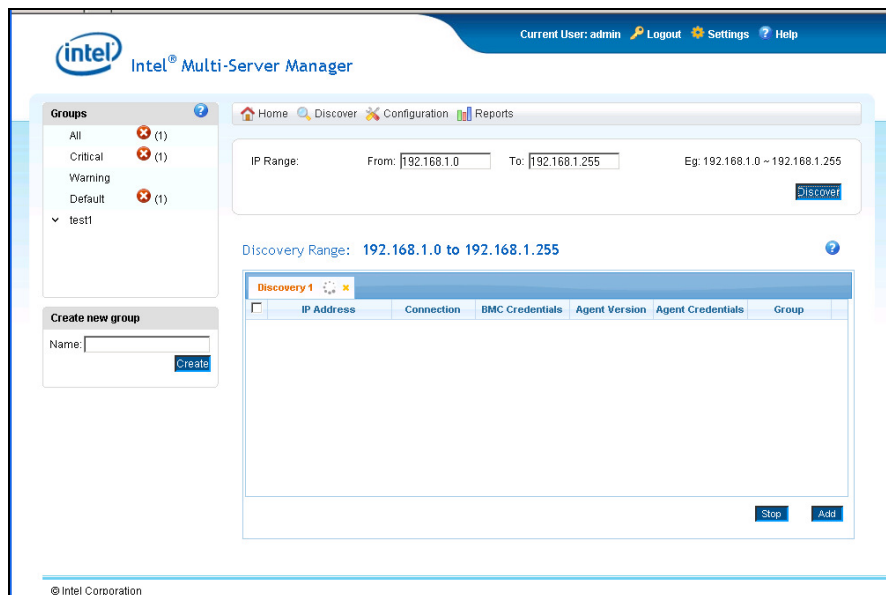


Figure 7. MSM Discover page

3.2.1 Discovery Operation

In the Discover page, enter the IP range (from and to) in the IP range box and click on Discover button.

To discover a single server, enter the single IP Address in both from as well as to space.

For example, as 192.168.1.1 to 192.168.1.255.

For a larger range enter the first and last number in the range.

For example, 192.168.1.1 to 192.168.1.255.

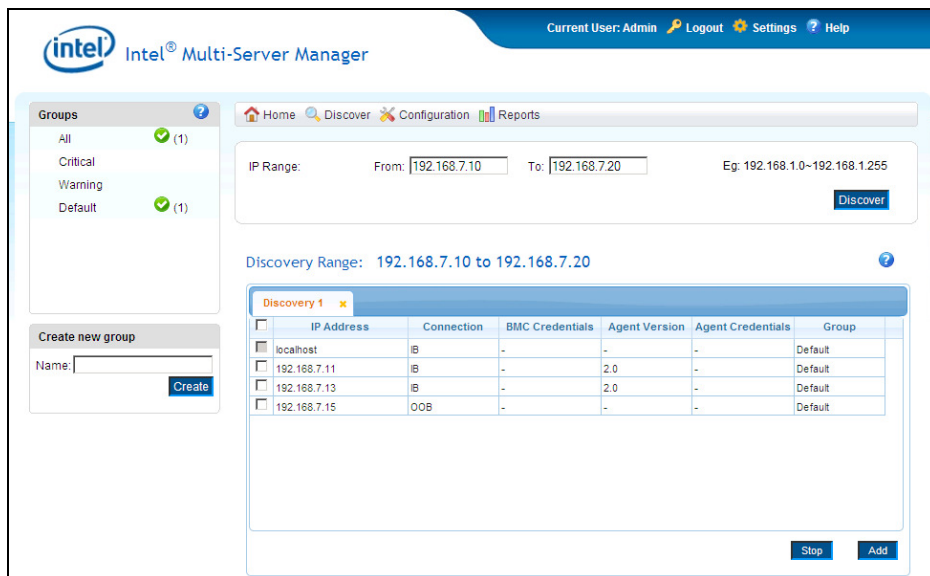
For multiple range discoveries in which different subnet masks are involved, two or more discoveries can be performed at the same time.

For example, enter 192.168.1.1 to 192.168.1.255, click on **Discover** button. A tab appears below the button showing the progress on the discovery.

Once the discovery kicks off, enter a new range 192.168.7.10 to 192.168.7.20, and click again on **Discover** button, a second tab appears showing the new discovery as well.

Before start the discover process, user need to install MSM agent on target managed server OS for In-Band (IB) management or setup BMC IP address and BMC user and password for Out-of-Band (OOB) management. The discovered servers are listed under the Connection as an In-Band (IB) or an Out-of-Band (OOB) connection.

- In-Band connections: A Server running SMS agent was discovered in the range given. The agent version is also shown.
- Out-of-Band connection: A Server with a management controller has been found in the range given.



The screenshot displays the Intel Multi-Server Manager interface. At the top, it shows the current user as Admin and options for Logout, Settings, and Help. The main area features a navigation bar with Home, Discover, Configuration, and Reports. The IP Range input field is set to From: 192.168.7.10 and To: 192.168.7.20, with an example of 192.168.1.0-192.168.1.255. The Discover button is visible. Below the input field, the Discovery Range is 192.168.7.10 to 192.168.7.20. A table titled 'Discovery 1' shows the results of the discovery:

IP Address	Connection	BMC Credentials	Agent Version	Agent Credentials	Group
localhost	IB	-	-	-	Default
192.168.7.11	IB	-	2.0	-	Default
192.168.7.13	IB	-	2.0	-	Default
192.168.7.15	OOB	-	-	-	Default

Figure 8. MSM Discovery operation

Select the Server or multiple Servers you want to manage and click on **Add**. A new form

asking for the BMC Credentials and Agent Credentials to contact the Server appears. Enter the Credentials and click on Submit. The Servers will be added to default group for further management.

Depending on the Servers discovered --either In-Band or Out-of-Band, two sets of Credentials must be entered.

- In-Band Servers. The SMS Agent credentials are needed to contact the agent. In addition, the management controller (BMC) username and password can also be added.
- Out-of-Band Servers. Only BMC credentials need to be entered.

Notes:

- If user do not have BMC credentials or do not know the credentials, you can enable BMC user and set password using Intel® Active System Console or via remote console within Multi-Server Manager if there is an SMS Agent running in the remote Server.
- Once added for management, the Servers will be moved from the discovery pane to default group of Home page. If the check-box for selecting the Server is grayed-out, it means the Server discovered is already added for management. You will not be able to add the Server again, such as localhost.

You can delete or cancel the discovery any time by clicking **Stop**.

If cancelled/stopped, the Servers discovered so far will remain in the discovery list. Once deleted the discovery range and the discovered servers will be removed from the database.

- User can start a discovery and go to any other page for monitoring or managing other Servers. Discovery will run in the background. Similarly you can logoff any time after starting a discovery. On subsequent logins you can see the discoveries in progress or finished lists.

3.3 Remote Console

MSM can launch the Remote Console for each selected server, the Remote Console is similar the Intel single server management tool – Intel® Active System console (IASC), which can help user in fine grain monitoring and trouble-shooting of the selected Server and also to configure the Server settings. The Remote Console can be accessed in both in-band and out-of-band conditions. During in-band condition the Remote console provides more information as Operating system along with the Intel agent helps in obtaining the additional information. During Out of Band condition the console provides minimal necessary information which it gets from the Baseboard Management Controller (BMC).

User can refer Intel® Active System console user guide for detailed operations of Remote Console.

4 Configuring Intel® Multi-Server Manager

This section explains configuring the MSM configuration includes MSM user setup, Email server and policies setup, Data Archives

Note: Only users with administrator privilege can configure MSM

4.1 Users

This section explains how to create, edit, and delete MSM users. User can click “Settings” button on the top of MSM window to enter user settings page.

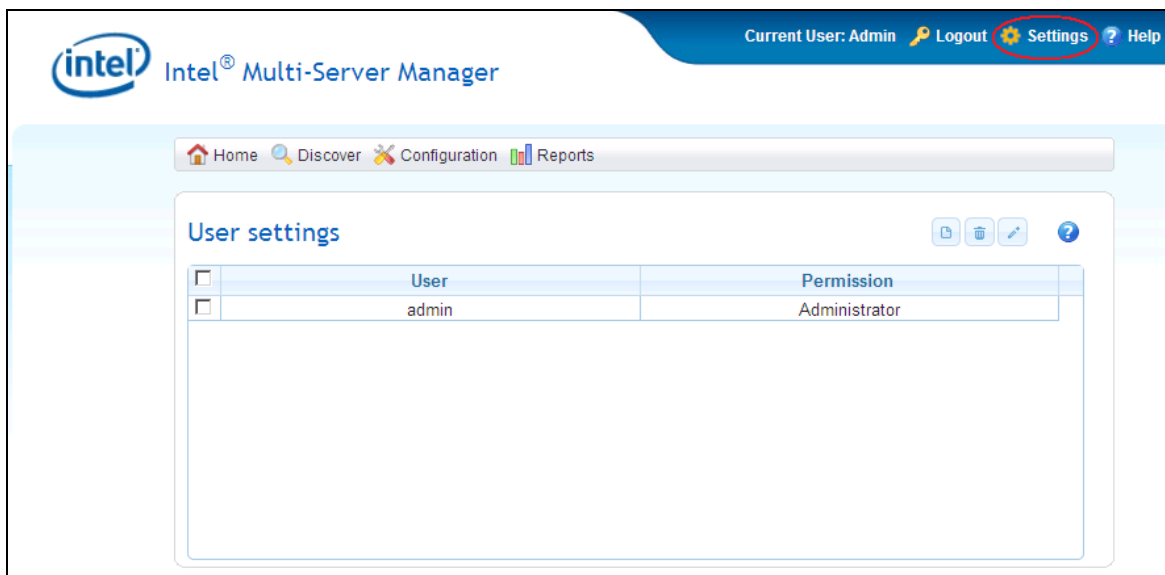



Figure 9. MSM User Settings

4.1.1 Creating a new User

1. Click on the icon  (Create New User) to extent the “Create New User” options
2. Enter the following details:
 - Username
 - Password
 - Confirm Password
 - Privileges


Choose either:

- Administrator

Or

- User
3. Click **Create** button to create the new user. Clicking **Cancel** closes the window without saving.

4.1.2 Deleting a User

To delete an already created user, select the specified user and then click on  (Delete icon). The user will get deleted.

Note: As a safety measure, the *admin* user cannot be deleted.

4.1.3 Editing a User

To edit a user, select the specified user and then click on  (Edit icon).

The Edit User window opens. Enter the required data and click on **Apply** to save the changes. For exiting the window without saving, click on **Cancel**.

4.2 Email Server

This section explains the process of email server setup, user can click the menu **Configuration** -> **Mail Server** to enter Mail Server setup page.

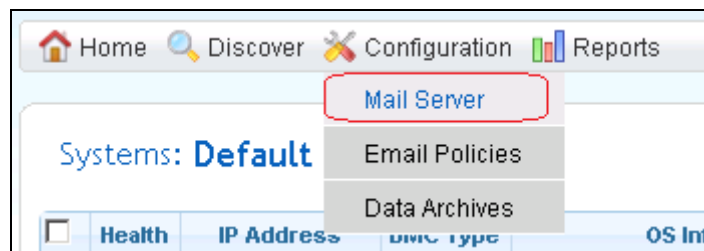




Figure 10. MSM Email Server configuration

4.2.1 Creating a New Mail Server

1. To create a new Mail server click on  (Create New) icon. The New Mail Server Configuration menu opens.
2. Enter the following details:
 - Name
 - Mail server Address
 - Mail ID (email account user name)
 - Mail Password (email account password)
 - Confirm Password
3. Click **Create** to create the new mail server. Else click on **Cancel** to close the window without saving.


Once the Mail server is created, the name, mail server address, and mail ID are displayed.

4.2.2 Deleting an already created mail server

Select the specified mail server to delete and then click on  (Delete icon). The mail server gets deleted.

Note: As a safety measure, the *admin* user cannot be deleted.

4.2.3 Editing a mail server

1. Select the mail server to edit and then click on the  (Edit icon). The Edit Mail server window opens.
2. Enter the required data and click on **Apply** to save the changes. Else click on **Cancel** to exit the window without saving.

4.3 Email Policies

This section explains the process of email alert policies setup, user can click the menu **Configuration** -> **Email Policies** to enter Email alert policy setup page.

Email alert policy can define what kind of events and what kind of severity events can trigger alert email.

The events types include:

Application	Configuration Alerts	Cooling
Memory	Misc	OS Boot Events
Peripheral Components	Power	Power State
Processor	Security	


The events severity includes: Critical, Warning and All (critical and warning)

By default, in the email policies, two email configurations are pre-created for ease of use. They are

- All Events (Default-1)
- All Critical Events (Default-2).

These are disabled by default.


4.3.1 Editing Email Alert Policy

1. Select any of the default policies and then click on the  (Edit icon) to edit the Email configuration.
2. Mark the check box for Enable to enable the email configuration.
3. Enter the Recipient ID (email address of receiver).
4. Select the already configured mail server.
Note: User needs to create mail server before email alert configuration.
5. In the Groups column, select the Group for which the email health alerts are required.

6. In the Alerts column, select either Critical Only, or Warning, or All depending on the types of alerts required.
7. Click on **Apply** to save the changes and exit. Else click **Cancel** to cancel without saving and exit.

In the main window, the email configuration status will show as enabled and the corresponding recipient email ID is listed.

4.3.2 Configuring New Email Alert Policy

1. Click on  (Create New) icon to create a new email configuration.
2. Mark the check box for Enable to enable the email configuration.
3. Enter the Recipient ID (email address of receiver).
4. Select the already configured mail server.
Note: User needs to create mail server before email alert configuration.
5. In the Groups column, select the Group for which the email health alerts are required.
6. In the Alerts column, select event severity, either Critical Only, or Warning, or All - depending on the types of alerts required.

4.3.3 Configuring Advanced Email Alert Policy

Either while creating a new email configuration or while editing, there is an option for Advanced configuration.

1. Click on the Advanced tab present on the right top corner of the same window.
2. Mark the check box for Enable to enable the email configuration.
3. Enter the Recipient Email ID (email address of receiver).
4. Select the already configured mail server.
Note: User needs to create mail server before email alert configuration.
5. In the Groups column, select the Group for which the email health alerts are required. Advanced email alert policy allows user select servers in each group.
6. Now, select the Systems under the specific group for which the alerts are required. After checking all the required systems and groups then go to the Alerts section.
7. In the Alerts column, select either Critical Only, or Warning, or All depending on the types of alerts required.
8. By default, all the alerts types are checked in the section of event types. Select the types of alerts which are required for administration based on your need.
9. Click on **Apply** to save the changes and exit, else click on **Cancel** to exit without saving.

In the main window, the email configuration status should show up as enabled and the corresponding recipient email ID listed.

4.3.4 Data Archive

Multi-Server Manager provides automatic archiving of Server events and configuration data periodically. This is to prevent the database from exceeding 1GB over a period of MSM usage.

Automatic archiving starts when the database size reaches 1GB. Entire Network summary (System Summary of all Servers in all Groups) along with events of each Server that are in closed state are archived to a file. All the events that are archived are purged from the database to reduce database size leaving only the latest 100 open events for each Server in the database.

Users can access the archive files under the Configuration→Data Archives page. The entire data is stored in html format

The schema of the archive is as follows:

```
<ActionLog>
  <Row>
    <Description></Description>
    .....
  </Row>
  <Row>
  </Row>
</ActionLog>
<SystemInfo>
  <Row>
    <GUID></GUID>
    .....
  </Row>
</SystemInfo>
```

Note: The archive files are not deleted during uninstallation. It is the User's responsibility to manage these files according to their data archival policies. To find the files to delete, go to

- Microsoft* Windows "C:\program files\intel\ASC\"
- Linux* " /usr/local/asc/bin".

5 Reports

This section explains the process of generate reports by the MSM. The report types include server assert information, server event log, server critical event log, server sensors reading and Server Configuration. MSM can generate reports for group of servers with HTML and CSV format.

Enter MSM report generation by clicking "Reports" menu at the tool-bar of MSM home page.

The screenshot shows the 'Report Generation' interface in the MSM application. The top navigation bar includes 'Home', 'Discover', 'Configuration', and 'Reports'. The main content area is titled 'Report Generation' and contains three steps:

- Step 1: Select Groups**: A table with a checked checkbox and the text 'Group Names'. Below it, a table lists 'Default' with a checked checkbox.
- Step 2: Select Systems**: A table with a header 'Systems' and three rows: 'localhost', '192.168.7.15', and '192.168.7.13', each with an unchecked checkbox.
- Step 3: Select Report Types**: A table with columns 'Name' and 'Description'. It lists five report types: 'Asset Info', 'All Events', 'Critical Events', 'Sensor Values', and 'Server Configuration', each with an unchecked checkbox.

At the bottom right, there is a 'Step 4: Export to:' section with three buttons: 'HTML', 'CSV', and 'Email'.

Figure 11. MSM Report generation

1. Select groups
2. Select server system in the selected group that user want to get their reports
3. Select the report types
4. Select "HTML" or "CSV" format. MSM can generate report with relative format and remind user to save the report.
5. User can select "Email" button to send report to user's email box directly.

6 Security Features

The Intel® Multi-Server Manager (MSM) 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.
- MSM 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 MSM 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 Microsoft Windows* Installation

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

1. 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.
2. Go to application installation directory (%ProgramFiles%\Intel\ASC\ in default case) and go inside conf folder.
3. Replace lighttpd.crt with your valid certificate. If the name is different rename it to lighttpd.crt.
4. Replace the private key file, lighttpd.pem with your private key file.
5. Set all the permissions of the key file to only Administrator. No other users should be able to read or write this file.
6. Set the permissions of the lighttpd.pem to read-write for Administrator and read-only for other users.
7. 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.
8. Restart the web-service *IASCServiceManager* from the Service window.

Replacing Certificate in Linux* Installation

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

7. After installation, shut down the web-server for Certificate replacement.
`/etc/init.d/lighttpd stop.`
8. Go to the folder `/etc/lighttpd/` and replace `lighttpd.crt` with your valid certificate. If the name is different rename it to `lighttpd.crt`.
9. Replace the private key file, `lighttpd.pem` with your private key file.
10. 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

11. 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.
 12. Restart the web-server
`/etc/init.d/lighttpd start`
- MSM 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 9393 to other number by editing the `/etc/lighttpd/lighttpd.conf` for Linux version and `%ProgramFiles%\Intel\ASC\conf\lighttpd-inc.conf` for Windows version and restarting the web-service.
 - MSM uses TCP port 7777 for the communication with its Agent or Intel® Active System Console (IASC).
 - MSM 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

MSM 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.

6.1 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 MSM and BMC user accounts, make them strong enough to minimize your risk that someone could guess the passwords and thus use the MSM to change the server configuration or interrupt its power/temperature controls. MSM 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 MSM 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.