



Supermicro Server Manager User's Guide

Revision 2.0

The information in this USER'S GUIDE has been carefully reviewed and is believed to be accurate. The vendor assumes no responsibility for any inaccuracies that may be contained in this document, makes no commitment to update or to keep current the information in this manual, or to notify any person organization of the updates. Please Note: For the most up-to-date version of this manual, please see our web site at www.supermicro.com.

Super Micro Computer, Inc. ("Supermicro") reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software, if any, and documentation may not, in whole or in part, be copied, photocopied, reproduced, translated or reduced to any medium or machine without prior written consent.

DISCLAIMER OF WARRANTY ON SOFTWARE AND MATERIALS. You expressly acknowledge and agree that use of the Software and Materials is at your sole risk. FURTHERMORE, SUPER MICRO COMPUTER INC. DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE SOFTWARE OR MATERIALS IN TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY SUPER MICRO COMPUTER INC. OR SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. SHOULD THE SOFTWARE AND/OR MATERIALS PROVE DEFECTIVE, YOU (AND NOT SUPER MICRO COMPUTER INC. OR A SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE) ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICE, REPAIR, OR CORRECTION.

LIMITATION OF LIABILITY. UNDER NO CIRCUMSTANCES INCLUDING NEGLIGENCE, SHALL SUPER MICRO COMPUTER INC. BE LIABLE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES THAT RESULT FROM THE USE OR INABILITY TO USE THE SOFTWARE OR MATERIALS, EVEN IF SUPER MICRO COMPUTER INC. OR A SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any disputes arising between manufacturer and customer shall be governed by the laws of Santa Clara County in the State of California, USA. The State of California, County of Santa Clara shall be the exclusive venue for the resolution of any such disputes. Super Micro's total liability for all claims will not exceed the price paid for the hardware product.

Manual Revision: 2.0
Release Date: 12/26/2019

Unless you request and receive written permission from Super Micro Computer, Inc., you may not copy any part of this document.

Information in this document is subject to change without notice. Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.

Copyright © 2019 Super Micro Computer, Inc.
All rights reserved.
Printed in the United States of America

Revision History

Date	Rev	Description
Sep-10-2014	1.0	<ol style="list-style-type: none">1. Initial document.
Dec-12-2014	1.0a	<ol style="list-style-type: none">1. Added support for SSM REST API.2. Added RHEL 7.x and SLES 12.x into system requirements.3. Added online installation of VNC applet on SSM Web.4. Changed some figures.5. Combine FRU into Power Supply type in the System Information.
Jan-23-2015	1.0b	<ol style="list-style-type: none">1. Changed “Check OOB Support” service to “Check SUM Support” service.2. Changed wording from “SMCI Key” to “Node Product Key”.3. Changed wording from “OOB product key” to “SFT-OOB-LIC key”.4. Added support for changing command arguments for selected services.5. Added systemctl supports for SSM services.6. Changed SSM product key activation and deactivation.
Apr-7-2015	1.1	<ol style="list-style-type: none">1. Added support for more REST API functions.2. Added online update for SUM package on SSM Web.3. Added support for configuring SuperDoctor 5 Port and IPMI MAC Address for host properties.4. Improved the user interface of notification options in the Host Properties dialog box.5. Added support for SSM to access the Windows version of SUM.6. Added support for SSM to monitor the memory health of systems installed with Windows.
May-15-2015	1.2	<ol style="list-style-type: none">1. Added a chapter for SSM notification.2. Added support for contacts to configure their “SNMP Trap Receivers” on SSM Web.3. Changed the version of Microsoft SQL supported in SSM to v2008 and above.4. Changed the service names for agent-managed hosts and IPMI hosts.5. Added an appendix for configuring MSSQL isolation levels.
Jun-18-2015	1.2a	<ol style="list-style-type: none">1. Added support for contacts to configure “OS Event Log”.2. Added more macro definitions.

		3. Added support for LSI MegaRAID 3108.
Aug-28-2015	1.2b	<ol style="list-style-type: none"> 1. Modified the steps of the Add Service Wizard. 2. Changed the VNC applet to a VNC viewer. 3. Added "IPMI SEL Health" services for IPMI hosts. 4. Added a web command to change user account and password for agent-managed hosts. 5. Added Compact View and All View for System Info on SSM Web. 6. Modified the password field on SSM Web to hide user password. 7. Changed the built-in JRE version in SSM from JRE 6 update 43 to JRE 8 update 60. 8. Added LSI MegaRAID driver limitation for the monitoring of RAID health. 9. Changed some figures.
Oct-30-2015	1.2c	<ol style="list-style-type: none"> 1. Added limitations for ChangeJVM utility. 2. Changed some figures.
Dec-11-2015	1.3	<ol style="list-style-type: none"> 1. Added a chapter about OS deployment. 2. Added support for configuring the SSM server addresses. 3. Changed some figures.
Api-29-2016	1.4	<ol style="list-style-type: none"> 1. Changed the support of database and web browser. 2. Upgraded the InstallAnywhere program to pack SSM and changed the installer interfaces. 3. Changed built-in JRE version to JRE 8 update 92. 4. Renamed some SUM web commands on SSM Web. 5. Added the support for TPM 1.2 provision and the Edit DMI Info functions for SUM web commands. 6. Added the chapters about Task View and Task Command. 7. Added the function of auto screen capture when the OS deployment task is failed.
May-20-2016	1.4a	<ol style="list-style-type: none"> 1. Added an option for DNS name preference in Host Discovery Wizard. 2. Added the Resolve Host Name command in the Host admin commands.
Jun-6-2016	1.5	<ol style="list-style-type: none"> 1. Changed the hardware requirements. 2. Changed user role configurations. 3. Added a matrix for user role feature support. 4. Added support for LDAP and AD integrations.

Oct-14-2016	1.6	<ol style="list-style-type: none"> 1. Added a new chapter about Service Calls. 2. Added support for SSM to deploy ESXi 6 update 2 and ESXi 5.5 to the managed system. 3. Replaced with some new figures. 4. Distinguished problem alert and recovery alert from notification alerts. 5. Added stunnel support for screen captures when failing to deploy OS on the target host with BMC 3.x FW. 6. Changed the "Add Host Group" web command to be two web commands "Add Logical Host Group" and "Add Physical Host Group". 7. Changed the built-in JRE version to JRE 8 update 102.
Dec-23-2016	1.6a	<ol style="list-style-type: none"> 1. Changed the figures in which date and time format are changed. 2. Added the "Sync Node PK" web command. 3. Added support for trigger setting, level 1/level 2 recipients, alert history, alert report and a test command in Service Calls. 4. Added the "Copy From" support for contractor, customer, and recipients in Service Calls. 5. Changed the message contents of a Service Calls alert. 6. Changed the built-in JRE version to JRE 8 update 112.
Mar-2-2017	1.6b	<ol style="list-style-type: none"> 1. Changed some figures. 2. Added related web commands in the command area for services while using a Service View.
May-4-2017	1.6c	<ol style="list-style-type: none"> 1. Changed some figures. 2. Refined Service Calls function. 3. Fixed typo in Server Address page. 4. Changed the built-in JRE version to JRE 8 update 121.
May-18-2017	1.6d	<ol style="list-style-type: none"> 1. Replaced SFT-OOB-LIC Activation with Node PK Activation.
Jun-22-2017	1.6e	<ol style="list-style-type: none"> 1. Changed TPM 1.2 module to TPM module.
Aug-3-2017	1.7	<ol style="list-style-type: none"> 1. Changed the built-in JRE version to JRE 8 update 141. 2. Added the "Check Now" web command for all hosts and services. 3. Added the "Change Arguments" web command for "IPMI SEL Health" service. 4. Added the notification periods for hosts, services, and contacts. 5. Added Windows Server 2016 64-bit to the supported OS list. 6. Renamed "View Detail" web command to "View Details."

Sep-14-2017	1.7a	<ol style="list-style-type: none"> 1. Added the support for keeping each triggered item tracked in a Service Call. 2. Added recovery messages in Alert Format for Service Calls. 3. Added the "Auto-update SystemInfo Data" for Service Calls. 4. Changed node product key used in Service Calls. 5. Changed the file structure in SSM MIB files.
Oct-19-2017	1.7b	<ol style="list-style-type: none"> 1. Added the "Assign Site Location" for Service Calls. 2. Changed some fields to be read-only on Edit Device Data page. 3. Added the "Control Device Options" for Service Calls. 4. Added a note for "Auto-update SystemInfo Data."
Nov-14-2017	1.7c	<ol style="list-style-type: none"> 1. Removed the "Apply SystemInfo Data" button. 2. Changed the scenario for "Change Arguments" of "IPMI SEL Health."
Dec-11-2017	1.7d	<ol style="list-style-type: none"> 1. Renamed "Disk Drive" to "Storage" in system information content and moved RAID information to Storage category. 2. Removed chapter 7.3.10 RAID Information.
Mar-21-2018	1.8	<ol style="list-style-type: none"> 1. Changed the implementation of "IPMI System Information" from SUM to FRU, OOB Full SMBIOS, and Supermicro BMC Redfish API. 2. Added support for "Maintenance Window" in "IPMI SEL Health" service. 3. Changed descriptions of the innoutconfig program.
May-2-2018	1.8a	<ol style="list-style-type: none"> 1. Removed the command "Download Troubleshooting Log." 2. Added support for connecting to BMC hosts when the SMC RAKP options are enabled.
Jul-25-2018	1.8b	<ol style="list-style-type: none"> 1. Removed Level 2 recipients. 2. Renamed "Level 1" to "Local Administrator" and "Level 2" to "Supermicro Service" on Service Calls pages. 3. Changed some figures. 4. Added support for acknowledging events on "ACK Events" pages.
Oct-2-2018	1.8c	<ol style="list-style-type: none"> 1. Added support for Redfish hosts. 2. Changed the way trigger items on the "Edit Trigger" page are collected from run time to the last check result of IPMI/Redfish Sensor Health. 3. Removed the SFT-DCMS-CALL-HOME product key. 4. Refined the Administration tree function and modified the related chapters in the user's guide.

		<ol style="list-style-type: none"> 5. Added support for the Discovery Warning function in the Host Discovery Wizard. 6. Renamed “IPMI ID” to “BMC ID” and “IPMI Password” to “BMC password” on SSM Web. 7. Updated the 3rd party software. 8. Added support for changing default /tmp folder for SSM Installer and Uninstaller.
Oct-31-2018	1.8d	<ol style="list-style-type: none"> 1. Changed the built-in JRE version to JRE 8 update 192. 2. Fixed typo in 3rd party software page. 3. Fixed typo in changejvm chapter.
Apr-22-2019	1.9	<ol style="list-style-type: none"> 1. Added custom scripts for contacts to execute a predefined script for notifications. 2. Added support for activating node product keys. 3. Added the function of auto-upgrading in SSM Installer GUI in interactive mode. 4. Removed Microsoft SQL from the support lists of both SSM Database and SSM dbtool utilities. 5. Changed the system requirements for hardware and browsers. 6. Removed -f option from innoutconfig program. 7. Changed some figures.
Dec-26-2019	2.0	<ol style="list-style-type: none"> 1. Added new chapters about system diagnostics and Redfish commands. 2. Changed auto-upgrading chapter. 3. Changed system requirements. 4. Allowed creating a login password for ADMIN user account when SSM is installed. 5. Added more OS supports for the OS Deployment function. 6. Changed some figures and download links.

Contents

Part 1 Background.....	19
1 SSM Overview	20
1.1 Key Features.....	20
1.2 Monitoring Functions.....	21
1.3 Control Functions.....	21
1.4 Notification Functions.....	22
1.5 System Information and Report Functions	22
1.6 SSM System Architecture.....	23
1.7 Minimum System Requirements	24
1.7.1 SSM Server, SSM Web, and SSM CLI (Management Server)	24
1.7.2 Managed System	25
1.7.3 Default TCP/UDP Ports	26
2 Setting Up SSM.....	27
2.1 Installing SSM.....	27
2.1.1 Windows Installation	27
2.1.2 Linux Installation.....	35
2.1.3 Silent Mode Installation.....	40
2.2 Activating SSM	46
2.2.1 Using Online Activation.....	46
2.2.2 Using Offline Activation	46
2.3 Verifying the Installation.....	48
2.4 Manually Controlling SSM Services.....	49
2.4.1 SSM Database Service.....	49
2.4.2 SSM Server Service.....	49
2.4.3 SSM Web Service	49
2.5 Deactivating SSM	50
2.5.1 Using Online Deactivation	50
2.5.2 Using Offline Deactivation	50
2.6 Uninstalling SSM	51
2.6.1 Uninstalling in Windows	51

2.6.2	Uninstalling in Linux.....	54
2.6.3	Silent Mode Uninstall.....	56
2.7	Using ssmlicense tool.....	57
2.7.1	-ona [product key]: Online activation.....	57
2.7.2	-ond: Online deactivation.....	57
2.7.3	-c [product key]: Create an activation request file.....	58
2.7.4	-ofa [product key] -of [specified directory]: Offline activation.....	58
2.7.5	-ofd: Offline deactivation.....	59
2.7.6	-ons: Online synchronization.....	59
2.7.7	-ofs -of [specified directory]: Offline synchronization.....	60
2.7.8	-ia: Check if product activated.....	60
2.8	Auto-Upgrading in Installer.....	61
2.8.1	Upgrading in Windows.....	61
2.8.2	Upgrading in Linux.....	64
2.8.3	Restoring SSM after Auto-Upgrade Fails.....	66
2.8.4	Restoring Alert History of Service Calls.....	68
Part 2 SSM Server.....		69
3	SSM Server Configurations.....	70
3.1	SSM Server Operational Concept.....	70
3.2	Configuring the SSM Server with Files.....	71
3.3	SSM Server Configuration Objects.....	73
3.3.1	Instance Definitions.....	73
3.3.2	Host Definitions.....	77
3.3.3	Host Group Definitions.....	83
3.3.4	Service Definitions.....	85
3.3.5	Contact Definitions.....	88
3.3.6	Contact Group Definitions.....	91
3.3.7	Command Definitions.....	92
3.3.8	Time Period Definitions.....	92
3.3.9	PTPolicy Definitions.....	93
3.3.10	The Use Attribute.....	98

3.4	Macros	99
4	SSM Server Built-in Commands	103
4.1	check_ftp	103
4.2	check_http	104
4.3	check_ipmi	104
4.4	check_ping	107
4.5	check_smtp	108
4.6	check_wol	109
4.7	jcheck_nrpe	110
Part 3 SSM Web		112
5	SSM Web Overview	113
5.1	Logging in to SSM Web	113
5.2	SSM Web Layout	114
6	SSM Web Administration Page	117
6.1	Administration Page Overview	117
6.2	Monitoring Setup	118
6.2.1	Delete a Host	119
6.2.2	Assign a Host Group	120
6.2.3	Add Service Wizard	122
6.3	Host Group Management	130
6.3.1	Adding Host Groups	130
6.3.2	Editing a Host Group	132
6.3.3	Deleting Host Groups	133
6.3.4	Assigning Host Members	134
6.3.5	Assigning Host Group Members	135
6.4	Contact Management	137
6.4.1	Adding a Contact	137
6.4.2	Editing a Contact	138
6.4.3	Editing Host Notifications for One Contact	138
6.4.4	Editing Host Notifications for Multiple Contact	140
6.4.5	Editing Service Notifications for One Contact	144

6.4.6	Editing Service Notifications for Multiple Contacts	146
6.4.7	Example of Simple Custom Script	149
6.5	Contact Group Management	151
6.5.1	Adding a Contact Group.....	151
6.5.2	Editing a Contact Group.....	152
6.5.3	Deleting a Contact Group	152
6.5.4	Assigning Members.....	154
6.6	Node PK Activation	155
6.7	User Roles	160
6.7.1	Adding a User.....	163
6.7.2	Editing a User	164
6.7.3	Deleting a User.....	165
6.8	Directory Services	166
6.8.1	Configuring Directory Services.....	167
6.8.2	Configuring User and Group Search Criteria.....	174
6.9	Software Update.....	178
6.9.1	Uploading a VNC Viewer.....	178
6.9.2	Updating Site.....	179
6.9.3	Updating SUM.....	179
6.10	E-Mail SMTP Setup.....	181
6.11	DB Maintenance	182
6.12	Server Address	183
6.13	System Events	184
6.14	About SSM	185
6.15	Host Discovery Wizard	186
7	SSM Web Monitoring Page	193
7.1	Navigation Area	193
7.2	Working Area	194
7.2.1	Monitoring Overview.....	194
7.2.2	Host View	195
7.2.3	Service View	196

7.2.4	ACK Events	196
7.2.5	Task View	203
7.2.6	Host Group View	205
7.3	Command Area	206
7.3.1	Agent Managed Commands	206
7.3.2	IPMI Commands.....	209
7.3.3	Power Management Commands	211
7.3.4	System Information Commands	212
7.3.5	Remote Control Commands	214
7.3.6	Host Admin Commands	218
7.3.7	Report Commands	224
7.3.8	Service Admin Commands	226
7.3.9	Task Commands	238
7.3.10	Redfish Commands	241
7.4	Notifications.....	243
7.4.1	Alert Events.....	243
7.4.2	Alert Receivers	244
7.4.3	Alert Format.....	245
7.4.4	Supermicro MIB	246
8	SSM Web Reporting Page	247
8.1	SSM Server Report.....	247
8.1.1	Server Availability Report	247
8.1.2	Server Detailed Report.....	248
8.1.3	History Report.....	249
8.2	Host Report.....	250
8.2.1	Host Availability Report	251
8.2.2	Single Host Status Report	252
8.2.3	Single Host with Services Status Report	253
8.2.4	Host Status Detailed Report	254
8.3	Service Report.....	255
8.3.1	Service Availability Report	255

8.3.2	Single Service Status Report	256
8.3.3	Service Status Detailed Report	257
9	Power Management	258
9.1	Power Management in SSM	258
9.2	Power Consumption Trend	260
9.2.1	Power Consumption Trend of Individual Hosts	260
9.2.2	Power Consumption Trend of a Group of Hosts.....	261
9.3	Power Policy Management	262
9.3.1	Host Policies.....	262
9.3.2	Host Group Policies.....	265
9.3.3	Policy Conflicts	269
9.4	Power Management Events.....	275
9.4.1	Host Events	275
9.4.2	Host Group Events	276
10	SUM Integration.....	277
10.1	SUM in SSM.....	277
10.2	Activating an IPMI Host.....	279
10.2.1	Checking Activation Status.....	279
10.2.2	Collecting MAC Addresses	280
10.2.3	Activating Node Product Keys of IPMI Hosts	281
10.3	SUM Services.....	283
10.4	SUM Web Commands	285
11	OS Deployment	290
11.1	OS Images	294
11.1.1	Uploading an ISO File.....	295
11.1.2	Checking Image Status	296
11.1.3	Deleting an ISO File	296
11.2	Answer File.....	297
11.2.1	Attributes in Template Answer Files.....	298
11.2.2	Adding an Answer File	301
11.2.3	Editing an Answer File.....	303

11.2.4	Deleting an Answer File	305
11.3	Deployment Progress.....	306
11.4	Installing Stunnel	309
12	Service Calls	311
12.1	Service Calls Configurations.....	312
12.1.1	Setup Management	312
12.1.2	Customer Management.....	329
12.1.3	Recipient Management.....	333
12.1.4	Site Management.....	336
12.2	Service Calls Alerts	340
12.2.1	Alert Events.....	340
12.2.2	Alert Receivers	341
12.2.3	Alert Format.....	341
12.2.4	Alert History	342
12.2.5	Alert Report	344
13	System Diagnostics	347
13.1	Prerequisites	347
13.2	Diagnosing Multiple Redfish Hosts	347
13.3	Diagnostic Progress.....	350
13.3.1	Diagnostic Report.....	351
13.4	Updating Diagnostic Software	357
Part 4 SSM CLI	359
14	SSM CLI.....	360
14.1	SSM CLI Overview	360
14.2	Using SSM CLI.....	361
14.2.1	Interactive Mode	361
14.2.2	Batch Mode.....	362
14.3	Common Arguments.....	363
14.4	Health Command	364
14.4.1	–h: Display health command arguments	364
14.4.2	–a: Use default thresholds to check all enabled health items.....	365

14.4.3	-a -x [index 1, index 2, ...]: Use default thresholds to check all enabled health items excluding those specified in the -x argument	366
14.4.4	-t: Display the name and reading of each health item.....	367
14.4.5	-t a -n [index] -ll [low limit] -hl [high limit]: Display a health item status with the specified item number as well as high and low limits.	369
14.5	IPMI Command	370
14.5.1	-h: Display IPMI command arguments.....	370
14.5.2	-a: Use default thresholds to check all enabled health items.....	371
14.5.3	-cr: Cold reset a BMC.....	371
14.5.4	-dul: Stop blinking UID LED	371
14.5.5	-eul: Blink UID LED.....	372
14.5.6	-l: Display all of monitored items and index	372
14.5.7	-n [index] -ll [low limit] -hl [high limit]: Display a health item status with the specified item number as well as high and low limits.....	373
14.6	Power Command	374
14.6.1	-h: Display power command arguments.....	374
14.6.2	-a -s: Shutdown hosts via SD5	375
14.6.3	-a -r: Reboot hosts via SD5	375
14.6.4	-a -p: Power up hosts via Wake on LAN (WOL)	376
14.6.5	-b -s: Shutdown hosts via IPMI	376
14.6.6	-b -r: Reboot hosts via IPMI.....	376
14.6.7	-b -p: Power up hosts via IPMI	377
14.6.8	-s: Shutdown hosts by IPMI or SD5	377
14.6.9	-r: Reboot hosts by SD5 or IPMI.....	377
14.6.10	-p: Power up hosts by WOL or IPMI	377
14.7	Status Command.....	378
14.7.1	-h: Display status command arguments	378
14.7.2	-G: Display host group status	378
14.7.3	-H: Display host status.....	379
14.8	List Command	380
14.8.1	-h: Display list command arguments.....	380

14.8.2	–ag: List all host groups	381
14.8.3	–ah: List all hosts.....	381
14.8.4	–G: List members of a host group.....	382
14.8.5	–H: List host groups of hosts.....	382
14.9	Systeminfo Command.....	383
14.9.1	–h: Display systeminfo command arguments.....	383
14.9.2	–l: Display system information types and index.....	383
14.9.3	–n: Display system information	384
14.10	Env Command.....	384
14.10.1	–h: Display env command arguments	384
14.10.2	–s: Display current data source setting	385
14.11	Storage Command	385
14.11.1	–h: Display storage command arguments	385
14.11.2	–n: Check the total number of hard drives.....	386
14.11.3	–s: Check the hard disks status with SMART	386
14.11.4	–r: Check the RAID status	387
14.12	Memory Command.....	388
14.12.1	–h: Display memory command arguments.....	388
14.12.2	–m: Check memory health by counting the number of CECC error events.....	388
14.12.3	–M: Check memory health by counting the number of UECC error events.....	390
Part 5	Advanced Topics.....	392
15	SSM Utilities.....	393
15.1	Export and Import Configuration Data	393
15.2	Using DBTool to Setup an SSM Database	396
15.3	Using ChangeJVM to Change a Java VM.....	400
16	SSM Certification	402
16.1	Introduction	402
16.2	Installing an SSM Certificate	403
16.2.1	Windows Graphic Mode	403
16.2.2	Linux Text Mode	407
16.3	Generating a Certification.....	407

16.3.1	Help Information.....	407
16.3.2	Generating key pairs for SSM Server and SD5.....	407
16.3.3	Overwriting Default Password for SD5.....	408
16.4	Using Customized Certification when Installing SSM and SD5.....	409
16.4.1	Windows.....	409
16.4.2	Linux.....	410
16.5	Manually Replacing SSM Server Certification.....	412
16.6	Manually Replacing the SD5 Certification.....	412
Part 6 Appendices.....		413
A.	Log Settings.....	414
B.	Third-Party Software.....	416
C.	Uncorrectable ECC Errors.....	420
Contacting Supermicro.....		423



Part 1 Background

1 SSM Overview

SSM (Supermicro Server Manager) is a server management system designed for optimizing the management of servers designed by Super Micro Computer, Inc. (“Supermicro”). SSM monitors both hosts (servers, computers, network devices and managed nodes) and the services running on the hosts.

1.1 Key Features

- Supports monitoring, control, and management functions.
- Streamlines integration with IPMI and Redfish¹ management.
- Power management via the Intel® Intelligent Power Node Manager (NM).
- BIOS and BMC firmware management via the Supermicro Update Manager (SUM).
- Easy to use Web-based and command line interfaces.
- Easy to customize:
 - Pluggable hardware and software monitoring plug-ins.
 - Compatible with Nagios plug-ins.
- Supports Windows and Linux platforms.
- Supports role-based access control.
- Supports host, service, event, system information queries, BIOS image, BMC firmware, BIOS settings and BMC configuration updates in REST API².
- Supports installations of Linux OS (RHEL, Ubuntu, CentOS, SLES and VMware ESXi) on the managed systems.

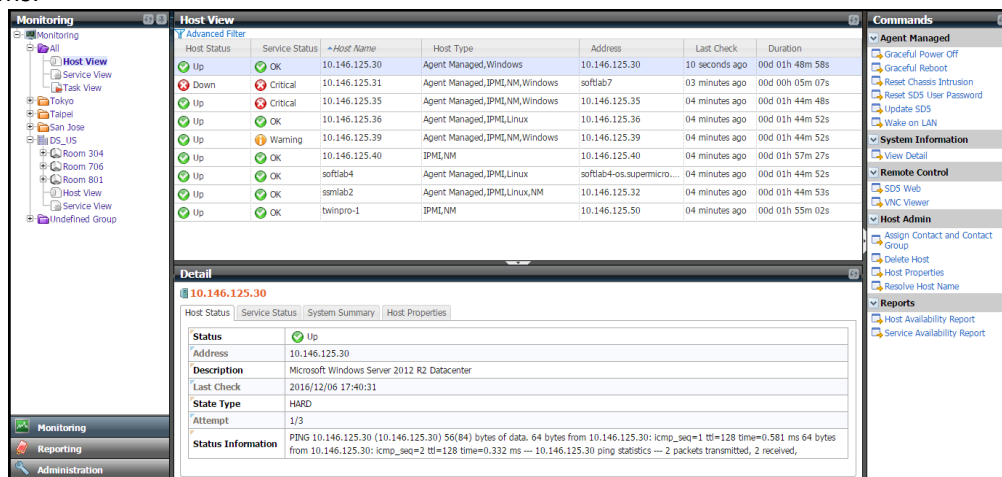


Figure 1-1: SSM Web-based Console

¹In addition to IPMI, SSM supports the Redfish protocol, which is designed to be the management standard of the next generation. SSM also supports SMC RAKP authentication with BMC, which is a stronger hash option designed by Supermicro for standard RAKP.

²To use SSM REST API in your own application, please refer to *SSM REST API Developer's Guide* or the documentation on SSM Web ([https://\[SSM Web address\]:8443/SSMWeb/api/documents](https://[SSM Web address]:8443/SSMWeb/api/documents)).

1.2 Monitoring Functions

- Host Monitoring: Agent Managed, Agentless, IPMI, and Redfish hosts.
- Hardware Monitoring: fan speed, temperature, voltage, chassis intrusion, redundant power failure, power consumption, disk health, raid health, and memory health.
- Software Monitoring: HTTP, FTP, and SMTP services.
- State Control: Supports hard state and soft state to avoid false alarms.

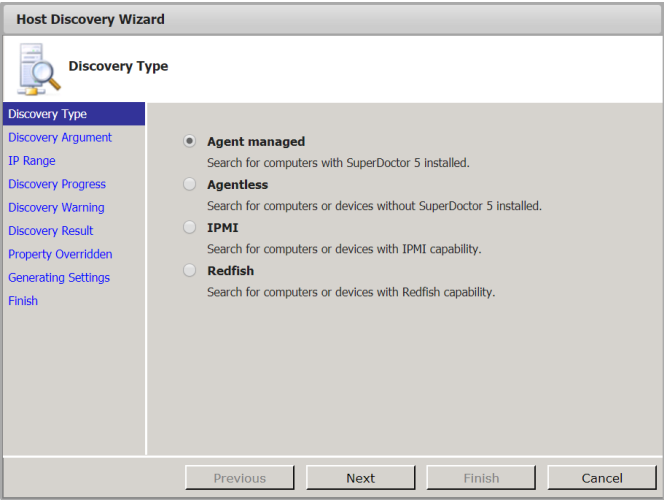


Figure 1-2: Host Discovery Wizard guides users on how to add hosts to be monitored

1.3 Control Functions

- Remote console redirection: VNC and iKVM via BMC Web.
- BMC Integration: BMC Web, blinking UID, and more.
- Power control and Wake-on-LAN (WOL).
- Power management: Static and dynamic power capping.
- SUM integration: BIOS and BMC management.
- Linux OS deployment.

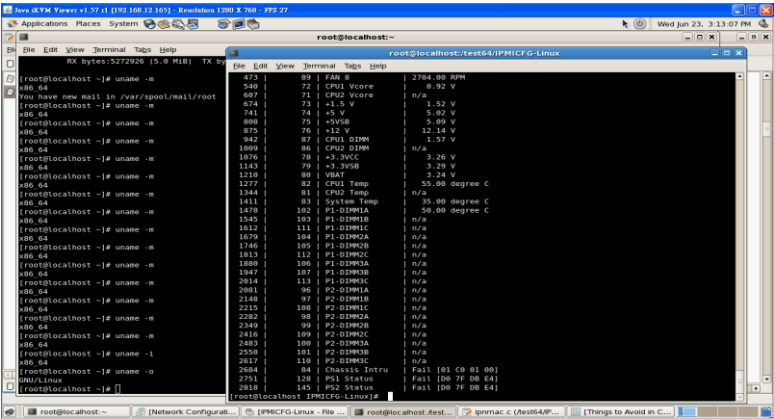


Figure 1-3: Remote Troubleshooting with iKVM via BMC Web

1.4 Notification Functions

- Notifications sent when:
 - Hosts are in a Down or Recovery state.
 - Services are in a Warning, Critical, Unknown, or Recovery state.
- Notifications sent via email.
- Notifications sent to contacts and contact groups.

1.5 System Information and Report Functions

- 20 Types of System Information³: BIOS, Baseboard, Chassis, Computer System, Disk Drives, Memory, Network, Printer, Processor, System Slot, BMC, Power Supply, Account, Operating System, Process, Service, Share, Time Zone, OEM Strings, and System Configuration Options.
- Six Report Types: SSM Server Availability, SSM Server Log, Host Availability, Service Availability, Host Status Change, and Service Status Change.

The screenshot shows a web interface for a Host Availability Report. At the top, there is a 'Host' field with the IP range '192.168.12.152-192.168.12', a 'Last Time' dropdown set to 'Last 7 Days', and 'Start Date' and 'End Date' fields set to '5/7/10' and '5/14/10' respectively. A 'Query' button is present. Below this, the 'Date Period' is 'May 7, 2010 11:24:29 AM To May 14, 2010 11:24:29 AM' with a 'Duration' of '07d 00h 00m 00s'. A language dropdown is set to 'English'. The main table has five columns: 'Host', 'Time Up', 'Time Down', 'Time Unreachable', and 'Time Undetermined'. The 'Time Up' column uses green background for 100% uptime, 'Time Down' uses red for 0% downtime, and 'Time Unreachable' uses yellow for 0% unreachable time. The 'Time Undetermined' column shows overall availability percentages.

Host	Time Up	Time Down	Time Unreachable	Time Undetermined
192.168.12.110	100% (0.4%)	0% (0%)	0% (0%)	99.6%
192.168.12.125	100% (0.4%)	0% (0%)	0% (0%)	99.6%
192.168.12.152	100% (0.1%)	0% (0%)	0% (0%)	99.9%
192.168.12.169	100% (0.4%)	0% (0%)	0% (0%)	99.6%
192.168.12.171	100% (0.4%)	0% (0%)	0% (0%)	99.6%
192.168.12.22	100% (0.6%)	0% (0%)	0% (0%)	99.4%
192.168.12.23	100% (0.6%)	0% (0%)	0% (0%)	99.4%
192.168.12.24	100% (0.6%)	0% (0%)	0% (0%)	99.4%
192.168.12.25	100% (0.6%)	0% (0%)	0% (0%)	99.4%
192.168.12.29	100% (0.6%)	0% (0%)	0% (0%)	99.4%
192.168.12.31	100% (0.1%)	0% (0%)	0% (0%)	99.9%
192.168.12.33	100% (0.1%)	0% (0%)	0% (0%)	99.9%
192.168.12.70	100% (0.4%)	0% (0%)	0% (0%)	99.6%
192.168.12.71	100% (0.1%)	0% (0%)	0% (0%)	99.9%
192.168.12.8	100% (0.4%)	0% (0%)	0% (0%)	99.6%
192.168.12.80	100% (0.4%)	0% (0%)	0% (0%)	99.6%
192.168.12.9	100% (0.4%)	0% (0%)	0% (0%)	99.6%
192.168.12.90	100% (0.4%)	0% (0%)	0% (0%)	99.6%
localhost-5.local	100% (0.6%)	0% (0%)	0% (0%)	99.4%
hw-jessy-nb.local	100% (0.1%)	0% (0%)	0% (0%)	99.9%
hw-soft-lab3.local	100% (0.1%)	0% (0%)	0% (0%)	99.9%

Figure 1-4: Observing Dependability with Host and Service Availability Reports

³ These 20 types of system information are available for Agent Managed hosts. For the types of system information available for IPMI/Redfish hosts, see 7.3.4 *System Information Commands*.

1.6 SSM System Architecture

SSM contains several key components as shown below:

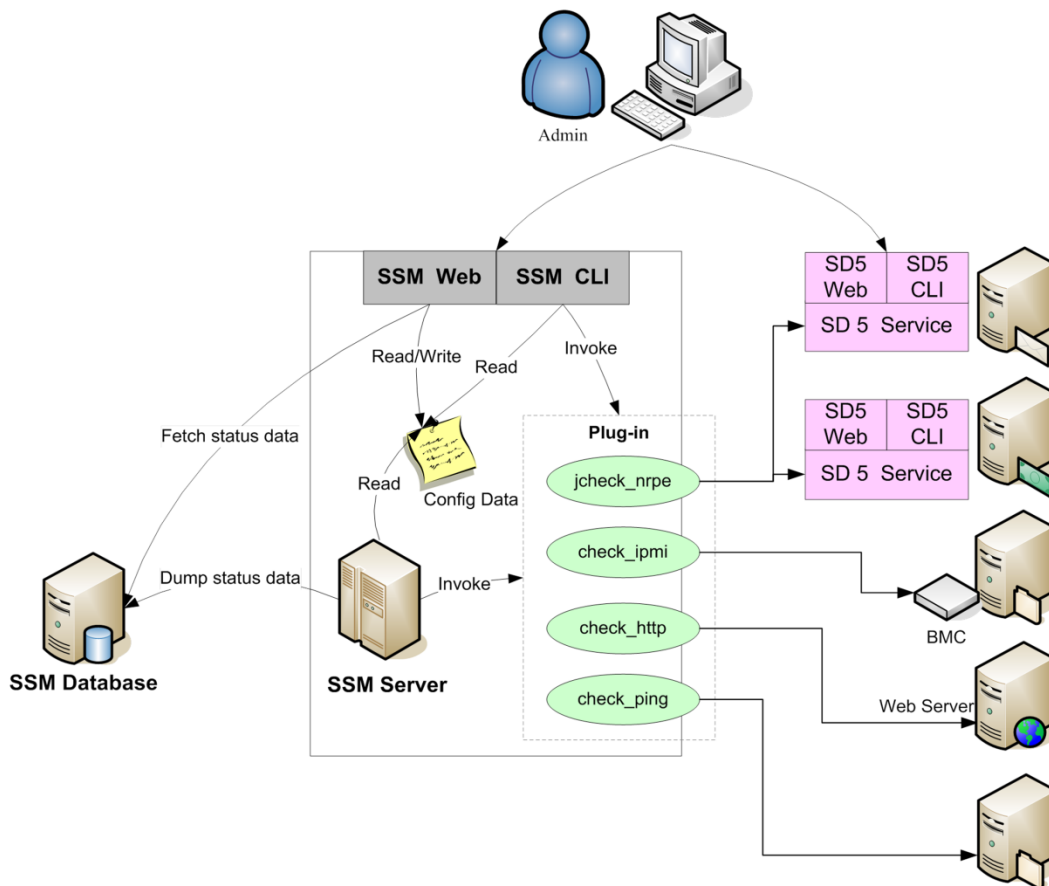


Figure 1-5: SSM System Architecture

- **SSM Server:** The SSM server is a service (a daemon) program that periodically monitors hosts and servers to check their status. It also updates the status to the SSM Database so that users can browse the information on the Web.
- **SSM Web:** The SSM Web is a service program that provides a Web-based interface for server management. Users can view hosts and services status and send commands such as power controls, and remote KVM via BMC Web to the hosts.
- **SSM CLI:** The SSM CLI is a command line interface program that supports server management in the text mode. The SSM CLI can be used interactively and can be executed in batch mode for script automation.
- **SSM Database:** SSM uses a database to store management data. A built-in PostgreSQL database is provided in the SSM Installer program.
- **SuperDoctor 5:** The SuperDoctor 5 is a service that runs on monitored hosts to provide local system health and information. Since it is designed with plug-in architecture, the monitored functions are extended by plug-ins.

-
- **BMC:** SSM is designed to be integrated with IPMI/Redfish, which is supported by Supermicro BMC equipped servers. SSM provides out-of-band management with IPMI/Redfish.
 - **Config Data:** Configuration data is a set of configuration objects (i.e., instance, host, host group, service, contact, contact group, command, timeperiod, and ptpolicy objects) that are used to model a managed environment under the control of SSM. Configuration data is used by SSM Server, SSM Web, and SSM CLI, and the data can be stored in the SSM Database and in plain text files.

1.7 Minimum System Requirements

1.7.1 SSM Server, SSM Web, and SSM CLI (Management Server)

- **Hardware**
 - 20.0 GB free disk space
 - 4 CPU cores
 - Available 16.0 GB RAM (More RAM may be needed depending on the number of the managed systems.)
 - An Ethernet network interface card



Notes:

- The free disk space depends on the number of OS images you will upload to SSM while using the OS deployment function.
- To use SSM to monitor a large number of systems, it is recommended that you contact Supermicro for assistance.
- To run SSM in a virtual machine, more CPU cores and RAMs may be needed depending on the number of the managed systems.

-
- **Operating System**
 - Red Hat Enterprise Linux Server 6.x (64-bit), 7.x (64-bit), 8.x (64-bit)
 - SUSE Linux Enterprise 12.x (64-bit)
 - Windows 2012 Server R2 64-bit
 - Windows 2016 Server 64-bit
 - Windows 2019 Server 64-bit
 - **Browser**
 - Internet Explorer 11.x or higher version
 - Firefox 45.x or higher version
 - **Screen resolution**
 - 1024 x 768 or higher resolution

1.7.2 Managed System

- **Agent-Managed Host (Running SD5):** See *1.2 Minimum System Requirements in SuperDoctor 5 User's Guide* for more information.



Notes:

- The SuperDoctor 5 function of monitoring memory health is not available on Supermicro desktop motherboards or on all Supermicro servers. Please refer to the Supermicro website for an up-to-date list of supported products.
- The SMART health status monitoring function supports non-RAID internal hard disks and does not support USB hard drives and flash disks. To use this function, install the smartctl utility first.
- The RAID health status monitoring function is available on LSI MegaRAID 2108, 2208 and 3108 controllers except for Windows drivers version MR6.6 code or higher. LSI MegaRAID 2008, LSI Fusion-MPT based and Intel Rapid Storage Technology controllers are not supported.
- The system information is platform dependent. Types of information include Desktop Monitor, Floppy, Keyboard, Port Connector, Parallel Port, Pointing Device, Serial Port, Computer Summary, Startup Command, and Video Controller. Note that this function is only supported on Windows platforms.

-
- **IPMI Host:**
 - For power management function, the managed system must have a PMBus instrumented power supply, and support Intel® Intelligent Power Node Manager (NM). For details, see *9.1 Power Management in SSM*.
 - To access most SUM functions, it is required to activate the product key. See *10.1 SUM in SSM* for more information.
 - **Redfish Host:**
 - The managed system must have a Supermicro X10 series motherboard equipped with BMC.
 - To access most Redfish functions, it is required to have the product key SFT-DCMS-Single on the BMC and provide the accounts with Administrator privileges.



Note: There are two-way communications between Redfish hosts and SSM. It is required to configure a valid server address and open ports in your firewall for SSM to receive messages from the Redfish hosts.

- For configuring a valid address, see *6.12 Server Address* for details.
- For opening ports used by SSM Web in the firewall, see *1.7.3 Default TCP/UDP Ports* for details.

1.7.3 Default TCP/UDP Ports

- **SSM Web**
 - Binds TCP port 8080 for HTTP
 - Binds TCP port 8443 for HTTPS
 - Binds for internal communications a free TCP port between 31000 and 32999
 - To use the OS deployment functions, it's required to bind more ports. See *11 OS Deployment* for details.
- **SSM Built-in Database**
 - Binds TCP port 9002
- **SSM Server**
 - Binds TCP port 5111
 - Binds TCP port 8555
 - Binds TCP port 8556
 - Binds a free TCP port between 31000 and 32999 for internal communications

2 Setting Up SSM

2.1 Installing SSM

SSM provides installers for both Windows and Linux platforms. A user can run the installers in either of two modes: GUI interactive mode and text-console mode. The text-console mode can be run with either interaction or silence.

2.1.1 Windows Installation

You must have Administrator privileges to install SSM. To install SSM in Windows, follow these steps.

1. Execute the SSM installer.
2. Click the **Next** button to continue.

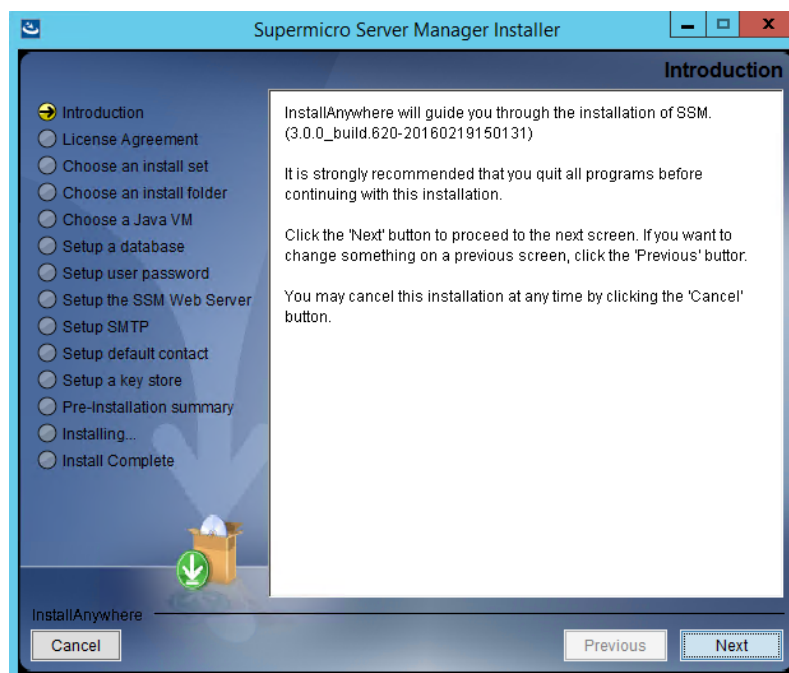


Figure 2-1

3. Accept the license agreement and click the **Next** button to continue.

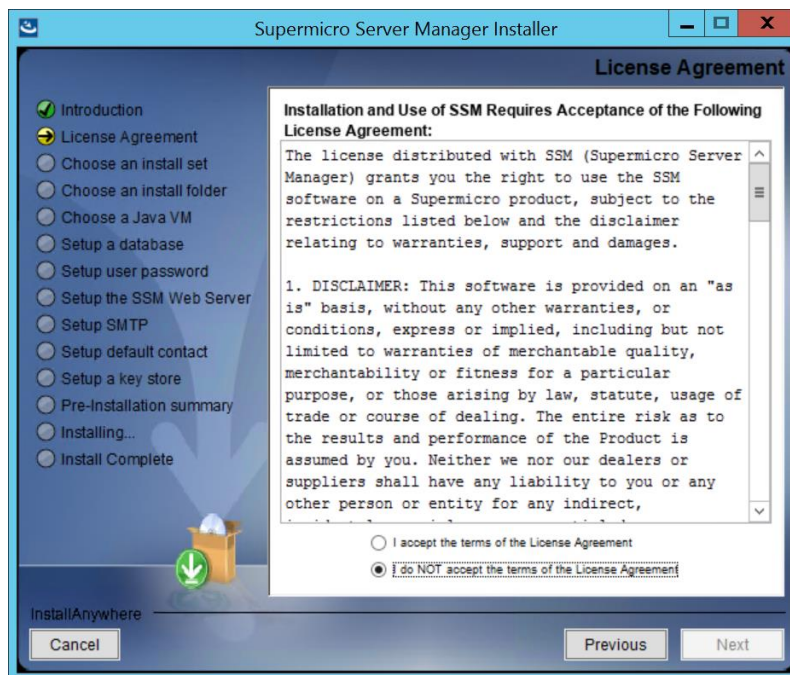


Figure 2-2

4. Select the **Install All** option and click the **Next** button to continue.

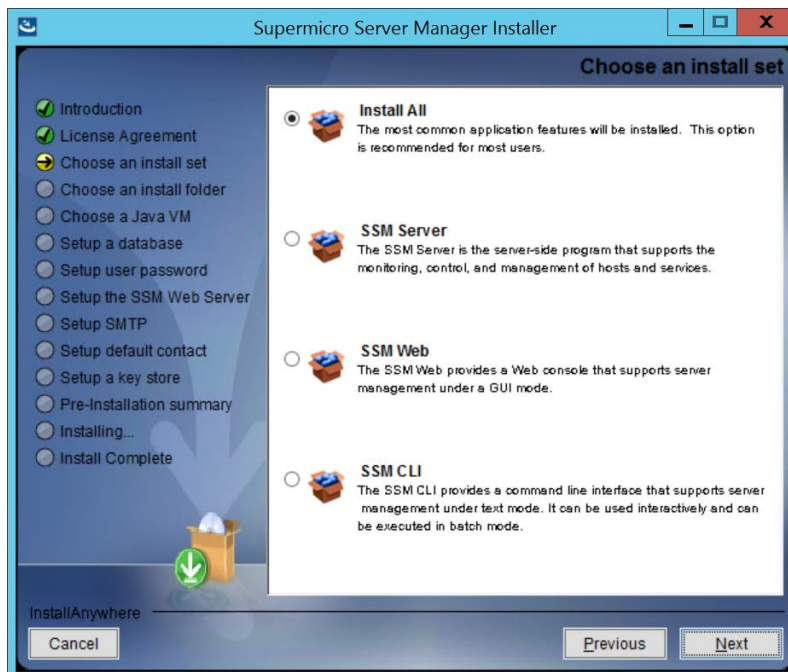


Figure 2-3

5. Select a directory to install SSM to and click the **Next** button to continue.

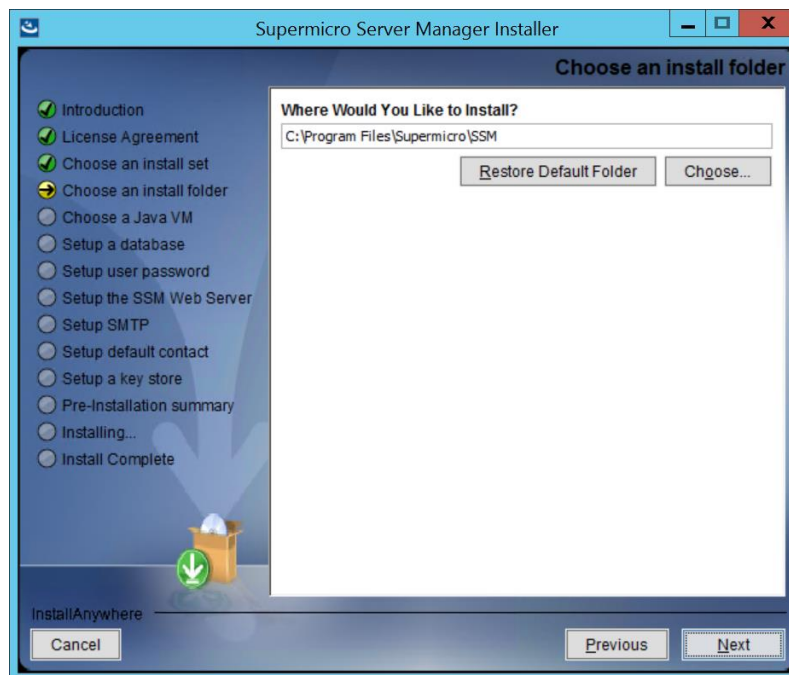


Figure 2-4

6. Use the built-in Java VM and click the **Next** button to continue.



Note: If you select “Choose a Java VM”, the architecture of the selected Java VM must be compatible with the installer. For example, to use an x86 version of SSM, you need to select an x86 version of Java VM. Also note that only JVM version newer than 1.8.0 is supported.

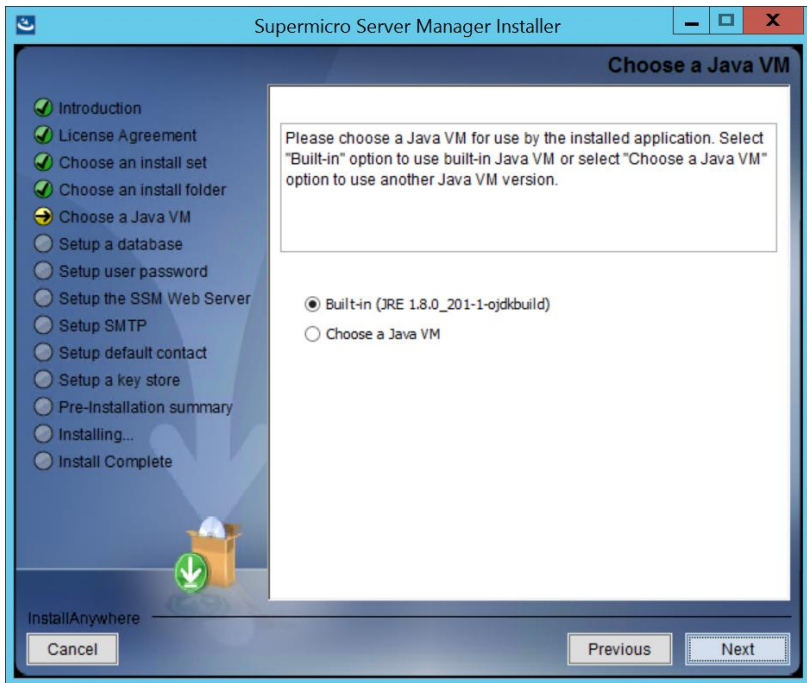


Figure 2-5

7. Use the built-in database and click the **Next** button to continue.

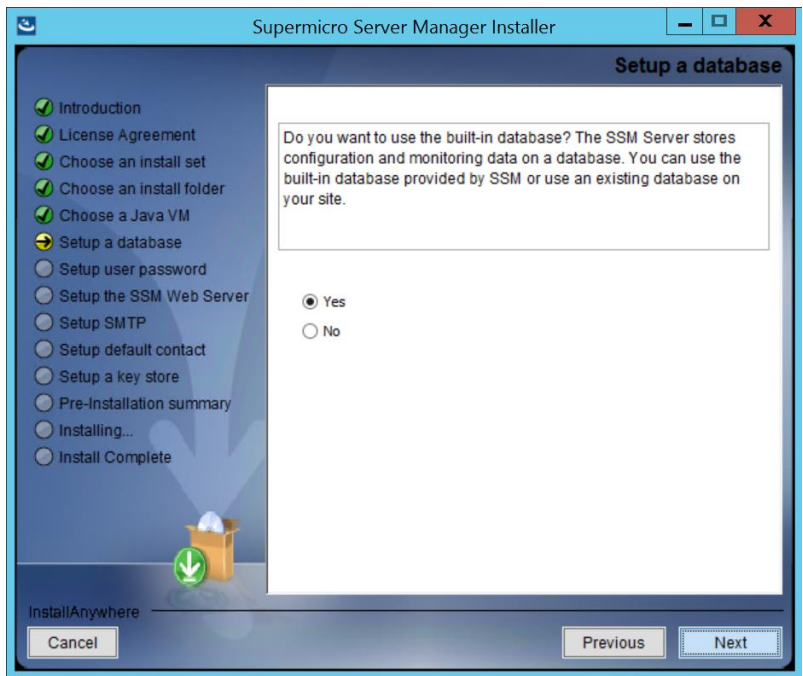


Figure 2-6

- You can configure the password for the built-in ADMIN account to access the SSM Web. When completed, click the **Next** button to continue.

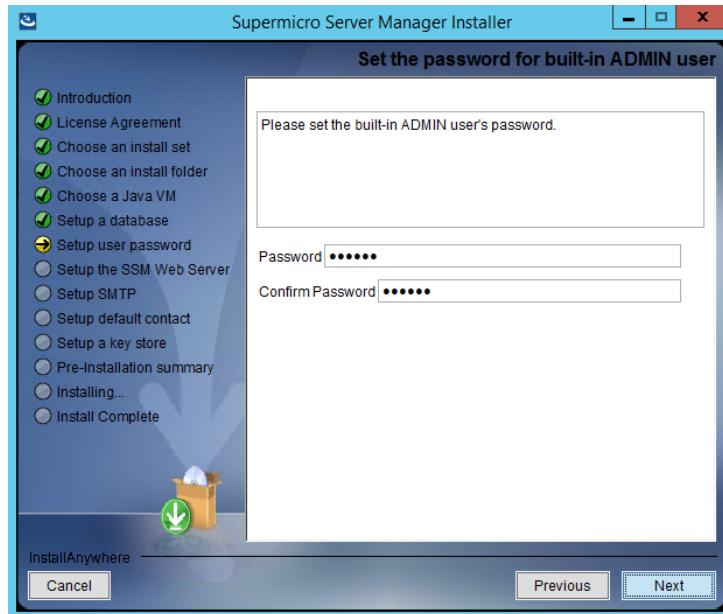


Figure 2-7

- Enter the default port numbers for HTTP and HTTPS and click the **Next** button to continue. Normally, you should accept the default values.

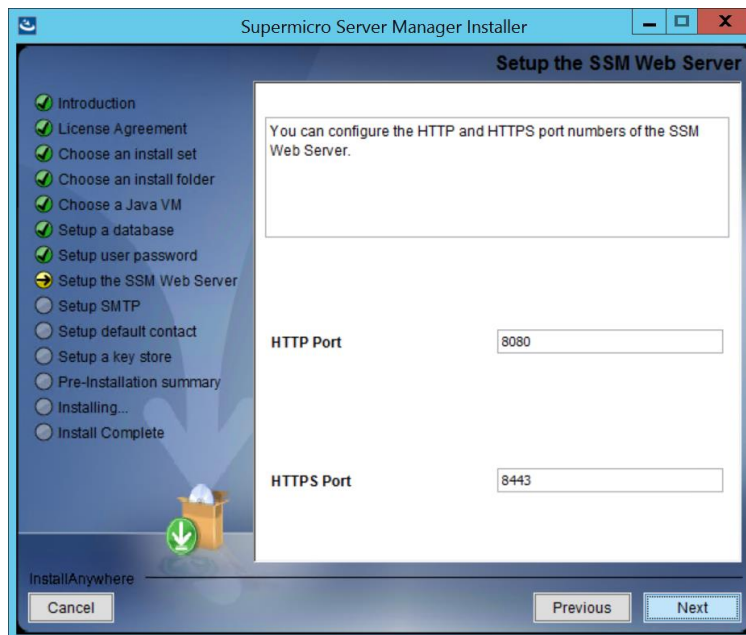


Figure 2-8

10. Enter an SMTP server, an SMTP port, a sender's email address, a user account and the password. Check SSL (Secure Sockets Layer) or TLS (Transport Layer Security) if the SMTP server uses secure connections. The data will be used by the SSM server to send notifications. When completed, click the **Next** button to continue. Note that you can modify the SMTP server settings latter on SSM Web. See *6.10 E-Mail SMTP Setup* for more information.

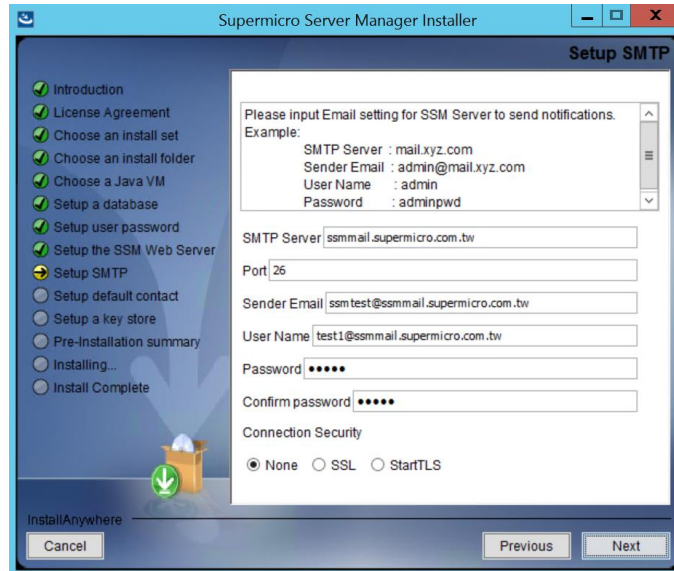


Figure 2-9

11. Enter the email address of the default contact.

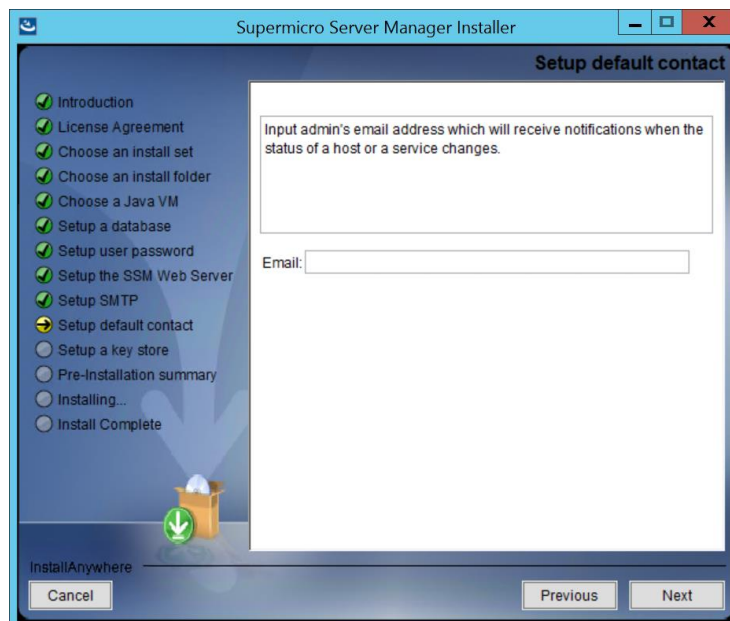


Figure 2-10

12. Select **Yes** to use the default key store and click the **Next** button to continue.

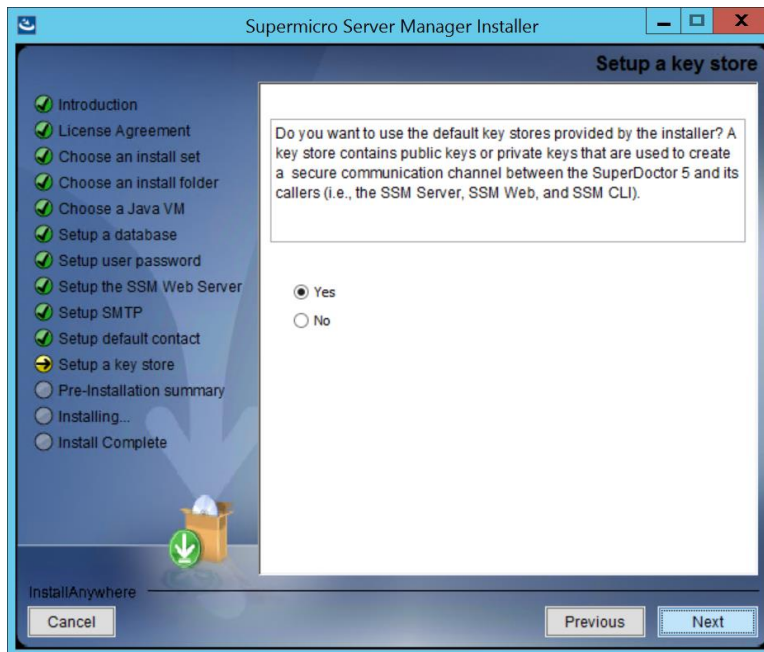


Figure 2-11

13. Click the **Install** button to install the SSM software on your computer.

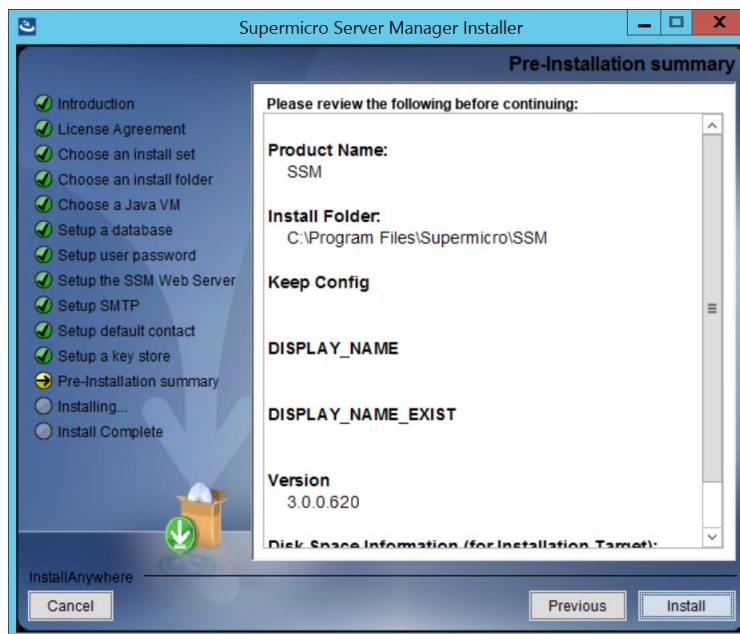


Figure 2-12

14. Installation is complete. Click the **Done** button to exit and restart your system to enable SSM services.

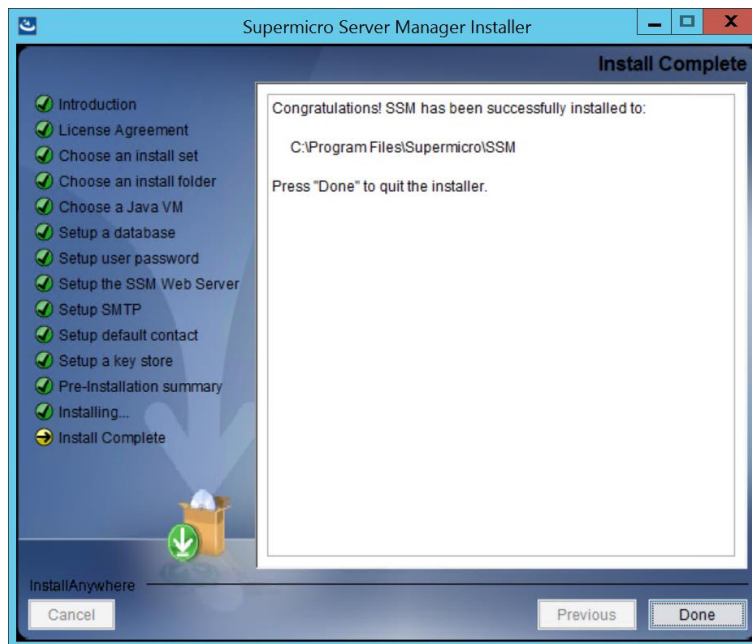


Figure 2-13

2.1.2 Linux Installation

You must have root privileges to install SSM. To install SSM in Linux, follow these steps.

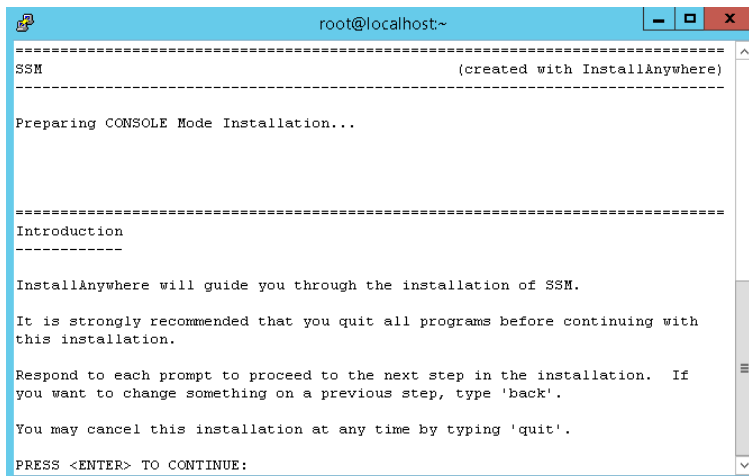
1. Execute the SSM installer.



Note: For Linux users who treat the default /tmp folder as a vulnerability and configure the folder to be read-only, you can set the IATEMPDIR and TEMP environment variables to an existing folder, for example:

- export IATEMPDIR=/opt/tmp, then the designated folder can be accessed by the SSM installer during installation.
- export TEMP=/opt/tmp, then the designated folder can be accessed by the built-in PostgreSQL database during installation.

2. Press the **<Enter>** key (on your keyboard) to continue.

A terminal window titled 'root@localhost:~' showing the SSM installer's introduction. The text includes: 'SSM (created with InstallAnywhere)', 'Preparing CONSOLE Mode Installation...', 'Introduction', 'InstallAnywhere will guide you through the installation of SSM.', 'It is strongly recommended that you quit all programs before continuing with this installation.', 'Respond to each prompt to proceed to the next step in the installation. If you want to change something on a previous step, type 'back'.', 'You may cancel this installation at any time by typing 'quit'.', and 'PRESS <ENTER> TO CONTINUE:'.

```
root@localhost:~
=====
SSM                               (created with InstallAnywhere)
=====
Preparing CONSOLE Mode Installation...

-----
Introduction
-----

InstallAnywhere will guide you through the installation of SSM.

It is strongly recommended that you quit all programs before continuing with
this installation.

Respond to each prompt to proceed to the next step in the installation.  If
you want to change something on a previous step, type 'back'.

You may cancel this installation at any time by typing 'quit'.

PRESS <ENTER> TO CONTINUE:
```

Figure 2-14

3. Accept the license agreement and press the **<Enter>** key to continue.

```
root@localhost:~  
6. COMPLETE AGREEMENT. This Licence constitutes the entire agreement between  
the parties with respect to the use of the Software and Materials, and  
supersedes all prior or contemporaneous understandings or agreements, written  
or oral, regarding such subject matter. No amendment to or modification of  
this Licence will be binding unless in writing and signed by a duly authorized  
representative of Super Micro Computer Inc.  
  
Super Micro Computer Inc.  
980 Rock Avenue  
San Jose, CA 95131  
USA  
  
(408) 503-8000 Voice  
  
PRESS <ENTER> TO CONTINUE:  
  
(408) 503-8008 Fax  
E-mail: support@supermicro.com  
Internet: http://www.supermicro.com  
  
SSM(Supermicro Server Manager) Copyright(c) 1993-2016 by Super Micro Computer  
Inc. and its licensors. All Rights Reserved.  
  
DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N):
```

Figure 2-15

4. Select the **Install All** option and press the **<Enter>** key to continue.

```
root@localhost:~  
(408) 503-8008 Fax  
E-mail: support@supermicro.com  
Internet: http://www.supermicro.com  
  
SSM(Supermicro Server Manager) Copyright(c) 1993-2016 by Super Micro Computer  
Inc. and its licensors. All Rights Reserved.  
  
DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N): y  
  
-----  
Choose an install set  
-----  
  
Please choose the Install Set to be installed by this installer.  
  
->1- Install All  
2- SSM Server  
3- SSM Web  
4- SSM CLI  
  
ENTER THE NUMBER FOR THE INSTALL SET, OR PRESS <ENTER> TO ACCEPT THE DEFAULT  
:
```

Figure 2-16

5. Enter a directory to install SSM to and press the **<Enter>** key to continue. We recommend installing SSM to the default folder (**/opt/Supermicro/SSM**).

```
root@localhost:~  
-----  
Choose an install folder  
-----  
  
Where would you like to install?  
  
Default Install Folder: /opt/Supermicro/SSM  
  
ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT  
:
```

Figure 2-17

6. Use the built-in Java VM and press the **<Enter>** key to continue.

```
root@localhost:~
=====
Choose a Java VM
=====
Please choose a Java VM for use by the installed application. Select
"Built-in" option to use built-in Java VM or select "Choose a Java VM"
option to use another Java VM version.

->1- Built-in (JRE 1.8.0_222-ojdkbuild)
   2- Choose a Java VM

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT::
```

Figure 2-18



Note: If you select “Choose a Java VM” option, the architecture of the selected Java VM must be compatible with the installer. For example, to use an x86 version of SuperDoctor 5, you need to select an x86 version of Java VM. Also note that only JVM version newer than 1.8.0 is supported.

7. Use the built-in database and press the **<Enter>** key to continue.

```
root@localhost:~
=====
Setup a database
=====
Do you want to use the built-in database? The SSM Server stores configuration
and monitoring data on a database. You can use the built-in database provided
by SSM or use an existing database on your site.

->1- Yes
   2- No

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT::
```

Figure 2-19

8. You can input the password for the built-in ADMIN account to access SSM Web and press the **<Enter>** key to continue.

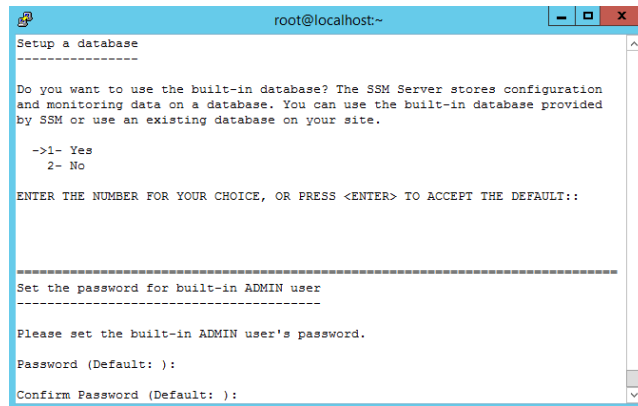


Figure 2-20

9. Enter the default port numbers for HTTP and HTTPS and press the **<Enter>** key to continue. Normally you should accept the default values.

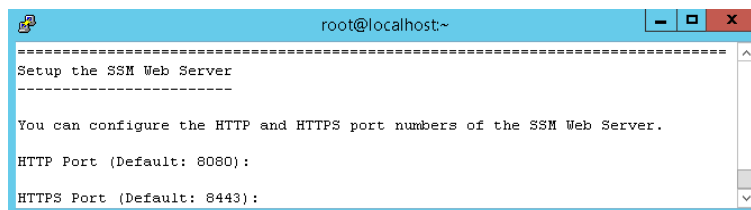


Figure 2-21

10. Enter an SMTP server, an SMTP port, a sender's email, a user account, and the password, which will be used by SSM server to send notifications. Note that you can modify the SMTP server settings latter on SSM Web. See *6.10 E-Mail SMTP Setup* for more information.

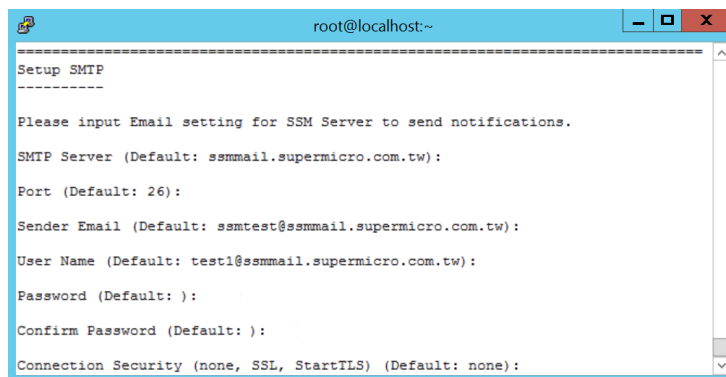


Figure 2-22

11. Enter the email address of the default contact.

```
root@localhost:~  
-----  
Setup default contact  
-----  
  
Input admin's email address which will receive notifications when the status  
of a host or a service changes.  
  
Email (Default: ): test@test.com.tw
```

Figure 2-23

12. Use the default key store and press the **<Enter>** key to continue.

```
root@localhost:~  
-----  
Setup a key store  
-----  
  
Do you want to use the default key stores provided by the installer? A key  
store contains public keys or private keys that are used to create a secure  
communication channel between the SuperDoctor 5 and its callers (i.e., the SSM  
Server, SSM Web, and SSM CLI).  
  
->1- Yes  
   2- No  
  
ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT::
```

Figure 2-24

13. This step shows the pre-installation summary. Press the **<Enter>** key to continue.

```
root@localhost:~  
-----  
Product Name:  
  SSM  
  
Install Folder:  
  /opt/Supermicro/SSM  
  
Java VM Installation Folder:  
  /opt/Supermicro/SSM/jre  
  
KEEP CONFIG  
  
DISPLAY_NAME  
  
Disk Space Information (for Installation Target):  
  Required: 809,613,886 Bytes  
  Available: 26,658,697,216 Bytes  
  
PRESS <ENTER> TO CONTINUE:
```

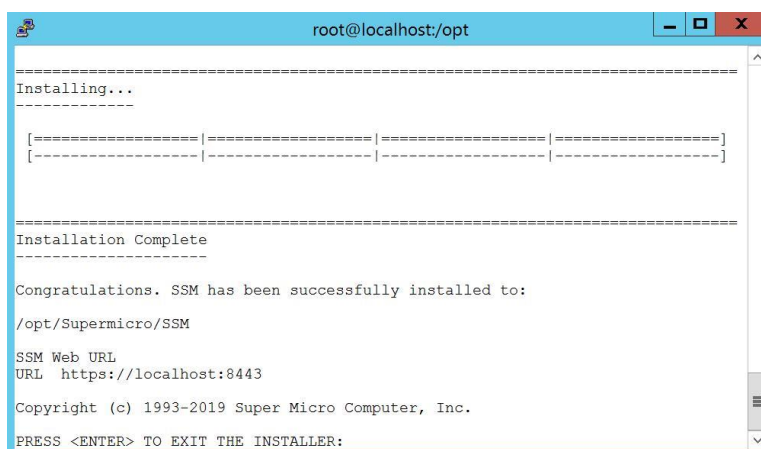
Figure 2-25

14. Press the **<Enter>** key to install the SSM software on your computer.

```
root@localhost:~  
-----  
Ready To Install  
-----  
  
InstallAnywhere is now ready to install SSM onto your system at the following  
location:  
  
  /opt/Supermicro/SSM  
  
PRESS <ENTER> TO INSTALL:
```

Figure 2-26

15. Installation is complete. Press the <Enter> key to exit the installer.



```
root@localhost/opt
=====
Installing...
=====
[=====|=====|=====|=====]
[-----|-----|-----|-----]
=====
Installation Complete
=====
Congratulations. SSM has been successfully installed to:
/opt/Supermicro/SSM
SSM Web URL
URL https://localhost:8443
Copyright (c) 1993-2019 Super Micro Computer, Inc.
PRESS <ENTER> TO EXIT THE INSTALLER:
```

Figure 2-27



Note: Under Linux you do not need to reboot your computer to use SSM.

2.1.3 Silent Mode Installation

Silent mode installation provides a way to install SSM without the interaction of users. To use silent mode installation, a property file that contains the necessary SSM installation settings must be provided.

1. Prepare a property file for silent mode installation. A property file that directs the SSM installer to install all SSM features (such as the SSM Server, SSM Web, and SSM CLI) on a Linux platform is shown below. All configuration options required by the SSM installer are included in the property file. Note that you should carefully trim spaces for the properties in the property file.

```
# -----
# This file was built by the Replay feature of InstallAnywhere.
# It contains variables that were set by Panels or Consoles.

#Choose Install Folder
# e.g., C:\Program Files\Supermicro\SSM
#      /opt/Supermicro/SSM
#-----
USER_INSTALL_DIR=/opt/Supermicro/SSM

#Choose Install Feature
#-----
CHOSEN_INSTALL_FEATURE_LIST=shared,SSMServer,SSMWeb,SSMCLI
```



```

#Choose a Java VM
#-----
USE_DEFAULT_JVM=Yes
#INSTALLED_JVM_PATH=/usr/java/jdk1.8.0_102/jre/bin/java

#Setup Web Server
#-----
SERVER_WEB_HTTP_PORT=8080
SERVER_WEB_HTTPS_PORT=8443

#Setup Email
#-----
SERVER_EMAIL_SMTP=mail.your-mail-server.com
SERVER_EMAIL_SENDER=your-account@your-mail-server.com
SERVER_EMAIL_USERNAME=your-account
SERVER_EMAIL_PASSWORD=your-password
#Setup SMTP server port. Default: 25
SERVER_EMAIL_SMTP_PORT=25
#Choose connection security for your SMTP server. Default: none
SERVER_EMAIL_SMTP_SECURITY=none

#Setup Contact Email
SERVER_DEFAULT_CONTACT=contact-account@your-mail-server.com

#Choice use default key
#-----
#Setup a keystore
#-----
USE_DEFAULT_KEYSTORE=Yes

#SERVER_PRIVATE_KEYSTORE_PATH=c:\\jchecknrpe.auth
#SERVER_PUBLIC_KEYSTORE_PATH=c:\\jchecknrpe.trust

#Setup DB
#-----
USE_SERVER_DEFAULT_DB=Yes
SERVER_CREATE_DB=Yes

#SERVER_DB_TYPE= PostgreSQL
#SERVER_DB_NAME= ssm
#SERVER_DB_PORT= 5432
#SERVER_DB_IP=your-DB-IP
#SERVER_DB_USERNAME=your-DB-Account
#SERVER_DB_PASSWORD=your-DB-password

#Default account of administrator
#-----
#Uncomment below statement to set the password for the built-in ADMIN user.
#SERVER_DEFAULT_PASSWORD=yourAdminPassword

```

1. Modify the property according to your needs. Possible attributes and values of the property file are shown below.

Attribute	Description	Option
-----------	-------------	--------

Attribute	Description	Option
USER_INSTALL_DIR	Install folder Note: It's necessary for you to choose the same install folder each time when you install each of these features on a host.	
CHOSEN_INSTALL_FEATURE_LIST	Install features Note: Keep features in one line and be separated by commas.	shared,SSMServer,SSMWeb,SSMCLI shared,SSMServer shared,SSMWeb shared,SSMCLI
USE_DEFAULT_JVM	Uses default Java VM	Yes No
INSTALLED_JVM_PATH	JVM path if USE_DEFAULT_JVM= No	
SERVER_WEB_HTTP_PORT	SSM Web listen port	8080
SERVER_WEB_HTTPS_PORT	SSM Web secure listen port	8443
SERVER_EMAIL_SMTP	SMTP server location	
SERVER_EMAIL_SENDER	Sender's E-Mail	
SERVER_EMAIL_USERNAME	Username (SMTP authentication)	
SERVER_EMAIL_PASSWORD	Password (SMTP authentication)	
SERVER_EMAIL_SMTP_PORT	Port	25
SERVER_EMAIL_SMTP_SECURITY	Connection security	none ssl tls
SERVER_DEFAULT_CONTACT	Contact's E-Mail	
USE_DEFAULT_KEYSTORE	Uses default key store	Yes No
SERVER_PRIVATE_KEYSTORE_PATH	Server private key store path if USE_DEFAULT_KEYSTORE= No	
SERVER_PUBLIC_KEYSTORE_PATH	Server public key store path if	

Attribute	Description	Option
ATH	USE_DEFAULT_KEYSTORE=No	
USE_SERVER_DEFAULT_DB	Installs default PostgreSQL database	Yes No
SERVER_CREATE_DB	Creates database	Yes No
SERVER_DB_TYPE	Chooses database if USE_SERVER_DEFAULT_DB=No	PostgreSQL
SERVER_DB_DRIVER_PATH	Database driver path if USE_SERVER_DEFAULT_DB=No	
SERVER_DB_NAME	Database name if USE_SERVER_DEFAULT_DB=No	
SERVER_DB_IP	Database location if USE_SERVER_DEFAULT_DB=No	
SERVER_DB_PORT	Database listen port if USE_SERVER_DEFAULT_DB=No	
SERVER_DB_USERNAME	Database username if USE_SERVER_DEFAULT_DB=No	
SERVER_DB_PASSWORD	Database password if USE_SERVER_DEFAULT_DB=No	
SERVER_DEFAULT_PASSWORD	The password for the built-in ADMIN user	

2. Begin silent mode installation.

For Windows platforms:

```
SSMInstaller.exe -i silent -f [property_file_name]
```

For Linux platforms:

```
./SSMInstaller.bin -i silent -f [property_file_name]
```



Notes:

- For Linux users who treat the default /tmp folder as a vulnerability and configure the folder to be read-only, you can set the IATEMPDIR and TEMP environment variables to an existing folder, for example:
 - export IATEMPDIR=/opt/tmp, then the designated folder can be accessed by the SSM installer during installation.
 - export TEMP=/opt/tmp, then the designated folder can be accessed by the built-in PostgreSQL database during installation.
- Under silent mode there is no error message shown on the console. Once the installation is completed, an **SSM_InstallLog.log** file is generated in the **[install folder]** folder. This file contains installation log data that can be used for debugging purposes.

You can open the following log files to check whether SSM is installed successfully. Note that these steps are optional and meant for troubleshooting only.

3. Check SSM_InstallResult.log file to make sure SSM is properly installed. Note that no error messages are shown on the console in silent mode. Once the installation is complete, the SSM_InstallResult.log file is generated in the [install folder] folder. The following SSM_InstallResult.log file shows that the SSM is properly installed.

```
Installation Result: Success
```

If a previous version of SSM is detected during the installation process, the log file will be shown as below:

```
Installation Time: Tue May 15 09:58:53 CST 2012
```

```
Detect previous: 'YES'
```

```
Installation Result: Failed
```

```
Root Cause: SSM already exists, please uninstall it before installing SSM
```

With the installation log data, you can start troubleshooting.

4. Check SSM_InstallLog.log. The SSM_InstallLog.log file is generated in the [install folder] folder. This file contains installation log data that can be used for debugging installation process. The following SSM_InstallResult.log file shows an example that guides you to check SSM_InstallLog.log file.

```
Installation Result: Failed
```

```
Root Cause: Installation Process Failed
```

Please open SSM_InstallLog.log to check "WARNING" or "ERROR" keywords and see if there are problems.

After opening the SSM_InstallLog.log, you are able to see warnings or errors in the log file as shown below.

```
....
```

```
Summary
```

```
-----
```

```
Installation: Successful
```

```
1885 Successes
```

```
5 Warnings
```

```
0 NonFatalErrors
```

```
0 FatalErrors
```



Note: All warnings and errors are logged in the file for reference.

2.2 Activating SSM

You must activate the software product key⁴ before adding hosts to be monitored by SSM that have no node product key⁵. Both online and offline activations are supported. Note that online activation is for users on the Internet and offline activation is for users who run on a closed network. Choose either online or offline activation to suit your needs.

2.2.1 Using Online Activation

To activate SSM online, follow these steps:

1. Contact Supermicro to generate your **software product key**⁶.
2. Find the **ssmlicense tool** located in the `[install folder]\shared\License` folder.
3. Run the tool to activate SSM with the product key from Supermicro and see if the activation is granted or not. See *2.7.1 -ona [product key]: Online activation* for more information. If it's granted, go to Step 4. If the activation is denied, go to Step 5.
4. SSM has been activated and now you can start to use SSM. Note that some SSM services could be started before the product activation. Make sure all services are functioning. See *2.3 Verifying the Installation* and *2.4 Manually Controlling SSM Services* for more information.
5. SSM isn't activated. Make sure the Internet connection is established and try again.

2.2.2 Using Offline Activation

To activate SSM offline, follow these steps:

1. Contact Supermicro to generate your **software product key**⁷.
2. Find the **ssmlicense tool** located in the `[install folder]\shared\License` folder.
3. Run the tool to create an **offline activation request file** with the product key from Supermicro. See *2.7.3 -c [product key]: Create an activation request file* for more information.
4. Send the activation request file to Supermicro.
5. Put the **activation response file** from Supermicro in the `[install folder]\shared\License` folder.
6. Find the license tool used in Step 1.
7. Run the tool to activate SSM and see if the activation is granted or not. See *2.7.4 -ofa [product key] -of [specified directory]: Offline activation* for more information. If it's granted, go to Step 8. If the activation is denied, go to Step 9.
8. SSM has been activated and now you can start to use SSM. Note that some SSM services could be started before the product activation. Make sure all services are functioning. See *2.3 Verifying the Installation* and *2.4 Manually Controlling SSM Services* for more information.
9. SSM isn't activated. Make sure the Internet connection is disconnected and try again.

⁴ By default, 5 software product keys are given by SSM.

⁵ See *10.2 Activating an IPMI Host* for more information about node product key.

⁶ It's a serial number, e.g. "ABCD-EFGH-IJKL-MNOP-...".

⁷ There's no difference between online and offline product keys. It's a serial number as shown above.



Notes:

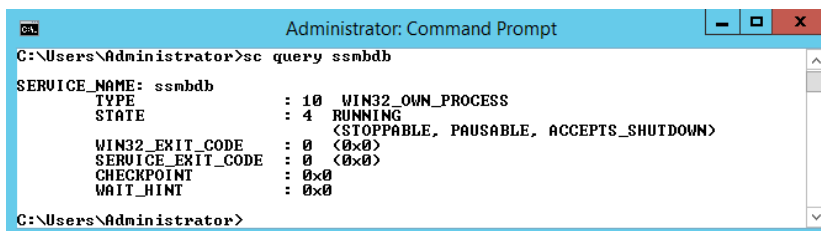
- Make sure the Internet connection is disabled in the offline activation process or the activation will fail.
 - The activation response is machine-dependent so that you have to activate SSM in the machine where you generate the activation request.
-

2.3 Verifying the Installation

You can use the following commands to check whether SSM has installed successfully and all SSM services are running. Note that these steps are optional and meant for troubleshooting only.

After restarting your Windows system, open a DOS prompt and enter the following commands to make sure all required SSM services have been installed and started.

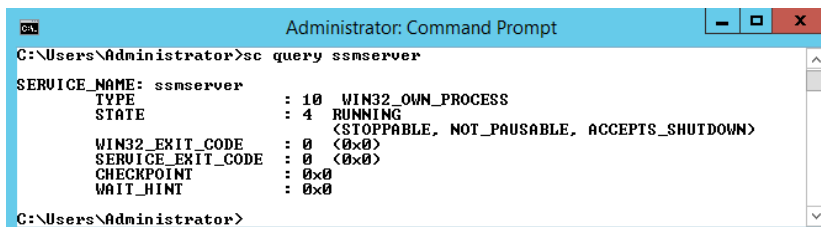
Check the SSM Database



```
Administrator: Command Prompt
C:\Users\Administrator>sc query ssmdb
SERVICE_NAME: ssmdb
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 4   RUNNING
                        (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE      : 0   (0x0)
        SERVICE_EXIT_CODE  : 0   (0x0)
        CHECKPOINT          : 0x0
        WAIT_HINT           : 0x0
C:\Users\Administrator>
```

Figure 2-28

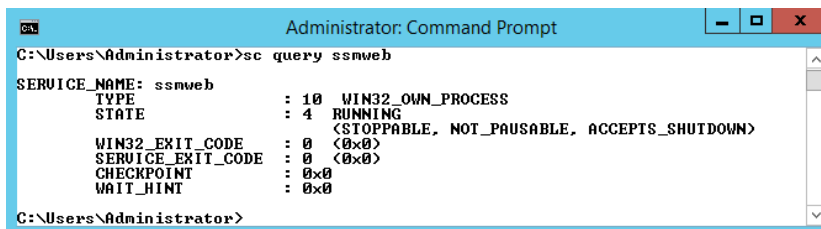
Check the SSM Server



```
Administrator: Command Prompt
C:\Users\Administrator>sc query ssmserver
SERVICE_NAME: ssmserver
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 4   RUNNING
                        (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE     : 0   (0x0)
        SERVICE_EXIT_CODE  : 0   (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
C:\Users\Administrator>
```

Figure 2-29

Check the SSM Web



```
Administrator: Command Prompt
C:\Users\Administrator>sc query ssmweb
SERVICE_NAME: ssmweb
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 4   RUNNING
                        (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE     : 0   (0x0)
        SERVICE_EXIT_CODE  : 0   (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
C:\Users\Administrator>
```

Figure 2-30

For Linux users, use the following commands to check SSM services:

```
# service ssmdb status
```

```
# service ssmserver status
```

```
# service ssmweb status
```

RHEL 7.x and SLES 12.x users have additional commands to check SSM services:

```
# systemctl status smbdb
```

```
# systemctl status ssmserver
```

```
# systemctl status ssmweb
```

2.4 Manually Controlling SSM Services

If SSM services (i.e., smbdb, ssmserver, and ssmweb) are not automatically started, you can start and stop these services manually.

2.4.1 SSM Database Service

For Windows platforms: In the **[install folder]\SSMDB** folder, execute **startSSMBDBService.bat** and **stopSSMBDBService.bat** to start and stop the SSM Database service, respectively.

For Linux platforms: In the **[install folder]/SSMDB** folder, execute **startSSMBDBService.sh** and **stopSSMBDBService.sh** to start and stop the SSM Database service, respectively.

2.4.2 SSM Server Service

For Windows platforms: In the **[install folder]\SSMServer** folder, execute **startSSMServerService.bat** and **stopSSMServerService.bat** to start and stop the SSM Server service, respectively.

For Linux platforms: In the **[install folder]/SSMServer** folder, execute **startSSMServerService.sh** and **stopSSMServerService.sh** to start and stop the SSM Server service, respectively.

2.4.3 SSM Web Service

For Windows platforms: In the **[install folder]\SSMWeb** folder, execute **startSSMWebService.bat** and **stopSSMWebService.bat** to start and stop the SSM Web service, respectively.

For Linux platforms: In the **[install folder]/SSMWeb** folder, execute **startSSMWebService.sh** and **stopSSMWebService.sh** to start and stop the SSM Web service, respectively.

2.5 Deactivating SSM

You have to deactivate the SSM software product key before uninstalling it. Choose online or offline deactivation depending on how you activated SSM. If you activate SSM via online activation, you have to deactivate SSM via online deactivation, and vice versa.

2.5.1 Using Online Deactivation

To deactivate SSM online, follow these steps:

1. Find the **ssmlicense tool** located in the **[install folder]\shared\License** folder.
2. Run the tool to deactivate SSM and see if the deactivation is granted. See *2.7.2 -ond: Online deactivation* for more information. If it's granted, go to Step 3. If it's denied, go to Step 4.
3. SSM is deactivated.
4. SSM isn't deactivated. Make sure the Internet connection is established and try again.

2.5.2 Using Offline Deactivation

To deactivate SSM offline, follow these steps:

1. Find the **ssmlicense tool** located in the **[install folder]\shared\License** folder.
2. Run the tool to deactivate SSM and see if the deactivation is granted or not. See *2.7.5 -ofd: Offline deactivation* for more information. If it's granted, go to Step 3. If it's denied, go to Step 4.
3. SSM is deactivated. Send the deactivation request generated in Step 2 to Supermicro.
4. SSM isn't deactivated. Make sure the Internet connection is disconnected and try again.



Note: Product deactivation will be performed automatically while you uninstall SSM. However, you still need to send the deactivation request to Supermicro if you use offline activation. Your activation record in Supermicro will not be cleared until you provide the deactivation request.

2.6 Uninstalling SSM

In this section, we will show you how to uninstall SSM on different platforms.

2.6.1 Uninstalling in Windows

You must have Administrator privileges to uninstall SSM. To uninstall SSM in Windows, follow these steps.

1. Execute **Uninstaller.exe** in the **[install folder]\Uninstall** folder.
2. Click the **Next** button to continue.

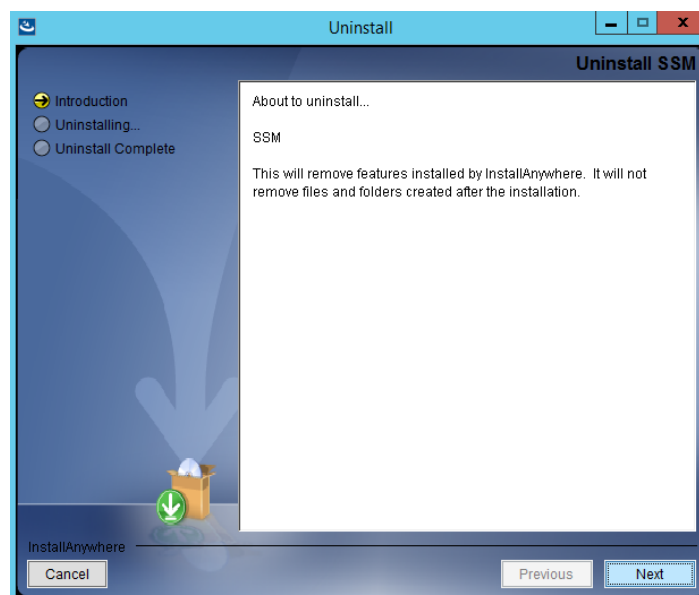


Figure 2-31

3. Select the **Complete Uninstall** option and click the **Next** button to continue.

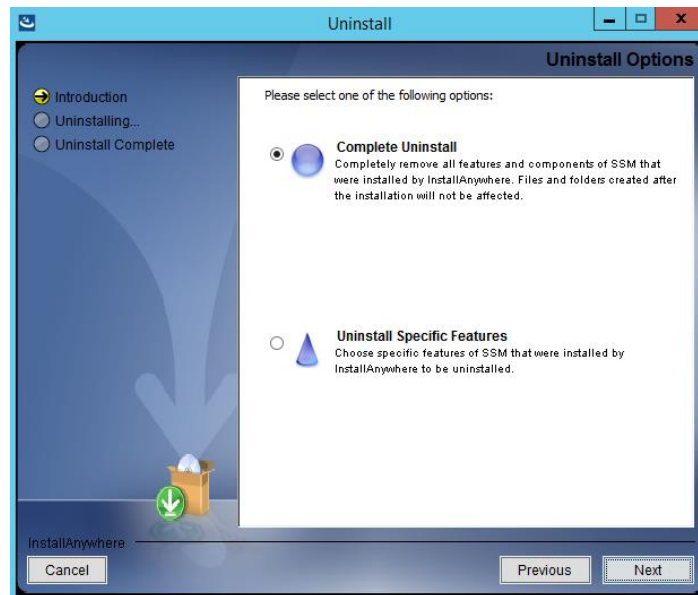


Figure 2-32

You can also select **Uninstall Specific Features** to uninstall specific SSM features, as shown below.

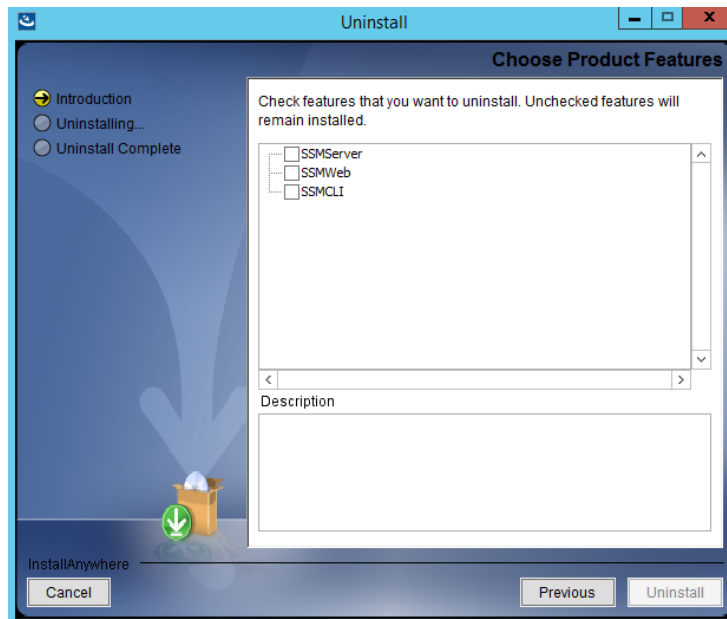


Figure 2-33

4. Please wait while the program uninstalls.

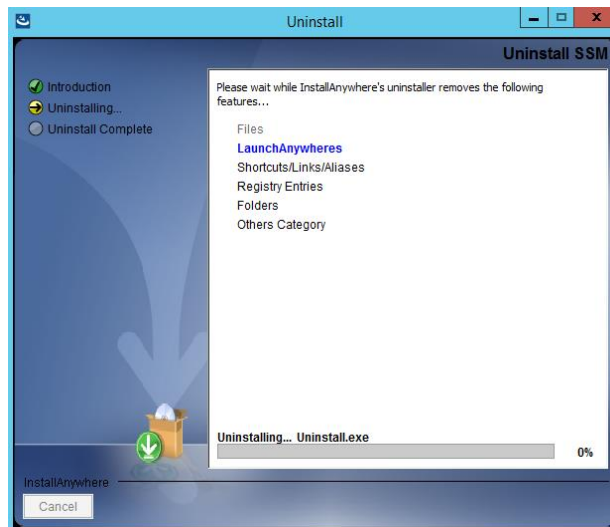


Figure 2-34



Note: If you uninstall SSM without using the `ssmlicense` tool to deactivate SSM first, the uninstaller will perform online or offline deactivation depending on how you activated SSM. Meanwhile, in the offline mode, the uninstaller will remind you to send the deactivation request file to Supermicro as shown below. The `SSMDeactivationRequest.xml` file is located in `[install folder]\` folder.

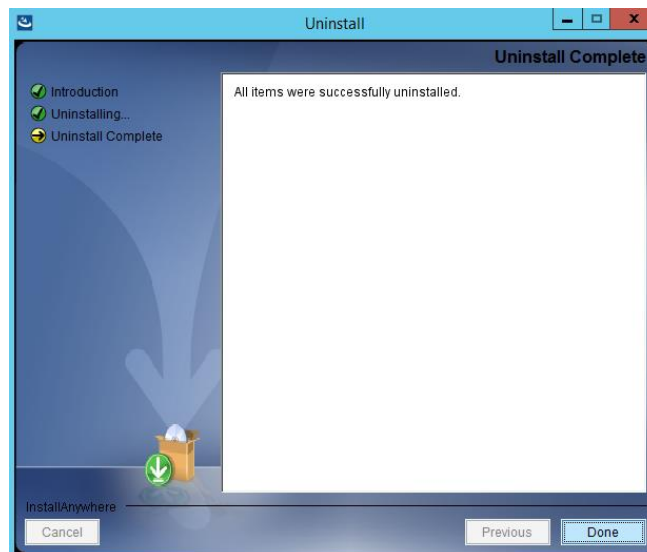
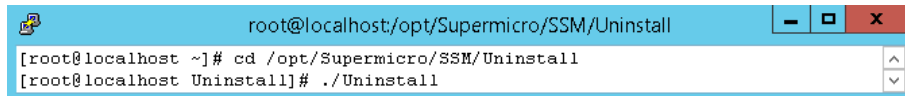


Figure 2-35

2.6.2 Uninstalling in Linux

You must have root privileges to uninstall SSM. To uninstall SSM in Linux, follow these steps.

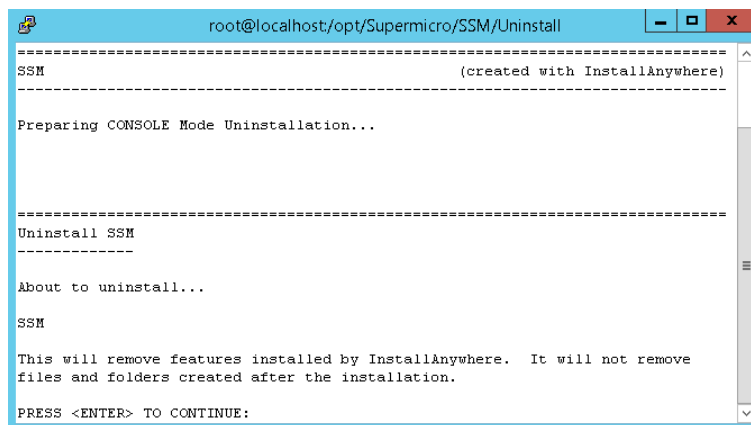
1. Execute the Uninstaller program located in the **[install folder]\Uninstall** folder. Note that if you set the IATEMPDIR environment variable during SSM installation, now you need to set it again so that it can be used while SSM is uninstalled.



```
root@localhost:opt/Supermicro/SSM/Uninstall
[root@localhost ~]# cd /opt/Supermicro/SSM/Uninstall
[root@localhost Uninstall]# ./Uninstall
```

Figure 2-36

2. Press the **<Enter>** key (on your keyboard) to continue.



```
root@localhost:opt/Supermicro/SSM/Uninstall
=====
SSM                                     (created with InstallAnywhere)
=====
Preparing CONSOLE Mode Uninstallation...

=====
Uninstall SSM
-----

About to uninstall...

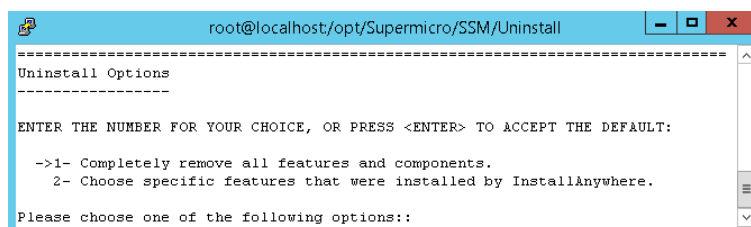
SSM

This will remove features installed by InstallAnywhere. It will not remove
files and folders created after the installation.

PRESS <ENTER> TO CONTINUE:
```

Figure 2-37

3. Select the **1- Completely remove all features and components** option and press the **<Enter>** key to continue.



```
root@localhost:opt/Supermicro/SSM/Uninstall
=====
Uninstall Options
-----

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:

->1- Completely remove all features and components.
   2- Choose specific features that were installed by InstallAnywhere.

Please choose one of the following options::
```

Figure 2-38

You can also choose **2** to uninstall specific SSM features.

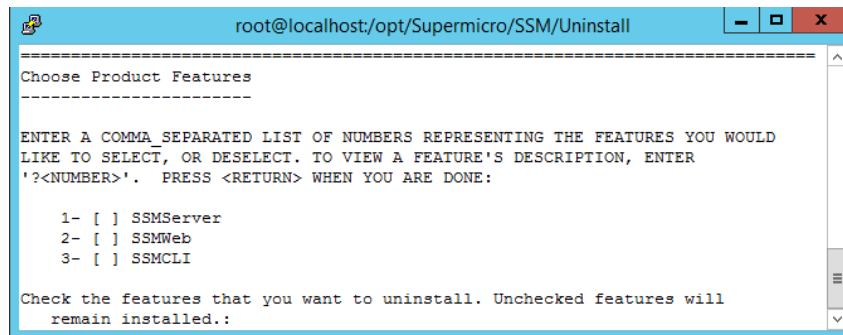


Figure 2-39

4. Please wait while the program uninstalls.

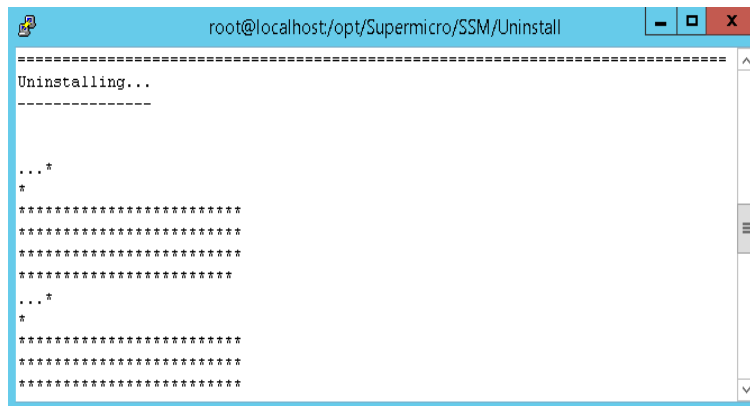


Figure 2-40

5. The uninstall is complete.

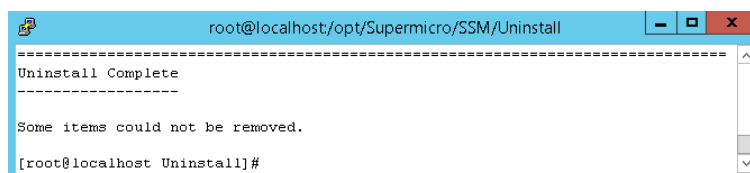


Figure 2-41



Note: If you uninstall SSM without using the `ssmlicense` tool to deactivate SSM first, the uninstaller will perform online and offline deactivation depending on how you activated SSM. Meanwhile, in the offline mode, the uninstaller will remind you to send the deactivation request file to Supernano as shown below. The `SSMDeactivationRequest.xml` file is located in **[install folder]** folder.

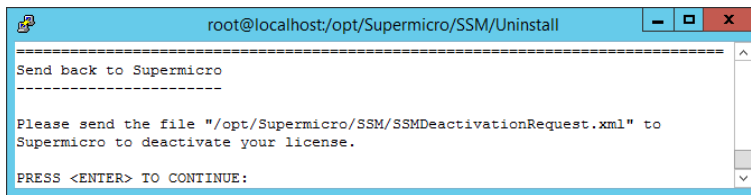


Figure 2-42

2.6.3 Silent Mode Uninstall

Use the following arguments to execute the **Uninstaller** program located in the **[install folder]\Uninstall** folder. **Note that you must have root privileges to uninstall SSM.**

```
Uninstall -i silent -f [property_file_name]
```



Notes:

- For Linux users, if you set the IATEMPDIR environment variable when installing SSM, now you need to set it again to access the designated folder while uninstalling SSM.
 - If you uninstall SSM without using the ssmlicense tool to deactivate SSM first, the uninstaller will perform online and offline deactivation depending on how you activated SSM. Meanwhile, in the offline mode, SSM_UninstallResult.log is created and you will be reminded to send the deactivation request file to Supermicro. The SSM_UninstallResult.log file is located in the **[install folder]** folder.
-

2.7 Using ssmlicense tool

The ssmlicense tool is mainly used to activate and deactivate SSM. Before using, see 2.2 *Activating SSM* and 2.5 *Deactivating SSM* for more information. This chapter shows you how to use ssmlicense to activate and deactivate SSM. The tool is located in the `[install folder]\shared\License` folder. To execute the tool, Windows users use `ssmlicense.bat` and Linux users use `ssmlicense.sh`.

2.7.1 -ona [product key]: Online activation

Online activation requires a product key provided by Supermicro. Contact Supermicro if you don't have one. Use the -ona argument to specify your product key. See the example below. Enter `ssmlicense -ona [product key]` then the activation status will be shown onscreen.

```
[softlab:/opt/Supermicro/SSM/shared/License] # ./ssmlicense.sh -ona ABCD-EFGH-1111 -  
2222-IJKL-3333-WXYZ
```

```
SSM is activated successfully.
```

The line in bold indicates the execution results.



Note: To determine proxy, please use `-p [your proxy setting]`.

2.7.2 -ond: Online deactivation

Use the -ond argument to deactivate SSM. See the example below. Enter `ssmlicense -ond`. The deactivation status will be shown onscreen.

```
[softlab:/opt/Supermicro/SSM/shared/License]# ./ssmlicense.sh -ond
```

```
SSM is deactivated successfully.
```

The line in bold indicates the execution results.



Note: To determine proxy, please use `-p [your proxy setting]`.

2.7.3 -c [product key]: Create an activation request file

Creating an offline activation request file requires a product key provided by Supermicro. Contact Supermicro if you don't have one. Use the -c argument to specify your product key. Enter `ssmlicense -c [product key]`. The activation request will be created as shown below.

```
[softlab:/opt/Supermicro/SSM/shared/License]# ./ssmlicense.sh -c ABCD-EFGH-1111 -  
2222-IJKL-3333-WXYZ
```

Create activation request file successfully !!

**Please email the SSMActivationRequest file to Supermicro and we will email
SSMActivationResponse file to let you activate SSM.**

**The file can be found in
/opt/Supermicro/SSM/shared/License/SSMActivationRequest.xml**

The line in bold indicates the execution results.



Notes:

- To specify the location of the activation request file, use **-of [specified directory]**.
- You have to send the SSMActivationRequest.xml file to Supermicro so that you could get SSMActivationResponse.xml in return.

2.7.4 -ofa [product key] -of [specified directory]: Offline activation

Before you execute the command, you need to get an offline activation response file provided by Supermicro. See 2.2 *Activating SSM* for more information. Use the -ofa argument to specify your product key. Also, use the -of argument to specify an existing folder where the response file is located. Use the -of argument only when the activation response file is not in the **[install folder]\shared\License** folder. See the example below. Enter `ssmlicense -ofa [product key] -of [file folder]`. The activation status will be shown onscreen.

```
[softlab:/opt/Supermicro/SSM/shared/License] # ./ssmlicense.sh -ofa ABCD-EFGH-1111 -  
2222-IJKL-3333-WXYZ -of /opt/SSM/shared/xml/
```

SSM is activated successfully.

The line in bold indicates the execution results.

2.7.5 -ofd: Offline deactivation

Use the -ofd argument to deactivate SSM. See the example below. Enter ssmlicense -ofd. The deactivation status will be shown onscreen.

```
[softlab:/opt/Supermicro/SSM/shared/License]# ./ssmlicense.sh -ofd
```

```
SSM is deactivated successfully.
```

```
Please email SSMDeactivationRequest file to Supermicro to deactivate SSM.
```

```
The file can be found in /opt/
```

```
Supermicro/SSM/shared/License/SSMDeactivationRequest.xml
```

The line in bold indicates the execution results.



Notes:

- To specify the location of the deactivation request file, use **-of [specified directory]**.
- You have to send the SSMDeactivationRequest.xml file to Supermicro so that your activation record in Supermicro can be cleared.

2.7.6 -ons: Online synchronization

Use the -ons argument to sync product features online. See the example below. Enter ssmlicense -ons. The sync status will be shown onscreen.

```
[softlab:/opt/Supermicro/SSM/shared/License]# ./ssmlicense.sh -ons
```

```
Sync product feature successfully.
```

The line in bold indicates the execution results.

2.7.7 -ofs -of [specified directory]: Offline synchronization

Use the -ofs argument to sync product features between your initial copy of SSM and the new activation response file. Use -of argument to specify an existed folder where the response file is located. Use -of argument only when the activation response file is not in the [install folder]\shared\License folder. See the example below. Enter ssmlicense -ofs -of [file folder] then the sync status will be shown onscreen.

```
[softlab:/opt/Supermicro/SSM/shared/License]# ./ssmlicense.sh -ofs -of /opt/Supermicro  
/SSM/shared/xml/
```

```
Sync product feature successfully.
```

The line in bold indicates the execution results.



Note: You are supposed to receive notifications from Supermicro once the product features are changed. Supermicro will give you an activation response file after receiving your new activation request file.

2.7.8 -ia: Check if product activated

Use the -ia argument to check if SSM is activated or not. Enter ssmlicense -ia then the activation status will be shown onscreen as below.

```
[softlab:/opt/Supermicro/SSM/shared/License]# ./ssmlicense.sh -ia
```

```
The product key has been activated.
```

The line in bold indicates the execution results.

2.8 Auto-Upgrading in Installer

The SSM installer provides you with automatic backup of data in an old version of SSM when upgrading, and it is optional for you to either transfer or restore it to a newer version after updating. When you execute the SSMinstaller, it will detect if SSM has been already installed and ask if you want to keep the data in the current version.

The old data in a file system or a database (such as configuration data, settings and reports) can be kept when upgrading. Once the SSMinstaller is finished with the data backup, the upgrade begins in silent mode by uninstalling the current version and installing the new version.



Note: This feature is only available when the SSM installer is in interactive mode. Also, make sure you meet the following requirements:

- Your SSM is connected to the built-in database.
- Your current version of SSM is older than the new SSM installer.

2.8.1 Upgrading in Windows

You must have Administrator privileges to upgrade SSM. To upgrade SSM in Windows, follow these steps.

1. Execute the SSMinstaller.
2. Select **Yes** to back up the data in the previous version and click the **Next** button to continue.

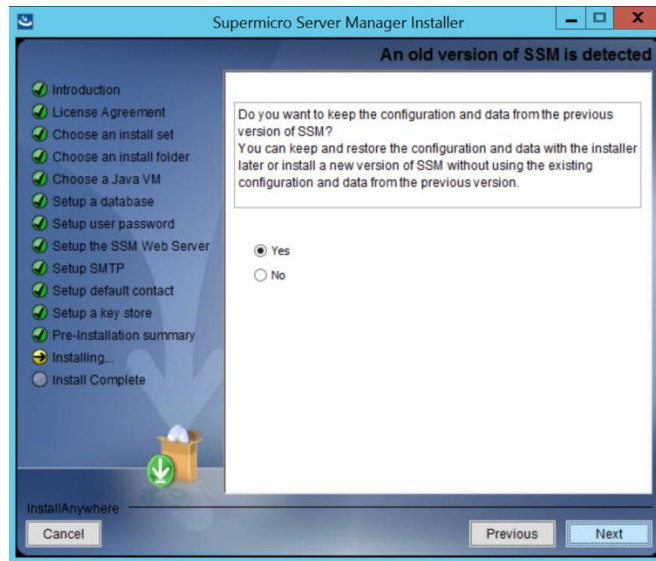


Figure 2-43

3. Input your password and click **Next**. Note that you will be forced to change the password if “ADMIN” is detected to be the password for the built-in ADMIN account.

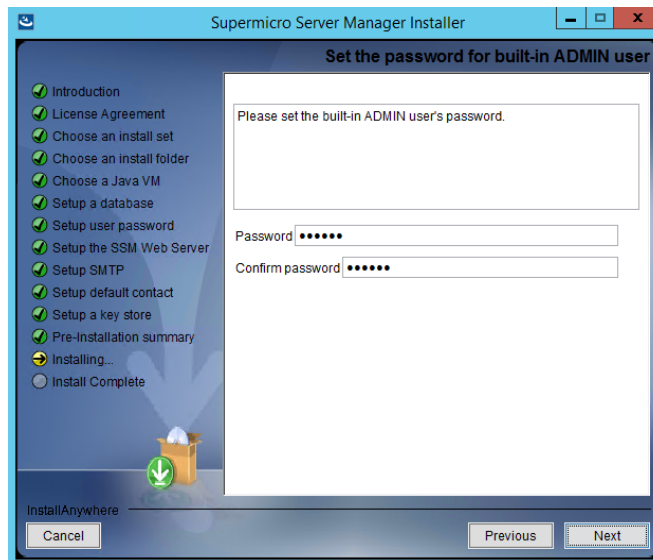


Figure 2-44

4. Please wait while the data of the current version of SSM is backed up.

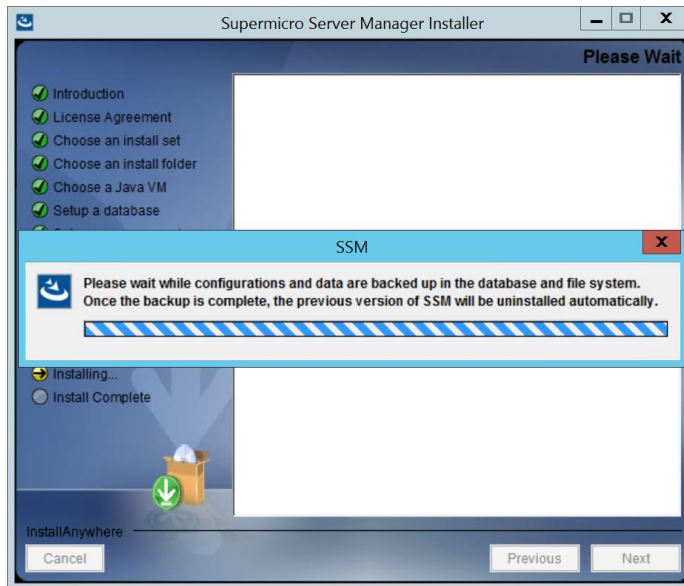


Figure 2-45

5. Please wait while the data is restored in the newer version of SSM.

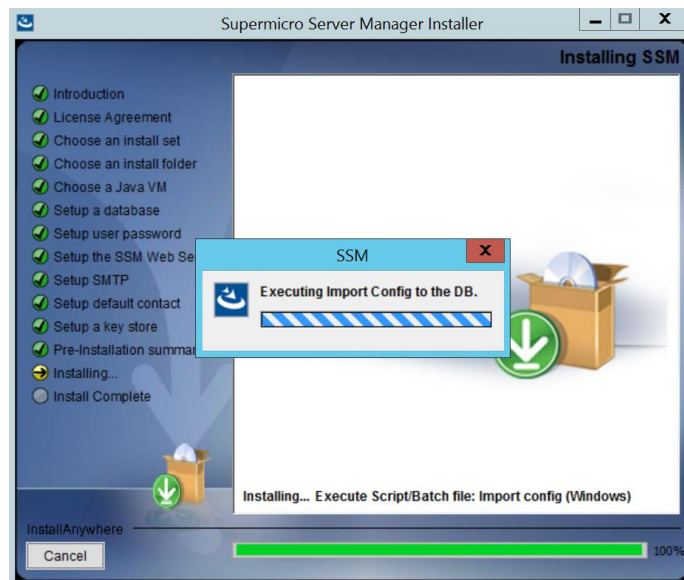


Figure 2-46

6. The upgrade is complete. Click the **Done** button to exit.

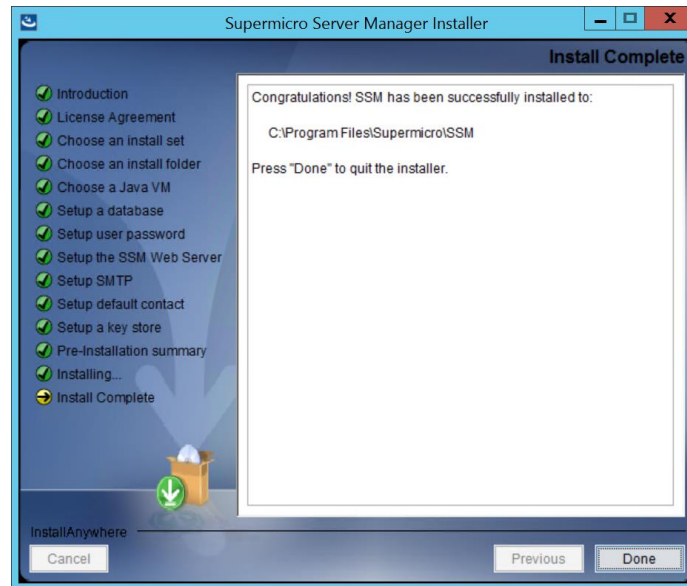


Figure 2-47



Note: If an error message appears onscreen, check the file `[install folder]/installLog/installer_debug_upgrade_backup_error.txt` or the log files generated in both the `[install folder]/Uninstall/Logs/` and `[install folder]/installLog/` folders. These files can be used for debugging. At the same time, it is highly recommended that you restore your SSM back to its earlier version and refer to *2.8.3 Restoring SSM after Auto-Upgrade Fails* for details.

2.8.2 Upgrading in Linux

You must have root privileges to install SSM. To upgrade SSM in Linux, follow these steps.

1. Execute the SSMInstaller.
2. Select **Yes** to back up the data of the current version of SSM and press the **<Enter>** key to continue.

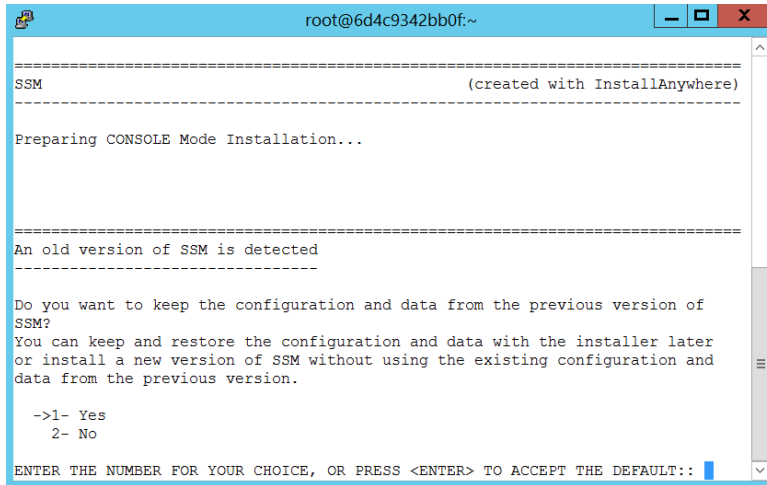


Figure 2-48

3. Please wait while the data of the current version of SSM is backed up. Note that you will be forced to change the password if “ADMIN” is detected to be the password for the built-in ADMIN account.

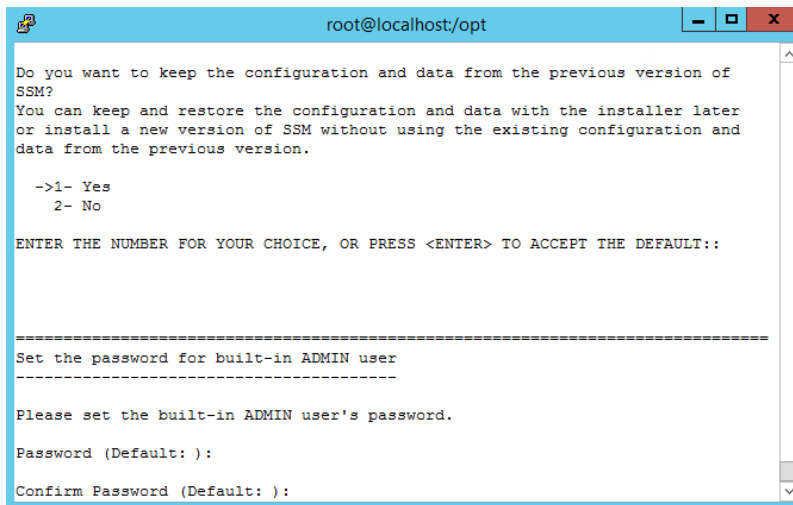


Figure 2-49

4. Please wait while the newer version of SSM is installed and the older version is uninstalled.

```

root@localhost/opt
-----
Please wait, this may take a few minutes.
...*
*
*****
*****
*****
*****
...*
*
*****
*****
*****
*****
-----
Installing...
-----
[=====|=====|=====|=====]
[-----|-----|-----|-----]

```

Figure 2-50

5. The upgrade is complete. Press the <Enter> key to exit.

```

root@localhost/opt
-----
Installing...
-----
[=====|=====|=====|=====]
[-----|-----|-----|-----]
-----
Installation Complete
-----
Congratulations. SSM has been successfully installed to:
/opt/Supermicro/SSM
SSM Web URL
URL https://localhost:8443
Copyright (c) 1993-2019 Super Micro Computer, Inc.
PRESS <ENTER> TO EXIT THE INSTALLER:

```

Figure 2-51



Note: If an error message appears onscreen, check the file `[install folder]/installLog/installer_debug_upgrade_backup_error.txt` or the log files generated in both the `[install folder]/Uninstall/Logs/` and `[install folder]/installLog/` folders. These files can be used for debugging. At the same time, it is highly recommended that you restore your SSM back to its earlier version and refer to *2.8.3 Restoring SSM after Auto-Upgrade Fails* for details.

2.8.3 Restoring SSM after Auto-Upgrade Fails

When SSM fails to auto-upgrade, it is highly recommended that you follow these steps to restore SSM:

1. Uninstall SSM. Refer to *2.6 Uninstalling SSM* for details. Note that it's recommended you delete the [Install folder] after uninstalling SSM in order to remove SSM completely.

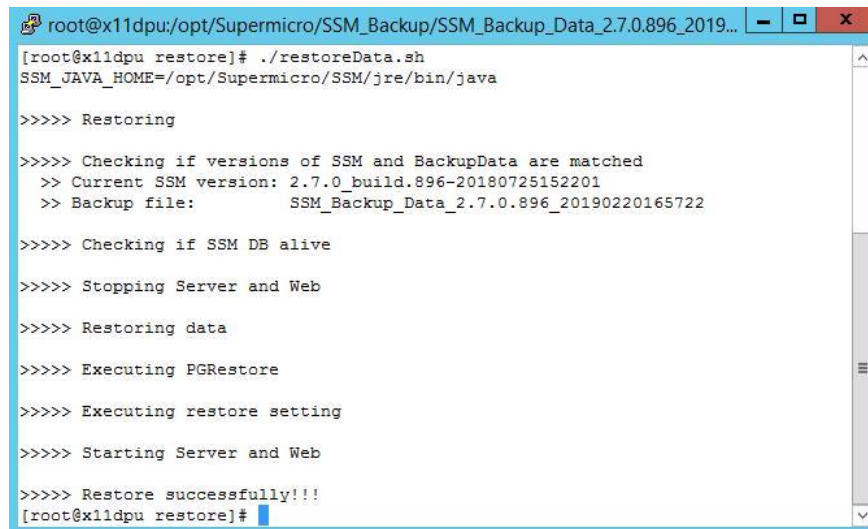
2. Execute the SSMInstaller from the previous version. Refer to *2.1 Installing SSM* for details. Note that if you've installed SSM 2.7.0 build 896 before, you need to install this version again.
3. Find **SSM_Backup_Data_[x].[y].[z].[###]_[timestamp].tar.gz** in the `./SSM_Backup/./[install folder]` folder. Note that each time you execute the SSMInstaller for an auto-upgrade, the installer builds a snapshot (`.tar.gz`) file to back up files such as configuration data, settings, and reports. You may select the latest snapshot (`.tar.gz`) file for restoration.
4. Extract the snapshot (`.tar.gz`) file and locate the `restoreData.sh/.bat` file.



```
root@x11dpu:/opt/Supermicro/SSM_Backup/SSM_Backup_Data_2.7.0.896_2019...  
[root@x11dpu restore]# pwd  
/opt/Supermicro/SSM_Backup/SSM_Backup_Data_2.7.0.896_20190220165722/restore  
[root@x11dpu restore]# ls  
config  libs  restoreData.bat  restoreData.sh  
[root@x11dpu restore]#
```

Figure 2-52

5. Execute the recovery program (“`restoreData.bat`” in Windows and “`restoreData.sh`” in Linux) to restore SSM back to its earlier version.



```
root@x11dpu:/opt/Supermicro/SSM_Backup/SSM_Backup_Data_2.7.0.896_2019...  
[root@x11dpu restore]# ./restoreData.sh  
SSM_JAVA_HOME=/opt/Supermicro/SSM/jre/bin/java  
  
>>>> Restoring  
  
>>>> Checking if versions of SSM and BackupData are matched  
>> Current SSM version: 2.7.0_build.896-20180725152201  
>> Backup file: SSM_Backup_Data_2.7.0.896_20190220165722  
  
>>>> Checking if SSM DB alive  
  
>>>> Stopping Server and Web  
  
>>>> Restoring data  
  
>>>> Executing PGRestore  
  
>>>> Executing restore setting  
  
>>>> Starting Server and Web  
  
>>>> Restore successfully!!!  
[root@x11dpu restore]#
```

Figure 2-53

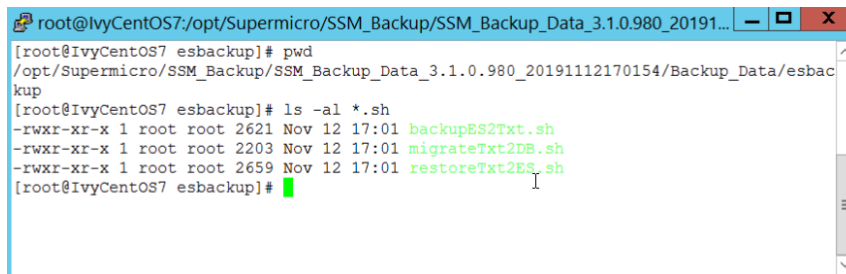
2.8.4 Restoring Alert History of Service Calls



Note: If your SSM is earlier than version 3.2 and you plan to upgrade to the latest version, refer to this section for details. Otherwise you may skip this section.

Since SSM version 3.2, the internal database of service calls has been merged into the SSM's PostgreSQL database. By default, three months of alert history is automatically kept in this database. If you wish to keep a longer alert history, follow these steps:

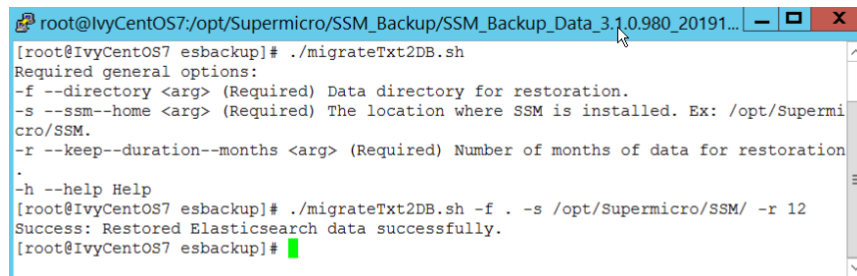
1. Find **SSM_Backup_Data_[x].[y].[z].[###]_[timestamp].tar.gz** in the `./SSM_Backup/./[install folder]` folder. Note that each time you execute the SSMInstaller for an auto-upgrade, the installer builds a snapshot (.tar.gz) file to back up files such as configuration data, settings, and reports. You need to select the file with its build date and time closest to your first upgrade.
2. Extract the selected snapshot (.tar.gz) file and locate the `migrateTxt2DB.sh/.bat` file (under `SSM_Backup_Data_[x].[y].[z].[###]_[timestamp]/Backup_Data/esbackup` folder).



```
root@IvyCentOS7:/opt/Supermicro/SSM_Backup/SSM_Backup_Data_3.1.0.980_2019112170154/Backup_Data/esbackup
[root@IvyCentOS7 esbackup]# pwd
/opt/Supermicro/SSM_Backup/SSM_Backup_Data_3.1.0.980_2019112170154/Backup_Data/esbackup
[root@IvyCentOS7 esbackup]# ls -al *.sh
-rwxr-xr-x 1 root root 2621 Nov 12 17:01 backupES2Txt.sh
-rwxr-xr-x 1 root root 2203 Nov 12 17:01 migrateTxt2DB.sh
-rwxr-xr-x 1 root root 2659 Nov 12 17:01 restoreTxt2ES.sh
[root@IvyCentOS7 esbackup]#
```

Figure 2-54

3. Execute the data migration program (“`migrateTxt2DB.bat`” in Windows and “`migrateTxt2DB.sh`” in Linux) to restore the alert history. Note that by default the backed-up alert history is in the same folder as the `migrateTxt2DB` tool.



```
root@IvyCentOS7:/opt/Supermicro/SSM_Backup/SSM_Backup_Data_3.1.0.980_2019112170154/Backup_Data/esbackup
[root@IvyCentOS7 esbackup]# ./migrateTxt2DB.sh
Required general options:
-f --directory <arg> (Required) Data directory for restoration.
-s --ssm--home <arg> (Required) The location where SSM is installed. Ex: /opt/Supermicro/SSM.
-r --keep--duration--months <arg> (Required) Number of months of data for restoration
.
-h --help Help
[root@IvyCentOS7 esbackup]# ./migrateTxt2DB.sh -f . -s /opt/Supermicro/SSM/ -r 12
Success: Restored Elasticsearch data successfully.
[root@IvyCentOS7 esbackup]#
```

Figure 2-55

Part 2 SSM Server

3 SSM Server Configurations

This chapter introduces the configuration objects for the SSM Server. The SSM Server uses nine types of configuration objects including **instance**, **host**, **hostgroup**, **service**, **contact**, **contactgroup**, **command**, **timeperiod**, and **ptpolicy**. These objects are essential for the SSM Server to perform monitoring, control, and management functions. For example, to monitor the memory health of a computer, a service object needs to be created. The **check_interval** attribute of the service object tells the SSM Server how frequently the service should be checked. The **check_command** attribute of the service object specifies the command (a program such as a shell script or a native program) used to check the service. Configuration objects also tell the SSM Server when and how to send alert messages and to whom the alerts should be sent.

3.1 SSM Server Operational Concept

To use the SSM Server to perform monitoring, control, and management functions, you need to define a **managed environment** by using configuration objects. First you define a host object, which represents a server, a desktop computer, a router, or a network printer to be monitored. Basically, devices that can be accessed via a network can be regarded as a host. Next, you define the services on the host. The services, also known as **monitored items**, include hardware-related items such as CPU temperature, fan speed, power consumption, and voltage as well as software-related items such as email servers, Web servers, and FTP servers. Services also include data such as CPU loading, free disk space, and concurrent database transactions. **Hosts** and **Servers** are two subjects monitored and managed by SSM. A host can contain multiple services; a service must belong to a host. When the status of hosts and services has changed, the SSM Server sends alert messages to its users. To receive alerts, you need to define **contacts** and assign the contacts to the hosts and services.

You can tell the SSM Server how to check the health of a host and a service by defining a **command** object, which links to a plug-in (a shell script or a native program) and keeps the necessary arguments required by the plug-in. Each host and service uses a command to check its health.

Suppose that you, David, are the administrator of two servers: mail.supero.com and web.supero.com. You run these servers on mail.supero.com and web.supero.com, respectively. You want to monitor these two servers and receive alerts when the CPU is overheating or when the Web and mail services are not accessible. To simplify your life, you use SSM to do the monitoring for you. First, you define a host object to represent the server mail.supero.com. You then define three services for CPU temperature, the email server, and the Web server. Next, for each service object, you define a command to check the service. Finally, you define a contact, David, and assign the contact to the hosts and service objects.

After setting this up, you will receive email alerts if the hosts and services encounter problems. You can login to the SSM Web to view their status using a Web browser.



Note: SSM configuration objects can be stored in the SSM Database or in text files. By default, the configuration data is stored in the SSM Database. You do not need to manually write configuration objects. The SSM Web provides an easy-to-use interface to manage these configuration objects. See *6.15 Host Discovery Wizard*, *6.2.3 Add Service Wizard*, *6.3 Host Group Management*, *6.4 Contact Management*, *6.5 Contact Group Management*, *7.3.6 Host Admin Commands*, and *7.3.8 Service Admin Commands* for more information.

3.2 Configuring the SSM Server with Files

The SSM Server's configuration data is stored in the SSM Database. One way to manipulate the configuration data in the SSM Database is to use administration functions provided by the SSM Web. Alternatively, you can use the utility program named **innoutconfig** provided by SSM to export configuration data from the SSM Database to files and to import configuration data from files to the SSM Database. In most situations, you do not need to export configuration data to files for modification. However, for advanced users who want to extend SSM by themselves, understanding how to configure the SSM Server with files is necessary.

There are three types of configuration files: the **main configuration file**, **object definition files**, and **resource files**. The main configuration file is the first file from which the SSM Server reads its configuration data. Object definition and resource files are included in the main configuration file with the **cfg_file/cfg_dir** and **resource_file** directives, respectively. The main configuration files located in the **[install folder]\shared\config** folder are named **ssm_win.cfg** and **ssm_linux.cfg** for Windows and Linux platforms, respectively. Object definition and resource files must be placed in the **[install folder]\shared\config** folder. You can also create sub-folders under the **[install folder]\shared\config** folder to organize configuration files. Always use **relative paths** to specify folders or files in configuration files. Note that **spaces are not allowed** in directive statements. A main configuration file example is shown below.

```
# A single line comment.
```

```
resource_file=resource_linux.cfg  
cfg_dir=builtin  
cfg_dir=generated  
cfg_file=localhost.cfg
```

```
#cfg_dir = local
```

```
#cfg_file=My personal file.cfg
```

```
# The above two statements are incorrect because they contains spaces.
```

1. The **resource_file** directive tells the SSM Server where to read custom macros. Custom macros are user-defined variables that can be used throughout the whole SSM system. The `resource_file` directive must be placed on the top of the main configuration file.
2. The **cfg_file** directive tells the SSM Server where to read an object definition file.
3. The **cfg_dir** directive tells the SSM Server where to read all object definition files in a folder. In the above examples, the SSM Server will read configuration files from the built-in and generated folders.
4. The **#** character indicates a single line comment.

The configuration files are used not only by the SSM Server, but also by SSM Web and SSM CLI. When you use the **innoutconfig** program to export configuration data from the SSM Database without specifying a target folder, configuration files are stored in **[install folder]\shared\config\builtin** and **[install folder]\shared\config\generated**. See *15.1 Export and Import Configuration Data* for more information. The former is used to store built-in configuration objects, which should not be modified by users. The latter stores generated configuration objects at runtime when hosts and services are discovered by SSM.

3.3 SSM Server Configuration Objects

3.3.1 Instance Definitions

An instance refers to an instance of the SSM Server. SSM was designed to support multiple instances in a managed domain for load sharing. The current implementation of SSM only supports one instance. The definition of an instance object is shown below.

```
define instance {
    instance_name           default
    description             default instance of SSM
    heartbeat_interval      300
    service_check_timeout  120
    host_check_timeout     30
    notification_timeout   30
    max_thread_count       50
    job_monitoring_interval 20
    sync_watcher_interval  10
    port                   5111
    use_implied_contact    1
    use_implied_contactgroup 1
    check_scheduled_ptpolicy_interval 60
    recalc_ptpolicy_interval 120
    aggregate_power_interval 120
    db_maintenance_time    00:00
    db_maintenance_command db_maintenance!2!12!0
    db_maintenance_command_timeout 14400
}
```

instance_name*

This attribute is used to define a unique name used to identify the instance (i.e., an instance of the SSM Server).

description*

This attribute is used to define the description of the instance.

heartbeat_interval*

This attribute specifies the interval in seconds between heartbeats of the SSM Server

and is sent to the SSM Database to measure the health of the SSM Server.

service_check_timeout

This attribute is used to specify the number of seconds before a service check times out.

host_check_timeout

This attribute is used to specify the number of seconds before a host check times out.

notification_timeout

This attribute is used to specify the number of seconds before a notification times out.

max_thread_count

This attribute defines the maximum size of concurrently executed threads used to perform host and service checks.

job_monitoring_interval

This attribute specifies the interval in seconds between checks for misfired jobs. On an overloaded computer, a scheduled job may not be executed on time. The SSM Server regularly checks this situation according to the value of this attribute and reschedules the misfired jobs.

sync_watcher_interval*

This attribute specifies the interval in seconds between attempts to synchronize the SSM data model with the SSM Database. Users can change the configuration data in the SSM Database when, for example, they add hosts to the SSM Database with the Host Discovery Wizard provided by SSM Web. This attribute tells the SSM Server how often it should synchronize with the SSM Database to update its runtime data model.

port*

This attribute defines the network port number used to indicate that an instance of the SSM Server is running. The SSM Server cannot be started if this port is occupied by another application.

use_implied_contact

This attribute tells the SSM Server whether to notify contacts of a host when the status of the host's services changes. If this attribute is set to 1, you do not need to assign a contact to each service of a host to receive service notification. Just assign a contact to the host and the contact will receive service notification every time the status of a service on the host changes. The default value is 1.

use_implied_contactgroup

This attribute tells the SSM Server whether to notify the contactgroups of a host when the status of the host's services changes. If this attribute is set to 1, you do not need to assign a contactgroup to each service of a host to receive service notification. Just assign a contactgroup to the host and all contacts in the contactgroup will receive service notification every time the status of a service on the host changes. The default value is 1.

check_scheduled_ptpolicy_interval

This attribute specifies the interval in seconds between attempts to check whether a scheduled policy should be activated or deactivated. The default value is 60 seconds.

recalc_ptpolicy_interval

This attribute specifies the interval in seconds between attempts to calculate the power limit for every NM host according to the policies of individual hosts and a group of hosts. The SSM Server will assign the calculated power limit to all NM hosts to cap their power consumption. The default value is 120 seconds.

aggregate_power_interval

This attribute specifies the interval in seconds between attempts to aggregate power consumption of hosts in a host group. The aggregated data is used to display a host group's power consumption trend. The default value is 120 seconds.

db_maintenance_time*

This attribute defines the time to execute a database maintenance program provided by SSM. The program will perform data aggregation tasks and remove raw performance data as well as monitor historical data to reduce the space needed by the SSM Database.

db_maintenance_command*

This attribute defines the command and arguments to execute a database maintenance program.

db_maintenance_command_timeout

This attribute specifies the number of seconds before a database maintenance program times out. The default value is 14400 seconds (4 hours).

(* indicates a required attribute)

3.3.2 Host Definitions

A host object represents a network device such as a computer, a network printer, or a hub. The definition of a host object is shown below.

```
define host{
    host_name          ipmi-kira
    alias              ipmi-kira
    address            192.168.12.4
    hostgroups         all-ipmi_server, Room_803
    check_period       24x7
    contacts           admin_us, admin_tw
    contact_groups     admin_us_groups, admin_tw_groups
    notification_period 24x7
    notification_interval 30
    max_check_attempts 3
    check_interval     120
    retry_interval     20
    check_command      ping
    notifications_enabled 1
    ipmi_id            ADMIN
    ipmi_password      <encoded-ADMIN-password>
    wol_mac_address    00-30-48-5B-D8-CC
    derated_ac_power   504
    derated_dc_power   432
    power_limit_base   0
    max_power_limit    32767
    power_limit_type   1
    max_report_period  3600
    max_ps_output      720
    max_correction_time 600
    min_report_period  1
    min_correction_time 6
    contain_perf_data  0
    process_perf_data  0
    nrpe_keypair_port  5999
    ipmi_mac_address   00:25:90:01:E7:EE
}
```

host_name*

This attribute specifies a unique name used to identify the host. The maximum size of this attribute is 64 characters in ASCII code.

alias*

This attribute specifies a description of the host.

address*

This attribute defines the network address of the host. It could be an IP address or a DNS name.

Hostgroups

This attribute refers to the hostgroup names that the host belongs to. Multiple values are separated by commas.

check_period*

This attribute refers to the name of a timeperiod object. The SSM Server performs a host check at the time period specified by the referred timeperiod object. This is a reserved attribute. Currently, only the built-in **24x7** timeperiod object is supported.

contacts*

This attribute refers to the names of contacts that are used to receive host notifications. Multiple values are separated by commas.

contact_groups*

This attribute refers to the names of contact groups that are used to receive host notifications. Multiple values are separated by commas.

notification_period*

This attribute refers to the name of a timeperiod object defining a time period for

sending notifications. Notifications occurring outside the notification period are ignored and are not sent to contacts. This is a reserved attribute. Currently, only the built-in 24x7 timeperiod object is supported.

notification_interval*

This attribute is reserved for future use.

max_check_attempts*

This attribute defines the maximum retry counts of the host until triggering a hard state change alert from an UP state to a non-UP status (i.e., DOWN or UNREACHABLE). When a host is in an UP state and the host check command returns a non-UP state, the SSM Server will retry the host check command to avoid false alarms due to transient problems such as network connection disruptions and host overloading. During the retry period, the host is in a soft state and will not trigger an alert. Setting this value to 1 indicates that no retry is attempted and an alert is generated immediately when a host state changes from UP to non-UP.

check_interval*

This attribute specifies the interval in seconds between host checks and is executed to measure its status.

retry_interval*

This attribute specifies the interval in seconds between checks of a host that is in soft state.

check_command*

This attribute refers to the name of a command object used to check the host. By default, a host is checked with the ping command provided by the operating system.

notifications_enabled*

This attribute is used to enable or disable host notifications. A value of 0 means disable and 1 means enable. If this attribute is set to 0, no host notifications will be sent.

ipmi_id

This attribute defines the user account to access IPMI BMC.

ipmi_password

This attribute defines the encoded password to access IPMI BMC. Note that when you use the innoutconfig program, use "<your-BMC-password>" in plain text to import ipmi_password into the SSM Database. For exporting configuration data from an SSM Database to files, the value of ipmi_password attribute is encoded.

wol_mac_address

This attribute specifies the MAC address of the host. It is used to send magic packets of Wake-on-LAN to power up the host.

power_limit_base

This attribute is reserved for future use.

max_power_limit

This attribute is reserved for future use.

power_limit_type

This attribute is reserved for future use.

max_report_period

This attribute is reserved for future use.

derated_dc_power

This attribute specifies the power supply's derated DC power of the host. This attribute is only applicable to NM hosts. When the SSM Server monitors the power consumption of an NM host, it monitors both DC and AC power and uses the values in the power consumption trend function. If the SSM Server cannot get DC power, it uses the value of this attribute to represent the host's DC power.

derated_ac_power

This attribute specifies the power supply's derated AC power of the host. This attribute is only applicable to NM hosts. When the SSM Server monitors the power consumption of an NM host, it monitors both DC and AC power and uses the values in the power consumption trend function. If the SSM Server cannot get AC power, it uses the value of this attribute to represent the host's AC power.

max_ps_output

This attribute specifies the maximum output of the power supply of the host. This attribute is only applicable to NM hosts. With this value, the host's power efficiency and loading can be calculated.

max_correction_time

This attribute is reserved for future use.

min_report_period

This attribute is reserved for future use.

min_correction_time

This attribute is reserved for future use.

contain_perf_data

This attribute indicates if the host check contains performance data.

process_perf_data

This attribute tells the SSM Server whether to process the performance data (i.e., to store the performance data in the SSM Database). This attribute is handled by the SSM Server only if a host contains performance data (i.e., the contain_perf_data attribute of the host is set to 1). Otherwise, the SSM Server ignores this attribute.

nrpe_keypair_port

This attribute specifies the port number connecting to a SuperDoctor 5 acceptor.

ipmi_mac_address

This attribute specifies the IPMI MAC address of the host.

(* indicates a required attribute)



Note: Either one contact or one contact group must be specified in a host definition.

3.3.3 Host Group Definitions

Host groups are used to organize hosts and define the hierarchy of hosts through nested host groups. One host could belong to multiple host groups and one host group could contain other host groups. Host groups provide the group management functions of SSM Web and SSM CLI. That is, many commands can be applied to all hosts in a host group. The definition of a host object is shown below.

```
define hostgroup{
    hostgroup_name      all-ipmi
    alias               all-ipmi
    members             ipmi-1, ipmi-2 ,ipmi-kira
    hostgroup_members  all-blade
    hostgroup_type      0
}
```

hostgroup_name*

This attribute specifies a unique name used to identify the host group. The maximum size of this attribute is 128 characters in ASCII code.

alias*

This attribute specifies a description for the host group.

members

This attribute refers to the names of hosts belonging to this host group. Multiple values are separated by commas.

hostgroup_members

This attribute refers to the host group names belonging to this host group. Multiple values are separated by commas.

hostgroup_type

This attribute specifies the hostgroup type. A hostgroup is either a logical group or a physical group. A value of 0 represents a logical group and a value of 1 represents a

physical group. A host can belong to any number of logical groups but can only belong to one physical group. Physical host groups contain only physical host group members but not logical ones. SSM provides four built-in physical groups: datacenter, room, row, and rack. A physical group must be one of the four types.

granularity

The grain size of a physical group. A physical group with larger granularity can contain one with smaller granularity. For example, the granularity values of the built-in physical groups datacenter, room, row, and rack are 5, 4, 3, and 2, respectively.

(* indicates a required attribute)

3.3.4 Service Definitions

A service object represents a “service” running on a host. Services take many forms, such as the attributes and functions of an HTTP server, an email server, a database, or an application. Services could be the attributes of a host or an application, such as CPU temperature, fan speed, the amount of free disk space, the status of a daemon, or the response time to access a database application. The SSM Server performs a service check based on the service definitions. Service object definitions are shown below.

```
define service {
    host_name          localhost
    service_description All System Information
    check_command      jcheck_sysinfo
    max_check_attempts 3
    check_interval     300
    retry_interval     1
    check_period       24x7
    notifications_enabled 1
    notification_interval 120
    notification_period 24x7
    contacts           admin
    contact_groups     admin_group
    contain_perf_data  0
    process_perf_data  0
}
```

host_name*

The host name that the service belongs to.

service_description*

This attribute specifies a description of the service. The maximum size of this attribute is 100 characters in ASCII code.

check_command*

This attribute refers to the name of a command object used to check the service.

max_check_attempts*

This attribute defines the maximum retry counts of the service before triggering a service state change alert from an OK state to a non-OK status (i.e., UNKNOWN or CRITICAL). When a service is in an OK state and the service check command returns a non-OK state, the SSM Server will retry the service check command to avoid false alarms due to transient problems such as network connection disruptions and host overloading. During the retry period, the service is in a soft state and will not trigger an alert. Setting this value to 1 indicates that no retry is attempted and an alert is generated immediately when a service state changes from OK to non-OK.

check_interval*

This attribute specifies the interval in seconds between checks of the service and is executed to measure its status.

retry_interval*

This attribute specifies the interval in seconds between checks of a service that is in soft state.

check_period*

This attribute refers to the name of a timeperiod object. The SSM Server performs a service check at the time period specified by the referred timeperiod object. This is a reserved attribute. Currently, only the built-in **24x7** timeperiod object is supported.

notifications_enabled*

This attribute is used to enable or disable service notifications. A value of 0 means disable and 1 means enable. If this attribute is set to 0, no service notifications will be sent.

notification_interval*

This attribute is reserved for future use.

notification_period*

This attribute refers to the name of a timeperiod object defining a time period for sending notifications. Notifications occurring outside the notification period are ignored and are not sent to contracts. This is a reserved attribute. Currently, only the built-in **24x7** timeperiod object is supported.

contacts*

This attribute refers to the names of contacts that are used to receive service notifications. Multiple values are separated by commas.

contact_groups*

This attribute refers to the names of contact groups that are used to receive service notifications. Multiple values are separated by commas.

contain_perf_data

This attribute indicates if the service check contains performance data.

process_perf_data

This attribute tells the SSM Server whether to process the performance data (i.e., to store the performance data in the SSM Database). This attribute is handled by the SSM Server only if a service contains performance data (i.e., the contain_perf_data attribute of the service is set to 1). Otherwise, the SSM Server ignores this attribute.

(* indicates a required attribute)



Notes:

- The combination of the `host_name` and the `service_description` used to identify a service must be unique.
- Either one contact or one contact group must be specified in a service definition.

3.3.5 Contact Definitions

Contacts are used to define a person who will receive notifications when the status of a host or a service changes. The definition of a contact object is shown below.

```
define contact {
    contact_name          admin-tw
    alias                 Administrator in Taiwan
    contactgroups         admins
    host_notification_options d, r, u
    host_notifications_enabled 0
    host_notification_period 24x7
    host_notification_commands host-notify-by-email,host-notify-by-snmpttrap,
    host-notify-by-locallogger

    service_notification_options c,r,u,w
    service_notifications_enabled 0
    service_notification_period 24x7
    service_notification_commands service-notify-by-email,service-notify-by-snmpttrap,
    service-notify-by-locallogger

    pager                011-44-1234-567890#123
    email                admin_tw@xyz.com
    address1             10.134.14.36:162
}
```

`contact_name*`

This attribute defines a unique name of the contact. The maximum size of this attribute is 64 characters in ASCII code.

`alias*`

This attribute specifies a description of the contact.

contactgroups

This attribute refers to the contactgroup names that the contact belongs to. Multiple values are separated by commas.

host_notification_options

This attribute defines the host states for which notifications can be sent out to the contact. Valid options are d (DOWN), r (UNREACHABLE), and u (UP).

host_notifications_enabled*

This attribute is used to enable or disable host notifications. A value of 0 means disable and 1 means enable. The contact cannot receive any host notifications if this attribute is set to 0.

host_notification_period*

This attribute refers to the name of a timeperiod object that defines a time period for receiving host notifications. Host notifications occurring outside the period are ignored and are not sent to contacts. This is a reserved attribute. Currently, only the built-in 24x7 timeperiod object is supported.

host_notification_commands*

This attribute is used by the SSM Server to send host notifications. Multiple values are separated by commas.

service_notification_options

This attribute defines the service states for which notifications can be sent out to the contact. Valid options are c (Critical), r (OK), u (Unknown) and w (Warning).

service_notifications_enabled*

This attribute is used to enable or disable service notifications. A value of 0 means disable and a value of 1 means enable. The contact cannot receive any service

notifications if this attribute is set to 0.

`service_notification_period*`

This attribute refers to the name of a timeperiod object that defines a time period for receiving service notifications. Service notifications occurring outside the period are ignored and are not sent to contacts. This is a reserved attribute. Currently, only built-in 24x7 timeperiod objects are supported.

`service_notification_commands*`

This attribute is used by the SSM Server to send service notifications. Multiple values are separated by commas.

`email`

This attribute defines the email address of the contact.

`pager`

This attribute defines the phone number of the contact.

`address1`

This attribute defines the SNMP trap recipients of the contact. Multiple recipients are separated by a comma.

`address2 to address6`

These five attributes define extra notification addresses of the contact.

(* indicates a required attribute)

3.3.6 Contact Group Definitions

Contact groups are used to organize contacts. They can be used as host and service notification receivers whenever a contact is applied. A contact group can have multiple contacts but cannot contain other contact groups. In other words, nested contact groups are not supported.

```
define contactgroup{
    contactgroup_name    admins
    alias                Administrators
    members              admin-tw, admin-us
}
```

contactgroup_name*

This attribute specifies a unique name used to identify the contact group. The maximum size of this attribute is 128 characters in ASCII code.

alias*

This attribute specifies a description of the contact group.

members*

This attribute refers to the names of contacts that belong to this contact group. Multiple values are separated by commas.

(*indicates a required attribute)

3.3.7 Command Definitions

A command object specifies a server-side plug-in (a shell script or a native program) that is used by the SSM Server to perform host and service checks as well as for sending notifications. The definition of a command object is shown below.

```
define command{
  command_name      check_http
  command_line      ..\shared\builtin\check_http.bat http://$HOSTADDRESS$: $ARG1$
}
```

command_name*

This attribute specifies a unique name used to identify the command.

command_line*

This attribute defines a plug-in and its arguments.

(* indicates a required attribute)

3.3.8 Time Period Definitions

A time period object defines a time range such as “working hours”, “maintenance hours”, and “national holidays”. This is a reserved object and users should not define or use other time period objects except for the built-in **24x7** time period object, which represents 24 hours a day and 7 days a week.

```
define timeperiod{
  timeperiod_name    24x7
  alias              Everyday
}
```

timeperiod_name*

This attribute specifies a unique name used to identify the time period. The maximum size of this attribute is 64 characters in ASCII code.

alias*

This attribute specifies a description used to describe the time period.

(* indicates a required attribute)

3.3.9 PTPolicy Definitions

A ptpolicy object defines power consumption limitations for an individual NM host and a group of NM hosts. When a ptpolicy applies to an individual NM host, it specifies a **static power limit** that the host should obey. For example, a host ptpolicy with a **threshold** value of 600 defines a power usage policy in which the corresponding host should not use more than 600W of power. When a ptpolicy applies to a host group, it specifies a **custom power limit** (also known as **dynamic power limit**) that all NM hosts in the host group should obey. The ptpolicy keeps a priority for each NM host in the host group. The SSM Server periodically uses the priority values, the previous calculated power limit value, and the **current power consumption** of each NM host as reported by the Power Consumption service to calculate a power limit of each NM host. It is called a custom or dynamic power limit because the calculated power limit may change over time due to the fact that the current power consumption value of a NM host may change over time. Basically, if all NM hosts in the same host group have the same priority, those that consume more power will be assigned more power.

A ptpolicy, whether static or custom, can be either **permanent** or **scheduled**. A permanent policy takes effect all the time once it is enabled. A scheduled policy takes effect only during its predefined time period.

```
define ptpolicy {
    ptpolicy_name      Room803_Policy
    description        60000W policy for Room803 group
    policy_type        1
    threshold          60000.0
    enabled            1
    permanent          1
    hostgroup_name     Rack1
    medium_host_members Web-001, Web-002
    low_host_members   Batch-Job
    critical_hostgroup_members DB-Group
    reserved_budget    0.0
    nmpolicy_id        8
}
```

ptpolicy_name*

This attribute specifies a unique name used to identify the ptpolicy. The maximum size of this attribute is 128 characters in ASCII code.

description

This attribute specifies the description of the ptpolicy.

policy_type

This attribute specifies the type of policy. A value of 0 means static power limit and 1 means custom power limit. A static power limit policy is directly applied to an individual NM host while a custom power limit policy is first calculated by the SSM Server before being applied to NM hosts.

threshold

This attribute specifies a power limit threshold for the ptpolicy.

enabled

This attribute is used to enable or disable the ptpolicy. A value of 0 means disable and 1 means enable. If this attribute is set to 0, the ptpolicy will not be processed by the SSM Server.

permanent

This attribute specifies whether the ptpolicy is permanent or scheduled. A value of 0 means scheduled and 1 means permanent. If this attribute is set to 0 (i.e., a scheduled power limit ptpolicy), the schedule_period attribute of the popolicy must be specified.

host_name

The host name that the ptpolicy belongs to.

hostgroup_name

The host group name that the ptpolicy belongs to.

medium_host_members

A list of host names belonging to a medium priority. Multiple values are separated by commas.

medium_hostgroup_members

A list of hostgroup names belonging to a medium priority. Multiple values are separated by commas.

low_host_members

A list of host names belonging to a low priority. Multiple values are separated by commas.

low_hostgroup_members

A list of hostgroup names belonging to a low priority. Multiple values are separated by commas.

high_host_members

A list of host names belonging to a high priority. Multiple values are separated by commas.

high_hostgroup_members

A list of hostgroup names belonging to a high priority. Multiple values are separated by commas.

critical_host_members

A list of host names belonging to a critical priority. Multiple values are separated by commas.

critical_hostgroup_members

A list of hostgroup names belonging to a critical priority. Multiple values are separated by commas.

reserved_budget

This attribute, which is applicable to host group policies only, defines a reserve power value that will not be allocated to the NM hosts of a host group. In other words, the actual power capping value equals the Threshold value minus the Reserve Budget value, which is called the **effective power budget** in SSM.

nmpolicy_id

This attribute refers to a policy ID in an NM. This attribute is updated by the SSM Server when users add a ptpolicy via the SSM Web interface. A value of 8 indicates this ptpolicy is active and is added to the NM. Any value rather than 8 indicates an inactive ptpolicy.

schedule_period

This attribute refers to a timeperiod name that is used to define a time period for a scheduled ptpolicy.

correction_time

The time in seconds for the NM to take action to meet an assigned power limit. This attribute is for SSM internal use.

report_period

The time in seconds for the NM to report power consumption statistics. This attribute is for SSM internal use.

exception_action

This attribute specifies an action taken by the NM when the power consumption exceeds the assigned power limit. This attribute is for SSM internal use.

(* indicates a required attribute)

3.3.10 The Use Attribute

SSM supports template objects to simplify configuration object definitions. A template object is similar to a regular object except that it is uniquely identified by the **name** attribute and its **register** attribute is set to 0. You can define common attributes and values in a template object and apply the template object to concrete object definitions with the **use** attribute. A concrete object inherits all attributes and values defined in a used template object and can override inherited attributes and values by redefining them. The definition of a service template object is shown below.

```
define service {  
    name                generic_service  
    check_period         24x7  
    max_check_attempts  3  
    check_interval       60  
    retry_interval       1  
    notification_interval 120  
    notifications_enabled 1  
    notification_period  24x7  
    notification_options w,u,c,r,f  
    contacts             admin  
    register            0  
}
```



Note: The register value in the above generic-service object is set to 0, which means that the generic-service is a template object. Since it is a template object, the SSM Server does not check its status and it is not shown in SSM Web. Template objects are used to define common and generic attributes that can be reused by concrete objects.

```

define service {
    use                generic-service
    host_name          localhost
    hostgroup_name     all-IPMI
    service_description System Information
    check_command       jcheck_sysinfo
    max_check_attempts 3
    check_interval     300
    contacts            localadmin
}

```

The definition of a concrete service object using the `generic_service` template object is shown above. The System Information service uses the `generic-service` template and as a result inherits the attributes defined in the template. For example, the `check_period` and `notification_interval` attributes in the System Information service are 24x7 and 120, respectively. However, the `contact` attribute defined in the template as `admin` is overridden in the System Information service as `localadmin`.

3.4 Macros

Macros enclosed with the `$` character are variables whose value will be replaced by the SSM Server at runtime. The SSM server has several pre-defined macros such as `$HOSTADDRESS$` and `$HOSTSTATE$`. These macros are usually used in the `command_line` attribute of a command object to refer to static attributes or the dynamic status of a host or a service at runtime. For example, the following ping command uses the `$HOSTADDRESS$` macro to represent the host address of a host. Suppose that two hosts whose addresses are 192.168.12.3 and 192.168.10.88 are monitored by SSM. When the SSM Server uses the ping command to check the two hosts, the `command_line` of the ping command becomes `.\scripts\local\check_ping.bat 192.168.12.3 3` and `.\scripts\local\check_ping.bat 192.168.10.88 3`, respectively.

```

define command{
    command_name      ping
    command_line      .\scripts\local\check_ping.bat $HOSTADDRESS$ 3
}

```

The following table lists the macros supported by the SSM Server.

Macro Name	Description
NOTIFICATIONTYPE	The type of notification (“Problem”, “Recovery”)
CONTACTEMAIL	The email value of a contact object.
HOSTALIAS	The alias value of a host.
HOSTADDRESS	The address value of a host.
SERVICEDESC	The service_description value of a service.
SERVICESTATE	The status of the latest service check. (“OK”, “Warning”, “Critical”, or “Unknown”)
SERVICEOUTPUT	The first line of the output message of the latest service check.
LONGDATETIME	The time of host or service check in long datetime format, which is “yyyy/MM/dd HH:mm:ss.SS”. (year, month, day, hour, minute, second and microsecond.)
NOTIFICATIONHOST	The address of the SSM Server sending notifications.
INSTANCEID	The object id of an instance stored in the database.
HOSTOBJECTID	The object id of a host stored in the database.
SERVICEOBJECTID	The object id of a service stored in the database.
NRPE_KEYPAIR_PORT	The nrpe_keypair_port of a host.
IPMIID	The ipmi_id value of a host.
IPMIPWD	The ipmi_password value of a host.
IPMI_MACADDRESS	The ipmi_mac_address value of a host.
HOSTSTATE	The status of the latest host check (“UP”, “DOWN”, or “UNREACHABLE”).
HOSTOUTPUT	The first line of the output message of the latest host check.
WOLMACADDRESS	The wol_mac_address value of a host.

Macro Name	Description
NEWLINETOKEN	A new line token used to separate two lines.
CONTACTADDRESS1	The SNMP trap recipients of the contact.
CONTACTADDRESS2	The address2 value of a contact.
CONTACTADDRESS3	The address3 value of a contact.
CONTACTADDRESS4	The address4 value of a contact.
CONTACTADDRESS5	The address5 value of a contact.
CONTACTADDRESS6	The address6 value of a contact.
HOSTNAME	The host_name value of a host.
IPMIADDRESS	The ipmi_address value of a host.
HOSTPERFDATA	The performance data of a host check.
SERVICEPERFDATA	The performance data of a service check.
HOST_ENTERPRISE_OID	The enterprise OID of a host notification.
HOST_SPECIFIC_TYPE	The specific type of a host notification.
SERVICE_ENTERPRISE_OID	The enterprise OID of a service notification.
SERVICE_SPECIFIC_TYPE	The specific type of a service notification decided by the check_command of a service.
NOTIFICATIONTYPE_INDEX	The index of the type of notification for Recovery(0) and Problem(1).
NEWDQUOTETOKEN	A new double quote token used to represent double quote.
CONTACTPAGER	The phone value of a contact object.
HOSTSTATETYPE	The state type of the latest host check ("HARD" or "SOFT").
SERVICESTATETYPE	The state type of the latest service check ("HARD" or "SOFT").
HOSTATTEMPT	The retry counts of the latest host check.

Macro Name	Description
SERVICESTATETYPE	The retry counts of the latest service check.

4 SSM Server Built-in Commands

The SSM Server relies on server-side plug-ins to monitor the status of hosts and services. These plug-ins, called **commands** in this Chapter, are external programs that can be directly called by users. In other words, users can write scripts to invoke these commands according to their unique automation needs. Built-in commands include **check_ftp**, **check_http**, **check_ipmi**, **check_ping**, **check_smtp**, **check_wol**, and **jcheck_nrpe**. All of these commands are located in the `[install folder]\shared\builtin` folder, except the `jcheck_nrpe` command, which is located in the `[install folder]\shared\jcheck_nrpe` folder.

4.1 check_ftp

This command is used to check the health of an FTP server. To execute the command, use **check_ftp.bat** for Windows platforms and **check_ftp.sh** for Linux platforms.

Usage:

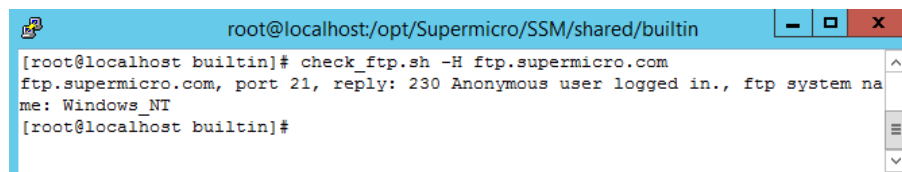
```
check_ftp [-H | --host <arg>] [-h | --help] [-p | --port <arg>] [-u | --name <arg>]
          [-w | --password <arg>]
```

Options:

- *-H, --host** The FTP server's IP address or a DNS name.
- h, --help** Shows the help menu.
- p, --port** The FTP server's port number. Default value is 21.
- u, --name** The user account to login to the FTP server. Default value is anonymous.
- w, --password** The password to login to the FTP server. Default value is anonymous.

(* indicates a required attribute)

Example:



```
root@localhost:/opt/Supermicro/SSM/shared/builtin
[root@localhost builtin]# check_ftp.sh -H ftp.supermicro.com
ftp.supermicro.com, port 21, reply: 230 Anonymous user logged in., ftp system na
me: Windows_NT
[root@localhost builtin]#
```

The execution results are shown in bold. Checking the exit code of the command can determine the status of the monitored FTP server. Exit code **0** indicates a normal status and exit code **2** indicates a critical status.

4.2 check_http

This command is used to check the health of an HTTP server. To execute the command, use **check_http.bat** for Windows platforms and **check_http.sh** for Linux platforms.

Usage:

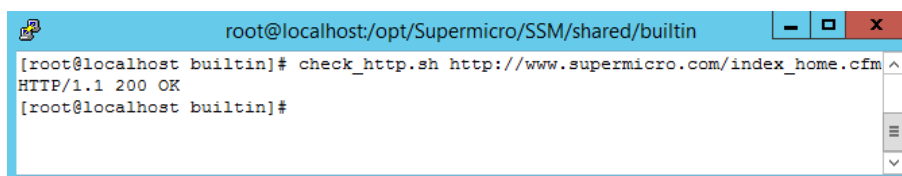
check_http URL

Options:

* **URL** The URL of the HTTP server.

(* indicates a required attribute)

Example:



```
root@localhost:/opt/Supermicro/SSM/shared/builtin
[root@localhost builtin]# check_http.sh http://www.supermicro.com/index_home.cfm
HTTP/1.1 200 OK
[root@localhost builtin]#
```

Exit code **0** indicates a normal status and exit code **2** indicates a critical status.

4.3 check_ipmi

This command is used to communicate with a remote IPMI BMC (i.e., an IPMI host). To execute the command, use **check_ipmi.bat** for Windows platforms and **check_ipmi.sh** for Linux platforms.

Usage:

check_ipmi [-a | --account <arg>] [-c | --changepassword <arg>] [-d | --definition]

[-da | --all] [-h | --help] [-hl | --highlimit <arg>] [-i | --ip <arg>]

[-ig | --ignore <arg>] [-l | --lan <arg>] [-ll | --lowlimit <arg>] [-n | --index <arg>]

[-p | --password <arg>] [-t | --type <arg>]

[-pc - crit <arg> -warn <arg>]

[-protocol]

Options:

<i>*-a, --account</i>	The account to login to the BMC.
<i>-c, --changepassword</i>	The new password to be set.
<i>-d, --definition</i>	Generates definitions of monitored items.
<i>-da, --all in one definition</i>	Generates all-in-one definitions of monitored items.
<i>-h, --help</i>	Shows the help menu.
<i>-hl, --highlimit</i>	The up threshold for the monitored item.
<i>*-i, --ip</i>	The IP address of the BMC.
<i>-l, --lan</i>	LAN Configuration
<i>-ll, --lowlimit</i>	The low threshold for the monitored item.
<i>-n, --index</i>	The number of the monitored item.
<i>*-p, --password</i>	The password to login to the BMC.
<i>-protocol</i>	The protocol used to communicate with the BMC.
<i>-t, --type</i>	
0	Shows the firmware and GUID.
1	Powers off the BMC host.
2	Powers on the BMC host.
3	Resets BMC power.
4	Powers off the host gracefully. The BMC raises an ACPI event that triggers a soft-shutdown of the OS.
5	Sets a new password for the ADMIN account.
6	Shows the SDR information of the BMC.
7	Shows the index and name information of all sensors monitored by the BMC.

- 8 Shows index, name and status information of all sensors monitored by the BMC.
- 9 Shows the status of the all-in-one monitored items.
- 10 Resets chassis intrusion.
- 11 BMC cold reset
- 12 Enables the UIDLED
- 13 Disables the UIDLED

(* indicates a required attribute)

Example:

```

root@localhost/opt/Supermicro/SSM/shared/builtin
[root@localhost builtin]# check_ipmi.sh -i 10.134.14.138 -a TEST -p TEST -t 9
Checked:40, OK:40|
FAN_1=9216RPM;0;0;784;33856 FAN_2=10404RPM;0;0;784;33856 FAN_3=9216RPM;0;0;784;33856 FAN_4=10404RPM;0;0;784;33856 FAN_5=9216RPM;0;0;784;33856 CPU1_Vcore=0.928Volts;0;0;0.824;1.352 CPU1_DIMM=1.512Volts;0;0;1.336;1.656 +1.5_V=1.512Volts;0;0;1.336;1.656 +5_V=5.088Volts;0;0;4.48;5.536 +5VSB=5.088Volts;0;0;4.48;5.536 +12_V=12.19Volts;0;0;10.706;13.25 +1.1_V=1.12Volts;0;0;0.976;1.216 +3.3VCC=3.312Volts;0;0;2.928;3.648 +3.3VSB=3.264Volts;0;0;2.928;3.648 VBAT=3.192Volts;0;0;2.928;3.648 System_Temp=33degreeC;0;0;-5;75 P1-DIMM1A=38degreeC;0;0;-5;75 P1-DIMM2A=37degreeC;0;0;-5;75 Chassis_Intru=0SWITCH;0;0;-1;2 PS_Status=0SWITCH;0;0;-1;2 PS2_Fan1=8544RPM;0;0;720;10000 PS2_Temperature1=44C;0;0;-10000;10000 PS2_Temperature2=39C;0;0;-10000;10000 PS2_ACInputCurrent=0.156A;0;0;-10000;10000 PS2_DC12VOutputCurrent=4.5A;0;0;-10000;10000 PS2_ACInputPower=29W;0;0;-10000;10000 PS2_DC12VOutputPower=56W;0;0;-10000;10000 PS2_ACInputVoltage=228Volts;0;0;-10000;10000 PS2_DC12VOutputVoltage=12.188Volts;0;0;-10000;10000 PS2_Status=0SWITCH;0;0;-1;2 PS1_Fan1=8448RPM;0;0;720;10000 PS1_Temperature1=44C;0;0;-10000;10000 PS1_Temperature2=39C;0;0;-10000;10000 PS1_ACInputCurrent=0.359A;0;0;-10000;10000 PS1_DC12VOutputCurrent=5.75A;0;0;-10000;10000 PS1_ACInputPower=76W;0;0;-10000;10000 PS1_DC12VOutputPower=70W;0;0;-10000;10000 PS1_ACInputVoltage=226.5Volts;0;0;-10000;10000 PS1_DC12VOutputVoltage=12.062Volts;0;0;-10000;10000 PS1_Status=0SWITCH;0;0;-1;2
[root@localhost builtin]#

```

Exit code **0** indicates a normal status and exit code **2** indicates a critical status.

4.4 check_ping

This command is used to check the health of a host with a ping command. To execute the command, use **check_ping.bat** for Windows platforms and **check_ping.sh** for Linux platforms.

Usage:

```
check_ping <arg1> <arg2>
```

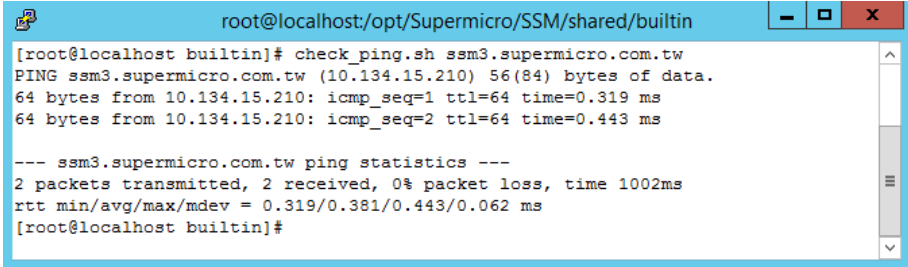
Options:

***arg1** An IP address or a DNS name.

arg2 Timeout in seconds to wait for reply messages.

(* indicates a required attribute)

Example:



```
root@localhost:/opt/Supermicro/SSM/shared/builtin
[root@localhost builtin]# check_ping.sh ssm3.supermicro.com.tw
PING ssm3.supermicro.com.tw (10.134.15.210) 56(84) bytes of data.
64 bytes from 10.134.15.210: icmp_seq=1 ttl=64 time=0.319 ms
64 bytes from 10.134.15.210: icmp_seq=2 ttl=64 time=0.443 ms

--- ssm3.supermicro.com.tw ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.319/0.381/0.443/0.062 ms
[root@localhost builtin]#
```

Exit code **0** indicates OK and exit code **1** indicates Critical.

4.5 check_smtp

This command is used to check the health of an SMTP server. To execute the command, use **check_smtp.bat** for Windows platforms and **check_smtp.sh** for Linux platforms.

Usage:

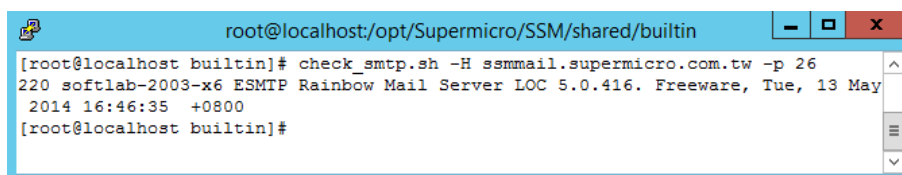
```
check_smtp [-H | --host <arg>] [-h | --help] [-p | --port <arg>]
```

Options:

- *-h, --host** An IP address or a DNS name.
- h, --help** Shows the help menu.
- p, --port** SMTP server port number. Default value is 25.

(* indicates a required attribute)

Example:



```
root@localhost:/opt/Supermicro/SSM/shared/builtin
[root@localhost builtin]# check_smtp.sh -H ssmmail.supermicro.com.tw -p 26
220 softlab-2003-x6 ESMTP Rainbow Mail Server LOC 5.0.416. Freeware, Tue, 13 May
2014 16:46:35 +0800
[root@localhost builtin]#
```

Exit code **0** indicates a normal status and exit code **2** indicates a critical status.

4.6 check_wol

This command is used to send “magic packets” to wake up a host supporting Wake-On-LAN. To execute the command, use **check_wol.bat** for Windows platforms and **check_wol.sh** for Linux platforms.

Usage:

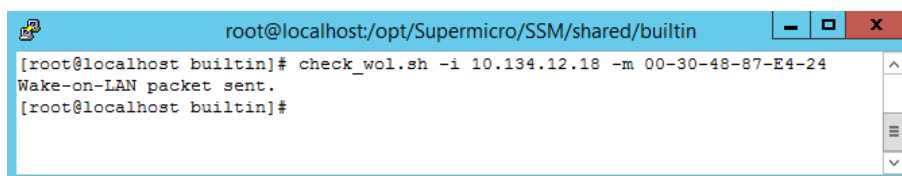
```
check_wol [-i | --ip <arg>] [-m | --mac <arg>]
```

Options:

- *-i, --ip** The broadcast address
- *-m, --mac** The MAC address. Format: xx-xx-xx-xx-xx-xx or xx:xx:xx:xx:xx:xx.

(* indicates a required attribute)

Example:



```
root@localhost:/opt/Supermicro/SSM/shared/builtin
[root@localhost builtin]# check_wol.sh -i 10.134.12.18 -m 00-30-48-87-E4-24
Wake-on-LAN packet sent.
[root@localhost builtin]#
```

If the magic packets were sent successfully, the exit code is **0** indicating a normal state. Otherwise, the exit code is **2** indicating a critical state.

4.7 jcheck_nrpe

This command is used to communicate with SuperDoctor 5 in order to perform the actions of SuperDoctor 5 plug-ins. Three communication modes are supported. See 3.2 *SuperDoctor 5 Connection Modes* in *SuperDoctor 5 User's Guide* for more information. This command is located in the **[install folder]\shared\jcheck_nrpe** folder. To execute the command, use **jcheck_nrpe.bat** for Windows platforms and **jcheck_nrpe.sh** for Linux platforms.

Usage:

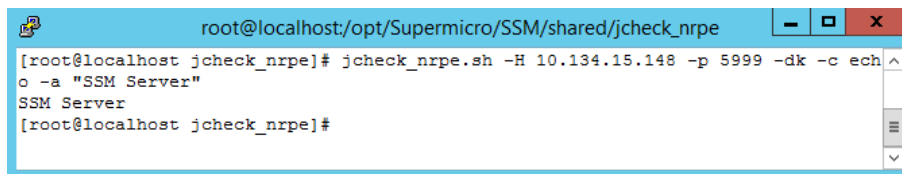
```
jcheck_nrpe [-a <arglist...>] [-c <command>] [-dk] [-H <host>] [-i <instanceId>]
            [-j <classes>] [-keyPassword <keyStorePassword>]
            [-keyStore <keyStore>] [-n] [-o <hostObjectId>] [-p <port>]
            [-plus] [-t <timeout>] [-trustKeyPassword <trustKeyStorePassword>]
            [-trustKeyStore <trustKeyStore>] [-u]
```

Options:

-a <arglist...>	Optional arguments passed to the command
*-c <command>	The name of an action to run on a SuperDoctor 5
-dk	Use default SSL key store
*-H <host>	An agent-managed host IP address or domain name
-i <instanceId>	The Instance ID that should be passed to the IObservers
-j <classes>	The Java class will be run after executing jcheck_nrpe
-keyPassword <keyStorePassword>	The password to access the SSL key store
-keyStore <keyStore>	The location of the SSL key store
-n	Use non-SSL connections
-o <hostObjectId>	The HostObjectId that should be passed to the IObservers
-p <port>	The port number connecting to a SuperDoctor 5 acceptor
-plus	Send NRPE Plus packets
-t <timeout>	Number of seconds before the connection times out

-
- trustKeyPassword <trustKeyStorePassword>** The trust key store password
- trustKeyStore <trustKeyStore>** The trust key store location
- u** Set socket timeouts as an UNKNOWN state instead of a CRITICAL state
- (* indicates a required attribute)

Example:



```
root@localhost:/opt/Supermicro/SSM/shared/jcheck_nrpe
[root@localhost jcheck_nrpe]# jcheck_nrpe.sh -H 10.134.15.148 -p 5999 -dk -c echo -a "SSM Server"
SSM Server
[root@localhost jcheck_nrpe]#
```

Exit code **0** indicates a normal status and exit code **2** indicates a critical status.

Part 3 SSM Web

5 SSM Web Overview

This Chapter introduces how to login to SSM Web and shows the general layout of SSM Web.

5.1 Logging in to SSM Web

Type the following URL in your browser to connect to SSM Web:

`https://[SSM Web address]:8443/SSMWeb`

To log in SSM Web, you can use the built-in ADMIN account and the password you configure while installing SSM.

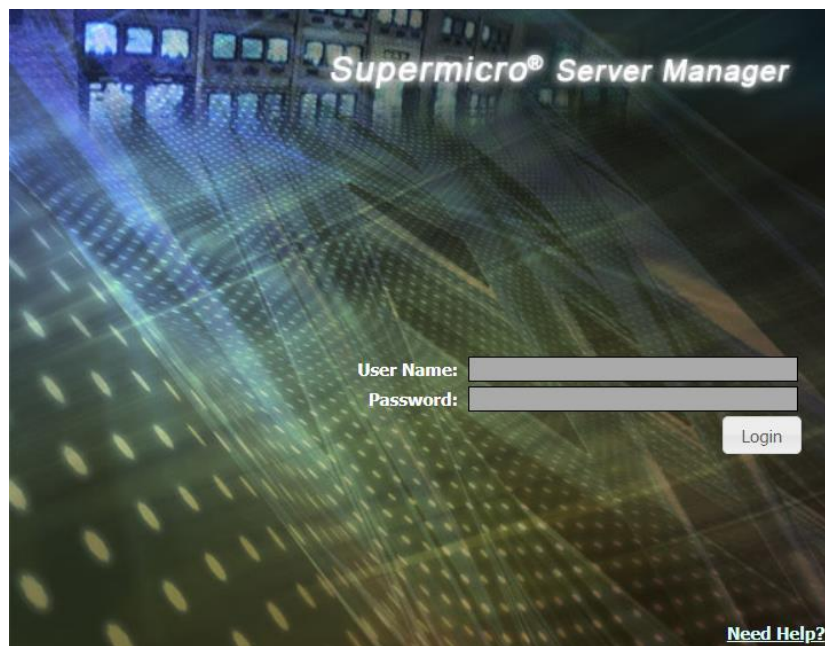


Figure 5-1

5.2 SSM Web Layout

After you login, you are directed to a Monitoring Overview page, as shown below. You can see that there is no host or service monitored by SSM. Use the Host Discovery Wizard in the Administration page to add any hosts to be monitored. See 6.2 for more information.

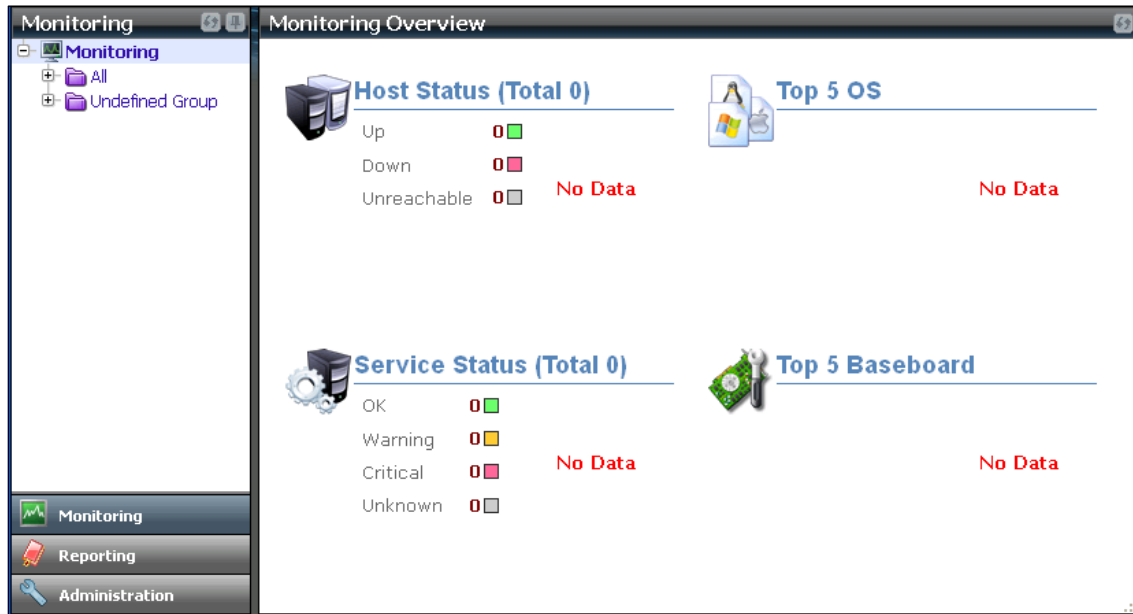


Figure 5-2

As shown below, the layout of SSM Web is divided into three parts:

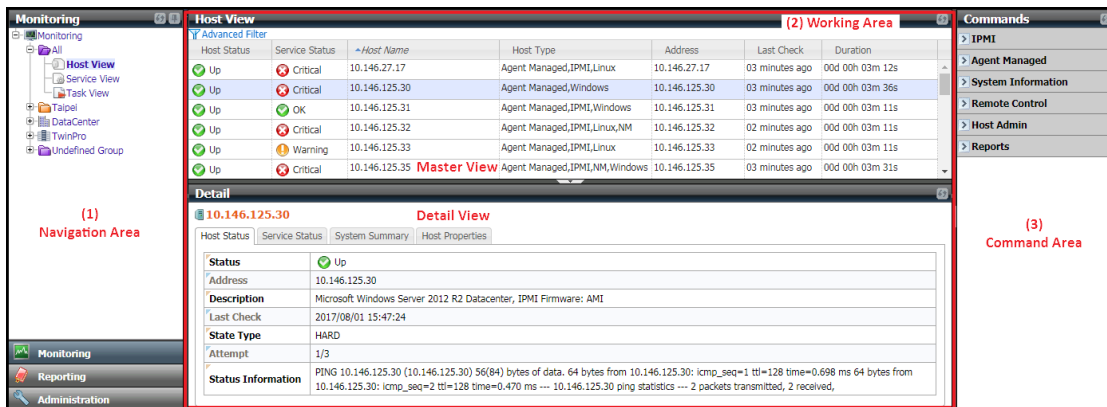


Figure 5-3

- **Navigation Area:** designed to change the “theme” of the SSM Web. Three themes are supported: Monitoring, Reporting, and Administration. A tree structure acting as a menu is shown in the navigation area. Each node on the tree structure represents a function, which usually changes the contents of the working area and the command area. Note that the **All** and the **Undefined Group** are two built-in (virtual) tree nodes that cannot be deleted by users.
- **Working Area:** shows detailed information for users to operate a function. Some functions, such as monitoring and host group management, further divide the working area into a **master view** and a **detailed view**. The master view shows a list of hosts or services while the detailed view shows extra information belonging to a selected host or a service in the master view. Some functions, such as reporting and user roles management, only show a master view in the working area.
- **Command Area** shows commands which can be applied to the items shown in the working area.

When you click a host group on the Navigation Area, the **Working Area** displays a **Group Monitoring Overview** page as shown below. This page is designed to support power management functions against a group of hosts. To use the power management functions, the managed hosts in the group need to support NM and have PMBus instrumented power supplies.

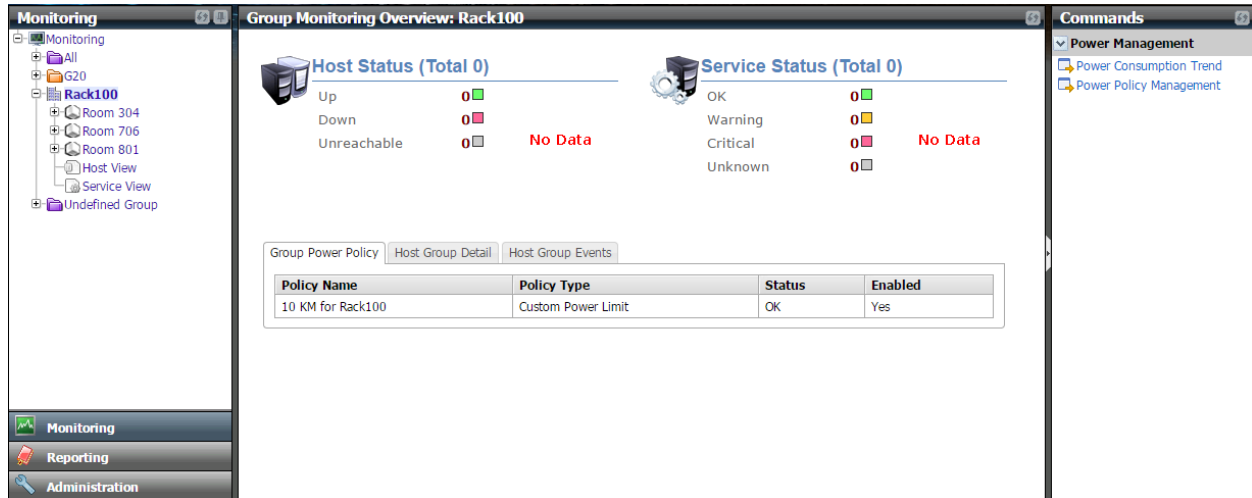


Figure 5-4

When you click the two built-in host groups **All** and the **Undefined Group**, a group overview page is shown without the **Command Area** as shown below. Since the two host groups are virtual groups that are used for classification purposes, commands are not allowed to apply to hosts in the virtual groups.

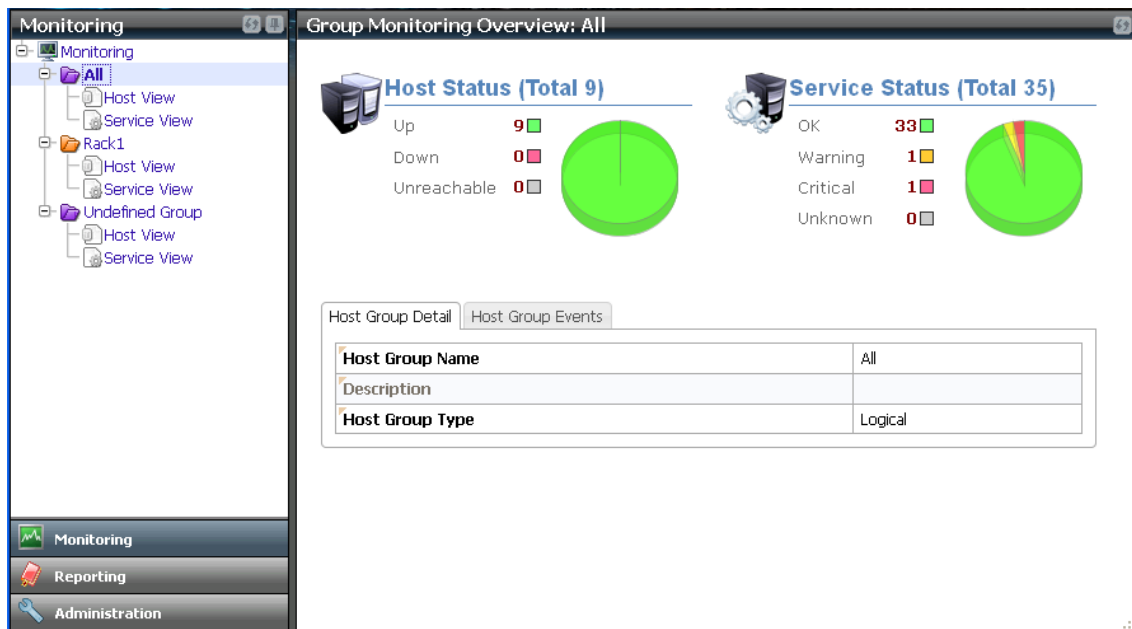


Figure 5-5

6 SSM Web Administration Page

6.1 Administration Page Overview

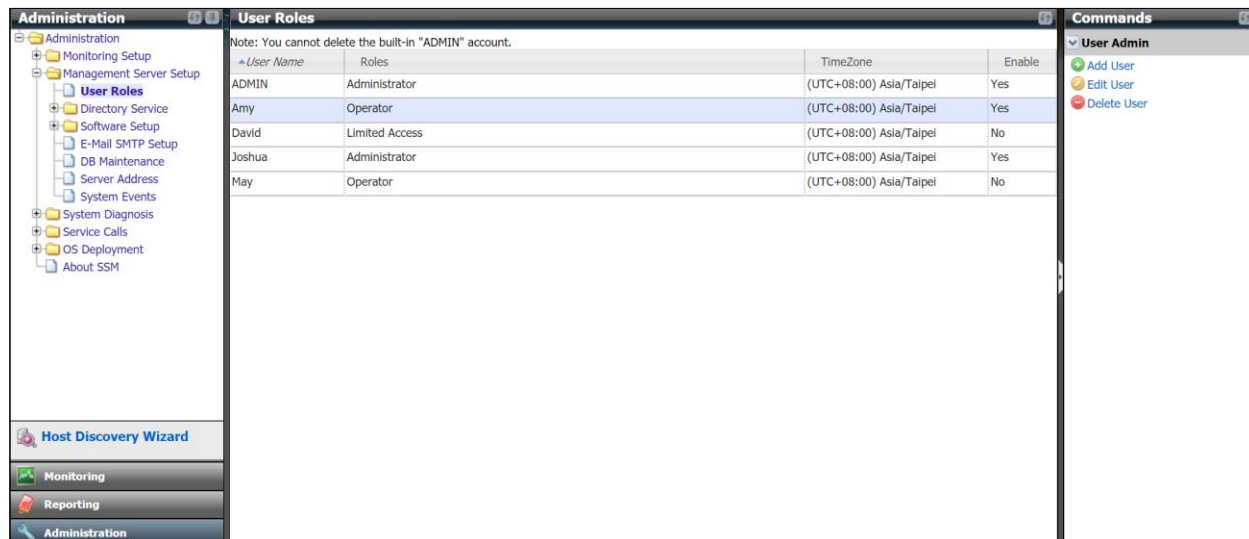


Figure 6-1

Most SSM administration functions are found on this page. On the administration page, you can perform:

- **Monitoring Setup**
 - **Host management:** You can delete hosts, assign host groups to a host, and add services to hosts.
 - **Host Group:** You can add, edit, and delete host groups as well as assign host group members (i.e., hosts and host groups).
 - **Contact:** You can add, edit, and delete contacts.
 - **Contact Group:** You can add, edit, and delete contact groups as well as assign contact group members (i.e., contacts).
- **Management Server Setup:** Functions in this category include: (1) adding, editing, and deleting user accounts, (2) setting up directory services configurations, (3) dependent software installations include uploading a VNC viewer and a SUM package, and configuring the SD5 update site (4) setting up e-mail SMTP configurations, (5) the database maintenance program (6) configuring the address of SSM Server, and (7) viewing, deleting and backing up system events.
- **Service Calls:** This feature allows Supermicro to respond more quickly when the host has problems that may require immediate attention. Refer to *12 Service Calls* for details.
- **OS Deployment:** You can edit the answer files, upload the ISO files and check the deployment progress. See *11 OS Deployment* for details.
- **About SSM:** You can view some SSM information (i.e., **SSM version number and the license expiration date**).
- **Host Discovery Wizard:** You can add hosts to be monitored by SSM with the Host Discovery Wizard.

6.2 Monitoring Setup

Monitoring Setup allows users to view, edit and delete configuration objects such as a host, a host group, a contact, or a contact group.

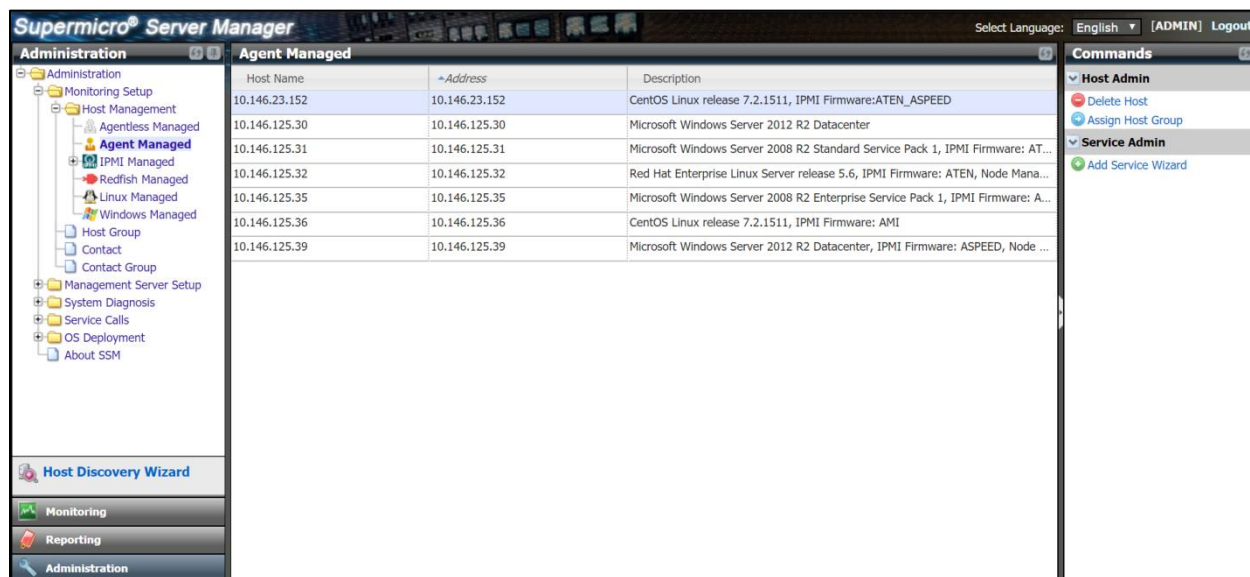


Figure 6-2

As shown above, in the Host Management function hosts are divided into six groups, including Agentless, Agent, IPMI, Redfish, Linux, and Windows. On this page you can delete hosts, assign host groups to a host, and add a built-in service to multiple hosts. Note that the first time you install and use SSM there are no hosts monitored by SSM. **To add hosts please use the Host Discovery Wizard.**

A host can be deleted after it has been monitored by SSM. Deleting a host does not actually delete its data from the database. Instead, the deleted host is marked as “disabled” in the database. Once the same host is added to SSM again, you can see its historical monitoring data such as availability reports and state change reports.

Host groups provide a better way to organize your managed hosts. You can assign a host to several host groups in the host management page with the **Assign Host Group** command, or assign group members to a host group in the host group page with the **Assign Members** command. On SSM Web, a host group containing a host view and a service view is displayed on the navigation area of the monitoring page. With SSM CLI, you can apply a command to a host group that will automatically send the command to each host in the host group.

To add built-in services to a host, use the **Add Service Wizard** command, which will guide you through the process.

6.2.1 Delete a Host

1. Select the hosts to be deleted in the working area. You can delete multiple hosts at a time.
2. Click **Delete Host** in the commands area and you will see a Delete Host dialog box as shown below.

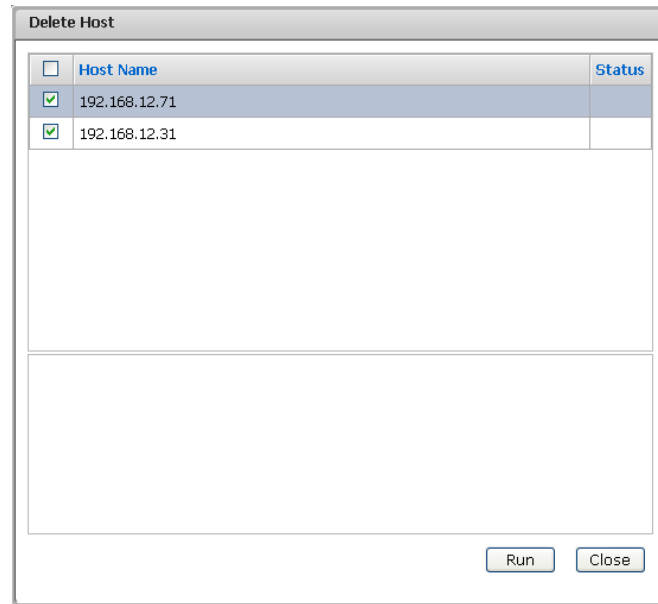


Figure 6-3

3. Click the **Run** button to delete the selected hosts or the **Close** button to abort and close this dialog box.

6.2.2 Assign a Host Group

1. Select a host in the working area.
2. Click **Assign Host Group** in the command area and you will see an Assign Host Group dialog box as shown below.

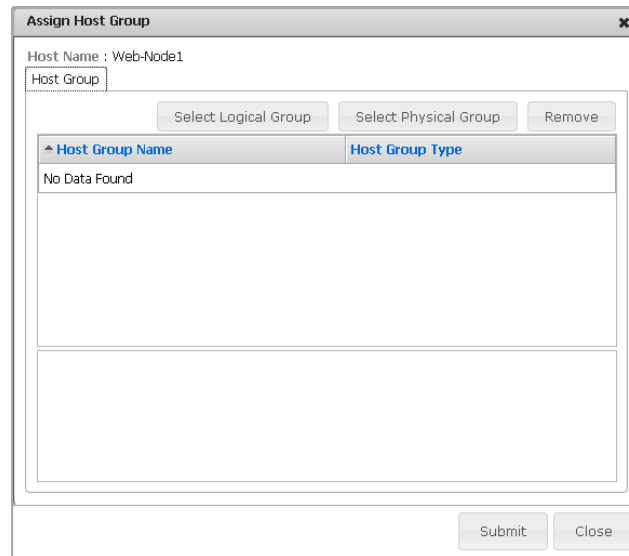


Figure 6-4

- To remove the host from host groups, click the **Remove** button.
- To assign the host to logical host groups, click the **Select Logical Group** button and you will see a host group query dialog box, as shown below. Select the logical host groups that will include the host and click the **Submit** button.

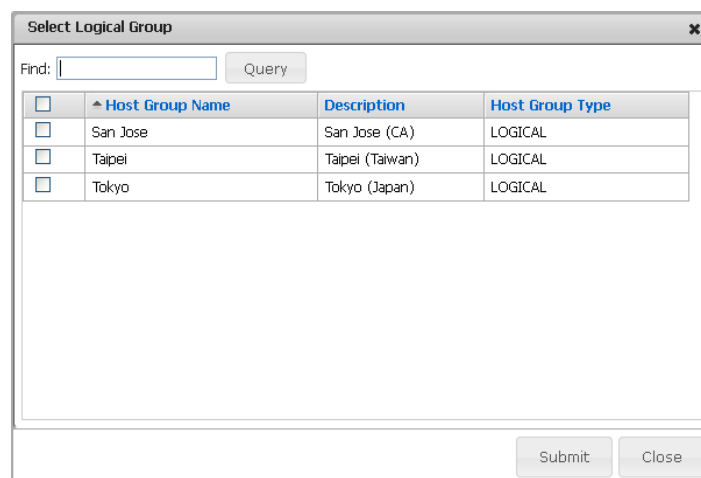


Figure 6-5

To assign the host to physical host groups, click the **Select Physical Group** button and you will see a host group query dialog box, as shown below. Select the physical host groups that will include the host and click the **Submit** button.

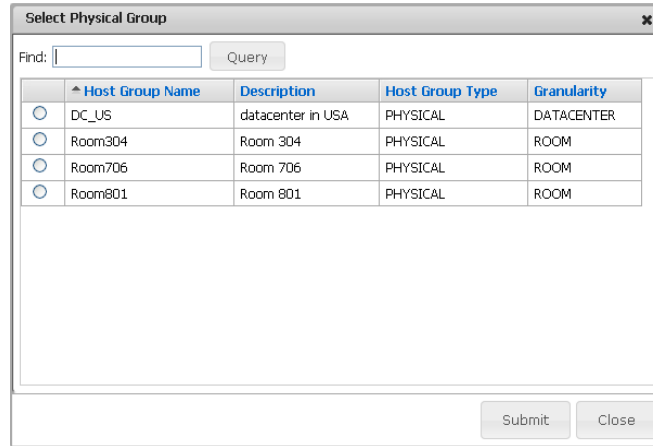


Figure 6-6

- The selected host groups will be added to the Assign Host Group dialog box, as shown below. Click the **Submit** button to confirm the change or the **Close** button to abort and close the dialog box.

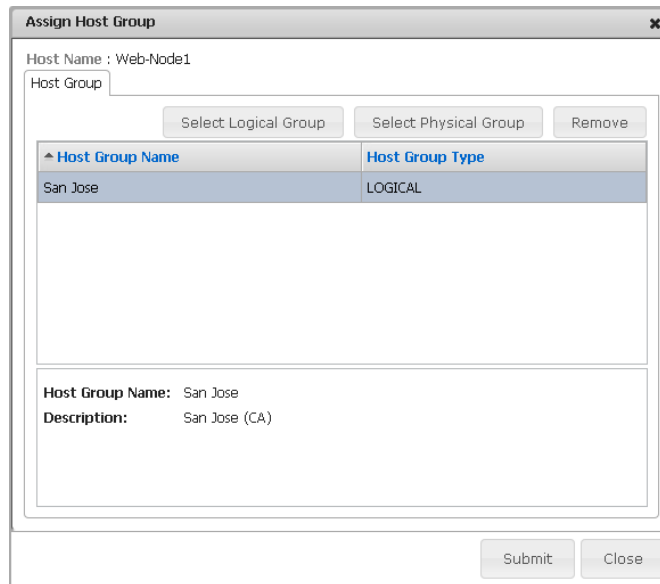


Figure 6-7

6.2.3 Add Service Wizard

According to the selected host types, four types of **Add Service Wizards** are provided in SSM, including Wizards for agent-managed hosts, agentless hosts, IPMI, and Redfish hosts. Note that Windows and Linux hosts are subtypes of the Agent Managed hosts.

6.2.3.1 Add Agent Managed Services

1. Select agent-managed hosts in the working area.
2. Click **Add Service Wizard** in the command area and an Add Service Wizard dialog box will pop up, as shown below.

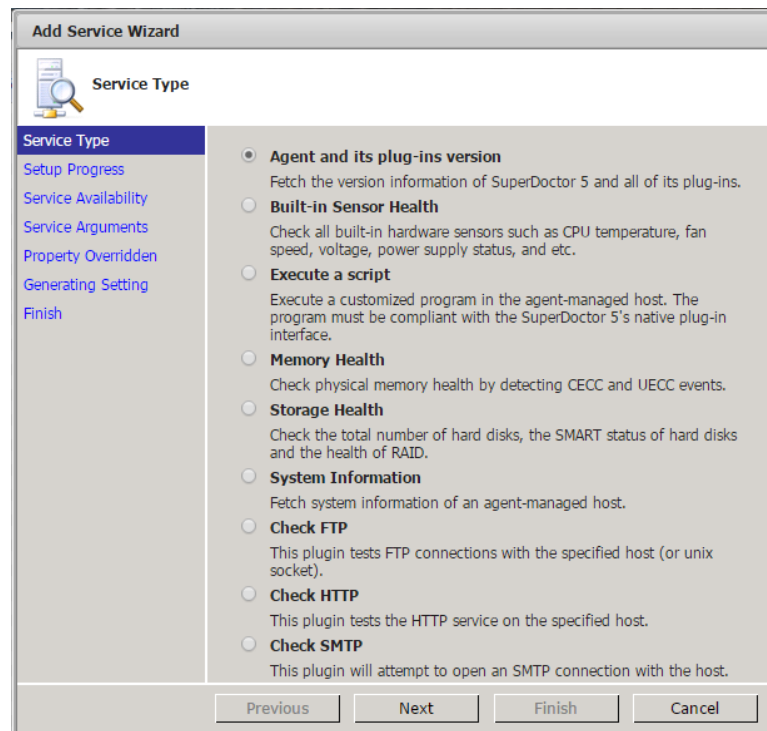


Figure 6-8

Built-in agent-managed services include:

- **Agent and its plug-ins versions:** Checks the health of a SuperDoctor 5 and display all versions of its plug-ins.
- **Built-in Sensor Health:** Checks the health of a host according to its hardware sensor readings such as fan speeds, temperature, voltages, chassis intrusion status, and so on. Note that this service is hardware dependent and therefore only applicable to Supermicro manufactured servers.
- **Execute a script:** Remotely executes an application (a plug-in) on the host. This service is the key to extending the monitoring features of agent-managed hosts.
- **Memory Health:** This service supports three checks. It checks the total number of DIMMs as well as the health of physical memory by detecting correctable error checking and correcting (CECC) and uncorrectable error checking and correcting (UECC) events. Note that the CECC

and UECC checks must be BIOS supported.

- **Storage Health:** Checks the total number of hard disks, the SMART (Self-Monitoring, Analysis and Reporting Technology) status of hard disks and the health status of RAID controllers. Note that the SMART check of hard disks checks non-RAID internal hard disks and does not check USB hard disks and flash disks. It checks the RAID health of LSI MegaRAID 2108, 2208 and 3108 controllers except Windows driver is MR6.6 code set or higher version, and does not check LSI MegaRAID 2008, LSI Fusion-MPT based and Intel Rapid Storage Technology controllers. The health status of a RAID controller includes the states of its components such as battery backup units, virtual drives, and hard disks. See *4.2 Health Information* in *SuperDoctor 5 User's Guide* for more information for more information.
- **System Information:** Checks the system information status, retrieves the system information data, and stores it in the database. If this service is not added to an agent managed host or it is not in the OK state, the **View Details** command under the System Information category on the monitoring page cannot be used or it may show out-of-date data.
- **Check HTTP:** Checks the health of an HTTP (Web) server.
- **Check FTP:** Checks the health of an FTP server.
- **Check SMTP:** Checks the health of an SMTP (e-mail) server.

Select one service and click the **Next** button to continue.

3. Setup service configuration is in progress. Please wait for a while.

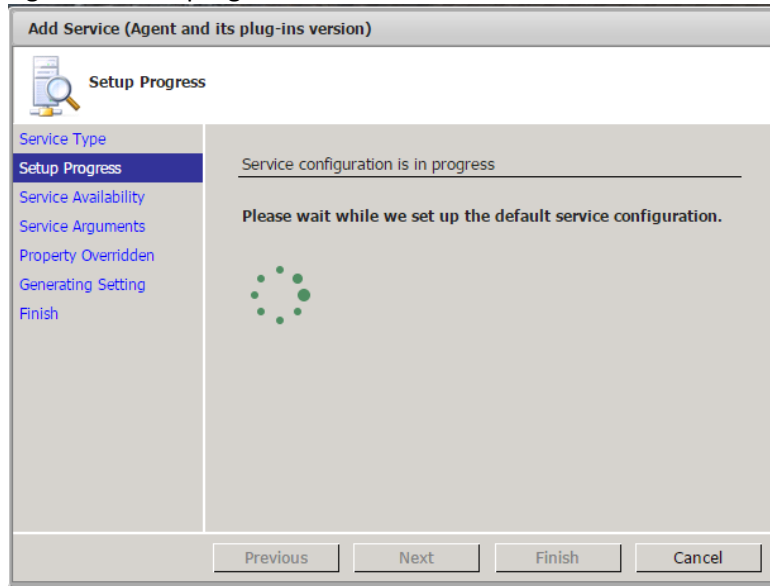


Figure 6-9

4. If the service is available on a host, the check box of the host is clicked. Click the **Next** button to continue.

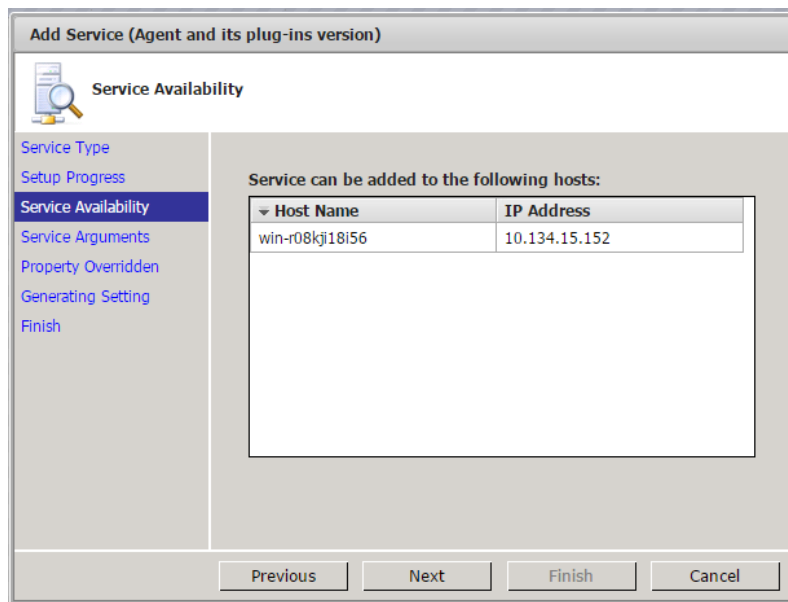


Figure 6-10

- If you choose **Check HTTP**, **Check FTP** or **Check SMTP** service in the previous step, you can configure the port number in this step. Usually you accept the default value and click the **Next** button to continue.

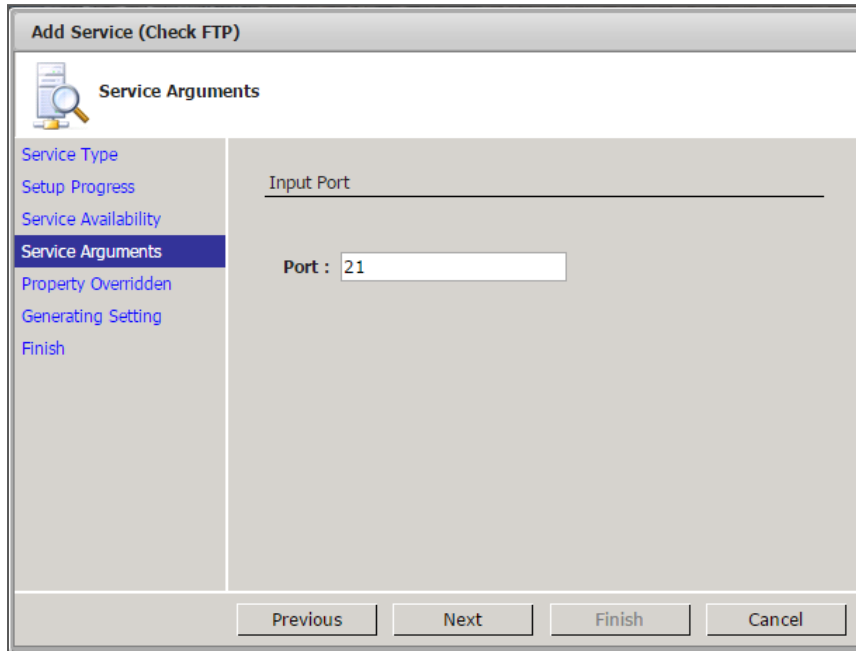


Figure 6-11

- You can override the default service monitoring properties in this step. Note that the service name must be unique in a host; otherwise the service cannot be added to the host. Click the **Next** button to continue.

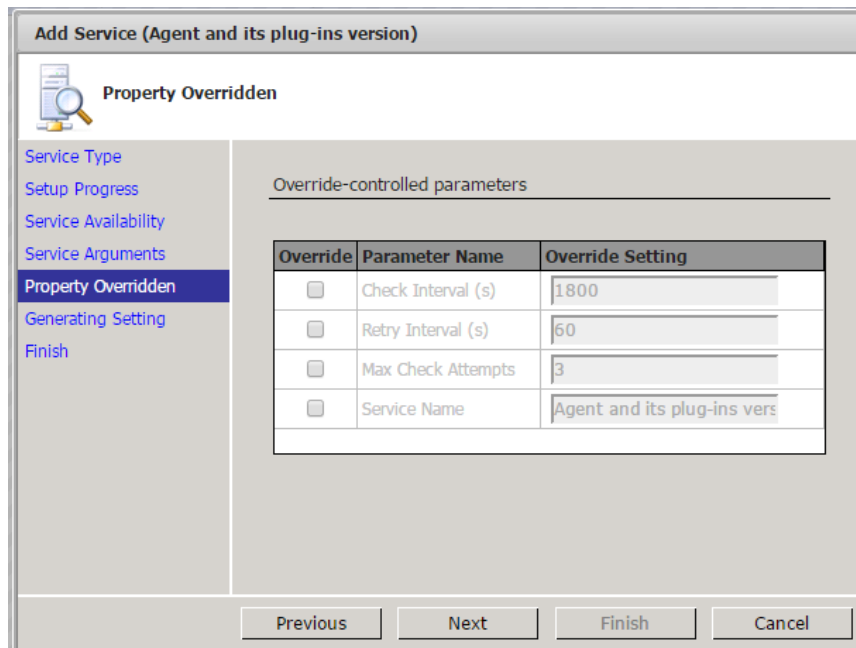


Figure 6-12

7. Please wait while SSM generates service configuration data.

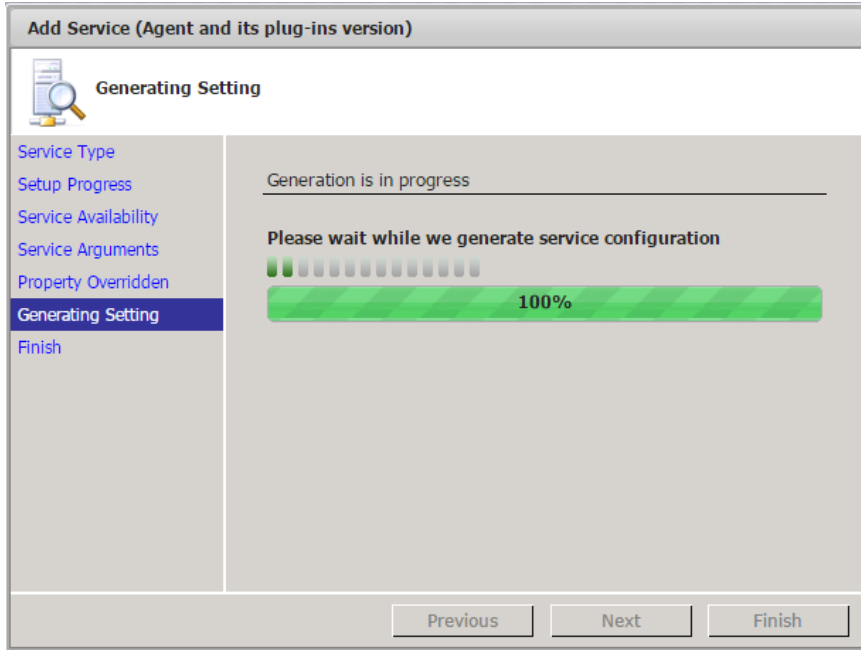


Figure 6-13

8. When the service has been successfully added to the host, you can see the newly added service on the monitoring page.

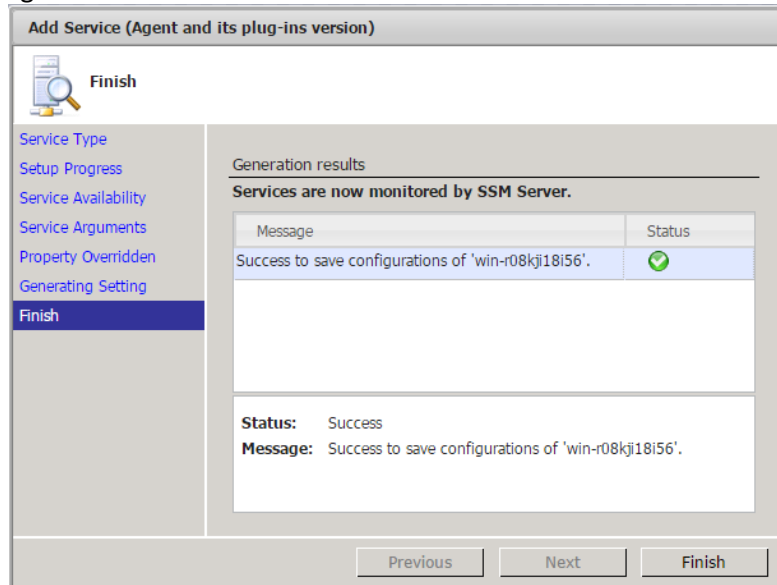


Figure 6-14

6.2.3.2 Add Agentless Services

1. Select agentless hosts in the working area.
2. Click **Add Service Wizard** in the commands area and an Add Service Wizard dialog box will pop up, as shown below.

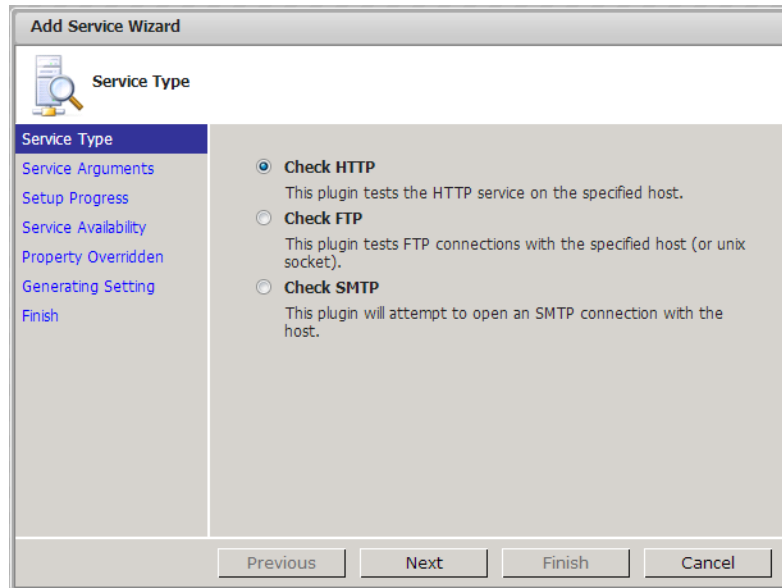


Figure 6-15

Built-in agentless services include:

- **Check HTTP:** Checks the health of an HTTP (Web) server.
- **Check FTP:** Checks the health of an FTP server.
- **Check SMTP:** Checks the health of an SMTP (e-mail) server.

Select one service and click the **Next** button to continue. The subsequent steps are similar to that of adding an agent managed service and so are not repeated here.

6.2.3.3 Add IPMI Services

1. Select the IPMI hosts in the working area.
2. Click **Add Service Wizard** in the commands area and an Add Service Wizard dialog box will pop up, as shown below.

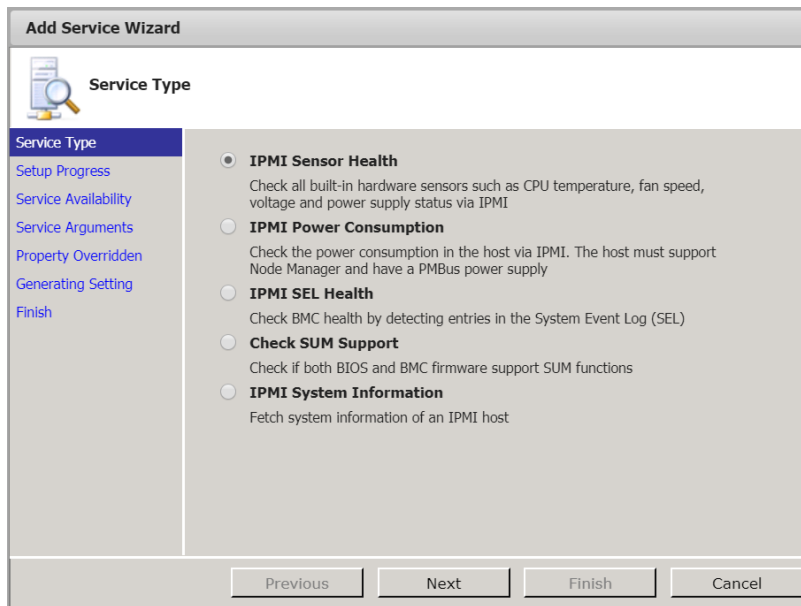


Figure 6-16

Built-in IPMI services include:

- **IPMI Sensor Health:** Checks the health of a host according to its hardware sensor readings such as fan speed, temperature, voltage levels, chassis intrusion status, and so on.
- **IPMI Power Consumption:** Checks the power consumption of a host. This is the fundamental service for power management functions in SSM. The SSM Server uses this service to monitor a host's power consumption and to draw the power consumption trend of individual hosts and a group of hosts (See 9.2 *Power Consumption Trend* for more information). When power management policies are assigned to individual hosts and a group of hosts, the SSM server also depends on this service to retrieve a host's current power consumption and to determine if the power management policies can be achieved. This service is added by default when NM enabled hosts are discovered and added by the Host Discovery Wizard.
- **IPMI SEL Health:** Checks the health of a host and is based on the System Event Log or SEL. "Maintenance Window" refers to the period of time when a system is being accessed for repair or replacement of components. Note that this is not logged as an entry but a kind of internal mechanism. To avoid false alarms after a failed component has been repaired, an event is automatically determined as a "Maintenance Window" in SEL when a component is replaced offline. After an "AC Power On" event occurs, and a "Chassis Intrusion" event occurs within an hour, this "Maintenance Window" event only is determined. SSM will then check if the "Maintenance Window" event is real. If a "Maintenance Window" event is found, SSM will report the log after the event "AC Power On." The logs prior to this entry will be ignored.
- **Check SUM Support:** Checks if both BIOS and BMC firmware support SUM functions.
- **IPMI System Information:** Checks the system information status, retrieves the system information data mainly via OOB Full SMBIOS, and stores it in the database.



Note: Both the Check SUM Support and the IPMI System Information services are designed for SUM. See *10 SUM Integration* for more information about SUM in SSM.

Select one service and click the **Next** button to continue. The subsequent steps are similar to that of adding an agent managed service and are not repeated here.

6.2.3.4 Add Redfish Services

1. Select the Redfish hosts in the working area.
2. Click **Add Service Wizard** in the commands area. And the Add Service Wizard dialog box will appear.

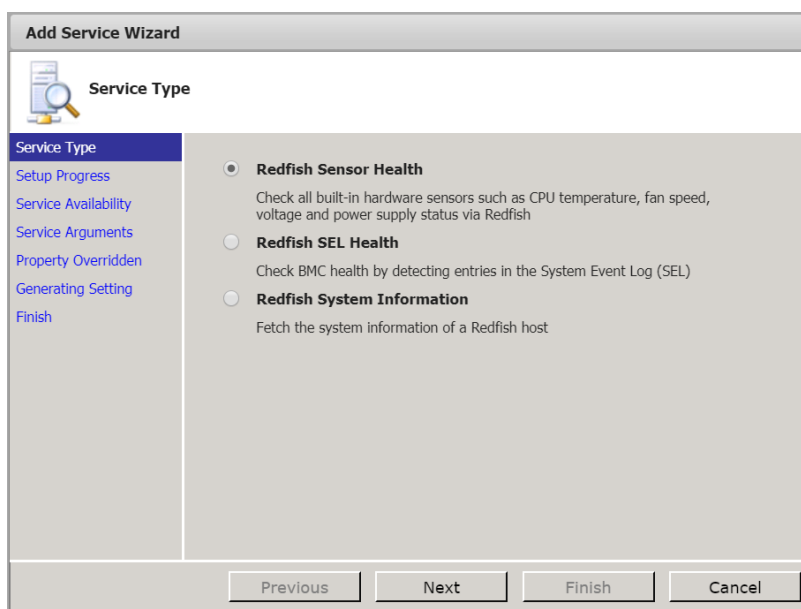


Figure 6-17

Built-in Redfish services include:

- **Redfish Sensor Health:** similar to IPMI Sensor Health, but uses Redfish protocol to communicate with the BMC and not IPMI.
- **Redfish SEL Health:** similar to IPMI SEL Health, but uses Redfish protocol to communicate with the BMC and not IPMI.
- **Redfish System Information:** similar to IPMI System Information, but uses Redfish protocol to communicate with the BMC and not IPMI.

Select one service and click the **Next** button to continue. The subsequent steps are similar to those of adding an agent managed service and are not repeated here.

6.3 Host Group Management

Click **Host Group** in the navigation area to perform host group management functions. A host group contains hosts and other host groups. In this page you can add, edit, delete host groups, and assign host group members.

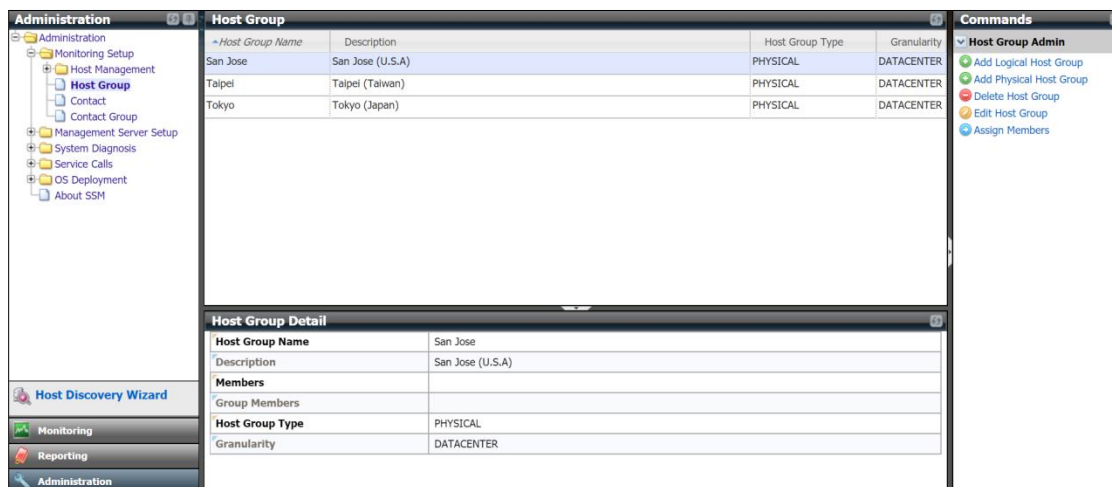


Figure 6-18

6.3.1 Adding Host Groups

Host groups are of two types: Logical and Physical. See 3.3.3 *Host Group Definitions* for more information about the difference between these two types. Note that you cannot change the host group type once a host group is created.

1. Click **Add Logical Host Group** in the command area and you will see an Add Logical Host Group dialog box, as shown below.

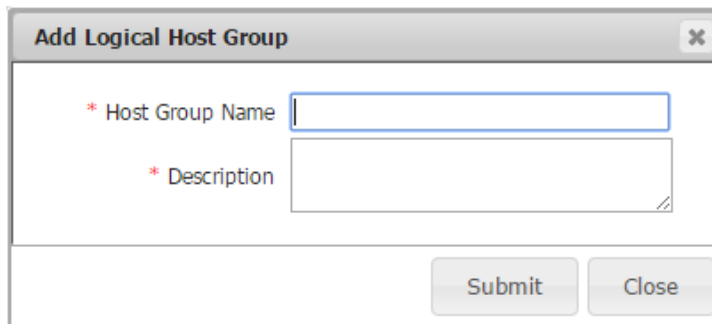
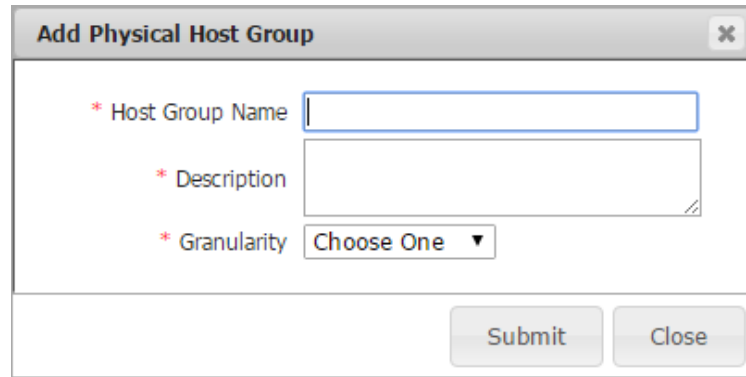


Figure 6-19

Or click **Add Physical Host Group** in the command area and an Add Physical Host Group dialog box appears.



The dialog box titled "Add Physical Host Group" contains three required fields, each marked with an asterisk (*):

- Host Group Name:** A text input field.
- Description:** A multi-line text area.
- Granularity:** A drop-down menu currently showing "Choose One".

At the bottom right of the dialog are two buttons: "Submit" and "Close".

Figure 6-20

2. Input the host group data in this dialog box. For physical group, select RACK, ROW, ROOM or DATACENTER from the Granularity drop-down list.
3. Click the **Submit** button to add the host group or the **Close** button to abort and close this dialog box.



Note: Logical host groups and physical host groups show different icons in the Monitoring view. As shown below, San Jose, Taipei, and Tokyo are logical host groups and DC_US and Room801 are physical groups.



Figure 6-21

6.3.2 Editing a Host Group

1. Select one host group to be edited in the working area. You can edit only one host group at a time.
2. Click **Edit Host Group** in the command area and you will see an Edit Host Group dialog box, as shown below. You can modify the host group data in this dialog box.



Note: You cannot change the host group type once a host group is created.

The screenshot shows a dialog box titled "Edit Host Group" with a close button (X) in the top right corner. The dialog contains three required fields, each marked with a red asterisk (*):

- * Host Group Name:** A text input field containing "San Jose".
- * Description:** A text input field containing "San Jose (CA)".
- * Host Group Type:** A dropdown menu currently showing "LOGICAL".

At the bottom right of the dialog, there are two buttons: "Submit" and "Close".

Figure 6-22

3. Click the **Submit** button to confirm the modification or the **Close** button to abort and close this dialog box.

6.3.3 Deleting Host Groups

1. Select the host group(s) to be deleted in the working area. You can delete multiple host groups at a time.

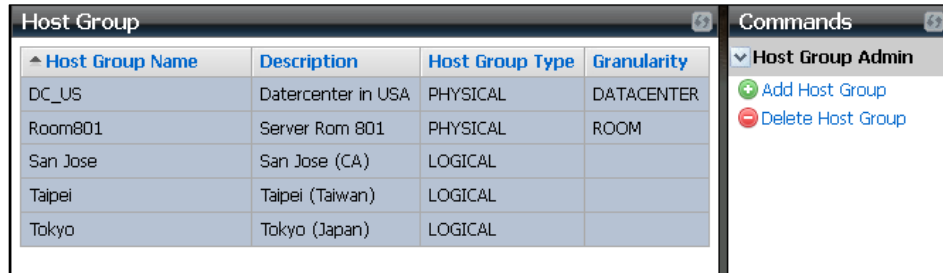


Figure 6-23

2. Click **Delete Host Group** in the command area and you will see a Delete Host Group dialog box, as shown below.

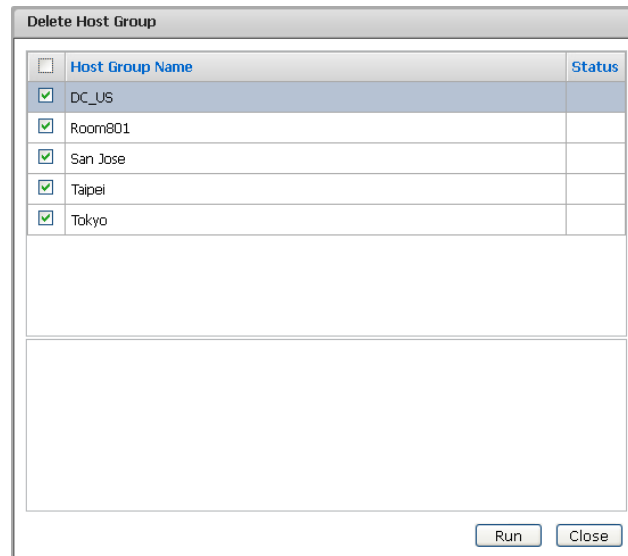


Figure 6-24

3. Click the **Run** button to delete the selected host groups or the **Close** button to abort and close this dialog box.

6.3.4 Assigning Host Members

1. Select a host group in the working area.
2. Click **Assign Members** in the command area and you will see an Assign Members dialog box, as shown below.

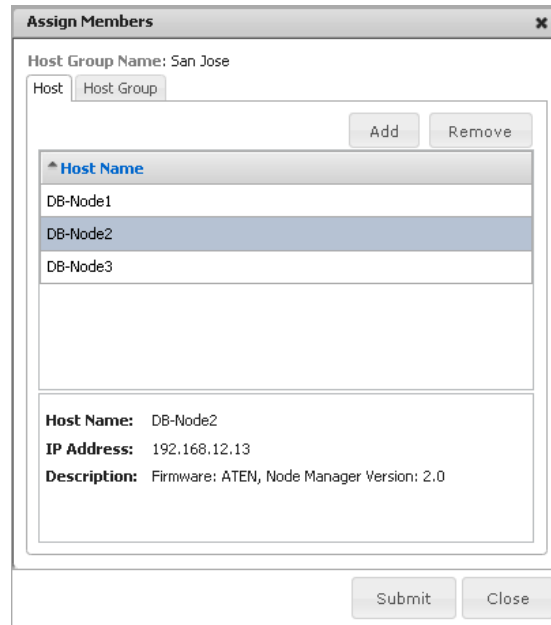


Figure 6-25

3. Select the **Host** tab.
4. To remove a host from the host groups, click the **Remove** button.
5. To add a host to the host group, click the **Add** button and you will see a host query dialog box, as shown below. Select hosts to be included in the host group. When completed, click the **Submit** button to add the selected hosts to this host group.

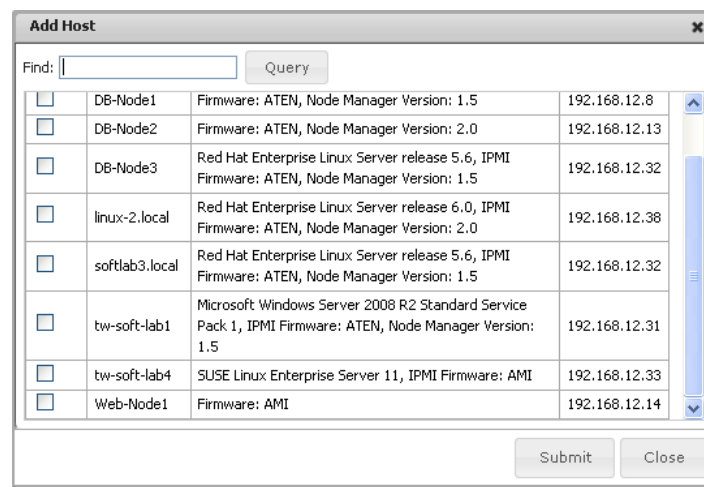


Figure 6-26

6.3.5 Assigning Host Group Members

1. Select a host group in the working area.
2. Click **Assign Members** in the command area and you will see an Assign Members dialog box, as shown below.

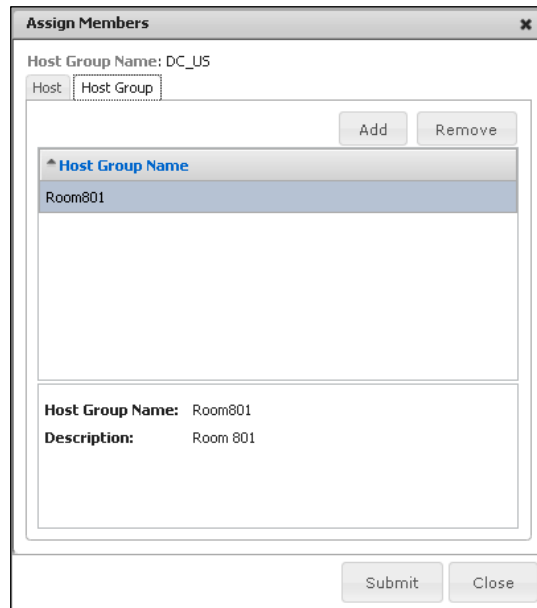


Figure 6-27

3. Select the **Host Group** tab.
4. To remove a host group from the host group, click the **Remove** button.
5. To add a host group to this host group, click the **Add** button and you will see a host group query dialog box, as shown below. Select which host groups will be included in the host group. When completed, click the **Submit** button to add the selected host groups to this host group.

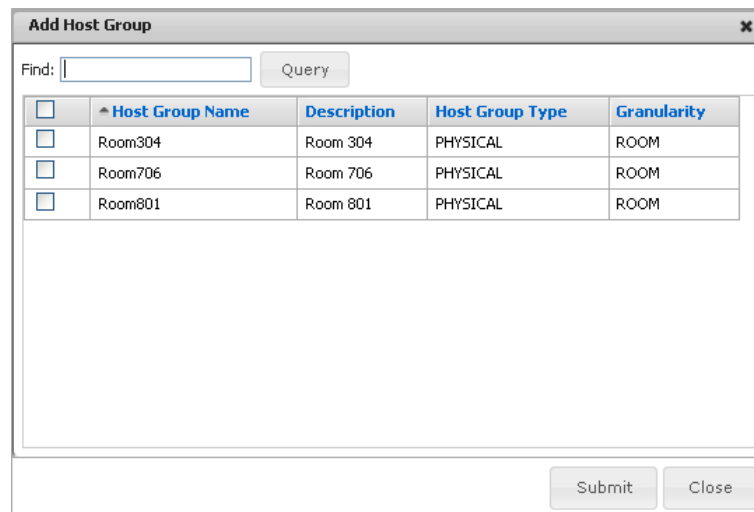


Figure 6-28



Note: As shown below, physical host groups can be added to logical host groups. For example, the DC_US physical host group is a member of the San Jose logical host group. However, logical host groups cannot be added to physical groups. In other words, Physical host groups contain only physical host group members but not logical ones. Thus, logical host groups will not be shown in the Host Group tab when you edit a physical host group.

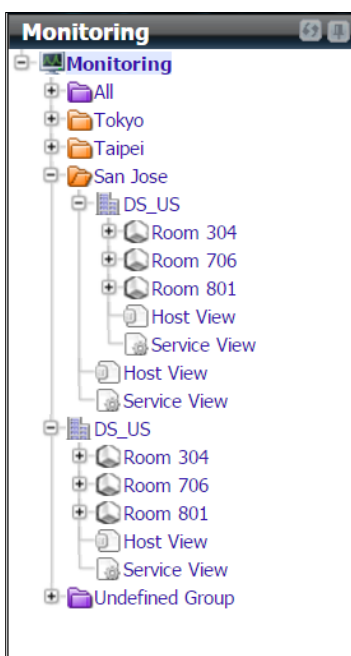


Figure 6-29

6.4 Contact Management

Click **Contact** in the navigation area to manage contacts. A contact is the receiver of a notification message, which is sent by the SSM Server when the status of a host or service has changed. Here you can add, edit, and delete host contacts. In addition, you can set up the host and server notifications for each contact on the same page.

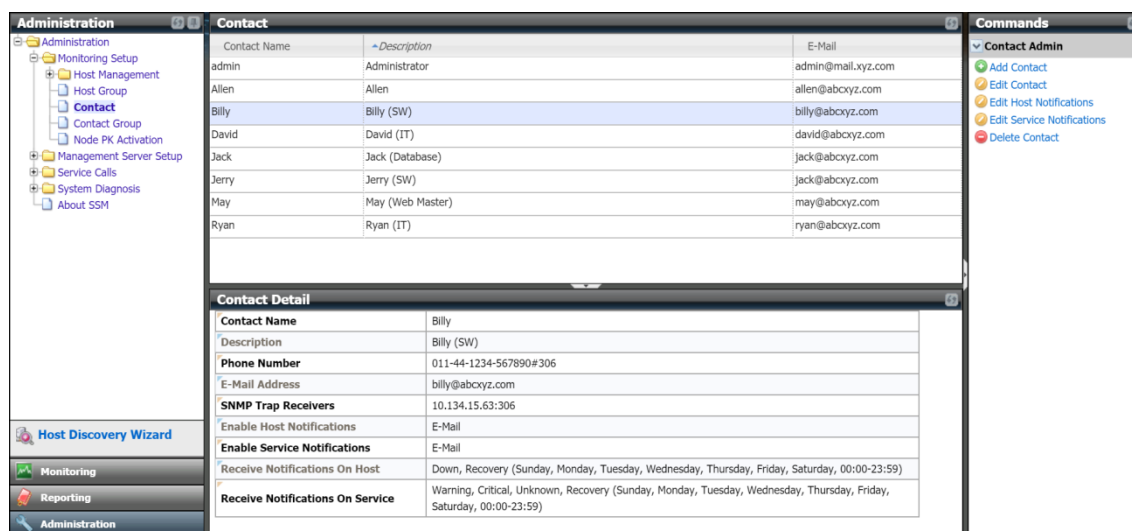


Figure 6-30

6.4.1 Adding a Contact

1. Click **Add Contact** in the Command area and an Add Contact dialog box appears. You can only add one contact at a time.

Add Contact

* Contact Name

* Description

Phone Number
(Multiple values are separated by a comma,)

* E-Mail Address
(Multiple values are separated by a comma,)

SNMTP Trap Receivers
(Format: IPv4:port or [IPv6]:port and multiple values are separated by a comma)

Send Test E-Mail

Send Test Trap

Submit Close

Figure 6-31

2. Input the contact data in this dialog box. Please note that the contact's name, description and e-mail address are required.
3. Click the **Submit** button to add the contact.



Notes: It is highly recommended that you click **Send Test E-Mail** and **Send Test Trap** to ensure your e-mail and trap receiver addresses are respectively accessible.

6.4.2 Editing a Contact

1. Select one contact to be edited in the working area. You can only edit one contact at a time.
2. Click **Edit Contact** in the command area and an Edit Contact dialog box appears.

The screenshot shows a dialog box titled "Edit Contact". It contains the following fields and controls:

- Contact Name:** Text field containing "admin".
- Description:** Text area containing "Administrator".
- Phone Number:** Text field, empty. Below it is the text "(Multiple values are separated by a comma.)".
- E-Mail Address:** Text field containing "admin@mail.xyz.com". Below it is the text "(Multiple values are separated by a comma.)". To the right of this field is a button labeled "Send Test E-Mail".
- SNMP Trap Receivers:** Text field, empty. Below it is the text "(Format: IPv4:port or [IPv6]:port and multiple values are separated by a comma)". To the right of this field is a button labeled "Send Test Trap".
- At the bottom right of the dialog are two buttons: "Submit" and "Close".

Figure 6-32

3. When you are done, click the **Submit** button to save the changes.



Notes: It is highly recommended that you click **Send Test E-Mail** and **Send Test Trap** once you change an e-mail address or a trap receiver address.

6.4.3 Editing Host Notifications for One Contact

1. Select one contact in the working area.
2. Click **Edit Host Notifications** in the command area and an Edit Host Notifications dialog box appears.

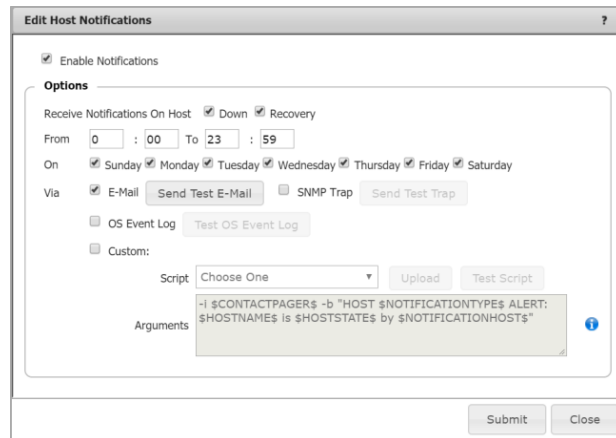


Figure 6-33

3. The **Enable Notification** checkbox is checked by default, meaning the selected contacts are able to receive notifications from hosts through e-mail at any time. You can uncheck the option to not receive any notifications from hosts and then click the **Submit** button to save the changes.
4. You can also specify which host states the contacts should be notified about: either down (**Down**) or recovering (**Recovery**). By default, the checkboxes of both the **Down** and **Recovery** options are selected.
5. To define a period of time for contacts to receive notifications, you can modify the From-To and On values:

From-To The notification is received during a certain period of time. By default, the time range is between 00:00 and 23:59.

On The notification is received on the selected weekdays. By default, all seven days in a week are selected.

6. Click the checkboxes to enable any or all of the four methods of notifications provided: E-Mail, SNMP Trap, OS Event Log and Custom Script.
 - **E-Mail:** Sends alerts via e-mail. To use this function, you need to set up the e-mail address for the contact and the E-Mail SMTP server for SSM to send the notifications. Please refer to the *6.10 E-Mail SMTP Setup* or details.
 - **SNMP Trap:** Sends alerts with SNMP traps. To use this function, you first need to set up the SNMP Trap receiver address for the contact.
 - **OS Event Log:** Writes alerts to Windows Logs for Windows platforms and system logs for Linux platforms.
 - **Custom Script:** Executes a predefined script for notifications. A script is needed if you want to expand the notification methods.
 - **Script:** Use the drop-down menu and select one script file. If none is available, click the **Upload** button, choose a script file and upload the file to SSM. Note that you are not allowed to upload file sizes larger than 50MB.
 - **Arguments:** You can edit arguments to suit your needs by referring to *3.4 Macro*. By default, SSM provides general information of notifications from hosts. In the figure below, a custom script (send_ssm.sh) is sent as a text message to a specific contact for notification. The parameters include a phone number (--phone) and a text message (--

message). The message includes the notification type (“PROBLEM” or “RECOVERY”), host name, the state of the host and the address of the SSM Server. For example, the command line might be like “send_ssm.sh --phone 123456789 --message “HOST PROBLEM ALERT: demohost is CRITICAL by demoSSMServer.”

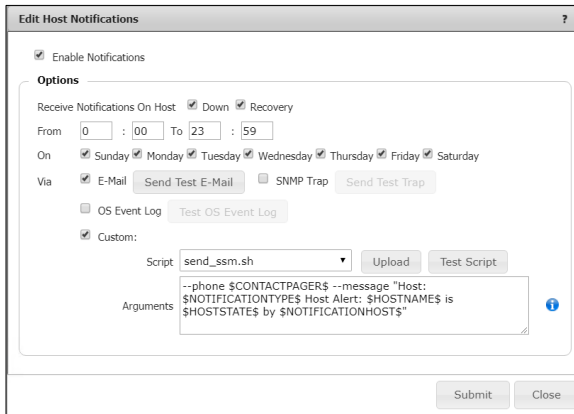


Figure 6-34

7. Click the **Submit** button to save the changes.



Notes: It is highly recommended that you click the **Send Test E-Mail**, **Send Test Trap**, **Test OS Event Log** or **Test Script** button to ensure the notification method is correctly set up.

6.4.4 Editing Host Notifications for Multiple Contact

1. Select multiple contacts in the working area. You can edit multiple contacts at once.
2. Click **Edit Host Notifications** in the command area and an Edit Host Notifications dialog box appears.

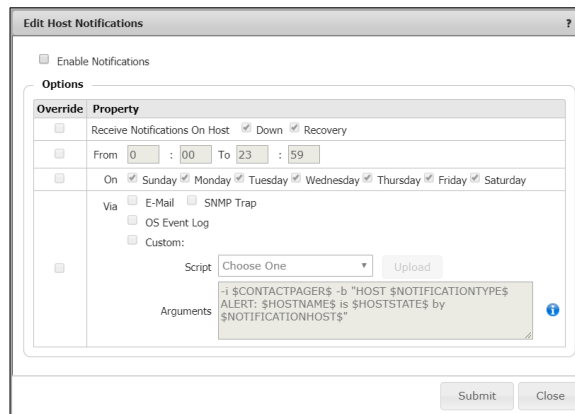


Figure 6-35

-
3. By default, the **Enable Notifications** checkbox is unchecked (see the figure above). To have all selected contacts not receive any notifications from hosts, leave the option unchecked and click the **Submit** button to save the changes (see the figures below).

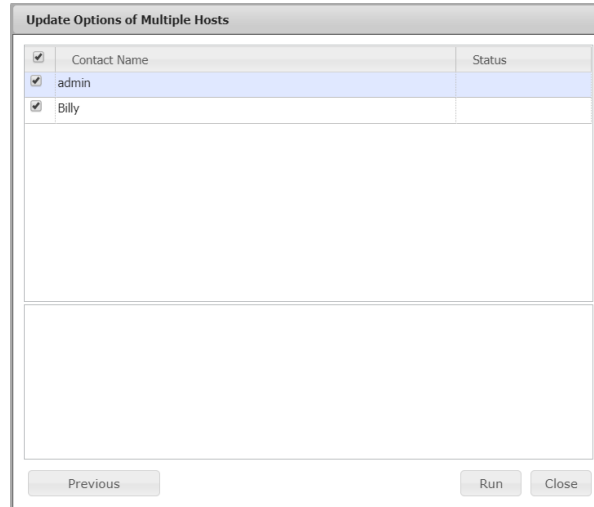


Figure 6-36

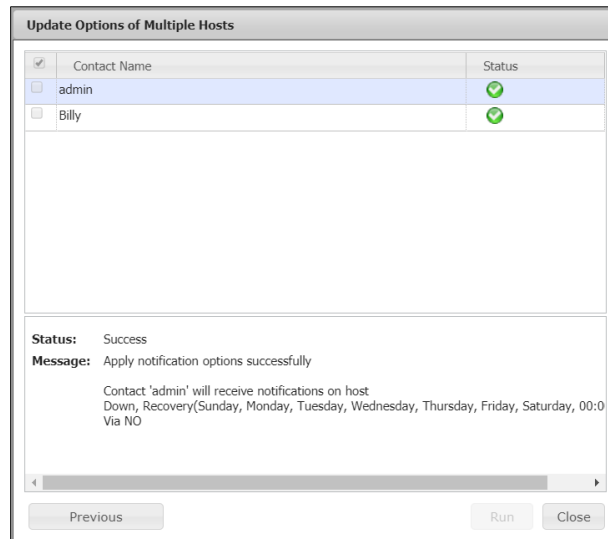


Figure 6-37

4. You can check the **Enable Notifications** option to enable the **Override** mode. The values you input will apply to all of the selected contacts. You can click the boxes in the Override column to apply the current settings to all selected contacts. If the boxes in the Override column are not selected, the original settings are kept.

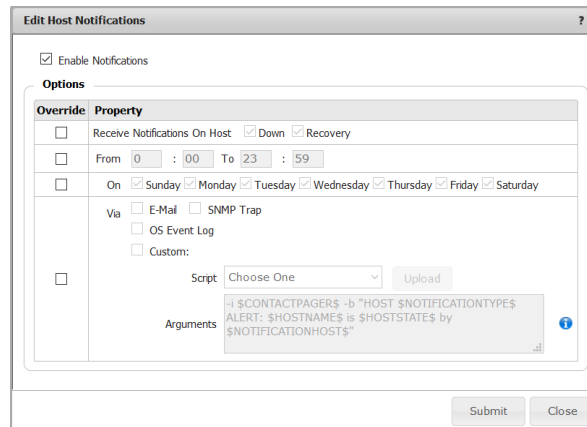


Figure 6-38

5. You can specify on which host states the contacts should be notified about: either down (**Down**) or recovering (**Recovery**). By default, the **Down** and **Recovery** options are both checked.
6. To define a period of time for contacts to receive notifications, you can modify the From-To and On values:

From-To The notification is received during a certain period of time. By default, the time range is between 00:00 and 23:59.

On The notification is received on the selected weekdays. By default, all seven days in a week are selected.

7. Click the checkboxes to enable any or all of the four methods of notifications provided: E-Mail, SNMP Trap, OS Event Log and Custom Script.
 - **E-Mail:** Sends alerts via e-mail. To use this function, you need to set up both the e-mail address for the contact and the e-mail SMTP server for SSM to send e-mail notifications. Please refer to the *6.10 E-Mail SMTP Setup* for details.
 - **SNMP Trap:** Sends alerts with SNMP traps. To use this function, you need to set up the SNMP Trap receiver address for the contact first.
 - **OS Event Log:** Writes alerts to Windows Logs for Windows platforms and system logs for Linux platforms.
 - **Custom Script:** Executes a predefined script for notification. A script is needed if you want to expand the notification methods.
 - **Script:** Use the drop-down menu and select one script file. If none is available, click the **Upload** button and choose a script file, then upload the file to SSM. Note that you are not allowed to upload files larger than 50MB.
 - **Arguments:** You can edit arguments to suit your needs by referring to *3.4 Macro*. By default, SSM provides general information of notifications from hosts. In the figure below, a custom script (send_ssm.sh) is sent as a text message to a specific contact for notification. The parameters include a phone number (--phone) and a text message (--message). The message includes the notification type ("PROBLEM" or "RECOVERY"), host name, the state of the

host and the address of the SSM Server. For example, the command line might be “send_ssm.sh --phone 123456789 --message “HOST PROBLEM ALERT: demohost is CRITICAL by demoSSMServer.”

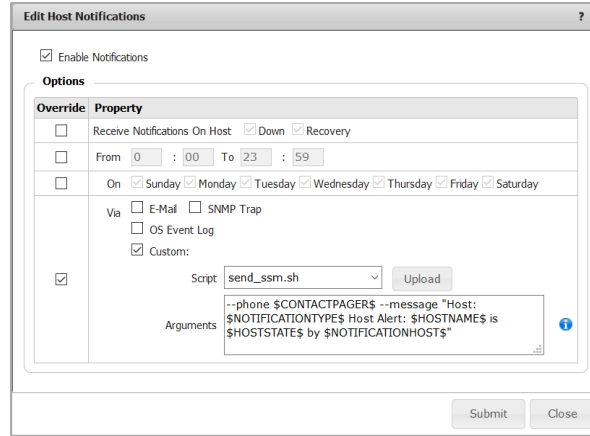


Figure 6-39

- When you are done, click the **Submit** button to save the changes (see the figure below), and all selected contacts will be applied with settings in the Override column. For the attributes in the Override column that are not selected, the original settings are kept.

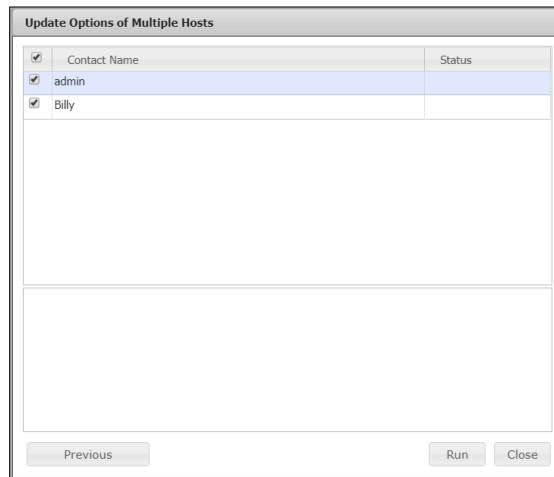


Figure 6-40

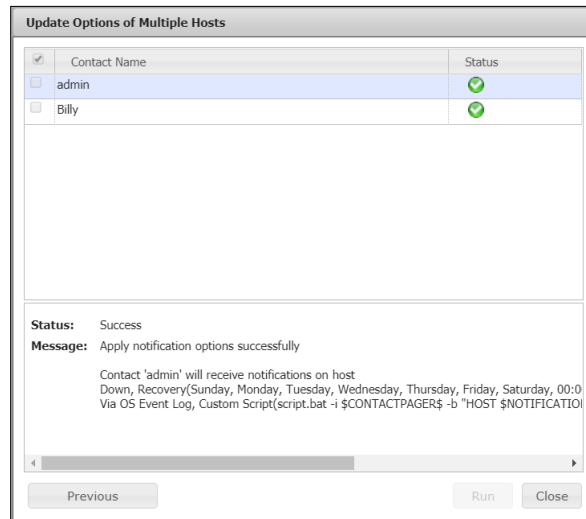


Figure 6-41

6.4.5 Editing Service Notifications for One Contact

1. Select multiple contacts in the working area. You can edit multiple contacts at once.
2. Click **Edit Service Notifications** in the command area and an Edit Service Notifications dialog box appears.

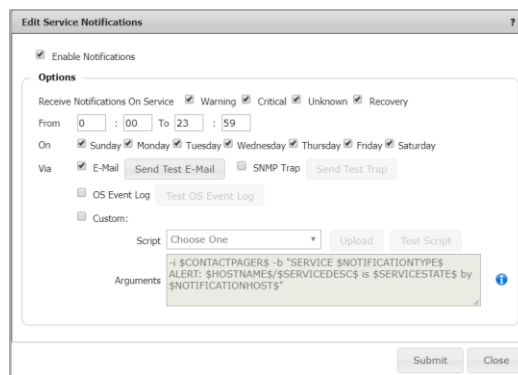


Figure 6-42

3. By default, the **Enable Notifications** checkbox is selected, meaning the selected contacts are capable of receiving notifications from services by e-mail at any time. You can uncheck the option to not receive any notifications from services and click the **Submit** button to save the changes.
4. You can also specify which service states contacts should be notified about. Services are either problematic or recovering: **Warning**, **Unknown**, **Critical** and **Recovery**. By default, the **Warning**, **Unknown**, **Critical** and **Recovery** options are all checked.
5. To define a period of time for contacts to receive notifications, you can modify the From-To and On data:

From-To

The notification is received during a certain period of time. By default, the time range is between 00:00 and 23:59.

On The notification is received on the selected weekdays. By default, all seven days in a week are selected.

6. Click the checkboxes to enable any or all of the four methods of notifications provided: E-Mail, SNMP Trap, OS Event Log and Custom Script.
 - **E-Mail:** Sends alerts via e-mail. Note that to use this function, you need to set up both the e-mail address for the contact and the e-mail SMTP server for SSM to send e-mail notifications. Please refer to the *6.10 E-Mail SMTP Setup* for details.
 - **SNMP Trap:** Sends alerts with SNMP traps. Note that to use this function, you need to set up the SNMP Trap Receiver address for the contact first.
 - **OS Event Log:** Writes alerts to Windows Logs for Windows platforms and system logs for Linux platforms.
 - **Custom Script:** Executes a predefined script for notification. A script is needed if you want to expand the notification methods.
 - **Script:** Use the drop-down menu and select one script file. If none is available, click the **Upload** button and choose a script file then upload the file to SSM. Note that you are not allowed to upload files larger than 50MB.
 - **Arguments:** You can edit arguments to suit your needs by referring to *3.4 Macro*. By default, SSM provides general information of notifications from services. In the figure below, a custom script (send_ssm.sh) is sent as a text message to a specific contact for notification. The parameters include a phone number (--phone) and a text message (--message). The message includes the notification type ("PROBLEM" or "RECOVERY"), host name, service description, the state of the service and the address of the SSM Server. For example, the command line might be like "send_ssm.sh --phone 123456789 --message "SERVICE PROBLEM ALERT: demohost/System Information is CRITICAL by demoSSMServer.""

The screenshot shows the 'Edit Service Notifications' window. It has a title bar with a question mark. The main area is divided into sections. At the top, 'Enable Notifications' is checked. Below that, 'Options' is a section header. Under 'Options', 'Receive Notifications On Service' is checked, and 'Warning', 'Critical', 'Unknown', and 'Recovery' are also checked. The 'From' time is set to 0:00 and 'To' is 23:59. Under 'On', all days of the week (Sunday through Saturday) are checked. Under 'Via', 'E-Mail' is selected, and 'Send Test E-Mail' is a visible button. 'OS Event Log' and 'Custom' are also checked. The 'Script' dropdown is set to 'send_ssm.sh', with 'Upload' and 'Test Script' buttons. The 'Arguments' field contains: '-i \$CONTACTPAGES\$ -b "SERVICE \$NOTIFICATIONTYPE\$ ALERT: \$HOSTNAME\$/\$SERVICEDESC\$ is \$SERVICESTATE\$ by \$NOTIFICATIONHOST\$"'." At the bottom right, there are 'Submit' and 'Close' buttons.

Figure 6-43

7. Click the **Submit** button to save the changes.



Note: It is highly recommended that you click the **Send Test E-Mail**, **Send Test Trap**, **Test OS Event Log** or **Test Script** button to ensure the notification method is correctly set up.

6.4.6 Editing Service Notifications for Multiple Contacts

1. Select multiple contacts in the working area. You can edit multiple contacts at once.
2. Click **Edit Service Notifications** in the command area and an Edit Service Notifications dialog box appears.

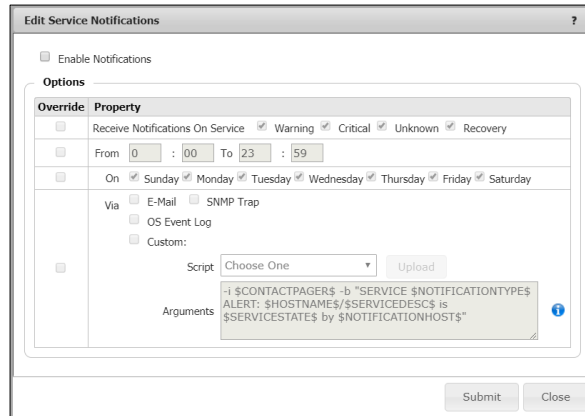


Figure 6-44

3. By default, the **Enable Notifications** checkbox is not selected (see the figure above). For all selected contacts to not receive any notifications from services, you can leave the option unchecked and click the **Submit** button to save the changes (see the figures below).

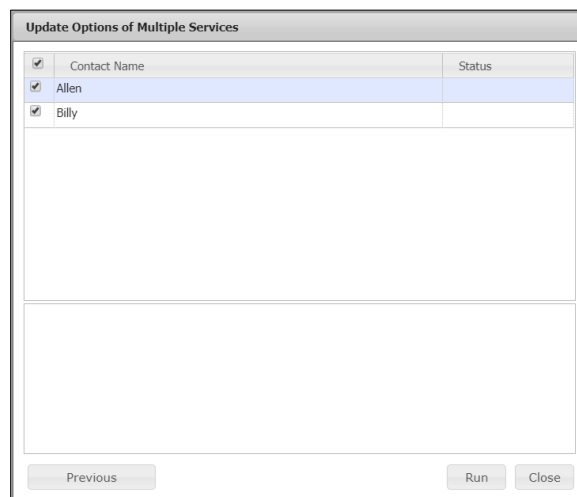


Figure 6-45

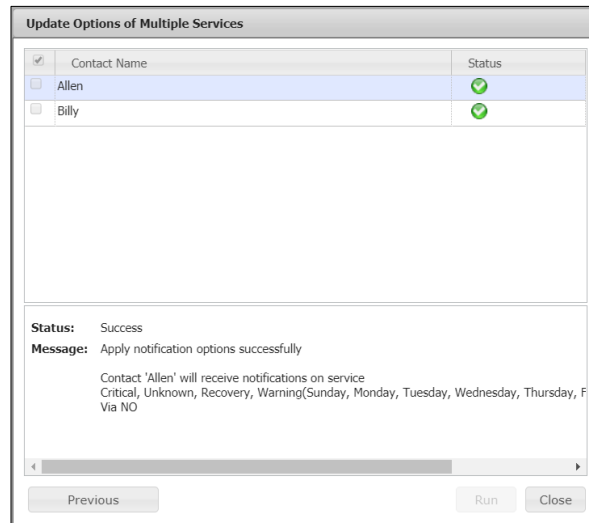


Figure 6-46

- You can click the **Enable Notification** option to enable **Override** mode so that the values you input will be set to all of the selected contacts. Or you can select the boxes in the Override column to apply the current settings to all selected contacts. If the boxes in the Override column are not selected, the original settings are kept.

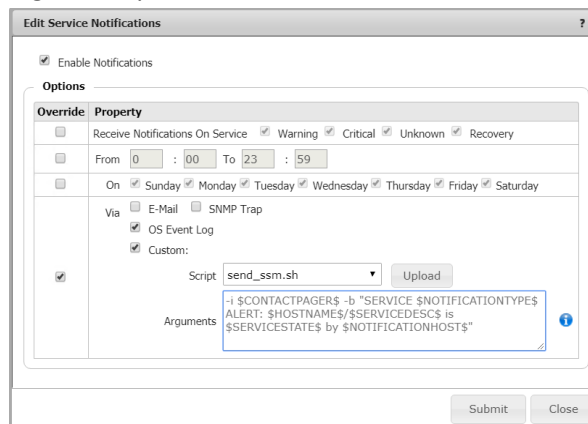


Figure 6-47

- You can also specify which service states the contacts should be notified about. Services are either problematic or recovering: **Warning**, **Unknown**, **Critical** and **Recovery**. By default, the **Warning**, **Unknown**, **Critical** and **Recovery** options are all checked.
- To define a period of time for contacts to receive notifications, you can modify the From-To and On value:

From-To The notification is received during a certain period of time. By default, the time range is between 00:00 and 23:59.

On The notification is received on the selected weekdays. By default, all seven days in a week are selected.

7. Click the checkboxes to enable any or all of the four methods of notifications provided: E-Mail, SNMP Trap, OS Event Log and Custom Script.
 - **E-Mail:** Sends alerts via e-mail. To use this function, you need to set up both the e-mail address for the contact and the e-mail SMTP server for SSM to send e-mail notifications. Please refer to the *6.10 E-Mail SMTP Setup* for details.
 - **SNMP Trap:** Sends alerts with SNMP traps. To use this function, you need to first set up the SNMP Trap receiver address for the contact.
 - **OS Event Log:** Writes alerts to Windows Logs for Windows platforms and system logs for Linux platforms.
 - **Custom Script:** Executes a predefined script for notification. A script is needed if you want to expand the notification methods.
 - **Script:** Use the drop-down menu and select one script file. If none is available, click the **Upload** button then choose a script file and upload the file to SSM. Note that you are not allowed to upload files larger than 50MB.
 - **Arguments:** You can edit arguments to suit your needs by referring to *3.4 Macro*. By default, SSM provides general information of notifications from services. In the figure below, a custom script (send_ssm.sh) is sent as a text message to a specific contact for notification. The parameters include a phone number (--phone) and a text message (--message). The message includes the notification type ("PROBLEM" or "RECOVERY"), host name, service description, the state of the service and the address of the SSM Server. For example, the command line might be "send_ssm.sh --phone 123456789 --message "SERVICE PROBLEM ALERT: demohost/System Information is CRITICAL by demoSMServer."

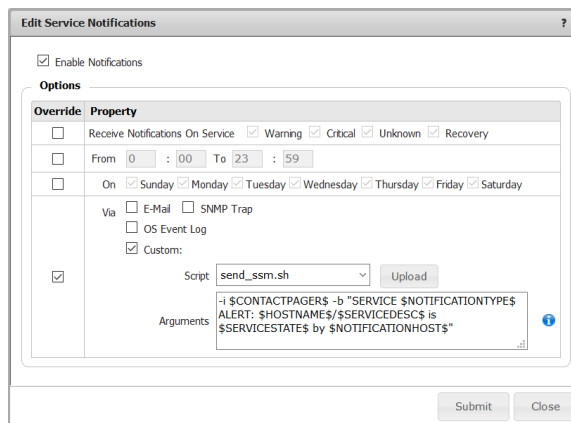


Figure 6-48

8. When you are done, click the **Submit** button to save the changes (see the figure below), and all selected contacts will be applied with the settings in the Override column. For the attributes in the Override column that are not selected, the original settings are kept.

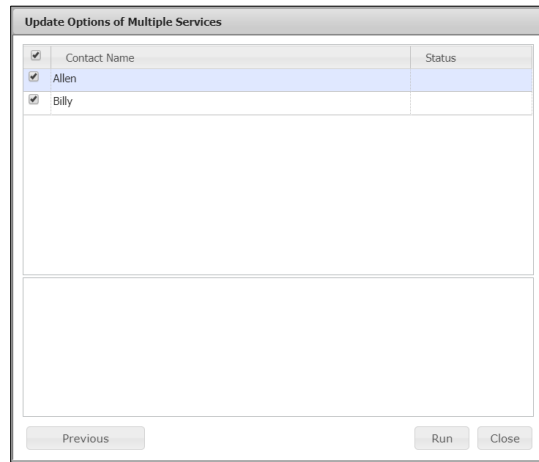


Figure 6-49

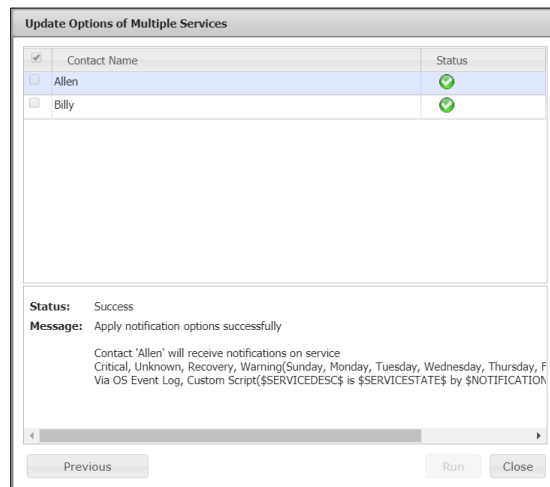


Figure 6-50

6.4.7 Example of Simple Custom Script

The example below illustrates how all arguments are echoed into the console. You are required to edit the custom script to meet your needs. Note that your own scripts must meet the OS your SSM Server is running on, for example, batch file (.bat) for Windows platforms and shell script (.sh) for Linux platforms.



```
root@6d4c9342bb0f:~/customscript
[root@6d4c9342bb0f customscript]# cat send_ssm.sh
#!/bin/sh

echo $1
echo $2
echo $3
echo $4

hostNaddress=$2
text=$(echo $4 | sed "s/'//g")
text=$(echo $text | sed 's/"//g')

echo \"$hostNaddress $text\" >> ./ENSTest.log

[root@6d4c9342bb0f customscript]#
```

Figure 6-51

6.5 Contact Group Management

Click **Contact Group** in the navigation area to perform contact group management functions. Similar to a contact, a contact group represents a group of receivers. Each of the contacts in a contact group receives a notification message sent from the SSM Server when the status of a host or service has changed. On this page you can add, edit, delete contact groups, and assign contact group members.

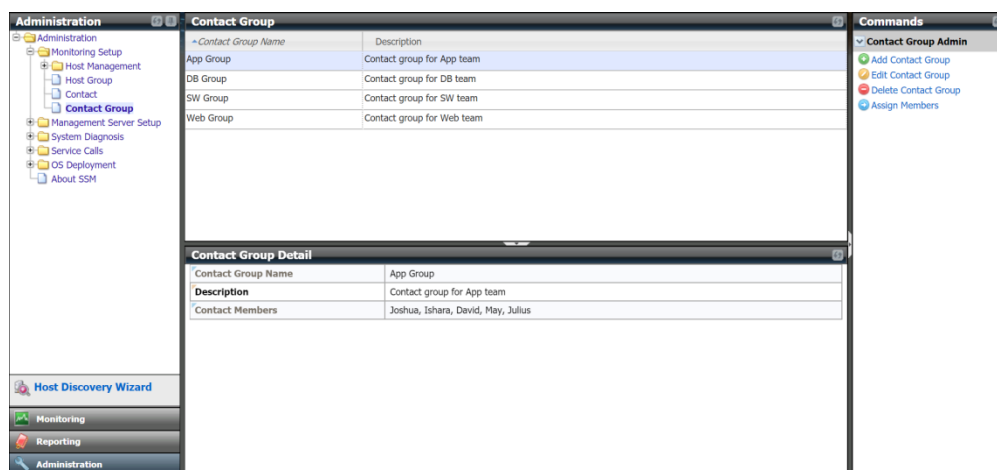


Figure 6-52

6.5.1 Adding a Contact Group

1. Click **Add Contact Group** in the commands area and you will see an Add Contact Group dialog box, as shown below.

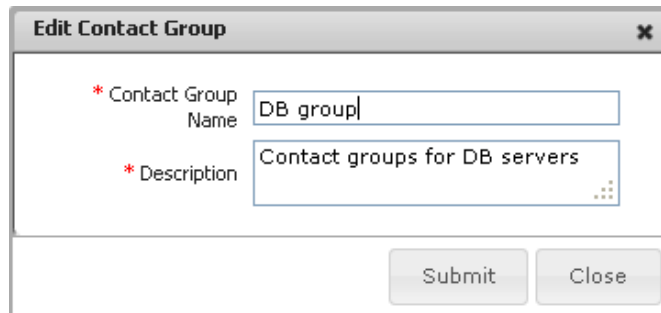
The dialog box titled 'Add Contact Group' contains two required input fields: 'Contact Group Name' and 'Description'. Both fields are marked with a red asterisk. Below the fields are 'Submit' and 'Close' buttons.

Figure 6-53

2. Input the contact group data in this dialog box.
3. When completed, click the **Submit** button to add the contact group or the **Close** button to abort and close this dialog box.

6.5.2 Editing a Contact Group

1. Select one contact group to be edited in the working area. You can edit only one contact group at a time.
2. Click **Edit Contact Group** in the area and you will see an Edit Contact Group dialog box, as shown below.



The screenshot shows a dialog box titled "Edit Contact Group". It has a close button (X) in the top right corner. The dialog contains two required fields, indicated by red asterisks: "Contact Group Name" with the text "DB group" and "Description" with the text "Contact groups for DB servers". At the bottom of the dialog are two buttons: "Submit" and "Close".

Figure 6-54

3. When completed, click the **Submit** button to confirm the modification or the **Close** button to abort and close this dialog box.

6.5.3 Deleting a Contact Group

1. Select contact groups to be deleted in the working area. You can delete multiple contact groups at a time.

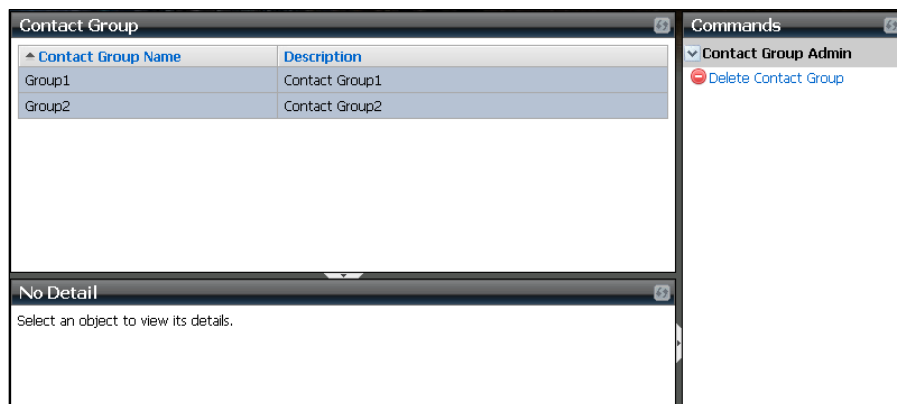


Figure 6-55

-
2. Click **Delete Contact Group** in the commands area and you will see a Delete Contact Group dialog box, as shown below.

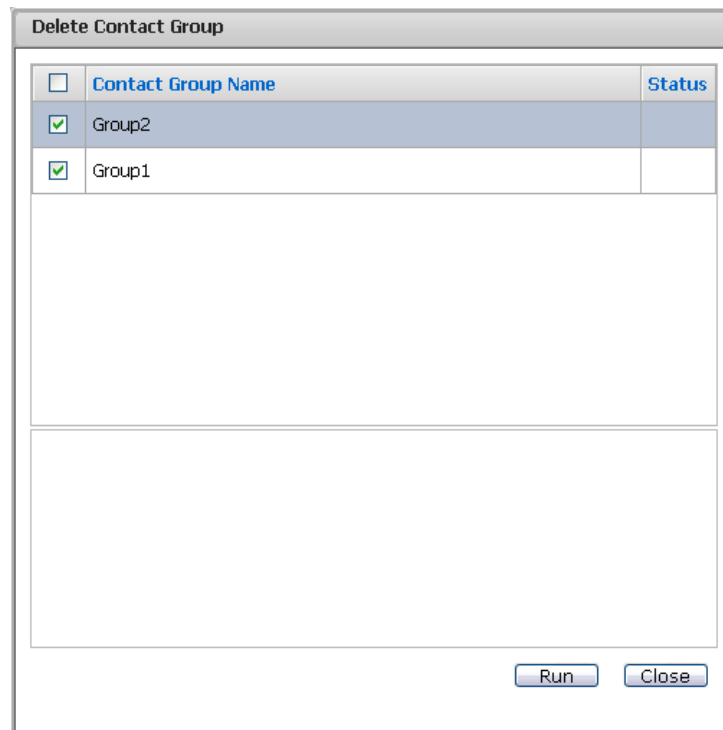


Figure 6-56

3. Click the **Run** button to delete the selected contact groups or the **Close** button to abort and close this dialog box.

6.5.4 Assigning Members

1. Select a contact group in the working area.
2. Click **Assign Members** in the command area and you will see an Assign Members dialog box, as shown below.

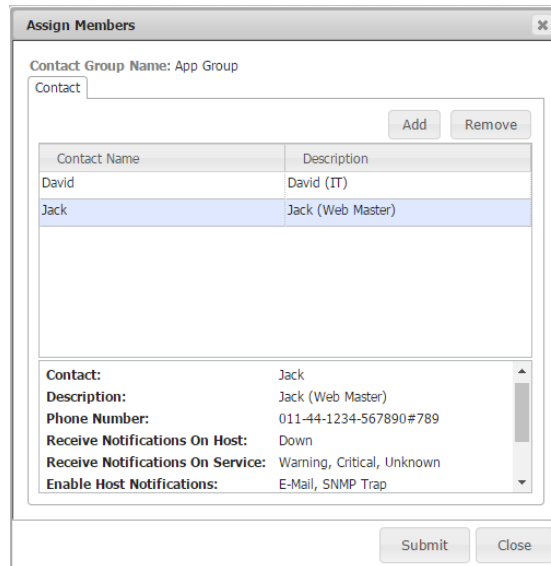


Figure 6-57

3. To remove a contact from the contact group, click the **Remove** button. To assign contacts to the contact group, click the **Add** button and you will see a contact query dialog box, as shown below. Select the contacts to be included in the contact group. When completed, click the **Submit** button to add the selected contacts to this contact group or the **Close** button to abort and close this dialog box.

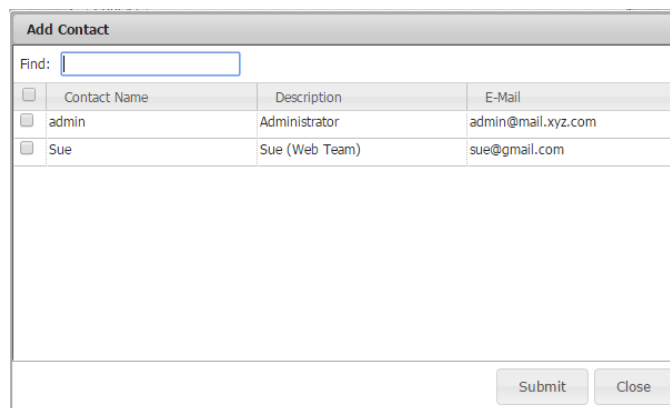


Figure 6-58

6.6 Node PK Activation

Before using SSM functions, IPMI hosts and Redfish hosts need to be activated. The **Node PK Activation** page allows you to activate numerous product keys from a file. Two types of license key formats are supported:

- **xxxx-xxxx-xxxx-xxxx-xxxx-xxxx**, e.g., SFT-OOB-LIC
- **a 344-byte ASCII string**, e.g., SFT-DCMS-Single, SFT-SUM-LIC or SFT-DCMS-SVC-KEY

Contact Supermicro if you are not sure if your license key is supported.

SSM activates the BMC via the Redfish protocol. If required Redfish API is not found, SSM will activate the BMC via the IPMI protocol.



Notes:

- This feature is for hosts that have not been managed by the SSM. For hosts that have been added to the SSM, please see *10.2.1 Checking Activation Status*.
- The Supermicro Redfish API does not support the activation of SFT-OOB-LIC key. The IPMI protocol must work on a BMC to activate a SFT-OOB-LIC key.

Here you will be guided through the steps on the Node PK Activation page to activate your product key.

The screenshot shows the 'Node PK Activation' page within the Supermicro Server Manager Administration console. The left sidebar contains a navigation tree with 'Node PK Activation' selected. The main content area is titled 'Node PK Activation' and includes the following sections:

- Header:** 'Activate multiple node product keys from the file obtained from Supermicro.'
- Instructions:** 'Follow the steps to complete the activation:'
- Step 1:** 'You need to collect the MAC addresses of the managed systems before contacting Supermicro to generate your node product keys (SFT-OOB-LIC Key, SFT-DCMS-Single, SFT-DCMS-SVC-KEY, etc.). Enter the BMC addresses, IDs and passwords of the managed systems and click the "Collect" button to download the activation request file. Note that all managed systems can be only accessed with the provided BMC ID and password.'
 - BMC Address:** Text input field containing '192.168.34.1,192.168.34.2,192.168.34.3'
 - BMC ID:** Text input field
 - BMC Password:** Text input field
 - Collect:** Button
- Step 2:** 'Contact Supermicro and provide the activation request file to generate a node product key. Supermicro will send you an activation response file with your node product keys.'
- Step 3:** 'Upload the activation response file and click the "Activate" button, and SSM will activate the managed systems one by one according to the file. Note that all managed systems can be only accessed with the provided BMC ID and password.'
 - File:** File selection area with 'Choose File' and 'No file chosen' options
 - BMC ID:** Text input field
 - BMC Password:** Text input field
 - Activate:** Button

Figure 6-59

1. Before activating any product key, you need to collect the MAC addresses of the managed systems.
 - (1). Fill out the fields Managed Systems, BMC ID and BMC Password, and then click the **Collect** button.

Step 1

You need to collect the MAC addresses of the managed systems before contacting Supermicro to generate your node product keys (SFT-OOB-LIC Key, SFT-DCMS-Single, SFT-DCMS-SVC-KEY, etc.). Enter the BMC addresses, IDs and passwords of the managed systems and click the "Collect" button to download the activation request file. Note that all managed systems can be only accessed with the provided BMC ID and password.

BMC Address

BMC ID

BMC Password

Figure 6-60

- (2). The Collect MAC Addresses dialog box will pop up if the input data in the three fields is valid. Note that SSM will eliminate redundant BMC addresses. Click the **Run** button to start collecting the MAC addresses of the managed systems.

Collect MAC Addresses

Run the command on these targets

<input checked="" type="checkbox"/>	BMC IP Address	Status
<input checked="" type="checkbox"/>	172.31.50.101	
<input checked="" type="checkbox"/>	172.31.50.104	
<input checked="" type="checkbox"/>	172.31.50.86	

Figure 6-61

- (3). Click the **Export MAC(s) File** button to export MAC addresses to a file. The output file ("mymacs.txt") includes a MAC address and a BMC address.

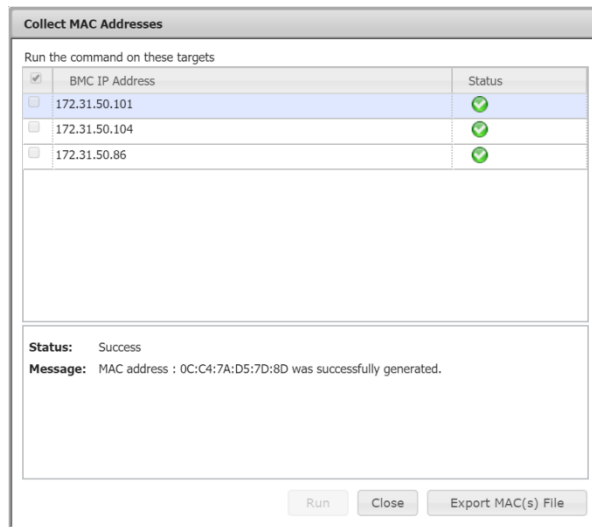


Figure 6-62

Example:

0CC47AD57D8D;172.31.50.101

0CC47AD57D8F;softlab-bmc.supermicro.com.tw



Note: SSM does not support the node product key activation for an IPv6 address of a BMC.

2. Contact Supermicro to generate an activation file with the exported MAC file. The activation file (“mymacs.txt”) includes a MAC address, a BMC address and a product key, which are separated with semicolons.

Step 2
 Contact Supermicro and provide the activation request file to generate a node product key. Supermicro will send you an activation response file with your node product keys.

Figure 6-63

Example:

0CC47AD57D8D;172.31.50.101;AAkAAAAAAAAAAAAAAAAAMjnO7OleNNWpc63TFto8dp6A5UrXzkBpQdkhtnMrUR/oTFKIdhLPpli6b32IQJFaoPly7uj2OztgzUxjKy1kdMDrEEFra1KILDrBoZC88fAWfuVXmnVBhjR7tNKSa4r29owr8M3ETun+GxqerDT8kDa+jafMEkETjDJ2Gln6sk7oRCLA7xVZhG1RfkyjcrO+qyYL4OOHH8GG8CUTDx/dlBCXH8i3TL3g5d7X8U/B2XO/z85JUWOeVgwEzUXxK0eN5I3ub/OGYXVzMAH0fiq0LU6srDV+Qvc82gwckcrUKGpi0c6DUXl/qWUWDsWFrG48w==

3. To upload the activation file provided by Supermicro, follow these steps:
 - (1). Click the **Choose File** button and select the activation file (“mymacs.txt”), fill in the BMC ID and BMC Password fields, and then click the **Activate** button.

Step 3

Upload the activation response file and click the "Activate" button, and SSM will activate the managed systems one by one according to the file. Note that all managed systems can be only accessed with the provided BMC ID and password.

File mymacs.txt

BMC ID

BMC Password

Figure 6-64

- (2). The Node PK Activation dialog box will pop up if the input data in the text fields is valid. Click the **Run** button to start activating the product keys on the managed systems. Note that if duplicated product keys are found, confirm the product keys with Supermicro and upload the product key again.

Node PK Activation

Run the command on these targets

<input checked="" type="checkbox"/>	BMC Address	Product Key	Status
<input checked="" type="checkbox"/>	172.31.50.101	AAKAAAAAAAAAAAAAAAAAMjnO701e...	
<input checked="" type="checkbox"/>	172.31.50.104	AAAYAAAAAAAAAAAAAAAAALYkleG6tX...	
<input checked="" type="checkbox"/>	172.31.50.86	AAAYAAAAAAAAAAAAAAAAAJnph9JFTG...	

Figure 6-65

- (3). Then the activation results are listed.

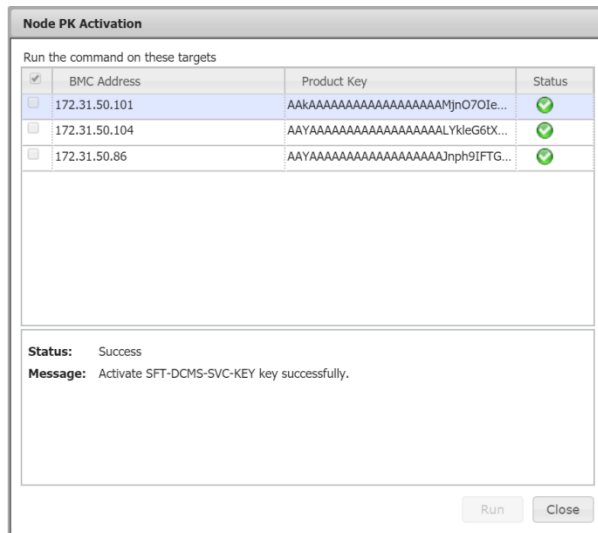


Figure 6-66

When a product key fails to activate on a host, it is automatically selected to be re-activated later. Click the **Run** button to activate the product key again in case the BMC is not available at the time.



Notes:

- Multiple product keys are allowed to exist on one BMC. If an error occurs, locate the problematic product key and report it to Supermicro.
- If you have multiple sets of BMC IDs and passwords to access the managed systems, it's required to divide the activation process into multiple groups.

6.7 User Roles

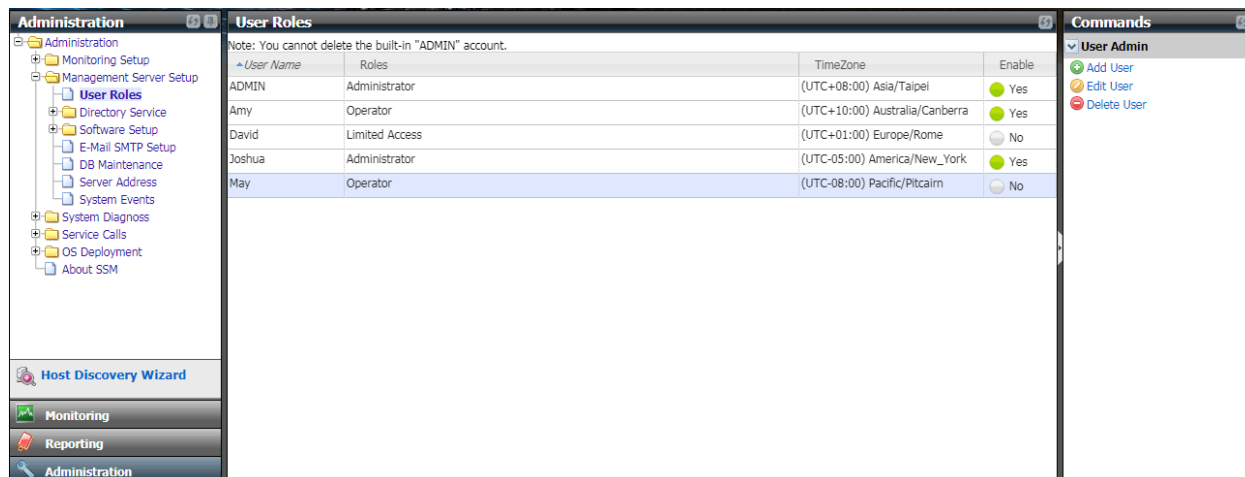


Figure 6-67

Click **User Roles** in the navigation area to perform user management functions. In this page you can add, edit, and delete users. A user represents a login account that can be used to access SSM Web. SSM supports role-based access control, which contains three different roles:

- **Limited Access:** Users with this role are basic users who can log in to SSM Web and perform read only monitoring and reporting functions.
- **Operator:** Users with the operator role can perform the monitoring, reporting and remote control functions.
- **Administrator:** Users with the admin role can perform all functions. SSM has a built-in **ADMIN** user belonging to this role. Note that the built-in **ADMIN** user cannot be deleted.

A user can be enabled or disabled. If a user is disabled, their account cannot be used to log in to SSM.

- The following matrix lists the specific commands for Limited Access, Operator and Administrator roles. To obtain the role of the login account, log into the SSM Web and click the upper-right corner.

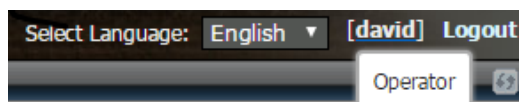


Figure 6-68

Feature	Role		
	Administrator	Operator	Limited Access
[Command category] Command			
[Monitoring Page] / [Agent Managed]			
Graceful Power Off	<input type="radio"/>	<input type="radio"/>	
Graceful Reboot	<input type="radio"/>	<input type="radio"/>	
Reset Chassis Intrusion	<input type="radio"/>		
Reset SD5 User Password	<input type="radio"/>	<input type="radio"/>	
Update SD5	<input type="radio"/>	<input type="radio"/>	
Wake on LAN	<input type="radio"/>	<input type="radio"/>	
[Monitoring Page] / [IPMI]			
BMC Cold Reset	<input type="radio"/>		
Blink UID LED	<input type="radio"/>	<input type="radio"/>	
Clear BMC Log	<input type="radio"/>	<input type="radio"/>	
Clear BMC and BIOS Log	<input type="radio"/>		
Clear TPM Provision	<input type="radio"/>		
Deploy OS	<input type="radio"/>		
Edit DMI Info	<input type="radio"/>		
Enable TPM Provision	<input type="radio"/>		
Export Asset Info	<input type="radio"/>		
Export BIOS Cfg	<input type="radio"/>		
Export BMC Cfg	<input type="radio"/>		
Export BMC Log	<input type="radio"/>		
Export DMI Info	<input type="radio"/>		
Export Factory BIOS Cfg	<input type="radio"/>		
Export System Utilization	<input type="radio"/>		

Feature	Role		
Graceful Power Off	<input type="radio"/>	<input type="radio"/>	
Import BIOS Cfg	<input type="radio"/>		
Import BMC Cfg	<input type="radio"/>		
Import DMI Info	<input type="radio"/>		
Load Factory BIOS Cfg	<input type="radio"/>		
Mount ISO Image	<input type="radio"/>		
Power Off	<input type="radio"/>	<input type="radio"/>	
Power On	<input type="radio"/>	<input type="radio"/>	
Reset	<input type="radio"/>	<input type="radio"/>	
Reset Chassis Intrusion	<input type="radio"/>		
Stop Blink UID LED	<input type="radio"/>	<input type="radio"/>	
Sync Node PK	<input type="radio"/>		
Unmount ISO Image	<input type="radio"/>		
Update BIOS	<input type="radio"/>		
Change BMC Password	<input type="radio"/>		
Update BMC	<input type="radio"/>		
[Monitoring Page] / [Redfish]			
BMC Cold Reset	<input type="radio"/>		
Blink UID LED	<input type="radio"/>		
Clear BMC Log	<input type="radio"/>		
Diagnose System	<input type="radio"/>		
Disable System Lockdown	<input type="radio"/>		
Enable System Lockdown	<input type="radio"/>		
Graceful Power Off	<input type="radio"/>	<input type="radio"/>	
Power Off	<input type="radio"/>	<input type="radio"/>	
Power On	<input type="radio"/>	<input type="radio"/>	
Reset	<input type="radio"/>	<input type="radio"/>	
Reset Chassis Intrusion	<input type="radio"/>		
Stop Blink UID LED	<input type="radio"/>		
Sync Node PK	<input type="radio"/>		
[Monitoring Page] / [Power Management]			
Power Consumption Trend	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Power Policy Management	<input type="radio"/>	<input type="radio"/>	
[Monitoring Page] / [System Information]			

Feature	Role		
View Details	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
[Monitoring Page] / [Remote Control]	<input type="radio"/>	<input type="radio"/>	
[Monitoring Page] / [Host Admin]	<input type="radio"/>		
[Monitoring Page] / [Reports]	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
[Monitoring Page] / [Service Admin]			
Service Properties	<input type="radio"/>		
Notification Properties	<input type="radio"/>		
Change Arguments	<input type="radio"/>		
Assign Contact and Contact Group	<input type="radio"/>		
Check Now	<input type="radio"/>		
Delete Service	<input type="radio"/>		
Performance Data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
[Reporting Page]	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
[Administration Page]	<input type="radio"/>		

6.7.1 Adding a User

1. Click **Add User** in the command area and you will see an Add User dialog box as shown below.

Figure 6-69

2. Enter the user data in this dialog box.
3. Click the **Submit** button to add the user or the **Close** button to abort and close this dialog box.

6.7.2 Editing a User

1. Select one user to be edited in the working area. You can edit only one user at a time.
2. Click **Edit User** in the command area and you will see an Edit User dialog box as shown below.

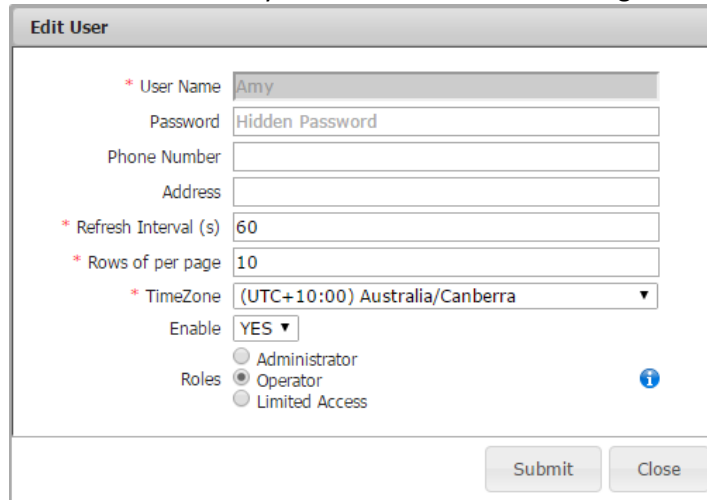


Figure 6-70

3. Modify the user data in this dialog box. Note that you cannot change the user name. To change a user name, you need to delete the user and add a new user.
4. Click the **Submit** button to confirm the modification or the **Close** button to abort and close this dialog box.



Note: A local user may modify his or her password, time zone, etc. by clicking [account name] in the upper right corner after logging in to SSM Web as shown below. It is not possible to see the detailed information of or to modify the login account for LDAP or AD accounts.

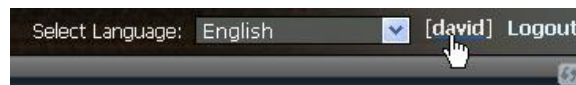


Figure 6-71

6.7.3 Deleting a User

1. Select users to be deleted in the working area. You can delete multiple users at a time⁸.

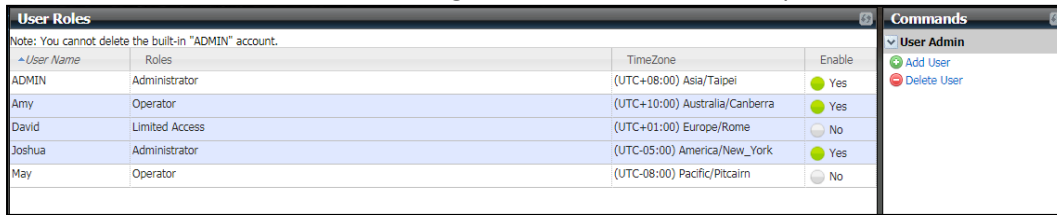


Figure 6-72

2. Click **Delete User** in the command area and you will see a Delete User dialog box, as shown below.

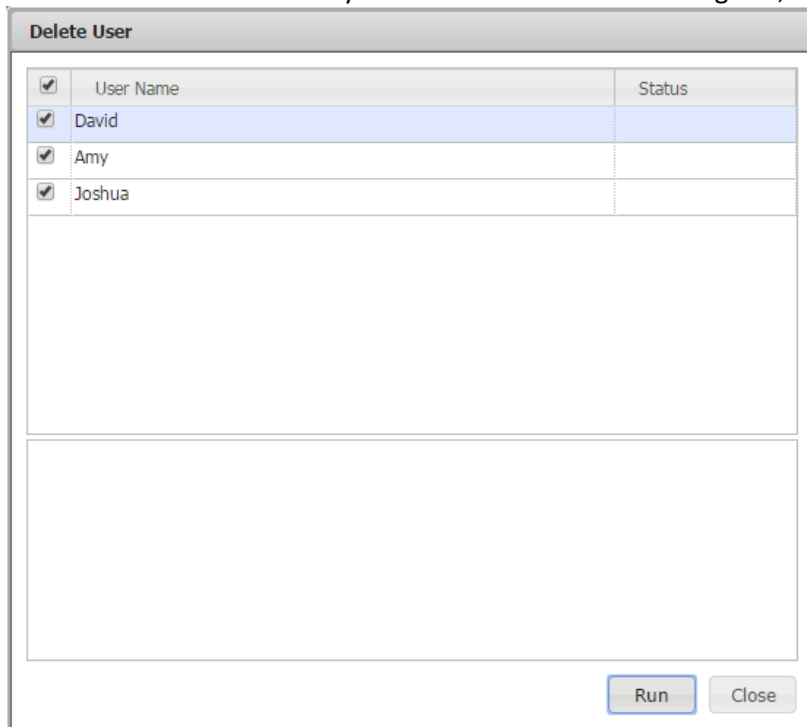


Figure 6-73

3. Click the **Run** button to delete the selected users or the **Close** button to abort and close this dialog box.

⁸ Use [ctrl] + [left mouse click button] to select multiple users in the working area.

6.8 Directory Services

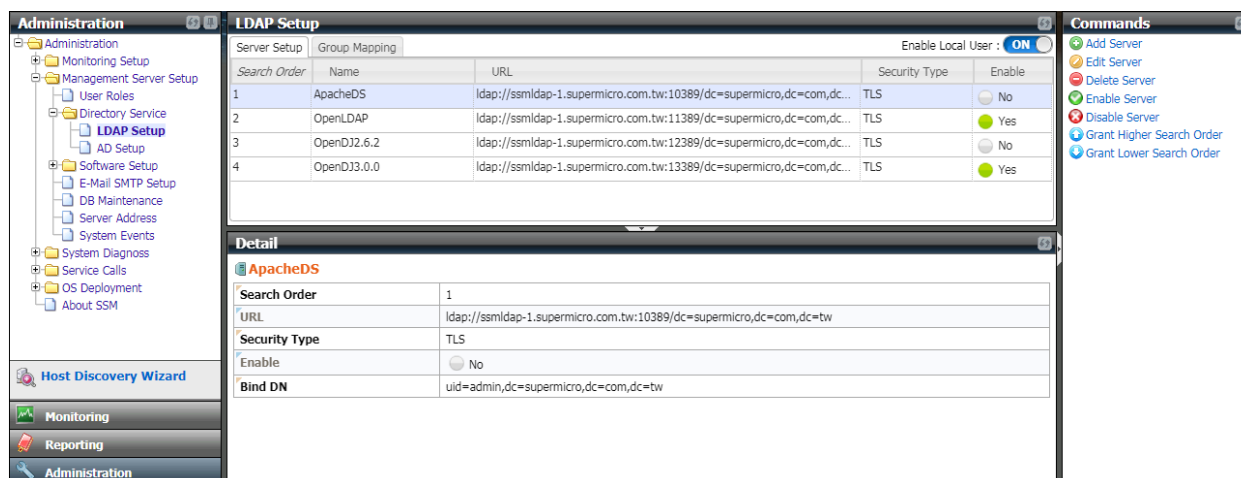


Figure 6-74

Click **LDAP Setup** (or **AD Setup**, whichever one suits your needs) in the navigation area to perform the **Directory Service** function. The **Directory Service** function allows SSM to contact Lightweight Directory Access Protocol (LDAP⁹) services or Active Directory (AD) services to authenticate the user.

The master view shows a list of directory servers while the detailed view shows the detailed contents of the directory server. The master view includes two tabs: **Server Setup** and **Group Mapping**. Select the **Server Setup** tab to add, edit, and delete directory servers in the commands area.

If configured, users are able to use their LDAP accounts to log into SSM. SSM searches the account in the directory servers one at a time until the login user is found or until all of the enabled servers are searched. Only accounts found in LDAP are allowed to access SSM.

By default, SSM will allow local users to log into SSM even if the directory service is configured. The **Enable Local User** toggle in the upper right corner of the master view is for users to enable or disable local users. Note that if you disable local users before properly configuring directory services, you will be unable to log onto SSM.

⁹ LDAPv3 (LDAP version 3) is supported only because LDAPv3 was developed in the late 1990's to replace LDAPv2.

6.8.1 Configuring Directory Services

6.8.1.1 Adding an LDAP Server

1. Click **Add Server** in the command area. The Add Server dialog box appears.

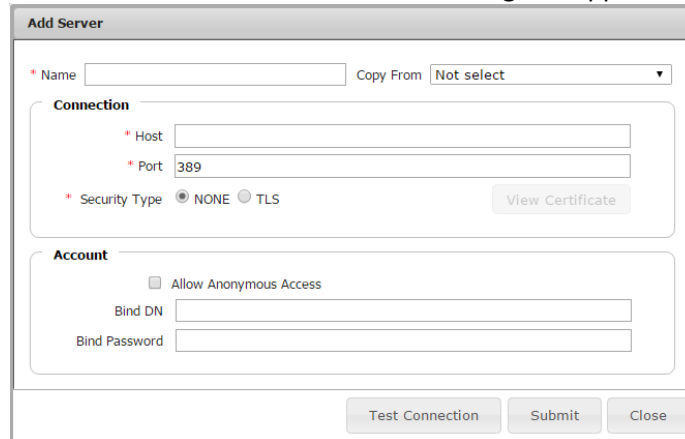


Figure 6-75

2. Input the LDAP server settings in this dialog box. An LDAP server is determined by the following attributes:

Name:	A unique name used to identify the directory server.
Host:	The host of the LDAP server. Either a DNS name (FQDN), an IPv4 address, or an IPv6 address. If a TLS connection is used between SSM and the LDAP server, only FQDN can be specified.
Port:	The directory server's port number.
Security Type:	The security type of the connection. If the directory server does not provide TLS connections, select NONE, otherwise, select TLS. StartTLS is used here to establish an encrypted connection within an already established unencrypted connection.
Allow anonymous access:	Checks whether the Bind requires a Distinguished Name (DN) as well as a password.
Bind DN:	Used to connect to the directory server.
Bind Password:	Used to connect to the directory server.

Figure 6-76



Note: You can click the selection of the **Copy From** option to copy the server settings from an existing LDAP server.

3. Click the **Test Connection** button to check if the server settings are correct. If you select a TLS connection between SSM and the directory server, you need to install the certificate first. A certificate information dialog box pops up. Read the certificate carefully and click **Install Certificate** to continue the installation or click **Cancel** to abort.

Issued To	ssmldap-1.supermicro.com.tw
Issued By	ssmldap-1.supermicro.com.tw
Valid From	2016/05/12 To 2066/04/30

Figure 6-77

4. After the certificate is installed, you can click **View Certificate** to check the certificate. The host in the Issued To field indicates the LDAP server. If the certificate's host name does not match the host name in the dialog box, an error message appears in the Certificate dialog box after the **Test Connection** button is clicked.



Figure 6-78

5. Click the **Submit** button to add the LDAP server or the **Close** button to abort and close this dialog box. Note that the LDAP server setting in this dialog box will be added no matter what the connection status of the LDAP server is; therefore it's recommended that you click **Test Connection** before **Submit** to ensure that it is connectable.

6.8.1.2 Adding an AD Server

1. Click **Add Server** in the command area. The Add Server dialog box appears.

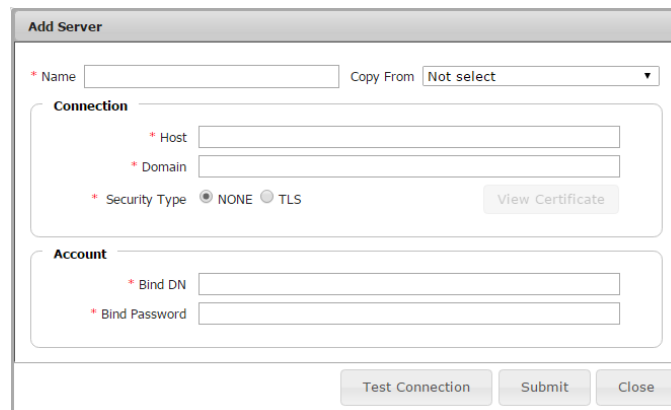


Figure 6-79

2. Input the AD server settings in this dialog box. An AD server is determined by the following attributes:

Name: A unique name used to identify the directory server.

Host: The host of the AD server. Either a DNS name (FQDN), an IPv4 address, or an IPv6 address. If a TLS connection is used between SSM

and the LDAP server, only FQDN can be specified.

- Domain:** The domain of the AD server. The name should consist of one or more labels separated by a period (“.”).
- Bind DN:** Used to connect to the directory server.
- Bind Password:** Used to connect to the directory server.
- Security Type:** The security type of the connection. If the directory server does not provide TLS connections, select NONE, otherwise, select TLS. StartTLS is used here to establish an encrypted connection within an already established unencrypted connection.



Note: You can click the selection of the **Copy From** option to copy the server settings from an existing AD server.

- Click the **Test Connection** button to check if the server settings are correct. If you select the TLS connection between SSM and the directory server, you need to install a certificate first. A certificate information dialog box (see the figure below) pops up. Read the certificate carefully and click **Install Certificate** to continue the installation or click **Cancel** to abort.

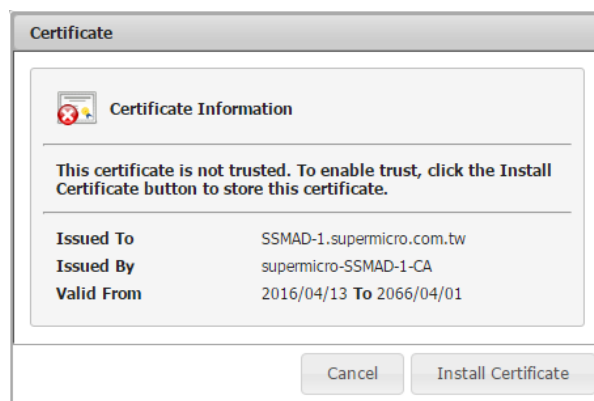


Figure 6-80

- After the installation of the certificate, you can click **View Certificate** to check the certificate. The host in the Issued To field indicates the AD server. If the certificate's host name does not match the host name in the dialog box, an error message appears in the Certificate dialog box after the **Test Connection** button is clicked.

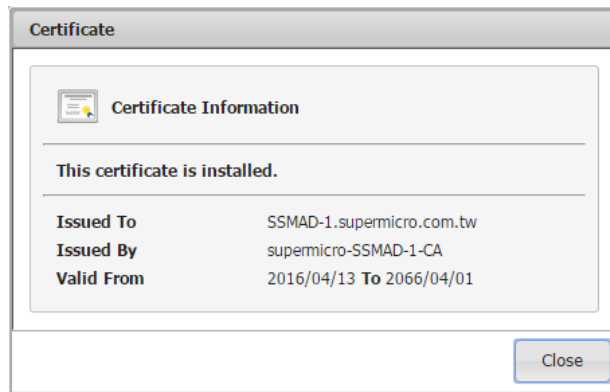


Figure 6-81

5. Click the **Submit** button to add the AD server or the **Close** button to abort and close this dialog box. Note that the LDAP server setting in this dialog box will be added no matter what the connection status of the LDAP server is; therefore it's recommended that you click **Test Connection** before **Submit** to ensure that it is connectable.

6.8.1.3 Editing an LDAP/AD Server

1. Click **Edit Server** in the command area and you will see the Edit Server dialog box. You can modify the LDAP (edit an AD Server is similar to edit an LDAP server) server settings in this dialog box.

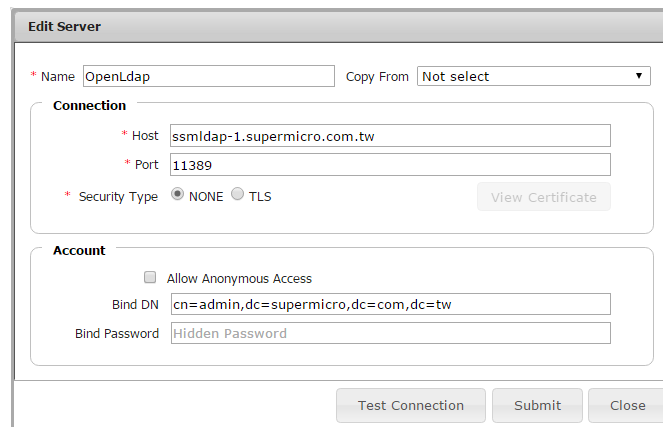


Figure 6-82



Note: The certificate for the TLS connection is host-dependent so that you have to re-install the certificate if you change the host in this dialog box.

2. Click the **Submit** button to confirm the modification or the **Close** button to abort and close this dialog box.

6.8.1.4 Deleting an LDAP/AD Server

1. Select one or more servers in the working area. You can delete multiple servers at a time.

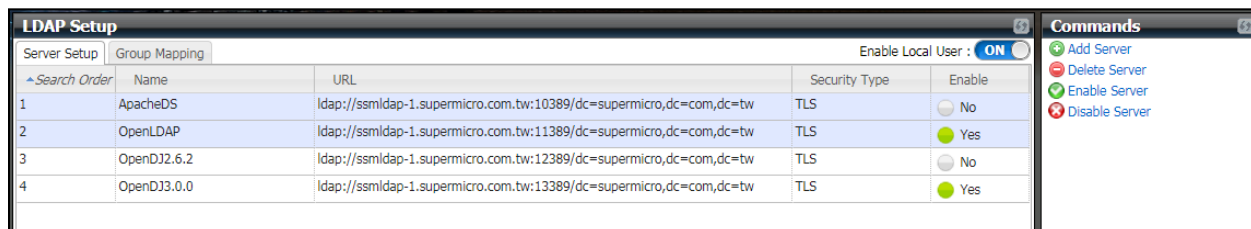


Figure 6-83

2. Click **Delete Server** in the command area and a Delete Server dialog box appears.

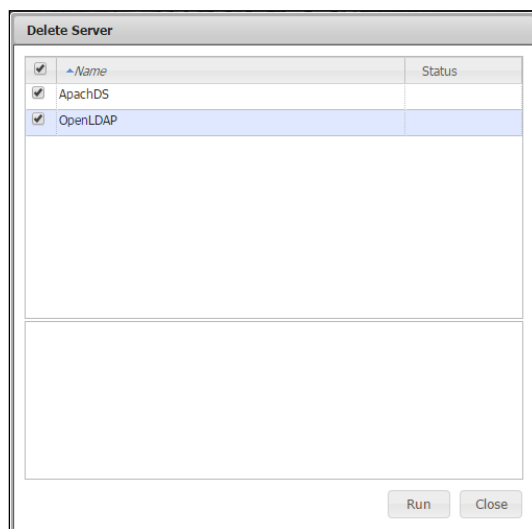


Figure 6-84

3. Click the **Run** button to delete the selected servers or the **Close** button to abort and close this dialog box.

6.8.1.5 Changing the Status of an LDAP/AD Server

The **Enable** column in the master view shows the status of the LDAP/AD server. Note that only the enabled directory servers will be used to look for the login users.

1. To enable or disable the directory servers, select multiple servers at a time in the working area.

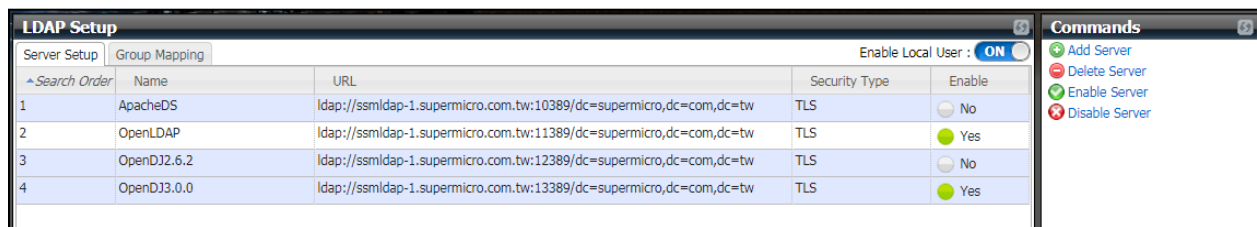


Figure 6-85

2. Click **Enable Server** (or **Disable Server**, the procedure is similar to that of enabling directory servers procedure) in the command area and a dialog box appears.

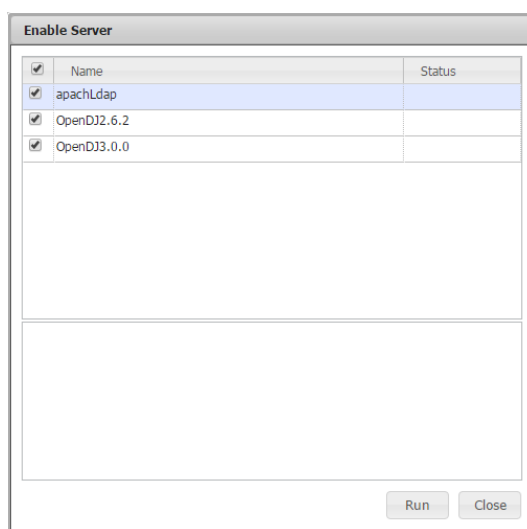


Figure 6-86

3. Click the **Run** button to enable or disable the selected servers or the **Close** button to abort and close this dialog box.

6.8.1.6 Changing the Search Order of an LDAP/AD Server

The **Search Order** column in the master view shows the search priority of the directory server. To give higher priority to the directory server, select one directory server in the working area, and then click **Grant Higher Search Order** in the commands area. To give lower priority to the directory server, select one directory server in the working area, and then click **Grant Lower Search Order** in the commands area. You can only select one server at a time to change the search order. SSM looks for the login user in the directory servers by the sequence of the predefined search orders.

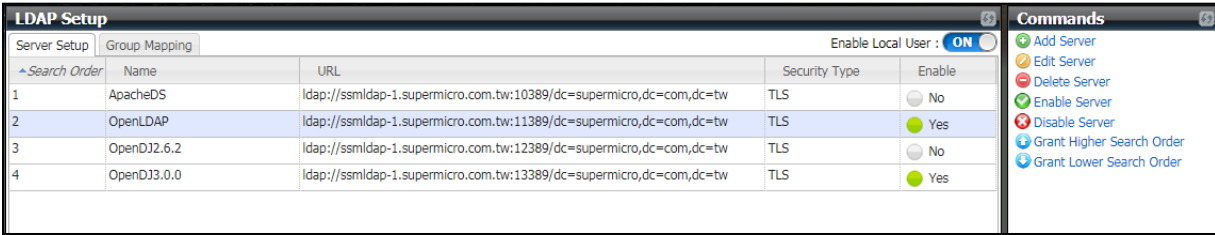


Figure 6-87

6.8.2 Configuring User and Group Search Criteria

The **Group Mapping** tab in the master view (see the figure below) is used to configure the user and group search criteria. The setting will be used to check if the login user has permission to access SSM and what permission the login user has. Note that the **Group Mapping** tab is available when at least one directory server exists. After you define search criteria in the **Group Mapping** tab, the settings will apply to all of the directory servers in the **Server Setup** tab.



Note: The configuration of group mapping in AD servers is a subset of that in LDAP servers. The following figure shows an example of Group Mapping for LDAP servers and will omit the explanation of AD.

LDAP Setup (Server Setup | Group Mapping) Enable Local User : **ON**

User Search Options

- * Base DN:
- * User Search Filter:
Define user search criteria. Use 'uid={0}' as default.
- User Search Base: ,dc=supermicro,dc=com,dc=tw
If you want to specify more precise user search criteria, specify here. e.g. 'ou=users,ou=Supermicro'.

Group Search Options

- * Group Search Filter:
Define group search criteria. Use 'uniqueMember={0}' as default.
- Group Search Base: ,dc=supermicro,dc=com,dc=tw
If you want to specify more precise group search criteria, specify here. e.g. 'ou=groups,ou=Supermicro'.
- Role : Administrator:
Specify groups that have Administrator Role and multiple values are separated by a comma.
- Role : Operator:
Specify groups that have Operator Role and multiple values are separated by a comma.
- Role : Limited Access:
Specify groups that have Limited Access Role and multiple values are separated by a comma.

Test Search Options Apply

Figure 6-88

- User Search Options is used to identify the login user. Note that it's necessary for you to configure the following attributes to ensure the uniqueness of the login user. Otherwise the user is likely to fail to log in.

Base DN: The base address for SSM to start a search. For example, if the Base DN is "dc=supermicro,dc=com,dc=tw", SSM will search the login user from "dc=supermicro,dc=com,dc=tw" for any account that matches the login user.

User Search Filter: A search filter to identify the user. The default is "uid={0}".

User Search Base: A DN is used to limit the search range. If not specified, SSM will search the login user from the base DN.

- Group Search Options is used to check the permissions a user has. Note that it's necessary for you to configure the following attributes to ensure the uniqueness of the group the login user belongs

to. Otherwise the user is likely to fail to log in.

- Group Search Filter:** A search filter identifies the group member. The default value is “uniqueMember={0}”.
- Group Search Base:** A DN is used to limit the search range. If not specified, SSM will search the group from the base DN.
- Role: Administrator:** Groups of LDAP servers act as Administrators in SSM.
- Role: Operator:** Groups of LDAP servers act as Operators in SSM.
- Role: Limited Access:** Groups of LDAP servers are granted with Limited Access in SSM.



Note: Do not specify the primary group in the “Role: Administrator”, “Role: Operator” and “Role: Limited Access” fields. For example, a group named as “Domain Users” group is the primary group of users in the Active Directory. If you specify “Domain Users” in the Role fields, no roles can be assigned to the users of “Domain Users”.

- **Test Search Options** button is for a user to test a login account before submitting the settings. Follow these steps to check whether a user is able to log into SSM or not.
 - 1). Click **Test Search Options** and the Test Search Options dialog box appears.

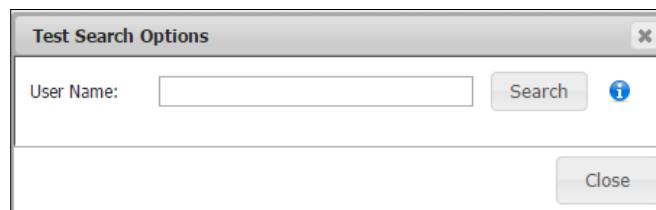
A screenshot of a dialog box titled "Test Search Options". It has a close button (X) in the top right corner. The main area contains a text input field labeled "User Name:" followed by a "Search" button and an information icon (i). Below this, there is a "Close" button.

Figure 6-89

- 2). Input the user name and then click **Search**.
- 3). SSM will check if the user is valid and will find the role permissions of the user. In this example (see the figure below), the account “tony” is found in the LDAP, and it belongs to Admin and SW groups of the LDAP. Meanwhile, the assigned roles for Ivy allow it to access SSM as an Administrator. (If multiple roles are assigned to a user, the user will have the highest privilege among the roles.)

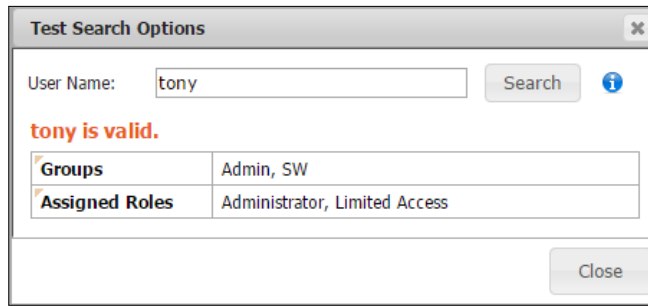


Figure 6-90

6.9 Software Update

6.9.1 Uploading a VNC Viewer

SSM Web supports remote control via VNC. To use this function, you need to install and setup a VNC Server on the host site and provide a VNC client to SSM Web so that you can use the VNC client to connect to a VNC server.

There are two ways of installing a VNC viewer.

To install a VNC viewer in the navigation area, click **Install VNC Viewer**. To install a VNC viewer in the working area, you can either upload a VNC viewer or directly install from the Internet.

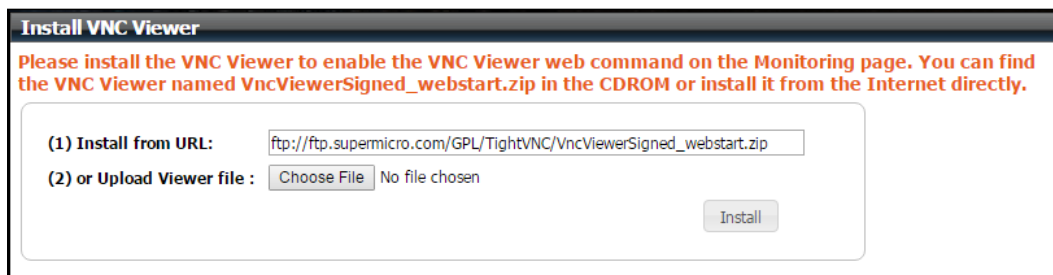


Figure 6-91

- **Install from URL**

Select this option and a GPL (GNU General Public License) 2.0 license agreement dialog box appears. Read the agreement carefully and click **I Agree** to continue installation if you accept the terms of the agreement.

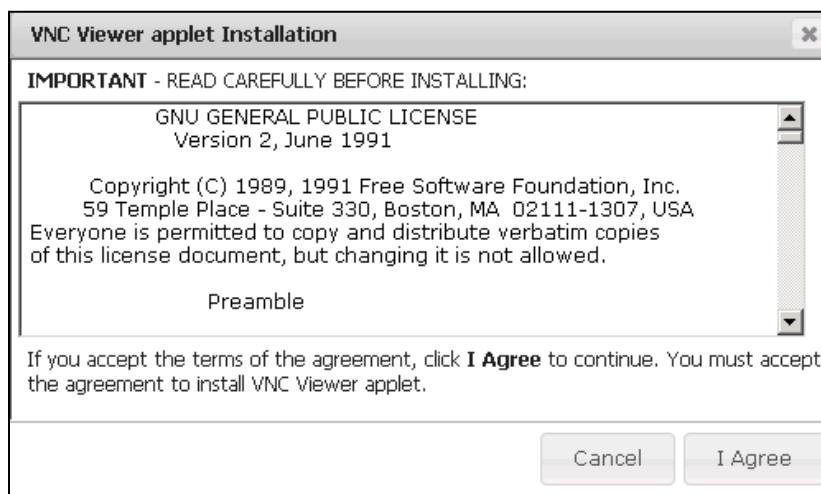


Figure 6-92

- **Upload VNC Viewer file**

You can find a VNC viewer named VncViewerSigned_webstart.zip on the Supermicro FTP site (<http://www.supermicro.com/wftp/GPL/TightVNC/>). After uploading, click the **Install** button to upload the VNC viewer to SSM Web.

6.9.2 Updating Site

The **Update Site** function allows users to setup a place to update a number of SD5s with the **Update SD5** web command. To use the **Update SD5** web command, you need to enable the **Update Site** first. Then, upload a SuperDoctor 5 update file to the SSM Web. Please contact Supermicro to get a SuperDoctor 5 update file.

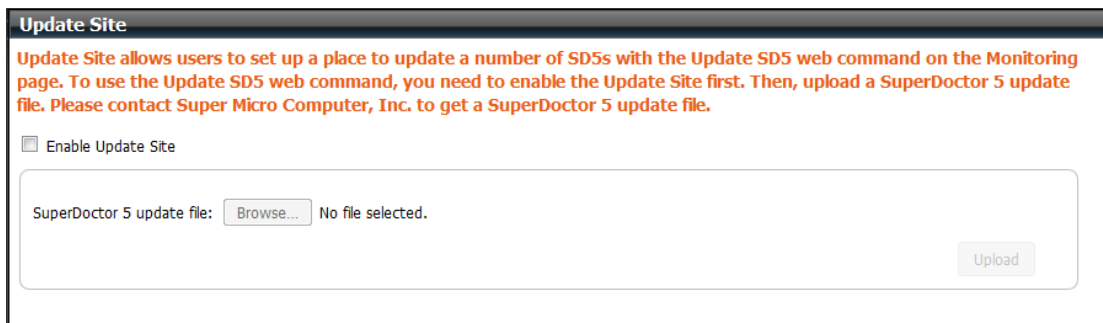


Figure 6-93

Click the **Upload** button to submit the update file. As shown below, if the update file is uploaded successfully, its file name and last upload date is shown on the Web page.

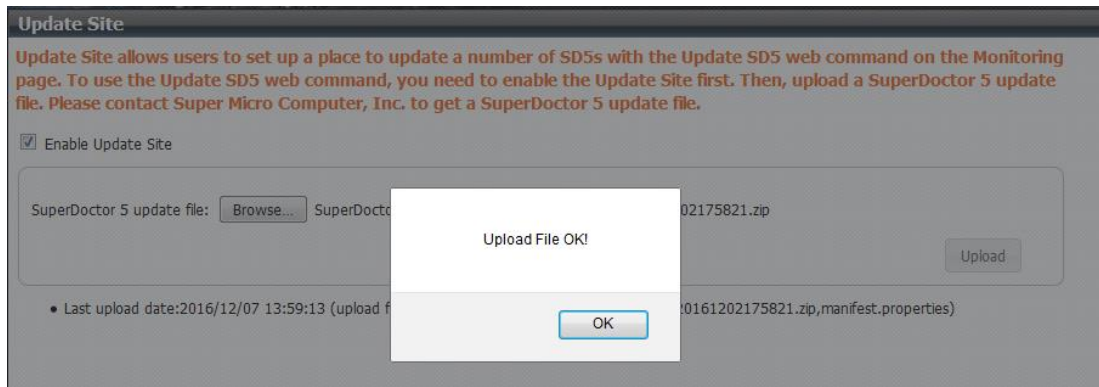


Figure 6-94

6.9.3 Updating SUM

The **Update SUM** function allows users to update the SUM package. Contact Supermicro to get a SUM update file before you begin.

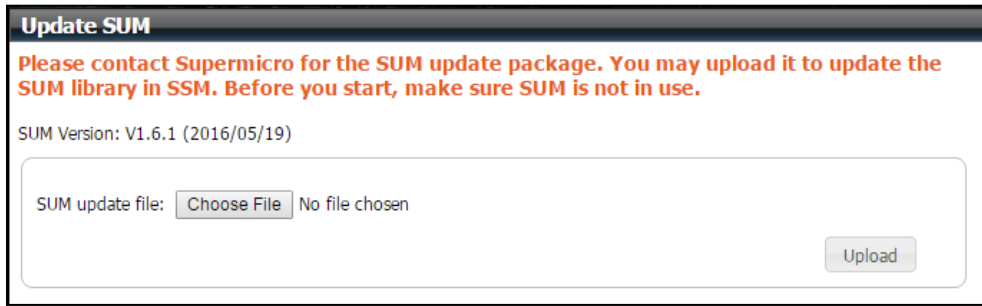


Figure 6-95

Click the **Upload** button to submit the update file. If the update file is uploaded successfully, both the SUM version and the last upload date are shown immediately (see the figure below).

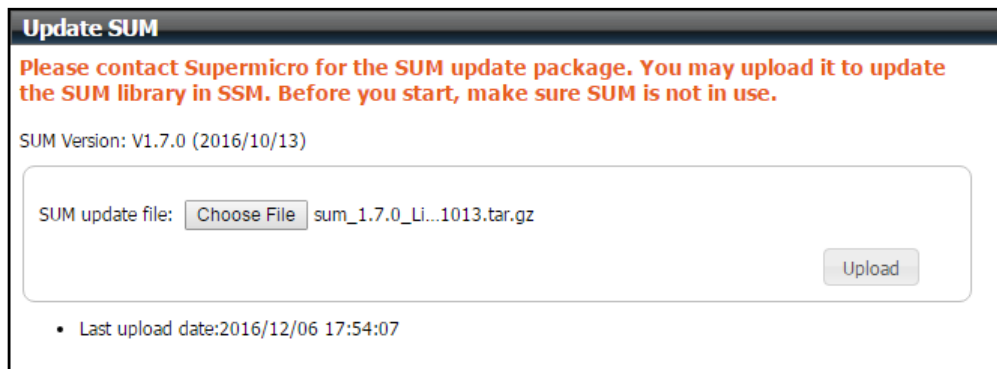
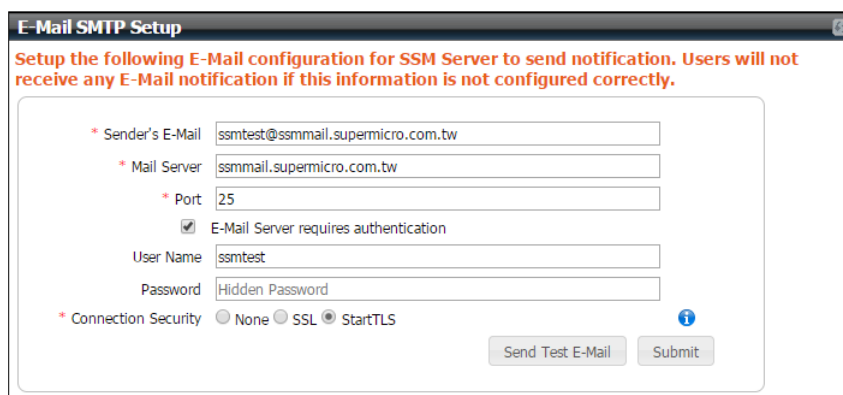


Figure 6-96

6.10 E-Mail SMTP Setup

The **E-Mail SMTP Setup** function allows users to modify the sender's e-mail, an SMTP mail server, an SMTP port, as well as a user name, the password and the connection security to access the SMTP server. These settings are used by SSM to send e-mail notifications. Note that both SSL and StartTLS provide a secure connection for TLS 1.2, TLS 1.1 and TLS 1.0. The latest TLS version supported by your SMTP server will be selected. For example, TLS 1.1 will be selected if your SMTP server supports both TLS 1.1 and TLS 1.0.



The screenshot shows a window titled "E-Mail SMTP Setup" with a warning message: "Setup the following E-Mail configuration for SSM Server to send notification. Users will not receive any E-Mail notification if this information is not configured correctly." The configuration fields are as follows:

- Sender's E-Mail:
- Mail Server:
- Port:
- E-Mail Server requires authentication
- User Name:
- Password:
- Connection Security: None SSL StartTLS

At the bottom right, there are two buttons: "Send Test E-Mail" and "Submit".

Figure 6-97

6.11 DB Maintenance

SSM has a database maintenance program that performs housekeeping jobs for the SSM Database daily. One of its primary jobs is to delete performance data from the SSM Database (see 7.3.8.7 *Performance Data Command* for more information). The SSM Database stores five types of performance data:

- Performance raw data for individual hosts
- Aggregated one-hour performance data for individual hosts
- Aggregated one-day performance data for individual hosts
- Performance raw data for host groups
- Aggregated one-hour performance data for host groups

The records of the five types of performance data, especially the raw data of hosts and host groups, can grow very fast if there are a number of performance-data-enabled services that are being monitored by the SSM Server. Holding a huge volume of performance data in the SSM Database will reduce the database performance. Thus, the database maintenance program removes out-of-date performance data to alleviate the performance impact.

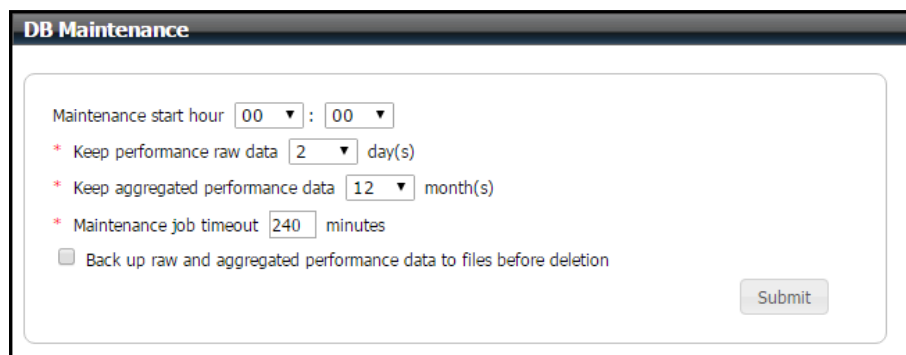


Figure 6-98

The **DB Maintenance** function allows users to setup arguments for the database maintenance program.

- **Maintenance start hour:** The time that the SSM Server executes the database maintenance program.
 - **Keep performance raw data:** This argument specifies how many days the performance raw data of hosts and host groups will be kept in the SSM Database.
 - **Keep aggregated performance data:** This argument specifies how many months the aggregated one-hour and one-day performance data of hosts and host groups will be kept in the SSM Database.
 - **Maintenance job timeout:** This argument specifies how many minutes the database maintenance program is allowed to be executed.
- **Backup raw and aggregated performance data to files before deleting:** If this argument is checked, the database maintenance program stores raw and aggregated performance data to files while it removes the out-of-date data from the SSM Database. The files are stored in the **[install folder]\share\dbmaintance** folder in the CSV (Comma Separated Values) format and can be processed by

other drawing tools. The following figure shows a service performance raw data file opened by Microsoft® Excel.

	A	B	C	D	E	F	G	H	I	J	K	L
1	SERVICE	INSTANC	SERVICE	SERVICE	CNAME	MEASURE	CURRENT	MIN_VAL	MAX_VAI	WARN_V	CRIT_VAI	UOM
2												
3	9031	1	158	1117	PS_Status	Fri Sep 16	0	-1	2	0	0	SWITCI
4	9030	1	158	1117	Chassis_Intru	Fri Sep 16	0	-1	2	0	0	SWITCI
5	9029	1	158	1117	P1-DIMM1A	Fri Sep 16	40	-5	65	0	0	degreeC
6	9028	1	158	1117	System_Temp	Fri Sep 16	36	-5	75	0	0	degreeC
7	9027	1	158	1117	VBAT	Fri Sep 16	3.192	2.928	3.648	0	0	Volts
8	9026	1	158	1117	+3.3VSB	Fri Sep 16	3.24	2.928	3.648	0	0	Volts
9	9025	1	158	1117	+3.3VCC	Fri Sep 16	3.312	2.928	3.648	0	0	Volts
10	9024	1	158	1117	CPU1_DIMM	Fri Sep 16	1.536	1.336	1.656	0	0	Volts
11	9023	1	158	1117	+12_V	Fri Sep 16	12.031	10.706	13.25	0	0	Volts
12	9022	1	158	1117	+5VSB	Fri Sep 16	5.056	4.48	5.536	0	0	Volts
13	9021	1	158	1117	+5_V	Fri Sep 16	5.056	4.48	5.536	0	0	Volts
14	9020	1	158	1117	+1.5_V	Fri Sep 16	1.528	1.336	1.656	0	0	Volts

Figure 6-99

6.12 Server Address

For a Supermicro server equipped with multiple network interfaces, it is required to configure a valid address for SSM to receive messages from the managed hosts.

Server Address

Set up a server address for SSM to receive messages from managed hosts. Either an IP address or a DNS name may be used.

* Server Address

Figure 6-100

6.13 System Events

Severity	Event Type	Message	Date	Target
INFO	SSM_SERVER_NOTIFICATION_PROBLEM_SENT	Notify contact 'admin'. Event : service has problem, message=SEL needs attention; 08/01/2017 06:54:34, WARNING, Critical Interrupt, Bus Correctable Error, Bus00(DevFn02) 08/01/2017 06:54:34, ERROR, Critical Interrupt, Bus Fatal Error, Bus00(DevFn00) 08/01/2017 06:54:33, CRITICAL, Critical Interrupt, Bus Uncorrectable Error, Bus03(DevFn00) 08/01/2017 06:54:32, WARNING, Critical Interrupt, PCI PERR, Bus00(DevFn00)	2017/08/01 14:56:59	10.146.125.134/PPM SEL Health
INFO	SSM_SERVER_NOTIFICATION_PROBLEM_SENT	Notify contact 'admin'. Event : service has problem, message=SEL needs attention; 08/01/2017 14:54:13, WARNING, Critical Interrupt, Bus Correctable Error, Bus00(DevFn02) 08/01/2017 14:54:13, ERROR, Critical Interrupt, Bus Fatal Error, Bus00(DevFn00) 08/01/2017 14:54:12, CRITICAL, Critical Interrupt, Bus Uncorrectable Error, Bus03(DevFn00) 08/01/2017 14:54:11, WARNING, Critical Interrupt, PCI PERR, Bus00(DevFn00)	2017/08/01 14:56:24	10.146.125.136/PPM SEL Health
INFO	SSM_SERVER_NOTIFICATION_PROBLEM_SENT	Notify contact 'admin'. Event : service has problem, message=SEL needs attention; 08/01/2017 14:54:58, WARNING, Critical Interrupt, Bus Correctable Error, Bus00(DevFn02) 08/01/2017 14:54:57, ERROR, Critical Interrupt, Bus Fatal Error, Bus00(DevFn00) 08/01/2017 14:54:56, CRITICAL, Critical Interrupt, Bus Uncorrectable Error, Bus03(DevFn00) 08/01/2017 14:54:55, WARNING, Critical Interrupt, PCI PERR, Bus00(DevFn00)	2017/08/01 14:56:22	10.146.125.137/PPM SEL Health
INFO	SSM_SERVER_NOTIFICATION_PROBLEM_SENT	Notify contact 'admin'. Event : service has problem, message=SEL needs attention; 08/01/2017 14:56:49, WARNING, Critical Interrupt, Bus Correctable Error, Bus00(DevFn02) 08/01/2017 14:56:48, ERROR, Critical Interrupt, Bus Fatal Error, Bus00(DevFn00) 08/01/2017 14:56:47, CRITICAL, Critical Interrupt, Bus Uncorrectable Error, Bus03(DevFn00) 08/01/2017 14:56:46, WARNING, Critical Interrupt, PCI PERR, Bus00(DevFn00)	2017/08/01 14:56:21	10.146.125.113/PPM SEL Health

Figure 6-101

The **System Events** function is designed to display SSM system events including events of the SSM Server, the SSM Web, the SSM CLI, etc. The **Event Type** field as shown above lists all event types. Currently, only a subset of events is supported:

- **SSM_SERVER_DB_MAINTENANCE_START**: An instance of this event is created when the SSM Server starts to execute the database maintenance program.
- **SSM_SERVER_DB_MAINTENANCE_STOP**: An instance of this is created when the SSM Server stops executing the database maintenance program.
- **SSM_SERVER_NOTIFICATION_PROBLEM_SENT**: An instance of this event is created when the SSM Server sends a problem alert to contacts and contact groups.
- **SSM_SERVER_NOTIFICATION_RECOVERY_SENT**: An instance of this event is created when the SSM Server sends a recovery alert to contacts and contact groups.
- **SSM_SERVER_POLICY_PROBLEM**: An instance of this event is created when power management policies of hosts or host groups are violated.
- **SSM_SERVER_POLICY_RECOVERY**: An instance of this event is created when violated power management policies become normal.

Events can be deleted and saved by clicking the **Delete** and **Save as** buttons, respectively. Note that the events will not be deleted by the database maintenance program and need to be manually deleted.

6.14 About SSM

This function shows the version number of the SSM installer, the SSM Web information, the database information, and the license information. The SSM Web information includes its version number and the server time. The database information includes the URL used to connect the SSM database and the SSM Database schema revision number as well as creation date. The license information includes the SSM edition, the number of monitored and managed nodes, and the expiration date.



Figure 6-102

6.15 Host Discovery Wizard

1. On the Administration page, click **Host Discovery Wizard**.

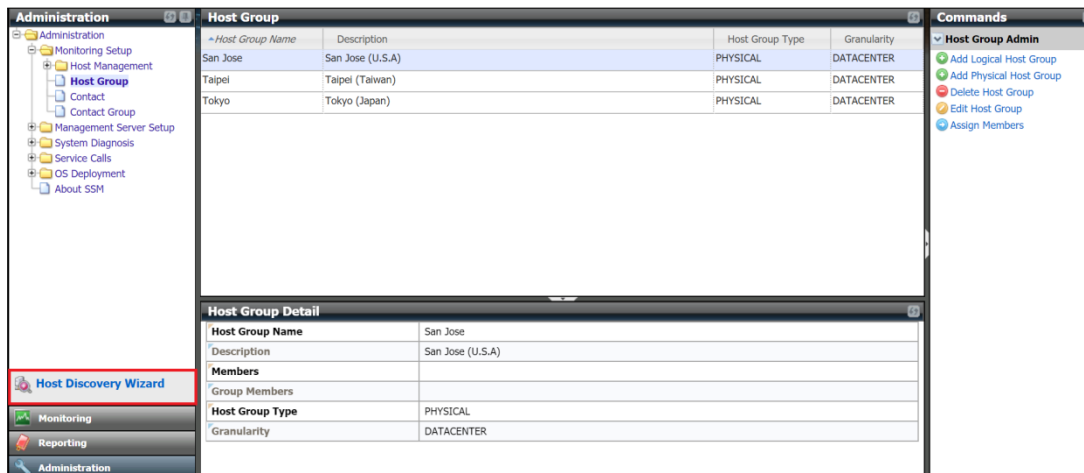


Figure 6-103

2. In the Discovery Type step of the Host Discovery Wizard, select the **Agent managed** option and click the **Next** button.

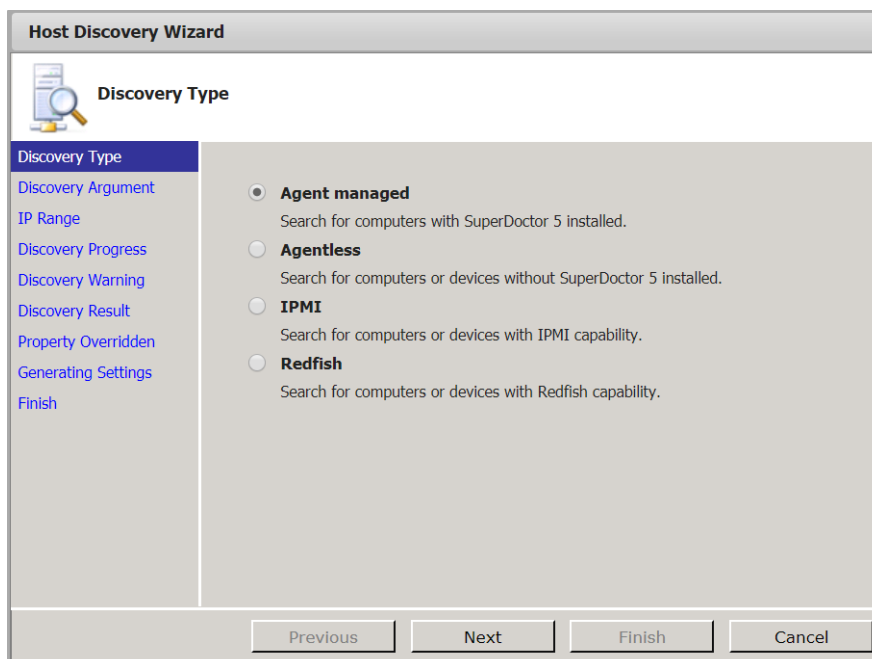


Figure 6-104

3. In the Discovery Argument step you can set the SuperDoctor 5 Port number and BMC ID (note that only accounts with the Administrator privileges can perform all IPMI commands) as well as the password. Click the **Next** button to continue.

Host Discovery Wizard (Agent Managed)

Discovery Argument

Discovery Type

Discovery Argument

IP Range

Discovery Progress

Discovery Warning

Discovery Result

Property Overridden

Generating Settings

Finish

Please enter the SuperDoctor 5 port number (default value is 5999). If your agent-managed computers are equipped with IPMI, you can explore the IPMI functions by clicking the Detect IPMI check box and entering BMC ID and password.

SuperDoctor 5 Port: 5999

BMC ID: ADMIN

BMC Password: [Empty]

Detect IPMI

Detect NM

Use DNS name to manage hosts

Previous Next Finish Cancel

Figure 6-105

If your hosts support Intel® Intelligent Power Node Manager (NM) and you want to use the power management functions provided by SSM, please click the **Detect NM** checkbox.

Host Discovery Wizard (Agent Managed)

Discovery Argument

Discovery Type

Discovery Argument

IP Range

Discovery Progress

Discovery Warning

Discovery Result

Property Overridden

Generating Settings

Finish

Please enter the SuperDoctor 5 port number (default value is 5999). If your agent-managed computers are equipped with IPMI, you can explore the IPMI functions by clicking the Detect IPMI check box and entering BMC ID and password.

SuperDoctor 5 Port: 5999

BMC ID: ADMIN

BMC Password: [Empty]

Detect IPMI

Detect NM

Clear existing policies for a new managed entity

Use DNS name to manage hosts

Previous Next Finish Cancel

Figure 6-106

If the **Clear existing policies for a new managed entity** checkbox is checked, the Host Discovery Wizard will clear all existing policies on an NM of the discovered hosts. Doing so makes sure that the NM is occupied by SSM and will not be affected by policies that were previously added by other power management software. Note that clearing all policies on a NM takes time. As a result, the entire discovery process takes longer if this checkbox is checked. You can uncheck this option to reduce the host discovery time if you are sure that SSM is the only power management software managing your NMs. See *9 Power Management* for more information about power management in SSM. Also, if the **Use DNS name to manage hosts** checkbox is clicked, the Host Discovery Wizard will allow the domain name to take precedence over the IP address to manage the host. Click the check box if your network environment uses DHCP.

4. In the IP range step you can input an IP address, an IP range (e.g., 192.168.12.10 to 192.168.12.80), a class C range (e.g., 192.168.12.*), or DNS names to discover hosts. Click the **Next** button to start the discovery process.

The screenshot shows the 'Host Discovery Wizard (Agent Managed)' window. The title bar reads 'Host Discovery Wizard (Agent Managed)'. Below the title bar is a magnifying glass icon and the text 'IP Range'. On the left side, there is a vertical navigation pane with the following items: 'Discovery Type', 'Discovery Argument', 'IP Range' (highlighted in blue), 'Discovery Progress', 'Discovery Warning', 'Discovery Result', 'Property Overridden', 'Generating Settings', and 'Finish'. The main area of the wizard contains the text 'Please enter an IP or an IP range to find hosts.' followed by a horizontal line. Below this line are four radio buttons: 'IP Range' (selected), 'Single IP', 'Class C Range', and 'DNS Name'. Underneath the radio buttons are two rows of input fields. The first row is labeled 'From:' and the second row is labeled 'To:'. Each row contains four input boxes separated by dots, representing the octets of an IP address. At the bottom of the wizard, there are four buttons: 'Previous', 'Next', 'Finish', and 'Cancel'.

Figure 6-107

- Please wait while the Discovery Wizard searches.

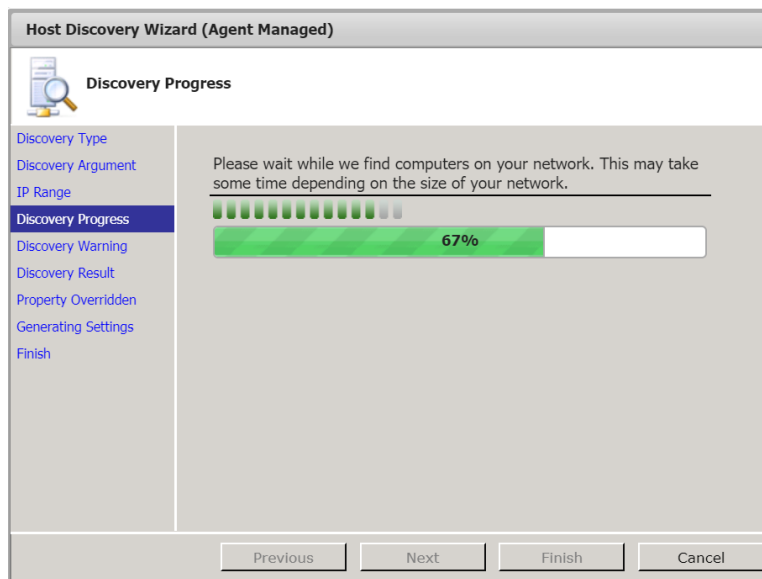


Figure 6-108

- The currently unavailable hosts are then listed.

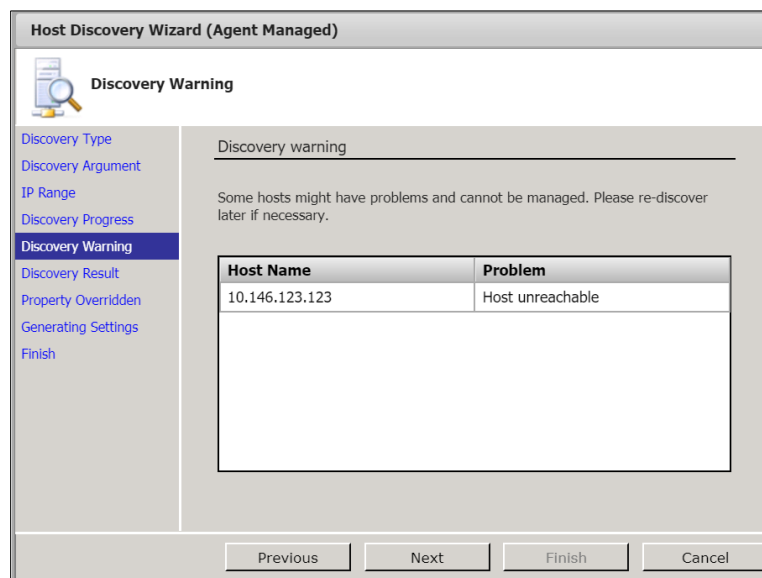


Figure 6-109

- Select the hosts to be monitored by SSM. Note that if an agent-managed host supports IPMI, the IPMI IP address is shown in the IPMI column. Otherwise, "None" is shown in the IPMI column. If a host with an IPMI IP address supports the Node Product Key and the Node Product Key is activated, "Yes" is shown in the Node PK column. Otherwise, "No" is shown. If a host with an IPMI IP address

does not support the Node Product Key, “None” is shown in the Node PK column. The green icon in the Valid BMC field indicates that the BMC ID and password are valid.

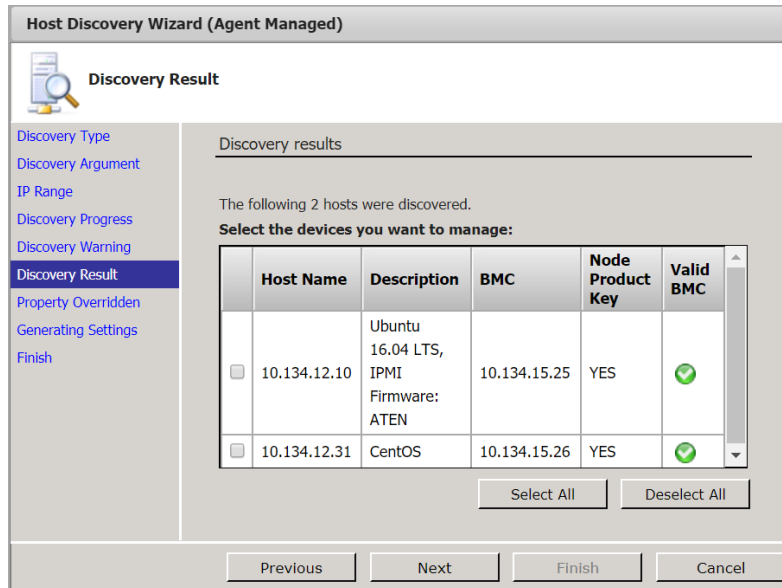


Figure 6-110

- In the Property Overridden step you can set the “Check Interval”, “Retry Interval” and “Max Check Attempts” arguments.

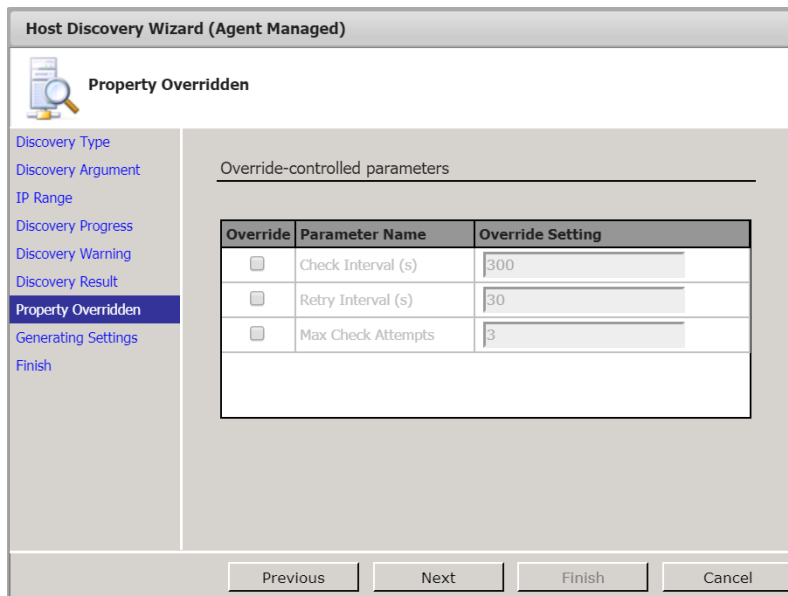


Figure 6-111

If NM enabled hosts are discovered, three more arguments, “Derated DC Power”, “Derated AC Power”, and “Max PS Output” are available to override.

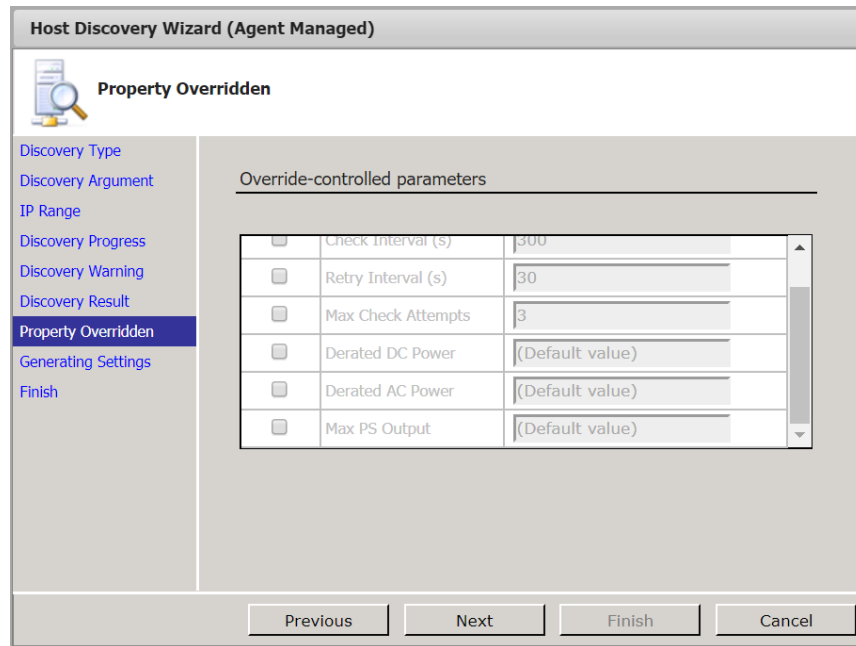


Figure 6-112

- Please wait while SSM generates the settings.

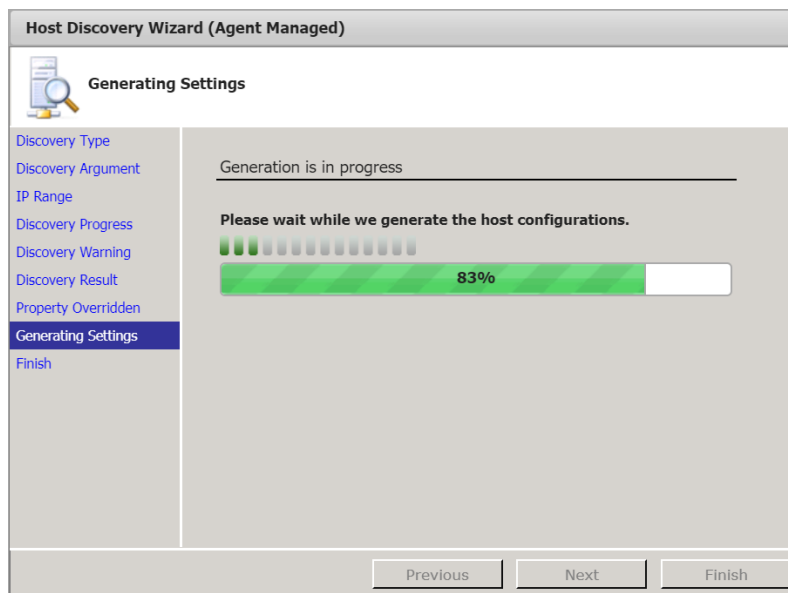


Figure 6-113

- When the Host Discovery Wizard is complete, click the **Finish** button to close the wizard.

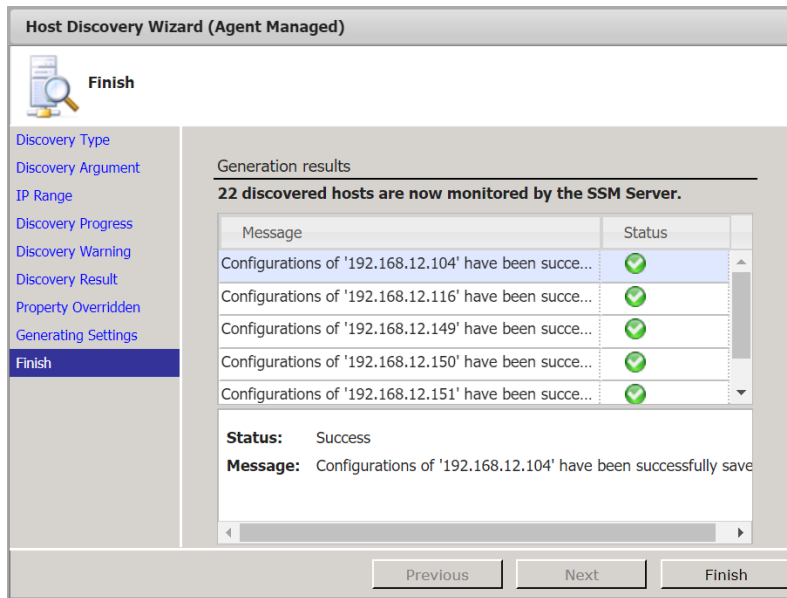


Figure 6-114



Note: You can follow similar steps to add agentless, IPMI, and Redfish hosts.

7 SSM Web Monitoring Page

The monitoring page displays the status of the hosts and services managed by SSM. Users can also issue commands to perform functions such as power control, remote control, and reporting on this page.

7.1 Navigation Area

A typical monitoring page is shown below. The navigation area located on the left side of the page shows a tree structure of the host groups. Each node represents a host group, which contains a **host view** and a **service view**. A host view contains all hosts belonging to the host group while a service view contains all services belonging to all hosts in the host group. When you click the host or service view, its content is shown in the working area.

The root node of the tree is a special node that shows an SSM overview page, which includes the number of monitored hosts and services as well as the top five types of motherboards and operating systems. Except for the root node, there are two built-in nodes in the tree: the **All** node and the **Undefined Group** nodes. The former comprises all hosts monitored by SSM and the latter includes all hosts not belonging to any host groups.

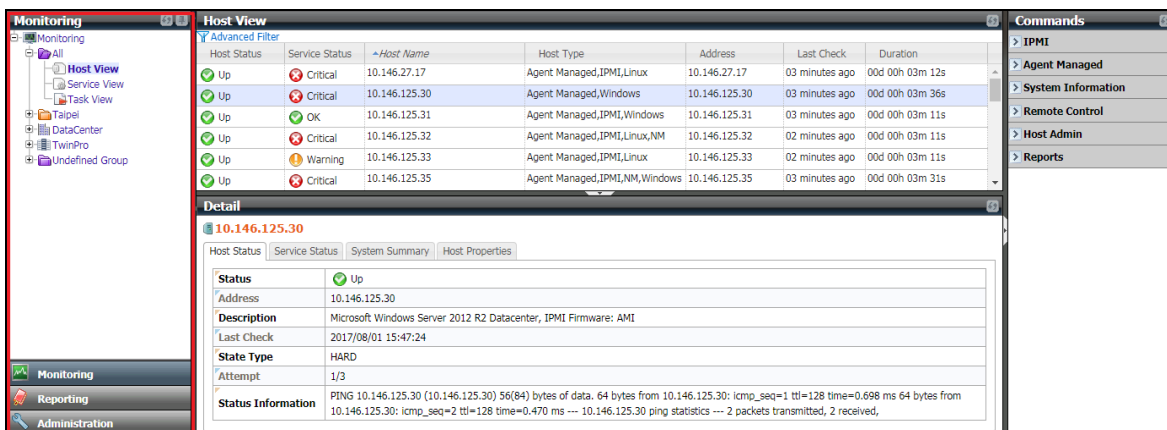


Figure 7-1

7.2 Working Area

The working area is located at the center of the monitoring page. Depending on the tree node selected, the working area shows one of the following four views:

7.2.1 Monitoring Overview

As shown below, selecting the **Monitoring** node on the navigation area displays a monitoring overview page in the working area. Clicking the **Host Status** link and the **Service Status** link can change the working area to the host view and the service view of the **All** group respectively.

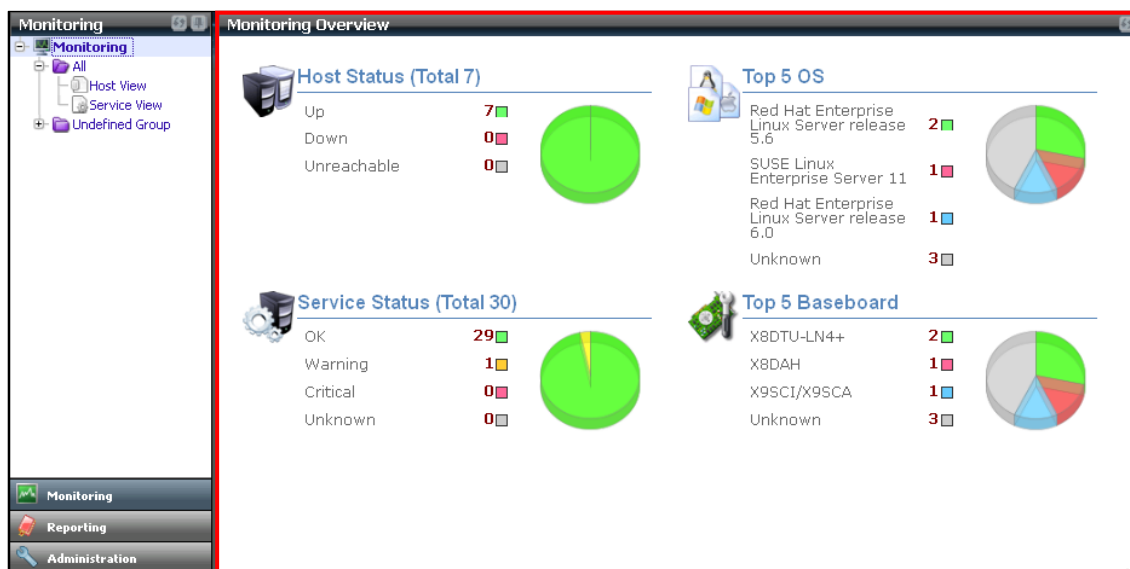


Figure 7-2

7.2.2 Host View

Selecting a Host View on the navigation area displays the content of the Host View in the working area. Clicking the **Host Status** link and the **Service Status** link can change the working area to the host view and the service view of the **All** group, respectively.

The working area is further divided into a host view and a detailed view.

- **Host View:** This table contains all hosts in the host group. The contents of the host table are:

Host Status:	This shows the current status of a host. Valid values are Up, Down, and Unreachable. If the host can be reached, this column shows Up or Down depends on the host whether is running. Otherwise, the column shows Unreachable that means the path from the server to the host is blocked, and the server can't know the host is running or offline. The states can help you quickly determine the root cause of network problems.
Service Status:	This displays the combined service status. If all services belonging to the host are OK, this column shows an OK state. Otherwise, it could be Warning, Unknown or Critical depends on the states of the services.
Host Name:	The name of the host is displayed here.
Host Type:	This displays the type of the host as identified by the Host Discovery Wizard. Valid values include Agent Managed, Agentless, IPMI, Redfish, NM, Linux, and Windows.
Address:	Host IP address or DNS name.
Last Check:	This displays the last check time.
Duration:	The total time the current host state has lasted is shown here.

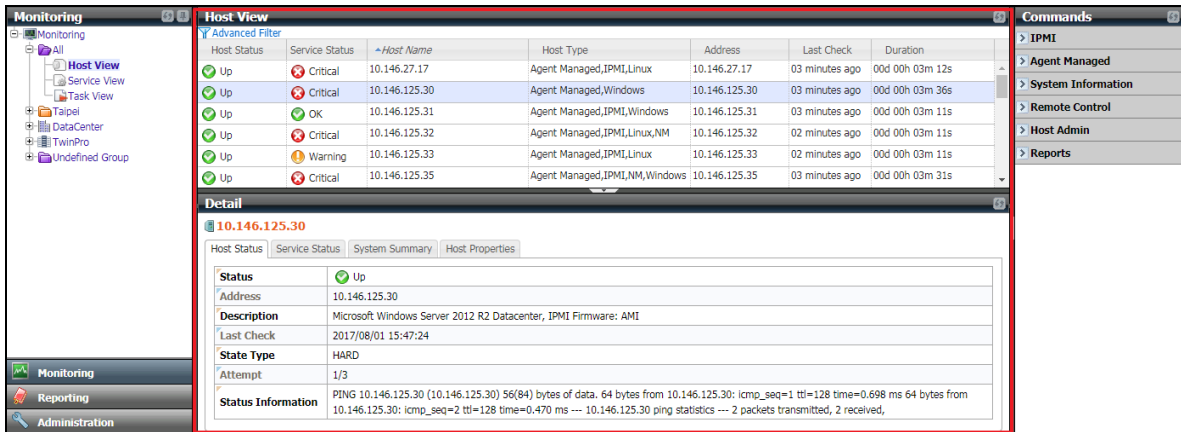


Figure 7-3

- **Detailed View:** This is a tab component that shows detailed information related to the host.

7.2.3 Service View

As shown below, selecting **Service View** on the navigation area displays the content of the Service View in the working area. A Service View is similar to a Host View except that the subjects monitored are services instead of hosts.

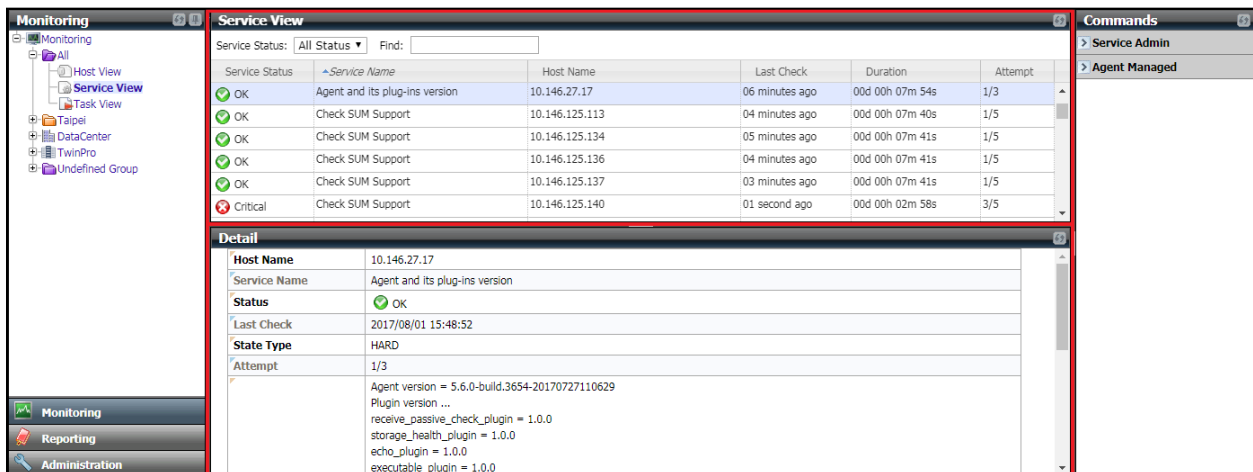


Figure 7-4

7.2.4 ACK Events

By acknowledging the current events on **IPMI/Redfish SEL Health** services, users can focus on major problems without being distracted by the minor ones. The acknowledged events will be stored and could be included in decision making at next service check. If the IPMI/Redfish SEL Health service is caused by one acknowledged event to be in a non-OK state, the state of the service will change to be OK. At the same time, the contacts are notified by a recovery alert accordingly. Clicking the **ACK Events** link

under the Service View group in the navigation area displays an acknowledgement page in the working area. The ACK Events view shows all non-OK SEL items from IPMI/Redfish SEL Health services. You can mark the selected events to be acknowledged or clear acknowledgements in this view.

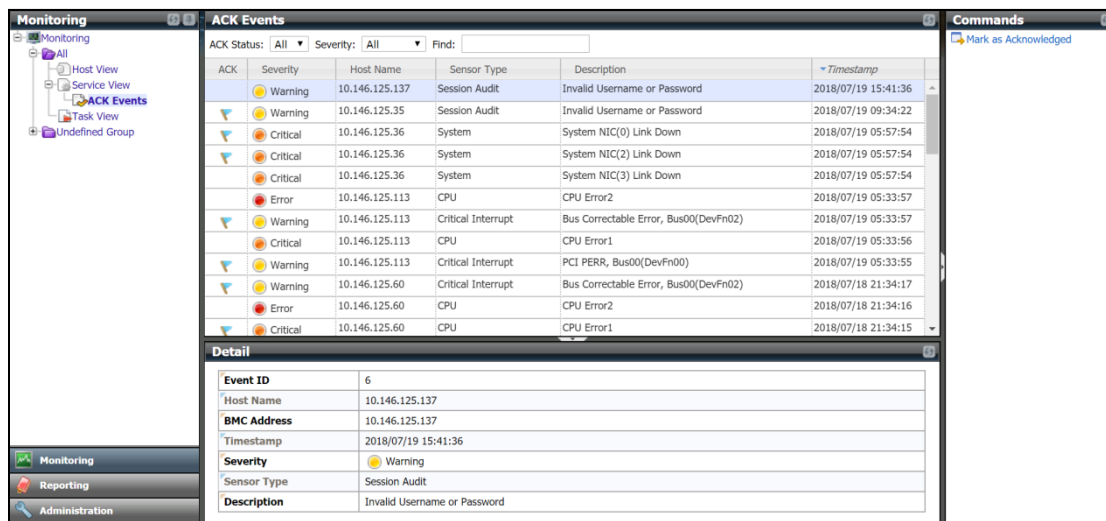


Figure 7-5




Notes:

- The events in this view result from the periodical checks of IPMI/Redfish SEL Health services by SSM, thus the real-time SEL items on BMC may not be the same. You can manually refresh the view if necessary.
- The acknowledged events should be set manually by users. By default, all SEL items on this view are not marked as acknowledged events.
- The combination of the Event ID and Timestamp is used to identify a unique SEL item. That is, if you acknowledge one SEL item of “Correctable ECC@DIMMA1(CPU1)” when another event “Correctable ECC@DIMMA1(CPU1)” shows, the second one will be regarded as a new event.

The working area is further divided into ACK Events and Detailed View.

- **ACK Events:** This table contains all non-OK SEL items from **IPMI/Redfish SEL Health** services. Here is the content of an SEL item:

ACK: Shows the current acknowledgement status of an SEL item. The  icon is shown to indicate the item has been acknowledged.

Severity: Shows the severity ( Error,  Critical and  Warning) of an SEL

item. The severity is defined by BMC SEL by default.

Host Name: The name of the host is displayed here.

Sensor Type: Shows the sensor type of an SEL item.

Description: Shows the description of an SEL item.

Timestamp: Shows the timestamp of an SEL item.

- **Detailed View:** This tab component shows the detailed information of the SEL item.

Event ID: Shows the unique ID to identify the SEL item.

BMC Address: BMC IP address or DNS name.

7.2.4.1 *Mark as Acknowledged Command*

[Scenario]

As shown below, some non-OK SEL items are found during the IPMI/Redfish SEL Health service check. Now, two items haven't been confirmed: one event type is "CPU Error2" (the severity is "ERROR") and the other is "CPU Error1" (the severity is "CRITICAL"). To highlight the remaining items that require more attention, we can mark the item "CPU Error2" and "CPU Error1" as the acknowledged events.

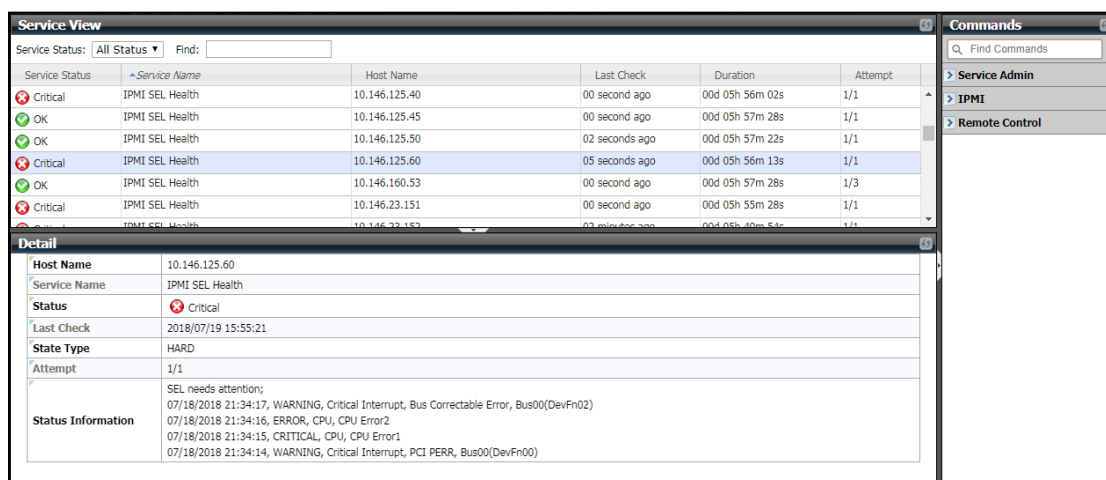


Figure 7-6

1. Click **ACK Events** in the navigation area to see all SEL items in the top right window. Select "CPU Error2" and "CPU Error1" in the working area. You can acknowledge multiple SEL items simultaneously.

ACK Events						Commands
ACK Status: All Severity: All Find: 10.146.125.60						Mark as Acknowledged
ACK	Severity	Host Name	Sensor Type	Description	Timestamp	
	Warning	10.146.125.60	Critical Interrupt	PCI PERR, Bus00(DevFn00)	2018/07/18 21:34:14	
	Critical	10.146.125.60	CPU	CPU Error1	2018/07/18 21:34:15	
	Error	10.146.125.60	CPU	CPU Error2	2018/07/18 21:34:16	
	Warning	10.146.125.60	Critical Interrupt	Bus Correctable Error, Bus00(DevFn02)	2018/07/18 21:34:17	

Figure 7-7

- Click **Mark as Acknowledged** in the command area and a Mark as Acknowledged dialog box appears.


Mark as Acknowledged						
<input checked="" type="checkbox"/>	Host Name	Severity	Sensor Type	Description	Status	
<input checked="" type="checkbox"/>	10.146.125.60	CRITICAL	CPU	CPU Error1		
<input checked="" type="checkbox"/>	10.146.125.60	ERROR	CPU	CPU Error2		
<div style="text-align: right;"> <input type="button" value="Run"/> <input type="button" value="Close"/> </div>						

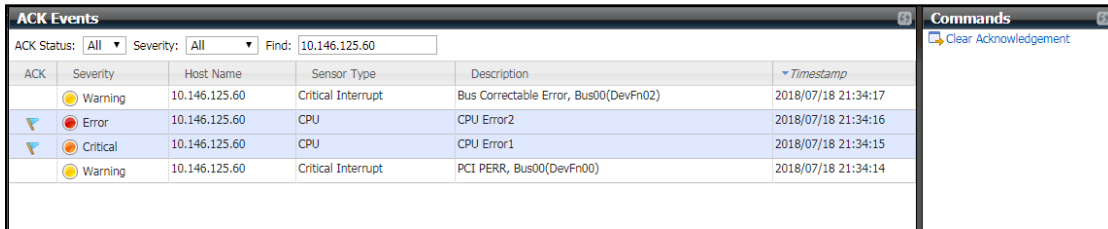
Figure 7-8

- Click the **Run** button to acknowledge the selected SEL items or the **Close** button to abort and close this dialog box. After the **Mark as Acknowledged** command is executed, click the **Close** button and return to the ACK Events page.

Mark as Acknowledged						
<input checked="" type="checkbox"/>	Host Name	Severity	Sensor Type	Description	Status	
<input type="checkbox"/>	10.146.125.60	CRITICAL	CPU	CPU Error1		✓
<input type="checkbox"/>	10.146.125.60	ERROR	CPU	CPU Error2		✓
<p>Status: Success</p> <p>Message: Mark the log as acknowledged event successfully.</p> <div style="text-align: right;"> <input type="button" value="Run"/> <input type="button" value="Close"/> </div>						

Figure 7-9

- In ACK Events master view, the  icons appear **before** the items “CPU Error2” and “CPU Error1” in the ACK column.





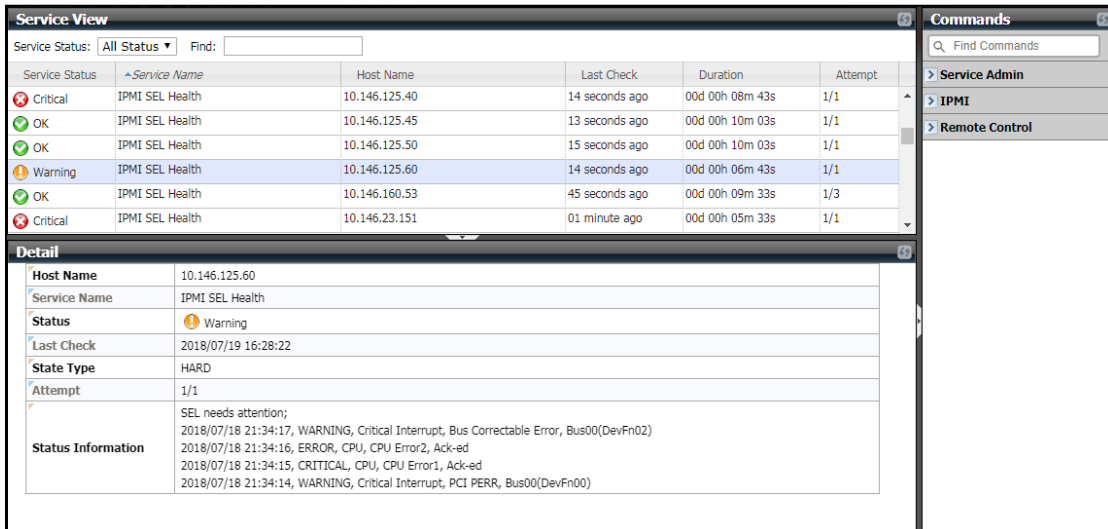






ACK	Severity	Host Name	Sensor Type	Description	Timestamp
	Warning	10.146.125.60	Critical Interrupt	Bus Correctable Error, Bus00(DevFn02)	2018/07/18 21:34:17
	Error	10.146.125.60	CPU	CPU Error2	2018/07/18 21:34:16
	Critical	10.146.125.60	CPU	CPU Error1	2018/07/18 21:34:15
	Warning	10.146.125.60	Critical Interrupt	PCI PERR, Bus00(DevFn00)	2018/07/18 21:34:14

Figure 7-10

- Return to the Service View and select the IPMI SEL Health service for host “10.146.125.60.” Wait until the next service check is performed, both items “CPU Error2” and “CPU Error1” have “Ack-ed” as the suffix. Meanwhile, the IPMI SEL Health service now changes from a Critical state to a Warning state.



Service Status	Service Name	Host Name	Last Check	Duration	Attempt
	IPMI SEL Health	10.146.125.40	14 seconds ago	00d 00h 08m 43s	1/1
	IPMI SEL Health	10.146.125.45	13 seconds ago	00d 00h 10m 03s	1/1
	IPMI SEL Health	10.146.125.50	15 seconds ago	00d 00h 10m 03s	1/1
	IPMI SEL Health	10.146.125.60	14 seconds ago	00d 00h 06m 43s	1/1
	IPMI SEL Health	10.146.160.53	45 seconds ago	00d 00h 09m 33s	1/3
	IPMI SEL Health	10.146.23.151	01 minute ago	00d 00h 05m 33s	1/1


Detail	
Host Name	10.146.125.60
Service Name	IPMI SEL Health
Status	 Warning
Last Check	2018/07/19 16:28:22
State Type	HARD
Attempt	1/1
Status Information	SEL needs attention; 2018/07/18 21:34:17, WARNING, Critical Interrupt, Bus Correctable Error, Bus00(DevFn02) 2018/07/18 21:34:16, ERROR, CPU, CPU Error2, Ack-ed 2018/07/18 21:34:15, CRITICAL, CPU, CPU Error1, Ack-ed 2018/07/18 21:34:14, WARNING, Critical Interrupt, PCI PERR, Bus00(DevFn00)

Figure 7-11

7.2.4.2 Clear an Acknowledgement Command

[Scenario]

As shown below, both SEL items “CPU Error2” and “CPU Error1” are marked as the acknowledged events.

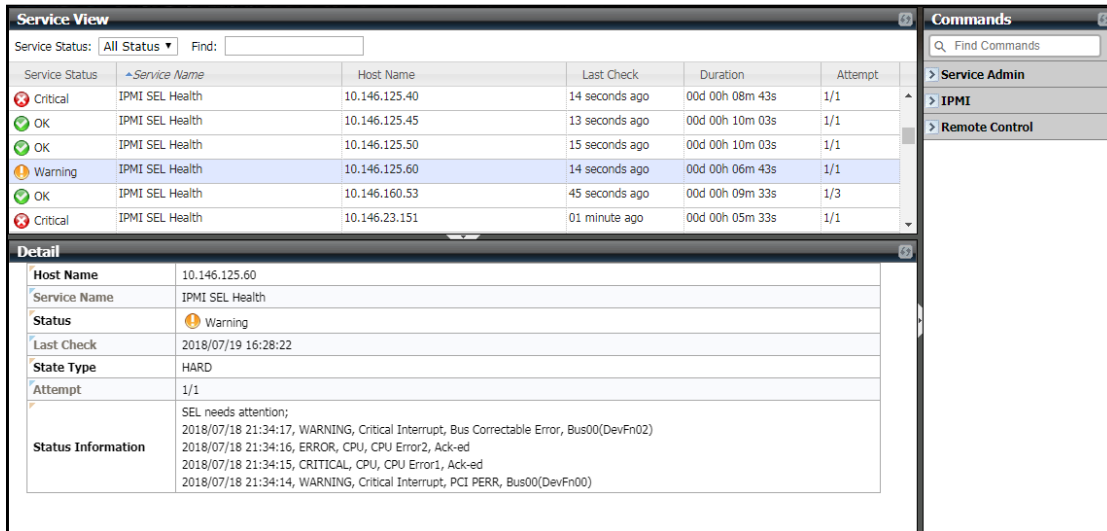


Figure 7-12

1. To clear acknowledgements, click **ACK Events** in the navigation area to see all SEL items in the top right window. Find and select the items “CPU Error2” and “CPU Error1” in the working area. You can remove acknowledgements from multiple SEL items simultaneously.

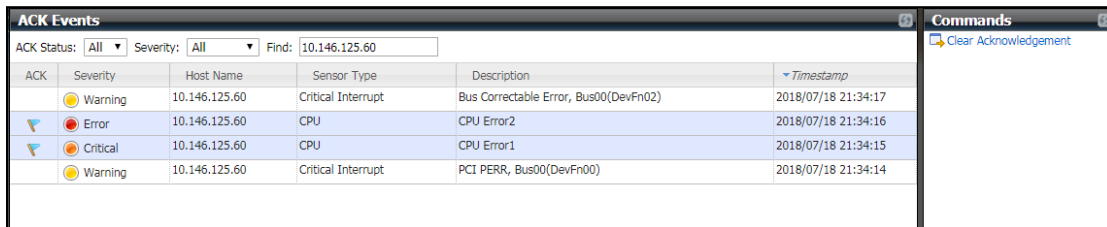


Figure 7-13

2. Click **Clear Acknowledgement** in the command area and a Clear Acknowledgement dialog box appears.

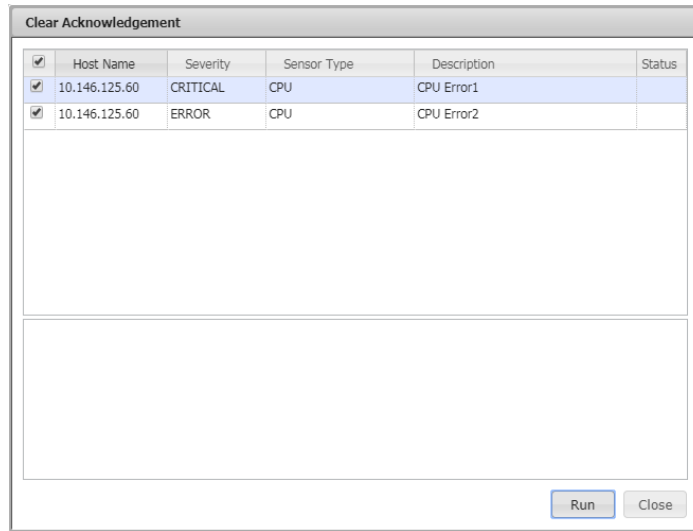


Figure 7-14

- Click the **Run** button to clear acknowledgements of the selected SEL items or the **Close** button to abort and close this dialog box. After the **Clear Acknowledgement** command is executed, click **Close** button and return to the ACK Events page.

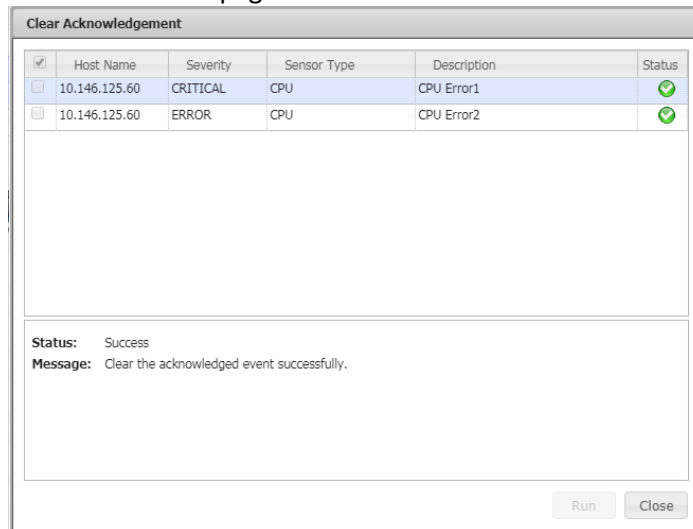


Figure 7-15

- In the ACK Events master view, the 🚩 icons before both items “CPU Error2” and “CPU Error1” in the **ACK** column disappear.

ACK Events					
ACK Status:	All	Severity:	All	Find:	10.146.125.60
ACK	Severity	Host Name	Sensor Type	Description	Timestamp
	Warning	10.146.125.60	Critical Interrupt	Bus Correctable Error, Bus00(DevFn02)	2018/07/18 21:34:17
	Error	10.146.125.60	CPU	CPU Error2	2018/07/18 21:34:16
	Critical	10.146.125.60	CPU	CPU Error1	2018/07/18 21:34:15
	Warning	10.146.125.60	Critical Interrupt	PCI PERR, Bus00(DevFn00)	2018/07/18 21:34:14

Figure 7-16

- Return to the Service View and select the IPMI SEL Health service for host “10.146.125.60.” Wait until the next service check is performed, the “Ack-ed” suffixes in both items “CPU Error2” and “CPU Error1” have disappeared. The IPMI SEL Health service now changes from a Warning state to a Critical state.

Service View					
Service Status:	All Status	Find:			
Service Status	Service Name	Host Name	Last Check	Duration	Attempt
Critical	IPMI SEL Health	10.146.125.40	12 seconds ago	00d 00h 42m 51s	1/1
OK	IPMI SEL Health	10.146.125.45	00 second ago	00d 00h 44m 16s	1/1
OK	IPMI SEL Health	10.146.125.50	12 seconds ago	00d 00h 44m 11s	1/1
Critical	IPMI SEL Health	10.146.125.60	12 seconds ago	00d 00h 02m 53s	1/1
OK	IPMI SEL Health	10.146.160.53	43 seconds ago	00d 00h 44m 11s	1/3
Critical	IPMI SEL Health	10.146.23.151	01 minute ago	00d 00h 40m 35s	1/1

Detail	
Host Name	10.146.125.60
Service Name	IPMI SEL Health
Status	Critical
Last Check	2018/07/19 17:02:22
State Type	HARD
Attempt	1/1
Status Information	SEL needs attention; 2018/07/18 21:34:17, WARNING, Critical Interrupt, Bus Correctable Error, Bus00(DevFn02) 2018/07/18 21:34:16, ERROR, CPU, CPU Error2 2018/07/18 21:34:15, CRITICAL, CPU, CPU Error1 2018/07/18 21:34:14, WARNING, Critical Interrupt, PCI PERR, Bus00(DevFn00)

Figure 7-17

7.2.5 Task View

A Task View is similar to a Host View except that the subjects are task-generated after web commands are issued.

The working area is further divided into Task View and Detailed View.

- Task View:** This table contains all tasks. Here is the list of tasks:

Task Status: Shows the current status of a task. The status values include RUNNING (the task has not completed), FAILED (the task has not completed successfully), FINISHED (the task has completed successfully) and PENDING (the task has been accepted but not yet

- processed).
- Task ID:** Shows the unique key to identify the Task.
- Task Name:** The asynchronous task represents a web command to managed hosts. Total number of selected hosts will be shown onscreen as well.
- Start Time:** Shows the start time of running the Task.
- Duration:** Shows the total time of running a Task.
- Host Name:** Displays the name of the host.
- Address:** Shows the IP address or DNS name of the host.
- Task Progress:** Shows the progress of the task. SSM will periodically automatically refresh the progress to reflect current status. Note that each web command has its progress representation.

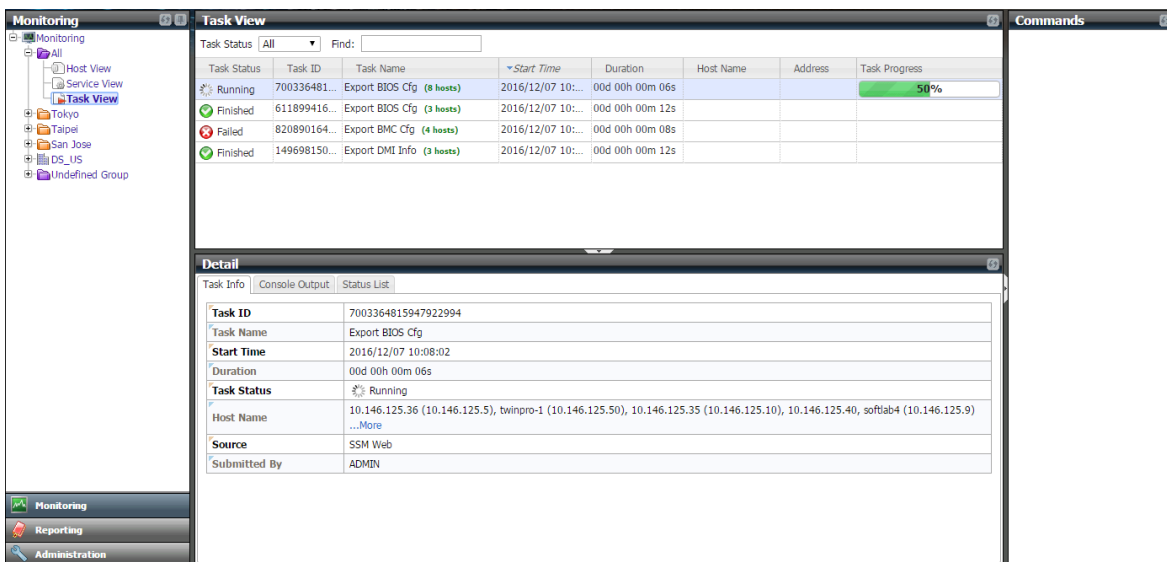


Figure 7-18

- Detailed View:** This tab component shows the detailed information of the task.
 - Task Info:** Includes information such as start time, duration and arguments.
 - Console Output:** Shows the task execution message.
 - Status List:** Shows the execution status and artifact link for each host. This tab is

available only when each host has its exit code returned on the Console Output tab.



Note: The tasks will be kept for only 30 minutes.

7.2.6 Host Group View

Selecting a Host Group view on the navigation area displays a Host Group Overview page in the working area. If the selected host group contains NM hosts, you can use the **Power Consumption Trend** command to display a host group power consumption trend graph and use the **Power Policy Management** command to add, delete and update power capping policies for the host group (see 9.2.2 *Power Consumption Trend of a Group of Hosts* and 9.3.2 *Host Group Policies* for more information).

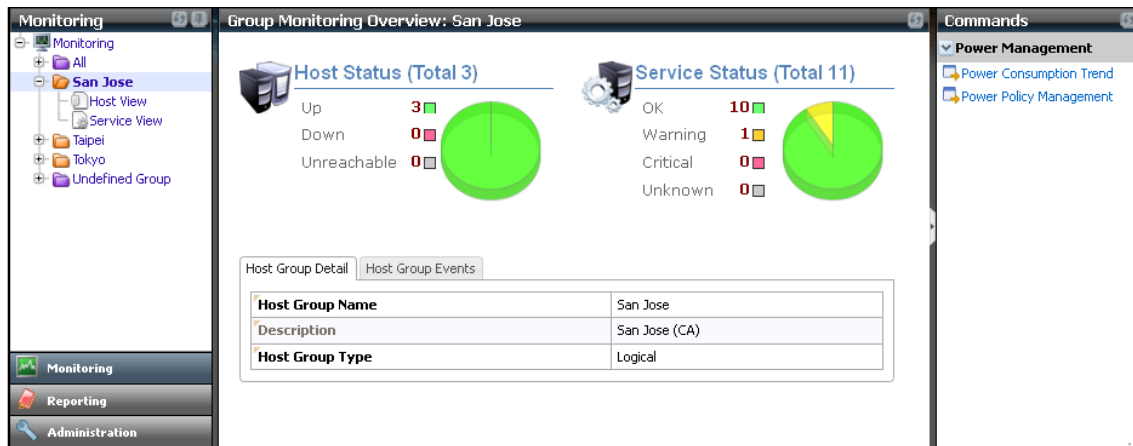


Figure 7-19

7.3 Command Area

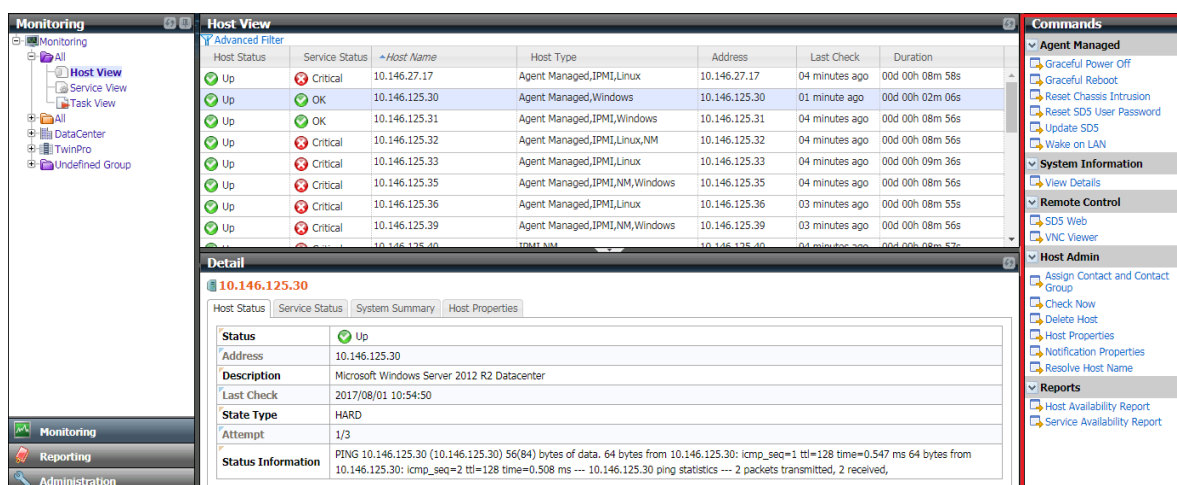


Figure 7-20

The Command Area as shown above displays a number of commands that can be used to perform management and control functions. Commands in this area are grouped by categories such as **Agent Managed**, **IPMI**, **System Information**, **Remote Control**, **Host Admin**, **Power Management** and **Reports**. A category will be displayed only if the applicable hosts are selected in the working area. For example, the IPMI category is not shown in the command area if a non-IPMI host is selected. For another example, the Agent Managed category is visible only if an agent-managed host is selected.

7.3.1 Agent Managed Commands

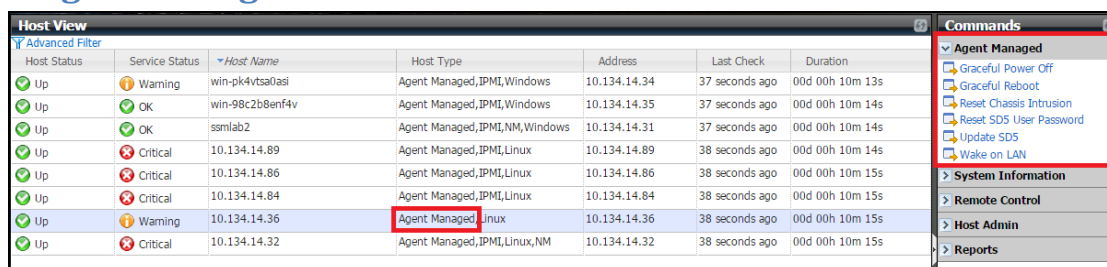


Figure 7-21

Commands in this category apply only to Agent Managed hosts. Six commands are included:

- **Graceful Power Off:** Powers off a host gracefully.
- **Graceful Reboot:** Reboots a host gracefully.
- **Reset Chassis Intrusion:** Resets a chassis intrusion flag.
- **Reset SD5 User Password:** Resets the user account and password on a host.
- **Update SD5:** Updates a SuperDoctor 5.
- **Wake-on-LAN:** Sends Wake-on-LAN magic packets to a host.

The command related to service will also appear in the Service View. For example, the command “Update SD5” will appear in the command area when a user clicks **Agent and its plug-ins version**.

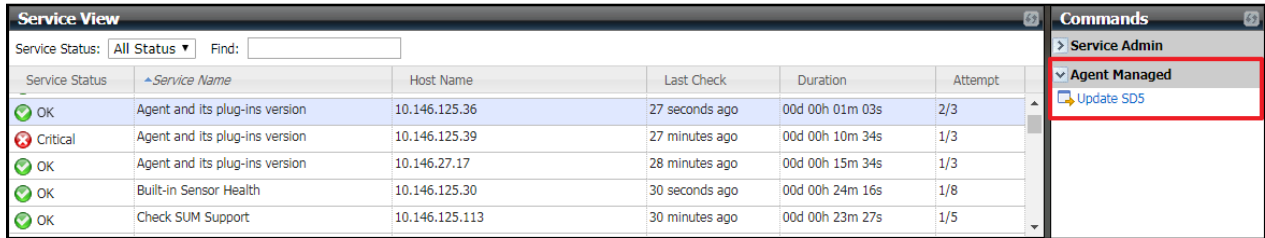


Figure 7-22

To execute a command, first select one or more hosts¹⁰ in the Host View table. Then click the command to be executed in the Command area. As shown below, a Command Execution dialog box will pop up with the selected hosts displayed. Click the **Run** button to perform the command (in this example, the Wake on LAN command) on each selected host.

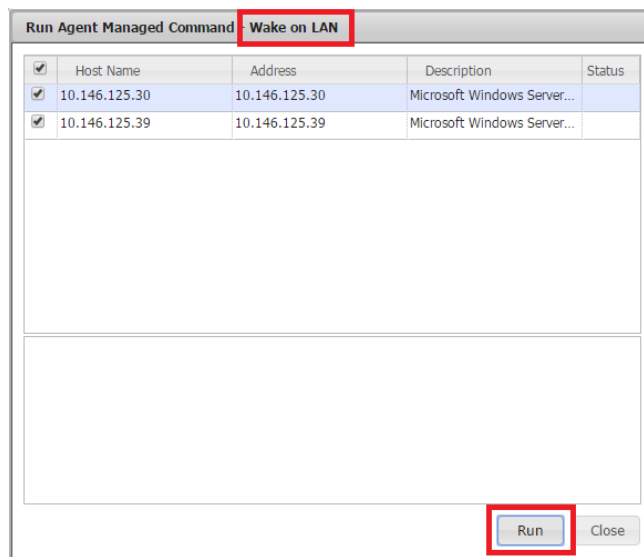


Figure 7-23

¹⁰ Use [ctrl] + [left mouse click button] to select multiple hosts in the working area.

The executed results are shown in the **Status** column of the host table.

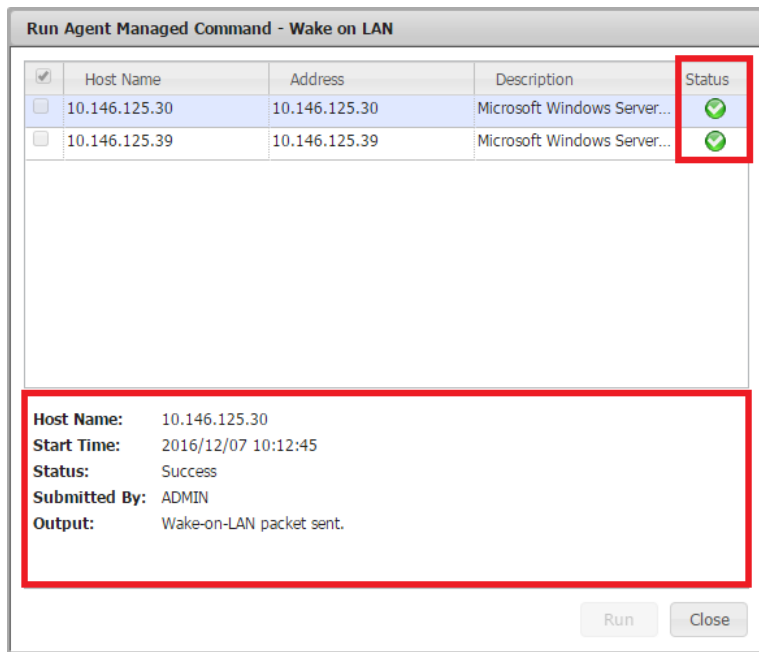


Figure 7-24

7.3.2 IPMI Commands

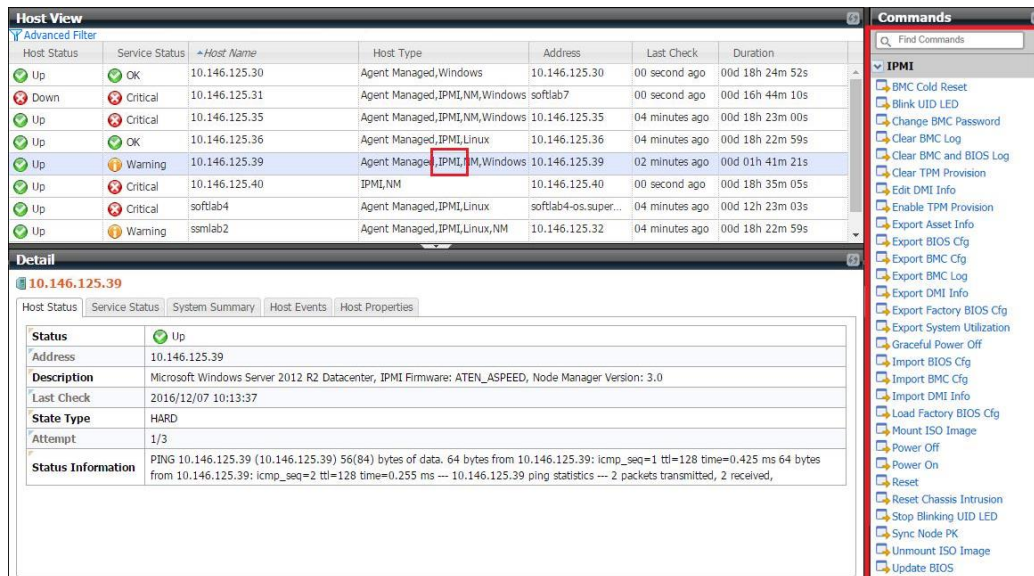


Figure 7-25

Commands in this category as shown below apply only to IPMI hosts.

- **BMC Cold Reset:** Resets (reboots) a host's BMC.
- **Blink UID LED:** Causes a host's UID LED to blink to identify a specific physical host in a data center.
- **Change BMC Password:** Resets the BMC password and updates the password saved by SSM.
- **Clear BMC Log:** Clears the BMC event logs.
- **Deploy OS:** Deploy Linux OS on a host. See *11 OS Deployment* for details.
- **Diagnose System:** Diagnose server components. See *13 System Diagnostics* for details.
- **Graceful Power Off:** Powers off a host gracefully.
- **Power Off:** Powers off a host immediately.
- **Power On:** Powers on a host.
- **Reset:** Resets (reboots) a host immediately.
- **Reset Chassis Intrusion:** Resets a chassis intrusion flag
- **Stop Blinking UID LED:** Stops a host's UID LED from blinking.
- **Sync Node PK:** Sync node product keys between SSM and BMC.

The command related to service will also appear in the Service View. For example, both commands “Update BIOS” and “Update BMC” commands will appear in the command area when a user clicks **Check SUM Support**.

The screenshot shows the 'Service View' interface. On the left, there is a table with columns: Service Status, Service Name, Host Name, Last Check, Duration, and Attempt. The table contains five rows of 'Check SUM Support' services on various hosts. On the right, there is a 'Commands' sidebar with a tree view. Under 'Service Admin', the 'IPMI' folder is expanded, showing 'Update BIOS' and 'Update BMC' commands. A red box highlights these two commands.

Service Status	Service Name	Host Name	Last Check	Duration	Attempt
OK	Check SUM Support	10.146.125.39	36 minutes ago	00d 00h 37m 17s	1/5
OK	Check SUM Support	10.146.125.40	32 minutes ago	00d 00h 15m 34s	1/5
Critical	Check SUM Support	10.146.125.44	26 minutes ago	00d 00h 04m 08s	1/5
OK	Check SUM Support	10.146.125.45	36 minutes ago	00d 00h 15m 33s	1/5
Critical	Check SUM Support	10.146.125.49	26 minutes ago	00d 00h 04m 23s	1/5

Figure 7-26



Note: 19 commands are designed for SSM and SUM integration, see *10.4 SUM Web Commands* for more information.

7.3.3 Power Management Commands

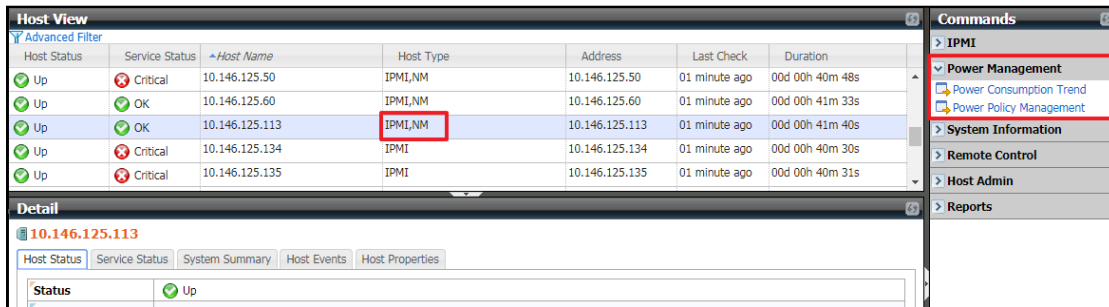


Figure 7-27

The power management commands are applicable for IPMI hosts with NM support (A NM host is always an IPMI host as well).

- **Power Consumption Trend:** Shows a power consumption trend graph containing the real-time and historical power consumption data of individual hosts and a group of hosts
- **Power Policy Management:** Adds, updates and deletes power policies of individual hosts and a group of hosts

The command related to service will also appear in the Service View. For example, the command “Power Policy Management” will appear in the command area when a user clicks **IPMI Power Consumption**.

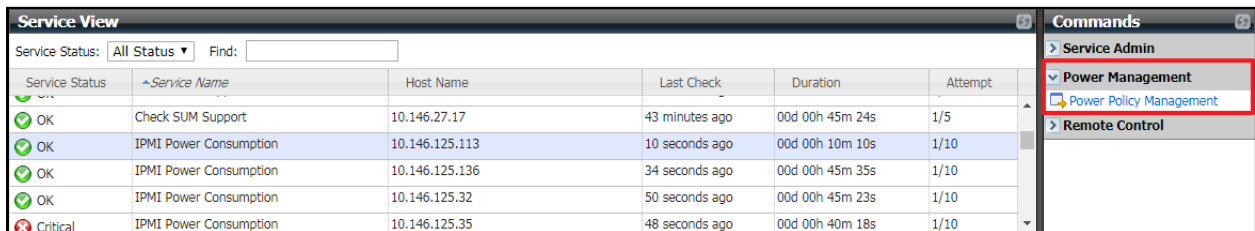


Figure 7-28

See 9 *Power Management* for more information about the power management functions.

7.3.4 System Information Commands

System Information commands apply to Agent Managed hosts and IPMI hosts. The System Information category is visible if any of these conditions exist:

- an agent-managed host is selected,
- a System Information service is selected,
- a Storage Health service is selected,
- an IPMI host is selected,
- an IPMI System Information service is selected.

Currently, only the View Details command is available for use.



Note: The function for an IPMI host is available when the node product key is activated.

Host Status	Service Status	Host Name	Host Type	Address	Last Check	Duration
Up	Critical	10.146.27.17	Agent Managed,IPMI,Linux	10.146.27.17	03 minutes ago	00d 00h 58m 42s
Up	OK	10.146.125.30	Agent Managed,Windows	10.146.125.30	01 minute ago	00d 00h 51m 14s
Up	OK	10.146.125.31	Agent Managed,IPMI,Windows	10.146.125.31	03 minutes ago	00d 00h 58m 42s
Up	Critical	10.146.125.32	Agent Managed,IPMI,Linux,NM	10.146.125.32	03 minutes ago	00d 00h 58m 41s
Up	Critical	10.146.125.33	Agent Managed,IPMI,Linux	10.146.125.33	03 minutes ago	00d 00h 58m 41s
Up	Critical	10.146.125.35	Agent Managed,IPMI,NM,Windows	10.146.125.35	03 minutes ago	00d 00h 58m 41s

Commands sidebar: Agent Managed, System Information (highlighted), View Details, Remote Control, Host Admin, Reports.

Figure 7-29

Service Status	Service Name	Host Name	Last Check	Duration	Attempt
OK	Storage Health	10.146.125.36	28 minutes ago	00d 00h 57m 46s	1/3
Critical	Storage Health	10.146.125.39	24 minutes ago	00d 00h 51m 20s	1/3
Critical	Storage Health	10.146.23.152	23 minutes ago	00d 00h 50m 30s	1/3
OK	System Information	10.146.125.119	26 minutes ago	00d 00h 57m 47s	1/3
OK	System Information	10.146.125.30	27 minutes ago	00d 00h 57m 19s	1/3
OK	System Information	10.146.125.31	29 minutes ago	00d 00h 57m 03s	1/3

Commands sidebar: Service Admin, System Information (highlighted), View Details, Remote Control.

Figure 7-30

As shown below, after executing the command, a new window containing system information objects will pop up. By default, the **Compact** view is displayed, and only the available objects are shown. Alternatively, you can select **All** in the top left corner to view all types of the system information objects.

Host Name: 10.146.23.152 Last Check : 2017/12/07 10:46:50

AVAGO 3108 MegaRAID

Properties	
Adapter ID	0
Product Name	AVAGO 3108 MegaRAID
Serial No	FW-ALLVVG6AARBWA
FW Package Build	24.18.0-0021
FW Version	4.670.00-6500
BIOS Version	6.34.01.0_4.19.08.00_0x06160200

Figure 7-31



Notes:

- For Agent Managed hosts, the system information contents are platform dependent. That is, particular information that is available on a Windows host may not be presented on a Linux host, and vice versa. Also, Linux does not support all types of system information objects in the same way that Windows supports them. Types including Desktop Monitor, Floppy, Keyboard, Port Connector, Parallel Port, Pointing Device, Serial Port, Computer Summary, Startup Command, and Video Controller are supported on Windows platforms only.
- Besides onboard controller, only LSI MegaRAID 2108, 2208 and 3108 RAID controllers are currently supported in the **Storage** category on both Windows and Linux platforms of SuperDoctor 5. Other LSI MegaRAID RAID controllers (i.e. LSI MegaRAID 2008 and 2308 RAID controllers) are not fully tested and non-LSI MegaRAID RAID controllers (i.e. LSI Fusion-MPT based and Intel Rapid Storage Technology) are not supported in this version.
- For IPMI hosts, BIOS, BaseBoard, Chassis, Computer System, Storage (onboard controller), Memory, Network, Processor, IPMI, Power Supply, OEM Strings, and System Cfg Options are supported.
- The **Current Clock Speed (MHz)** in the **Processor** category as shown below is read from the DMI table. It may not reflect the real time data when you check the current clock speed under operating systems.

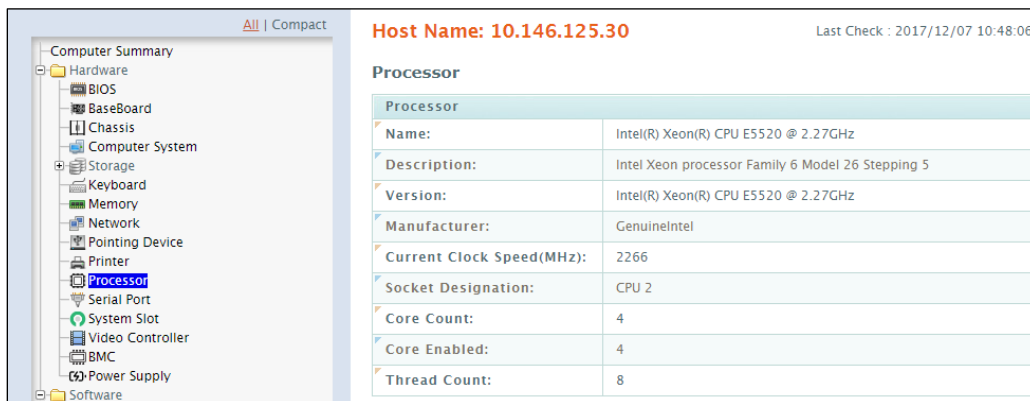


Figure 7-32

7.3.5 Remote Control Commands

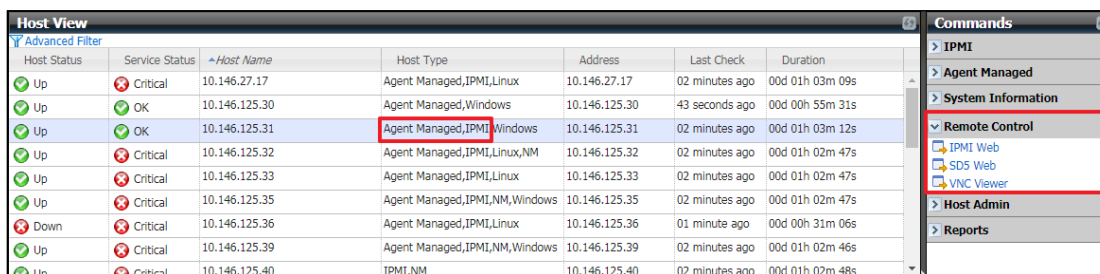


Figure 7-33

Commands in this category apply only to Agent Managed hosts and IPMI hosts. For Agent Managed hosts, two remote control commands are available:

VNC Viewer: Use the VNC viewer to control a remote host. Note that you need to properly install and configure a VNC server on the remote host and upload the VNC viewer via the SSM Web before using this function. See 6.9 *Software Update*

Uploading a VNC Viewer

for more information about how to upload a VNC viewer to the SSM Web to use this function. Clicking the **VNC Viewer** command opens a VNC connection window, as shown below. Input the VNC host address and port then click the **Connect** button to connect to the VNC server.

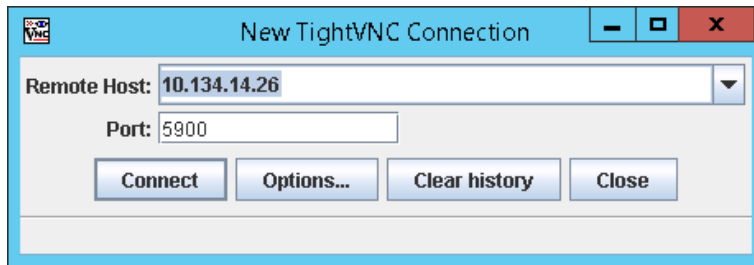


Figure 7-34

Input the VNC password and click the **Login** button to connect to the VNC server.

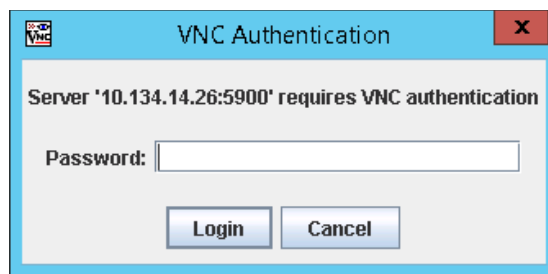


Figure 7-35

After connecting to the VNC server, you can see the remote desktop, as shown below.

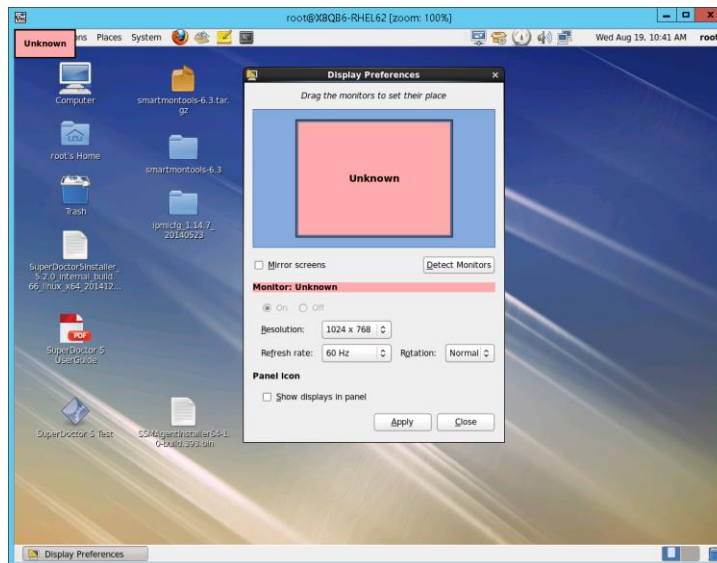


Figure 7-36

- **SD5 Web:** This opens a Web browser to connect to an SD5 Web. See *CHAPTER 4 SD5 Web in SuperDoctor 5 User's Guide* for more information.

For IPMI Managed hosts, *one remote control command* is available:

- **IPMI Web:** This opens a Web browser to connect to an IPMI Web running on an IPMI BMC. You can **use this command** to perform many IPMI functions, such as opening remote KVM, refreshing the IPMI firmware, viewing health information, using virtual media and so on.

Click the **IPMI Web** command to open a browser and connect to the IPMI Web. Enter an IPMI username and password to login to the IPMI Web.

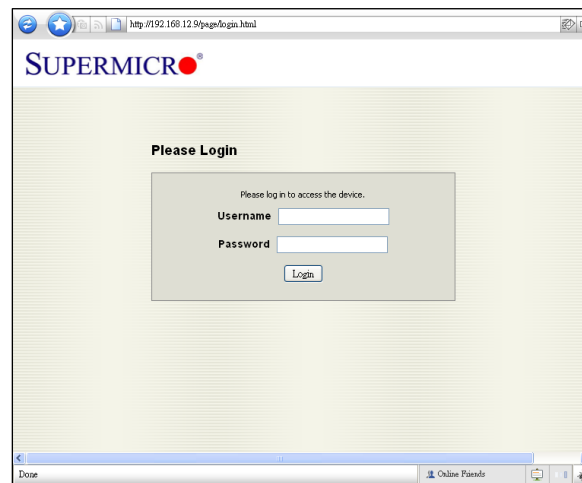


Figure 7-37

An IPMI Web example is shown below. Please read your IPMI user manual for more information about how to use the IPMI Web.

The screenshot shows the Supermicro Server Manager web interface. At the top, the browser address bar displays 'http://192.168.12.9/index.html'. The page header includes the Supermicro logo and a 'Host Identification' box showing 'Server: SMC00259001E7EE (192.168.12.9)' and 'User: ADMIN (Administrator)'. A navigation menu contains 'System Information', 'Server Health', 'Configuration', 'Remote Control', 'Maintenance', 'Miscellaneous', and 'Language'. The main content area is titled 'Server Health' and includes a description: 'This section shows you data related to the server's health, such as sensor readings and the event log.' Below this is the 'Sensor Readings' section, which contains a description, a 'Select a sensor type category:' dropdown menu set to 'All Sensors', and a table of sensor data. A sidebar on the left offers 'Options' (Server Health, Sensor Readings, Event Log), 'Refresh Page', and 'Logout'. The status bar at the bottom shows 'Done' and 'Online Friends'.

Host Identification
 Server: SMC00259001E7EE (192.168.12.9)
 User: ADMIN (Administrator)

Server Health
 This section shows you data related to the server's health, such as sensor readings and the event log.

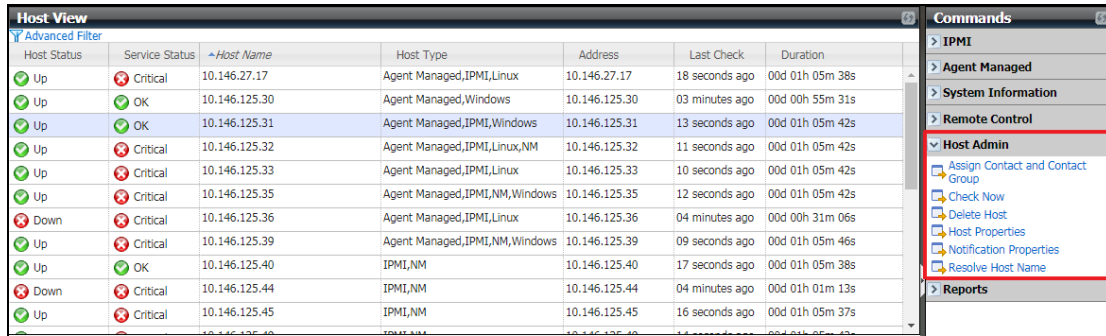
Sensor Readings
 This page displays system sensor information, including readings and status. You can toggle viewing the thresholds for the sensors by pressing the Show Thresholds button below.
 Select a sensor type category:
 All Sensors

Sensor Readings: 27 sensors

Name	Status	Reading
CPU1 Temp	Normal	Low
CPU2 Temp	Not Available	No Reading
System Temp	Normal	48 degrees C
CPU1 Vcore	Normal	0.92 Volts
CPU2 Vcore	Not Available	No Reading
CPU1 VTT	Normal	1.152 Volts
CPU2 VTT	Not Available	No Reading
DIMM1	Normal	1.52 Volts
DIMM2	Not Available	No Reading
+1.5V	Normal	1.472 Volts
+1.8V	Normal	1.816 Volts

Figure 7-38

7.3.6 Host Admin Commands



The screenshot shows the 'Host View' interface with a table of host status and a sidebar with a 'Host Admin' command category highlighted. The table has columns for Host Status, Service Status, Host Name, Host Type, Address, Last Check, and Duration. The sidebar has a 'Host Admin' category highlighted in red, containing sub-items: Assign Contact and Contact Group, Check Now, Delete Host, Host Properties, Notification Properties, and Resolve Host Name.

Host Status	Service Status	Host Name	Host Type	Address	Last Check	Duration
Up	Critical	10.146.27.17	Agent Managed,IPMI,Linux	10.146.27.17	18 seconds ago	00d 01h 05m 38s
Up	OK	10.146.125.30	Agent Managed,Windows	10.146.125.30	03 minutes ago	00d 00h 55m 31s
Up	OK	10.146.125.31	Agent Managed,IPMI,Windows	10.146.125.31	13 seconds ago	00d 01h 05m 42s
Up	Critical	10.146.125.32	Agent Managed,IPMI,Linux,NM	10.146.125.32	11 seconds ago	00d 01h 05m 42s
Up	Critical	10.146.125.33	Agent Managed,IPMI,Linux	10.146.125.33	10 seconds ago	00d 01h 05m 42s
Up	Critical	10.146.125.35	Agent Managed,IPMI,NM,Windows	10.146.125.35	12 seconds ago	00d 01h 05m 42s
Down	Critical	10.146.125.36	Agent Managed,IPMI,Linux	10.146.125.36	04 minutes ago	00d 00h 31m 06s
Up	Critical	10.146.125.39	Agent Managed,IPMI,NM,Windows	10.146.125.39	09 seconds ago	00d 01h 05m 46s
Up	OK	10.146.125.40	IPMI,NM	10.146.125.40	17 seconds ago	00d 01h 05m 38s
Down	Critical	10.146.125.44	IPMI,NM	10.146.125.44	04 minutes ago	00d 01h 01m 13s
Up	Critical	10.146.125.45	IPMI,NM	10.146.125.45	16 seconds ago	00d 01h 05m 37s

Figure 7-39

Commands in this category are used to modify host configurations such as **Host Name**, **Host Address**, **Check Interval**, **Resolve Host Name** and so on. Host admin commands apply to all types of hosts.

- **Host Properties:** Views and modifies basic host configuration data.
- **Notification Properties:** Views and modifies host notification configurations.
- **Assign Contact and Contact Group:** Views and assigns Contacts and Contact Groups to a host.
- **Check Now:** Forces a host to check to be checked immediately.
- **Delete Host:** Deletes hosts from the SSM Database.
- **Resolve Host Name:** Updates the host name by its address.

7.3.6.1 Host Properties Command

A Host Properties dialog box pops up when a host is selected and the **Host Properties** command is executed. Note that a host object represents a network device. Before your modifications, see 3.3.2 *Host Definitions* for detailed attribute information.

The screenshot shows a dialog box titled "Host Properties" with a close button (X) in the top right corner. The dialog contains several input fields, each with a red asterisk (*) indicating it is required. The fields and their values are as follows:

* Host Name	10.146.125.31
* Description	Microsoft Windows Server 2008 R2 Standard Service Pack 1, IPMI Firmware: ATEN
* Address	10.146.125.31
* SuperDoctor 5 Port	5999
* Check Interval (s)	300
* Retry Interval (s)	30
* Max Check Attempts	3
Location	
Notes	
* BMC ID	ADMIN
BMC Password	Hidden Password
* BMC Address	10.146.125.8
BMC MAC Address	00:25:90:2B:0F:C7
WOL MAC Address	00-25-90-2b-08-40

At the bottom right of the dialog, there are two buttons: "Submit" and "Close".

Figure 7-40

When selecting multiple hosts and executing the command, a Host Properties dialog will pop up as shown below. The values you input will be set to all of the selected hosts. You can select the boxes in the Override column to apply the current settings to all selected hosts. If the boxes in the Override column are not selected, the original settings are kept.

The screenshot shows a dialog box titled "Host Properties" with a close button (X) in the top right corner. The dialog contains a table with two columns: "Override" and "Property". The "Override" column contains checkboxes, and the "Property" column contains input fields. The rows are as follows:

Override	Property
<input type="checkbox"/>	SuperDoctor 5 Port
<input type="checkbox"/>	Check Interval (s)
<input type="checkbox"/>	Retry Interval (s)
<input type="checkbox"/>	Max Check Attempts
<input type="checkbox"/>	Notes
<input type="checkbox"/>	BMC ID
<input type="checkbox"/>	BMC Password

At the bottom right of the dialog, there are two buttons: "Submit" and "Close".

Figure 7-41

When multiple hosts¹¹ are selected, only the **Common Attributes** of the selected hosts are shown in the Host Properties dialog box. For example, suppose that you select an Agent-Managed host and an IPMI host and execute the **Host Properties** command.

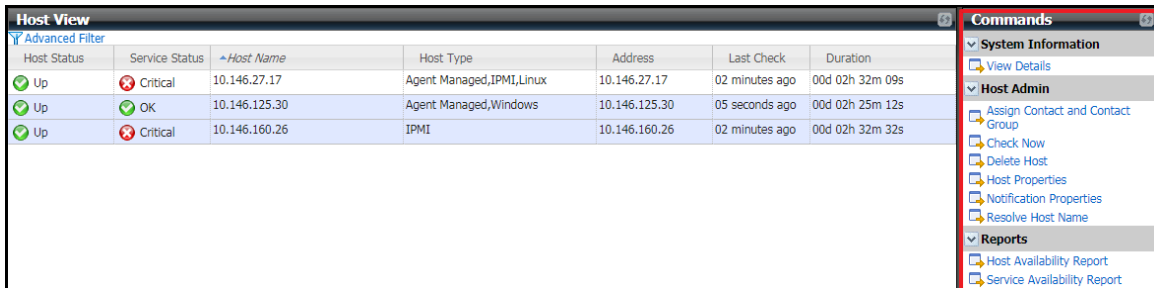


Figure 7-42

A Host Properties dialog pops up as shown below. **BMC ID** and **BMC Password** are not displayed in the dialog since the Agent-Managed host does not contain these attributes.

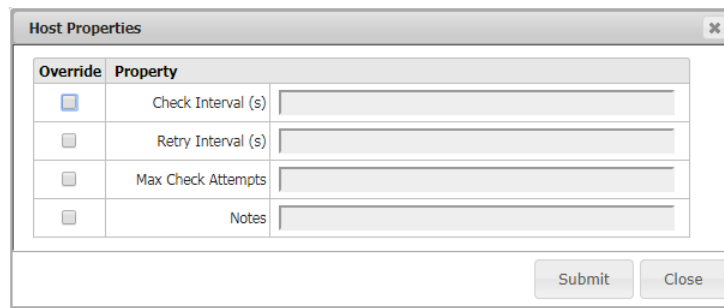


Figure 7-43

For another example, suppose that you select two IPMI with NM hosts and execute the **Host Properties** command.

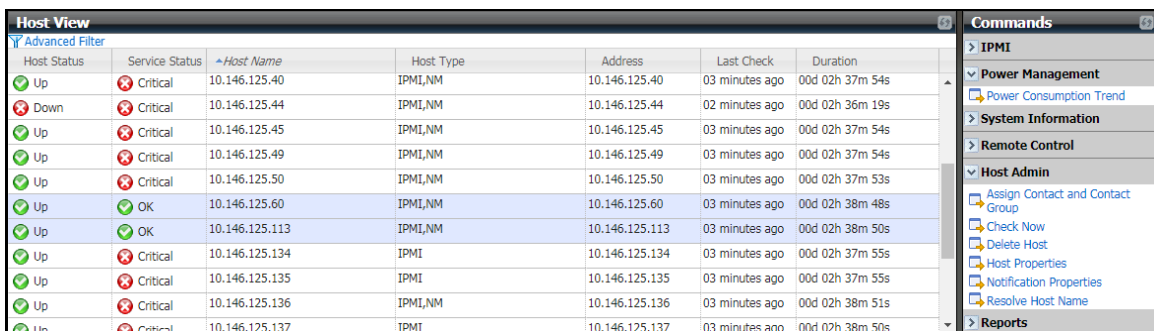


Figure 7-44

¹¹ Use [ctrl] + [left mouse click button] to select multiple hosts in the working area.

A Host Properties dialog pops up as shown below. You can see that IPMI specific attributes including **BMC ID** and **BMC Password**. Also, NM specific attributes including **Derated DC Power**, **Derated AC Power** and **Max PS Output** are displayed in the dialog.

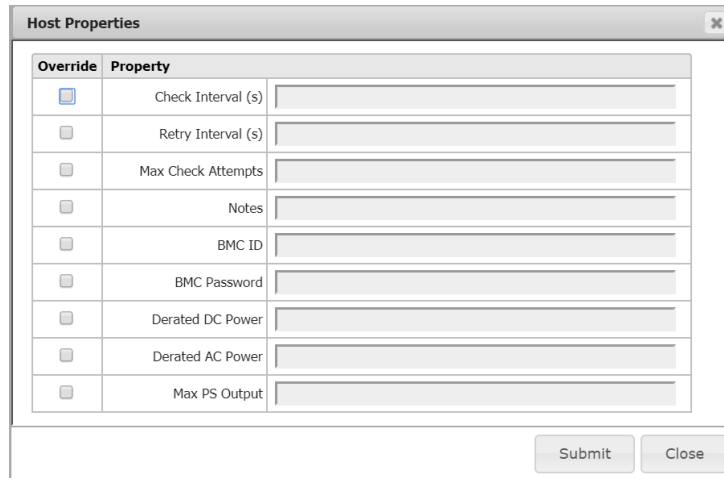


Figure 7-45

7.3.6.2 Notification Properties Command

Select one host in the Host View table, execute the **Notification Properties** command and a Notification Properties dialog box pops up.

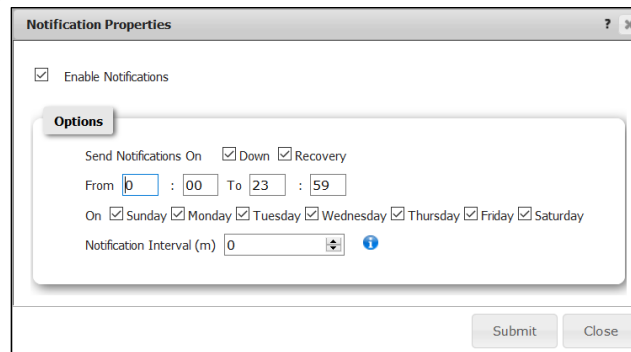


Figure 7-46

Send Notifications On When a host is down (**Down**) or recovering (**Recovery**), the contact is notified according to the host state. By default, the **Down** and **Recovery** options are both checked.

From-To The notification is sent during a period of time. By default, the time range is between 00:00 and 23:59 in a day.

- On The notification is sent on the selected days. By default, all 7 days in a week are selected.
- Notification Interval Sets the time interval for re-sending notifications when the host is still in a non-UP state. The default value of 0 means no notification will be sent again if the host remains problematic.

7.3.6.3 Assign Contact and Contact Group Command

A dialog box pops up when a host is selected and the **Contact** and **Contact Group** command is executed. You can modify the contacts and contact groups of a host in this dialog box.

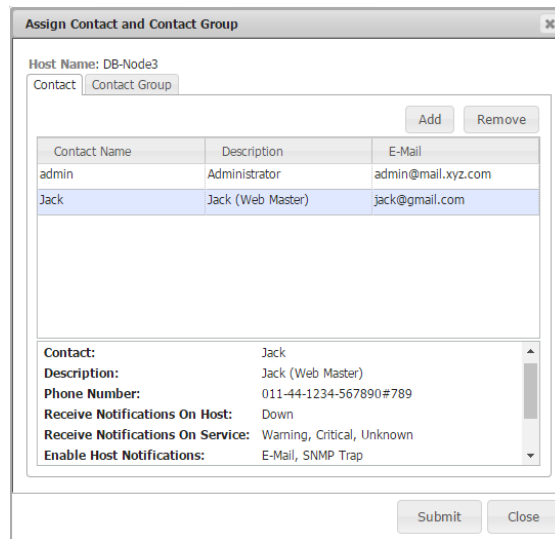


Figure 7-47

7.3.6.4 Check Now Command

Normally, the SSM Server knows how frequently a host should be checked based on the **check_interval** attribute of the host. The **Check Now** command allows a user to forcibly perform a host check immediately on the SSM Server. A Check Now dialog box pops up when the hosts are selected and the Check Now command is executed. Click the **Run** button to wait for all check results, or you can click the **Background** button to view the health status check result on the monitoring page.



Note: A host check is not exactly performed immediately. If the command is executed to run on multiple hosts simultaneously, the selected hosts to be checked will have to wait.

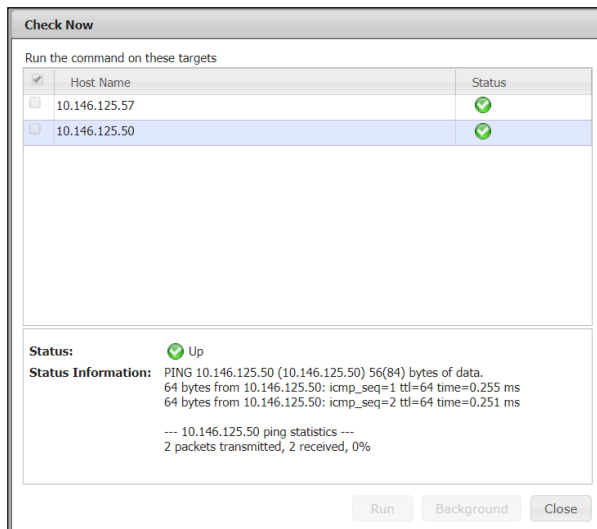


Figure 7-48

7.3.6.5 Delete Host Command

A Delete Host dialog box pops up when hosts are selected and the **Delete Host** command is executed. Click the **Run** button to delete the selected hosts from the SSM Database.



Note: There is NO Undo function provided, so data cannot be recovered once it has been modified or deleted.

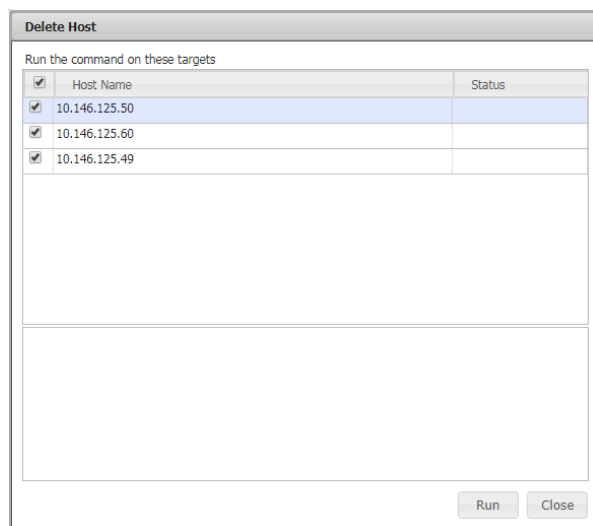


Figure 7-49

7.3.6.6 Resolve Host Name Command

A dialog box pops up when multiple hosts are selected, and the **Resolve Host Name** command is executed. You can change these hosts' names to the DNS names in this dialog box. Note that the command is applicable for a host with an IP address in the Address field.

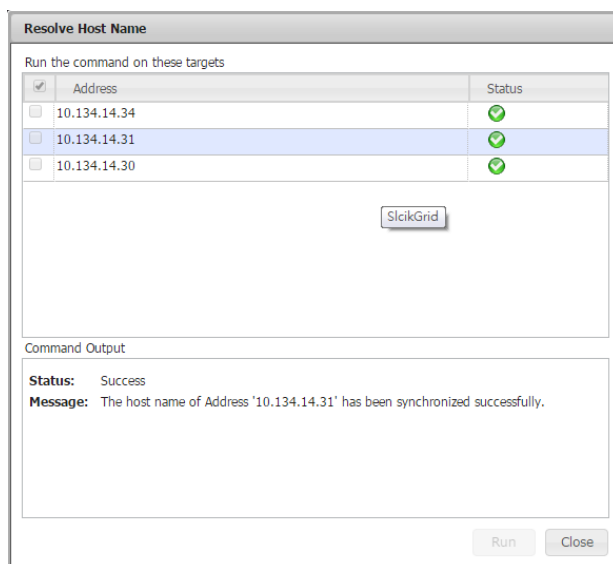


Figure 7-50

7.3.7 Report Commands

Commands in this category are used to show availability reports of hosts and services. They apply to all types of hosts.

- **Host Availability Report:** Shows a host availability report during a user-defined time period
- **Service Availability Report:** Shows a service availability report during a user-defined time period

You can also find the same availability reports on the **Reporting** page. The two commands above are shortcuts to generate the two availability reports. See *8 SSM Web Reporting Page* for more information.

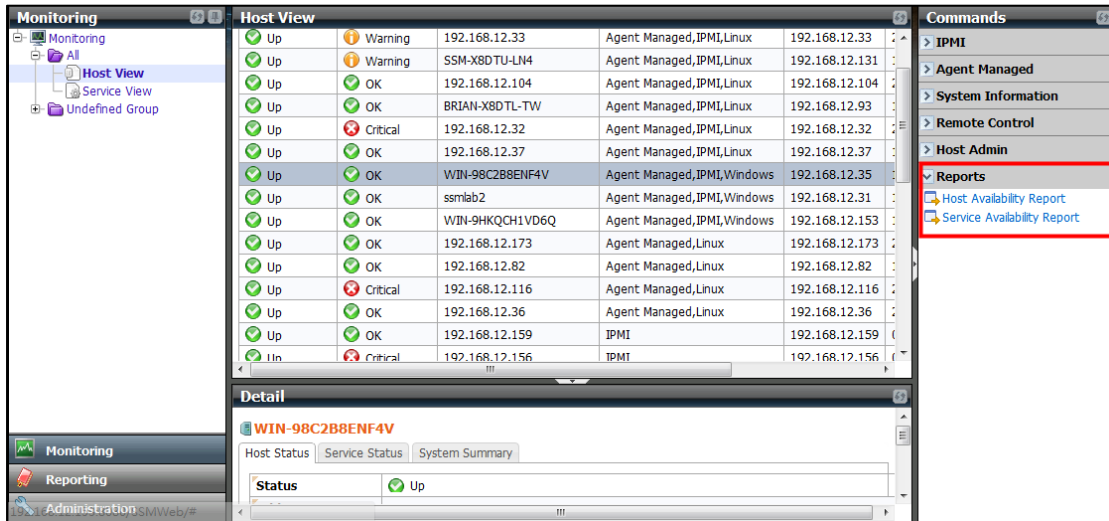


Figure 7-51

Host Name: 10.146.125.35, 10.146.125.3

Last Time: Last 7 Days Start Date: 2016/11/30 10 : 53 End Date: 2016/12/07 10 : 53 Query

Date Period : 2016/11/30 10:53:20 To 2016/12/07 10:53:20 Duration : 07d 00h 00m 00s

Host Name	Time Up	Time Down	Time Unreachable	Time Undetermined
10.146.125.35	100% (11.3%)	0% (0%)	0% (0%)	88.7%
10.146.125.39	41.47% (4.67%)	58.53% (6.6%)	0% (0%)	88.73%

Figure 7-52 Host Availability Report (Example)

Host Name: 10.146.125.35, 10.146.125.3

Last Time: Last 7 Days Start Date: 2016/11/30 10 : 55 End Date: 2016/12/07 10 : 55 Query

Date Period : 2016/11/30 10:55:58 To 2016/12/07 10:55:58 Duration : 07d 00h 00m 00s

Host Name	Service Name	Time OK	Time Warning	Time Unknown	Time Critical	Time Undetermin...
10.146.125.35	Check SUM Support	1.16% (0.1%)	0% (0%)	0% (0%)	98.84% (8.74%)	91.15%
10.146.125.35	System Information	100% (11.08%)	0% (0%)	0% (0%)	0% (0%)	88.92%
10.146.125.35	Memory Health	98.68% (11.15%)	0% (0%)	0% (0%)	1.32% (0.15%)	88.7%
10.146.125.35	IPMI Sensor Health	100% (11.3%)	0% (0%)	0% (0%)	0% (0%)	88.7%
10.146.125.35	Storage Health	97.34% (10.88%)	0% (0%)	0% (0%)	2.66% (0.3%)	88.82%
10.146.125.35	IPMI Power Cons...	100% (11.3%)	0% (0%)	0% (0%)	0% (0%)	88.7%
10.146.125.39	Storage Health	0.37% (0.04%)	38.48% (4.31%)	2.62% (0.29%)	58.53% (6.55%)	88.81%
10.146.125.39	System Information	44.08% (4.93%)	0% (0%)	0% (0%)	55.92% (6.25%)	88.82%
10.146.125.39	Memory Health	39.86% (4.5%)	0% (0%)	0% (0%)	60.14% (6.79%)	88.7%

Figure 7-53 Service Availability Report (Example)

7.3.8 Service Admin Commands

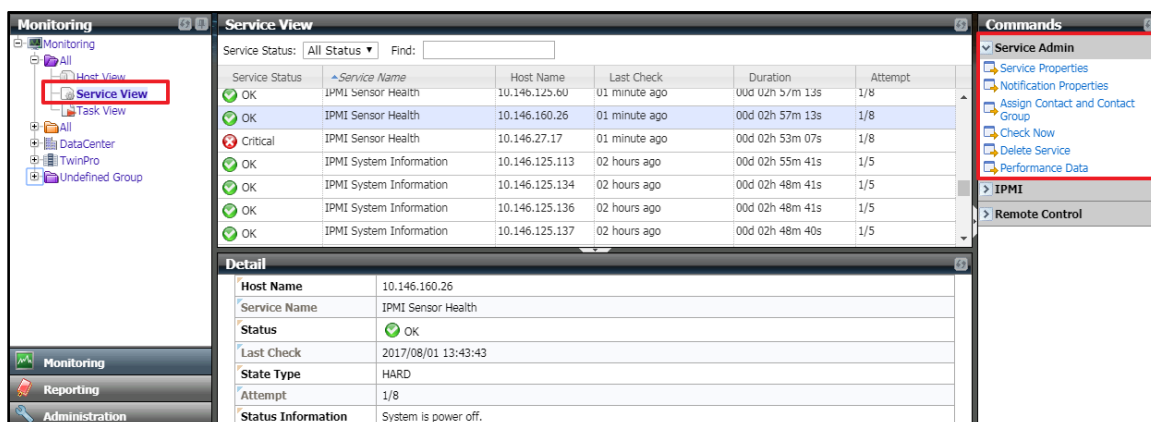


Figure 7-54

As shown above, **Service Admin** commands are available while using a Service View. Commands in this category are used to modify service configurations such as service name, check interval and so on.

- **Service Properties:** Views and modifies the basic service properties of selected services.
- **Notification Properties:** Views and modifies the service notification configurations.
- **Change Arguments:** Views and modifies the command arguments of selected services. (Note that this command will be displayed only when the selected services require command arguments such as Check HTTP, Check FTP, Check SMTP, Execute a script, Storage Health and Memory Health.)
- **Check Now:** Forces a service check to be performed immediately.
- **Contact and Contact Group:** Views and assigns Contacts and Contact Groups to selected services.
- **Delete Service:** Deletes services from the SSM Database.
- **Performance Data:** Shows a dialog to display a service's performance data. Note that this command is available when **Contain Perf Data** property in the Service Properties is Yes.

7.3.8.1 Service Properties Command

When selecting a service and executing the command, a Service Properties dialog box will pop up as shown below. Note that a service object represents a "service" running on a host. Before your modifications, see 3.3.4 *Service Definitions* for detailed attribute information.

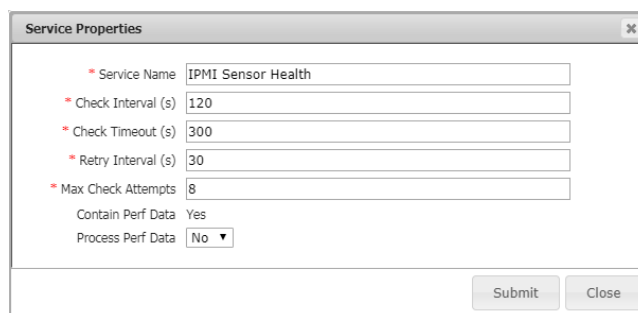


Figure 7-55

Also, when selecting multiple services¹² and executing the command, a Service Properties dialog will pop up as shown below. The values you input will be set to all of the selected services. You can select the boxes in the Override column to apply the current settings to all selected services. If the boxes in the Override column are not selected, the original settings are kept.

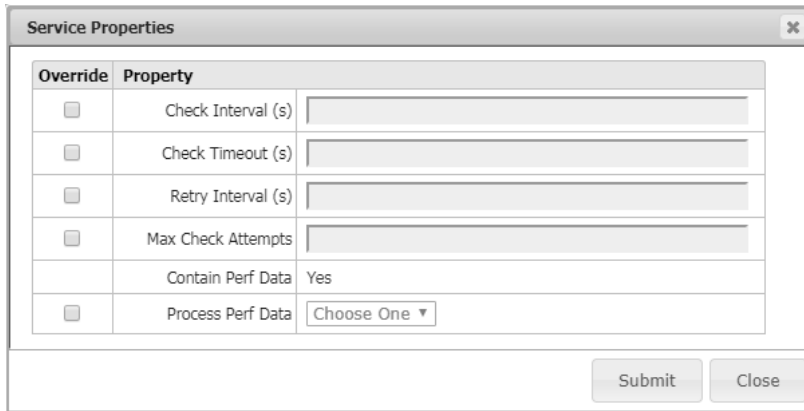


Figure 7-56

When multiple services are selected, only the **Common Attributes** of the selected services are shown in the Service Properties dialog box. For example, suppose that you select an IPMI Power Consumption service and a Storage Health service and execute the **Service Properties** command.

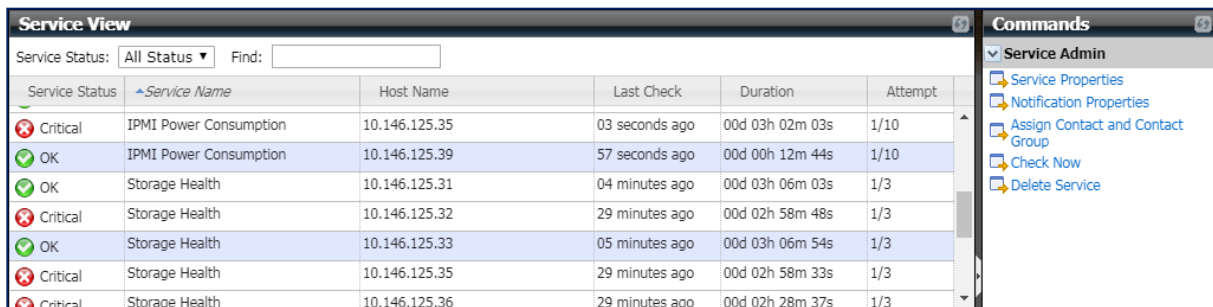


Figure 7-57

A Service Properties dialog pops up as shown below. **Contain Perf Data** and **Process Perf Data** attributes are not displayed in the dialog since the Storage Health service does not contain these attributes.

¹² Use [ctrl] + [left mouse click button] to select multiple services in the working area.

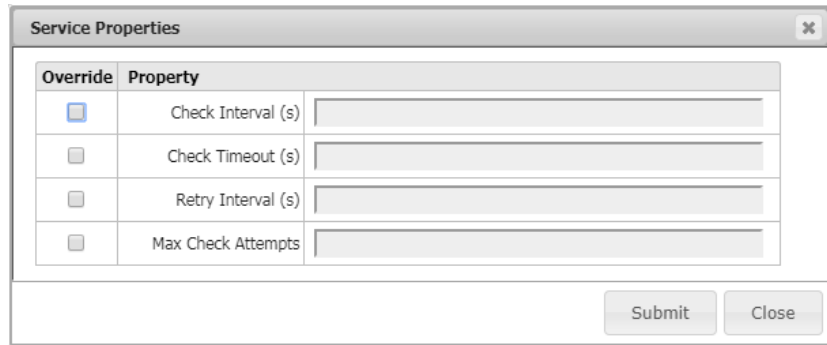


Figure 7-58

For another example, suppose that you select two IPMI Power Consumption services and execute the **Service Properties** command.

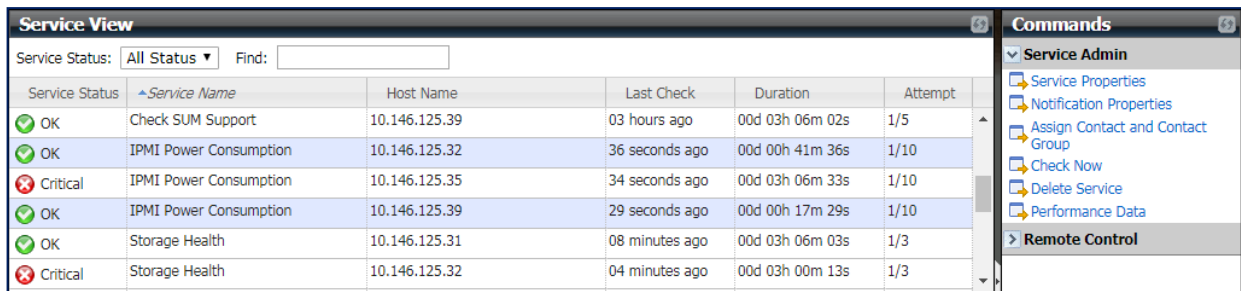


Figure 7-59

A Service Properties dialog pops up as shown below. You can see that the IPMI Power Consumption specific attributes **Contain Perf Data** and **Process Perf Data** are displayed in the dialog.

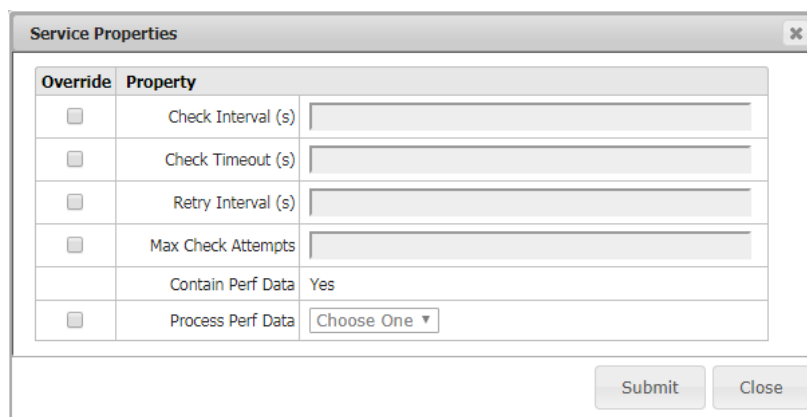


Figure 7-60

7.3.8.2 Notification Properties Command

Select one service in the Service View table, execute the **Notification Properties** command and a Notification Properties dialog box pops up.

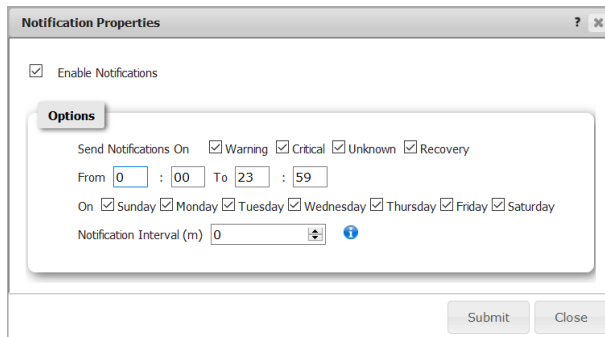


Figure 7-61

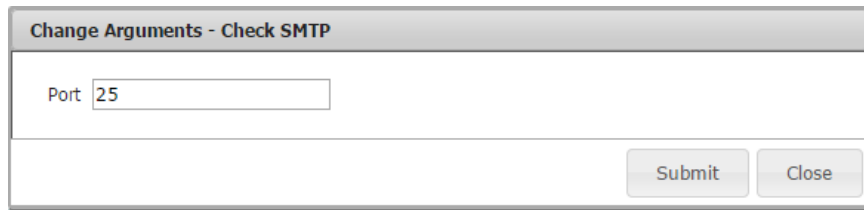
- Send Notifications On** When services are either problematic or recovering, the notification is sent according to the service state (**Warning, Unknown, Critical and Recovery**). By default, the **Warning, Unknown, Critical and Recovery** options are all checked.
- From-To** The notification is sent during a period of time. By default, the time range is between 00:00 and 23:59 in a day.
- On** The notification is sent on the selected days. By default, all 7 days in a week are selected.
- Notification Interval** Sets the time interval for re-sending notifications when the host is still in a non-UP state. The default value of 0 means no notification will be sent again if the host remains problematic.

7.3.8.3 Change Arguments Command

This function is used to modify the command arguments of selected services. Currently, only these services are supported: **Check HTTP, Check FTP, Check SMTP, Execute a script, Storage Health, Memory Health and IPMI SEL Health**. Note that only these services require command arguments, so the Change Arguments command is visible in the command area only when the above services are selected. The **Check SMTP, Storage Health, and IPMI SEL Health** services are given as examples below.

Check SMTP

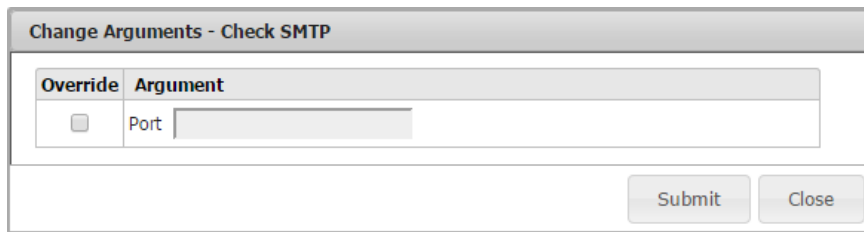
When you select a **Check SMTP** service and execute the command, a Change Arguments dialog box will appear.



A dialog box titled "Change Arguments - Check SMTP". It contains a text input field labeled "Port" with the value "25" entered. At the bottom right, there are two buttons: "Submit" and "Close".

Figure 7-62

When you select multiple Check SMTP services and execute the command, a Change Arguments dialog will pop up. Note that the values you enter will apply to all of the selected services.

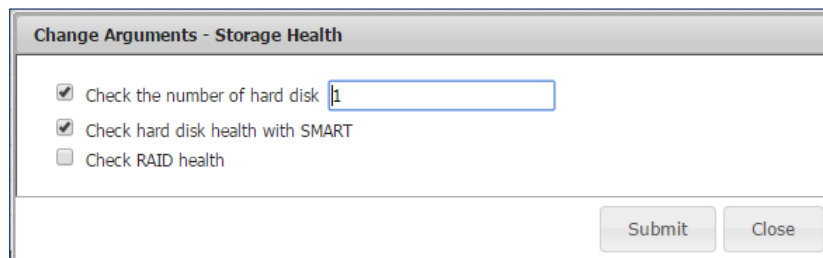


A dialog box titled "Change Arguments - Check SMTP". It features a table with two columns: "Override" and "Argument". The "Override" column contains a checkbox that is currently unchecked. The "Argument" column contains a text input field with the value "Port" and an empty text box. At the bottom right, there are two buttons: "Submit" and "Close".

Figure 7-63

Storage Health

When you select a **Storage Health** service and execute the command, a Change Arguments dialog box will appear.



A dialog box titled "Change Arguments - Storage Health". It contains three checked checkboxes: "Check the number of hard disk" (with a text input field containing "1"), "Check hard disk health with SMART", and "Check RAID health" (which is unchecked). At the bottom right, there are two buttons: "Submit" and "Close".

Figure 7-64

When you select multiple **Storage Health** services and execute the command, a Change Arguments dialog will appear. The values you enter will apply to all of the selected services. You can select the boxes in the Override column to apply the current settings to all selected services. If the boxes in the Override column are not selected, the original settings are kept.

In the figure below, the number of hard disks will be checked based on the settings on each system. The hard disk health of all systems will not be checked whether this service is already enabled or not. The RAID health of all systems will be checked.

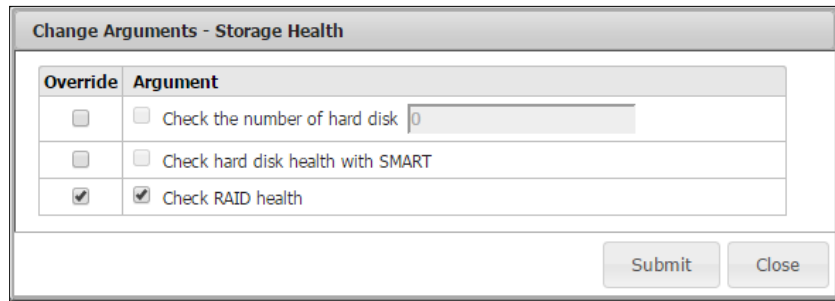


Figure 7-65

IPMI SEL Health

To avoid minor notifications sent due to issues with the IPMI SEL Health service, you can use the Change Arguments command to filter SEL items by specifying either severities or specific events. Those specified severities and events will not be checked by the IPMI SEL Health service. The example below illustrates the steps taken to ignore specific events.

[Scenario]

A SEL item is checked by the IPMI SEL Health service. The severity of this SEL item is “ERROR”, its sensor type is “Memory” and its event type is “Uncorrectable ECC.”

Service Status	Service Name	Host Name	Last Check	Duration	Attempt
Critical	IPMI SEL Health	10.146.125.137	45 seconds ago	00d 00h 04m 11s	1/3
OK	IPMI Sensor Health	10.146.125.137	01 minute ago	00d 00h 06m 19s	1/8
OK	IPMI System Information	10.146.125.137	05 minutes ago	00d 00h 05m 07s	1/5

Host Name	10.146.125.137
Service Name	IPMI SEL Health
Status	Critical
Last Check	2017/11/13 16:22:05
State Type	HARD
Attempt	1/3
Status Information	SEL needs attention; 11/13/2017 16:21:29; ERROR Memory Uncorrectable ECC@DIMMA1(CPU1)

Severity Sensor Type Event Type

Figure 7-66

1. To filter this event, execute the command, and a Change Arguments dialog box appears. There are events such as temperature, voltage, and fan already filtered by default so it is unnecessary to repeat the same checkup done by other services.

Change Arguments - IPMI SEL Health

You can specify severities or add a specific event to be ignored by the IPMI/Redfish SEL Health service.

Severity: ERROR CRITICAL WARNING

Sensor Type	Event Type	Severity
Temperature	All Events	
Voltage	All Events	
Current	All Events	
Fan	All Events	
Physical Security (Chassis)	General Chassis Intrusion	CRITICAL

Figure 7-67

2. Click the **ERROR** check box to ignore all events with ERROR severity.

Change Arguments - IPMI SEL Health

You can specify severities or add a specific event to be ignored by the IPMI/Redfish SEL Health service.

Severity: ERROR CRITICAL WARNING

Sensor Type	Event Type	Severity
Temperature	All Events	
Voltage	All Events	
Current	All Events	
Fan	All Events	
Physical Security (Chassis)	General Chassis Intrusion	CRITICAL

Figure 7-68

3. Otherwise, click the **Add Event** button to specify the event.
4. Add an event with its sensor type as “Memory” and event type as “Uncorrectable ECC.” Note that “All Events” can be selected as the “Memory” sensor type, which means all events classified as “Memory” will be ignored by the IPMI SEL Health service.

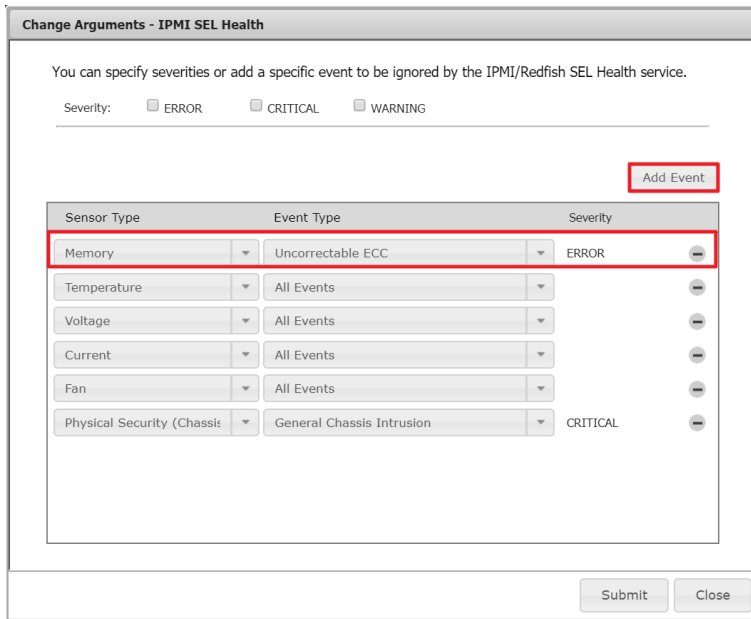


Figure 7-69

5. Click the **Submit** button to complete the configuration. Note that the excluded events will belong to both severities and event types.
6. Wait until the next service check is performed. The IPMI SEL Health service now changes from a non-OK state to an OK state.

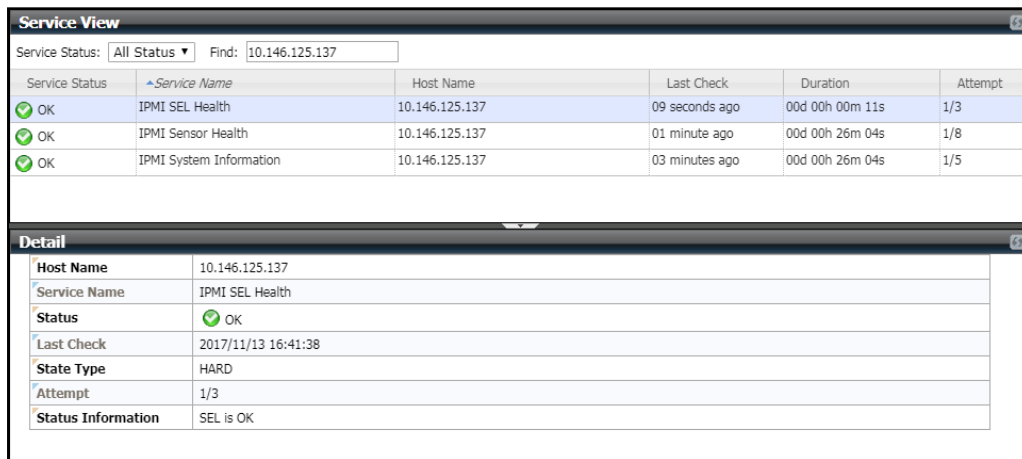


Figure 7-70

7. If you select multiple **IPMI SEL Health** services and execute the command, a Change Arguments dialog box appears. You can select **Append** or **Override** to set up events of the selected service.

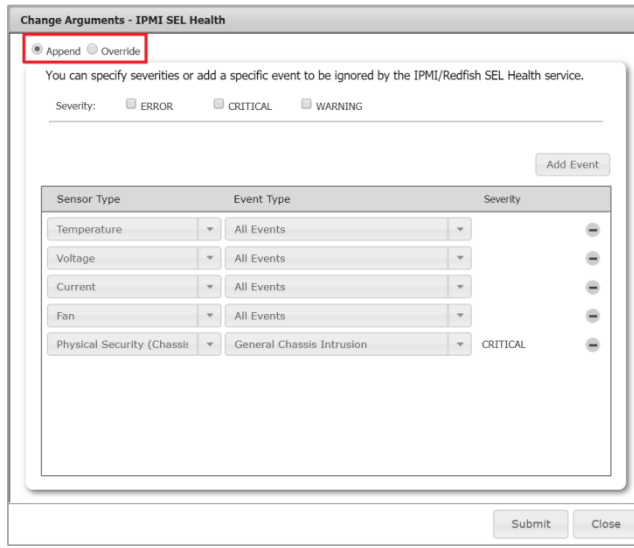


Figure 7-71

7.3.8.4 Contact and Contact Group Command

When selecting a service and executing the **Contact** and **Contact Group** command, a dialog box will pop up. You can modify the contacts and contact groups of a service in this dialog box.

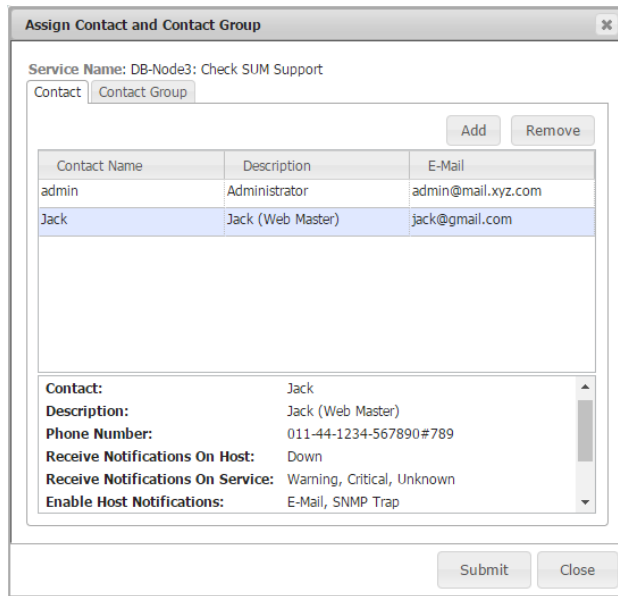


Figure 7-72

7.3.8.5 Check Now Command

Normally, the SSM Server knows how frequently the service should be checked based on the **check_interval** attribute of the service. The **Check Now** command allows a user to forcibly perform a

service check immediately on the SSM Server. A Check Now dialog box pops up when the services are selected and the Check Now command is executed. Click the **Run** button to wait for all check results, or you can click the **Background** button to see the health status result on the monitoring page.



Note: The time a service check is not exactly performed immediately. The commands will be queued for execution if multiple services are submitted simultaneously.

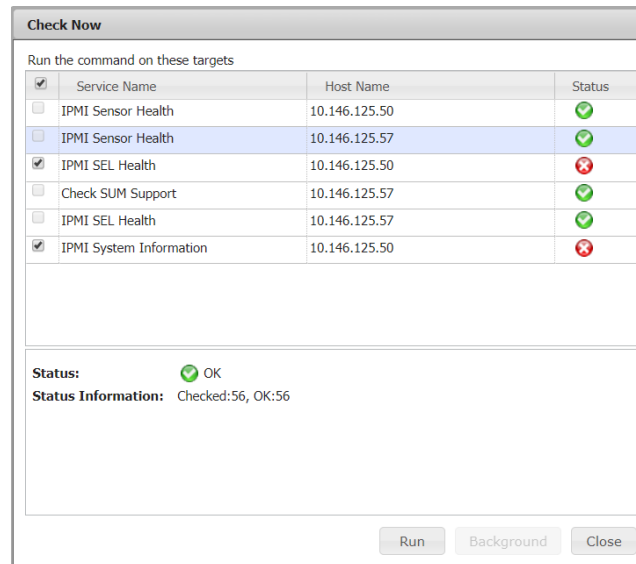


Figure 7-73

7.3.8.6 Delete Service Command

A Delete Service dialog box pops up when services are selected and the **Delete Service** command is executed. Click the **Run** button to delete the selected services from the SSM Database.



Note: There is no undo function provided so data cannot be recovered once it is modified or deleted.

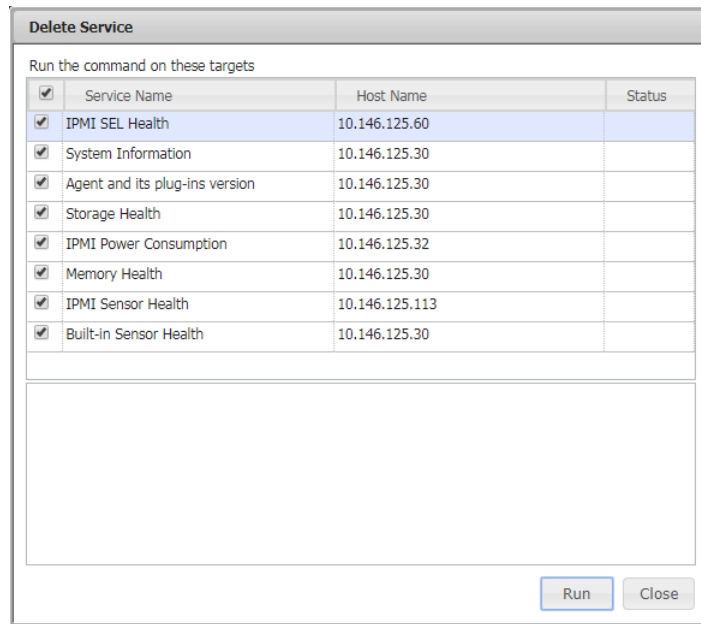


Figure 7-74

7.3.8.7 Performance Data Command

Three SSM built-in services, the **IPMI Sensor Health**, **Built-in Sensor Health**, and **IPMI Power Consumption** support performance data. The **Contain Perf Data** property in the Service Properties dialog denotes whether a service supports performance data or not. For a service supporting performance data, you can further setup the **Process Perf Data** property to tell SSM Server to handle the data and to store it in the SSM Database. If the **Process Perf Data** property is set to **No**, performance data will not be processed by the SSM Server and thus no performance data will be shown.

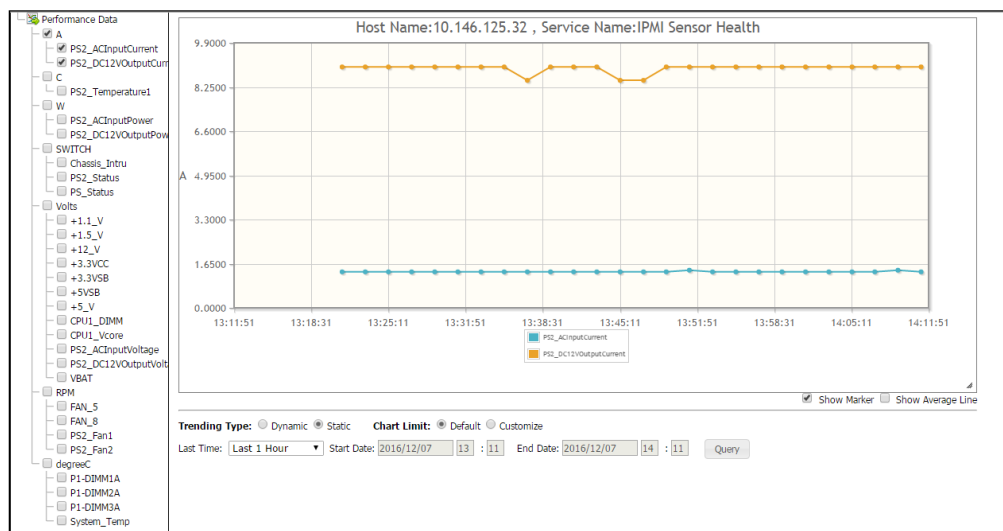


Figure 7-75: Performance Data dialog of an IPMI Sensor Health service

The performance data of an individual host stored in the SSM Database contains three different formats: raw data, aggregated one-hour data and aggregated one-day data. The Performance Data dialog shows raw data when the query time period is less than the setting of the **Keep performance raw data attribute** of the database maintenance program (see *6.11 DB Maintenance* for more information). The aggregated one-hour data is shown when the query time period is greater than the setting of the **Keep performance raw data attribute** of the database maintenance program, and less than 30 days. The aggregated one-day data is shown when the query time period is greater than 30 days.

The performance data of a host group stored in the SSM Database contains two different formats: raw data and aggregated one-hour data. The Performance Data dialog applies the same logic to show performance data of an individual host and a host group except that for a host group the aggregated one-day performance data is not available. In other words, The Performance Data dialog uses the aggregated one-hour data of a host group when the query time period is greater than the setting of the **Keep performance raw data attribute** of the database maintenance program.

A service's performance data usually contains more than one item. For example, performance data of the IPMI Sensor Health service as shown above contains 23 items: **PS1_ACInputPower(W)**, **PS1_DC12VOuput(W)**, **P1_DIMM1A(°C)** and **System_Temp(°C)**, and so on. A new record of an item in the performance data is created and stored in the SSM Database every time a service is checked by the SSM Server.

Suppose that the check interval of the IPMI Sensor Health service is 60 seconds, which means 23 different records in the SSM Database are created every 60 seconds for a single **IPMI Sensor Health** service. If you have 100 IPMI Sensor Health services, 3312,000 records will be created in one day. As a result, a huge volume of records will be stored in the SSM Database over time. Storing too many records in the SSM Database causes serious performance issues. To alleviate this, by default only the **IPMI Power Consumption** service's performance data is enabled and processed by the SSM Server. You can enable other services' performance data manually using the **Service Properties** command. SSM Server removes the performance data from the SSM Database regularly; see *6.11 DB Maintenance* for more information.

7.3.9 Task Commands

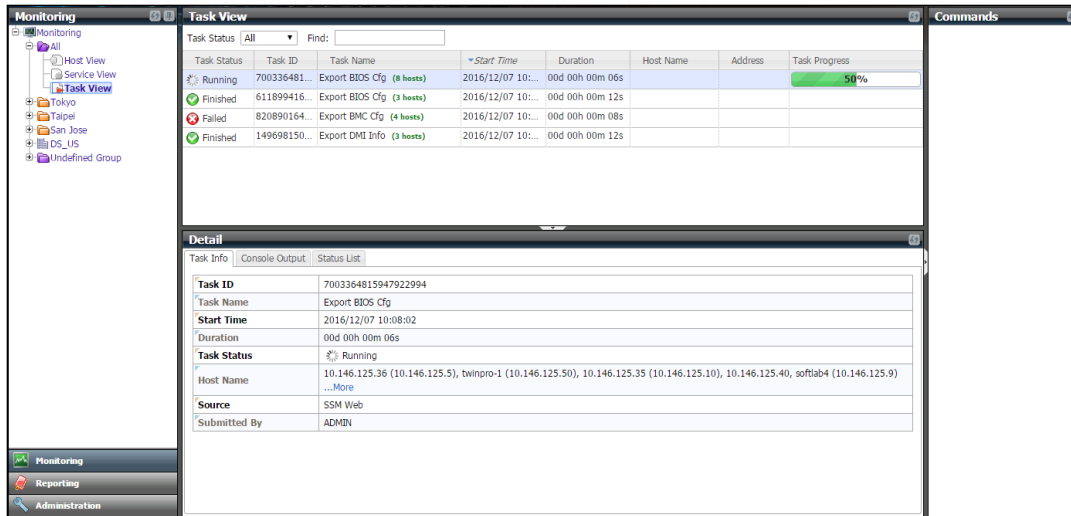


Figure 7-76

As shown above, **Task** commands are available when the Task View is in use.

- **Run Again:** Retries the task with the original arguments. The command is only available when the task status is **Failed**.
- **Delete Task:** Deletes the task when the task is complete.
- **Download Artifacts:** Downloads artifacts generated by the task.

7.3.9.1 Run Again Command

The Run Again command applies to the failed tasks. Follow these steps to issue a Run Again request.

1. When you select a task and execute the command, a **Run Again** dialog box appears.

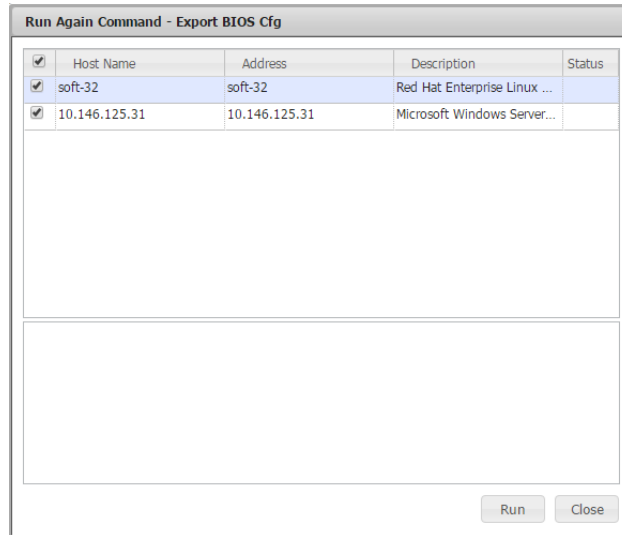


Figure 7-77

2. Click the **Run** button to start the original arguments and commands of the task. The host of the OK status returned in the task will not be in the run-again list. For example, both “10.146.125.31” and “soft_32” are in the run-again list because the users did not successfully export BIOS Cfg from them.
3. Check the retry status of each host. In the example below, the **Export BIOS Cfg** command for “soft_32” is successfully executed while the command for “10.146.125.31” is not.

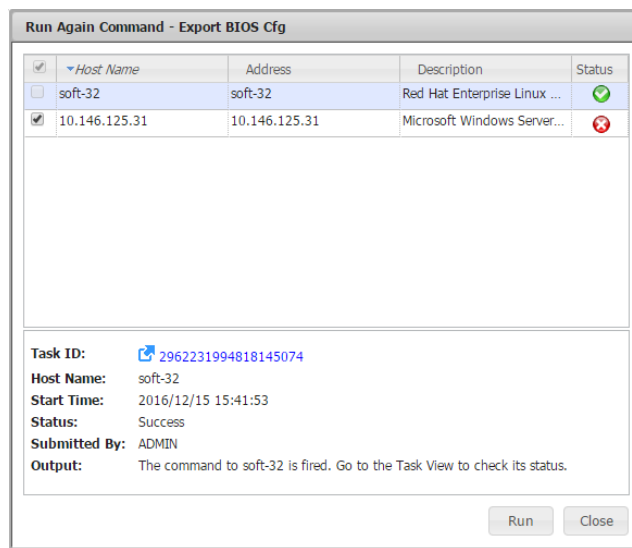


Figure 7-78

7.3.9.2 Delete Task Command

The **Delete Task** command applies to the finished or failed tasks. When you select multiple tasks and execute the command, a dialog box (see the figure below) appears. Click the **OK** button to delete the selected tasks from SSM.



Note: No undo function is provided for recovering the deleted data.

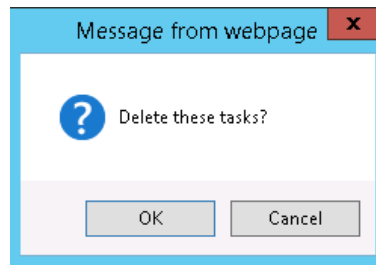


Figure 7-79

7.3.9.3 Download artifact Command

The **Download Artifacts** command applies to the tasks that have generated artifacts. Follow these steps to make a request and retrieve the artifacts.

1. When you select multiple tasks and execute the command, a **Download Artifacts** dialog box appears.

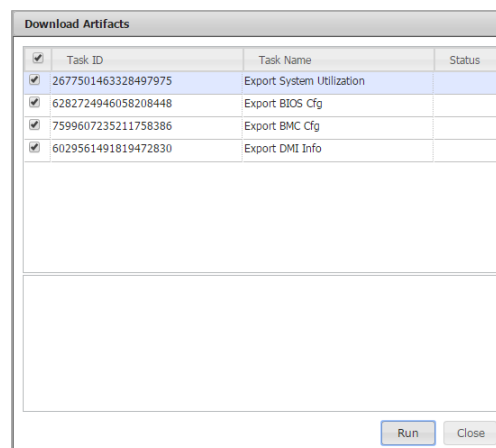


Figure 7-80

2. Click the **Run** button to start packing artifacts or click the **Close** button to abort and close this dialog box. In the dialog box (see the figure below), the green check icon in the Status field

indicates that the request has been sent. Check the output message and retry if there is no green check icon.

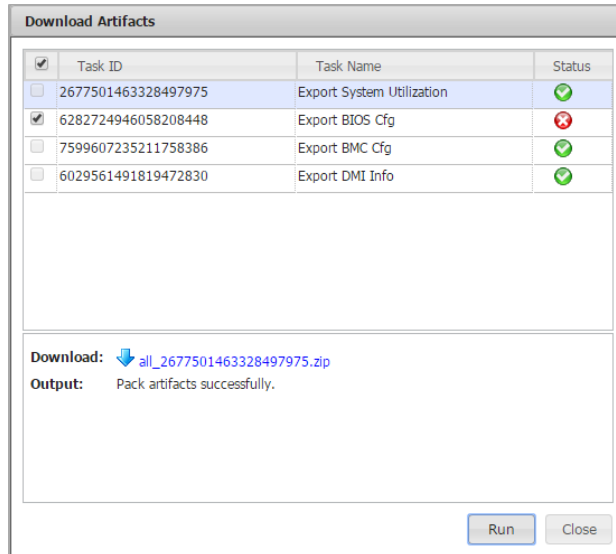


Figure 7-81

3. Select the first item and click the **Download** link to download the artifacts it generates. For example, in the figure above, select the task # 2677501463328497975 and click the **Download** link. The all-in-one zip file contains log files, the output files from the selected hosts, and a readable file in CSV format stores all exported Information from the selected hosts if available.

7.3.10 Redfish Commands

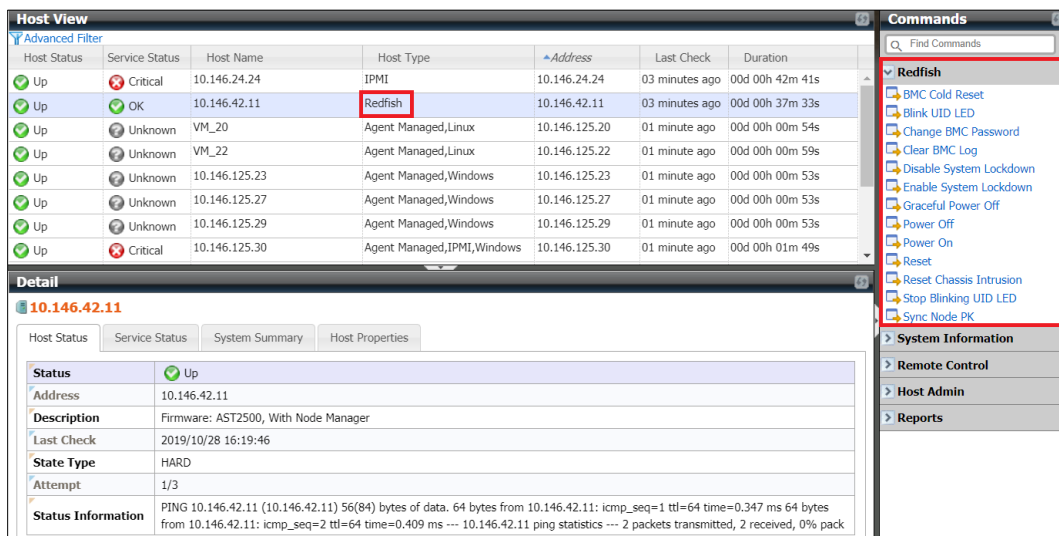


Figure 7-82

Commands in this category as shown below apply only to Redfish hosts. They are similar to those in the IPMI category, but are run with the Redfish protocol to communicate with the BMC.

- **BMC Cold Reset:** Resets (reboots) a host's BMC.
- **Blink UID LED:** Causes a host's UID LED to blink to identify a specific physical host in a data center.
- **Change BMC Password:** Resets the BMC password and updates the password saved by SSM.
- **Clear BMC Log:** Clears the BMC event logs.
- **Enable System lockdown:** Enables a host's lockdown mode. Note that the managed system must be Supermicro X12/H12 series or later.
- **Disable System lockdown:** Disables a host's lockdown mode. Note that the managed system must be Supermicro X12/H12 series or later.
- **Graceful Power Off:** Powers off a host gracefully.
- **Power Off:** Powers off a host immediately.
- **Power On:** Powers on a host.
- **Reset:** Resets (reboots) a host immediately.
- **Reset Chassis Intrusion:** Resets a chassis intrusion flag
- **Stop Blinking UID LED:** Stops a host's UID LED from blinking.
- **Sync Node PK:** Sync node product keys between SSM and BMC.

7.4 Notifications

7.4.1 Alert Events

SSM will trigger a problem alert when the following two conditions are met: a hard state change occurs on a host, and the status of the host changes from an UP state to a non-UP state¹³ (i.e. DOWN or UNREACHABLE).

SSM will send a recovery alert when the status of the host changes from a non-UP state to an UP state. If the host is in the soft state, SSM will retry the host check command and will not trigger an alert.

In terms of services, SSM will trigger a hard state change alert when the state changes: an OK state changes to a non-OK state¹⁴ (i.e. WARNING, UNKNOWN or CRITICAL) or a non-OK state changes to an OK state. If the service is in a soft state, SSM will retry the service check command and will not trigger an alert.

By default, all hosts and services enable notifications. Select one host in the Host View table, execute the **Notification Properties** command and a Notification Properties dialog box pops up. Notifications will be sent 24 hours a day, 7 days a week when the host is in a non-UP or Recovery state.

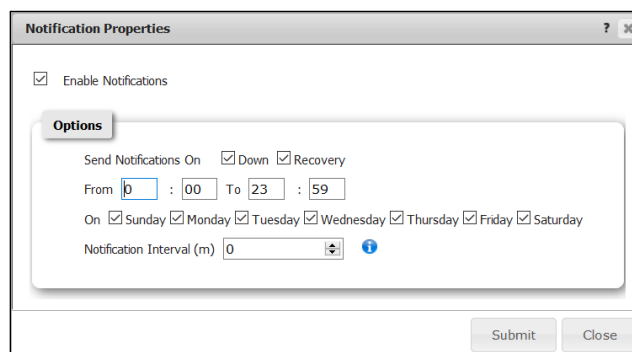


Figure 7-83

Select one service in the Service View table, execute the **Notification Properties** command and a Notification Properties dialog box pops up. Notifications will be sent 24 hours a day, 7 days a week when the service is in a non-OK or Recovery state.

¹³ The status of the host changes from a non-UP state to another non-UP state will also trigger a problem alert.

¹⁴ The status of the service changes from a non-OK state to another non-OK state will also trigger a problem alert.

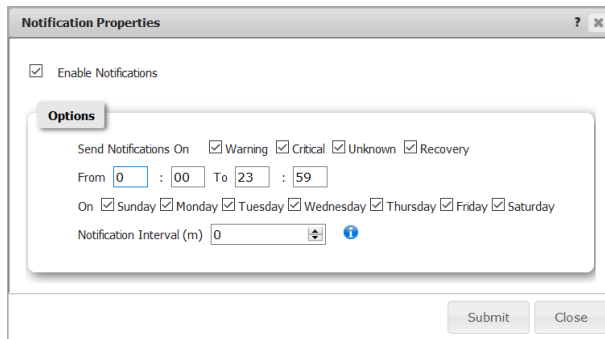


Figure 7-84

7.4.2 Alert Receivers

To receive alerts, you need to define contacts or contact groups and then assign them to the hosts and services. Select one host in the Host View table, execute the **Contact and Contact Group** command and a dialog box pops up. In the figure below, “admin” and “Jack” are DB-Node3 host’s contacts.

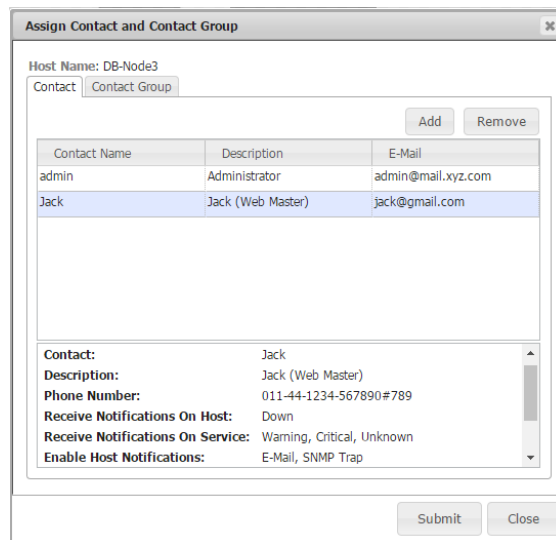


Figure 7-85

Each contact can define its time period and notification methods to receive notifications. See *0 Figure 6-30*

Adding a Contact for details.

When you are unable to receive notifications, use the checklist below to find the possible cause:

- Have any hosts or services had a hard state change?
- Is notification enabled for hosts or services?
- Have hosts or services been assigned to contacts or contact groups?
- Have the notification options (Down and Recovery for Hosts; Warning, Unknown, Critical and Recovery for Services) for hosts or services been checked?

-
- Has the notification period for hosts or services expired?
 - Have the notification options (Down and Recovery for hosts; Warning, Unknown, Critical and Recovery for services) for the contact been checked?
 - Has the notification period for the contact expired?

7.4.3 Alert Format

The message format in E-Mail and SNMP trap are defined by the following attributes:

Item 1: the address of the SSM Server sending notifications

Item 2: the type of alert (“Problem”, “Recovery”)

Item 3: the information of the monitored item (host name, host address, service name, etc.)

Item 4: the status of the monitored item (“UP”, “DOWN”, “OK”, “Warning”, “Critical” or “Unknown”)

Item 5: the time of an alert in date time format

Item 6: the output message about the status of the monitored item

7.4.4 Supermicro MIB

The Supermicro proprietary management information bases (MIBs) subtree begins from .1.3.6.1.4.1.10876. Please find a file named **SSM_MIB.zip** on your SSM CD to get detailed SNMP MIB/OID information.

- **SUPERMICRO-SMI.my:** The file contains Supermicro MIB information used by SuperDoctor®, SuperDoctor 5 and SSM.
- **SUPERMICRO-HEALTH-MIB.my:** The file contains HEALTH MIB module used by SuperDoctor® and SuperDoctor 5.
- **SUPERMICRO-SSM-MIB.my:** The file contains SSM MIB module used by SSM.
- **SUPERMICRO-SD5-MIB.my:** The file contains SSM MIB module used by SuperDoctor 5.
- **xtree.txt:** The file represents HEALTH, SD5 and SSM module structure in tree structure format.
- **xiden.txt:** The file represents HEALTH, SD5 and SSM module structure in identifier format.

Several trap OIDs have been defined in the SSM-MIB file to identify different service state changes. The figure below indicates that SSM will trigger a `trapStorageHealthStatusCritical` alert if the status of Storage Health service changes from an OK state to a CRITICAL state.

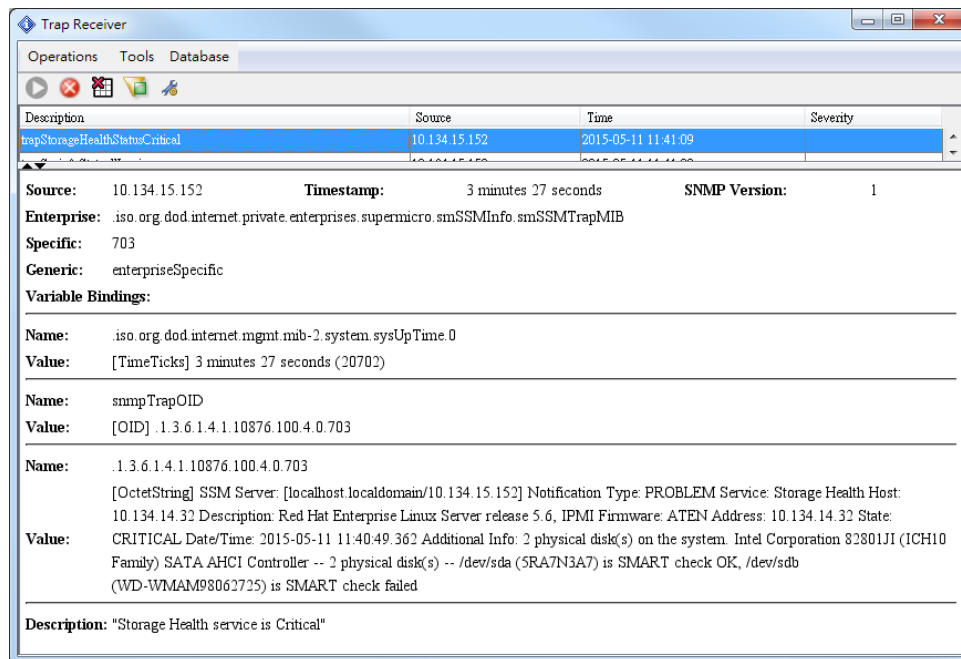


Figure 7-86

8 SSM Web Reporting Page

8.1 SSM Server Report

Three reports related to the SSM Server are supported:

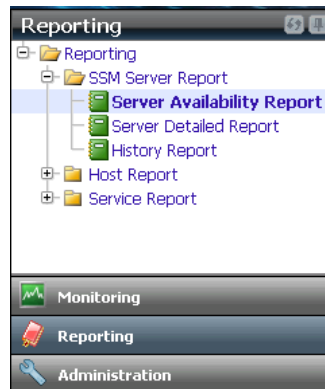


Figure 8-1

- **Server Availability Report:** Shows the availability of the SSM Server over time.
- **Server Detailed Report:** Shows the records over a time period in which the SSM Server was started and stopped.
- **History Report:** Shows the historical monitoring records that the SSM Server stores in the SSM Database when it checks hosts and services. Each record includes the **host name**, **service name**, **state time**, **state**, **state type**, **attempt**, and **status** information.

8.1.1 Server Availability Report

Click **Reporting** → **SSM Server Report** → **Server Availability Report** to use the Server Availability Report function. At the top of the working area, you can set the time period of the availability report by modifying the year and month options. When completed, click the **Query** button to generate the report. Note that in the availability report, the **Time Up** column indicates the total time in a period (one day) that the SSM Server was running. By contrast, the **Time Down** column shows the total time the SSM Server was not running.

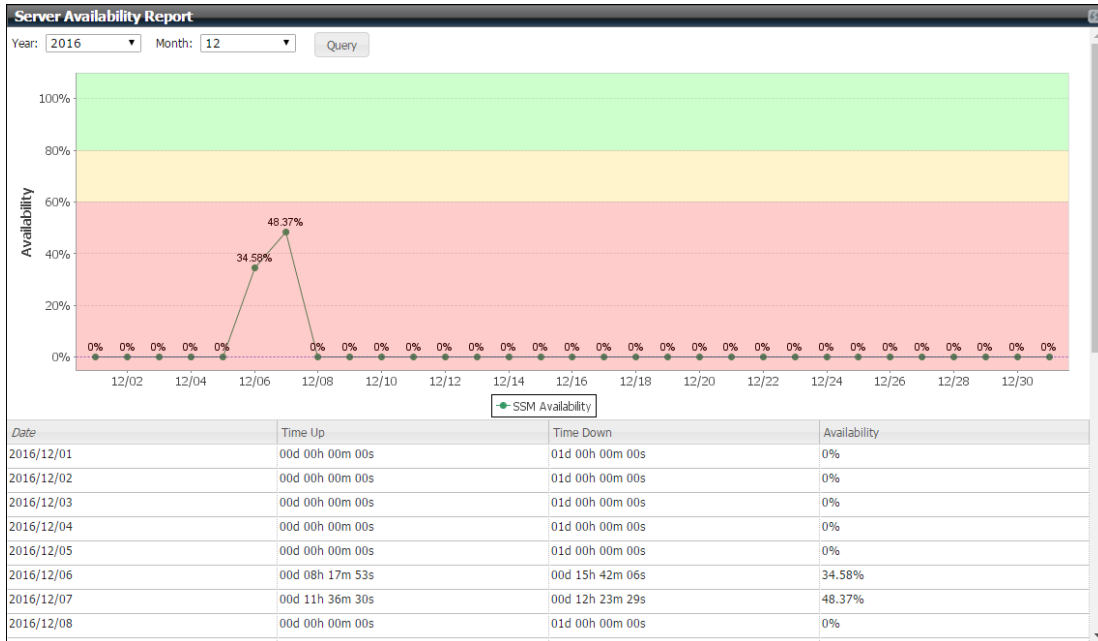


Figure 8-2

8.1.2 Server Detailed Report

Click **Reporting** → **SSM Server Report** → **Server Detailed Report** to use the Server Detailed Report function. At the top of the working area you can set the time period of the detail report and click the **Query** button to generate the report. In this report, the **Start Date** and the **Stop Date** columns indicate the date the SSM Server was started and stopped, respectively. The **Duration** column shows the total time in a session that the SSM Server was started and stopped.

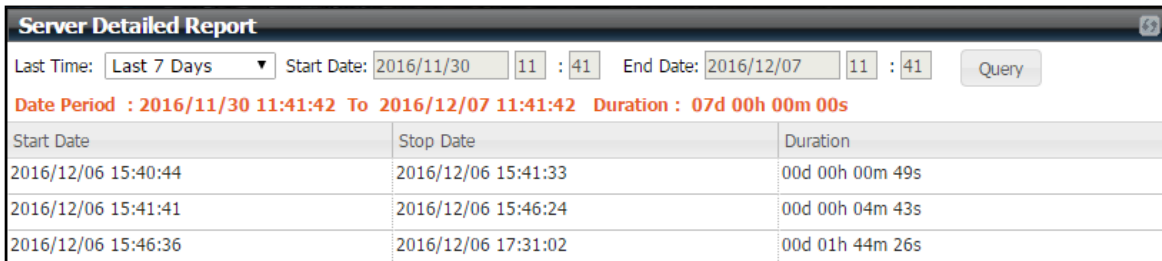


Figure 8-3

8.1.3 History Report

Click **Reporting** → **SSM Server Report** → **History Report** to use the History Report function. At the top of the working area you can set the time period and click the **Query** button to generate the report.

The screenshot shows the 'History Report' window with the following configuration: History Type: State History, Monitor: All, State: All State, State Type: All State Type, Last Time: Last 24 Hours, Start Date: 2016/12/06 11:43, End Date: 2016/12/07 11:43. The table below displays the results of the query.

Host Name	Service Name	State Time	State	State Type	Attempt	Status Information
10.146.20.23	IPMI Sensor Health	2016/12/06 15:41:43	Critical	HARD	1/1	Checked:18, OK:17, Critical:1 Critical items: Chassis Intru=Bad;
10.146.125.60	IPMI SEL Health	2016/12/06 15:41:48	Critical	HARD	1/1	SEL needs attention; 12/06/2016 07:28:45, Critical Interrupt, Bus Correctable Error, Bus00(DevFn02) 12/06/2016 07:28:44, Critical Interrupt, Bus Fatal Error, Bus00(DevFn00) 12/06/2016 07:28:43, Critical Interrupt, Bus Uncorrectable Error, Bus03(DevFn00) 1
10.146.125.40	IPMI SEL Health	2016/12/06 15:41:50	Critical	HARD	1/1	SEL needs attention; 12/06/2016 07:28:52, Critical Interrupt, Bus Correctable Error, Bus00(DevFn02) 12/06/2016 07:28:51, Critical Interrupt, Bus Fatal Error, Bus00(DevFn00) 12/06/2016 07:28:50, Critical Interrupt, Bus Uncorrectable Error, Bus03(DevFn00) 1
10.146.125.113	IPMI SEL Health	2016/12/06 15:41:50	Critical	HARD	1/1	SEL needs attention; 12/06/2016 07:28:57, Critical Interrupt, Bus Correctable Error, Bus00(DevFn02) 12/06/2016 07:28:56, Critical Interrupt, Bus Fatal Error, Bus00(DevFn00) 12/06/2016 07:28:55, Critical Interrupt, Bus Uncorrectable Error, Bus03(DevFn00) 1
10.146.125.137	IPMI SEL Health	2016/12/06 15:41:51	Critical	HARD	1/1	SEL needs attention; 12/06/2016 15:29:09, Critical Interrupt, Bus Correctable Error, Bus00(DevFn02) 12/06/2016 15:29:08, Critical Interrupt, Bus Fatal Error, Bus00(DevFn00) 12/06/2016 15:29:07, Critical Interrupt, Bus Uncorrectable Error, Bus03(DevFn00) 1

Figure 8-4

8.2 Host Report


Four types of host reports are supported:

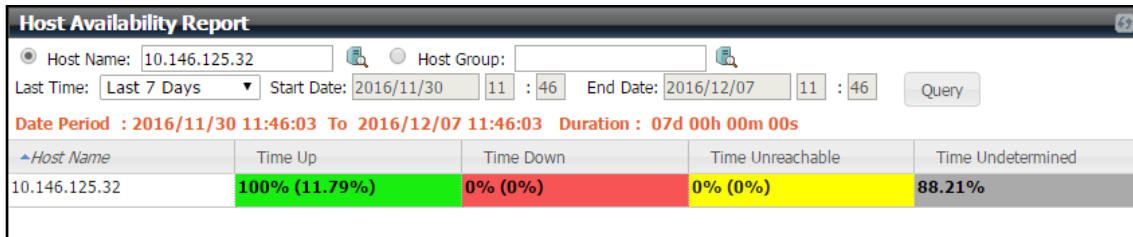


Figure 8-5

- **Host Availability Report:** Shows an availability report of hosts or host groups.
- **Single Host Status Report:** Shows the percentages of the three status types of a host (up, down, and unreachable) over a time period. This information is calculated on a daily basis.
- **Single Host with Service Status Report:** This is similar to the **Single Host Status Report** except that it includes the status of all services in a host.
- **Host Status Detailed Report:** This draws a diagram to show every status change of a host over time.

8.2.1 Host Availability Report


Click **Reporting** → **Host Report** → **Host Availability Report** to use the Host Availability Report function. At the top of the working area you can click the  icon to select the hosts to be included in the report and set the time period by modifying the **Last Time** or the **Start Date**, as well as the **End Date** options. When completed, click the **Query** button to generate the report. In the host availability report, the **Time Up**, **Time Down**, and **Time Unreachable** columns show the percentage by time over the specified time period in which a host was running, not running, and unreachable, respectively. The **Time Undetermined** column indicates the percentage by time during the specified time period in which the SSM Server was not running. If you specify a time period in the past or in the future in which the SSM Server was not or will be not running, then there is no way to determine the status of a monitored host. In such cases, the percentage of time is displayed in the **Time Undetermined** column.



Host Name	Time Up	Time Down	Time Unreachable	Time Undetermined
10.146.125.32	100% (11.79%)	0% (0%)	0% (0%)	88.21%

Figure 8-6

8.2.2 Single Host Status Report

Click **Reporting** → **Host Report** → **Single Host Status Report** to use the Single Host Status Report function. At the top of the working area you can click the  icon to select a host to be included in the report and set the time period by modifying the **Year** and the **Month** options. You can choose the generated graphic style by selecting the **Stacked Bar Chart** radio button or the **Line Chart** radio button. Any undetermined time will be included if you click the **Include undetermined** check box. When completed, click the **Query** button to generate the report.

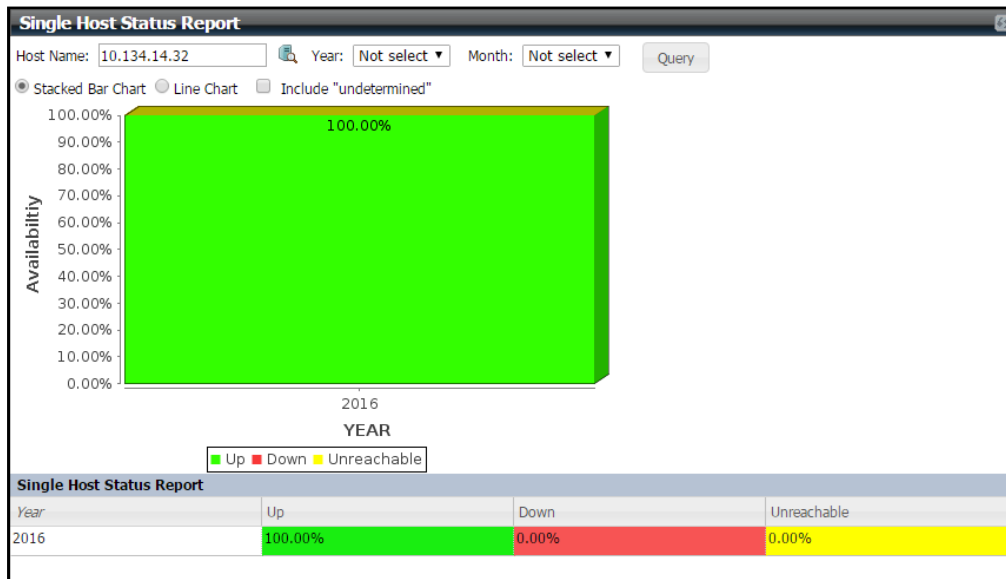



Figure 8-7

8.2.3 Single Host with Services Status Report

Click **Reporting** → **Host Report** → **Single Host with Services Status Report** to use the Single Host with Services Status Report function. At the top of the working area you can click the  icon to select a host with all its services to be included in the report and set the time period by modifying the **Last Time** and the **Start Date** as well as the **End Date** options. You can choose the generated graphic style by selecting the **Bar Chart** radio button or the **Pie Chart** radio button. When completed, click the **Query** button to generate the report.

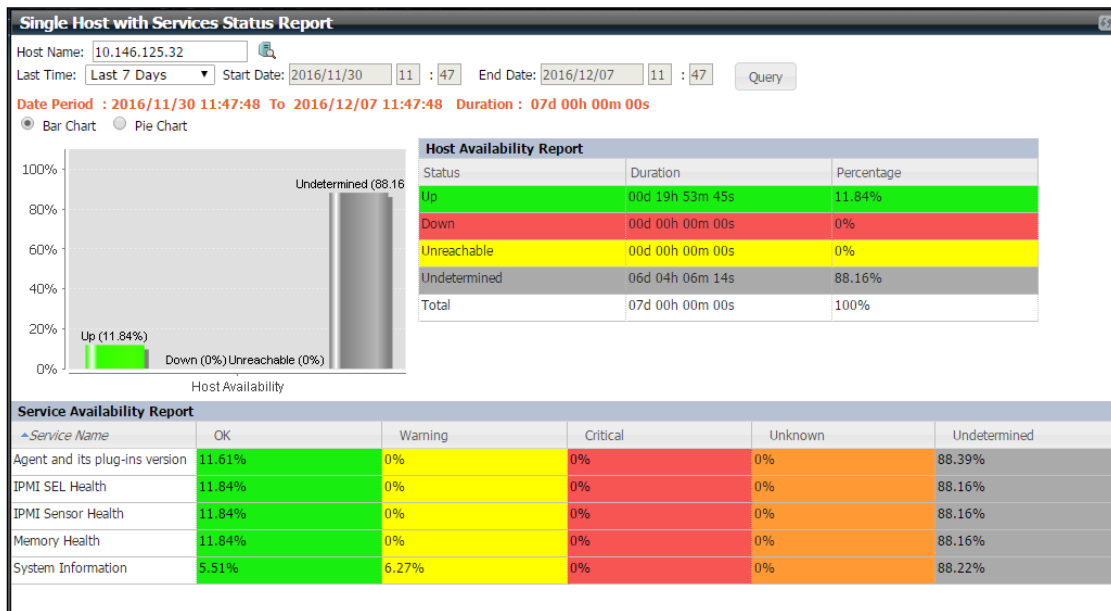



Figure 8-8

8.2.4 Host Status Detailed Report

Click **Reporting** → **Host Report** → **Host Status Detail Report** to use the Host Status Detailed Report function. At the top of the working area you can click the  icon to select a host to be included in the report and set the time period by modifying the **Last Time** and the **Start Date** as well as the **End Date** options. When completed, click the **Query** button to generate the report.

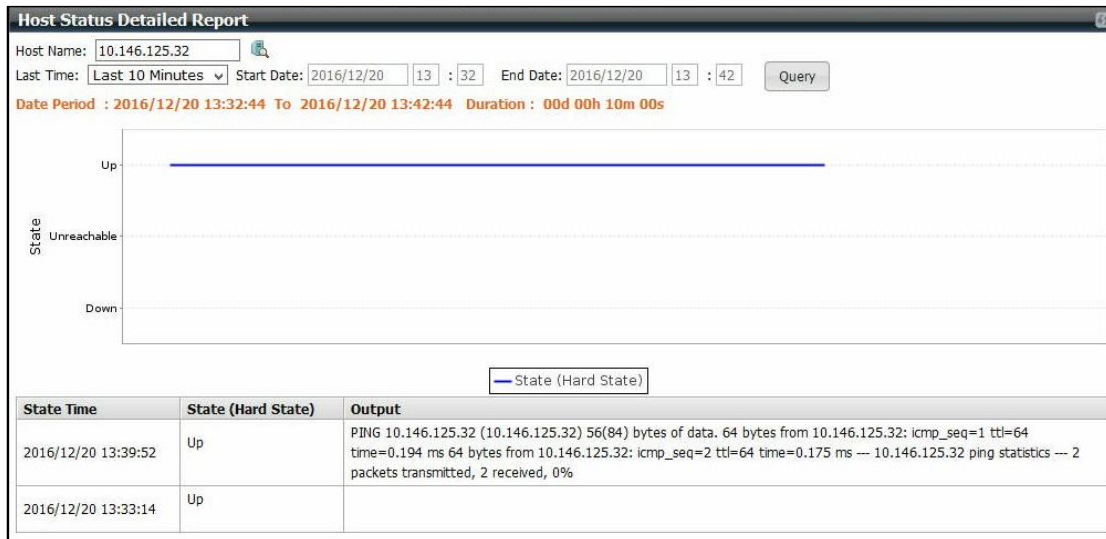


Figure 8-9

8.3 Service Report

Three types of service reports are supported:

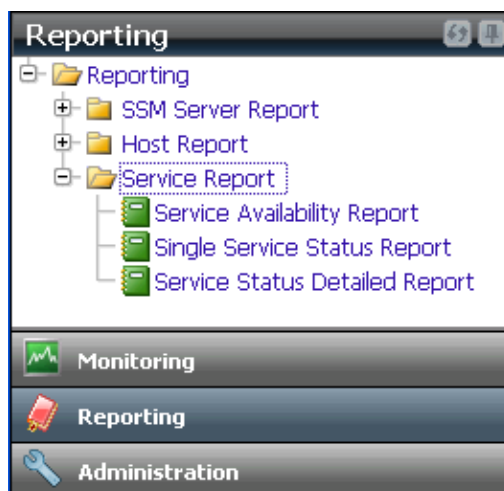



Figure 8-10

- **Service Availability Report:** Shows the availability records of services belonging to the selected hosts or host groups.
- **Single Service Status Report:** This shows the percentages of the four status types of a service (OK, warning, unknown, and critical) in a time period. This information is calculated on a daily basis.
- **Service Status Detailed Report:** This draws a diagram to show every status change of a service over time.

8.3.1 Service Availability Report

Click **Reporting** → **Service Report** → **Service Availability Report** to use the Service Availability Report function. At the top of the working area you can click the  icon to select the hosts to be included in the report and set the time period by modifying the **Last Time** or the **Start Date** as well as the **End Date** options. When completed, click the **Query** button to generate the report.

In this report, the **Time OK**, **Time Warning**, **Time Unknown** and **Time Critical** columns show the percentage of time in the specified time period in which the status of a service was normal, warning, unknown, and critical, respectively. The **Time Undetermined** column indicates the percentage of time in the specified time period in which the SSM Server was not running. If you specify a time period in the past or in the future in which the SSM Server was not, or will be not running, then there is no way to determine the status of a monitored service. In such cases, the percentage of time is displayed in the **Time Undetermined** column.

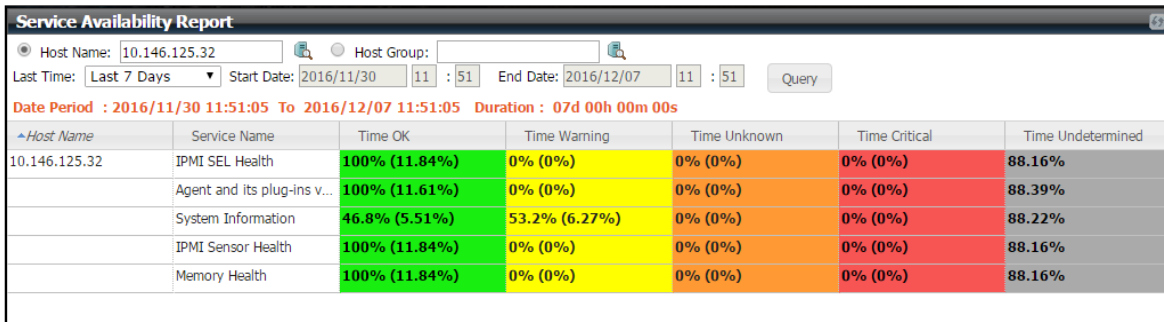


Figure 8-11

8.3.2 Single Service Status Report

Click **Reporting** → **Service Report** → **Single Service Status Report** to use the Single Service Status Report function. At the top of the working area first click the icon to select a host and then select a service from the **Service** drop-down list to be included in the report. You can set the time period by modifying the **Year** and the **Month** options. You can choose the generated graphic style by selecting the **Stacked Bar Char** radio button or the **Line Chart** radio button. Undetermined time will be included if you click the **Include undetermined** check box. When completed, click the **Query** button to generate the report.

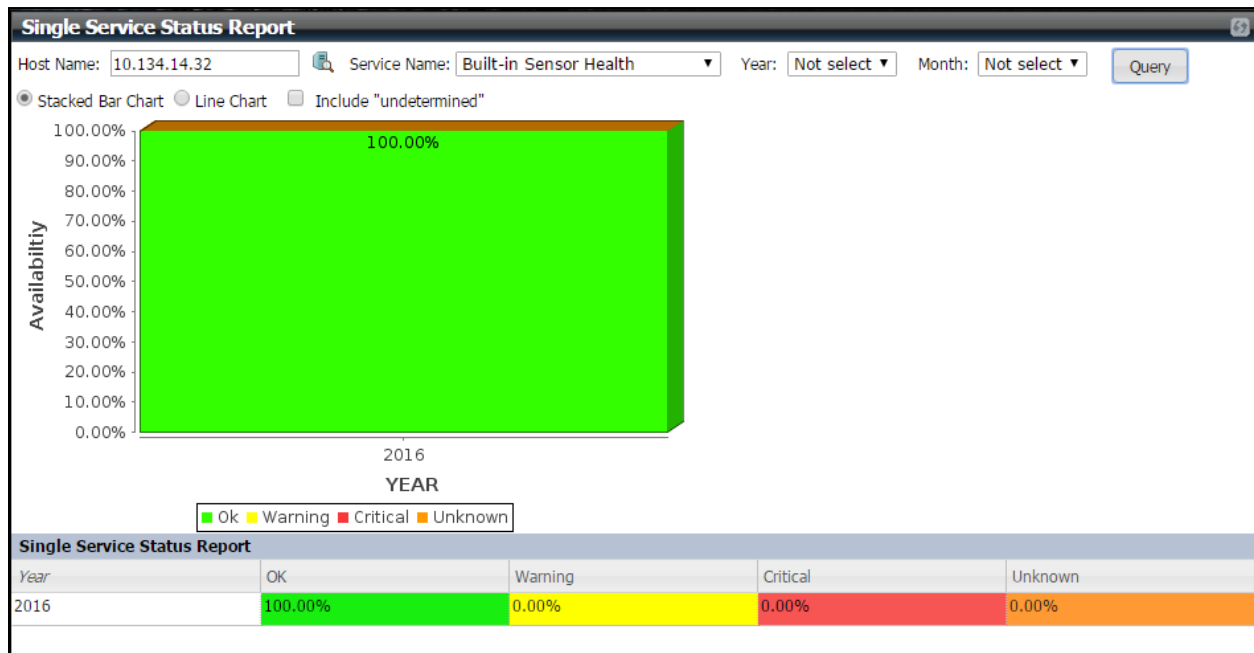



Figure 8-12

8.3.3 Service Status Detailed Report

Click **Reporting** → **Service Report** → **Service Status Detailed Report** to use the Service Status Detailed Report function. At the top of the working area first click the  icon to select a host and then select a service from the **Service** drop-down list to be included in the report. You can set the time period by modifying the **Last Time** and the **Start Date** as well as the **End Date** options. When completed, click the **Query** button to generate the report.

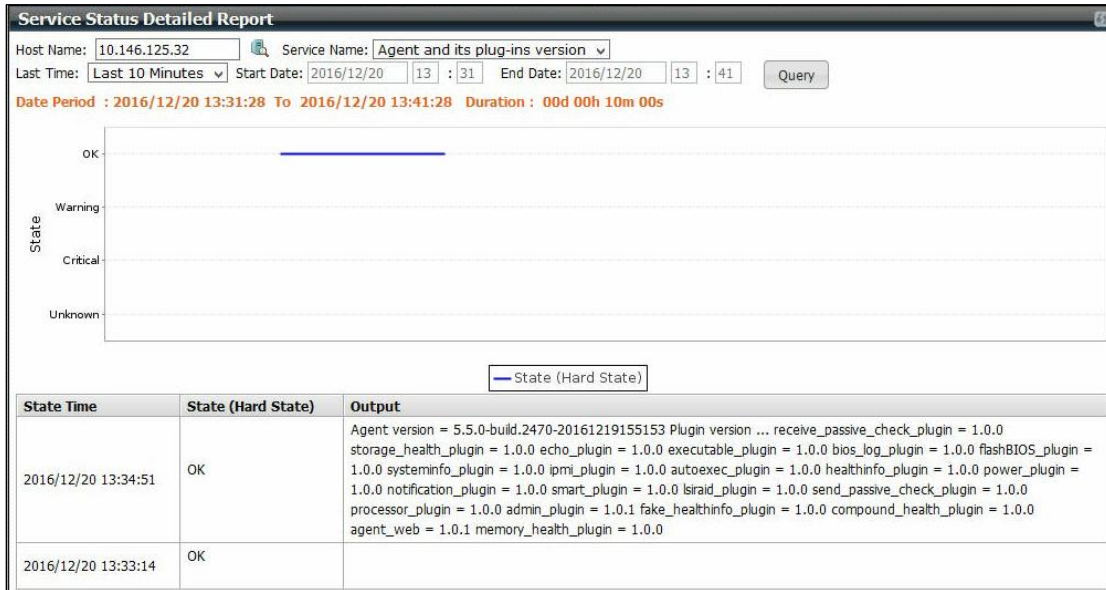


Figure 8-13

9 Power Management

9.1 Power Management in SSM

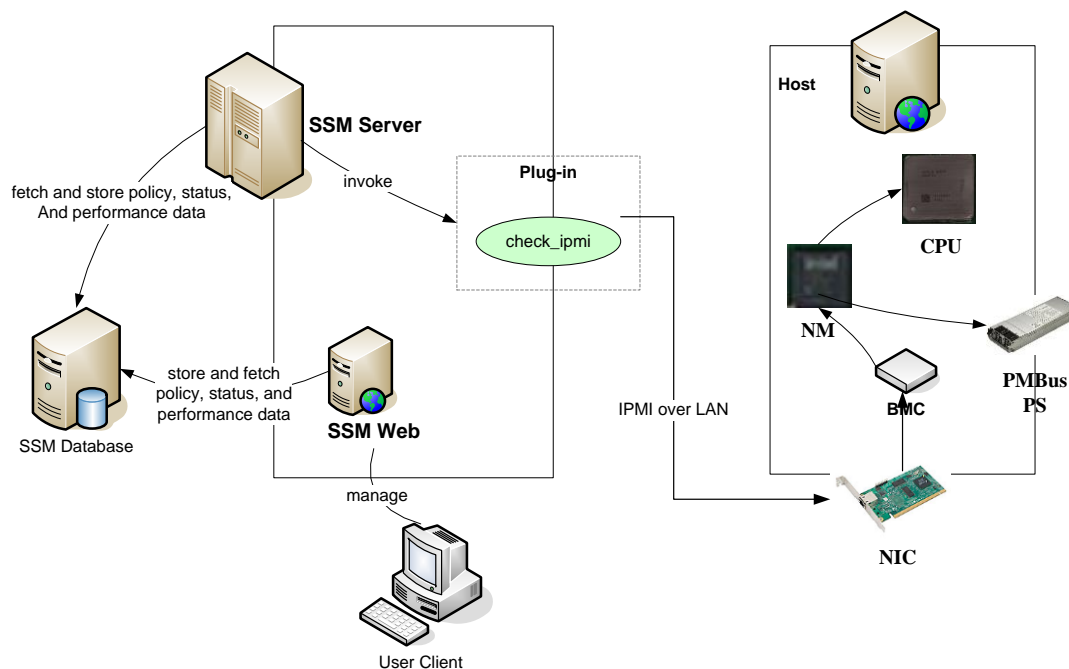


Figure 9-1

SSM enables you to monitor and manage power consumption for Intel® Intelligent Power Node Manager (NM) equipped hosts. As shown below, the SSM Server gets power consumption readings from NM via BMC, using IPMI over LAN and stores power consumption as well as performance data in the SSM Database. Users can use the data to view power consumption trends on the SSM Web interface.

Users can cap power consumption across individual hosts and groups of hosts by assigning policies on individual hosts or host groups via the SSM Web interface. The SSM Server will be notified about the newly added policies and calculate a power limit for each individual host and groups of hosts. Then, the SSM Server sets a power limit policy on the NM of each host, allowing the NM to control the host's power consumption. The NM is responsible for achieving the assigned power limit by adjusting the CPU's P-State and T-State according to the real-time power consumption data reading from the PMBus instrumented power supply.

To use the SSM power management functions, your hosts must have a **BMC**, a **PMBus instrumented power supply**, and support **NM 1.5**. When you use the Host Discovery Wizard to add an IPMI host and enable the NM detection check box, the SSM Web will determine whether a discovered host supports NM or not. If a discovered host supports NM, the NM host type is assigned to the host and the built-in Power Consumption service is added as well, which is used to periodically gather the raw power consumption data of a host. The SSM Web uses this raw data to draw the power consumption trend of a host and a group of hosts. **To summarize, only NM hosts and the built-in Power Consumption service support the power management functions. The power management functions will not work correctly if an NM host's Power Consumption service is not working (e.g., has been removed by users).**

9.2 Power Consumption Trend

Before you start to set a policy to cap the power consumption of individual hosts or a group of hosts, you can use the Power Consumption Trend function to determine a power limit for each host. The Power Consumption Trend can also be used to observe the real-time and historical power consumption of individual hosts or a group of hosts.

9.2.1 Power Consumption Trend of Individual Hosts

Host View					Commands
Host Status: All Status					> IPMI
					> Agent Managed
					> Power Management
					> Power Consumption Trend
					> Power Policy Management
					> System Information

Host Status	Service Status	Host	Host Type	Address
Up	OK	DB-Node3	Agent Managed,IPMI,Linux,NM	192.168.12.32
Up	OK	DB-Node1	IPMI,NM	192.168.12.8
Up	OK	DB-Node2	IPMI,NM	192.168.12.13

Figure 9-2

Select an NM host (a host with the NM Host Type) on the Monitoring page and click the Power Consumption Trend command. A Power Consumption Trend window pops up as shown below.

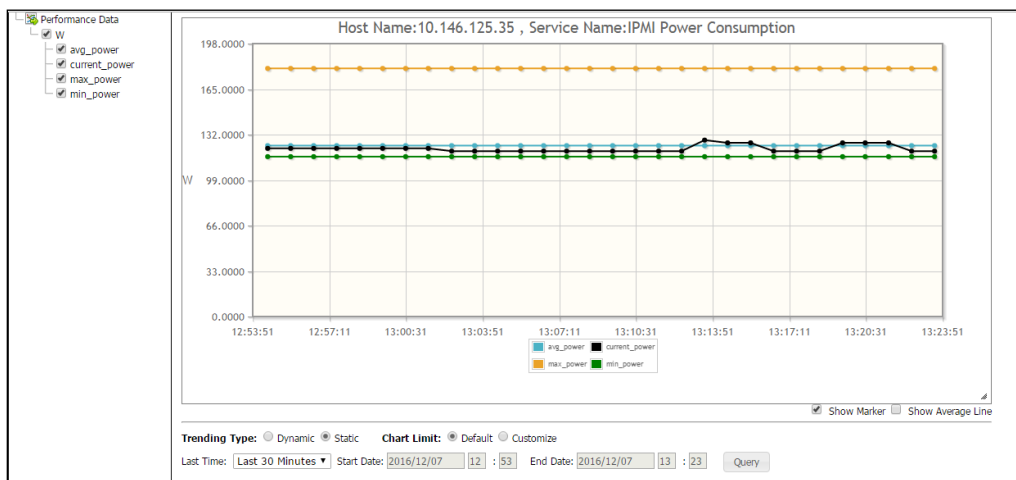


Figure 9-3

One item is supported and shown on the left side of the Power Consumption Trend window:

- **current_power**: The current power trend of the power supply used by the monitored NM host.
- **max_power**: The maximum power trend of the power supply used by the monitored NM host.
- **min_power**: The minimum power trend of the power supply used by the monitored NM host.
- **avg_power**: The average power trend of the power supply used by the monitored NM host.

The values are sampled from the NM and stored in the SSM Database every time the Power Consumption service is executed by the SSM Server. You can change the sampling frequency by setting the **Check Interval** attribute of the Power Consumption service.

Two trending types are supported:

- **Dynamic:** Shows the dynamic power consumption trend. The power consumption trend graph automatically refreshes periodically to include new power consumption data.
- **Static:** Shows the static (historical) power consumption trend based on the specified display period. Newly added power consumption data is not illustrated in the static power consumption trend graph after this graph is generated.

9.2.2 Power Consumption Trend of a Group of Hosts

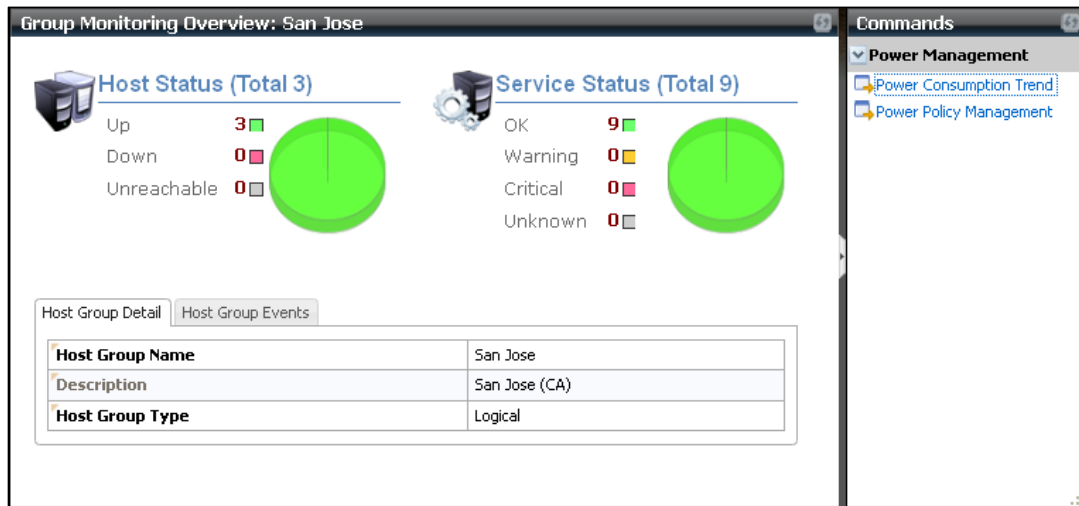


Figure 9-4

This function is similar to the Power Consumption Trend of Individual Hosts except that it shows the power consumption trend of a group of hosts. To use this function, select a host group on the Monitoring page and click the Power Consumption Trend command.

9.3 Power Policy Management

This function allows users to define power capping policies for individual NM hosts or a group of NM hosts. A policy is either permanent or scheduled. A permanent policy takes effect all the time once it is enabled. A scheduled policy is activated when it enters its scheduled time period and deactivated when it leaves its scheduled time period. See 3.3.9 *PTPolicy Definitions* for more information.

9.3.1 Host Policies

1. Select a NM host and execute the Power Policy Management command.

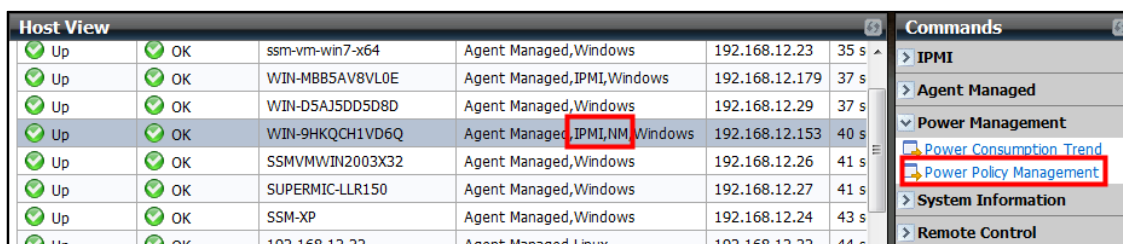


Figure 9-5

2. A Power Policy Management dialog pops up as shown below. This dialog shows existing policies of the selected NM host. Click the **Add** button to create a new policy.

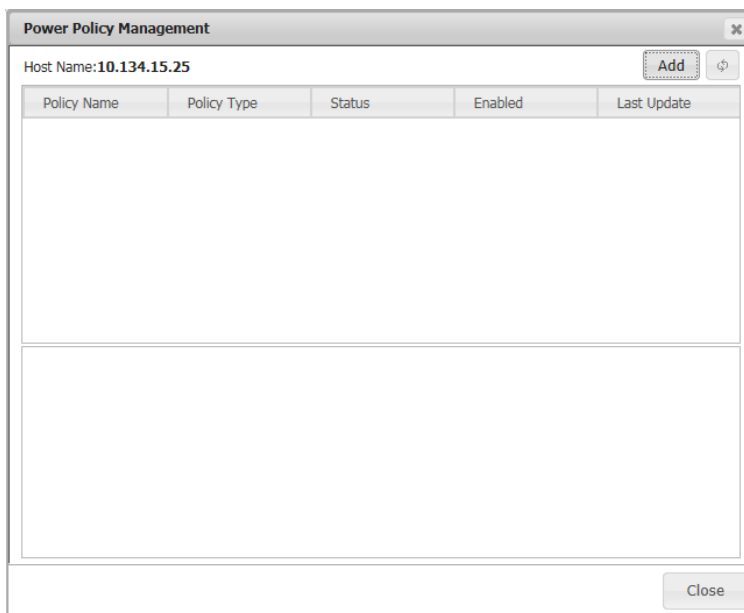
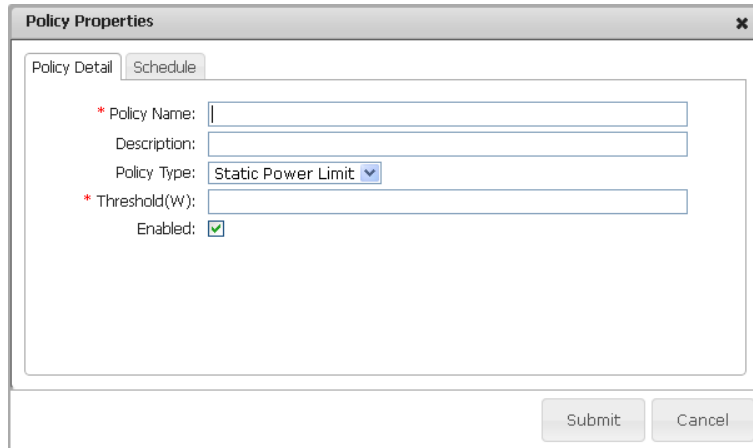


Figure 9-6

3. A Policy Properties dialog pops up as shown below. The **Threshold** attribute defines the power capping value for the host. In other words, the host is not supposed to consume more power than the specified threshold value. If the **Enabled** attribute is not set, the SSM Server will not handle this policy after it is created.



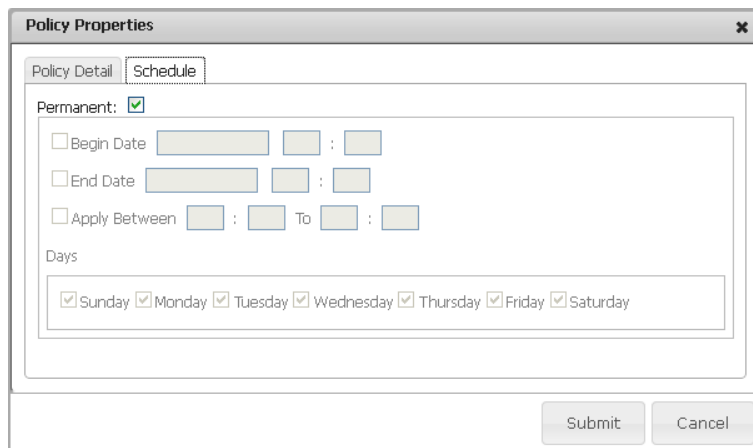
The screenshot shows the 'Policy Properties' dialog box with the 'Policy Detail' tab selected. The dialog contains the following fields and controls:

- * Policy Name:** A text input field.
- Description:** A text input field.
- Policy Type:** A dropdown menu with 'Static Power Limit' selected.
- * Threshold(W):** A text input field.
- Enabled:** A checked checkbox.

At the bottom right, there are 'Submit' and 'Cancel' buttons.

Figure 9-7

4. To modify a policy's schedule attribute, click the **Schedule** tab. A policy is permanent by default, which means it takes effect all the time. Uncheck the **Permanent** checkbox to create a scheduled policy.



The screenshot shows the 'Policy Properties' dialog box with the 'Schedule' tab selected. The dialog contains the following fields and controls:

- Permanent:** A checked checkbox.
- Begin Date:** An unchecked checkbox followed by a date and time input field.
- End Date:** An unchecked checkbox followed by a date and time input field.
- Apply Between:** An unchecked checkbox followed by two time input fields separated by 'To'.
- Days:** A list of days with checkboxes: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. All are checked.

At the bottom right, there are 'Submit' and 'Cancel' buttons.

Figure 9-8

A scheduled policy is determined by the following attributes:

- **Begin Date:** When the policy begins to take effect. If the Begin Date is not specified, the policy takes effect immediately (from the day the policy is created).
- **End Date:** When the policy ends. If the End Date is not specified, the policy never expires.
- **Apply Between:** Which time in a day the policy takes effect. If the Apply Between is not specified,

- the policy takes effect all day long (24 hours a day).
- **Days:** Which days in a week the policy takes effect.



Note: As shown below, if all the above attributes are not specified, a permanent policy will be created even if the **Permanent** checkbox is unchecked.

Policy Properties

Policy Detail | Schedule

Permanent:

Begin Date 2016/12/07 13 : 28

End Date 2016/12/07 13 : 28

Apply Between 0 : 00 To 23 : 59

Days

Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Submit Close

Figure 9-9

5. Click the **Submit** button to add the policy and the Policy Properties dialog will be closed. In the Power Policy Management dialog, you can see a “The policy is adding to NM” message, which means that the policy is adding to the SSM Database. At this time, the policy is still waiting to be added to the NM by the SSM Server. Thus, its **Active** status is **No**.

Power Policy Management

Host Name: 10.134.15.25 Add Modify Delete

Policy Name	Policy Type	Status	Enabled	Last Update
p1-500w	Static Power Limit	OK	Yes	2016/12/07 13:31:04

Policy Name: p1-500w

Description:

Policy Type: Static Power Limit

Threshold(W): 500

Status: OK

Message: The policy is adding to NM.

Enabled: Yes

Permanent: Yes

Active: No

Close

Figure 9-10

The **Active** status becomes **Yes** after the SSM Server successfully adds the policy to the NM. You can see the message “The policy is added to NM successfully” in the dialog.

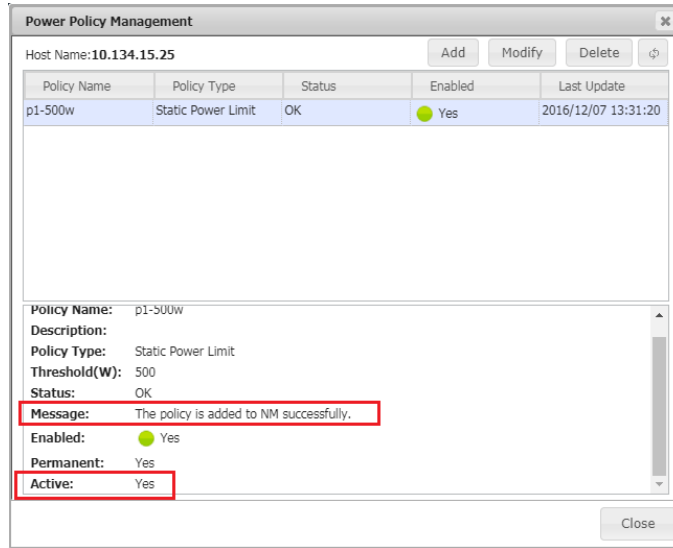


Figure 9-11

9.3.2 Host Group Policies

1. Select a host group and execute the Power Policy Management command.

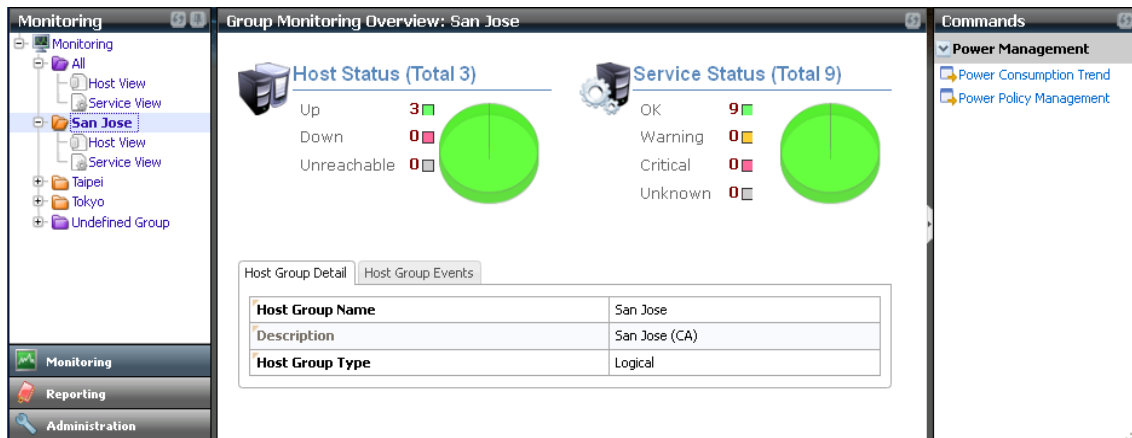


Figure 9-12

2. A Power Policy Management dialog pops up as shown below. This dialog shows the existing policies of the selected NM host group. Click the **Add** button to create a new policy.

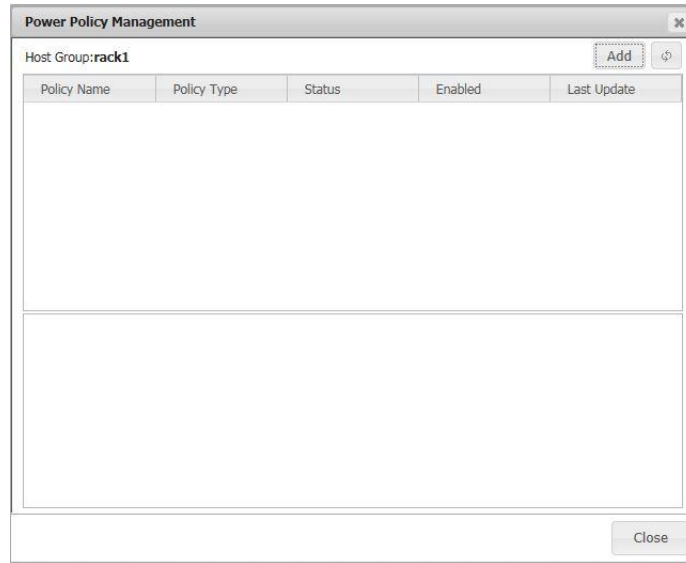


Figure 9-13

3. A Policy Properties dialog pops up as shown below. The **Threshold** attribute defines the power capping value for the group. The **Reserve Budget** attribute, which is not available in the host policy function, defines a reserve power value that will not be allocated to NM hosts in this group. In other words, the actual power capping value equals the Threshold minus the Reserve Budget, which is called the **effective power budget** in SSM. For example, a group policy has a Threshold of 1000 W and a Reserve Budget of 200 W. Only 800 W (the effective power budget) will be allocated to all NM hosts in the group. All NM hosts in this host group are not supposed to consume more power than the effective power budget. If the **Enabled** attribute is not set, the SSM Server will not handle this policy after it is created.

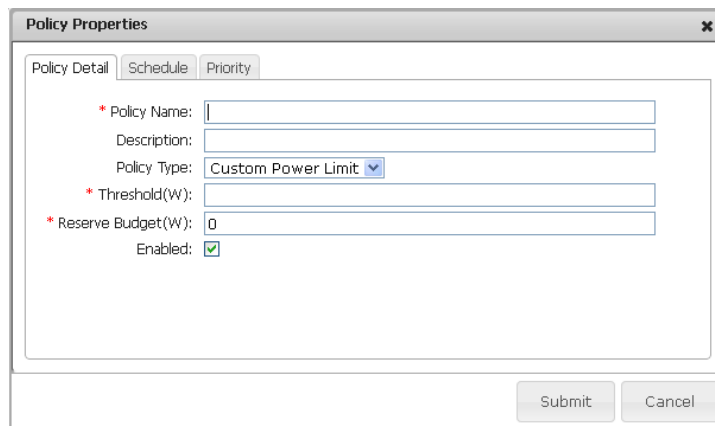
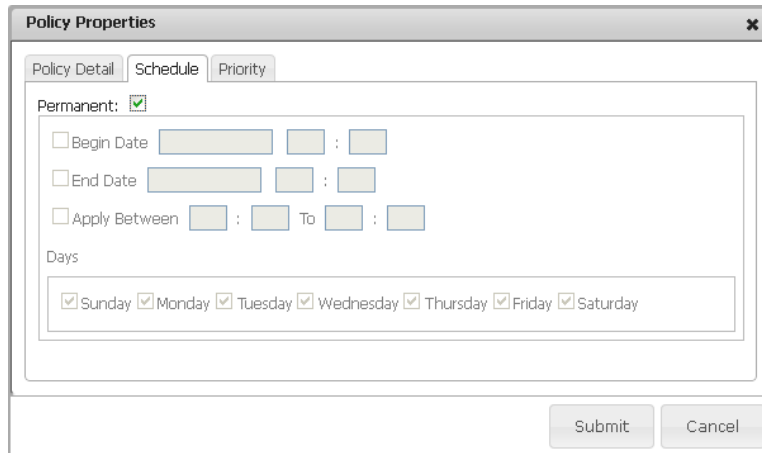


Figure 9-14

The purpose of the Reserve Budget attribute is to reserve power for non-NM hosts located in a host group. For example, suppose that there are ten hosts in a host group named DB-Servers. Eight are NM hosts and two are non-NM hosts. Your power budget for the entire DB-Servers group is 2000W, which is supposed to be equally allocated to each host in the group (i.e., 200W per host). If you add a policy with a Threshold of 2000W to the host group, each NM host gets 250W (i.e., 2000W / 8 = 250W). The actual power consumption of the DB-Servers group will be greater than 2000W since the power consumption values of other two non-NM hosts are not included. To deal with this situation, you should add a policy with a Threshold 2000W and a Reserve Budget 400W (assuming the other two non-NM hosts consume 400W in total). By so doing, only 1600W (i.e., the effective power budget) is allocated to the eight NM hosts and each of the NM hosts will get a 200W power limit.

4. To modify a group policy's schedule attribute, click the **Schedule** tab. Please refer to the *9.3.1 Host Policies* (Step 4) for more information.



The screenshot shows a 'Policy Properties' dialog box with three tabs: 'Policy Detail', 'Schedule', and 'Priority'. The 'Schedule' tab is active. It contains the following options:

- Permanent:**
- Begin Date:** :
- End Date:** :
- Apply Between:** : To :
- Days:** Sunday Monday Tuesday Wednesday Thursday Friday Saturday

At the bottom right, there are 'Submit' and 'Cancel' buttons.

Figure 9-15

5. Click the **Priority** tab to modify the power consumption priority of all NM hosts in the group. **It is important to notice that only NM hosts are shown in this tab.** If a host group contains non-NM hosts, they are not included in this tab. In fact, the power consumption of non-NM hosts, even they are in the host group, will not be controlled and affected by any host group policy. The SSM will allocate more power to a host with a higher priority than a host with a lower priority.



Note: LOW<MEDIUM<HIGH<CRITICAL.

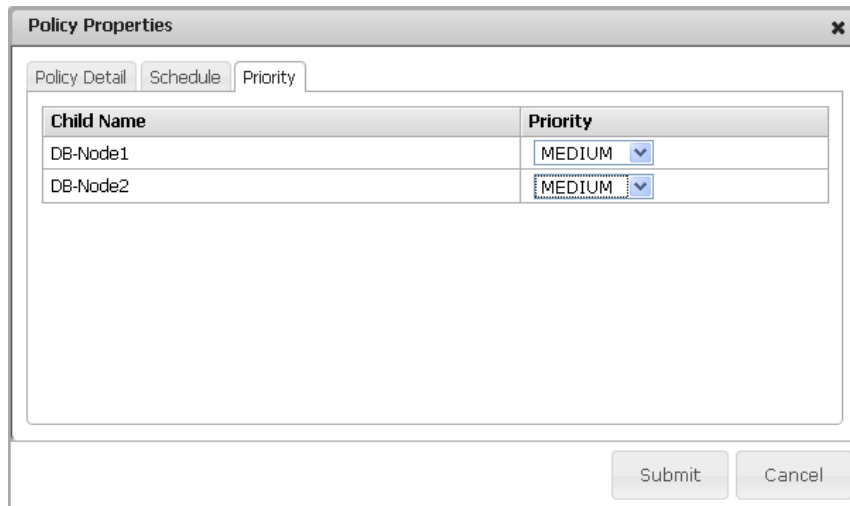


Figure 9-16

- Click the **Submit** button to add the policy and the Policy Properties dialog will be closed. In the Power Policy Management dialog, you can see a “The policy is adding to NM” message, which means that the group policy is adding to the SSM Database. At this time, the policy is still waiting to be added to each NM host in the host group by the SSM Server. Thus, its **Active** status is **No**.

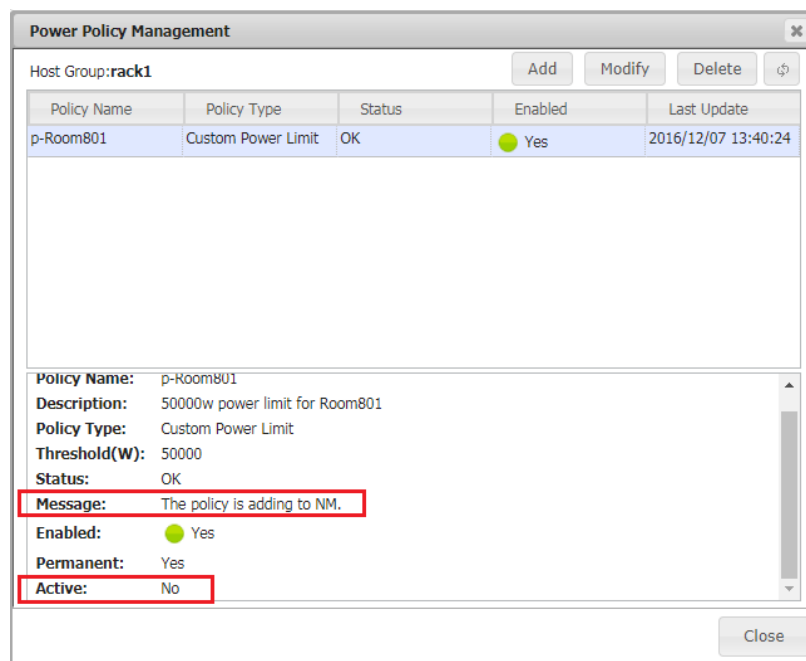


Figure 9-17

When the host group policy is processed by the SSM Server, its **Active** status changes to **Yes**. You can see the message “The policy is processed successfully” in the dialog.

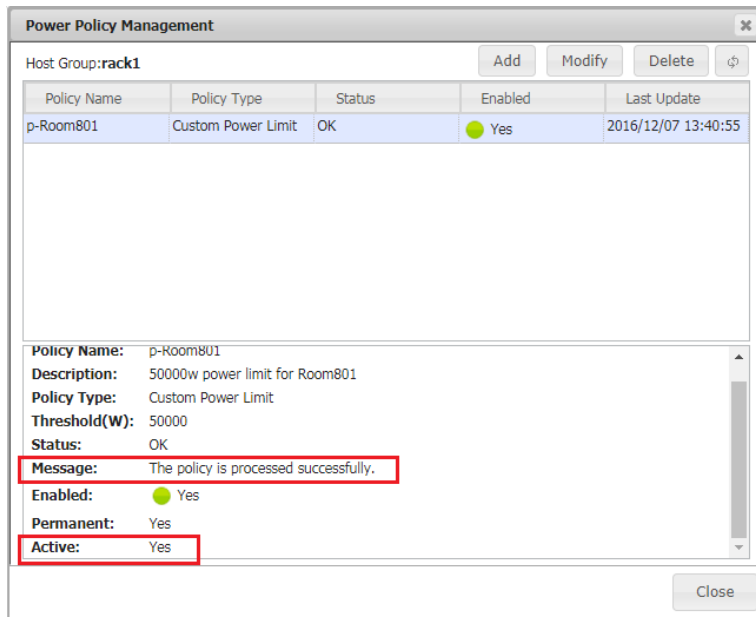


Figure 9-18

9.3.3 Policy Conflicts

When several policies are added to a host and a host group, there may be conflicts among these policies. Conflicts may be caused by the policies of a host or a host group and the interaction among host policies and host group policies. For example, adding two permanent policies to a host (or a host group) causes a conflict since only one permanent policy of a host (or a host group) can be active at any time. The SSM Server will inform users about the conflicts via the SSM Web interface.

9.3.3.1 Conflicts caused by Multiple Enabled Policies

Conflicts happen when several enabled policies are added to a host or a host group. For example, adding two permanent policies to a host or a host group causes a conflict. For another example, adding two scheduled policies to a host or a host group causes a conflict if the scheduled time periods of these two policies overlap. This section shows a conflict example caused by two enabled permanent host policies.

Suppose that a permanent policy named p1-500W for a host named 10.134.15.25 is active. You are adding another permanent policy p2-300W to the 10.134.15.25 host, as shown below.

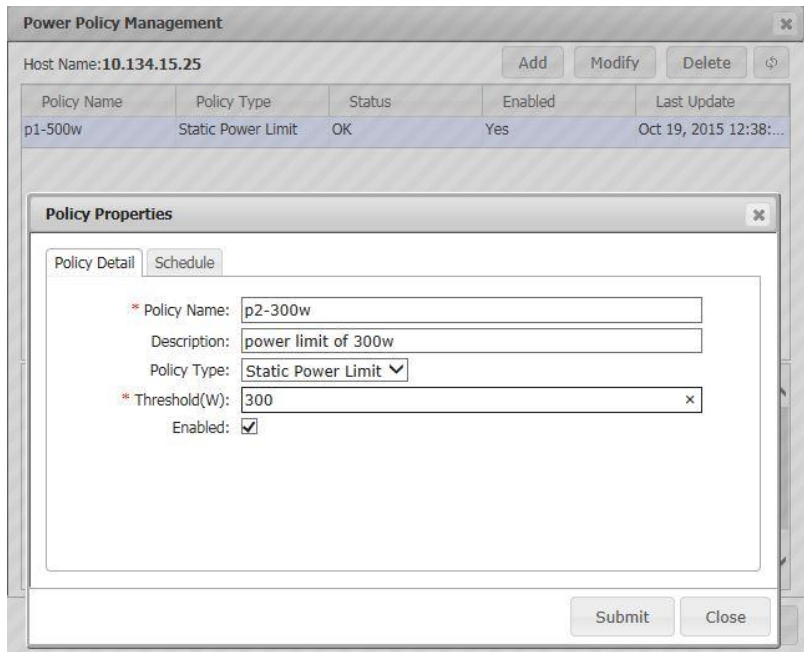


Figure 9-19

After the p2-300W policy was added, the Power Policy Management dialog shows the message “The policy is adding to NM”, which means that it was added to the SSM Database. Right now, the Status of the p2-300W policy is OK.

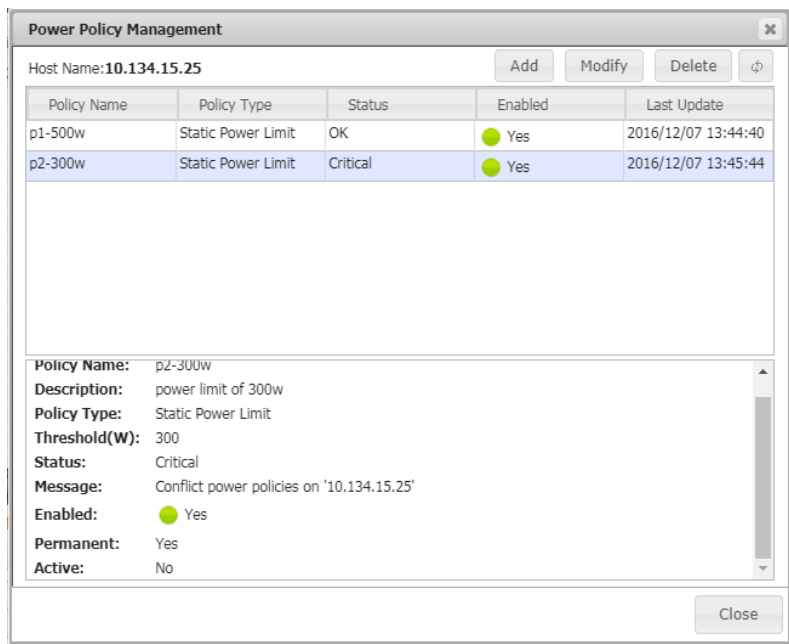


Figure 9-20

A few seconds later, when the SSM Server tries to add the p2-300W policy to the NM, it detects that the p2-300W conflicts with the p1-500W policy. Since only one active policy on a host is allowed at a time and the p1-500W policy is already in the Active state, the p2-300W policy is not activated. In other words, although the p2-300W policy is enabled, it will not be processed by the SSM Server since it is not in the Active state.

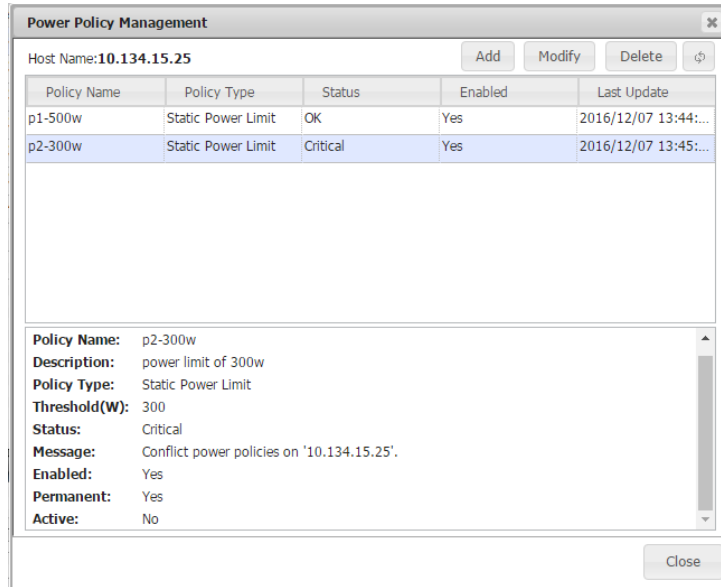


Figure 9-21

However, if you delete the active policy (in this case, the p1-500W policy) and there are other enabled policies on the host, the SSM Server will select a suitable policy and try to activate it automatically.

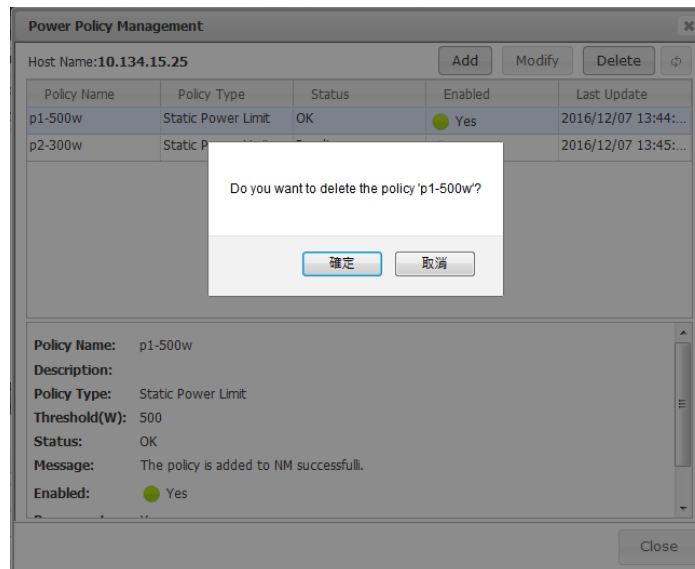


Figure 9-22

You can see that the p1-500W policy was deleted. At this time, the p2-300W policy is not in the Active state yet.

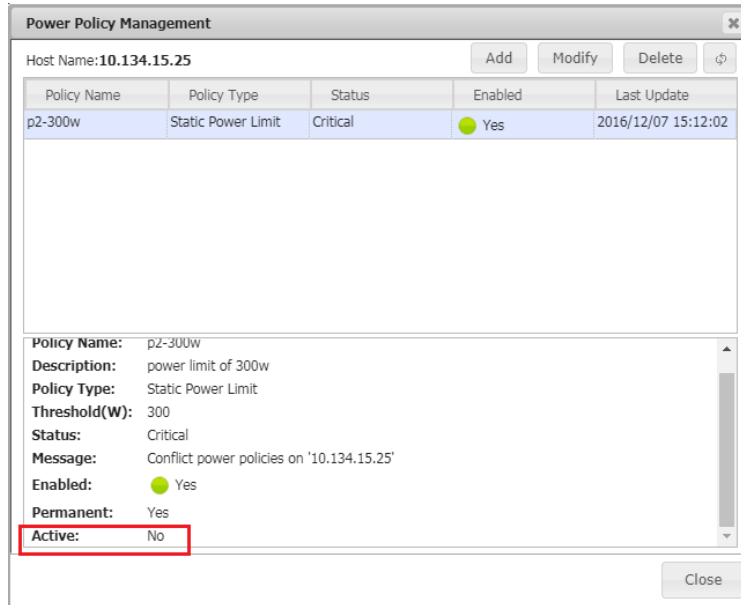


Figure 9-23

Few seconds later, the p2-300W policy is automatically activated by the SSM Server.

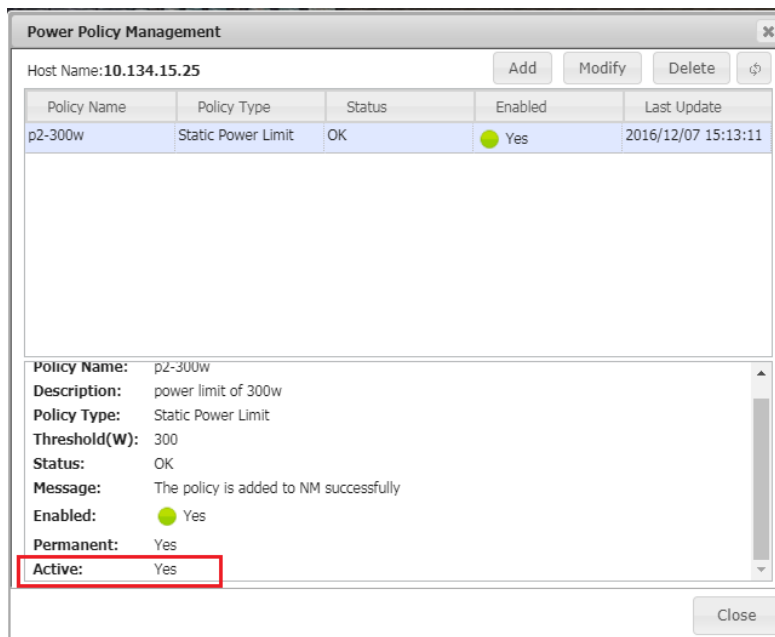


Figure 9-24



Note: Although only host policies are presented, the above situation applies to policies of hosts and hostgroups. It is recommended that only one permanent policy is added to a host/hostgroup at a time. If a host has multiple enabled policies, when the active policy is deleted the SSM Server will iterate all of the enabled policies until one is successfully added to the NM. Such an automatic reactivation process is non-determined; you cannot predict which one will be reactivated if an active policy is removed. Keeping one enabled policy for a host at a time can prevent such non-determined behavior.

9.3.3.2 Conflicts Between a Hostgroup Policy and a Permanent Host Policy

Suppose that a host named DB-Node1 is in the rack1 host group.

Host Status	Service Status	Host	Host Type	Address	
Up	OK	DB-Node3	Agent Managed,IPMI,Linux,NM	192.168.12.32	02
Up	Critical	DB-Node1	IPMI,NM	192.168.12.8	25
Up	OK	DB-Node2	IPMI,NM	192.168.12.13	13

Figure 9-25

DB-Node1 has an active permanent policy named host-p-800w with a threshold of 800W.

Policy Name	Policy Type	Status	Enabled	Last Update
host-p-800w	Static Power Limit	OK	Yes	2016/12/07 15:16:11

Policy Name: host-p-800w
Description: power limit of DB-Node1
Policy Type: Static Power Limit
Threshold(W): 800
Status: OK
Message: The policy is added to NM successfully
Enabled: Yes
Permanent: Yes
Active: Yes

Figure 9-26

You add a new permanent policy named group-p-500w to the rack1 host group. When the policy is processed by the SSM Server, it detects that the policy cannot be calculated because the group-p-500w policy contains the DB-Node1 host, which has an active 800w static policy. There is just not enough power budgeted for the group policy to allocate to its members.

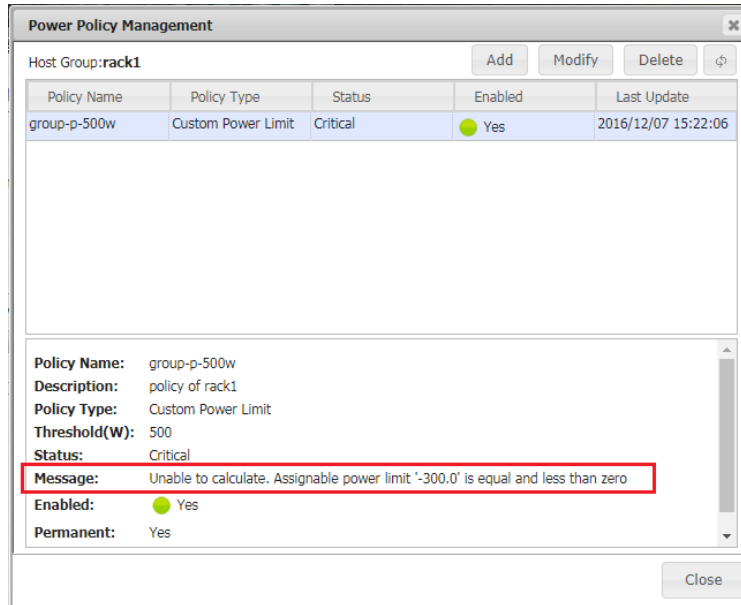


Figure 9-27



Note: When multiple policies (host and host group policies) apply to an NM host, the static host policies (either permanent or scheduled) have priority.

9.4 Power Management Events

When a power capping policy cannot be achieved, an event is added to the SSM Database and is displayed on the **Host Events** or **Host Group Events** tab in the monitoring page. When the capping policy is recovered, a recovery event is added to the SSM Database and is shown on the Host Events or Host Group Events tab as well.

9.4.1 Host Events

Suppose that a permanent policy with a 100W threshold is added to a host named DB-Node3. The host is running a number of jobs and its CPU loading is very high. The NM of the DB-Node3 tries to limit its power consumption but fails to do so. The DB-Node3 still consumes more than 100W of power. The SSM Server detects this situation and writes a problem event to the SSM Database, which is displayed on the SSM Web interface as shown below. To achieve the power limit, some of the jobs running on the DB-Node3 are migrated to other hosts and the CPU loading of the DB-Node3 is reduced. The NM can now limit the DB-Node3's power consumption to under 100W and a recovery event is shown on the Host Events tab to indicate this situation.

The screenshot shows the SSM Host View interface. The top section displays a table of host status:

Host Status	Service Status	Host Name	Host Type	Address	Last Check	Duration
Up	OK	DB-Node1	Agent Managed,IPMI,NM,...	10.146.125.31	09 seconds a...	00d 00h 35m 12s
Up	Critical	DB-Node3	Agent Managed,IPMI,NM,...	10.146.125.35	44 seconds a...	00d 00h 35m 12s

The bottom section shows the **Detail** view for **DB-Node3**. It includes tabs for Host Status, Service Status, System Summary, Host Events, and Host Properties. Below the tabs is a 'Max Results' dropdown set to 100 and a 'Delete' button. A table of events is displayed, highlighted with a red box:

Severity	Event Type	Message	Date	Target
INFO	SSM_SERVER_POLICY_RECOVERY	Recovery: Host 'DB-Node3' current power consumption(90W) belows the threshold(100W) defined in policy 'p-100w'.	2016/12/07 15:28:51	DB-Node3
ERROR	SSM_SERVER_POLICY_PROBLEM	Problem: Host 'DB-Node3' current power consumption(124W) exceeds the threshold(100W) defined in policy 'p-100w'.	2016/12/07 15:26:51	DB-Node3

Red circles with numbers 1 and 2 are overlaid on the interface. Circle 1 points to the 'Delete' button, and circle 2 points to the event table.

Figure 9-28

You can clear the host events by clicking the **Delete** button and the events will be deleted from the SSM Database.

9.4.2 Host Group Events

Host group events show events related to the policies of a host group and the policies of individual hosts in the host group. For example, suppose that a DB-Node3 host is a member of a Rack1 host group. The DB-Node3 host's events are shown on the Rack1's Host Group Events tab. Note that events of the nested host groups are not shown on the Host Group Event tab of the outer host group.

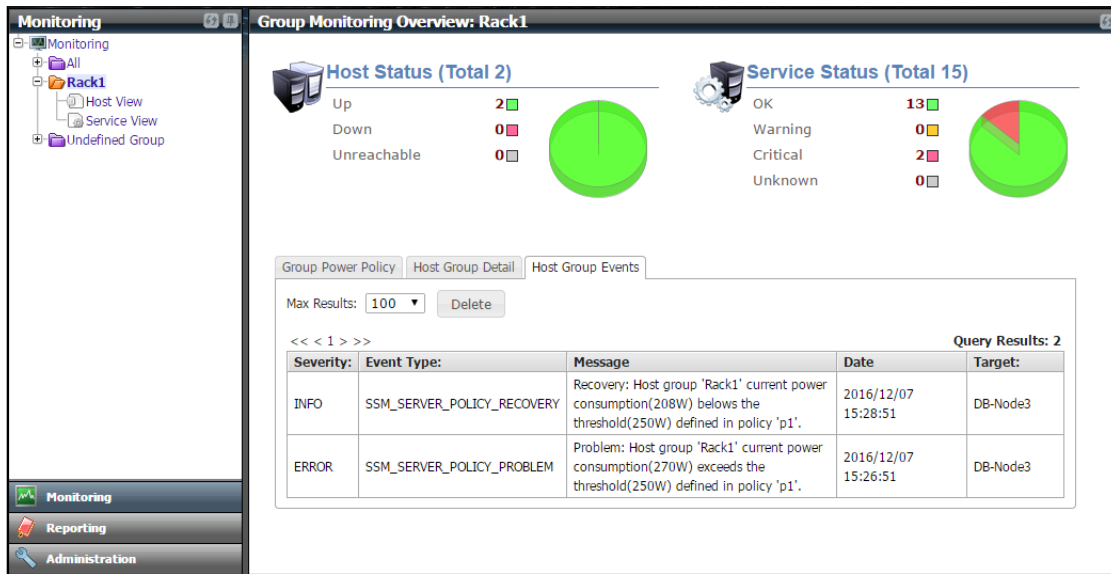


Figure 9-29

You can clear the host group events by clicking the **Delete** button and the events will be deleted from the SSM Database.

10 SUM Integration

10.1 SUM in SSM

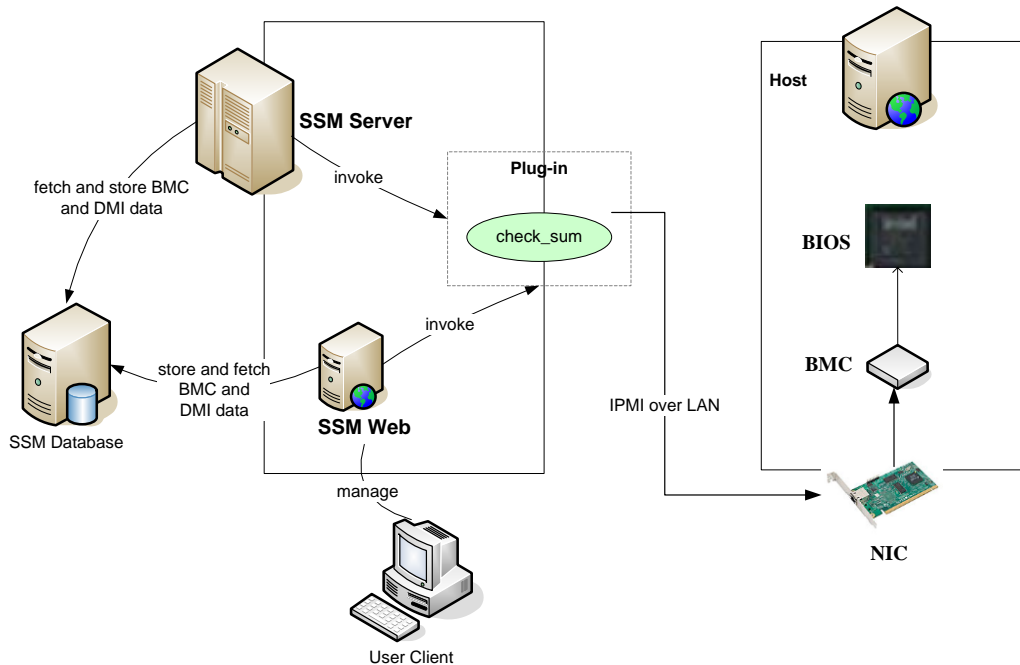


Figure 10-1

SSM enables user to manage IPMI hosts by integrating the Supermicro Update Manager (SUM) as check_sum plug-in, as shown above. For more information on what SUM is, see *Supermicro Update Manager User's Guide* in the `[install folder]\shared\sum\sum` folder.

Currently, SSM integrates SUM functions including:

- BIOS Management
 - Export BIOS configuration (both current and factory)
 - Export DMI information
 - Change BIOS configuration
 - Change DMI information
 - Update BIOS
- BMC Management
 - Export BMC configuration
 - Change BMC configuration
 - Update BMC
- Other System Management
 - Export Asset information
 - Export BMC event logs

- Clear BMC and BIOS event logs
- Export System Utilization
- Mount and unmount ISO image
- Enable and clear TPM module capabilities

These functions all work through the OOB (Out-Of-Band) communication channel. By the OOB channel, operations are independent of the OS on the managed system and can be executed before the system OS is installed.

To use SUM functions in SSM, check the requirements before use. For the managed system, your motherboard/system of Supermicro X9/X10 series and later generations must have a **BMC** with node product key activation. Firmwares on the managed system must meet the following requirements:

Firmware	Requirements
BMC Version	<p>X9 ATEN platform (SMT_X9): 3.14 or later</p> <p>X10 ATEN platform (SMT_X10): 1.52 or later</p> <p>X11 ATEM platform (SMT_X11): 1.00 or later</p> <p>X9 AMI platform (SMM_X9): 2.32 or later</p>
BIOS Version	<p>Version 2.0 or later for select X9 Intel® Xeon® processor E5-2600 product family and X10 Intel® Xeon® Processor E3-1200 v3 Product Family systems.</p> <p>Version 1.0 or later for select X10 Intel® Xeon® Processor E5 v3/v4 Product Family/X11 systems</p>

The CheckSystemUtilization command requires additional packages to be installed on the managed system.

Program/Script	Description
TAS_XXX	The Thin Agent Service (TAS) program should be installed on the managed systems. It collects utilization information on managed system and update information to BMC.

When you use the Host Discovery Wizard to add an IPMI host, the built-in Check SUM Support service and IPMI System Information service are added. Check SUM Support service is used to check if both BIOS and BMC firmware support OOB functions. Meanwhile, IPMI System Information service is used to

periodically gather the DMI data and Asset information from an IPMI host. Users can see system information on the SSM Web interface.

Besides built-in services, the SSM Web interface provides web commands to update BIOS image, BIOS settings and DMI information. For flashing BIOS image, user can upload new BIOS to update multiple IPMI hosts. For changing the BIOS settings and the DMI information, user can use these commands to export readable text files from managed systems, edit the files, and then import them later to managed systems. Other commands will show in the following chapters.

10.2 Activating an IPMI Host

Before using SUM functions, you must activate the IPMI hosts. Users only need to activate the product key of an IPMI host once. The supported product keys include **SFT-DCMS-Single**, **SFT-SUM-LIC** and **SFT-OOB-LIC**. The product key is bound with the MAC address of the BMC LAN port. To access the SUM functions, make sure your **Node Product Key** includes at least one of the three product keys above and has not expired.



Note: SFT-DCMS-Single and SFT-SUM-LIC product keys only support Supermicro motherboards of X10 series and later generations.

10.2.1 Checking Activation Status

Host Name	BMC Address	Has...	Node Product Key S...	Description
10.146.125.44	10.146.125.50	YES	OK	Firmware: ATEN_ASPEED, Node Manager Version: 3.0
10.146.125.60	10.146.125.60	YES	OK	Firmware: ATEN_MICROBLADE_NODE, Node Manager Version: 2.0
TokyoMachine	10.146.125.113	YES	OK	Firmware: ATEN_MICROBLADE_NODE, Node Manager Version: 2.0
10.146.125.134	10.146.125.134	No	OK	Firmware: ATEN_MICROBLADE_NODE
10.146.125.135	10.146.125.135	No	Not Available	Firmware: ATEN
TaipeiMachine	10.146.125.136	YES	OK	Firmware: ATEN_ASPEED, Node Manager Version: 3.0
10.146.125.137	10.146.125.137	No	OK	Firmware: ATEN_ASPEED
10.146.125.138	10.146.125.138	No	Not Available	Firmware: ATEN
10.146.125.139	10.146.125.139	No	Not Available	Firmware: ATEN

Detail	
10.146.125.44	
Host Name	10.146.125.44
BMC Address	10.146.125.50
Has NM	YES
Description	Firmware: ATEN_ASPEED, Node Manager Version: 3.0
Node Product Key Status	SFT-DCMS-Single SFT-DCMS-CALL-HOME SFT-OOB-LIC

Figure 10-2

The **Node Product Key Status** of each host is shown on the **IPMI Managed** page under the Host Management category (see the figure above). This shows the activation status of an IPMI host. Valid values are Not Available, OK, Warning and Critical. If the node product key is activated and has not

expired, the value shows OK. If the node product key is going to expire in 15 days, the value shows Warning. Critical means product keys are expired. If the IPMI host does not have any node product key, “Not Available” is shown in the Node Product Key Status column.

Note that if the product keys SFT-DCMS-Single and SFT-SUM-LIC exist, SFT-DCMS-Single is prioritized and decides the **Node Product Key Status**. For example, if the SFT-DCMS-Single will soon expire, the value shows Warning no matter what the status of the SFT-SUM-LIC product key is.

The **Node Product Key Status** column in the Detailed View shows extra product key information belonging to a selected host in the master view. In the above example, the status of each node product key is shown, including SFT-DCMS-Single and SFT-SUM-LIC.



Note: SSM periodically checks the activation status of an IPMI host, thus it may not reflect the real time data when you check the activation status.

10.2.2 Collecting MAC Addresses

You need to collect MAC addresses of managed systems before you contact Supermicro to generate your node product keys (SFT-OOB-LIC Key, SFT-DCMS-Single, SFT-DCMS-SVC-KEY, etc.). On the **IPMI Managed** page, SSM allows user to collect IPMI MAC addresses and list them in one file. The output file (“mymacs.txt”) includes the MAC address and IP address.

Example:

```
003048001012;192.168.34.1
003048001013;192.168.34.2
003048001014;192.168.34.3
```

To perform **Export MAC Address** function, select multiple hosts and click **Export MAC Address** in the command area. Click the **Run** button and wait SSM to get MAC addresses. When finished, clicking the **Export File** button will download the output file (“mymacs.txt”), as shown below.

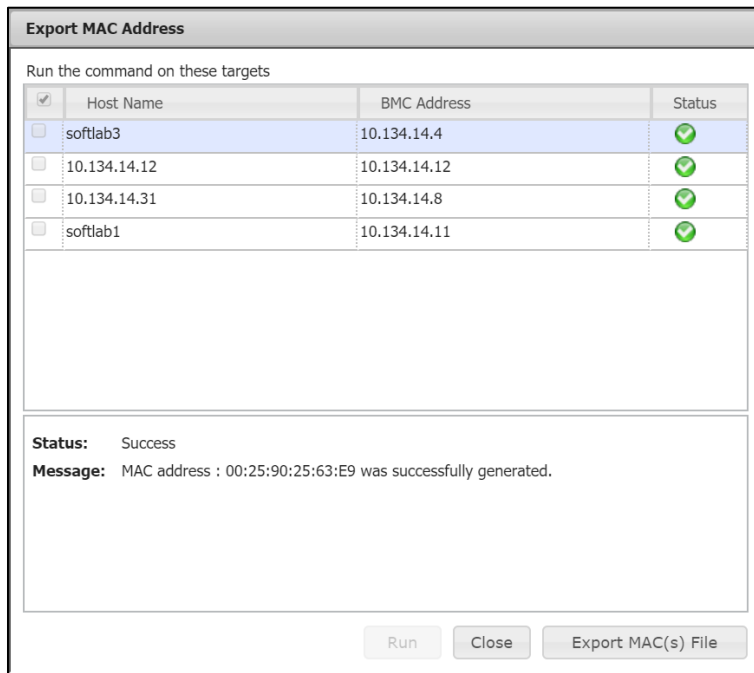


Figure 10-3

10.2.3 Activating Node Product Keys of IPMI Hosts

Contact Supermicro to generate a node product key to activate. For an SFT-OOB-LIC key, the example below shows how to activate this key via the SSM Web console.

The **activation response file** (“mymacs.txt”) from Supermicro includes the MAC address, IP address and product key.

Example:

```
003048001012;192.168.34.1;1111-1111-1111-1111-1111-1111
```

```
003048001013;192.168.34.2;2222-2222-2222-2222-2222-2222
```

```
003048001014;192.168.34.3;3333-3333-3333-3333-3333-3333
```

Node PK Activation page allows users to activate numerous product keys from a file. To activate IPMI hosts, upload the file obtained from Supermicro, set the BMC ID as well as the password then click the **Activate** button. A **Node PK Activation** dialog box will pop up as shown below if the uploaded file is valid.

Click the **Run** button to start activating or the **Close** button to abort and close this dialog box. Note that all IPMI hosts in the file should be accessed with the provided ID and password.

Node PK Activation

Run the command on these targets

<input checked="" type="checkbox"/>	BMC Address	Product Key	Status
<input checked="" type="checkbox"/>	10.146.125.12	1D1C-D24T-3BH8-48G4-CD95-66A1	
<input checked="" type="checkbox"/>	10.146.125.45	2J22-1KO3-4444-5HK6-6CC9-FF77	
<input checked="" type="checkbox"/>	10.146.125.47	2EER-3CC5-4UI7-55CC-5896-7777	

Figure 10-4

10.3 SUM Services

Two services, **Check SUM Support** and **IPMI System Information** designed for SUM functions, are supported in SSM. The services are added by default when using the Host Discovery Wizard to add an IPMI host.

- **Check SUM Support:** This shows if the IPMI host supports SUM or not. The health of this service is a combined status that depends on the states of the following items:
 - Product Key Activated. The valid values are: No/OOB/SUM/SUM (expired)/DCMS/DCMS (expired).
 - BMC Supports OOB BIOS Config. The valid values are: No/Yes.
 - BMC Supports OOB DMI Edit. The valid values are: No/Yes.

If one item is No or expired, the status of the service shows Critical. Otherwise, it shows OK. You can check if the IPMI host supports OOB by viewing this service.

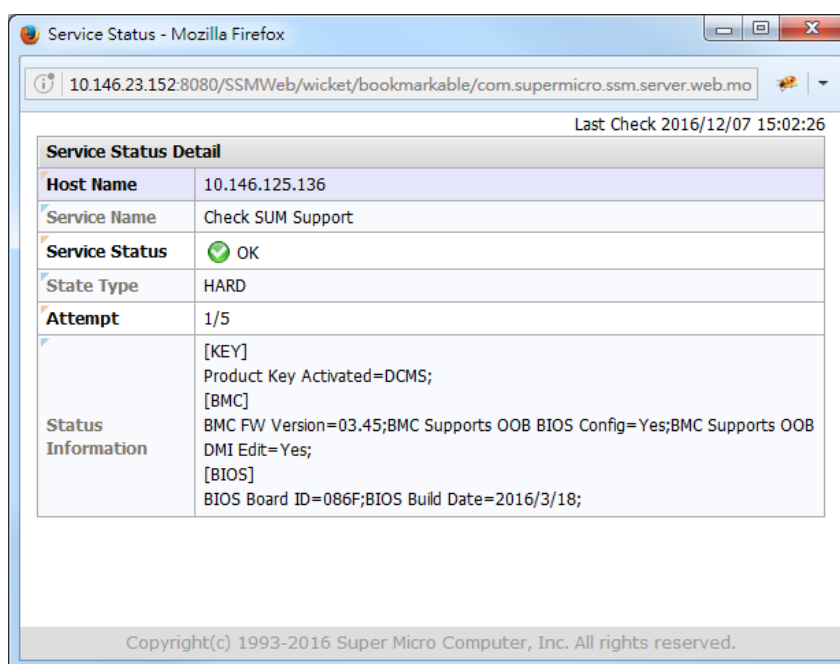


Figure 10-5

- **IPMI System Information:** This service gathers system information via FRU, OOB Full SMBIOS, and Supermicro BMC Redfish API. It periodically retrieves the **Asset Information** and **DMI information** from BIOS via BMC, and Ethernet interfaces and storage information via BMC Redfish API, and then stores them in the database. Meanwhile, SSM also adds itself as an event subscriber to the target BMC. Besides regular fetching frequency, SSM will then fetch system information immediately whenever BMC SEL changes.
- Users can use this data to see system information on the SSM Web interface. If this service is not added to an IPMI managed host, the View Details command under the System Information

category on the monitoring page cannot be used. See *10.4 SUM Web Commands* for more information.

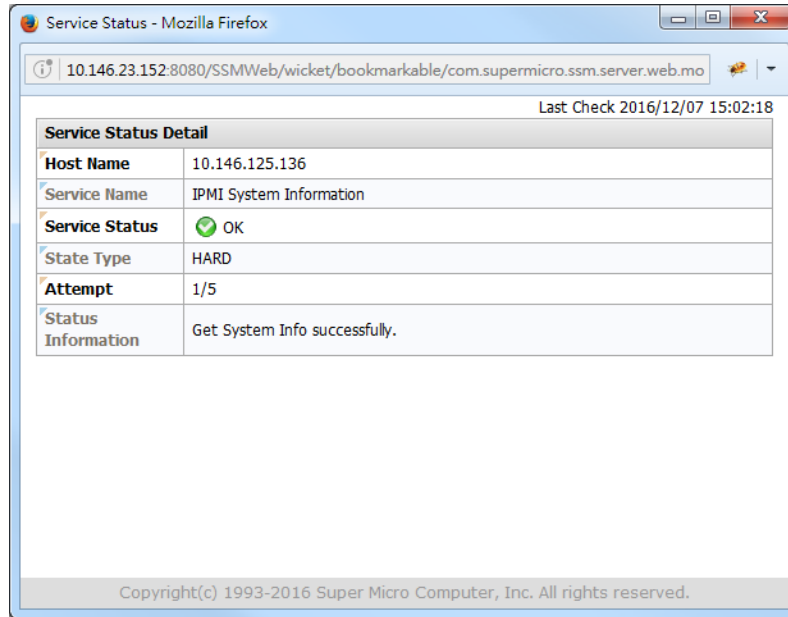


Figure 10-6

Besides the System Information command, the System Summary tab in the Detailed View also depends on the service, as shown below.

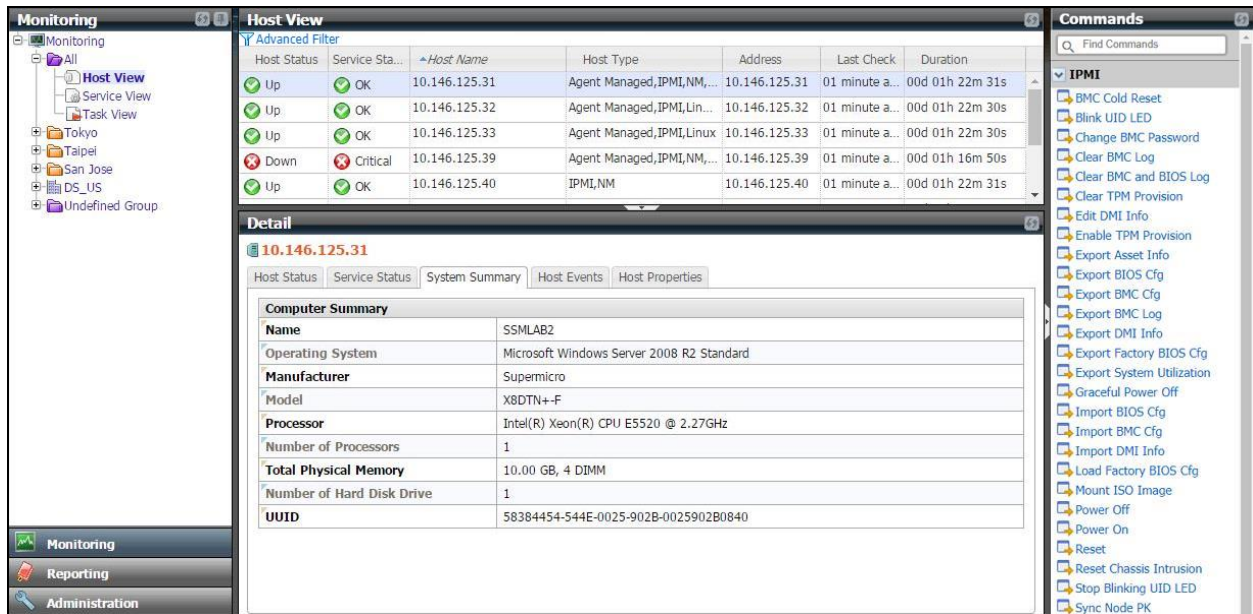


Figure 10-7

10.4 SUM Web Commands

The SUM web commands are applicable for IPMI hosts. SSM supports the following commands:

- **Export DMI Info:** Exports the editable DMI information.
 - 1). Select hosts in the working area. You can select multiple hosts at a time.
 - 2). Click **Export DMI Info** in the command area and an Export DMI Info dialog box will pop up.
 - 3). Click the **Run** button to get the DMI information or the **Close** button to abort and close this dialog box.

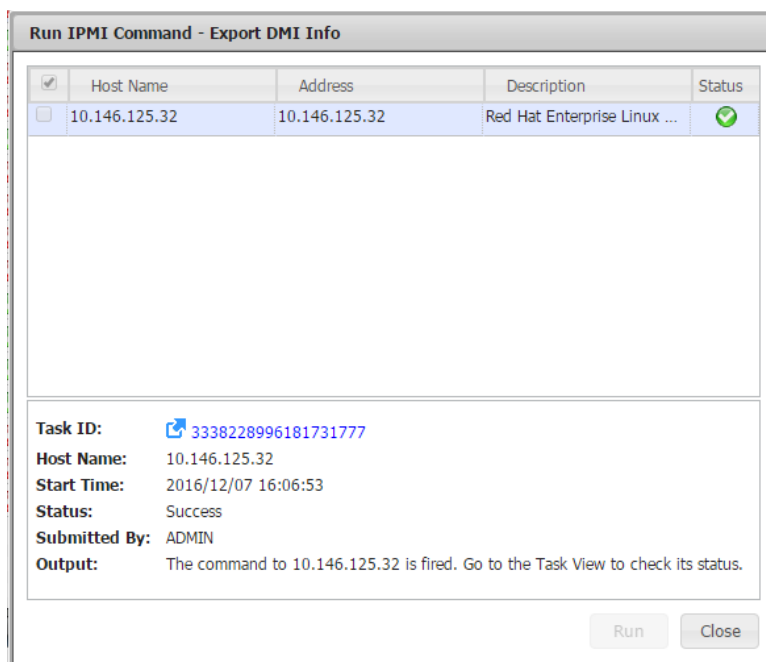


Figure 10-8

- 4). Click the **Task ID** link to go the Task View. SSM uses an asynchronous task to represent the request for the long task completion.
- **Import DMI Info:** Imports the DMI information.
 - 1). Prepare a new-configured DMI information file. You can download and edit the DMI Info text file from **Export DMI Info** command. Note that you can select one IPMI host as the golden sample for DMI information.
 - 2). Select hosts in the working area. You can select multiple hosts at a time.
 - 3). Click **Import DMI Info** in the command area and you will see a Change DMI Info Arguments dialog box pop up.
 - 4). Click the **Browse** button to upload the new-configured DMI information file, as shown below.

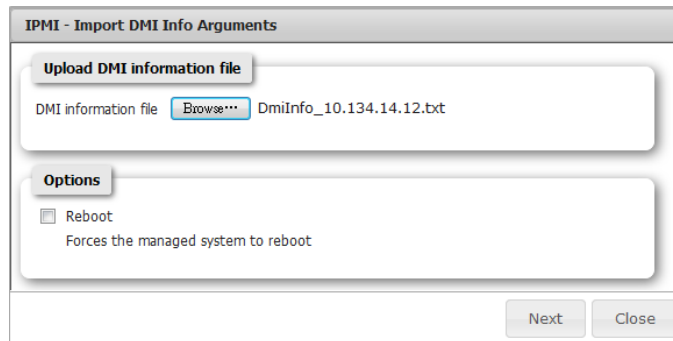


Figure 10-9

- 5). Click the **Reboot** check box to force the host reboot for the changes to take effect.
- 6). Click the **Next** button to continue or the **Close** button to abort and close this dialog box.
- 7). Click the **Previous** button to return to the previous Arguments page, as shown below.

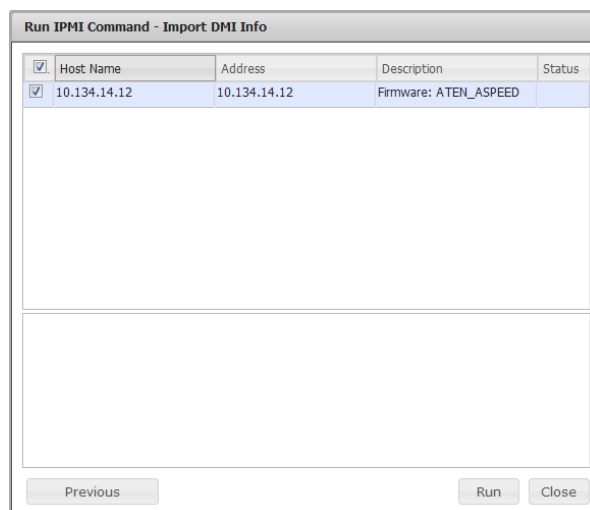


Figure 10-10

- 8). Click the **Run** button to start updating a managed system's DMI information or the **Close** button to abort and close this dialog box.
- 9). Click the **Task ID** link to go to the Task View. SSM uses an asynchronous task to represent the request for the long task completion.



Note: The DMI information will only take effect after a system reboots or powers up. You can select the **Reboot** option in Arguments dialog box for rebooting after updating.

- **Edit DMI Info:** Changes specific of DMI information items. The execution is similar to that of the

- **Import DMI Info** command. You can select the specific DMI items or inputs if there are no existing DMI items to be updated.
- **Export BIOS Cfg:** Exports the BIOS settings. The operation and result are similar to those of the **Export DMI Info** command.
- **Import BIOS Cfg:** Imports the BIOS settings. The operation is similar to that of the **Import DMI Info** command. You need to upload a new-configured BIOS setting file in the Arguments dialog box.
- **Export Factory BIOS Cfg:** Exports the default factory BIOS settings. The operation and result are similar to those of the **Export DMI Info** command.
- **Load Factory BIOS Cfg:** Restores the BIOS to the default factory settings. The operation is similar to that of the **Import BIOS Cfg** command. The configurations will only take effect after the selected hosts reboot or power up.
- **Update BIOS:** Updates the selected hosts with a BIOS image file. In Arguments dialog box, you need to upload a BIOS image file and choose the flash options, as shown below.

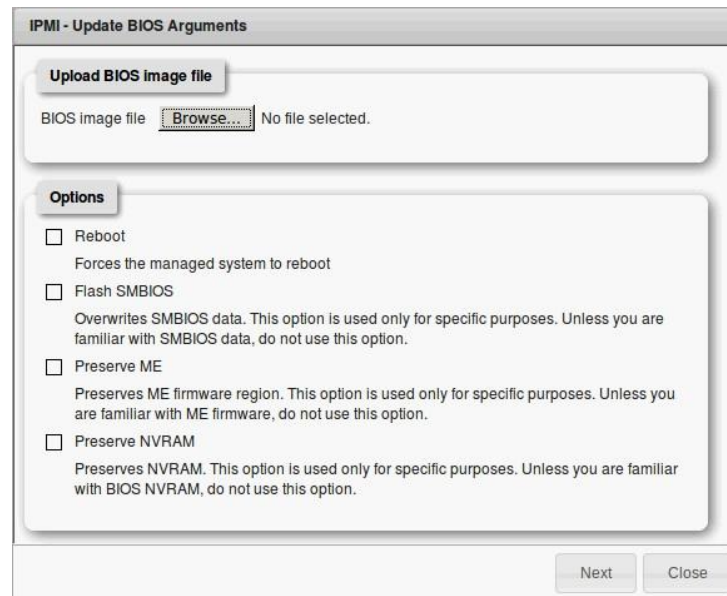


Figure 10-11



Notes:

- You have to reboot or power up the selected hosts for the changes to take effect. You can select the **Reboot** option for rebooting after updating.
 - The **Preserve NVRAM** and **Flash SMBIOS** functions cannot be used at the same time.
- **Export BMC Cfg:** Exports the BMC settings. The operation and result are similar to those of the **Export DMI Info** command.
 - **Import BMC Cfg:** Imports the BMC settings. The operation is similar to that of the **Import DMI Info** command. You need to upload a new-configured BMC setting file in the Arguments dialog box.
 - **Update BMC:** Updates the selected hosts with a BMC image file. You need to upload a BMC image

- file in the Arguments dialog box.
- **Export Asset Info:** Exports the Asset Information. The operation and result are similar to those of the **Export DMI Info** command.
 - **Export System Utilization:** Exports the system utilization information. The operation and result are similar to those of the **Export DMI Info** command.
 - **Export BMC Log:** Exports the BMC event logs. The operation and result are similar to those of the **Export DMI Info** command.
 - **Clear BMC and BIOS Log:** Clears the BMC and BIOS event logs.
 - Event logs in BMC will be cleared immediately.
 - Event logs in BIOS will be cleared only after system reboot.
 - **Mount ISO Image:** Provides the selected hosts an ISO Image as a Virtual Media through BMC and SAMBA Server. In Arguments dialog box, you need to designate an image URL and input the access options, as shown below.

Figure 10-12

- **Unmount ISO Image:** Removes ISO image as a virtual media from the selected hosts.
- **Enable TPM Provision:** Enables TPM module capabilities for the selected hosts.
- **Clear TPM Provision:** Clears TPM module capabilities from the selected hosts.
- **System Information Command:** Shows the system information of individual selected hosts. Currently, and **View Details** are provided.

Host Status	Service Stat...	Host Name	Host Type	Address	Last Check	Duration
Up	Critical	10.146.125.135	IPMI	10.146.125.135	03 minutes a...	00d 00h 04m 00s
Up	Critical	10.146.125.136	IPMI,NM	10.146.125.136	03 minutes a...	00d 00h 04m 00s
Up	Critical	10.146.125.137	IPMI	10.146.125.137	03 minutes a...	00d 00h 04m 34s
Up	OK	10.146.125.138	IPMI	10.146.125.138	03 minutes a...	00d 00h 03m 59s
Up	Critical	10.146.125.139	IPMI	10.146.125.139	03 minutes a...	00d 00h 04m 00s
Up	OK	10.146.125.140	IPMI	10.146.125.140	03 minutes a...	00d 00h 03m 59s

Commands panel:

- IPMI
 - System Information
 - View Details
 - Download Troubleshooting Log
 - Remote Control
 - Host Admin
 - Reports

Figure 10-13

A new window containing all types of system information objects (see the figure below) will pop up after the execution of this command.

The screenshot shows a window titled "All | Compact" with a tree view on the left and a details pane on the right. The tree view includes categories like Hardware (BIOS, BaseBoard, Chassis, Computer System, Storage, Memory, Network, Processor, System Slot, BMC, Power Supply) and Software (Account, Operating System, Process, Service, Time Zone, OEM Strings). The BaseBoard item is selected. The details pane shows the Host Name as 10.146.125.119 and the last check time as 2017/12/07 10:48:58. Below this, the BaseBoard details are listed in a table:

Baseboard	
Product:	X10DRW-ET
Manufacturer:	Supermicro
Serial Number:	HM14CS000053
Asset Tag:	Default string
Version:	1.01

Figure 10-14



Notes:

- The system information is based on SUM through OOB channel. Available types: BIOS, BaseBoard, Chassis, Computer System, Disk Drive, Memory, Network, Processor, BMC, Power Supply, OEM Strings, and System Cfg Options.
- The Check Interval attribute of the **IPMI System Information** service determines the fetch frequency.

11 OS Deployment

The **Deploy OS** function allows users to deploy Linux OS on the managed IPMI hosts. The supported versions of 64-bit Linux OS include:

- Red Hat Enterprise Linux Server 6.x, 7.x, 8.x
- CentOS Server 6.x, 7.x, 8.x
- Ubuntu Server 14.x, 15.x, 16.4
- SUSE Linux Enterprise Server 11 SP3¹⁵, 11 SP4, 12.x, 15.x
- VMware ESXi 5.5, 6.0¹⁶, 6.5, 6.7

To use this function in SSM, check the requirements before use.

For network environment,

- For mass deployment, DHCP is required. If multiple subnets are present, then multiple DHCP servers for each subnet are needed unless the gateway acts as a DHCP relay.

For the management server,

- The **Deploy OS** function is currently only available on Linux platforms.
- TCP ports 139, 445 and 514¹⁷ need to be opened. UDP port 514 needs to be opened.
- For SSM to receive the installation logs from the managed host, the SSM server address is required for configuration if the management server is equipped with multiple network interfaces. See *6.12 Server Address* for more information.

For the managed system,

- Your motherboard/system of Supermicro X10 series and later generations must have a **BMC** with its SFT-DCMS-Single product key activated and both BMC and system LAN are accessible from the network.
- The Deploy OS function is based on SUM through the OOB channel, so the managed system must meet SUM's requirements. See *10 SUM Integration* for more details.
- It's recommended that you use the latest version of BIOS and BMC for the managed host before you install the OS on it. See *10.4 SUM Web Commands* for the steps to update the BMC and BIOS.

¹⁵ SLES versions older than 11.3 are no longer supported.

¹⁶ SSM does not support VMware ESXi 5.5 or VMware ESXi 6.0 Update 2 OS deployment on Supermicro H11 series.

¹⁷ SSM will disable the local SAMBA server and use its built-in SAMBA server for the OS Deployment function.

SSM allows users to deploy an OS in unattended mode. In this mode, users will only have to provide an answer file (e.g., Kickstart¹⁸ in RHEL, AutoYAST¹⁹ in SLES) and an OS image (the file format must be ISO) to start the automatic installation. Make sure you have both an answer file and an OS image before beginning. For more details on OS images, see *11.1 OS Images*.

The example below shows how to use the **Deploy OS** web command to deploy RHEL 7 to multiple IPMI hosts. Follow these steps to make a request and retrieve the deployment.

1. Select multiple IPMI hosts (hosts with node product keys) on the Monitoring page for mass deployment.

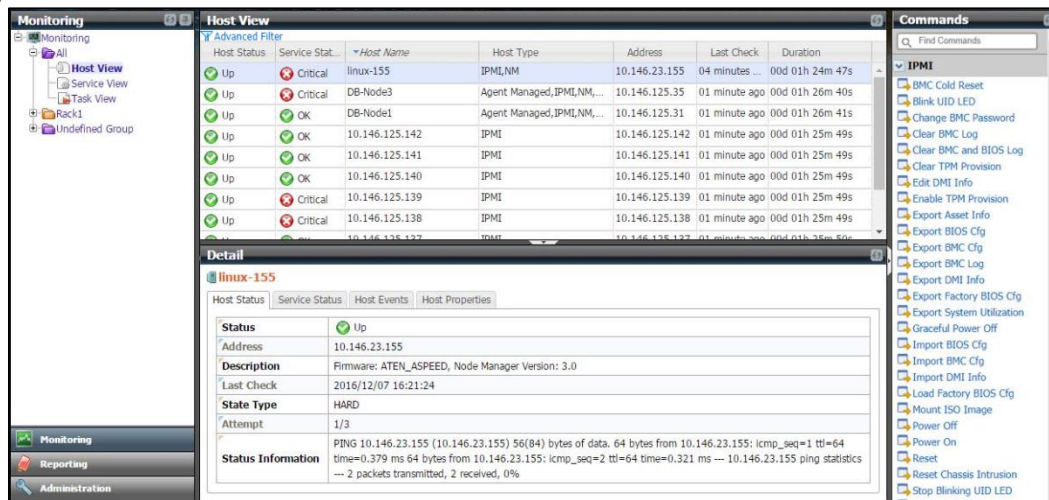


Figure 11-1

2. Click **Deploy OS** in the command area and a Deploy OS Arguments dialog box will appear.

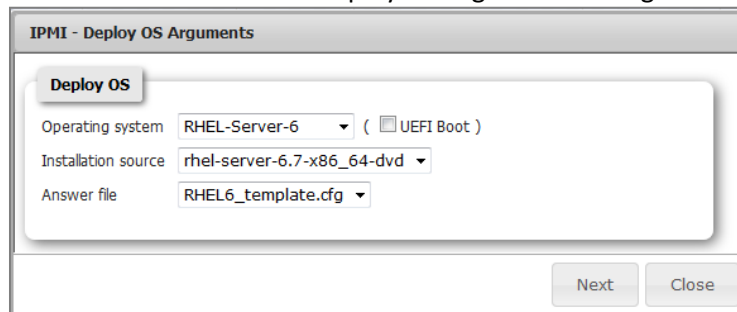


Figure 11-2

¹⁸ Kickstart, a file containing the system installation information and configurations used on most Linux systems, can be used without user intervention.

¹⁹ AutoYAST, an XML file containing the system installation information and configurations used on SLES systems, can be used without user intervention.

- Use the drop-down menus and click the checkbox to select the **Operating system**, **UEFI Boot**, **Installation source** and **Answer file**. Note that only operating systems such as RHEL Server CentOSUbuntuSLES, and VMware ESXi are supported in SSM. The options for Installation source and Answer file are determined by what you choose for the Operating system and the UEFI Boot. Note that the Deploy OS function supports installations in legacy bootable devices and UEFI bootable devices; however, not all operating systems are UEFI-aware²⁰. For example, if you select RHEL-Server-6 and clear the selection of the UEFI Boot option, the Installation source options and Answer file options will include all RHEL-Server-6 OS images and all RHEL-Server-6 answer files. If you select RHEL-Server-6 and check the UEFI Boot option, the Installation source options and the Answer file options will include all RHEL-Server-6 64-bit OS images (RHEL-Server-6 32-bit OS does not support UEFI) and all RHEL-Server-6 answer files. Click the **Next** button to continue or the **Close** button to abort and close this dialog box.
- Click the **Run** button to start deployment or the **Close** button to abort and close this dialog box. In the figure below, the green check icons in the Status fields indicate that the request has been sent. If no green check icons appear, check the output message and retry.

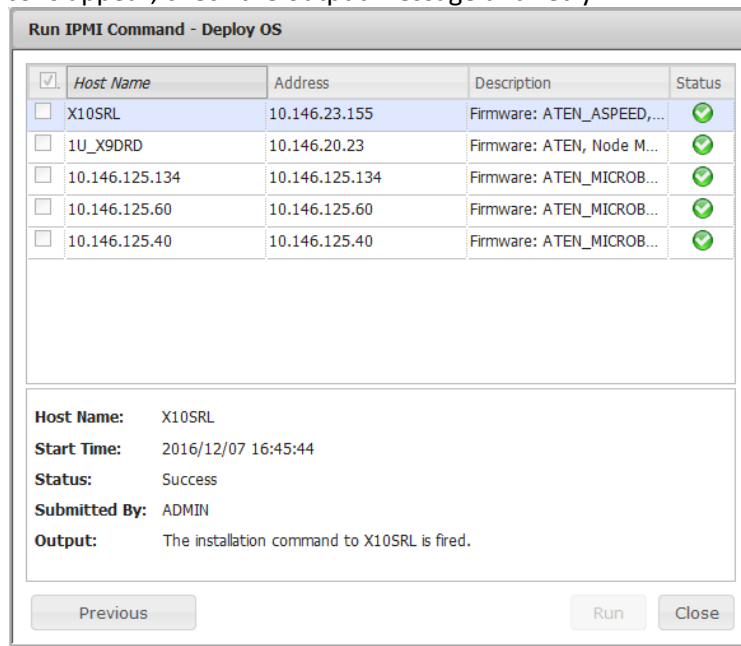


Figure 11-3

- SSM uses an asynchronous task to represent the request. To view the deployment results, click **Deployment Progress** in the navigation area on the administration page to see five tasks running in the top right window.

²⁰ To select an operating system supporting UEFI, see if its OS image contains the EFI\Boot folder.

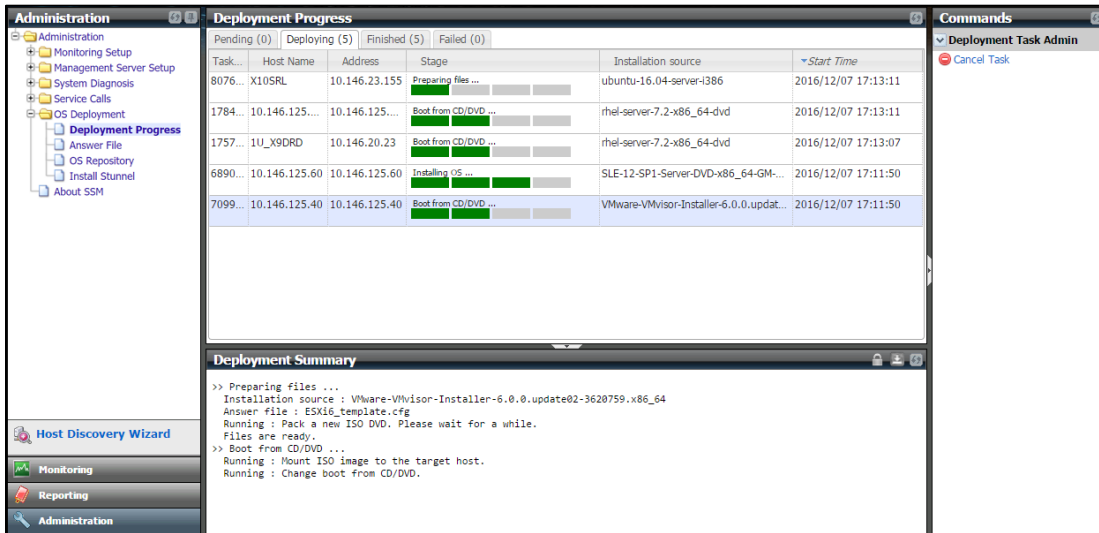


Figure 11-4

- On the Deployment Progress page, the master view shows a list of hosts. In the Deployment Summary, the detailed progress of a selected host is shown. The master view includes 4 tabs: **Pending**, **Deploying**, **Finished** and **Failed**. See 11.3 for more details on the Deployment Progress.
- Continue to inquire about the task status until the task is finished (see the figure below). You will see the task shown in the **Finished** tab if the deployment succeeds.

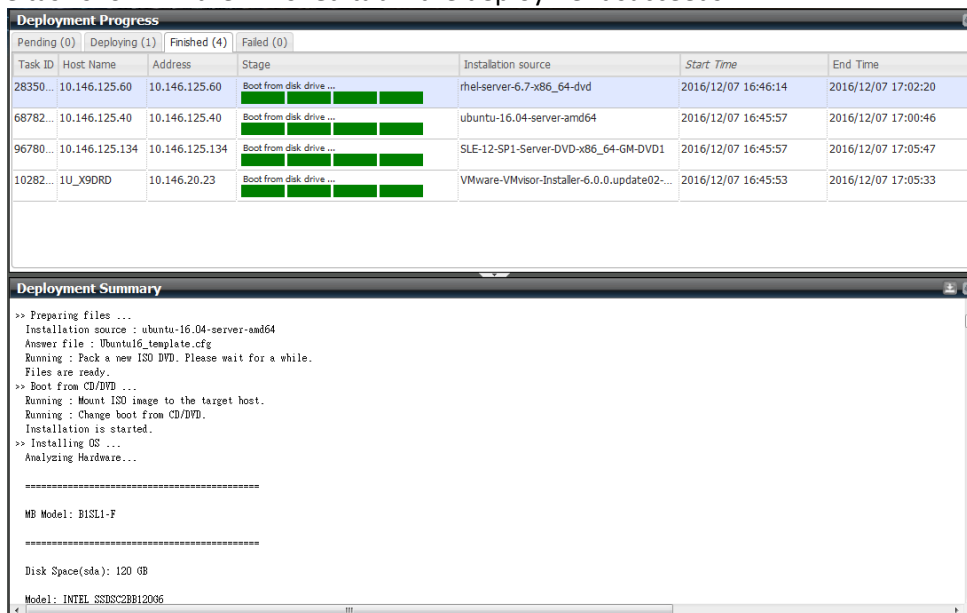


Figure 11-5

- If the deployment fails, the task is shown in the **Failed** tab. You can see the screenshot of the target host by clicking **View** link, or click the **Download Result** icon  for troubleshooting. See 11.3 *Deployment Progress* for more details.

Deployment Progress

Tas...	Host Name	Address	Stage	Installation source	Start Time	End Time	Screenshot
336...	10.146.125.134	10.146.125.134	Installing OS ...	ubuntu-16.10-server-amd64	2017/03/01 10:05:56	2017/03/01 10:10:15	View
650...	X105RL	10.146.125.133	Boot from CD/DVD ...	CentOS-7-x86_64-Minimal-1511	2017/03/01 10:25:12	2017/03/01 10:26:18	N/A (Error)
857...	10.146.20.23	10.146.20.23	Installing OS ...	ubuntu-16.10-server-amd64	2017/03/01 10:01:52	2017/03/01 10:07:09	View
706...	X10DR1-T	10.146.23.155	Installing OS ...	ubuntu-16.10-server-amd64	2017/03/01 10:06:09	2017/03/01 10:12:14	View
528...	linux-155	10.146.23.155	Boot from CD/DVD ...	CentOS-7-x86_64-Minimal-1511	2017/03/01 10:24:23	2017/03/01 10:25:41	View

Deployment Summary

```

>> Preparing files ...
Installation source : ubuntu-16.10-server-amd64
Answer file : Ubuntu16_template.cfg
Running : Pack a new ISO DVD. Please wait for a while.
Files are ready.
>> Boot from CD/DVD ...
Running : Mount ISO image to the target host.
Running : Change boot from CD/DVD.
Installation is started.
>> Installing OS ...
Timed out. The installation log is returned.
Additional Information:
[common header]
version: 0x01
session_offset: 0x04
debuginfo_offset: 0x15
checksum: 0xe6
[session info]
Update Stage: 0
StartTime: 1488334135875
[network info]
Error code: 0x00
PCI Eth num: 0x02
>80861f45
>80861f45
Sys Eth num: 0x02
>enp0s20f0(002590eb7192): LINK-UP
>enp0s20f1(002590eb7193): NO-CARRIER

```

Figure 11-6

9. You can also use the IPMI Web command to remotely troubleshoot with IPMI KVM. See 7.3.5 *Remote Control Commands* for details.



Note: Finished/Failed tasks will be kept for 24 hours.

11.1 OS Images

An OS image is necessary for the OS installation. For example, if you use RHEL Server 6.4, you need to run the **Upload ISO** web command to upload an OS image (an ISO file, such as `rhel-server-6.4-x86_64-dvd.iso`). Note that SSM will unpack the files in the image when it is put in the SSM folder. Delete the original OS image afterwards. Use **OS Repository** in the navigation area on the administration page to manage OS images.

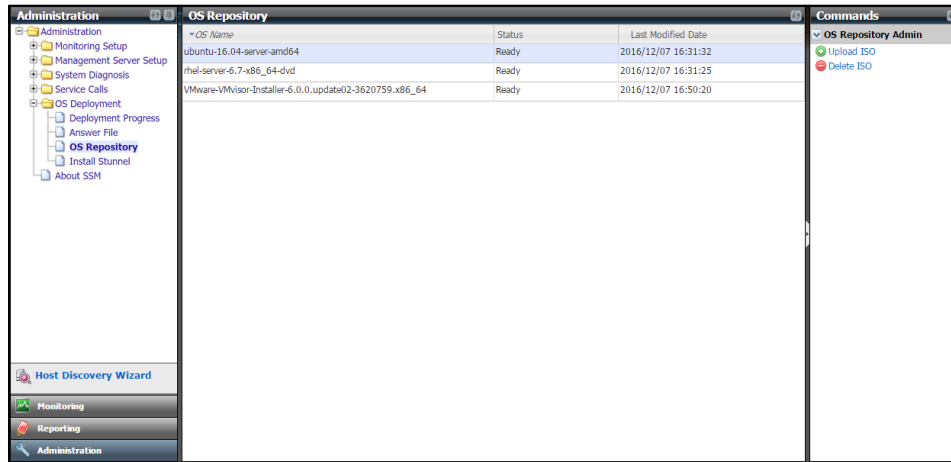


Figure 11-7

11.1.1 Uploading an ISO File

1. Click **Upload ISO** in the command area and an Upload ISO File dialog box appears (see the figure below).



Figure 11-8

2. Two methods of selecting ISO files are supported in this dialog box. You can select multiple ISO files at a time. In the figure below, rhel-server-6.4-x86_64-dvd.iso is ready to be uploaded.
3. Drag and drop the ISO files to the gray area (drag and drop ISO files to here or click here).
4. Click the gray area, and select the ISO files in the File Browse dialog box.

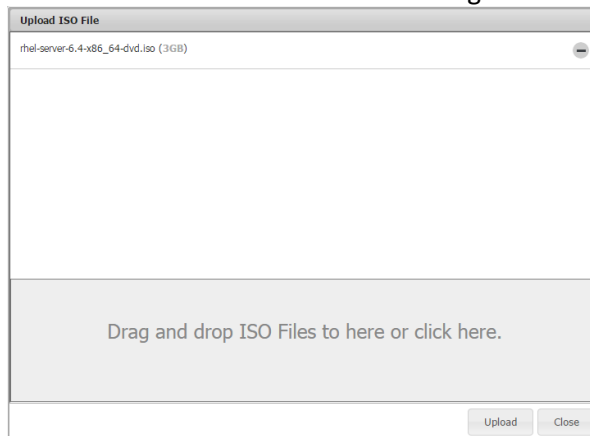


Figure 11-9

- Click the **Upload** button to start uploading ISO files to the SSM folder. The upload progress is shown.

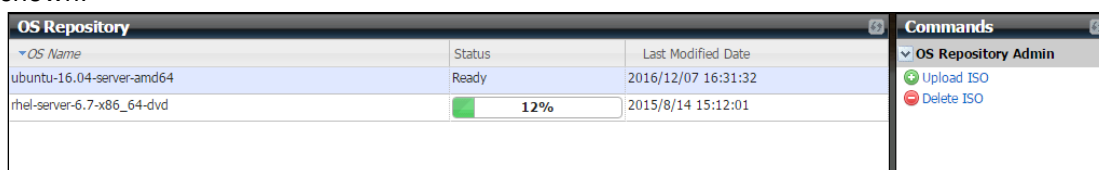


Figure 11-10

- Users may run the **Cancel Uploading ISO** web command to cancel the upload.

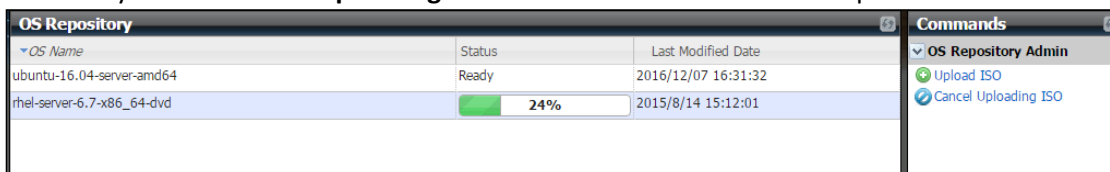


Figure 11-11

11.1.2 Checking Image Status

Use **OS Repository** to see the status of OS images. A **Ready** status means the OS image has been uploaded and unpacked completely. Please wait until the Status changes to “Ready” to start your OS installation. If the Status shows “Initial”, “Extracting” or “Failed”, the OS image cannot be used for OS deployment.

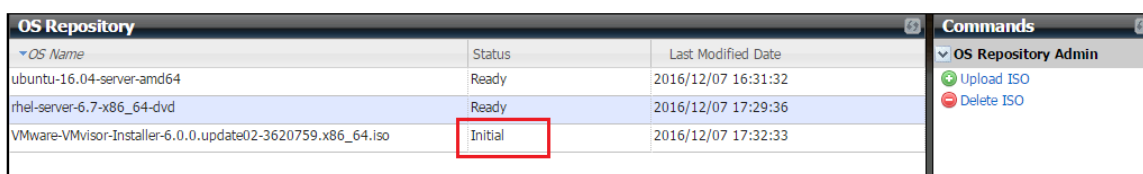


Figure 11-12

11.1.3 Deleting an ISO File

- Select the ISO file(s) to be deleted in the working area. You can delete multiple ISO files at a time.

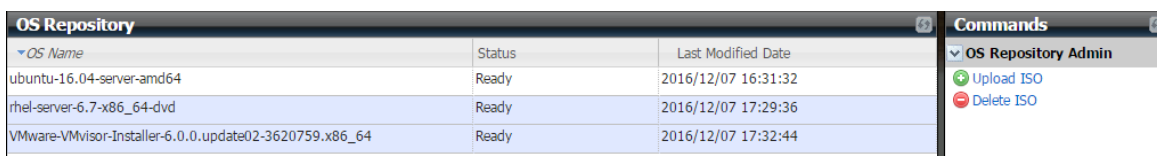


Figure 11-13

- Click **Delete ISO** in the command area and a Delete ISO File dialog box appears.

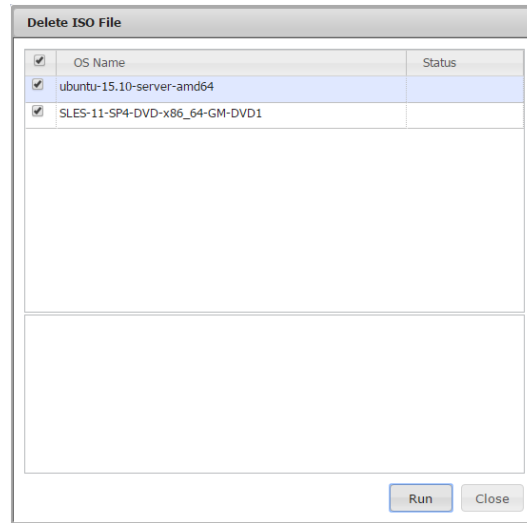


Figure 11-14

3. Click the **Run** button to delete the selected ISO files or the **Close** button to abort and close this dialog box.

11.2 Answer File

To install the OS automatically, an answer file is required. To alleviate this, SSM provides built-in answer files (templates) for supported operating systems, e.g., RHEL6_template for RHEL-Server-6.x, CentOS6_template for CentOS 6.x, and Ubuntu14_template for Ubuntu 14.x and so on. These answer files are fully validated by Supermicro and are designed to have minimal installation steps so that users can quickly deploy the OS to remote hosts. Knowing how to use answer file configurations helps you edit your own answer file to suit your needs.



Note: Although each template answer file is designed to be used in all major versions, there are some differences between the minor versions. For example, a CentOS6_template cannot be used for an unattended CentOS 6.1 installation; an installation menu or dialog box will pop up to require user configuration.

Click **Answer File** in the navigation area to perform file management functions. The master view shows a list of answer files while the detailed view shows the contents of the answer file. As shown below, the master view includes two tabs: **User Defined** and **Template**. Select the **User Defined** tab to add, edit, and delete answer files in the commands area.

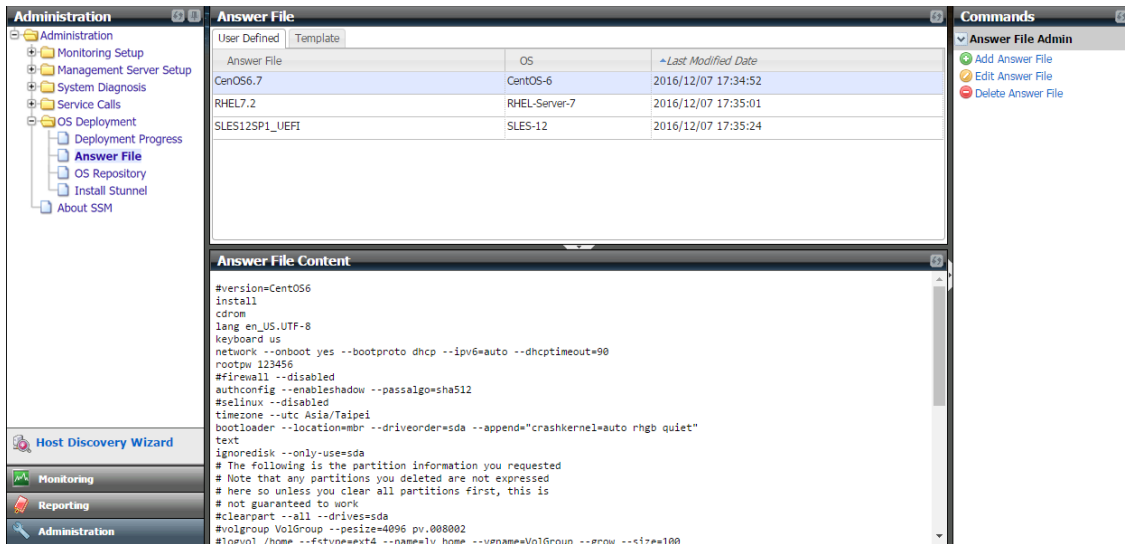


Figure 11-15

The functions of adding, editing and deleting are not supported in the **Template** tab.

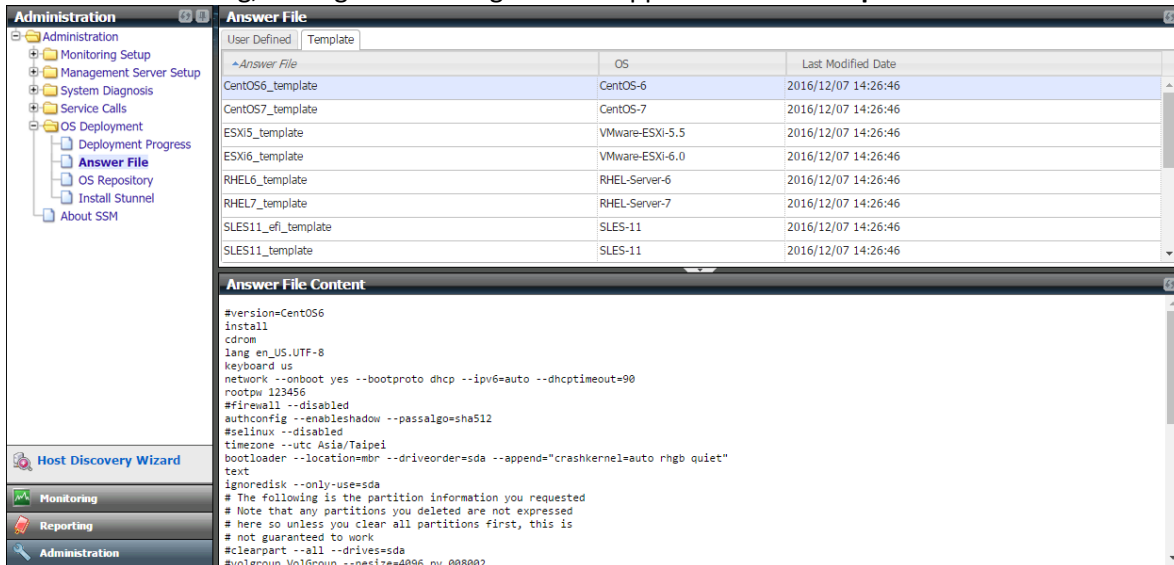


Figure 11-16

11.2.1 Attributes in Template Answer Files

Template Answer Files	Attribute	Description
CentOS/	ignoredisk --only-use=sda	Specifies that only the sda drive is used and other disks should be ignored.

Template Answer Files	Attribute	Description
RHEL/ Ubuntu		Note: Use of the attribute "ignoredisk" is recommended so that other disk except sda can be ignored.
	clearpart --initlabel --drives= sda	Removes partitions of the sda drive.
	autopart / part	Creates partitions. Note: One of the attributes "autopart", "part / partition", "raid", "logvol" or "volgroup" should be selected.
	Zerombr	Clears the master boot record of the sda drive. Note: The attribute "zerombr" should be specified to clear any invalid partition tables or previously initialized data on disks.
CentOS/ RHEL	bootloader --driveorder= sda	Selects the sda drive to be the first in the BIOS boot order. Note: Specifying how the bootloader should be loaded is required.
Ubuntu	user ubuntu --password 123456	Creates the account "ubuntu" with the password "123456" to log on the Ubuntu OS. It's recommended that you change the account and password in your answer file.
Ubuntu	%post echo "blacklist mei_me" >> /etc/modprobe.d/blacklist.conf	To solve a known issue in some Ubuntu OSs, the post section is used to force the Ubuntu OS not to load the mei driver.
Ubuntu	bootloader --location=mbr	Demands the boot record to be written to mbr. UEFI is enabled to determine the value to be partition.
SLES	<enable_firewall config:type="boolean">true</enable_firewall> <start_firewall config:type="boolean">true</start_firewall>	Specifies the firewall is enabled.

Template Answer Files	Attribute	Description
SLES	<boot_mbr>true</boot_mbr>	Demands the boot record to be written to mbr. UEFI is enabled to determine the value to be false.
SLES	<device>/dev/sda</device>	Specifies the sda drive is used and configured.
CentOS/ RHEL/ Ubuntu	network --bootproto= dhcp	Specifies that DHCP should be used on a Linux OS. For mass deployment, it is recommended that you specify DHCP when you deploy multiple hosts at a time, and then configure each host's network setting after the installation is complete.
VMware ESXi	network --bootproto=dhcp --device=vmnic0	(CentOS/RHEL/Ubuntu)Note: In order to remotely check the installation progress, the options "noipv4", "--onboot=no", and "--onboot no" may not be used.
SLES	<bootproto> dhcp </bootproto>	(VMware ESXi) Note: Only one record of network is allowed or the installation will fail.
SLES	<loader_type> grub2 </loader_type> >	Uses grub2 as the boot loader. The loader type is determined by the SLES version and the fact that UEFI is enabled.
CentOS/ RHEL/	rootpw 123456	Defines the password for the root account to log on the Linux OS. It's recommended that you change the password in your answer file.
SLES	<user_password>123456</user_password> <username>root</username>	Note: It's required when performing an unattended installation on a system.
VMware ESXi	rootpw default_PW	
CentOS/ RHEL	install cdrom	Install from the first optical drive on the system. Note: It is required to specify "cdrom" to be the data source for installation.
VMware ESXi	install --firstdisk --overwritevmfs	Install from the first drive and overwrite VMFS partitions on the system.

Template Answer Files	Attribute	Description
		Note: The first drive on system is decided by the port sequence instead of the disk order on BIOS SETUP configurations. You can specify a disk by giving a specific model name of the disk, for example, install --firstdisk='KINGSTON SV300S3,local' --overwritevmfs.
CentOS/ RHEL/ VMware ESXi	reboot	Specifying that the system should be rebooted after the installation is successfully completed. Note: It's required so that the remote host can verify the system status.
CentOS/ RHEL	lang en_US.UTF-8	Defines the default language to be used during installation and on the installed system. Note: It's required when performing an unattended installation on a system.
CentOS/ RHEL	keyboard us	Defines the type of keyboard layouts on the system.
VMware ESXi	keyboard 'US Default'	Note: It's required when performing an unattended installation on a system.
CentOS/ RHEL	authconfig --enablesshadow -- passalgo=sha512 auth --enablesshadow -- passalgo=sha512	Sets up the authentication options on the system. Note: Either "auth" or "authconfig" is required to configure the authentication on the system.
VMware ESXi	vmaccepteula	Accept the VMware End User License Agreement.

11.2.2 Adding an Answer File

1. Click **Add Answer File** in the command area and an Add Answer File dialog box appears (see the figure below).

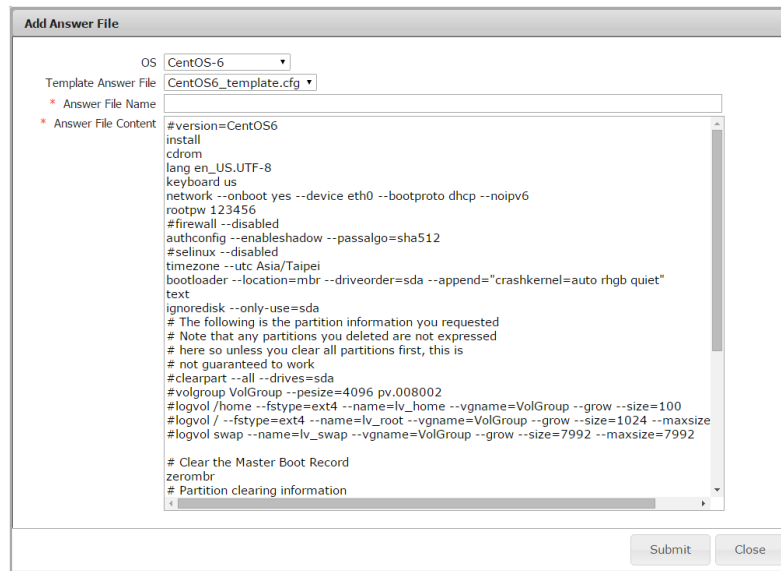


Figure 11-17

2. Select the OS type.

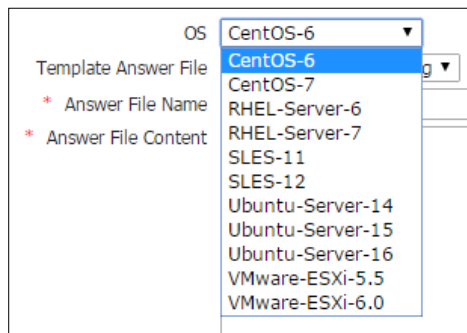


Figure 11-18

3. Select the template answer file. The drop-down list options may vary depending on the OS you selected.



Figure 11-19

4. Input the Answer File Name.
5. The Answer File Content shows the contents of the template answer file. If you select RHEL-Server-7 for the OS, the default Answer File Content options come from the RHEL7_template. You can modify the contents to meet your needs.
6. Click the **Submit** button to add the answer file or the **Close** button to abort and close this dialog box.

7. If the answer file contains incorrect usages, a Precheck Result of Answer File dialog will appear, . Read the details carefully and click **Cancel** to go back to edit the answer file, or click **Save** to ignore the precheck result.

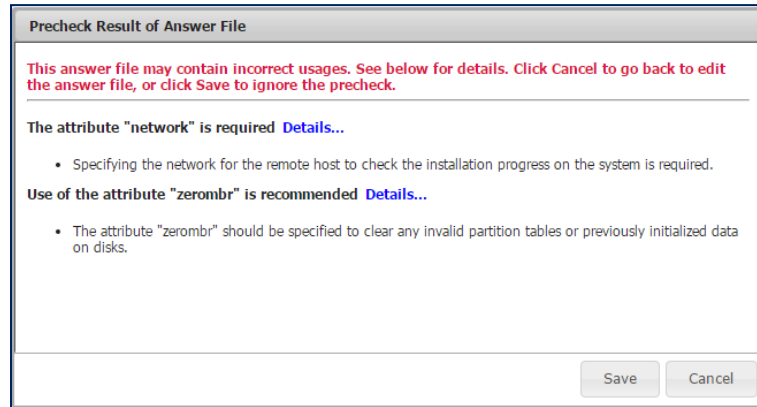


Figure 11-20

11.2.3 Editing an Answer File

1. Select one answer file to be edited in the working area. You can edit only one answer file at a time.
2. Click **Edit Answer File** in the command area and an Edit Answer File dialog box appears. You can modify the answer file name and content in this dialog box.

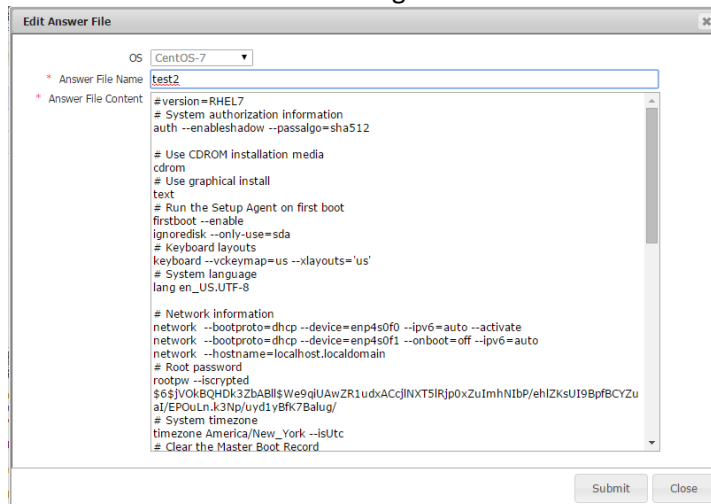


Figure 11-21

3. Click the **Submit** button to confirm the modification or the **Close** button to abort and close this dialog box.
4. If the answer file contains incorrect usages, a Precheck Result of Answer File dialog will appear. Read the details carefully and click **Cancel** to go back to edit the answer file, or click **Save** to ignore the precheck result.

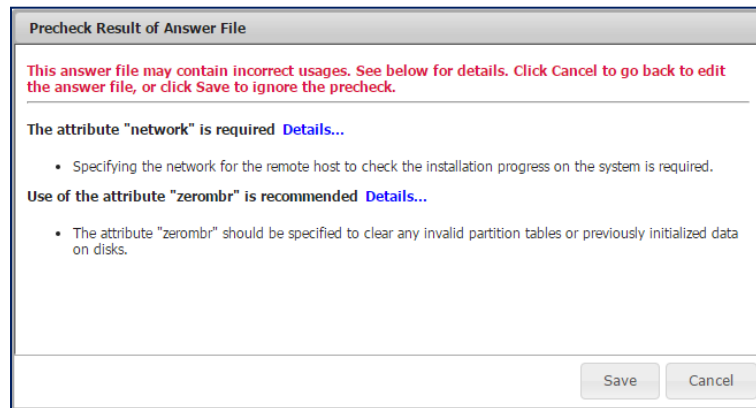


Figure 11-22



Note: The OS type is unchangeable once an answer file is created.

11.2.4 Deleting an Answer File

1. Select the answer file(s) to be deleted in the working area. You can delete multiple answer files at a time.

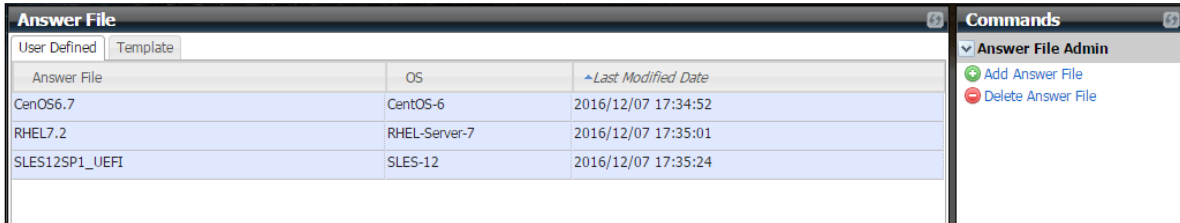


Figure 11-23

2. Click **Delete Answer File** in the command area and a Delete Answer File dialog box appears.

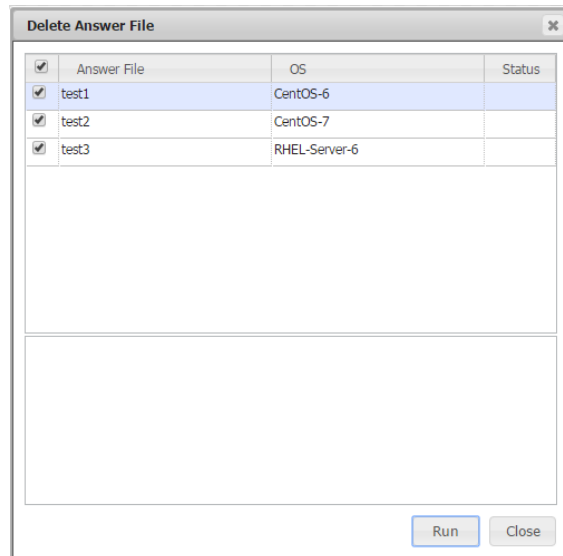


Figure 11-24

3. Click the **Run** button to delete the selected answer files or the **Close** button to abort and close this dialog box.

11.3 Deployment Progress

The working area is further divided into a task view and a detailed view. The Deployment Progress includes 4 tabs: **Pending**, **Deploying**, **Finished** and **Failed**. The detailed view shows a detailed progress of the selected task in the master view.

The screenshot shows the 'Deployment Progress' window with a table of tasks and a 'Deployment Summary' section below it.

Tas...	Host Name	Address	Stage	Installation source	Start Time	End Time	Screenshot
336...	10.146.125.134	10.146.125.134	Installing OS ...	ubuntu-16.10-server-amd64	2017/03/01 10:05:56	2017/03/01 10:10:15	View
650...	X10SRL	10.146.125.133	Boot from CD/DVD ...	CentOS-7-x86_64-Minimal-1511	2017/03/01 10:25:12	2017/03/01 10:26:18	N/A (Error)
857...	10.146.20.23	10.146.20.23	Installing OS ...	ubuntu-16.10-server-amd64	2017/03/01 10:01:52	2017/03/01 10:07:09	View
706...	X10DRE-T	10.146.23.155	Installing OS ...	ubuntu-16.10-server-amd64	2017/03/01 10:06:09	2017/03/01 10:12:14	View
528...	linux-155	10.146.23.155	Boot from CD/DVD ...	CentOS-7-x86_64-Minimal-1511	2017/03/01 10:24:23	2017/03/01 10:25:41	View


```
>> Preparing files ...
Installation source : ubuntu-16.10-server-amd64
Answer file : Ubuntu16_template.cfg
Running : Pack a new ISO DVD. Please wait for a while.
Files are ready.
>> Boot from CD/DVD ...
Running : Mount ISO image to the target host.
Running : Change boot from CD/DVD.
Installation is started.
>> Installing OS ...
Timed out. The installation log is returned.
Additional Information:
[common header]
version: 0x01
session_offset: 0x04
debugInfo_offset: 0x15
checksum: 0xe6
[session info]
Update Stages: 0
StartTime: 1488334135875
[network info]
Error code: 0x00
PCI Eth num: 0x02
>88861f45
>88861f45
Sys Eth num: 0x02
>emp0s20f0(802590eb7192): LINK-UP
>emp0s20f1(802590eb7193): NO-CARRIER
```

Figure 11-25

- The four tabs in Deployment Progress are:
 - Pending:** The task has been accepted but not yet processed by SSM. By default, SSM allows up to 10 execution tasks to run simultaneously. When 10 tasks are concurrently being executed, any remaining tasks will be queued. Users can run the **Cancel Task** web command to cancel a task.
 - Deploying:** The task has been accepted and processed by SSM. Users can run the **Cancel Task** web command to cancel the task.
 - Finished:** The task has completed successfully.
 - Failed:** The task has not completed successfully.



Note: The task will disappear immediately once it is canceled.

- The contents of the task table in the Deployment Progress are:

Task ID: The asynchronous task represents a request to deploy OS to an IPMI host.

Host Name: The name of the host is displayed here.

Address: Host IP address or DNS name.

Stage: The stages of the task. SSM will periodically automatically refresh the stages to reflect current progress. The four stages are:

- (1) **Preparing files:** in this stage, the task will check if the system is on and prepare the selected answer file and OS image for installation.
- (2) **Boot from CD/DVD:** in this stage, the task will ask BIOS to boot from a CD/DVD by changing the BIOS boot menu and rebooting the system.
- (3) **Installing OS:** in this stage, the task begins to deploy OS on the IPMI host and gets feedback with an installation message in the deployment summary area.
- (4) **Boot from disk drive:** in this stage, the task detects if installation is complete and asks BIOS to boot from a disk drive.




Installation Source The version of the OS you installed.

Start Time: Task start time.

End Time: Task end time.

Screenshot: SSM will capture the screen view of the IPMI host only when the deployment task fails. The four status of the screenshot are:

- (1) **View:** A screenshot has been captured successfully. Click the View link to view the screen of the deployment host.
- (2) **N/A (Error):** An error occurred while capturing the screenshot.
- (3) **N/A (Not supported):** Screenshot capturing is not supported for the IPMI host.
- (4) **N/A:** SSM will not capture a screenshot when deployment fails during file preparation or booting from CD/DVD.

-
- The **Download Result** icon  on the detailed view:
The **Download Result icon**  becomes available on the detailed view when the deployment task is in “**Deploying**”, “**Finished**” or “**Failed**” progress. Click the **Download Result icon**  to download a zip file of the configuration files and installation information during the deployment process. The all-in-one zip file includes:

Summary file:	The detailed progress of the deployment.
Answer file:	The answer file chosen for the deployment.
Screenshot:	A screen view of the IPMI host. Note that this file will appear depends on task status (failed), task stage (neither Installing OS stage nor Boot from disk drive stage), and the capability of the IPMI host.
Tar file:	The local information from the IPMI host, such as hardware information and network settings. SSM will collect information only when the task has timed out.

11.4 Installing Stunnel

SSM will capture the screen view of the IPMI host only when the deployment task fails. To use this function, you need to install Stunnel so that you can see the screenshot shown in Deploy Progress. Note that since BMC version 3.0 or later, the screen capture needs Stunnel for security manner.

If you haven't installed Stunnel, SSM will show the license agreement dialog box when you click **Deploy Progress**. Read the agreement carefully and click **I Agree** to continue installation.

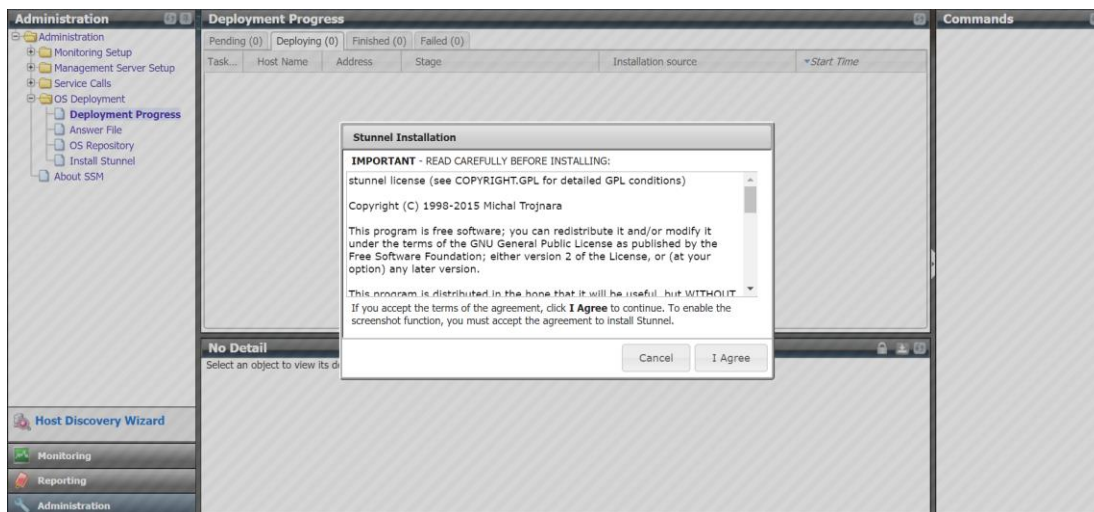


Figure 11-26

To install Stunnel, click **Install Stunnel** in the navigation area. You can either upload a Stunnel zip file or directly install from the Internet.

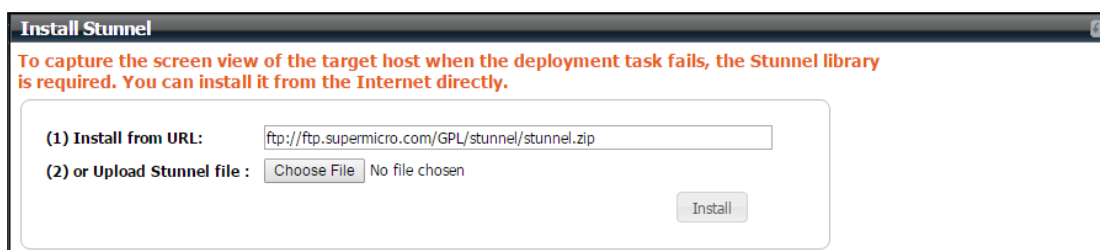


Figure 11-27

- **Install from URL**

Select this option and a license agreement dialog box appears. Read the agreement carefully and click **I Agree** to continue installation.

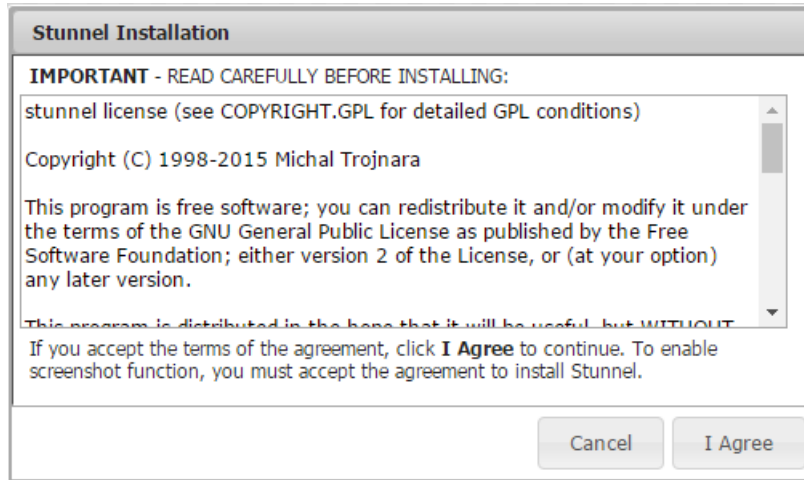


Figure 11-28

- **Upload Stunnel file**

You can find a Stunnel zip file named "stunnel.zip" on the Supermicro FTP site (<http://www.supermicro.com/wftp/GPL/stunnel/>). After selecting the Stunnel zip file, click the **Install** button to upload it.

12 Service Calls

Service Calls is an SSM feature capable of promptly responding to hosts' urgent problems. Service calls are delivered via email with messages to help the recipient diagnose the issue.

The following are some prominent features of Service Calls:

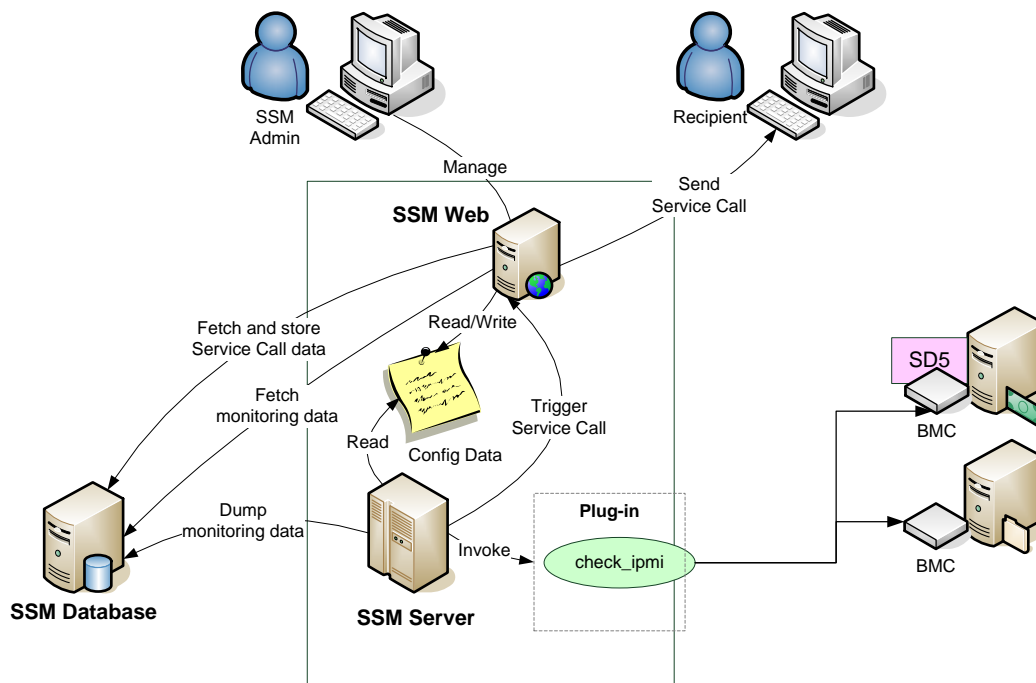


Figure 12-1

- **SSM Server:** The SSM server is a service (a daemon) program that periodically monitors hosts and services to check their status. When hosts and services encounter problems, SSM server will send internal messages to notify SSM Web.
- **SSM Web:** The SSM Web is a service program that provides a Web-based interface for Service Calls configurations. Users can manage setups, devices, customers, recipients, etc. When SSM Web receives a message from SSM Server, it will process the message and check with the setup configurations to see if any recipients are interested in the problematic host. All contacts in the recipients will be notified via emails.
- **Recipients:** Any contact in the recipients list will receive emails when their affiliated hosts have problems.

Before use, check if your managed Supermicro X10 series system is equipped with a dedicated network interface and a BMC with **SFT-DCMS-SVC-KEY** key activated. This means your host must be an IPMI host.

12.1 Service Calls Configurations

12.1.1 Setup Management

Setup is a management unit allowing users to configure a group of hosts to trigger service calls when errors occur. Click **Setup Management** in the navigation area to perform Setup Management functions. The master view shows a list of setups and the detailed view shows devices belonging to a selected setup. Besides the **Devices** tab, the detailed view also includes the **Customer** and **Recipients** tabs. Devices are a list of hosts that are defined in the setup. For example, the setup (SW Team’s Machine) includes 2 groups (DataCenter/ER/Autotest and DataCenter/ER/TwinPro) and one individual host (10.146.125.45). Therefore, the total devices in SW Team’s Machine will be 10.146.125.136 (belonging to DataCenter/ER/Autotest), 10.146.125.137 (belonging to DataCenter/ER/Autotest), 10.146.125.139 (belonging to DataCenter/ER/Autotest), 10.146.125.49 (belonging to DataCenter/ER/TwinPro), 10.146.125.50 (belonging to DataCenter/ER/TwinPro), and 10.146.125.45. Each device can be assigned to trigger service calls or not.

To complete a Service Call setup, you first need to add a site location (See 12.1.4.1 *Adding a Site Location*), a customer (See 12.1.2.1 *Adding a Customer*), and a recipient (See 12.1.3.1 *Adding a Recipient*).

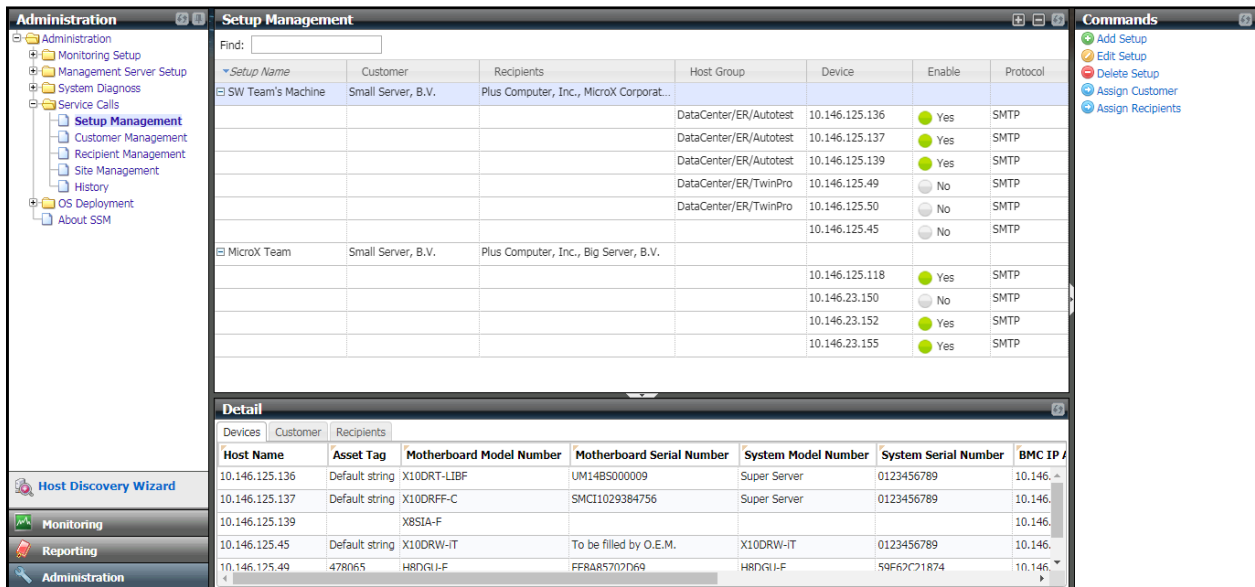


Figure 12-2

12.1.1.1 Adding a Setup

1. Click **Add Setup** in the commands area and an Add Setup dialog box appears.

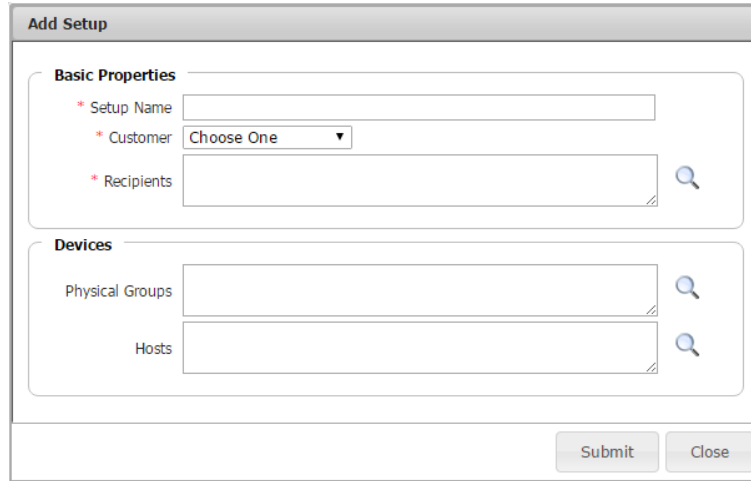





Figure 12-3

2. Input the Setup settings in this dialog box.

Name	A unique name used to identify the setup.
Customer	The customer of the selected devices. Select a customer from the Customer drop-down list. To add customers, see <i>12.1.2.1 Adding a Customer</i> for details.
Recipients	Contacts defined as a recipient can be notified by Service Calls. Click the  icon and a query dialog box appears. Multiple recipients may be selected simultaneously, but selecting at least one is required. To add recipients, see <i>12.1.3.1 Adding a Recipient</i> for details. .
Physical Groups	Click the  icon to select the physical host groups. Hosts that belong to physical host groups will send Service Calls when problems occur. Multiple physical host groups may be selected simultaneously.
Hosts	Select a host that will send Service Calls when problems occur. Click the  icon to select a host which is either an individual host or belongs to a logical group. Multiple hosts may be selected simultaneously.

Select Recipients

Find:

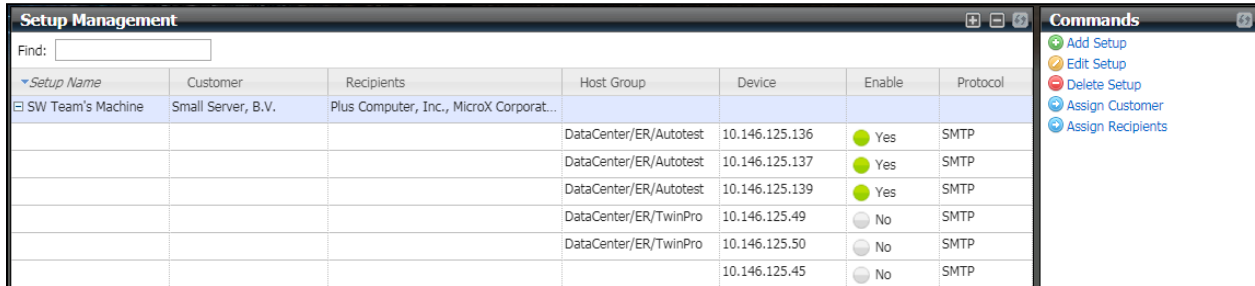
<input type="checkbox"/>	Company	Address	Contact Persons	Trigger Level
<input type="checkbox"/>	MicroY Corporation	3F., No.150, Jian 1st R...	Joshua	Local Administrator
<input type="checkbox"/>	Big Server, B.V.	Het Sterrenbeeld 28, 52...	David, May	Local Administrator
<input type="checkbox"/>	Plus Computer, Inc.	980 Rock Avenue, San ...	Ishara, Julius	Local Administrator

Figure 12-4

3. When completed, click the **Submit** button to add the setup or the **Close** button to abort and close this dialog box.

12.1.1.2 Editing a Setup

1. Select the setup to be edited in the working area. You can only edit one setup at a time.

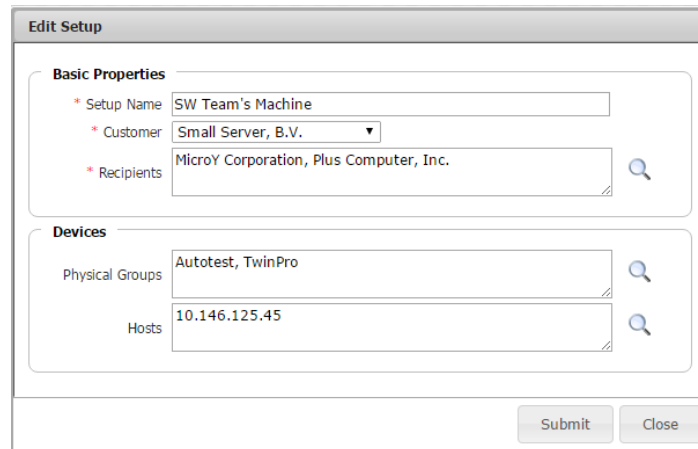


The screenshot shows the 'Setup Management' window with a search bar and a table of setups. The 'Commands' panel on the right lists actions like 'Add Setup', 'Edit Setup', 'Delete Setup', 'Assign Customer', and 'Assign Recipients'.

Setup Name	Customer	Recipients	Host Group	Device	Enable	Protocol
SW Team's Machine	Small Server, B.V.	Plus Computer, Inc., MicroX Corporat...	DataCenter/ER/Autotest	10.146.125.136	<input checked="" type="radio"/> Yes	SMTP
			DataCenter/ER/Autotest	10.146.125.137	<input checked="" type="radio"/> Yes	SMTP
			DataCenter/ER/Autotest	10.146.125.139	<input checked="" type="radio"/> Yes	SMTP
			DataCenter/ER/TwinPro	10.146.125.49	<input type="radio"/> No	SMTP
			DataCenter/ER/TwinPro	10.146.125.50	<input type="radio"/> No	SMTP
				10.146.125.45	<input type="radio"/> No	SMTP

Figure 12-5

2. Click **Edit Setup** in the commands area and an Edit Setup dialog box appears.



The 'Edit Setup' dialog box contains two sections: 'Basic Properties' and 'Devices'. The 'Basic Properties' section has fields for 'Setup Name' (SW Team's Machine), 'Customer' (Small Server, B.V.), and 'Recipients' (MicroY Corporation, Plus Computer, Inc.). The 'Devices' section has fields for 'Physical Groups' (Autotest, TwinPro) and 'Hosts' (10.146.125.45). There are 'Submit' and 'Close' buttons at the bottom.

Figure 12-6

3. Modify the setup data in the dialog box.
4. Click the **Submit** button to confirm the modification or the **Close** button to abort and close this dialog box.

12.1.1.3 Deleting a Setup

1. Select one or more setups to be deleted in the working area. You can delete multiple setups simultaneously.

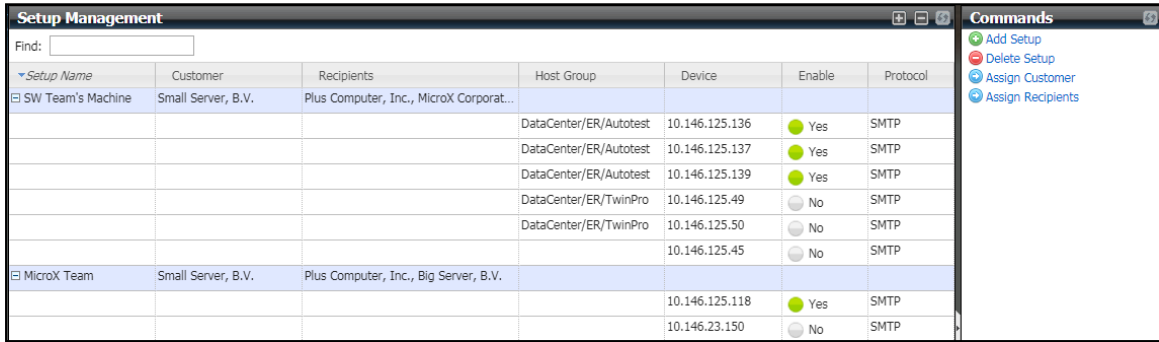


Figure 12-7

2. Click **Delete Setup** in the command area and a Delete Setup dialog box appears.

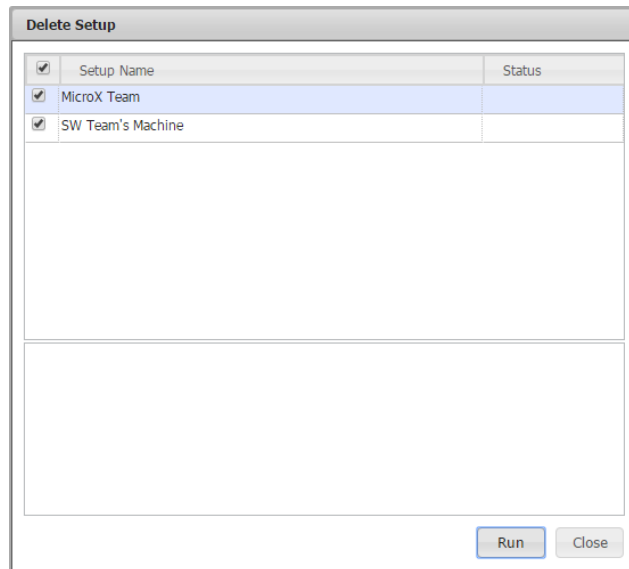


Figure 12-8

3. Click the **Run** button to delete the selected setups or the **Close** button to abort and close this dialog box.

12.1.1.4 Assigning a Customer

1. Select the setup to be edited in the working area. You can apply the same customer to different setups simultaneously.

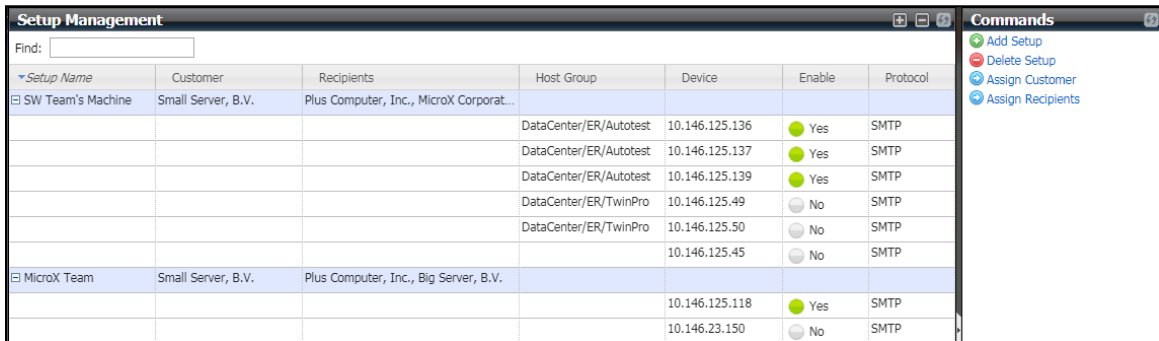


Figure 12-9

2. Click **Assign Customer** in the command area and an Assign Customer query dialog box appears.

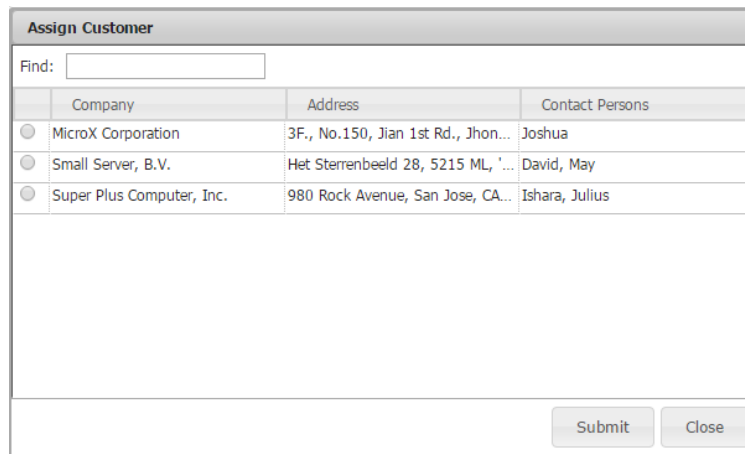


Figure 12-10

3. Select the customer to be assigned and click the **Submit** button.

12.1.1.5 Assigning a Recipient

1. Select one or more setups to be edited in the working area. You can apply the same recipients to different setups simultaneously.

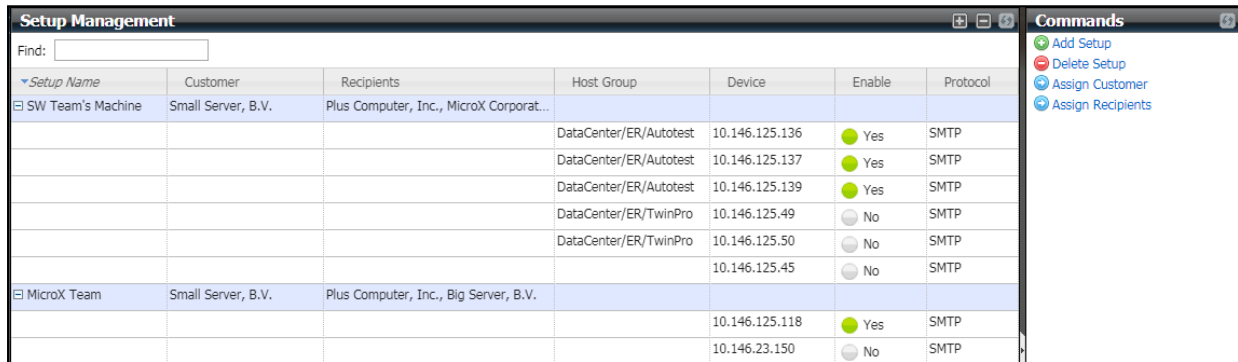


Figure 12-11

2. Click **Assign Recipients** in the command area and an Assign Recipients query dialog box appears.

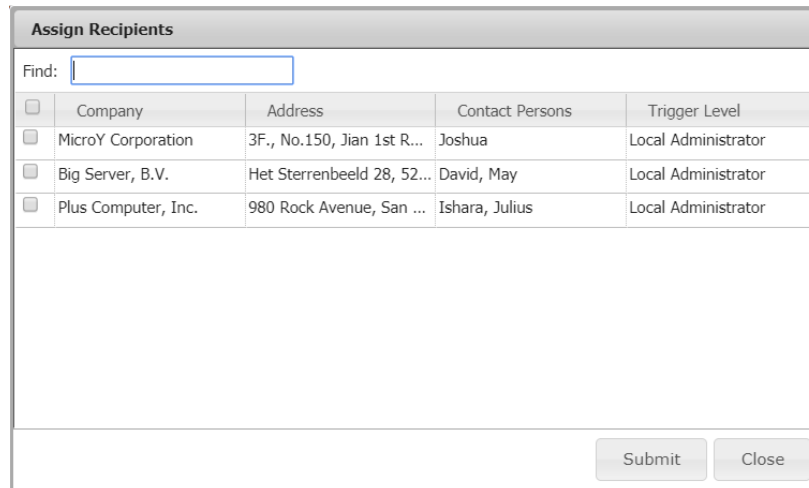


Figure 12-12

3. Select the recipients to be assigned and click the **Submit** button.

12.1.1.6 Editing a Device

Device data is the information that will be included in the Service Call alert. Ensure the device data you enter or edit is correct or it will be hard to identify the problematic device.

1. Select a device to be edited in the working area. This **Edit Device Data** only supports IPMI hosts with the SFT-DCMS-SVC-KEY product key activated. You can only edit one device at a time.

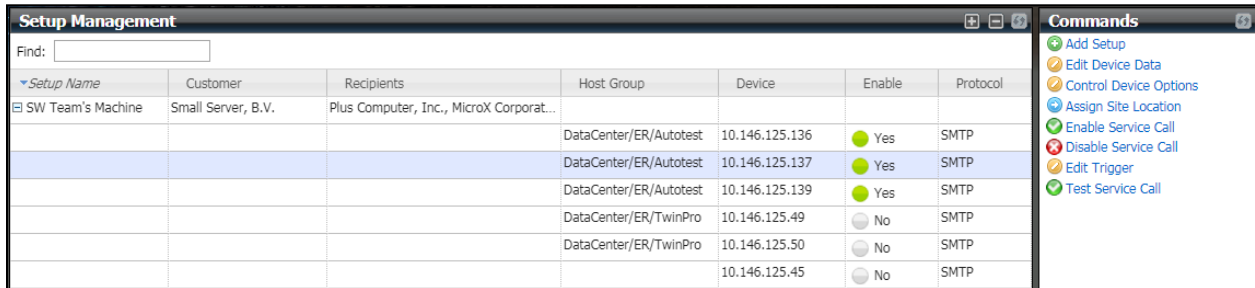


Figure 12-13

2. Click **Edit Device Data** in the commands area and an Edit Device Data dialog box appears.

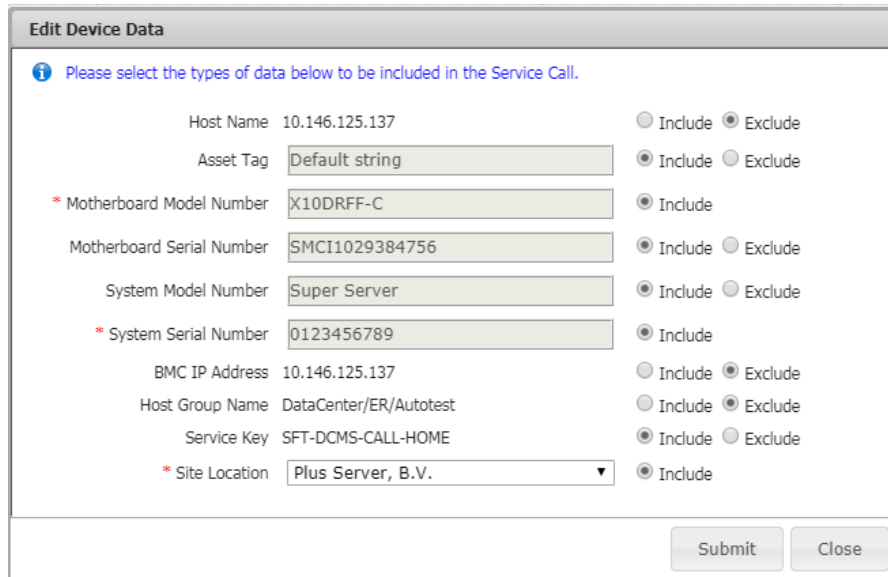


Figure 12-14

3. Edit the device data in the dialog box.

Host Name	A unique name used to identify the host.
Asset Tag	The asset tag of the motherboard. The value will be automatically provided by System Information Service (if available).
Motherboard Model Number	The model number of the motherboard. The value will be automatically provided by System Information Service (if available).
Motherboard Serial Number	The serial number of the motherboard. The value will be automatically provided by System Information Service (if available).
System Model Number	The model number of the system. The value will be automatically provided by System Information Service (if available).
System Serial Number	The serial number of the system. The value will be automatically provided by System Information Service (if available).
IPMI IP Address	The IP address of the IPMI host. The read only value is converted from the address of the host.
Host Group Name	The host group that the host belongs to.
Service Key	The service key of the host.
Site Location	The site location of the host. Select a site location from the Site Location drop-down list. See <i>12.1.4.1 Adding a Site Location</i> for more information about adding a site location.



Notes:

- Only when the **Include** checkbox is checked will the Service Call alert include all of the attributes.
 - “Asset Tag”, “Motherboard Model Number”, “Motherboard Serial Number”, “System Model Number”, and “System Serial Number” in device data will be updated later whenever DMI or Asset data are gathered by
-

System Information service. You should check if the status of IPMI System Information/System Information service is in OK Hard state, if not, try to resolve the failed items and execute “Check Now” web command to force the service check to be performed immediately.

4. Click the **Submit** button to confirm the modification or the **Close** button to abort and close this dialog box.

12.1.1.7 Control Device Options

1. Select one or more devices to be edited in the working area. You can apply the same device options to different devices simultaneously.

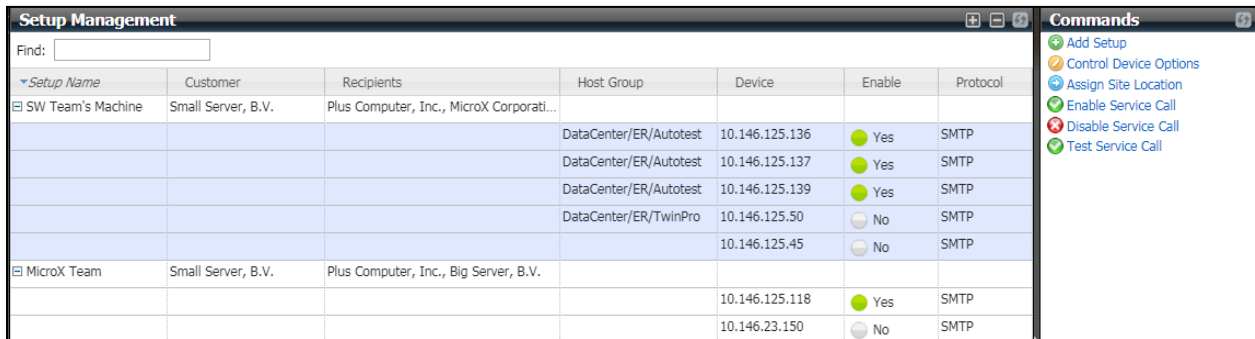


Figure 12-15

2. Click **Control Device Options** in the command area and a Control Device Options query dialog box appears.

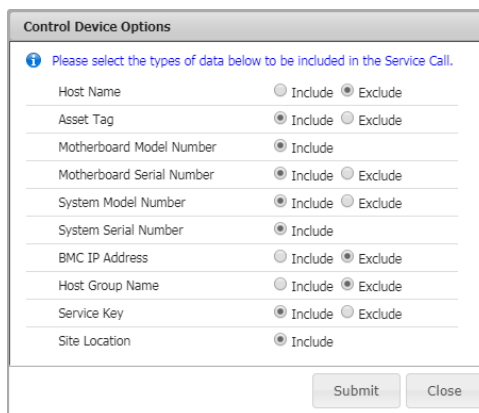


Figure 12-16

3. Select the attributes to be included in Service Call alert and click the **Submit** button.

12.1.1.8 Assigning a Site Location

1. Select one or more devices to be edited in the working area. You can apply the same site location to different devices simultaneously.

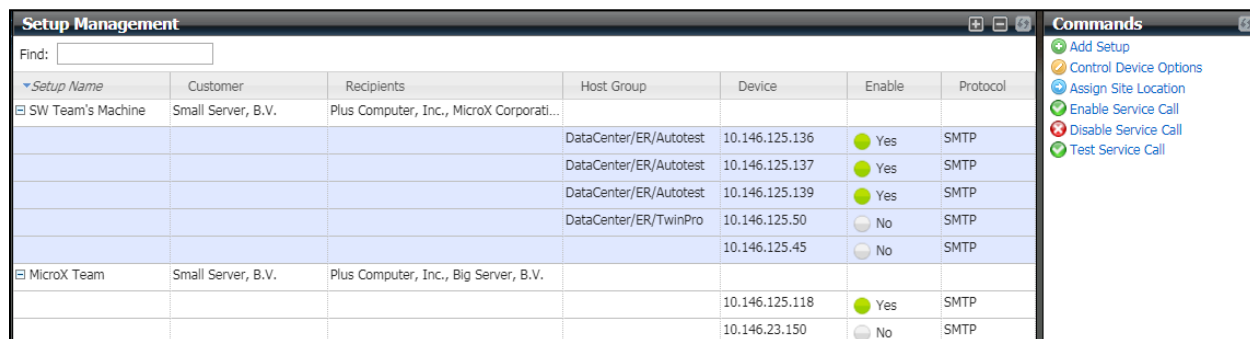


Figure 12-17

2. Click **Assign Site Location** in the command area and an Assign Site Location query dialog box appears.

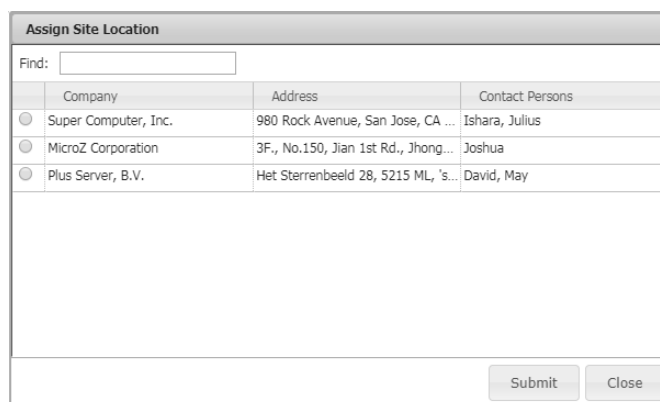


Figure 12-18

3. Select the site location to be assigned and click the **Submit** button.

12.1.1.9 Editing Trigger

SSM fetches the trigger items from the SDR information and SEL definitions in the BMC based on the last check result of IPMI/Redfish Sensor Health services. It will collect all trigger items and store them into the cache. After initialization, the trigger items will be loaded from the cache. The cache is changed while the service check of IPMI/Redfish Sensor Health is performed. Note that only hardware failures in SEL can be selected as the trigger items.

Follow these steps to edit the triggers for a device:

1. Select one device to set for triggering in the working area.

Setup Management							Commands
Setup Name	Customer	Recipients	Host Group	Device	Enable	Protocol	
SW Team's Machine	Small Server, B.V.	Plus Computer, Inc., MicroX Corporat...	DataCenter/ER/Autotest	10.146.125.136	<input checked="" type="radio"/> Yes	SMTP	<input checked="" type="radio"/> Add Setup
			DataCenter/ER/Autotest	10.146.125.137	<input checked="" type="radio"/> Yes	SMTP	<input checked="" type="radio"/> Edit Device Data
			DataCenter/ER/Autotest	10.146.125.139	<input checked="" type="radio"/> Yes	SMTP	<input checked="" type="radio"/> Control Device Options
			DataCenter/ER/TwinPro	10.146.125.49	<input type="radio"/> No	SMTP	<input checked="" type="radio"/> Assign Site Location
			DataCenter/ER/TwinPro	10.146.125.50	<input type="radio"/> No	SMTP	<input checked="" type="radio"/> Enable Service Call
				10.146.125.45	<input type="radio"/> No	SMTP	<input checked="" type="radio"/> Disable Service Call
							<input checked="" type="radio"/> Edit Trigger
							<input checked="" type="radio"/> Test Service Call

Figure 12-19

2. Click **Edit Trigger** in the command area and the Edit Trigger dialog box appears.

Edit Trigger				
Find Trigger Item: <input type="text"/>				
Trigger Items	Local Administrator Setting			Supermicro Service Setting
	<input type="checkbox"/> Error	<input type="checkbox"/> Critical	<input type="checkbox"/> Warning	<input checked="" type="checkbox"/> Error
BMC is not available	<input type="checkbox"/> Error			
FAN1	<input type="checkbox"/> Error	<input type="checkbox"/> Critical	<input type="checkbox"/> Warning	<input checked="" type="checkbox"/> Error
FAN2	<input type="checkbox"/> Error	<input type="checkbox"/> Critical	<input type="checkbox"/> Warning	<input checked="" type="checkbox"/> Error
FAN3	<input type="checkbox"/> Error	<input type="checkbox"/> Critical	<input type="checkbox"/> Warning	<input checked="" type="checkbox"/> Error
FAN4	<input type="checkbox"/> Error	<input type="checkbox"/> Critical	<input type="checkbox"/> Warning	<input checked="" type="checkbox"/> Error
FANA	<input type="checkbox"/> Error	<input type="checkbox"/> Critical	<input type="checkbox"/> Warning	<input checked="" type="checkbox"/> Error
FANB	<input type="checkbox"/> Error	<input type="checkbox"/> Critical	<input type="checkbox"/> Warning	<input checked="" type="checkbox"/> Error
PS2 Status	<input type="checkbox"/> Error			<input checked="" type="checkbox"/> Error
Memory - Correctable ECC			<input type="checkbox"/> Warning	
Memory - Uncorrectable ECC	<input type="checkbox"/> Error			<input checked="" type="checkbox"/> Error
Drive Slot (Bay) - Drive Presence (HDD removed)	<input type="checkbox"/> Error			
CPLD - CATERR	<input type="checkbox"/> Error			<input checked="" type="checkbox"/> Error
BIOS OEM - Failing DIMM: DIMM location and Mapped-Out	<input type="checkbox"/> Error			<input checked="" type="checkbox"/> Error

Figure 12-20

3. Check any trigger items that Local Administrator recipients are interested in. By default, all triggers for a device are left unchecked. For Local Administrator recipients, you can select the checkboxes of all Error items in the Error column under the Local Administrator Setting. For Supermicro Service recipients, the type of triggers is limited: only Error items are available. Also, all triggers for a device are locked and checked by default.
4. Click the **Submit** button or the **Close** button to exit.

Follow these steps to edit triggers for multiple devices:

1. Select more devices to be set triggers simultaneously in the working area.

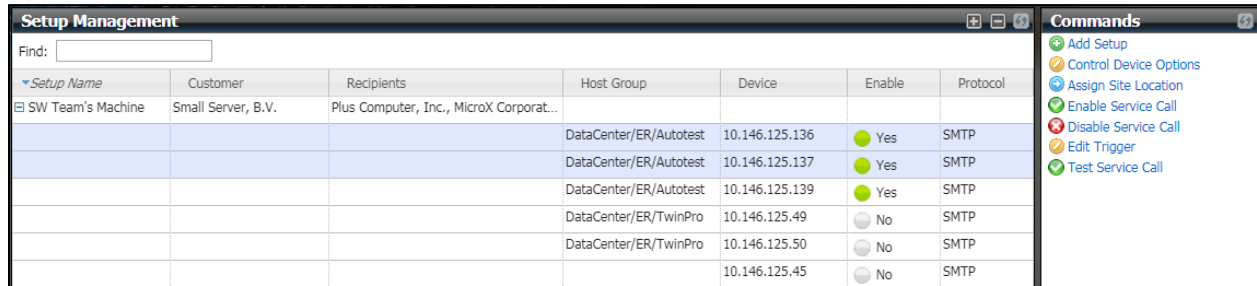


Figure 12-21

2. Click **Edit Trigger** in the command area and the Edit Trigger dialog box appears. You can select the boxes in the Override column to apply the current settings to all selected devices. If the boxes in the Override column are not selected, the original settings are kept. When multiple devices are selected, only the **Common Trigger Items** of the selected devices are shown in the Edit Trigger dialog box.

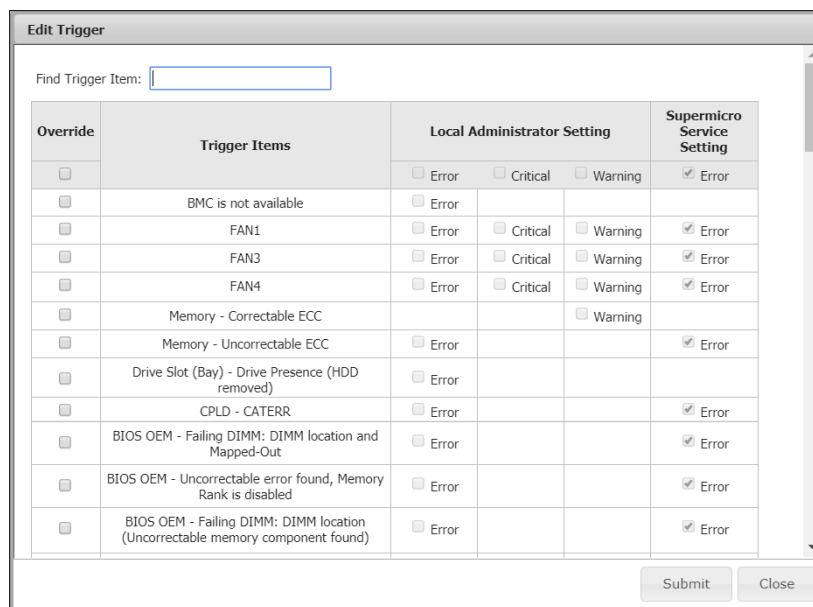


Figure 12-22

3. Check any trigger items that Local Administrator recipients are interested in. For Local Administrator recipients, you can select the checkbox in the Error column under the Local Administrator Setting, to check all Error items at once. For Supermicro Service recipients, the type of triggers is limited: only Error items are available. Also, all triggers for a device are locked and checked by default.
4. Click the **Submit** button or the Close button to exit.

12.1.1.10 Enabling a Service Call

The Enable status means the device is configured and is ready to trigger alerts whenever the device encounters an error. Hosts requiring immediate attention should have the value of the Enable attribute set to **Yes**. By default, all devices disable service calls. The **Enable Service Call** command is designed for users to quickly enable multiple devices simultaneously. Note that **Enable Service Call** only supports IPMI hosts with the SFT-DCMS-SVC-KEY product key activated. In the figure below, all devices in the setup are shown in the detailed view. Follow these steps:

Host Name	Asset Tag	Motherboard Mo...	Motherboard Serial ...	System Model Nu...	System Serial ...	BMC IP Ad...	Host Group Name	Enable	Protocol	Service Key	Site Location
10.146.125.136	Default str...	X10DRT-LIBF	UM14BS000009	Super Server	0123456789	10.146.125.136	DataCenter/ER/Autotest	<input checked="" type="radio"/> Yes	SMTP	OK	Plus Server, B.V.
10.146.125.137	Default str...	X10DRFF-C	SMCI1029384756	Super Server	0123456789	10.146.125.137	DataCenter/ER/Autotest	<input checked="" type="radio"/> Yes	SMTP	OK	Plus Server, B.V.
10.146.125.139		X8SIA-F				10.146.125.139	DataCenter/ER/Autotest	<input checked="" type="radio"/> Yes	SMTP	NOK	Plus Server, B.V.
10.146.125.45	Default str...	X10DRW-IT	To be filled by O.E.M.	X10DRW-IT	0123456789	10.146.125.45		<input type="radio"/> No	SMTP	OK	
10.146.125.49	478065	H8DGU-F	FEBA85702D69	H8DGU-F	59E62C21874	10.146.125.49	DataCenter/ER/TwinPro	<input type="radio"/> No	SMTP	NOK	
10.146.125.50	SUMTEST	X10DRT-PT	ZM15AS013805	@@Super Server Mac...	0123456789	10.146.125.50	DataCenter/ER/TwinPro	<input type="radio"/> No	SMTP	OK	

Figure 12-23

1. Select one or more devices to be enabled in the working area. You can enable multiple devices simultaneously.

Setup Name	Customer	Recipients	Host Group	Device	Enable	Protocol
SW Team's Machine	Small Server, B.V.	Plus Computer, Inc., MicroX Corporat...				
			DataCenter/ER/Autotest	10.146.125.136	<input checked="" type="radio"/> Yes	SMTP
			DataCenter/ER/Autotest	10.146.125.137	<input checked="" type="radio"/> Yes	SMTP
			DataCenter/ER/Autotest	10.146.125.139	<input checked="" type="radio"/> Yes	SMTP
			DataCenter/ER/TwinPro	10.146.125.49	<input type="radio"/> No	SMTP
			DataCenter/ER/TwinPro	10.146.125.50	<input type="radio"/> No	SMTP
				10.146.125.45	<input type="radio"/> No	SMTP

Commands

- Add Setup
- Control Device Options
- Assign Site Location
- Enable Service Call
- Disable Service Call
- Edit Trigger
- Test Service Call

Figure 12-24

2. Click **Enable Service Call** in the command area and an Enable Service Call dialog box appears.

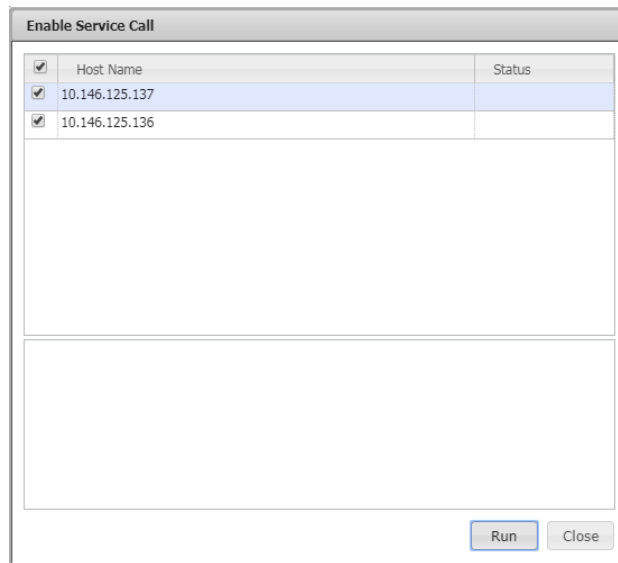


Figure 12-25



Note: Since the IPMI Sensor Health and IPMI SEL Health²¹ services are used to check the health status of a device, if both services are unavailable the device will fail to be enabled.

3. Click the **Run** button to enable the selected devices or the **Close** button to abort and close this dialog box.

12.1.1.11 Disabling a Service Call

1. Select one or more devices to be disabled in the working area. You can disable multiple devices simultaneously.

Setup Management							Commands
Setup Name	Customer	Recipients	Host Group	Device	Enable	Protocol	
SW Team's Machine	Small Server, B.V.	Plus Computer, Inc., MicroX Corporat...	DataCenter/ER/Autotest	10.146.125.136	<input checked="" type="radio"/> Yes	SMTP	<ul style="list-style-type: none"> <input checked="" type="radio"/> Add Setup <input type="radio"/> Control Device Options <input type="radio"/> Assign Site Location <input checked="" type="radio"/> Enable Service Call <input type="radio"/> Disable Service Call <input type="radio"/> Edit Trigger <input checked="" type="radio"/> Test Service Call
			DataCenter/ER/Autotest	10.146.125.137	<input checked="" type="radio"/> Yes	SMTP	
			DataCenter/ER/Autotest	10.146.125.139	<input checked="" type="radio"/> Yes	SMTP	
			DataCenter/ER/TwinPro	10.146.125.49	<input type="radio"/> No	SMTP	
			DataCenter/ER/TwinPro	10.146.125.50	<input type="radio"/> No	SMTP	
				10.146.125.45	<input type="radio"/> No	SMTP	

Figure 12-26

2. Click **Disable Service Call** in the command area and a Disable Service Call dialog box appears.

²¹ Currently, only hardware failure sensors support Service Calls. When non-hardware sensor item in IPMI SEL Health becomes critical, no alert will be sent.

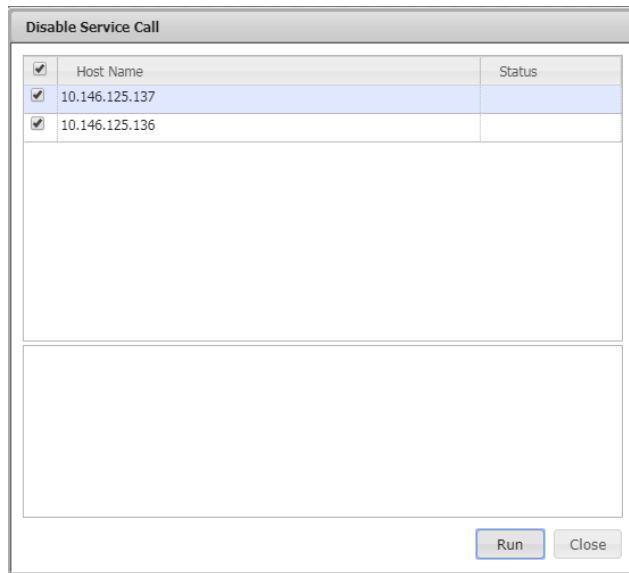


Figure 12-27

3. Click the **Run** button to disable the selected devices or the **Close** button to abort and close this dialog box.

12.1.1.12 Testing Service Call

1. Select one or more devices to be tested in the working area. You can test multiple devices simultaneously.

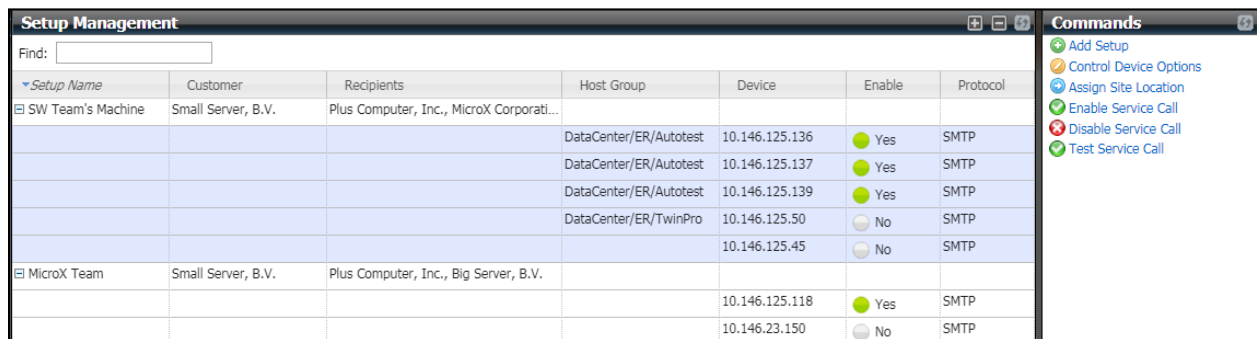


Figure 12-28

The Test Service Call is designed to pre-check if any settings will prevent users from receiving any service calls. Below is the list of check items:

Check Items	Solution
The SFT-DCMS-SVC-KEY product key should be available.	Contact Supermicro if you don't have node product key for BMC.
At least one of the contacts in the recipient(s) field should have an e-mail address.	You should review the e-mail addresses of the contacts in recipient(s) field since Service Call alerts are delivered via e-mail. See <i>12.1.3.2 Editing a Recipient, 12.1.2.4 Assigning a Contact, and 6.4 Contact Management</i> for details.
At least one of the trigger items should be set.	By default, none of the trigger items are selected and no Service Call alert is to be sent. Remember to select the triggers that you are interested in. Refer to <i>12.1.1.9 Editing Trigger</i> .
Local Administrator triggers should have their recipients.	Service Call alerts are delivered to Local Administrator recipients by their designations.
The services used to check the health status of the device should be available.	If either one of IPMI Sensor Health and IPMI SEL Health services used to check the health status of a device is not available, you should use the Add Service Wizard to add services. See <i>6.2.3 Add Service Wizard</i> .
Attributes for device data cannot be left blank.	To identify the problematic devices, it's required to provide the necessary device data. See <i>12.1.1.6 Editing a Device</i> .
The device is enabled.	To enable Service Call, see <i>12.1.1.10 Enabling a Service Call</i> for details.

2. Click **Test Service Call** in the command area and a Test Service Call dialog box appears.

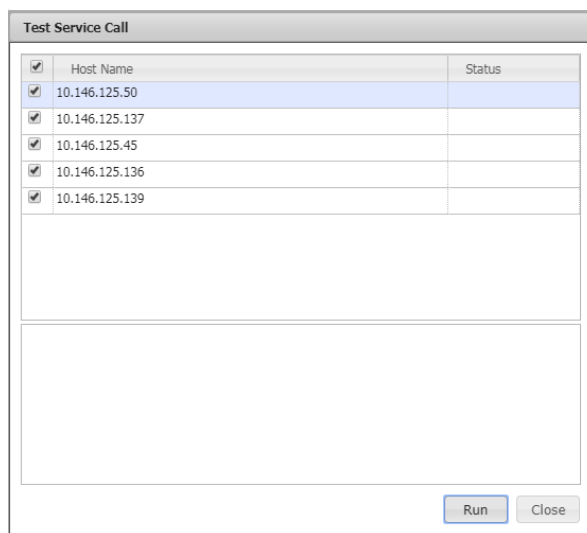


Figure 12-29

3. Click the **Run** button to check the device setting or the **Close** button to abort and close this dialog

box.



Note: You should try to resolve the failed items if the test fails; otherwise you cannot receive any Service Calls alerts.

12.1.2 Customer Management

Customers will be used in Setup configurations. Click **Customer Management** in the navigation area to perform Customer Management functions.

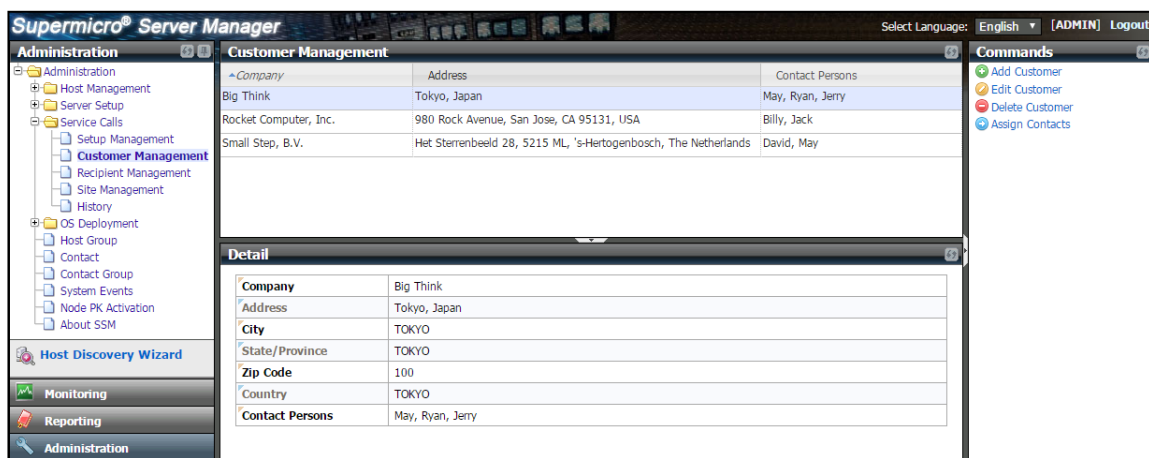


Figure 12-30

12.1.2.1 Adding a Customer

1. Click **Add Customer** in the commands area and an Add Customer dialog box appears.

Add Customer

* Company Copy From

Address

City

State/Province

Zip Code


Country

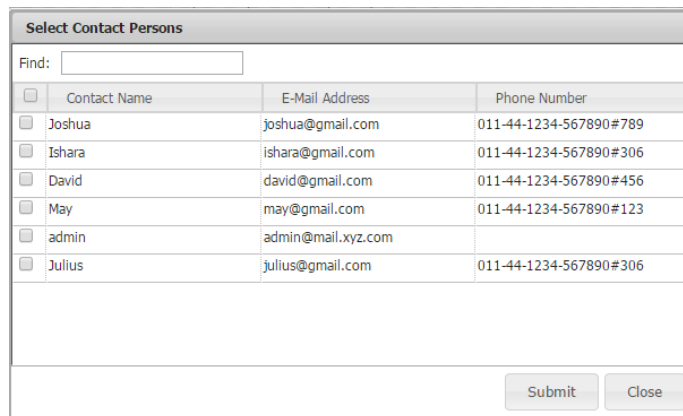
Contact Persons

Submit Close

Figure 12-31

2. Input the customer data in this dialog box.

Company	A unique name used to identify the company of the customer.
Address	The address of the customer.
City	The city where the customer is located.
State/Province	The state or province where the customer is located.
Zip Code	The zip code of the address.
Country	The country of the customer.
Contact Persons	Contacts that belong to the company. Click the  icon to select the contact persons and a query dialog box appears. You can refer to <i>6.4 Contact Management</i> to add contacts first.



<input type="checkbox"/>	Contact Name	E-Mail Address	Phone Number
<input type="checkbox"/>	Joshua	joshua@gmail.com	011-44-1234-567890#789
<input type="checkbox"/>	Ishara	ishara@gmail.com	011-44-1234-567890#306
<input type="checkbox"/>	David	david@gmail.com	011-44-1234-567890#456
<input type="checkbox"/>	May	may@gmail.com	011-44-1234-567890#123
<input type="checkbox"/>	admin	admin@mail.xyz.com	
<input type="checkbox"/>	Julius	julius@gmail.com	011-44-1234-567890#306

Figure 12-32



Note: You can click on the **Copy From** pull-down menu to copy the customer data from an existing customer.

- When complete, click the **Submit** button to add the customer or the **Close** button to abort and close this dialog box.

12.1.2.2 Editing a Customer

1. Click **Edit Customer** in the commands area and an Edit Customer dialog box appears. You can only edit one customer at a time.

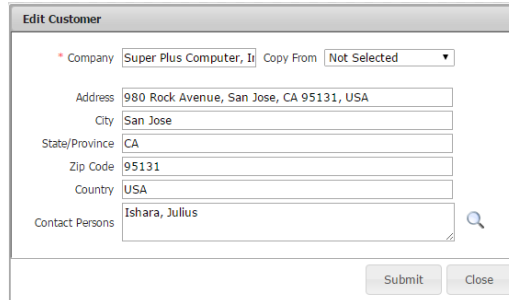


Figure 12-33

2. Modify the customer data in the dialog box.
3. Click the **Submit** button to confirm the modification or the **Close** button to abort and close this dialog box.

12.1.2.3 Deleting a Customer

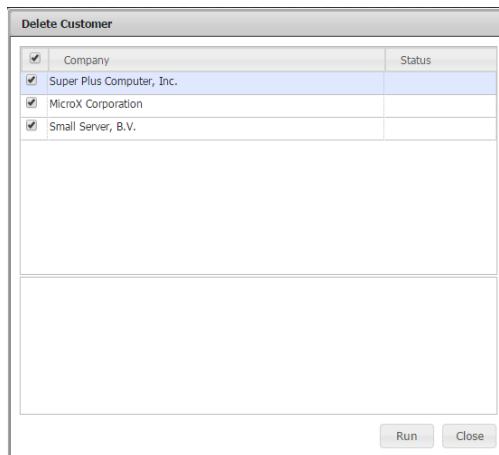
1. Select one or more customers to be deleted in the working area. You can delete multiple customers simultaneously.



Company	Address	Contact Persons
Super Plus Computer, Inc.	980 Rock Avenue, San Jose, CA 95131, ...	Ishara, Julius
Small Server, B.V.	Het Sterrenbeeld 28, 5215 ML, 's-Hertog...	David, May
MicroX Corporation	3F., No.150, Jian 1st Rd., Jhonghe Dist...	Joshua

Figure 12-34

2. Click **Delete Customer** in the command area and a Delete Customer dialog box appears.



Company	Status
<input checked="" type="checkbox"/> Super Plus Computer, Inc.	
<input checked="" type="checkbox"/> MicroX Corporation	
<input checked="" type="checkbox"/> Small Server, B.V.	

Figure 12-35

3. Click the **Run** button to delete the selected customers or the **Close** button to abort and close this dialog box.

12.1.2.4 Assigning a Contact

1. Select one or more customers in the working area. You can assign multiple contacts to one customer simultaneously.



Figure 12-36

2. Click **Assign Contacts** in the command area and an Assign Contacts query dialog box appears.

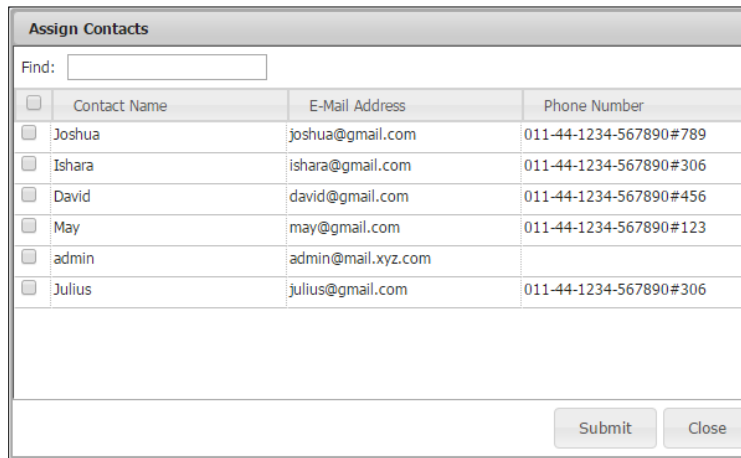


Figure 12-37

3. Select the contacts to be assigned and click the **Submit** button.

12.1.3 Recipient Management

Recipients will be used in Setup configurations. Click **Recipient Management** in the navigation area to perform Recipient Management functions. Configure it carefully since only contacts listed as recipients will receive emails when their affiliated hosts encounter problems.

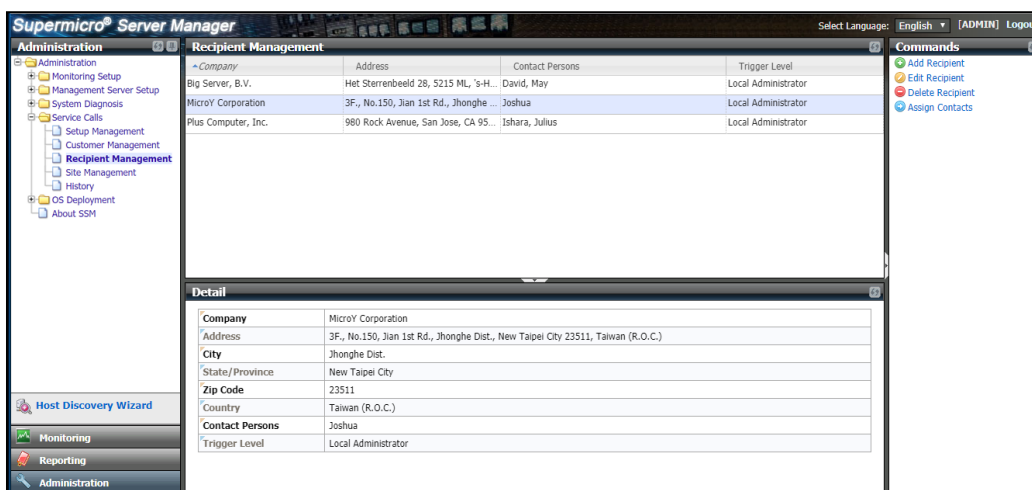


Figure 12-38

12.1.3.1 Adding a Recipient

1. Click **Add Recipient** in the commands area and an Add Recipient dialog box appears.

Add Recipient

* Company Copy From

Address

City

State/Province

Zip Code


Country

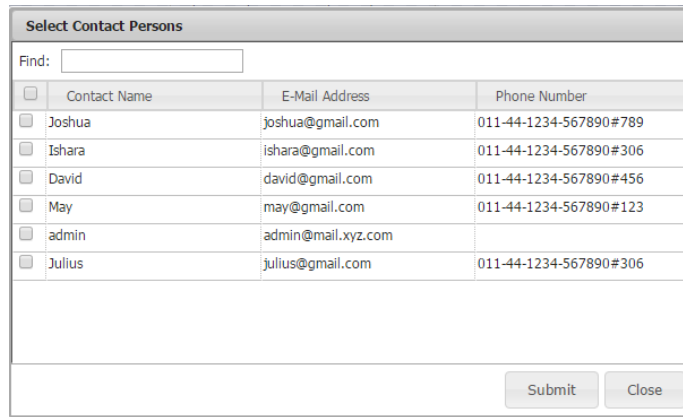
* Contact Persons

Trigger Level Local Administrator

Figure 12-39

2. Input the recipient data in this dialog box.
 - Company A unique name used to identify the company of the recipient.
 - Address The address of the recipient.
 - City The city where the recipient is located.

State/Province	The state or province where the recipient is located.
Zip Code	The zip code of the address.
Country	The country of the recipient.
Contact Persons	Contacts that will be notified by SSM when their affiliated hosts encounter problems. Click the  icon to select the contact persons and a query dialog box appears. You can refer to <i>6.4 Contact Management</i> to add contacts first.
Trigger Level	Sets the level of support. Currently, only the Local Administrator is supported. Local Administrator is for the local tech support in the customer's company or the outsourced tech support team.



<input type="checkbox"/>	Contact Name	E-Mail Address	Phone Number
<input type="checkbox"/>	Joshua	joshua@gmail.com	011-44-1234-567890#789
<input type="checkbox"/>	Ishara	ishara@gmail.com	011-44-1234-567890#306
<input type="checkbox"/>	David	david@gmail.com	011-44-1234-567890#456
<input type="checkbox"/>	May	may@gmail.com	011-44-1234-567890#123
<input type="checkbox"/>	admin	admin@mail.xyz.com	
<input type="checkbox"/>	Julius	julius@gmail.com	011-44-1234-567890#306

Figure 12-40

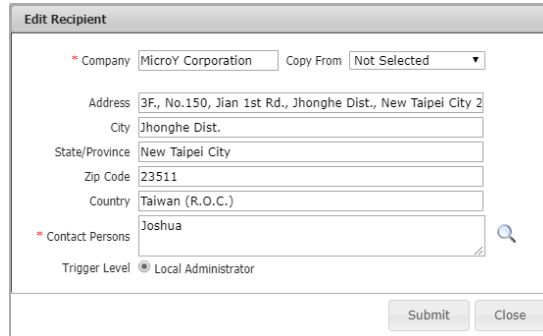


Note: You can click on the **Copy From** pull-down menu to copy the recipient data from an existing recipient.

- When completed, click the **Submit** button to add the recipient or the **Close** button to abort and close this dialog box.

12.1.3.2 Editing a Recipient

1. Click **Edit Recipient** in the commands area and an Edit Recipient dialog box appears. You can only edit one recipient at a time.



The 'Edit Recipient' dialog box contains the following information:

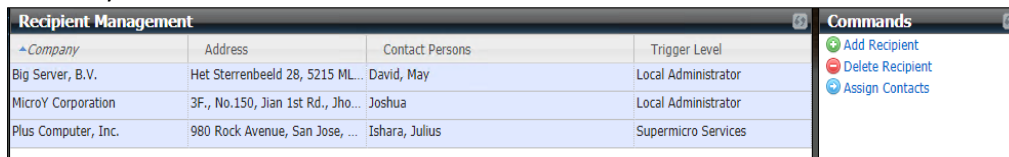
- Company: MicroY Corporation
- Copy From: Not Selected
- Address: 3F, No.150, Jian 1st Rd., Jhonghe Dist., New Taipei City 2
- City: Jhonghe Dist.
- State/Province: New Taipei City
- Zip Code: 23511
- Country: Taiwan (R.O.C.)
- Contact Persons: Joshua
- Trigger Level: Local Administrator

Figure 12-41

2. Modify the recipient data in the dialog box.
3. Click the **Submit** button to confirm the modification or the **Close** button to abort and close this dialog box.

12.1.3.3 Deleting a Recipient

1. Select one or more recipients to be deleted in the working area. You can delete multiple recipients simultaneously.



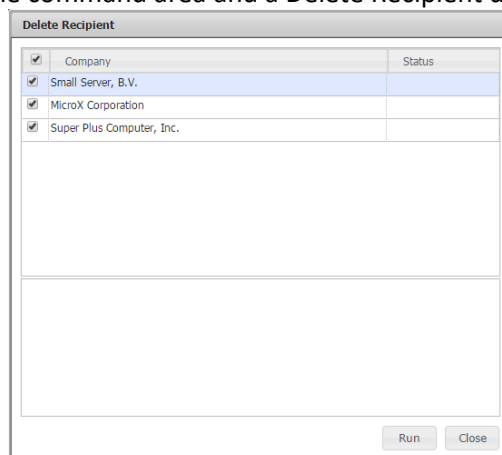
Company	Address	Contact Persons	Trigger Level
Big Server, B.V.	Het Sterrenbeeld 28, 5215 ML...	David, May	Local Administrator
MicroY Corporation	3F., No.150, Jian 1st Rd., Jho...	Joshua	Local Administrator
Plus Computer, Inc.	980 Rock Avenue, San Jose, ...	Ishara, Julius	Supermicro Services

Commands panel:

- Add Recipient
- Delete Recipient
- Assign Contacts

Figure 12-42

2. Click **Delete Recipient** in the command area and a Delete Recipient dialog box appears.



The 'Delete Recipient' dialog box contains the following information:

Company	Status
<input checked="" type="checkbox"/> Small Server, B.V.	
<input checked="" type="checkbox"/> MicroX Corporation	
<input checked="" type="checkbox"/> Super Plus Computer, Inc.	

Figure 12-43

3. Click the **Run** button to delete the selected recipients or the **Close** button to abort and close this dialog box.

12.1.3.4 Assigning a Contact

In Service Calls, users are required to assign contacts when managing the “Customers”, “Recipients” and “Site Locations.” The steps to assign a contact are all the same in different configurations. For details, please see 12.1.2.4 *Assigning a Contact*.

12.1.4 Site Management

Site Location will be used in Editing a Device. Click **Site Management** in the navigation area to perform Site Management functions.

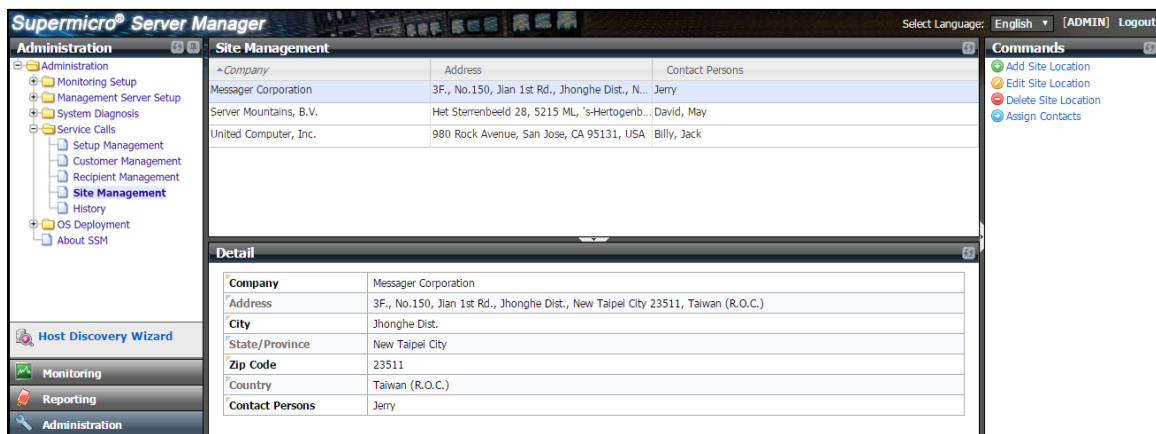


Figure 12-44

12.1.4.1 Adding a Site Location


1. Click **Add Site Location** in the commands area and an Add Site Location dialog box appears.

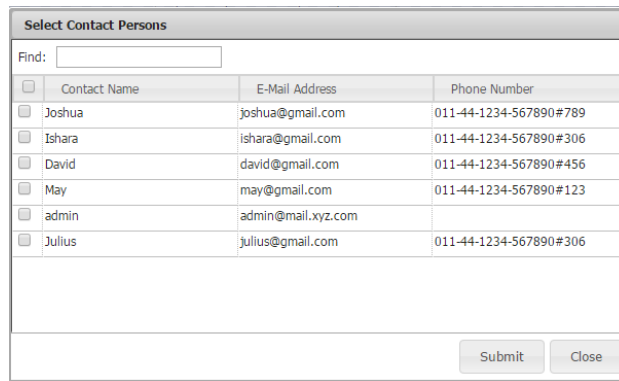
The Add Site Location dialog box contains the following fields and controls:

- Company**: Input field with a red asterisk, followed by a **Copy From** dropdown menu set to **Not Selected**.
- Address**: Input field.
- City**: Input field.
- State/Province**: Input field.
- Zip Code**: Input field.
- Country**: Input field.
- Contact Persons**: Input field with a red asterisk and a search icon.
- Submit** and **Close** buttons at the bottom right.

Figure 12-45

2. Input the site location data in this dialog box.

Company	A unique name used to identify the company of the site location.
Address	The address of the site location.
City	The city where the site location is located.
State/Province	The state or province where the site location is located.
Zip Code	The zip code of the address.
Country	The country of the site location.
Contact Persons	Contacts that belong to the company. Click the  icon to select the contact persons and a query dialog box appears. You can refer to 6.4 Contact Management to add contacts first.



<input type="checkbox"/>	Contact Name	E-Mail Address	Phone Number
<input type="checkbox"/>	Joshua	joshua@gmail.com	011-44-1234-567890#789
<input type="checkbox"/>	Ishara	ishara@gmail.com	011-44-1234-567890#306
<input type="checkbox"/>	David	david@gmail.com	011-44-1234-567890#456
<input type="checkbox"/>	May	may@gmail.com	011-44-1234-567890#123
<input type="checkbox"/>	admin	admin@mail.xyz.com	
<input type="checkbox"/>	Julius	julius@gmail.com	011-44-1234-567890#306

Figure 12-46




Note: You can click on the **Copy From** pull-down menu to copy the site location data from an existing site location.

- When completed, click the **Submit** button to add the contact or the **Close** button to abort and close this dialog box.

12.1.4.2 Editing a Site Location

1. Click **Edit Site Location** in the commands area and an Edit Site Location dialog box appears. You can only edit one site location at a time.



The dialog box titled "Edit Site Location" contains the following fields and values:

- Company: MicroZ Corporation
- Copy From: Not Selected
- Address: 3F., No.150, Jian 1st Rd., Jhonghe Dist., New Taipei City
- City: Jhonghe Dist.
- State/Province: New Taipei City
- Zip Code: 23511
- Country: Taiwan (R.O.C.)
- Contact Persons: Joshua

Buttons: Submit, Close

Figure 12-47

2. Modify the site location data in the dialog box.
3. Click the **Submit** button to confirm the modification or the **Close** button to abort and close this dialog box.

12.1.4.3 Deleting a Site Location

1. Select one or more site locations to be deleted in the working area. You can delete multiple site locations simultaneously.



Company	Address	Contact Persons
United Computer, Inc.	980 Rock Avenue, San Jose, CA 95131, USA	Billy, Jack
Server Mountains, B.V.	Het Sterrenbeeld 28, 5215 ML, 's-Hertogenbosch, The Netherla...	David, May
Messenger Corporation	3F., No.150, Jian 1st Rd., Jhonghe Dist., New Taipei City 2351...	Jerry

Commands:

- Add Site Location
- Delete Site Location
- Assign Contacts

Figure 12-48

2. Click **Delete Site Location** in the command area and a Delete Site Location dialog box appears.

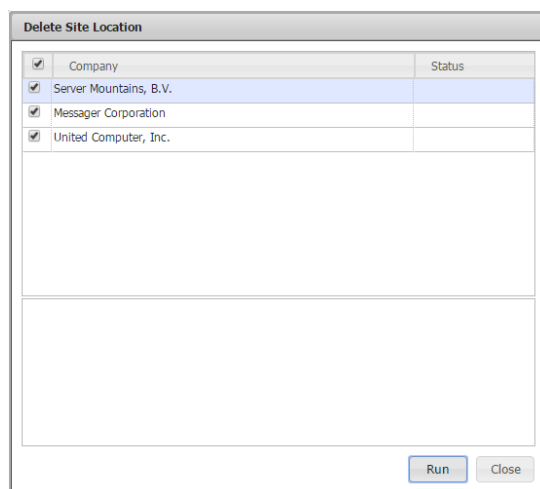


Figure 12-49

3. Click the **Run** button to delete the selected site locations or the **Close** button to abort and close this dialog box.

12.1.4.4 Assigning a Contact

In Service Calls, users are required to assign contacts when managing the “Customers”, “Recipients” and “Site Locations.” The steps to assign a contact are all the same in different configurations. For details, please see *12.1.2.4 Assigning a Contact*.

12.2 Service Calls Alerts

12.2.1 Alert Events

Problem and recovery service calls are triggered when these two conditions meet:

- Your managed system of Supermicro X10 series is equipped with a dedicated network interface and a BMC with the **SFT-DCMS-SVC-KEY** product key activated.
- The IPMI host defined in a setup is enabled. See *12.1.1.10 Enabling a Service Call* for details.

There are additional conditions specific to each type of service calls.

A problem service call is triggered when

- The IPMI service goes into a **HARD** problem state.
 - The IPMI Sensor Health service is in a non-OK state (i.e. “WARNING”, “UNKNOWN” or “CRITICAL”) or
 - The IPMI SEL Health²² service is in a non-OK state (i.e. “WARNING”, “UNKNOWN” or “CRITICAL”)
- More problematically triggered items are in the current HARD state.

A recovery service call is triggered when

- The IPMI service goes into a **HARD** state.
- Recovery items are triggered in the current HARD state.



Notes:

- SSM supports both hard states and soft states to avoid false alarms. SSM only triggers an alert when the service is in a hard state. While SSM retries checking devices, the service is in a soft state and will not trigger an alert. When the service remains in a hard state, the notification will be sent only once whether the multiple check results are the same or not.
- If necessary, you can change the check interval attributes of the host and its services (IPMI Sensor Health and IPMI SEL Health) to shorten/extend the frequency of checking the monitored items.
- Each sensor item is tracked in a Service Call so that an alert could contain both

²² Currently, only hardware failure sensor items support Service Calls. When non-hardware sensor item in IPMI SEL Health becomes critical, no alert will be sent.

problem and recovery messages. For example, the subject line of an e-mail alert shows “Service Call Alert: 10.146.24.125 has some problems (Error:0 Critical:1 Warning:0) and 1 recovered item(s).”

12.2.2 Alert Receivers

To receive alerts, you need to define contacts in recipients and then assign recipients to the setups. Select one setup in the Setup View table to see the detailed contacts in recipients in the detailed view. For example, in the figure below the Setup (SW Team’s Machine) has two recipients MicroX Corporation and Super Plus Computer, Inc. with **Joshua** and **Ishara, Julius** as contact persons respectively.

The screenshot shows the 'Setup Management' interface. The top part is a table with columns: Setup Name, Customer, Recipients, Host Group, Device, Enable, and Protocol. Below this is a 'Detail' section with tabs for Devices, Customer, and Recipients. The 'Recipients' tab is active, showing a table with columns: Company, Address, City, State/Province, Zip Code, Country, Contact Persons, and Trigger Level.

Company	Address	City	State/Province	Zip Code	Country	Contact Persons	Trigger Level
Super Plus Computer, Inc.	980 Rock Avenue, San Jose, CA 95131, USA	San Jose	CA	95131	USA	Ishara, Julius	Supermicro Service
MicroX Corporation	3F., No.150, Jian 1st Rd., Zhonghe Dist., New Taipei City 23511, Taiwan (R.O.C.)	Jhonghe Dist.	New Taipei City	23511	Taiwan (R.O.C.)	Joshua	Local Administrator

Figure 12-50

12.2.3 Alert Format

The message format in E-Mail is defined by the following attributes:

- E-Mail subject line
 - Item 1: the name of the device
 - Item 2: number of the problematic items ("Error", "Critical", and "Warning")
 - Item 3: number of the recovered items

- E-Mail body
 - Item 1 [Event ID]: the unique ID of an event.
 - Item 2 [Event Source]: the host that sent out the alert event.
 - Item 3 [Date/Time]: the time the event occurred in date/time format.

- Item 4 [Problematic Items]: sensor items with problems. Each problematic item includes severity, date, name, message, etc. The value [NEW] is used to point out this item is new.
- Item 5 [Recovered Items (Last Check)]: the recovered sensor items. The errors detected on the last check are displayed. Each recovered item includes severity, date, name, message, etc.
- Item 6 [Summary]: the status of the check.
 - For Local Administrator recipients:
 - Total number of error items
 - Total number of critical items
 - Total number of warning items
 - Total number of recovered items
 - For Supermicro Service recipients:
 - Total number of error items
 - Total number of recovered items
- Item 7 [Device Info]: the information of the host having problems. Note that the attributes included in the mail depend on the device configuration.
- Item 8 [Additional Items]: more information that helps the recipients diagnose the issue. For example, it might include other sensor readings and their thresholds (high/low limits).
- Item 9 [Customer Info]: the customer who owns the host.

12.2.4 Alert History

The **History** function shows the historical alerts that the SSM has sent to recipients. SSM will preserve the settings at the time when the events occurred. Each record includes the Event ID, Date, Device, Asset Tag, System Serial Number, Motherboard Serial Number, IPMI IP Address, Trigger Level, and Summary. To delete the alert events, click the **Delete** button. Note that the events cannot be deleted via the database maintenance program and must be manually deleted.

Event ID	Date	Device	Asset Tag	System Serial Number	Motherboard Serial Number	BMC IP Address	Trigger Level	Summary
8G8tEup2uQ	2018/09/21 13:07:03	10.146.125.137	Supernico	0223456789	SMC11029384756	10.146.125.137	Local Administrator	Error Items: 1, Critical Items: 0, Warning Items: 1, Recovered Items: 0
3DQvWhtdQ	2018/09/21 10:44:22	10.146.125.137	Supernico	0223456789	SMC11029384756	10.146.125.137	Local Administrator	Error Items: 0, Critical Items: 0, Warning Items: 1, Recovered Items: 0
4R23U561K	2018/09/21 10:01:31	10.146.125.137	Supernico	0223456789	SMC11029384756	10.146.125.137	Supernico Service	Error Items: 1, Critical Items: 0, Warning Items: 1, Recovered Items: 0
6c08WKA11E	2018/09/21 09:56:02	10.146.125.137	Supernico	0223456789	SMC11029384756	10.146.125.137	Local Administrator	Error Items: 1, Critical Items: 0, Warning Items: 1, Recovered Items: 0
							Supernico Service	Error Items: 1, Recovered Items: 0

Figure 12-51

To see the details of the setup settings and alert information, click the **View Details** link of the event and the Detail dialog box appears. The Detail dialog includes 6 tabs: **Problematic Items**, **Recovered Items**, **Additional Items**, **Setup Configuration**, **Device Info** and **Trigger Setting**.

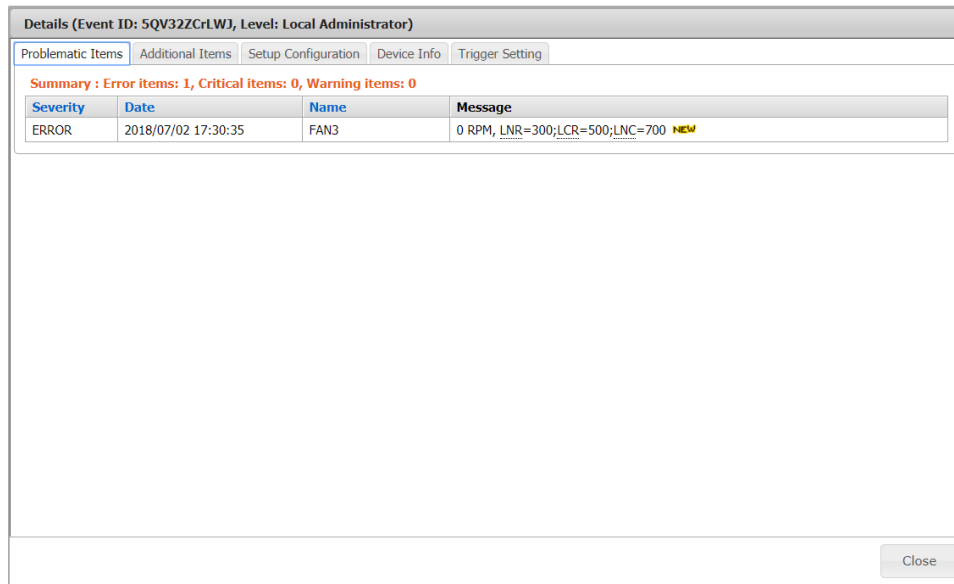


Figure 12-52

These five tabs show the following information:

- Problematic Items: Shows sensor items with problems. Each problematic item includes severity, date, name, message, etc.
- Recovered Items: Shows the recovered sensor items. Each recovered item includes severity, date, name, message, etc.
- Additional Items: Shows more information that helps the recipient diagnose the issue. For example, it might include other sensor readings and their thresholds (high/low limits).
- Setup Configuration: Shows the setup settings (See *12.1.1.1 Adding a Setup*), customer data (See *12.1.2.1 Adding a Customer*), and recipient data (See *12.1.3.1 Adding a Recipient*).
- Device Info: Shows the device data (See *12.1.1.6 Editing a Device*) and site location data (See *12.1.4.1 Adding a Site Location*).
- Trigger Setting: Shows the trigger settings. For those sensors triggering alerts, a trigger item is shown in red.

Details (Event ID: 6qKaCnCphIy, Level: Supermicro Service)	
Trigger Items	Supermicro Service Setting
FAN1	Error
FAN3	Error
FAN4	Error
PS1 Status	Error
Memory - Uncorrectable ECC *	Error
Drive Slot (Bay) - Drive Fault	Error
Critical Interrupt - Bus Fatal Error	Error
Management Subsystem Health - Controller access degraded or unavailable	Error
Battery - Battery failed	Error
Battery - Battery presence	Error
CPLD - CATERR *	Error
BIOS OEM - Failing DIMM: DIMM location and Mapped-Out	Error
BIOS OEM - Uncorrectable error found, Memory Rank is disabled	Error
BIOS OEM - Failing DIMM: DIMM location (Uncorrectable memory component found)	Error

Figure 12-53

12.2.5 Alert Report

At the top of the History working area, you can set the time period and click the **Save as** button to generate the results as a PDF file.

SSM - Service Call History Report	
Duration: 2018/06/02 08:25:24 UTC+08:00 ~ 2018/07/03 08:25:24 UTC+08:00	
Table of Contents	
Device: 10.146.125.136	2
Setup Configuration - SW Team's Machine	2
Device Info	2
Trigger Setting	2
Events (Total: 5)	6
Device: 10.146.125.137	6
Setup Configuration - SW Team's Machine	6
Device Info	7
Trigger Setting	7
Events (Total: 2)	11
Device: 10.146.33.1	11
Setup Configuration - SW Team's Machine	11
Device Info	11
Trigger Setting	12
Events (Total: 1)	12

Figure 12-54

For each device, the Setup data (Customer and Recipients), Device Info (Device Data and Site Location) and Trigger Setting will be printed first, followed by the events in chronological order.

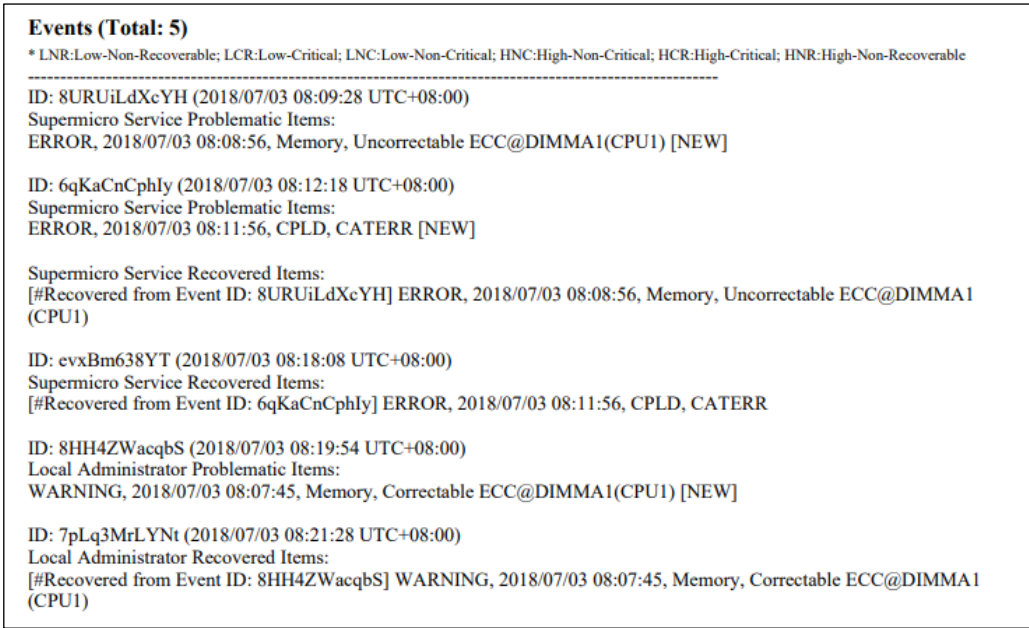


Figure 12-55



13 System Diagnostics

The **System Diagnostics** function helps users determine the root cause of faults or problems at system boot-up on managed Redfish hosts. By diagnosing remote server components, including BIOS, CPUs, memory, fans, HDDs, USB, PCIe, IPMI, power supplies, serial interfaces and networks, the failed components can be identified.

13.1 Prerequisites

This function requires support for SDO (Supermicro Super Diagnostics Offline) and BIOS. Please check the detailed requirements of the managed host before use:

- Your motherboard/system based on Supermicro X12/H12 series and later generations must have a **BMC** with its SFT-DCMS-Single product key activated.
- Both the BMC and **system LAN1** must be accessible from the network.
- The boot mode of the managed system must be UEFI or DUAL.
- It's recommended that you use the latest versions of BIOS and BMC for the managed host before you run the **Diagnose System** command.

13.2 Diagnosing Multiple Redfish Hosts

The example below shows how the **Diagnose System** web command is run to diagnose multiple Redfish hosts.

1. In the Monitoring pane, click **Monitoring**, click **All**, click **Host View**, select the desired Redfish hosts listed in Host View to be diagnosed, and then click **Diagnose System** in the command area on the right.

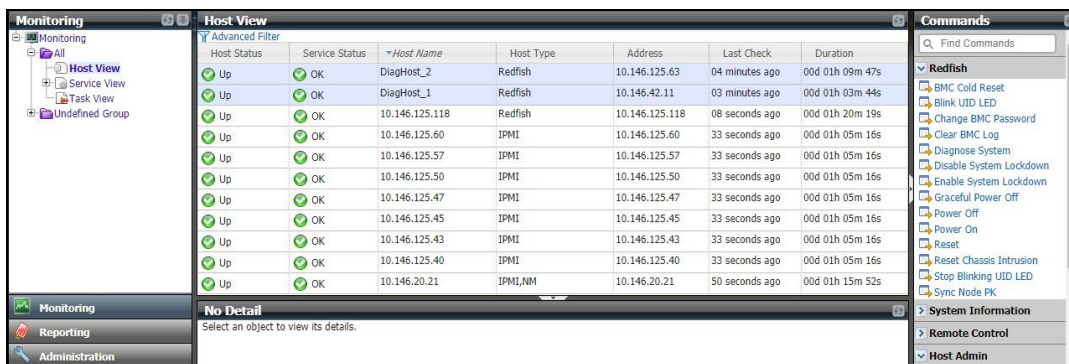


Figure 13-1

2. In the Redfish - Diagnose System Arguments dialog box, click the checkboxes to select the components to be diagnosed, and then click the **Next** button to continue. If you click the **Diagnose**

all components checkbox to have all components diagnosed simultaneously, note that the diagnosis will take a longer time.

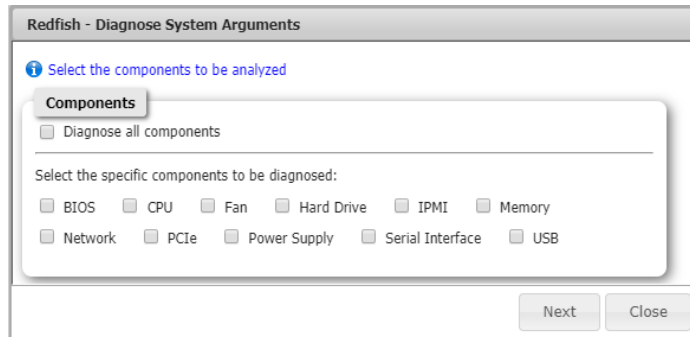


Figure 13-2

3. Click the **Run** button to start the diagnostic process.

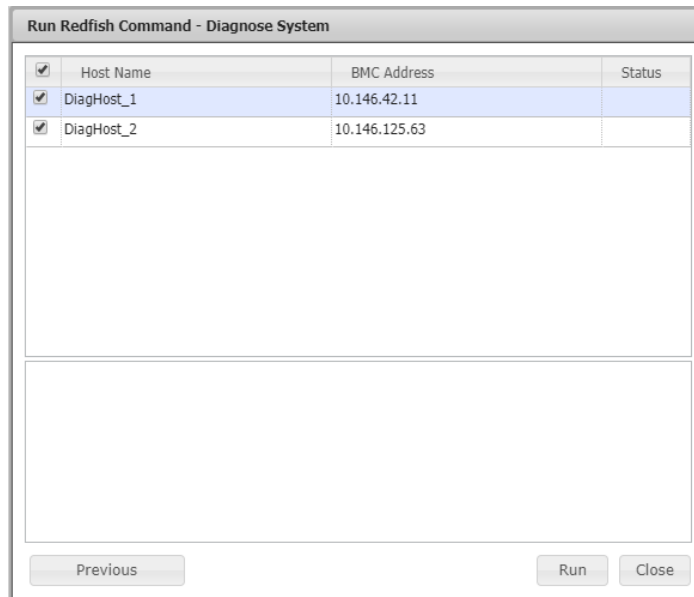


Figure 13-3

4. The green check icon in the Status field (see the figure below) indicates that the request has been sent. If no green check icons appear, check the output message and retry.

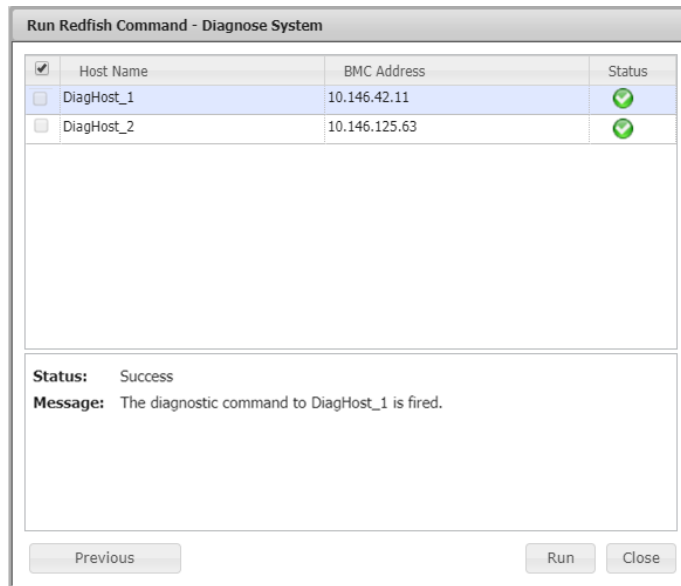


Figure 13-4

- To view the diagnostic progress, click **Administration** in the Administration pane, click **System Diagnostics**, and then click **Diagnostic Progress** to view the tasks running in the Diagnostic Progress pane on the right.

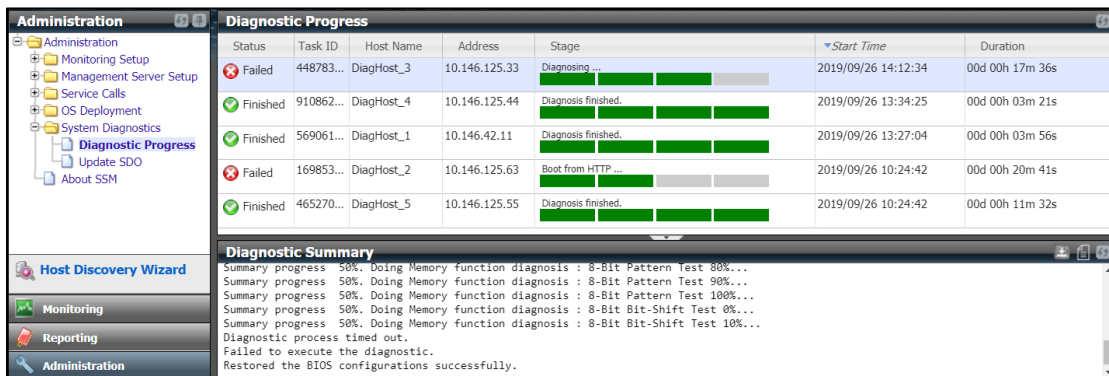


Figure 13-5

- If the diagnostics fail, view the **Diagnostic Summary** pane below to get the detailed messages.

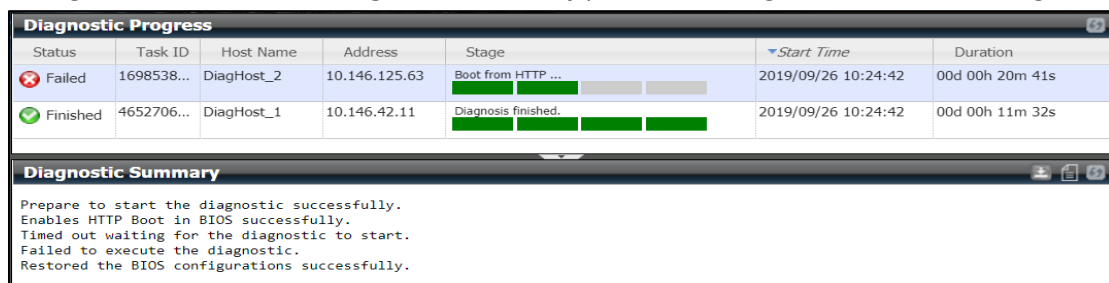


Figure 13-6

- If the diagnostics finish successfully, click the **View Report** icon in the top right corner of Diagnosis Summary toolbar to view the diagnostic report.

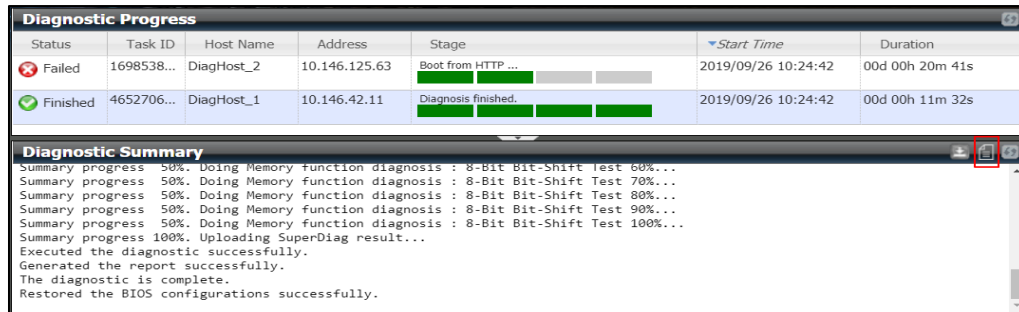


Figure 13-7

- The diagnostic report is summarized and shown in graphic display in Hypertext (.html) for easier access.

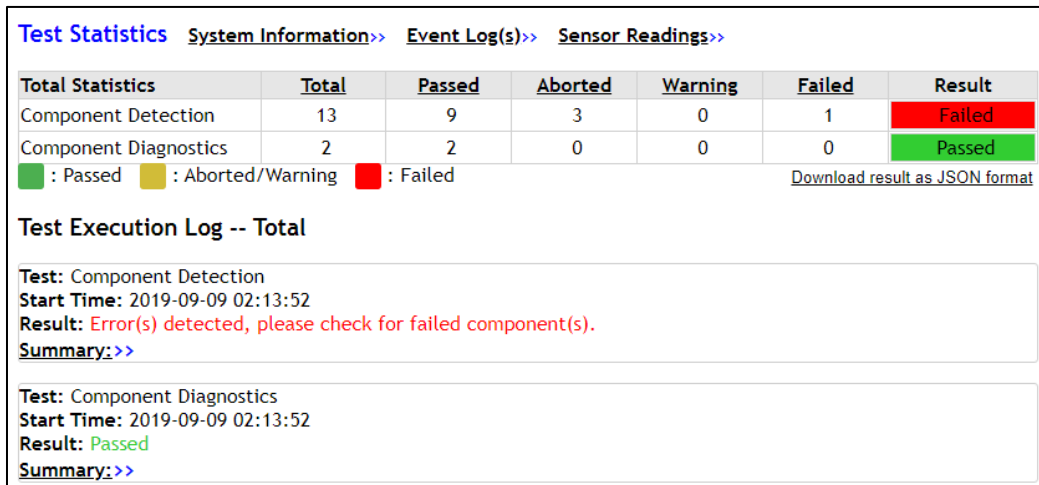


Figure 13-8



13.3 Diagnostic Progress

Once started, the **Diagnose System** process collects information from the devices installed on the managed system, then detects the devices and ensures their presence. Upon detection, it diagnoses the devices based on the detection results. SSM allows up to 50 diagnostic tasks to run simultaneously. When that threshold is reached, the rest of the diagnostic tasks will be queued.

Status	Task ID	Host Name	Address	Stage	Start Time	Duration
Failed	448783...	DiagHost_3	10.146.125.33	Diagnosing ...	2019/09/26 14:12:34	00d 00h 17m 36s
Finished	910862...	DiagHost_4	10.146.125.44	Diagnosis finished.	2019/09/26 13:34:25	00d 00h 03m 21s
Finished	569061...	DiagHost_1	10.146.42.11	Diagnosis finished.	2019/09/26 13:27:04	00d 00h 03m 56s
Failed	169853...	DiagHost_2	10.146.125.63	Boot from HTTP ...	2019/09/26 10:24:42	00d 00h 20m 41s
Finished	465270...	DiagHost_5	10.146.125.55	Diagnosis finished.	2019/09/26 10:24:42	00d 00h 11m 32s

Diagnostic Summary
Diagnostic process timed out. Failed to execute the diagnostic. Restored the BIOS configurations successfully.

Figure 13-9

- **Status:** The current status of the running task.
- **Task ID:** The asynchronous task represents a request to diagnose a Redfish host.
- **Host Name:** The name of the host is displayed here.
- **Address:** Host IP address or DNS name.
- **Stage:** SSM periodically and automatically refreshes the Diagnostic Progress stages.
 - **Prepare:** in this stage, the task will check if the system is on and prepare the diagnostic ISO image.
 - **Change to Boot:** in this stage, the task will change BIOS to HTTP boot mode.
 - **Diagnose:** in this stage, the task begins to diagnose the remote Redfish host and will provide the progress for the selected items.
 - **Generate Report:** in this stage, the task detects if the diagnostic is complete and will restore the BIOS configuration to the pre-diagnosis state.
- **Start Time:** Task start time.
- **End Time:** Task end time.
- The icons on the Diagnosis Summary toolbar:
 - The **View Report** icon  becomes available on the detailed view when the diagnostic task has completed. Click the **View Report** icon to see the diagnostic report. See [13.3.1 Diagnostic Report](#) for more information.
 - The **Download Result** icon  becomes available on the detailed view when the diagnostic task has completed. Click the **Download Result** icon to download an all-in-one zip file. The file contains the diagnostic results and logs for troubleshooting if available.

13.3.1 Diagnostic Report

The summarized diagnostic report uses three labels of different colors to indicate the results in the table: green for passed, brown for aborted/warning, and red for failed. Each type of result is hyperlinked and available for further examination when you click the related column title in the table.

13.3.1.1 Total Statistics

The Total Statistics table lists the results of detecting and diagnosing system components. Component Detection is designed to check if the selected components are present, while Component Diagnostics is used to determine if the selected components are healthy.

Total Statistics Table-

Total Statistics	Total	Passed	Aborted	Warning	Failed	Result
Component Detection	13	8	5	0	0	Passed
Component Diagnostics	11	8	2	0	1	Failed

■ : Passed ■ : Aborted/Warning ■ : Failed [Download result as JSON format](#)

Test Execution Log -- Total

Test: Component Detection
Start Time: 2019-07-31 14:10:37
Result: **Passed**
[Summary:>>](#)

Test: Component Diagnostics
Start Time: 2019-07-31 14:11:03
Result: **Error(s) detected, please check for failed component(s).**
[Summary:>>](#)

Figure 13-10

Here we use the Total results as an example to illustrate the process. To access the Total results, click the column title **Total**.

Column Titles

Total Statistics	Total	Passed	Aborted	Warning	Failed	Result
Component Detection	13	8	5	0	0	Passed
Component Diagnostics	11	8	2	0	1	Failed

■ : Passed ■ : Aborted/Warning ■ : Failed [Download result as JSON format](#)

Figure 13-11

The summary of the selected type of test result then appears. To view a summary of each log record, click **Summary**.

Test: Component Diagnostics Start Time: 2019-07-31 14:11:03 Result: Error(s) detected, please check for failed component(s). Summary:>>

Figure 13-12

The summary of results then appears. You can click the result label of the selected test to find out more details. For the failed items, remedial actions are provided in the summary.


```

Test: Component Diagnostics
Start Time: 2019-07-31 14:11:03
Result: Error(s) detected, please check for failed component(s).
Summary:<<


- TEST BIOS Diagnostics:Passed>>
- TEST CPU Diagnostics:Passed>>
- TEST Memory Diagnostics:Passed>>
- TEST Storage Diagnostics:Aborted>>
- TEST Network Diagnostics:Passed>>
- TEST PCIe Diagnostics:Passed>>
- TEST PSU Diagnostics:Aborted>>
- TEST FAN Diagnostics:Passed>>
- TEST IPMI Diagnostics:Failed<<
  - [I2C Bus Diagnostics]: Passed>>
  - [NIC Mode Diagnostics]: Failed<<
    - [Dedicated Mode]
      - Supported : Yes
      - Health Test : Failed
      - Fail Information : The NIC mode(Dedicated) connection test failed.
      - Remedial Action : Make sure a good cable is plugged into the BMC Dedicated LAN port, and the network environment is good. Ensure that the BMC is operating properly.
      - Result Code : #20920202
    - [Shared Mode]
      - Supported : Yes
      - Health Test : Passed
    - [Mode Capability Check]
      - Health Test : Passed
  - [Network Service Diagnostics]: >>
  - [Manufacturer-FRU-Data Checks]: Passed>>
- TEST Serial I/O Diagnostics:Passed>>
- TEST USB Diagnostics:Passed>>

```

Figure 13-13

13.3.1.2 System Information

A list of system components can be viewed in the diagnostic report. Click **System Information** beside Test Statistics.

Total Statistics	Total	Passed	Aborted	Warning	Failed	Result
Component Detection	13	11	2	0	0	Passed
Component Diagnostics	11	10	1	0	0	Passed

■ : Passed
 ■ : Aborted/Warning
 ■ : Failed
 [Download result as JSON format](#)

Figure 13-14

A complete list of system components appears.

Test Statistics>> System Information		Event Log(s)>>	Sensor Readings>>
Hardware Information			
CPU			
CPU #001	Intel(R) Xeon(R) Gold 6130 CPU @ 2.10GHz		
Memory			
DIMM #001	Manufacturer : Samsung Device Locator : P1-DIMMA1 ECC Support : Yes Speed : 2133 MHz Size : 8 GB		
DIMM #002	Manufacturer : Samsung Device Locator : P1-DIMMB1 ECC Support : Yes Speed : 2133 MHz Size : 8 GB		
PCIe			
PCIe #001	Manufacturer : ASPEED Technology, Inc. Device Class : VGA-Compatible Controller Device Location : Onboard Device Designation : ASPEED Video AST2500 Link Width Status : Capability ID not found Link Speed Status : Capability ID not found		
PCIe #002	Manufacturer : Intel Corporation Device Class : Ethernet Controller Device Location : Onboard Device Designation : Intel Ethernet X540 #1 Link Width Status : X8 Link Speed Status : Gen 2		
PCIe #003	Manufacturer : Intel Corporation Device Class : Ethernet Controller Device Location : Onboard Device Designation : Intel Ethernet X540 #2 Link Width Status : X8 Link Speed Status : Gen 2		
Storage			
Storage #001	Interface Type : AHCI Storage Type : HDD Manufacturer : Seagate Model : ST1000NX0303 RPM : 7200		
RAID			
No devices installed.			
PSU			
PSU #001	Location : PSU1 Manufacturer : SUPERMICRO		
SMBIOS Information			
System			
Manufacturer	Supermicro		
Product Name	Super Server		
Board			
Manufacturer	Supermicro		
Product Name	X11DPU		
Version	1.10		
Serial Number	OM173S033970		
Firmware Information			
BIOS			
Version	3.1a		
Release Date	05/27/2019		
ME			
Operational Firmware Version	4.1.4.296		
Recovery Firmware Version	4.1.4.296		
IPMI			
Revision	1.70		
Build Date	2019-05-20		
GUID	4101MS		
Board			
CPLD Revision	03.B0.06		

Figure 13-15

13.3.1.3 Event Logs

A list of event logs can be viewed in the diagnostic report. Click **Event Log(s)**.

Test Statistics		System Information>>	Event Log(s)>>	Sensor Readings>>		
Total Statistics	Total	Passed	Aborted	Warning	Failed	Result
Component Detection	13	11	2	0	0	Passed
Component Diagnostics	11	10	1	0	0	Passed
■ : Passed ■ : Aborted/Warning ■ : Failed						
Download result as JSON format						

Figure 13-16

A complete list of BIOS DMI event logs and IPMI event logs appears.

BIOS DMI Event Logs		IPMI Event Logs	
#001		#001	
Date	2019-06-28	Timestamp	2019-04-11 05:46:33
Time	09:15:41	Sensor Name	Management Subsystem Health
Code	SMBIOS 0x16	Event Dir	Assertion
Severity	N/A	Description	Unknown Event
Description	Log Area Reset/Cleared	Remedial Action	N/A
Remedial Action	N/A	#002	
		Timestamp	2019-04-11 05:48:27
		Sensor Name	Management Subsystem Health
		Event Dir	Deassertion
		Description	OEM event
		Remedial Action	N/A
		#003	
		Timestamp	2019-05-08 03:15:52
		Sensor Name	OEM
		Event Dir	Assertion
		Description	OEM event
		Remedial Action	N/A
		#004	
		Timestamp	2019-05-16 05:36:23
		Sensor Name	CPU Error
		Event Dir	Assertion
		Description	CPU Error0
		Remedial Action	N/A
		#005	
		Timestamp	2019-05-16 05:37:20
		Sensor Name	CPU Error
		Event Dir	Assertion
		Description	CPU Error0
		Remedial Action	N/A
		#006	
		Timestamp	2019-05-16 05:38:52
		Sensor Name	Memory
		Event Dir	Assertion
		Description	Correctable ECC
		Remedial Action	Check the DIMM is properly installed. If this failure persists, please contact Supermicro Technical Support or an FAE for troubleshooting.

Figure 13-17

13.3.1.4 Sensor Readings

A list of sensor readings can be viewed in the diagnostic report. Click **Sensor Readings**.

Test Statistics						
		System Information >>		Event Log(s) >>		Sensor Readings >>
Total Statistics	Total	Passed	Aborted	Warning	Failed	Result
Component Detection	13	11	2	0	0	Passed
Component Diagnostics	11	10	1	0	0	Passed
■ : Passed ■ : Aborted/Warning ■ : Failed						Download result as JSON format

Figure 13-18

A complete list of sensor readings appears.

Test Statistics >> System Information >> Event Log(s) >> Sensor Readings

IPMI Sensor Readings		
Sensor Name	Status	Reading
CPU1 Temp	Normal	55C/131F
CPU2 Temp	N/A	Not Present
PCH Temp	Normal	43C/109F
System Temp	Normal	25C/77F
Peripheral Temp	Normal	30C/86F
MB_NIC_Temp1	Normal	47C/117F
MB_NIC_Temp2	N/A	Not Present
VRMCpu1 Temp	Normal	34C/93F
VRMCpu2 Temp	N/A	Not Present
VRMP1ABC Temp	Normal	31C/88F
VRMP1DEF Temp	Normal	30C/86F
VRMP2ABC Temp	N/A	Not Present
VRMP2DEF Temp	N/A	Not Present
FAN1	N/A	Not Present
FAN2	N/A	Not Present
FAN3	N/A	Not Present
FAN4	N/A	Not Present
FAN5	Normal	1900 RPM
FAN6	N/A	Not Present
FAN7	N/A	Not Present
FAN8	N/A	Not Present
RSC FAN	N/A	Not Present
P1-DIMMA1 Temp	Normal	33C/91F
P1-DIMMA2 Temp	N/A	Not Present
P1-DIMMB1 Temp	Normal	32C/90F
P1-DIMMB2 Temp	N/A	Not Present
P1-DIMMC1 Temp	N/A	Not Present
P1-DIMMC2 Temp	N/A	Not Present
P1-DIMMD1 Temp	N/A	Not Present
P1-DIMMD2 Temp	N/A	Not Present

Figure 13-19

13.3.1.5 Diagnosis in Raw Data

To view the raw data in JSON format, click the **Download result as JSON format** link.

Test Statistics System Information >> Event Log(s) >> Sensor Readings >>

Total Statistics	Total	Passed	Aborted	Warning	Failed	Result
Component Detection	13	11	2	0	0	Passed
Component Diagnostics	11	10	1	0	0	Passed

■ : Passed
 ■ : Aborted/Warning
 ■ : Failed

[Download result as JSON format](#)

Figure 13-20

You can view the JSON log file directly after downloading it.

```

1
2
3 {
4   "$SMC.UtilityName": "Super Diagnostics Offline",
5   "$SMC.UtilityVersion": "1.2.0",
6   "$SMC.Copyright": "Copyright © 2016-2019 Super Micro Computer, Inc.",
7   "$odata.type": "Information Data",
8   "Timestamp": "2019-06-28 09:52:05",
9   "System Information": {
10    "System Name": "Super Server",
11    "Chassis Type": "00h",
12    "Board Name": "X11DPU+",
13    "Serial Number": "0123456789",
14    "CPUD Revision": "03.B0.06"
15  },
16  "BIOS Information": {
17    "Release Date": "2019-05-27",
18    "Version": "3.1a"
19  },
20  "Memory Information": {
21    "Memory Device #001": {
22      "Vendor": "Samsung",
23      "Part Number": "M999A1G40DB0-CPB",
24      "Speed": "2133 MHz",
25      "Size": "8 GB",
26      "Serial Number": "32AEC1BB",
27      "Device Locator": "P1-DIMM1A",
28      "ECC Support": "Yes",
29      "ECC Error Detected": "No"
30    },
31    "Memory Device #002": {
32      "Vendor": "Samsung",
33      "Part Number": "M999A1G40DB0-CPB",
34      "Speed": "2133 MHz",
35      "Size": "8 GB",
36      "Serial Number": "32D36A74",
37      "Device Locator": "P1-DIMM1B",
38      "ECC Support": "Yes",
39      "ECC Error Detected": "No"
40    }
41  },
42  "PCIe Information": {
43    "PCIe Device #001": {
44      "Manufacturer": "ASPEED Technology, Inc.",
45      "Device Class": "VGA-Compatible Controller",
46      "VendorID": "1A03h",
47      "DeviceID": "2000h",
48      "Link Width Capability": "Capability ID not found",
49      "Link Width Status": "Capability ID not found",
50    }
51  }
52 }

```

Figure 13-21

13.4 Updating Diagnostic Software

To update the Diagnostic Software package, you can contact Supermicro to get the latest version of the package first, and then follow these steps.

1. Click **System Diagnostics**, and then click **Update SDO** in the navigation area on the Administration pane. The Update SDO dialog box appears.
2. Click **Choose File** to select the SDO file to be updated, and then click **Upload**.

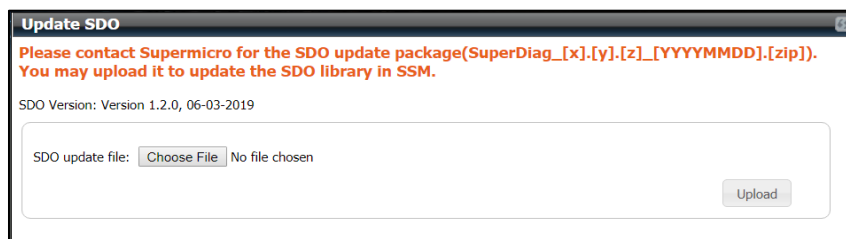


Figure 13-22

3. If the update is successful, both the version and the last upload date of SDO are changed accordingly in the **Update SDO** dialog box.

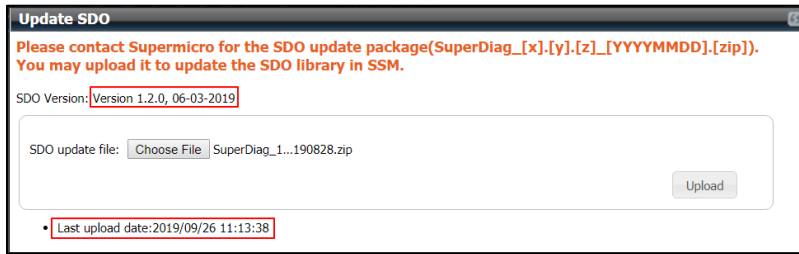


Figure 13-23

Part 4 SSM CLI

14 SSM CLI

14.1 SSM CLI Overview

SSM CLI is a command line interface program that talks to SD5s and the IPMI BMC to provide real-time health information and perform power management functions. SSM CLI applies the same configuration data (i.e., hosts, host groups, services, contacts, contact group, and so on) used by the SSM Server and SSM Web. The configuration settings can be read from the SSM Database or from local files. Unlike the SSM Server, SSM CLI does not periodically execute commands issued by users. SSM CLI waits for a command, executes it, and shows the results on the screen or sends them to a file.

SSM CLI supports two usage modes: an **interactive mode** and a **batch mode**. In the interactive mode, SSM CLI waits indefinitely for a user command until the **exit** command is received, which terminates SSM CLI. In the batch mode, SSM CLI returns the result to its caller and terminates immediately when it completes the execution of a command. The batch mode is suitable for script automation where SSM CLI is invoked by user-defined scripts. SSM CLI does not store the command execution results in the SSM Database. Instead, SSM CLI shows the results onscreen or writes the results to a user-specified file.

SSM CLI is typically used for management automation. For example, by writing a script you can use SSM CLI to reboot 100 hosts belonging to a particular host group at 01:00 AM every day. Although the same can be done via the SSM Web console, it requires several mouse clicks and therefore is not suitable for automation.

SSM CLI supports the following commands.

Command	Description
ipmi	Checks host health information via IPMI BMC.
power	Controls host power via SuperDoctor 5, IPMI BMC, and WOL.
health	Checks host health information via the SuperDoctor 5.
list	Displays host and host group configurations.
status	Displays host status (Up or Down).
systeminfo	Displays system information.
env	Displays SSM CLI environmental settings.
storage	Shows storage health information via the SuperDoctor 5.
memory	Shows memory health information via the SuperDoctor 5.



Notes:

- The memory commands do not apply to hosts with desktop motherboards.
- The SMART check of the storage health checks non-RAID internal hard disks; and this function is not available on USB hard disks and flash disks. The RAID check of the storage health is designed to check the health of LSI MegaRAID 2108, 2208 and 3108 controllers.

14.2 Using SSM CLI

In the SSM CLI installation folder, you will find two batch programs. One is for the interactive mode (**cli.bat** for Windows and **cli.sh** for Linux) and the other is for the batch mode (**clibatch.bat** in Windows and **clibatch.sh** in Linux).

14.2.1 Interactive Mode

In a text console, execute **cli.sh** and you will see the SSM CLI prompt as shown below:

```
[root@localhost SSMCLI]# cli.sh

Welcome to SSM command line interface.([1.0.0_build.457-20140708203130])

Type in 'help' to see commands.

Type in 'exit' to logout.

Enjoy the shell mode!

Powered by Supermicro.

SSM CLI>
```

Figure 14-1

Use the **help** command to show help information.

```
SSM CLI>help
| Command | Description |
|-----|-----|
| ipmi | Execute IPMI Command |
| power | Power Control |
| health | Show Health Info. via SuperDoctor 5 |
| list | Display Configure Information |
| status | Display Host Status |
| systeminfo | Display System Information |
| env | Display System Environment |
| storage | Show Storage Health Info. via Super |
| | Doctor 5 |
| memory | Show Memory Health Info. via SuperD |
| | octor 5 |
SSM CLI>
```

Figure 14-1

Use the **exit** command to leave SSM CLI.

14.3 Common Arguments

The following four arguments can be applied to all SSM CLI commands.

Arguments	Description
-H or --host	Issues the command to the specified hosts. Use a comma to separate multiple hosts.
-G or --hostgroup	Issues the command to all hosts in the specified host group. Use a comma to separate multiple host groups.
-csv or --csv	Uses the CSV format to display results.
-f or --file	Writes results to the specified file and overwrites the file if it already exists.



Notes:

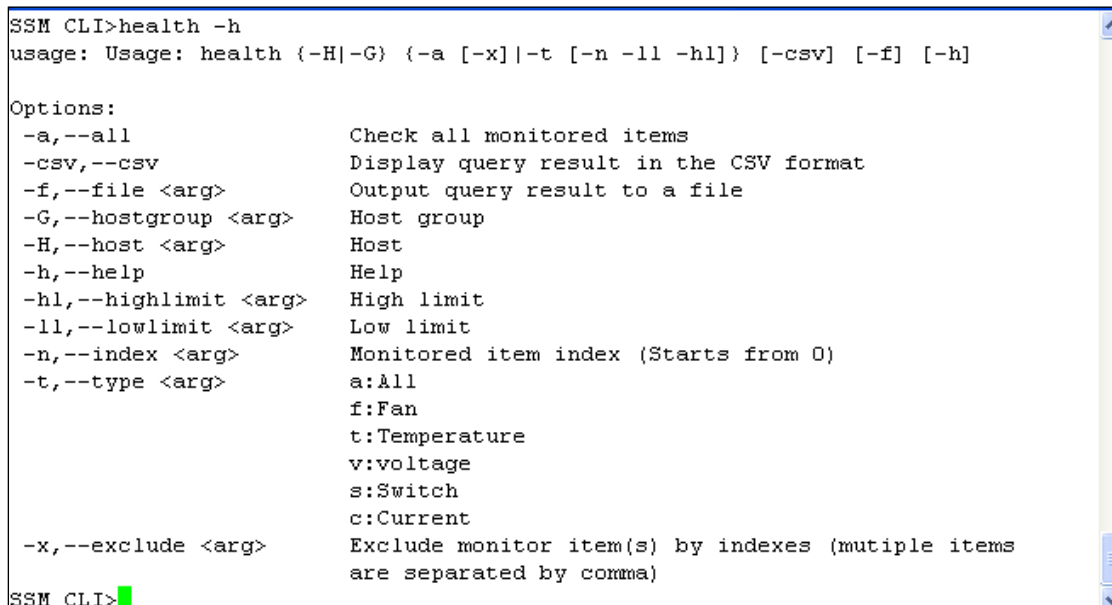
- Arguments are case sensitive.
 - The specified host names and host group names must be defined in the SSM Database or in the configuration files.
-

14.4 Health Command

The **health** command is an in-band command that supports the monitoring of a host's health information via a SuperDoctor 5.

14.4.1 -h: Display health command arguments

Enter **health** or **health -h** at the SSM CLI prompt to display all supported arguments onscreen.



```
SSM CLI>health -h
usage: Usage: health (-H|-G) (-a [-x]|-t [-n -ll -hl]) [-csv] [-f] [-h]

Options:
-a,--all                Check all monitored items
-csv,--csv              Display query result in the CSV format
-f,--file <arg>        Output query result to a file
-G,--hostgroup <arg>   Host group
-H,--host <arg>        Host
-h,--help              Help
-hl,--highlimit <arg>  High limit
-ll,--lowlimit <arg>   Low limit
-n,--index <arg>       Monitored item index (Starts from 0)
-t,--type <arg>        a:All
                       f:Fan
                       t:Temperature
                       v:voltage
                       s:Switch
                       c:Current
-x,--exclude <arg>     Exclude monitor item(s) by indexes (mutiple items
                       are separated by comma)

SSM CLI>
```

Figure 14-3

14.4.2 **-a: Use default thresholds to check all enabled health items**

Checking the health status with the **-a** argument tells SSM CLI to use the default thresholds of each health item to determine its overall health. An OK value will be returned only if all health items are in the normal state. Any non-health item will cause a CRITICAL value to be returned.

Enter **health -H [host name] -a** at the SSM CLI prompt to display the health status check results onscreen.

```
SSM CLI>health -H jcis-server -a
| Host          | Address        | Status | Message                               |
| -----|-----|-----|-----|
| jcis-server| 192.168.12.4| OK     | Checked: 17, OK: 17. |
#Summary of execution: OK[1]
SSM CLI>
```

Figure 14-4

Using the **-a** argument checks all enabled health items and eliminates the need to manually enumerate every health item to be checked. If all you need to know is whether the relevant items in a particular host are all healthy and do not care about the exact reading of each health item, then the **-a** argument is suitable for use.

14.4.3 `-a -x [index 1, index 2, ...]`: Use default thresholds to check all enabled health items excluding those specified in the `-x` argument

The `-a` argument checks all enabled health items on a host but sometimes not all enabled health items are used. For example, a host (a motherboard) is designed to support a maximum of five fans but only four are used in a particular configuration. Checking the health items with the `-a` argument will always get a CRITICAL result due to the false alarm of the non-used health item. In this situation, you can use the `-x` argument to exclude the non-used item. For example, suppose that items 2 and 3 are not used in the host to be checked. You can use the `health -H [host name] -a -x 2,3` command to exclude these items.

```
SSM CLI>health -H jcis-server -a -x 2,3
| Host          | Address        | Status | Message                                     |
| -----|-----|-----|-----|
| jcis-server| 192.168.12.4| OK     | Excluded: 2, Checked: 15, O...|
#Summary of execution: OK[1]

SSM CLI>
```

Figure 14-5

14.4.4 -t: Display the name and reading of each health item

The **-t** argument displays the number, name, and reading of all health items in a host or category. Enter **health -H [host name] -t a** at the SSM CLI prompt to display the results of all health items in the specified host. Note that the **Message** column shown below is composed of [health item number] [health item name + health item reading].

The following parameters can be used in the argument.

- a : Lists all health items.
- f : Lists all fan items.
- t : Lists all temperature items.
- v : Lists all voltage items.
- s : Lists all switch items (e.g., chassis intrusion).
- c : Lists all current items.

```
SSM CLI>health -H softlab4 -t a
| Host      | Address      | Status | Message
|-----|-----|-----|-----|
| softlab4 | 192.168.12.33 | OK    | [8]DIMM2 is OV
| softlab4 | 192.168.12.33 | OK    | [4]CPU2 Vcore is OV
| softlab4 | 192.168.12.33 | OK    | [5]CPU1 VTT is 1.16V
| softlab4 | 192.168.12.33 | OK    | [1]CPU2 Temp=NA
| softlab4 | 192.168.12.33 | OK    | [0]CPU1 Temp=Low
| softlab4 | 192.168.12.33 | OK    | [7]DIMM1 is 1.528V
| softlab4 | 192.168.12.33 | OK    | [9]+1.5V is 1.472V
| softlab4 | 192.168.12.33 | OK    | [6]CPU2 VTT is OV
| softlab4 | 192.168.12.33 | OK    | [3]CPU1 Vcore is 0.92V
| softlab4 | 192.168.12.33 | OK    | [2]System Temp is 29C
| softlab4 | 192.168.12.33 | OK    | [16]VBAT is 3.24V
| softlab4 | 192.168.12.33 | OK    | [11]+5V is 5.12V
| softlab4 | 192.168.12.33 | OK    | [10]+1.8V is 1.816V
| softlab4 | 192.168.12.33 | OK    | [17]Fan1 is ORPM
| softlab4 | 192.168.12.33 | OK    | [12]+12V is 12.19V
| softlab4 | 192.168.12.33 | OK    | [15]+3.3VSB is 3.24V
| softlab4 | 192.168.12.33 | OK    | [14]+3.3V is 3.264V
| softlab4 | 192.168.12.33 | OK    | [13]+1.1V is 1.112V
| softlab4 | 192.168.12.33 | OK    | [19]Fan3 is ORPM
| softlab4 | 192.168.12.33 | OK    | [18]Fan2 is 1755RPM
| softlab4 | 192.168.12.33 | OK    | [26]PS Status is normal
| softlab4 | 192.168.12.33 | OK    | [21]Fan5 is ORPM
| softlab4 | 192.168.12.33 | OK    | [25]Intrusion is normal
| softlab4 | 192.168.12.33 | OK    | [22]Fan6 is ORPM
| softlab4 | 192.168.12.33 | OK    | [23]Fan7 is ORPM
| softlab4 | 192.168.12.33 | OK    | [24]Fan8 is ORPM
| softlab4 | 192.168.12.33 | OK    | [20]Fan4 is 2700RPM
#Summary of execution: OK[27]
SSM CLI>
```

Figure 14-6



Notes:

- The Status column in the output table shown above indicates the status of

executing the command (i.e., `health -H [host name] -t a`) rather than the health status of each health item. To determine health status please use `-t`, `-n`, `-ll`, and `-hl`. See 14.4.5 for more information.

- Some SSM CLI commands require the number of a health item as arguments. You can use the `health -t a` command to query this information.
-

14.4.5 `-t a -n [index] -ll [low limit] -hl [high limit]`: Display a health item status with the specified item number as well as high and low limits.

Using the `-t` argument with the `-n`, `-ll`, and `-hl` arguments will check the health status of a health item.

Argument description:

- `-t`: The category of a health item to be checked.
- `-n`: The number of a health item.
- `-ll`: The user-defined lower limit (threshold) of the health item. This argument must be used with the `-n` argument.
- `-hl`: The user-defined higher limit of the health item. This argument must be used with the `-n` argument.

For example, entering `health -H [host name] -t a -n 19 -ll 0 -hl 712` at the SSM CLI prompt displays the health status of the 19th health item, as shown below.

```
SSM CLI>health -H jcis-server -t a -n 19 -ll 0 -hl 712
| Host          | Address        | Status | Message                                     |
| -----|-----|-----|-----|
| jcis-server| 192.168.12.4| OK    | [19] Fan7 is normal(1755RPM>=0) |
#Summary of execution: OK[1]
SSM CLI>
```

Figure 14-7



Note: The number of a health item is determined by the `-t` parameter. For example, the number of a +12V item is “10” when the `health -t a` command is used (i.e., it is the 10th item among all health items). Its number could be “0” when the `health -t v` is issued (i.e., it is the number 0 item in the voltage category). To prevent the incorrect use of item numbers, the `-n` argument should be used with the `-t a` argument.

14.5 IPMI Command

The **ipmi** command is an out-of-band command that supports the monitoring of hosts' health information via IPMI BMC.

14.5.1 -h: Display IPMI command arguments

Entering **ipmi** or **ipmi -h** at the SSM CLI prompt displays all supported arguments onscreen.

```
SSM CLI>ipmi -h
usage: Usage: ipmi {-H|-G} {-a|-t|-l|-n|-n -ll -hl} [-f] [-h] [-csv]

Options:
-a,--all           Display a combind sensor status
-cr,--coldreset   BMC Cold Reset
-csv,--csv        Display query result in the CSV format
-dul,--disableuidled Stop Blinking UID LED
-eul,--enableuidled Blink UID LED
-f,--file <arg>   Output query result to a file
-G,--hostgroup <arg> Host group
-h,--help         Help
-H,--host <arg>   Host
-hl,--highlimit <arg> High limit
-l,--list         Display all sensor names
-ll,--lowlimit <arg> Low limit
-n,--index <arg>  Sensor number
-t,--allofsensor  Display status of all sensors
SSM CLI>
```

Figure 14-8

14.5.2 **-a: Use default thresholds to check all enabled health items**

The use of the **-a** argument in the **ipmi** command is similar to that in the **health** command. Entering **health -H [host name] -a** at the SSM CLI prompt displays the health status results onscreen.

```
SSM CLI>ipmi -H Server-30 -a
| Host      | Address      | Status | Message                |
| ----- | ----- | ----- | ----- |
| Server-30 | 192.168.12.11 | OK    | Checked:14, Ok:14 |
#Summary of execution: OK[1]
SSM CLI>
```

Figure 14-9

14.5.3 **-cr: Cold reset a BMC**

The **-cr** argument resets (reboots) a BMC. At the SSM CLI prompt, enter **ipmi -H [host name] -cr**.

```
SSM CLI>ipmi -H DB-Node1 -cr
| Host      | Address      | Status | Message                |
| ----- | ----- | ----- | ----- |
| DB-Node1 | 192.168.12.8 | OK    | BMC cold reset successfully. |
#Summary of execution: OK[1]
SSM CLI>
```

Figure 14-10

14.5.4 **-dul: Stop blinking UID LED**

The **-dul** argument stops the UID LED from blinking. At the SSM CLI prompt, enter **ipmi -H [host name] -dul**

```
SSM CLI>ipmi -H DB-Node1 -dul
| Host      | Address      | Status | Message                |
| ----- | ----- | ----- | ----- |
| DB-Node1 | 192.168.12.8 | OK    | Disable UID LED successfully. |
#Summary of execution: OK[1]
SSM CLI>
```

Figure 14-11

14.5.5 -eul: Blink UID LED

The `-eul` argument causes the UID LED to blink. At the SSM CLI prompt, enter `ipmi -H [host name] -eul`

```
SSM CLI>ipmi -H DB-Node1 -eul
| Host      | Address      | Status | Message                               |
| -----| -----| -----| -----|
| DB-Node1 | 192.168.12.8| OK     | Enable UID LED successfully.         |
#Summary of execution: OK[1]
SSM CLI>
```

Figure 14-12

14.5.6 -l: Display all of monitored items and index

The `-l-list` argument shows the name and index of all monitored items. At the SSM CLI prompt, enter `ipmi -H [host name] -l-list`.

```
SSM CLI>ipmi -H Server-30 -l
| Host      | Address      | Status | Message                               |
| -----| -----| -----| -----|
| Server-30 | 192.168.12.11| OK     | -86:Intrusion                         |
| Server-30 | 192.168.12.11| OK     | 96:P1-DIMM1A Temp                     |
| Server-30 | 192.168.12.11| OK     | 22:PS Status                           |
| Server-30 | 192.168.12.11| OK     | 13:VBAT                                 |
| Server-30 | 192.168.12.11| OK     | 11:+5V                                  |
| Server-30 | 192.168.12.11| OK     | 12:+12V                                 |
| Server-30 | 192.168.12.11| OK     | 3:System Temp                           |
| Server-30 | 192.168.12.11| OK     | 21:Fan8                                 |
| Server-30 | 192.168.12.11| OK     | 1:CPU1 Temp                             |
| Server-30 | 192.168.12.11| OK     | 10:+3.3VSB                             |
| Server-30 | 192.168.12.11| OK     | 6:CPU1 DIMM                             |
| Server-30 | 192.168.12.11| OK     | 4:CPU1 Vcore                             |
| Server-30 | 192.168.12.11| OK     | 9:+3.3V                                  |
| Server-30 | 192.168.12.11| OK     | 8:+1.5V                                  |
#Summary of execution: OK[14]
SSM CLI>
```

Figure 14-13



Notes:

- The status column in the output table shown above indicates the status of executing the command (i.e., `ipmi -H [host name] -t`) rather than the health status of each health item. To determine health status, please use `-a` or `-n`.
 - The `ipmi -list` command only returns item names and indexes. If you want to see the reading, enter `health -t` instead.
-

14.5.7 `-n [index] -ll [low limit] -hl [high limit]`: Display a health item status with the specified item number as well as high and low limits.

Using the `-n` argument will check the health status with default thresholds. Using the `-n` argument with the `-ll`, and `-hl` arguments will check the health status of a health item with specified low and high limits. For example, enter `ipmi -H [host name] -n 19 -ll 1000 -hl 10000` in the SSM CLI prompt to see the health status of health item number 19, as shown below.

```
SSM CLI>ipmi -H Server-30 -n 21 -ll 1000 -hl 10000
| Host      | Address      | Status | Message                                     |
| ----- | ----- | ----- | ----- |
| Server-30 | 192.168.12.11 | OK     | Fan8,Reading=2700.0, (RPM) |
#Summary of execution: OK[1]
SSM CLI>
```

Figure 14-14

Argument description:

- `-n` : The number of a health item.
- `-ll` : A user-defined lower limit (threshold) of the health item. This argument must be used with the `-n` argument.
- `-hl` : A user-defined higher limit of the health item. This argument must be used with the `-n` argument.



Note: The IPMI `-H [host name] -n [index]` command is similar to `health -H [host name] -n [index]`.

14.6 Power Command

The **power** command supports power control functions via SuperDoctor 5 and IPMI BMC.

14.6.1 -h: Display power command arguments

Enter **power** or **power -h** at the SSM CLI prompt to display all supported arguments onscreen.

```
SSM CLI>power -h
usage: Usage: power [-a|-b] {-H|-G} {-r|-s|-p} [-f] [-h]

Options:
-a,--agent           Power control through SuperDoctor 5
-b,--ipmi            Power control through IPMI
-csv,--csv           Display query result in the CSV format
-f,--file <arg>     Output query result to a file
-G,--hostgroup <arg> Host group
-H,--host <arg>     Host
-h,--help            Help
-p,--poweron         Power on
-r,--reboot          Reboot
-s,--shutdown        Shutdown
SSM CLI>
```

Figure 14-15

14.6.2 -a -s: Shutdown hosts via SD5

Enter the **power -H [host name] -a -s** command at the SSM CLI prompt to shut down a host via the SuperDoctor 5.

```
SSM CLI>power -H Server-32 -a -s
| Host      | Address      | Status | Message
| -----| -----| -----| -----
| Server-32| 192.168.12.32| OK    | The shutdown command is fired.
#Summary of execution: OK[1]
SSM CLI>
```

Figure 14-16



Note: After this command is issued, a returned OK status means that the SuperDoctor 5 on the specified host has received the shutdown command and has tried to initiate a shutdown process. It does not mean that the host has been shut down successfully. Many situations, such as an application hanging or an unexpected operating system crash, could prevent the host from being shut down successfully.

14.6.3 -a -r: Reboot hosts via SD5

Enter the **power -H [host name] -a -r** command at the SSM CLI prompt to reboot a host via the SuperDoctor 5.

```
SSM CLI>power -H Server-32 -a -r
| Host      | Address      | Status | Message
| -----| -----| -----| -----
| Server-32| 192.168.12.32| OK    | The reboot command is fired.
#Summary of execution: OK[1]
SSM CLI>
```

Figure 14-17



Note: After this command is issued, a returned OK status means that the SuperDoctor 5 on the specified host has received the reboot command and has tried to initiate a reboot process. It does not mean that the host has been rebooted successfully. Many situations, such as an application hanging or an unexpected operating system crash, could prevent the host from being rebooted successfully.

14.6.4 -a -p: Power up hosts via Wake on LAN (WOL)

Enter the **power -H [host name] -a -p** command at the SSM CLI prompt to power up a host via WOL.

```
SSM CLI>power -H Server-32 -a -p
| Host      | Address      | Status | Message                               |
|-----|-----|-----|-----|
| Server-32| 192.168.12.32| OK    | Wake-on-LAN packet sent.           |
#Summary of execution: OK[1]
SSM CLI>
```

Figure 14-18



Note: To use this function, please make sure your BIOS, OS and network driver all support WOL and have been configured correctly.

14.6.5 -b -s: Shutdown hosts via IPMI

Enter the **power -H [host name] -b -s** command at the SSM CLI prompt to shut down a host via IPMI.

```
SSM CLI>power -H Server-30 -b -s
| Host      | Address      | Status | Message                               |
|-----|-----|-----|-----|
| Server-30| 192.168.12.11| OK    | IPMI power down successfully       |
#Summary of execution: OK[1]
SSM CLI>
```

Figure 14-19

14.6.6 -b -r: Reboot hosts via IPMI

Enter the **power -H [host name] -b -r** command at the SSM CLI prompt to reboot a host via IPMI.

```
SSM CLI>power -H Server-30 -b -r
| Host      | Address      | Status | Message                               |
|-----|-----|-----|-----|
| Server-30| 192.168.12.11| OK    | IPMI Reset successfully           |
#Summary of execution: OK[1]
SSM CLI>
```

Figure 14-20

14.6.7 -b -p: Power up hosts via IPMI

Enter the **power -H [host name] -b -p** command at the SSM CLI prompt to power up a host via IPMI.

```
SSM CLI>power -H Server-30 -b -p
| Host          | Address      | Status | Message                                     |
| -----|-----|-----|-----|
| Server-30| 192.168.12.11| OK     | IPMI power up successfully|
#Summary of execution: OK[1]

SSM CLI>
```

Figure 14-21

14.6.8 -s: Shutdown hosts by IPMI or SD5

Enter the **power -H [host name] -s** command at the SSM CLI prompt to shut down a host. For IPMI hosts, shutdown is conducted with IPMI. For Agent Managed hosts, shutdown is performed by the SuperDoctor 5. If a host supports IPMI and SD5, IPMI is given priority.

```
SSM CLI>power -H 192.168.12.9,192.168.12.31 -s
| Host          | IP           | Status | Message                                     |
| -----|-----|-----|-----|
| 192.168.12.9 | 192.168.12.9 | OK     | IPMI power down successfully |
| 192.168.12.31| 192.168.12.31| OK     | The shutdown command is fired.|
#Summary of execution: OK[2]

SSM CLI>
```

Figure 14-22

14.6.9 -r: Reboot hosts by SD5 or IPMI

Enter the **power -H [host name] -r** command at the SSM CLI prompt to reboot a host. For IPMI hosts, the reboot is conducted with IPMI. For Agent Managed hosts, the reboot is performed by the SuperDoctor 5. If a host supports IPMI and SuperDoctor 5, IPMI is given priority.

```
SSM CLI>power -H 192.168.12.9,192.168.12.31 -r
| Host          | IP           | Status | Message                                     |
| -----|-----|-----|-----|
| 192.168.12.9 | 192.168.12.9 | OK     | IPMI Reset successfully |
| 192.168.12.31| 192.168.12.31| OK     | The reboot command is fired.|
#Summary of execution: OK[2]

SSM CLI>
```

Figure 14-23

14.6.10 -p: Power up hosts by WOL or IPMI

Enter the **power -H [host name] -p** command at the SSM CLI prompt to power up a host. IPMI hosts are powered up with IPMI while Agent Managed hosts are powered up with WOL. If a host supports IPMI and SuperDoctor 5, IPMI is given priority.

```
SSM CLI>power -H 192.168.12.9,192.168.12.31 -p
| Host          | IP          | Status | Message |
| -----|-----|-----|-----|
| 192.168.12.9 | 192.168.12.9 | OK     | IPMI power up successfully|
| 192.168.12.31| 192.168.12.31| OK     | Wake-on-LAN packet sent. |
#Summary of execution: OK[2]
SSM CLI>
```

Figure 14-24

14.7 Status Command

The **status** command checks whether hosts are operating or are down.

14.7.1 -h: Display status command arguments

Enter **status -h** at the SSM CLI prompt to display all supported arguments onscreen.

```
SSM CLI>status -h
usage: Usage: status (-H|-G) [-f] [-h]

Options:
-csv,--csv           Display query result in the CSV format
-f,--file <arg>     Output query result to a file
-G,--hostgroup <arg> Host group
-H,--host <arg>     Host
-h,--help           Help
SSM CLI>
```

Figure 14-25

14.7.2 -G: Display host group status

Enter **status -G [host group name]** at the SSM CLI prompt to display the status of all hosts belonging to the host group, as shown below.

```
SSM CLI>status -G Agent_Managed
| Host          | IP          | Status |
| -----|-----|-----|
| jcis-server | 192.168.12.4 | UP     |
| Server-93   | 192.168.12.93| UP     |
| Server-30   | 192.168.12.30| DOWN   |
#Summary of execution: Up[2] Down[1]
SSM CLI>
```

Figure 14-26

If a non-existent host group is specified, the specified host group is displayed in the Host column and an Unknown message is shown in the IP and Status columns, respectively, as shown below.

```
SSM CLI>status -G all_host
| Host| IP| Status |
| ----| --| -----|
Hostgroup all_host does not exist.

SSM CLI>
```

Figure 14-27

Multiple host groups are separated by commas.

```
SSM CLI>status -G Agent_Managed,IPMI_Host
| Host          | IP          | Status|
| -----| -----| -----|
| Server-30    | 192.168.12.30| UP   |
| Server-93    | 192.168.12.93| UP   |
| 192.168.12.56| 192.168.12.56| UP   |
| 192.168.12.53| 192.168.12.53| UP   |
| 192.168.12.57| 192.168.12.57| UP   |
| jcis-server  | 192.168.12.4 | UP   |
#Summary of execution: Up[6]

SSM CLI>
```

Figure 14-28



Note: Spaces are not allowed after and before a comma when multiple host groups are specified.

14.7.3 -H: Display host status

Enter **status -H [host name]** at the SSM CLI prompt to display the host status as shown below.

```
SSM CLI>status -H jcis-server
| Host          | IP          | Status|
| -----| -----| -----|
| jcis-server  | 192.168.12.4| UP   |
#Summary of execution: Up[1]

SSM CLI>
```

Figure 14-29

14.8 List Command

The **list** command enumerates all hosts and host groups defined in the SSM Database or configuration files.

14.8.1 -h: Display list command arguments

Enter **list -h** at the SSM CLI prompt to display all supported arguments onscreen.

```
SSM CLI>list -h
usage: Usage: list (-ah|-ag|-H|-G) [-h] [-csv] [-f]

Options:
-ag,--allGroup      List all host groups
-ah,--allHost       List all hosts
-csv,--csv          Display the query in CSV format
-f,--file <arg>    Output file
-G,--hostgroup <arg> Display host members of host groups
-H,--host <arg>    Display host groups of hosts
-h,--help           Help
SSM CLI>
```

Figure 14-30

14.8.2 -ag: List all host groups

Enter **list -ag** at the SSM CLI prompt to display all host groups defined in the SSM Database or configuration files.

```
SSM CLI>list -ag
| Group Name | Member | Address |
| -----| -----| -----|
| Agent_Managed| Server-30 | 192.168.12.30 |
| Agent_Managed| jcis-server | 192.168.12.4 |
| Agent_Managed| Server-93 | 192.168.12.93 |
| DataCenter1 | 192.168.12.118| 192.168.12.118|
| DataCenter1 | 192.168.12.138| 192.168.12.138|
| DataCenter1 | 192.168.12.143| 192.168.12.143|
| DataCenter1 | 192.168.12.151| 192.168.12.151|
| DataCenter1 | 192.168.12.158| 192.168.12.158|
| IPMI_Host | 192.168.12.53 | 192.168.12.53 |
| IPMI_Host | 192.168.12.56 | 192.168.12.56 |
| IPMI_Host | 192.168.12.57 | 192.168.12.57 |
SSM CLI>
```

Figure 14-31

14.8.3 -ah: List all hosts

Enter **list -ah** at the SSM CLI prompt to display all managed hosts defined in the SSM Database or configuration files, as shown below.

```
SSM CLI>list -ah
| Host Name | Group Name | Address |
| -----| -----| -----|
| Server-30 | Agent_Managed| 192.168.12.30|
| Server-32 | Agent_Managed| 192.168.12.32|
| Server-33 | Agent_Managed| 192.168.12.33|
| 192.168.12.53| IPMI_Host | 192.168.12.53|
| 192.168.12.55| | 192.168.12.55|
| 192.168.12.54| | 192.168.12.54|
| 192.168.12.56| IPMI_Host | 192.168.12.56|
| 192.168.12.24| | 192.168.12.24|
| 192.168.12.23| | 192.168.12.23|
| 192.168.12.36| | 192.168.12.36|
| 192.168.12.9 | | 192.168.12.9 |
| Server-11 | | 192.168.12.11|
SSM CLI>
```

Figure 14-32

14.8.4 -G: List members of a host group

Enter **list -G all-agent** at the SSM CLI prompt to display host group members as defined in the SSM Database or configuration files. Multiple host groups are separated by commas.

```
SSM CLI>list -G Agent_Managed
| Group Name | Member | Address |
| -----| -----| -----|
| Agent_Managed| Server-30| 192.168.12.30|
| Agent_Managed| Server-32| 192.168.12.32|
| Agent_Managed| Server-33| 192.168.12.33|
SSM CLI>
```

Figure 14-33

14.8.5 -H: List host groups of hosts

Enter **list -H [host name]** at the SSM CLI prompt to display the host groups of the specified hosts as defined in the SSM Database or configuration files. Multiple hosts are separated by commas.

```
SSM CLI>list -H Server-30,192.168.12.53
| Host Name | Group Name | Address |
| -----| -----| -----|
| Server-30 | Agent_Managed| 192.168.12.30|
| 192.168.12.53| IPMI_Host | 192.168.12.53|
SSM CLI>
```

Figure 14-34

14.9 Systeminfo Command

The **systeminfo** command supports host device information gathered from operating systems by SD5s²³.

14.9.1 -h: Display systeminfo command arguments

Enter **systeminfo** or **systeminfo -h** at the SSM CLI prompt to display all supported arguments onscreen.

```
SSM CLI>systeminfo -h
usage: Usage: systeminfo {-H|-G} {-n} [-csv] [-f] [-h] [-l]

Options:
-csv,--csv           Display query result in the CSV format
-f,--file <arg>     Output query result to a file
-G,--hostgroup <arg> Host group
-H,--host <arg>     Host
-h,--help           Help
-l,--list           Show device list
-n,--index <arg>   Assign a device to be shown
SSM CLI>
```

Figure 14-35

14.9.2 -l: Display system information types and index

Enter **systeminfo -H [host name] -l** command at the SSM CLI prompt to display system information types and indexes.

```
SSM CLI>systeminfo -l
Index: System Info Type
-----
0      account
1      baseboard
2      bios
3      cdrom
4      chassis
5      computer system
6      disk
7      floppy
8      keyboard
9      logical disk
10     logical memory
11     memory
12     desktop monitor
13     network
14     os
15     processor
16     process
17     port connector
18     pointing device
19     parallel port
20     printer
21     service
23     share
24     serial port
25     system slot
26     computer summary
27     time zone
28     video controller
30     ipmi
34     startup command
35     fru
36     oem strings
37     system cfg options
38     power supply

SSM CLI>_
```

Figure 14-36

²³ System information is only available on agent-managed hosts.

14.9.3 -n: Display system information

Enter the **systeminfo -H [host name] -n [index]** command at the SSM CLI prompt to display the system information of a specified index. For example, enter **system info -H Server-33 -n 2** to display the BIOS information of host Server-33, as shown below.

```
SSM CLI>systeminfo -H Server-33 -n 2
| Server-33 <10.134.14.33>
|-----|
| System Info Type      | bios
| SMBIOSMajor Version  | 2
| SMBIOSMinor Version  | 6
| SMBIOSPresent        | TRUE
| Manufacturer         | American Megatrends Inc.
| Version              | 2.0a
| Release Date         | 2011-04-08 00:00:00.00
|-----|
#Summary of execution: OK[1]
SSM CLI>_
```

Figure 14-37

14.10 Env Command

Two configuration data sources (data source for short) are supported by SSM CLI: **SSM Database** and **configuration files**. By default, SSM CLI reads configuration data from the SSM Database. Users can use the **env** command to display current data source setting. Note that the setting affects SSM CLI only.

14.10.1 -h: Display env command arguments

Enter **env** or **env -h** at the SSM CLI prompt to display all supported arguments onscreen.

```
SSM CLI>env -h
usage: Usage: env [-s] [-h]

Options:
-h, --help      Help
-s, --show      Display current data source mode
SSM CLI>_
```

Figure 14-38

14.10.2 -s: Display current data source setting

Enter the **env -s** command at the SSM CLI prompt to display the current data source setting. Two data sources are supported: DB (database) and file. The default value is from the DB.

```
SSM CLI>env -s
Connect datasource from DB.
SSM CLI>
```

Figure 14-39

14.11 Storage Command

The **storage** command is an in-band command that supports the monitoring of a host's hard disk health information via a SuperDoctor 5. To use this command, the hard disks must support SMART. Note that the SMART check does not support RAID hard drives, USB hard drives or USB flash drives. The RAID health check function is available on LSI MegaRAID 2108, 2208 and 3108 controllers except Windows driver is MR6.6 code set or higher version, and it is not available on LSI MegaRAID 2008, LSI Fusion-MPT based and Intel Rapid Storage Technology controllers.

14.11.1 -h: Display storage command arguments

Enter **storage -h** at the SSM CLI prompt to display all supported arguments onscreen.

```
SSM CLI>storage -h
usage: Usage: storage {-H|-G} {-n|-s|-r} [-csv] [-f] [-h]

Options:
-csv,--csv           Display query result in the CSV format
-f,--file <arg>     Output query result to a file
-G,--hostgroup <arg> Host group
-H,--host <arg>     Host
-h,--help           Help
-n,--number <arg>   Check the total number of hard disks.
-r,--raid <arg>     Check RAID health. 1:enable, 0:disable
-s,--smart <arg>    Check hard disk health with SMART. 1:enable,
                    0:disable
SSM CLI>
```

Figure 14-40

14.11.2 -n: Check the total number of hard drives

The `-n` argument checks the total number of hard disks in a host. Enter `storage -H [host name] -n [expected hard disk number]` at the SSM CLI prompt to display the hard disk number check results onscreen.

```
SSM CLI>storage -H 192.168.12.104 -n 4
| Host          | Address        | Status | Message                                     |
| -----|-----|-----|-----|
| 192.168.12.104| 192.168.12.104| OK     | 4 physical disk(s) on system.           |
|              |               |       | Intel Corporation Patsburg 6           |
|              |               |       | Port SATA AHCI Controller -- 1       |
|              |               |       | physical disk(s)                       |
#Summary of execution: OK[1]
SSM CLI>
```

Figure 14-41

14.11.3 -s: Check the hard disks status with SMART

The `-s` argument checks the hard disk status with SMART. Enter `storage -H [host name] -s 1` at the SSM CLI prompt to display the hard disk status check results onscreen.

```
SSM CLI>storage -H 192.168.12.104 -s 1
| Host          | Address        | Status | Message                                     |
| -----|-----|-----|-----|
| 192.168.12.104| 192.168.12.104| OK     | 4 physical disk(s) on system.           |
|              |               |       | Intel Corporation Patsburg 6           |
|              |               |       | Port SATA AHCI Controller -- 1       |
|              |               |       | physical disk(s) -- /dev/sda         |
|              |               |       | (VNP210B2GHRK3B) is SMART check     |
|              |               |       | k OK                                   |
#Summary of execution: OK[1]
SSM CLI>
```

Figure 14-42

Using the `-csv` argument you can see the full format of the returned message including the serial number of each disk under monitoring.

```
SSM CLI>storage -H 192.168.12.104 -s 1 -csv
Host,Address,Status,Message
192.168.12.104,192.168.12.104,OK,4 physical disk(s) on system.

Intel Corporation Patsburg 6 Port SATA AHCI Controller
-- 1 physical disk(s)
-- /dev/sda (VNP210B2GHRK3B) is SMART check OK
SSM CLI>
```

Figure 14-43

The `-s` and `-n` arguments can be used at the same time. In other words, you can check the total number of hard disks and check the status of hard disks with SMART at the same time. For example, enter

storage -H [host name] -s 1 -n 3 -csv at the SSM CLI prompt to display the hard disk status and the total number of hard disk drives checked.

```
SSM CLI>storage -H 192.168.12.104 -s 1 -n 3 -csv
Host,Address,Status,Message
192.168.12.104,192.168.12.104,CRITICAL,Physical disk number is incorrect on system, expect: 3, actual: 4

Intel Corporation Patsburg 6 Port SATA AHCI Controller
-- 1 physical disk(s)
-- /dev/sda (VNP210B2GHRK3B) is SMART check OK
SSM CLI>
```

Figure 14-44

14.11.4 -r: Check the RAID status

The **-r** argument checks the health of RAID controllers. Enter **storage -H [host name] -r 1** at the SSM CLI prompt to display the RAID status check results onscreen.

```
SSM CLI>storage -H 192.168.12.104 -r 1
| Host          | Address        | Status | Message                                     |
| -----|-----|-----|-----|
| 192.168.12.104| 192.168.12.104| OK     | 4 physical disk(s) on system.           |
|              |               |       | Intel Corporation Patsburg 6           |
|              |               |       | Port SATA AHCI Controller -- 1       |
|              |               |       | physical disk(s) Supermicro         |
|              |               |       | SMC2108 Controller #0 -- 3 phy      |
|              |               |       | sical disk(s) -- The status of      |
|              |               |       | RAID is normal.                       |
#Summary of execution: OK[1]
SSM CLI>
```

Figure 14-45

14.12 Memory Command

The **memory** command is an in-band command that supports the monitoring of a host's physical memory health via a SuperDoctor 5. Note that this command does not support desktop computers.²⁴

14.12.1 -h: Display memory command arguments

Enter **memory -h** at the SSM CLI prompt to display all supported arguments onscreen.

```
SSM CLI>memory -h
usage: Usage: memory {-H|-G} {-n|-m|-M} [-csv] [-f] [-h]

Options:
-csv,--csv           Display query result in the CSV format
-f,--file <arg>     Output query result to a file
-G,--hostgroup <arg> Host group
-H,--host <arg>      Host
-h,--help            Help
-M,--uecc <arg>     Check UECC, e.g., 2h1 means 1 time in 2 hours.
-m,--cecc <arg>     Check CECC, e.g., 1d2 means 2 times in 1 day per 1
                    G.
-n,--number <arg>   Check the total number of DIMM(s)
SSM CLI>
```

Figure 14-46

14.12.2 -m: Check memory health by counting the number of CECC error events

Use the **-m** argument to specify a user-defined threshold for a memory health check by counting the number of CECC (correctable ECC) error events during a time period. The argument format is as follows:

[duration][failure count]

- [duration]:
 - d: day
 - h: hour
 - m: minute
- [failure count]: The acceptable number of CECC errors. To trigger a critical status, the failure counts must be greater than this value.

For example, **-m 1d2** specifies a threshold for memory that indicates two CECC errors per 1GB RAM within one day (24 hours) are allowed. The threshold for CECC applies to a RAM size of 1GB. If you have a 4GB DIMM and specify the **-m 1d2** threshold, the acceptable CECC error counts for the 4GB DIMM are 8.

²⁴ Not all Supermicro servers support this function. Please refer to the Supermicro Web site for the supported list.

Enter **memory -H [host name] -m 1d2** at the SSM CLI prompt to display the memory health status check results onscreen.

```
SSM CLI>memory -H jcis-server -m 1d2
| Host          | IP          | Status | Message                                     |
| -----|-----|-----|-----|
| jcis-server | 192.168.12.4 | OK    | Memory is OK; 6 DIMM(s), 24...|
#Summary of execution: OK[1]
SSM CLI>
```

Figure 14-47

If the memory status is in critical state, the problematic DIMM number is shown onscreen as shown below.

```
SSM CLI>memory -H jcis-server -m 1d2 -csv
Host,IP,Status,Message
jcis-server,192.168.12.4,CRITICAL,6 DIMM(s), 24.0 GB RAM; CECC error, thres
hold: 2 time(s) in 1 day, PO_DIMM3A: 9 time(s) in 1 day
SSM CLI>
```

Figure 14-48

14.12.3 -M: Check memory health by counting the number of UECC error events

Use the **-M** argument to specify a user-defined threshold for the memory health check by counting the number of UECC (uncorrectable ECC) error events during a time period. The argument format is as follows:

[duration][failure count]

- [duration]:
 - d: day
 - h: hour
 - m: minute
- [failure count]: The acceptable number of UECC errors. To trigger a critical status, the failure counts must be greater than this value.

For example, **-M 1d0** specifies a threshold for memory that indicates zero UECC errors within one day (24 hours) are allowed. Unlike the **-m** argument, the threshold for UECC is irrelevant to the DIMM size to be checked.

Enter **memory -H [host name] -M 1d0** at the SSM CLI prompt to display the memory health status check results onscreen.

```
SSM CLI>memory -H jcis-server -M 1d0
| Host          | IP          | Status| Message
| -----|-----|-----|-----|
| jcis-server| 192.168.12.4| OK    | Memory is OK; 6 DIMM(s), 24...|
#Summary of execution: OK[1]
SSM CLI>
```

Figure 14-49

If the memory status is in critical state, the problematic DIMM is shown onscreen.

```
SSM CLI>memory -H jcis-server -M 1d0 -csv
Host,IP,Status,Message
jcis-server,192.168.12.4,CRITICAL,6 DIMM(s), 24.0 GB RAM; ; UECC error, threshold: 0 time(s) in 1 day, PO_DIMM3A: 1 time(s) in 1 day.
SSM CLI>
```

Figure 14-50

The **-m** and **-M** arguments can be used at the same time. For example, enter **memory -H [host name] -m 1d1 -M 1d0 -csv** at the SSM CLI prompt to display the memory status check results onscreen.

```
SSM CLI>memory -H jcis-server -m 1d1 -M 1d0 -csv
Host,IP,Status,Message
jcis-server,192.168.12.4,CRITICAL,6 DIMM(s), 24.0 GB RAM; CECC OK, threshold: 1 time(s) in 1 day; UECC error, threshold: 0 time(s) in 1 day, PO_DIMM3A : 1 time(s) in 1 day.
SSM CLI>
```

Figure 14-51



Notes: For memory health monitoring, the check logic is based on the following two factors:

- There are memory error logs existing in the BIOS event log.
- A log entry's generated time falls within the check time period specified by users.

For example, suppose that a user employs the **-M 1d0** option (i.e., any UECC error occurring in one day will cause a critical state) to conduct a memory error check. Once a UECC error has occurred, the status will remain critical for one day, even after the user has manually replaced the failed memory module. To get an OK status immediately after manually repairing the memory, the user needs to clear the BIOS event logs from the BIOS setup menu.

Part 5 Advanced Topics

15 SSM Utilities

Three SSM utility applications, **innoutconfig**, **dbtool** and **changejvm**, are provided to import/export configuration data, to create a database for SSM and to change Java VM used by SSM. This chapter shows you how to use these three utilities.

15.1 Export and Import Configuration Data

innoutconfig is a utility program located in the `[install folder]\shared\tools` folder that can export and import configuration data from and to a database²⁵.

Usage:

```
innoutconfig [-h | --help ] [-n <arg>] [-o <arg>] [-t <arg>]
```

Options:

-h, --help	Show the help menu.
-n	The instance in the database to be exported in case there are multiple instances in the same database. The default value is “default” if the execution mode is set to “db2f”.
-o	The output folder. This argument is required if the execution mode is set to “db2f”.
*-t	The execution mode: f2db: import files to database db2f: export database to files

²⁵ The configuration data used in SSM 2.0 is not backward compatible with that in SSM 1.0. Make sure you know the version of SSM before importing configuration data to the SSM Database.

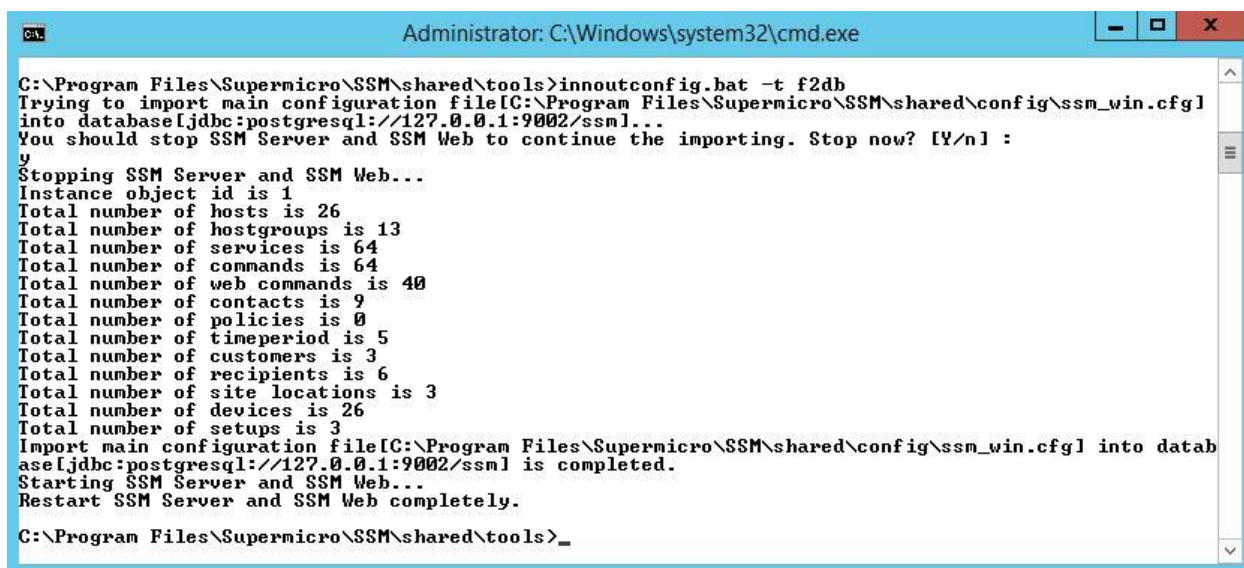
There are mainly two scenarios in using innoutconfig utility. Examples are shown as below.

Scenario 1:

By default, users employ a Web browser connected to SSM Web to manage configuration data. For example, host and associated built-in service configurations are added by the Host Discovery Wizard. However, it may be more convenient for some users to edit configuration data with a text editor. In such cases, you can use **innoutconfig** (by specifying execution mode db2f) to export configuration data from an SSM database to files, modify them with a text editor, and then import the data into the same SSM database by specifying execution mode f2db for **innoutconfig**.

However, it's strongly recommended that you should only modify configuration files in the [output folder]\shared\config\generated folder. Users are not allowed to modify the built-in configuration files in the [output folder]\shared\config\builtin.

The following figure shows an example using the **innoutconfig -t f2db** command to import configurations from files (all file changes have been put in [install folder]\shared\config) to an SSM database. The result shows that 64 commands, 40 web commands, 9 contact, and 1 time period were imported into the database.



```
Administrator: C:\Windows\system32\cmd.exe
C:\Program Files\Supermicro\SSM\shared\tools>innoutconfig.bat -t f2db
Trying to import main configuration file[C:\Program Files\Supermicro\SSM\shared\config\ssm_win.cfg]
into database[jdbc:postgresql://127.0.0.1:9002/ssm]...
You should stop SSM Server and SSM Web to continue the importing. Stop now? [Y/n] :
y
Stopping SSM Server and SSM Web...
Instance object id is 1
Total number of hosts is 26
Total number of hostgroups is 13
Total number of services is 64
Total number of commands is 64
Total number of web commands is 40
Total number of contacts is 9
Total number of policies is 0
Total number of timeperiod is 5
Total number of customers is 3
Total number of recipients is 6
Total number of site locations is 3
Total number of devices is 26
Total number of setups is 3
Import main configuration file[C:\Program Files\Supermicro\SSM\shared\config\ssm_win.cfg] into databa
se[jdbc:postgresql://127.0.0.1:9002/ssm] is completed.
Starting SSM Server and SSM Web...
Restart SSM Server and SSM Web completely.
C:\Program Files\Supermicro\SSM\shared\tools>_
```

Figure 15-1

Besides editing, for the purpose of migrating data between different versions of SSM, you can copy the configuration files from the older version to the newer one, and then use **innoutconfig** to import the data into the newer version of SSM. Two folders [install folder of old SSM]\shared\config\CallHome and [install folder of old SSM]\shared\config\generated must be copied to the corresponding SSM folders of the newer version first.

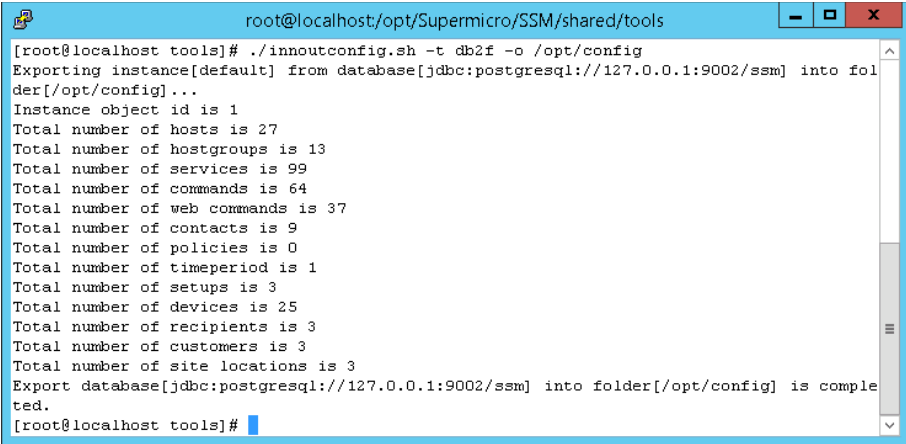


Note: You need to manually restart the SSM Server and SSM Web when importing configurations from files to the SSM Database.

Scenario 2:

In order to keep the configuration data (of hosts, services, contacts, etc.) while migrating from an old version of SSM to a newer version of SSM, you can use `innoutconfig` to export configurations from the SSM database to files. Later, after you install the new version of SSM, copy the configuration files stored in `[install folder of old SSM]\shared\config\CallHome` and `[install folder of old SSM]\shared\config\generated` to the corresponding SSM folders of the newer version.

The following figure shows an example using the `innoutconfig -t db2f -o /opt/config` command to export configurations from an SSM Database to files. The result shows that 56 commands, 30 web commands, 1 contact, and 1 time period were exported from an SSM Database to files. These files are placed in the `/opt/config` folder.



```
root@localhost:opt/Supermicro/SSM/shared/tools
[root@localhost tools]# ./innoutconfig.sh -t db2f -o /opt/config
Exporting instance[default] from database[jdbc:postgresql://127.0.0.1:9002/ssm] into folder[/opt/config]...
Instance object id is 1
Total number of hosts is 27
Total number of hostgroups is 13
Total number of services is 99
Total number of commands is 64
Total number of web commands is 37
Total number of contacts is 9
Total number of policies is 0
Total number of timeperiod is 1
Total number of setups is 3
Total number of devices is 25
Total number of recipients is 3
Total number of customers is 3
Total number of site locations is 3
Export database[jdbc:postgresql://127.0.0.1:9002/ssm] into folder[/opt/config] is completed.
[root@localhost tools]#
```

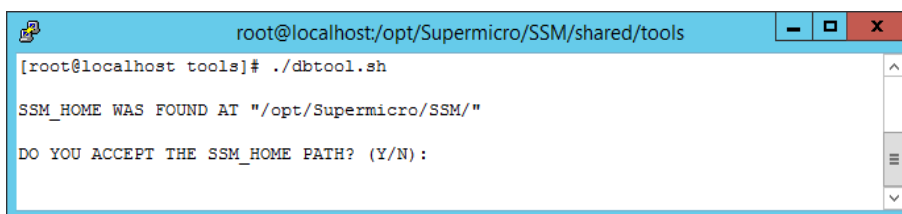
Figure 15-2

15.2 Using DBTool to Setup an SSM Database

When users install SSM they can choose which database server is to be used. SSM also provides a utility called **dbtool**, which can be used to create a database for SSM. Suppose that you choose to use the built-in PostgreSQL database when you install SSM. After completing the installation, you decide to use an external PostgreSQL instead of the built-in PostgreSQL. In this situation, you do not need to reinstall SSM. Just use **dbtool** to create a new database on the PostgreSQL then use **innoutconfig** to import/export default configuration data.

The following shows the steps to use **dbtool**.

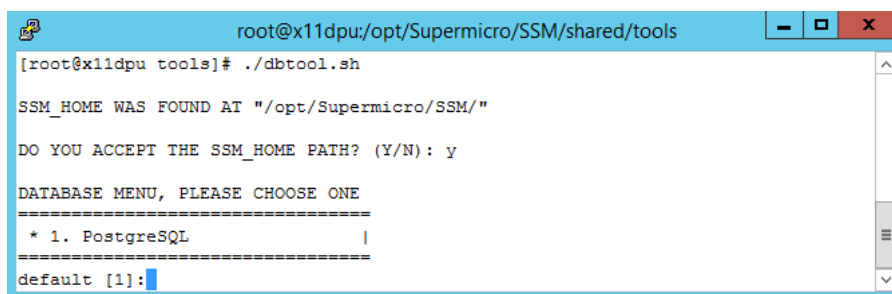
1. Execute the **dbtool.bat** or **dbtool.sh** command located in the **[install folder]\shared\tools** folder. Type **Y** to accept the **SSM_HOME** path, which represents the root folder of SSM, and then press the **<Enter>** key to continue.



```
root@localhost/opt/Supermicro/SSM/shared/tools
[root@localhost tools]# ./dbtool.sh
SSM_HOME WAS FOUND AT "/opt/Supermicro/SSM/"
DO YOU ACCEPT THE SSM_HOME PATH? (Y/N):
```

Figure 15-3

2. Choose the database to be used from the menu. PostgreSQL is chosen as an example. Type **1** and press the **<Enter>** key to continue.



```
root@x11dpu:/opt/Supermicro/SSM/shared/tools
[root@x11dpu tools]# ./dbtool.sh
SSM_HOME WAS FOUND AT "/opt/Supermicro/SSM/"
DO YOU ACCEPT THE SSM_HOME PATH? (Y/N): y
DATABASE MENU, PLEASE CHOOSE ONE
=====
* 1. PostgreSQL
=====
default [1]:
```

Figure 15-4



Note: The **dbtool** can create the SSM databases and required tables for PostgreSQL.

3. Choose built-in PostgreSQL database or external PostgreSQL database. Type **N** and press the **<Enter>** key to continue.

```
root@x11dpu:/opt/Supermicro/SSM/shared/tools
DATABASE MENU, PLEASE CHOOSE ONE
=====
* 1. PostgreSQL |
=====
default [1]:
DETECT DATABASE JDBC DRIVER....
FIND DRIVER...

IS BUILT-IN DATABASE OF SSM ? (Y/N)
default [N]
```

Figure 15-5

- 4. Enter the SSM database name and press the <Enter> key to continue.

```
root@x11dpu:/opt/Supermicro/SSM/shared/tools
=====
default [1]:
DETECT DATABASE JDBC DRIVER....
FIND DRIVER...

IS BUILT-IN DATABASE OF SSM ? (Y/N)
default [N]N

ENTER DB NAME, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
default [ssm]:smc
```

Figure 15-6

- 5. Enter the database IP address or DNS name and press the <Enter> key to continue.

```
root@x11dpu:/opt/Supermicro/SSM/shared/tools
FIND DRIVER...

IS BUILT-IN DATABASE OF SSM ? (Y/N)
default [N]N

ENTER DB NAME, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
default [ssm]:smc

ENTER IP, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
default [127.0.0.1]:ssmdb.supermicro.com.tw
```

Figure 15-7

- 6. Enter the database port number and press the <Enter> key to continue.

```
root@x11dpu:/opt/Supermicro/SSM/shared/tools
default [N]N

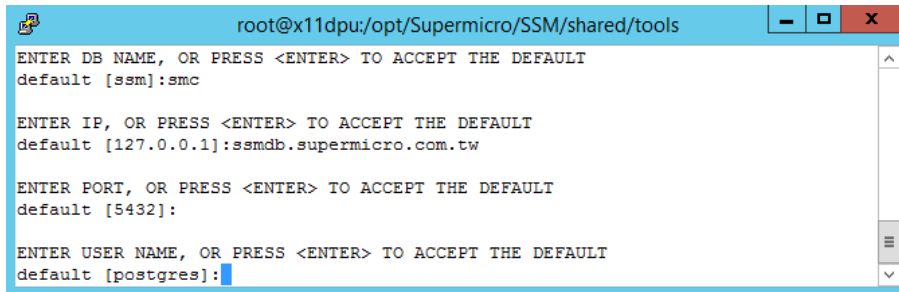
ENTER DB NAME, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
default [ssm]:smc

ENTER IP, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
default [127.0.0.1]:ssmdb.supermicro.com.tw

ENTER PORT, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
default [5432]:
```

Figure 15-8

7. Enter the database account and press the **<Enter>** key to continue.



```
root@x11dpu:/opt/Supermicro/SSM/shared/tools
ENTER DB NAME, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
default [ssm]:smc

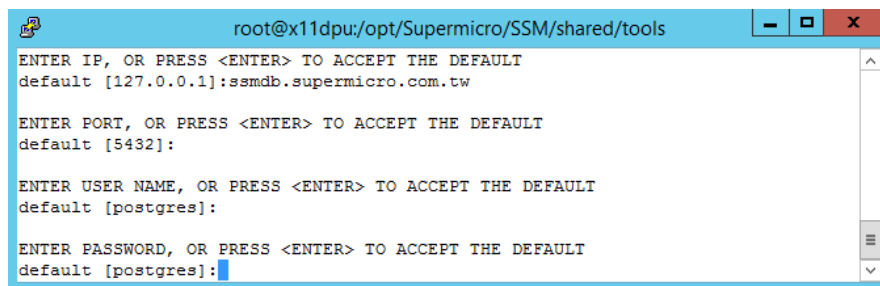
ENTER IP, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
default [127.0.0.1]:ssmdb.supermicro.com.tw

ENTER PORT, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
default [5432]:

ENTER USER NAME, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
default [postgres]:
```

Figure 15-9

8. Enter the password to access the database and press the **<Enter>** key to continue.



```
root@x11dpu:/opt/Supermicro/SSM/shared/tools
ENTER IP, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
default [127.0.0.1]:ssmdb.supermicro.com.tw

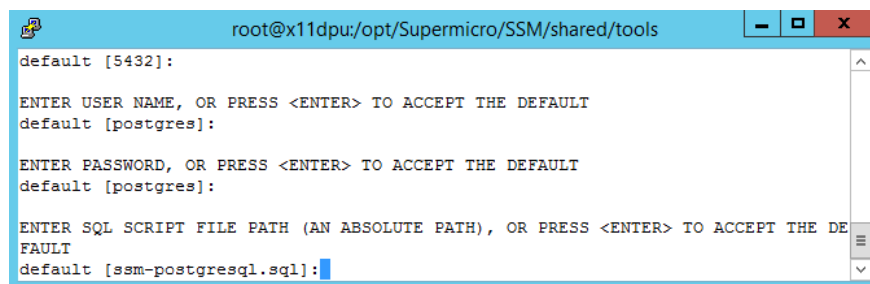
ENTER PORT, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
default [5432]:

ENTER USER NAME, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
default [postgres]:

ENTER PASSWORD, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
default [postgres]:
```

Figure 15-10

9. Press the **<Enter>** key to accept the script file used to create the SSM database.



```
root@x11dpu:/opt/Supermicro/SSM/shared/tools
default [5432]:

ENTER USER NAME, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
default [postgres]:

ENTER PASSWORD, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
default [postgres]:

ENTER SQL SCRIPT FILE PATH (AN ABSOLUTE PATH), OR PRESS <ENTER> TO ACCEPT THE DE
FAULT
default [ssm-postgresql.sql]:
```

Figure 15-11

10. Type **Y** to start to create the SSM database and press the **<Enter>** key to continue.

```
root@x11dpu:/opt/Supermicro/SSM/shared/tools
default [postgres]:
ENTER PASSWORD, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
default [postgres]:
ENTER SQL SCRIPT FILE PATH (AN ABSOLUTE PATH), OR PRESS <ENTER> TO ACCEPT THE DE
FAULT
default [ssm-postgresql.sql]:
FIND SQL SCRIPT:sqlScript/ssm-postgresql.sql
START TO IMPORT DATABASE SCHEMA? (Y/N):
```

Figure 15-12

11. Wait briefly while dbtool creates the SSM database.

```
root@x11dpu:/opt/Supermicro/SSM/shared/tools
ENTER SQL SCRIPT FILE PATH (AN ABSOLUTE PATH), OR PRESS <ENTER> TO ACCEPT THE DE
FAULT
default [ssm-postgresql.sql]:
FIND SQL SCRIPT:sqlScript/ssm-postgresql.sql
START TO IMPORT DATABASE SCHEMA? (Y/N): Y

Create new DB...
#Test Database connection...
Drop smc...
#####
```

Figure 15-13

12. Type **Y** to save the database settings to the property files that are used by SSM Web, SSM Server and SSM CLI.

```
root@localhost:/opt/Supermicro/SSM/shared/tools
Execute sql: sqlScript/ssm-data-create-view.sql
Execute sql: sqlScript/ssm-data-insert-users-withoutid.sql
IMPORT DATABASE SCHEMA SUCCESSFULLY!!
SAVE AS "datasource.properties" ? (Y/N): Y
```

Figure 15-14

13. The SSM database is created.

```
root@localhost:/opt/Supermicro/SSM/shared/tools
IMPORT DATABASE SCHEMA SUCCESSFULLY!!
SAVE AS "datasource.properties" ? (Y/N): Y
Save file:/opt/Supermicro/SSM/shared/config/datasource.properties
SAVE DATASOURCE PROPERTIES SUCCESSFULLY!!
[root@localhost tools]#
```

Figure 15-15

15.3 Using ChangeJVM to Change a Java VM

When users install SSM, they can choose the kind of Java VM to be used. The utility **changejvm** located in the **[install folder]\shared\tools** folder can be used to change a Java VM.

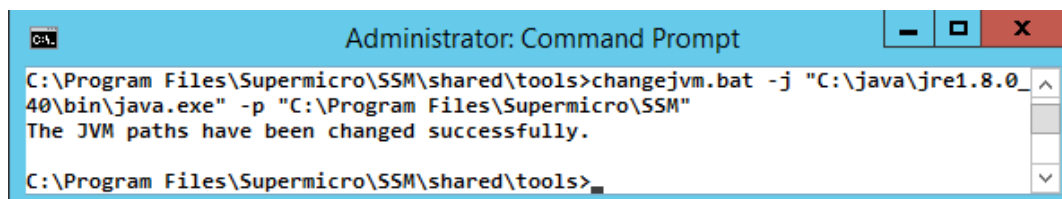
Usage:

```
changejvm [-p <arg>] [-h | --help ] [-j <arg>]
```

Options:

- p** The search folder. The argument is optional and the default value is **[install folder]**.
- *-j** The kind of Java VM to be used, e.g., `/usr/java/jdk1.8.0_51/jre/bin/java`.
- h, --help** Shows the help menu.

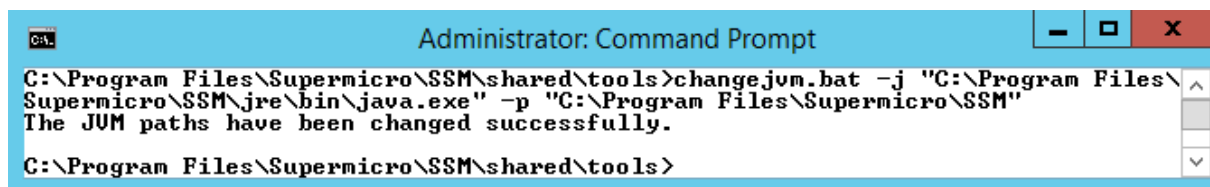
The following figure shows how the command **changejvm.bat -j "C:\Java\jre1.8.0_40 \bin\java.exe" -p "C:\Program Files\Supermicro\SSM"** is used to change to another version of Java VM (JRE 1.8.0_40).



```
Administrator: Command Prompt
C:\Program Files\Supermicro\SSM\shared\tools>changejvm.bat -j "C:\Java\jre1.8.0_40\bin\java.exe" -p "C:\Program Files\Supermicro\SSM"
The JVM paths have been changed successfully.
C:\Program Files\Supermicro\SSM\shared\tools>
```

Figure 15-16

The following figure shows how the command **changejvm.bat -j "C:\Program Files\Supermicro\SSM\jre\bin\java.exe" -p "C:\Program Files\Supermicro\SSM"** is used to change to the built-in Java VM of SSM. The built-in Java VM is located in the **[install folder]\jre\bin** folder.



```
Administrator: Command Prompt
C:\Program Files\Supermicro\SSM\shared\tools>changejvm.bat -j "C:\Program Files\Supermicro\SSM\jre\bin\java.exe" -p "C:\Program Files\Supermicro\SSM"
The JVM paths have been changed successfully.
C:\Program Files\Supermicro\SSM\shared\tools>
```

Figure 15-17



Notes:

- You need to stop the SSM services before changing Java VM if SSM is still running.
 - You need to manually restart the SSM service after changing Java VM.
 - The architecture of Java VM you selected must suit the installation program. For example, to use an x86 version of SSM, you need to install an x86 version of Java VM first.
 - It's recommended that you use the latest version of OpenJDK 8 in SSM. Other Oracle JREs (i.e. JRE 6, JRE 7, and JRE 11+) and Non-Oracle Java VMs (i.e. OpenJDK 6, OpenJDK 7, and OpenJDK 11+) are not supported in this version.
-

16 SSM Certification

When server-side applications (i.e. SSM Server, SSM Web, and SSM CLI) communicate with a SuperDoctor 5, the communication channel can be configured to use Secure Sockets Layer (SSL). SSM supports secure communications with SSL and a public key infrastructure (PKI). A built-in key pair shared by the SSM Server, SSM Web, and SSM CLI and a key pair for the SuperDoctor 5 are included in the SSM installation program. By default, SSM uses the built-in key pairs to establish an SSL channel for communications. This chapter shows you how to replace the default key pairs by using the **SSM Certificate** program.

16.1 Introduction

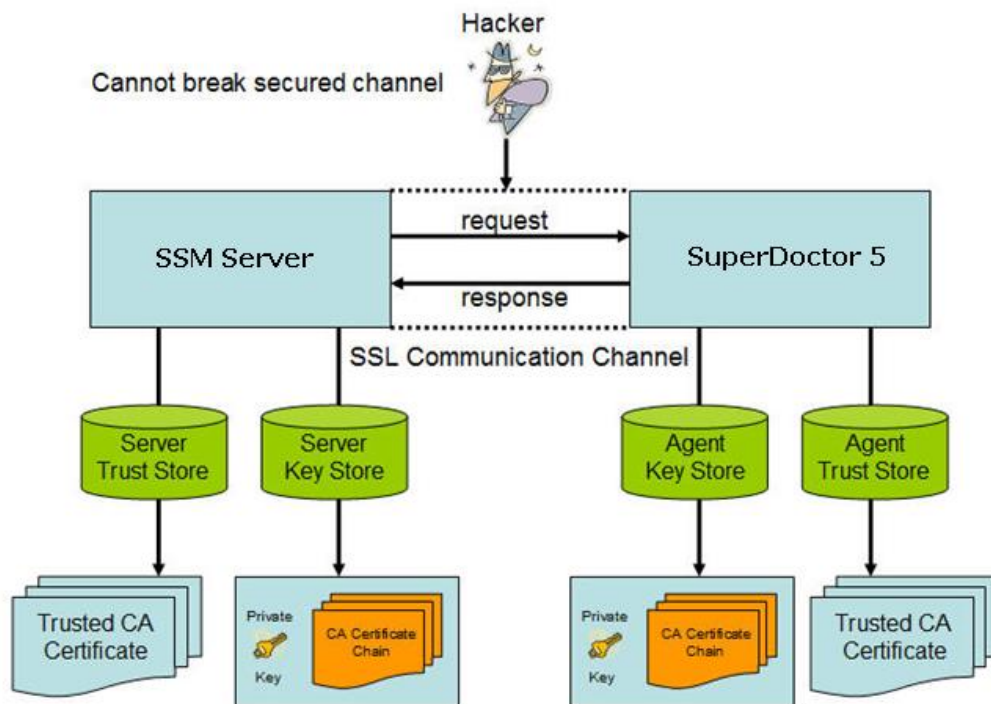


Figure 16-2

As shown above, the SSM Server and SuperDoctor 5 use two key stores to preserve their key pairs and the trusted client's public keys, respectively (Note that the SSM Server, SSM Web, and SSM CLI use the same Server Trust Store and Server Key Store to establish secure communication channels with the SuperDoctor 5.) For the SSM Server, the Server Key Store contains an SSM Server private key. For the SuperDoctor 5, the Agent Key Store contains a SuperDoctor 5 private key. The Agent Trust Store

contains SSM Server public keys. To ensure secure communications, the SSM Server uses the SuperDoctor 5's public key to encipher messages and sends the enciphered messages to the SuperDoctor 5. The enciphered messages can only be deciphered with the SuperDoctor 5's private key, which is safely kept by the SuperDoctor 5. When the SuperDoctor 5 sends messages back to the SSM Server, it uses the SSM Server's public key to encipher the messages that are then deciphered by the SSM Server with its own private key. Even if the messages are sniffed by hackers, they cannot understand the enciphered messages.

16.2 Installing an SSM Certificate

16.2.1 Windows Graphic Mode

1. Log in to Windows as an **administrator**.
2. Execute the **SSMCertificateInstaller.exe** program.



Note: An individual SSM Certificate installation program is available for x86 and amd64 platforms.

3. Click the **Next** button to continue.

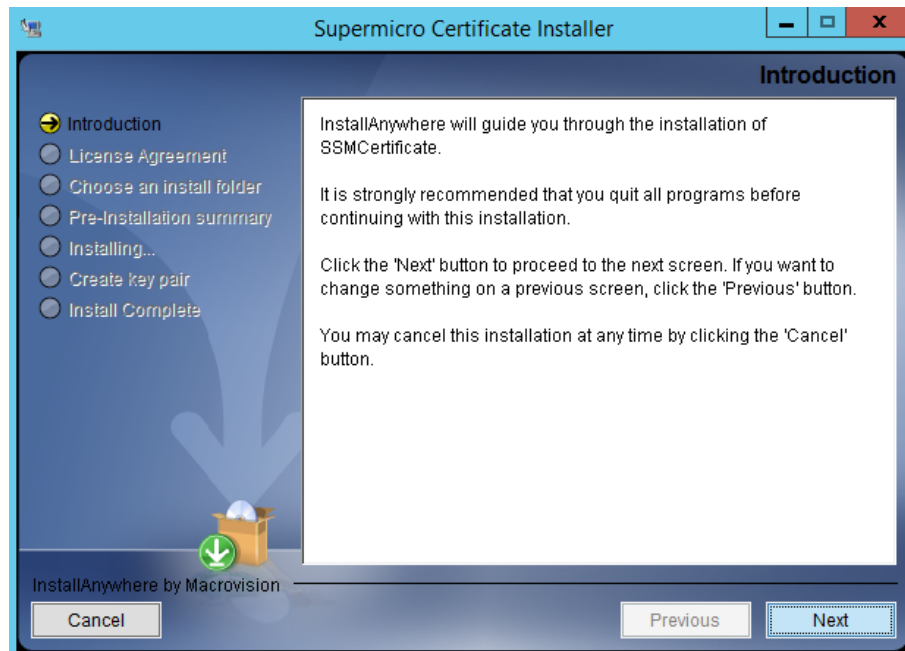


Figure 16-3

- Accept the copyright and click the **Next** button to continue.

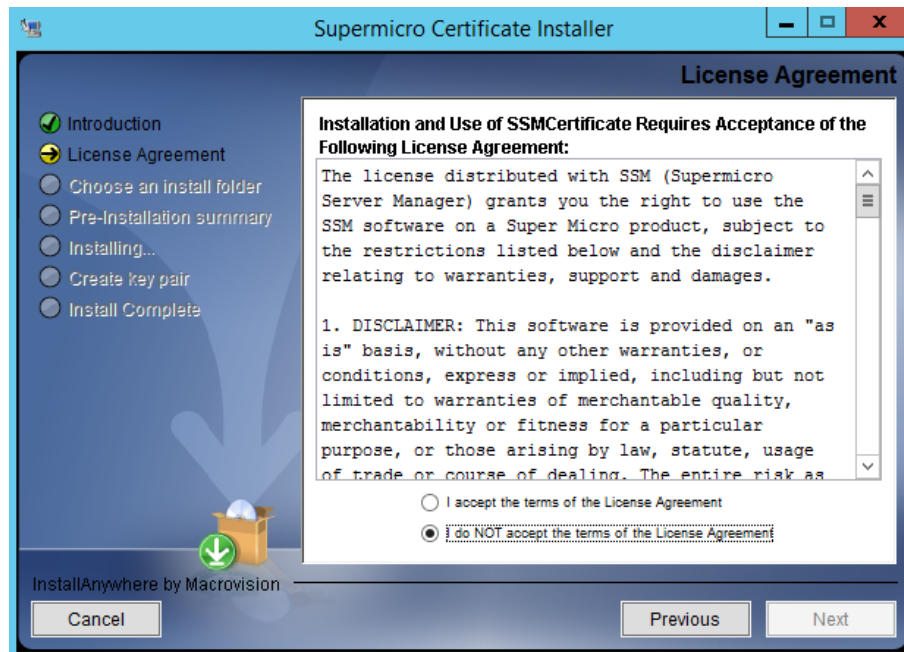


Figure 16-4

- Choose an installation folder. The default folder is **C:\Program Files\Supermicro\SSMCertificate**.

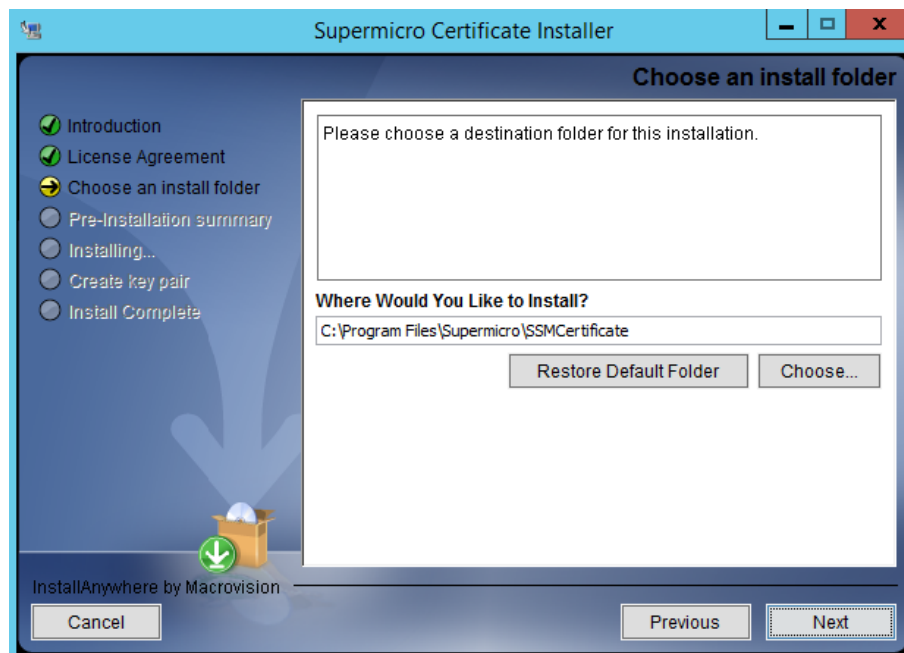


Figure 16-5

6. The figure shown below is the pre-installation summary. Click the **Install** button to install the program.

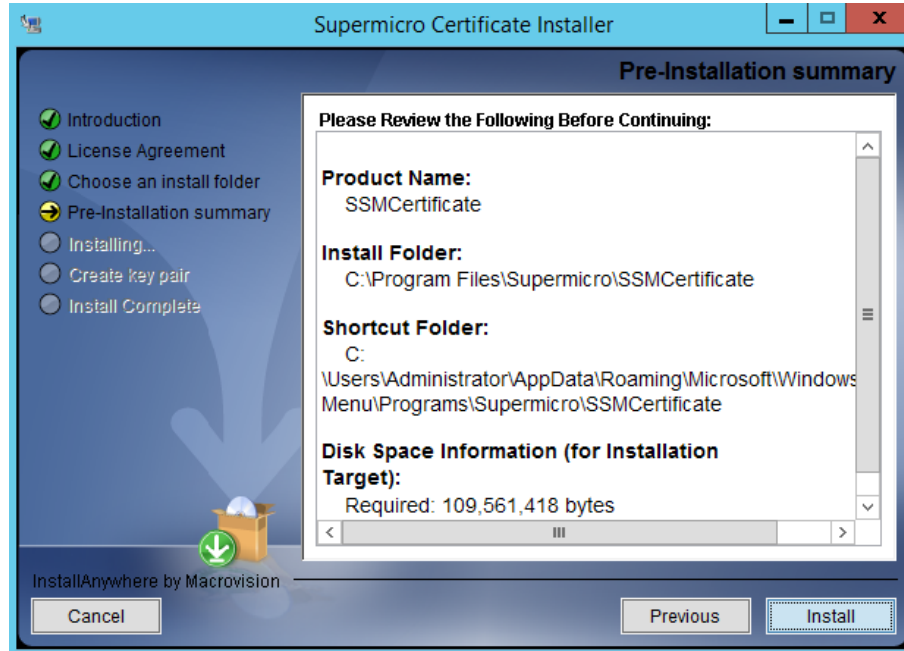


Figure 16-6

7. Please wait while the installation is in progress.

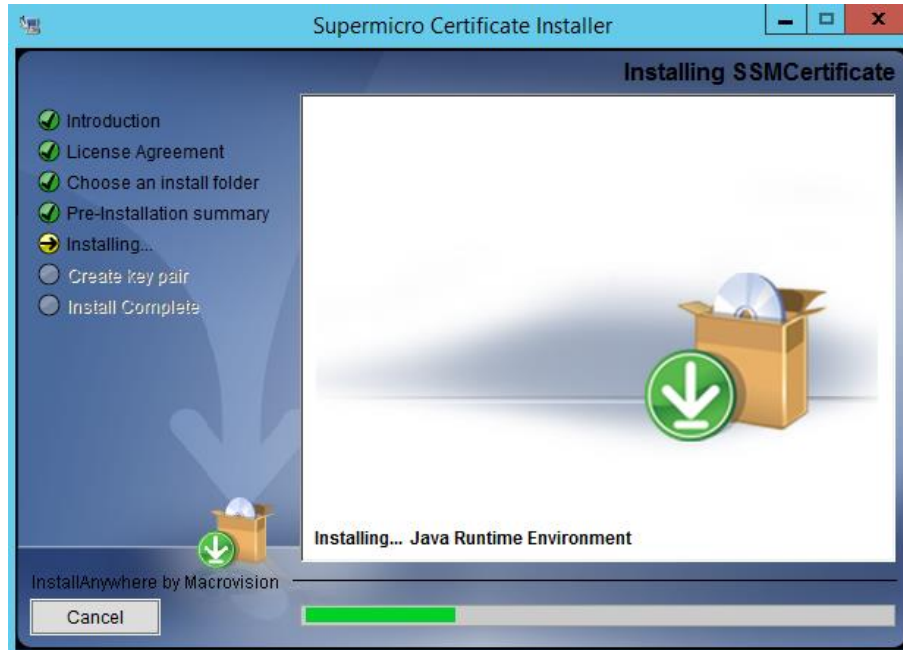


Figure 16-7

- To generate new key pairs right away, choose the **Yes** radio button and click the **Next** button to continue. You can generate key pairs later by executing the **ssmkeytool** program.

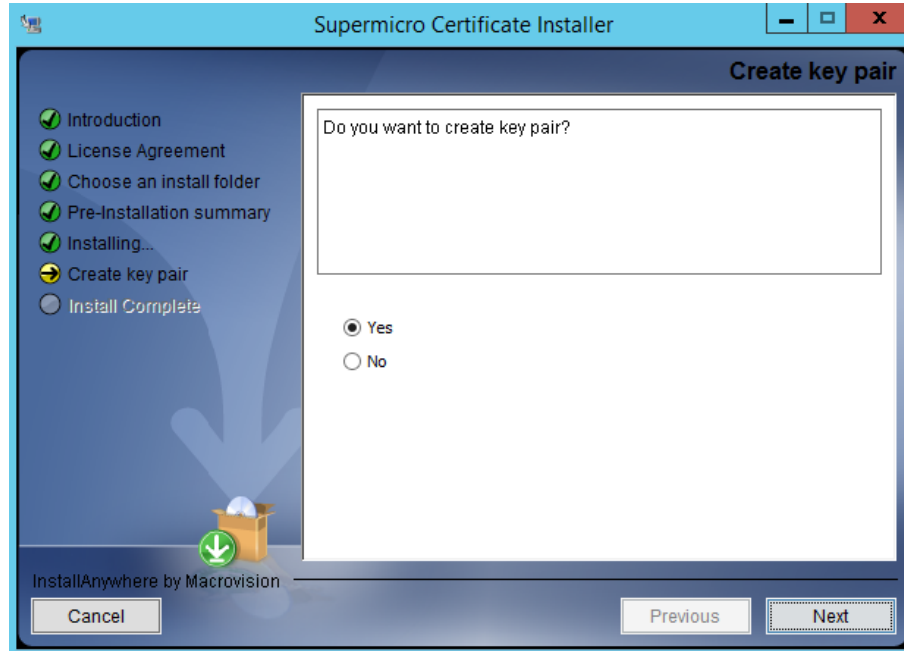


Figure 16-8

- The installation is complete. Click the **Done** button to close the installation program.

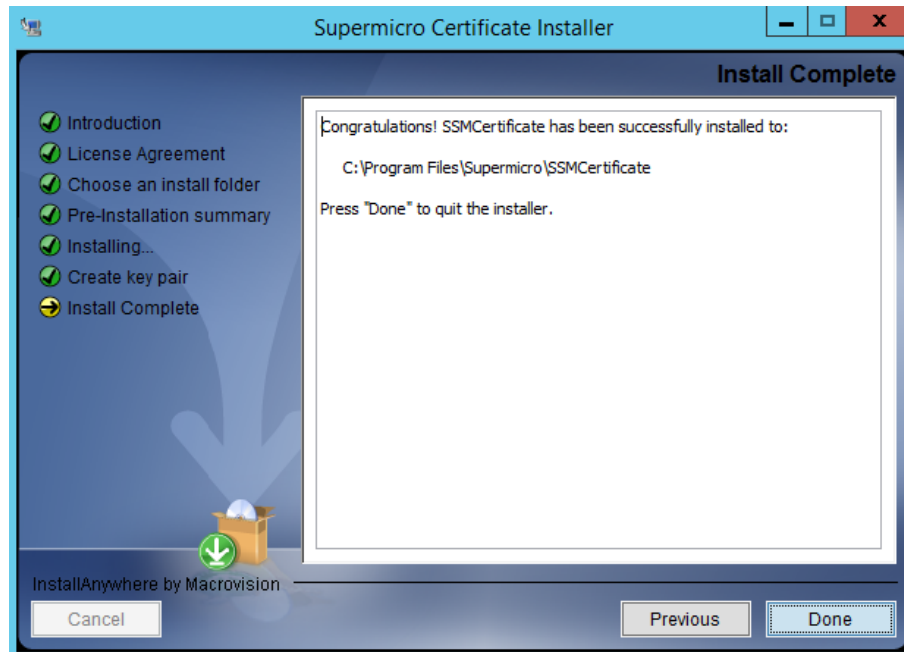


Figure 16-9



Note: The generated key pairs in step 8 are stored in the [install folder]\SSMCertificate\certificates folder.

16.2.2 Linux Text Mode

The installation steps are similar to the steps in the Windows graphic mode. See 16.2.1 *Windows Graphic Mode* for detailed information.

16.3 Generating a Certification

SSM Certificate provides a text mode tool that can be used to generate key pairs. The tool is located in the SSM Certificate application folder. Windows users should use **ssmkeytool.bat** and Linux users should use **ssmkeytool.sh**.

16.3.1 Help Information

Executing the **ssmkeytool** command without any argument or with the **-h** argument will display a help menu as shown below.

```
Administrator: Command Prompt
C:\Program Files\Supermicro\SSMCertificate>ssmkeytool.bat -h
usage: ssmkeytool [-ap <arg>] [-c [-d <arg>]] [-h]
-ap,--agentpwd <arg> Set password for Agent
-c,--create Create keystore for Server and Agent
-d,--directory <arg> Output Directory
-h,--help Help
C:\Program Files\Supermicro\SSMCertificate>
```

Figure 16-10

16.3.2 Generating key pairs for SSM Server and SD5

Executing the **ssmkeytool -c** command creates key pairs for the SSM Server and SuperDoctor 5. The generated key pairs are located in the [install folder]\SSMCertificate\certificates folder.

In the **certificates** folder, you can find **Server** and **Agent** subfolders containing the following files:

In the [install folder]\SSMCertificate\certificates\Server\ folder:

1. **jchecknrpe.auth**: This is the Server key store containing an SSM Server's private key.
2. **jchecknrpe.trust**: This is the Server trust store containing a SuperDoctor 5's public key.

In the [install folder]\SSMCertificate\certificates\Agent\ folder:

1. **agent.auth**: This is the Agent key store containing a SuperDoctor 5's private key.
2. **agent.trust**: This is the Agent trust store containing an SSM Server's public key.

When you install SSM (SSM Server, SSM Web, and/or SSM CLI) and choose to use a user-defined key pair, please import the **jchecknrpe.auth** and **jchecknrpe.trust** files generated in the [install folder]\

SSMCertificate\certificates\Server folder. Use the **agent.auth** and **agent.trust** files when you install a SuperDoctor 5 and choose to use a user-defined key pair.

Executing the **ssmkeytool -c -d [output directory]** command generates key pairs in the specified folder.



Note: Every time you execute **ssmkeytool**, new key pairs are generated (i.e., the four files **jchecknrpe.auth**, **jchecknrpe.trust**, **agent.auth**, and **agent.trust**). The four files generated at the same time must be used together, otherwise an SSL channel cannot be established when the SSM Server communicates with the SuperDoctor 5.

16.3.3 Overwriting Default Password for SD5

You can create key pairs with customized password by running this command:

ssmkeytool -c -ap [password]

For more information on how to use the customized certification when installing SSM, see *16.4 Using Customized Certification when Installing SSM*.

16.4 Using Customized Certification when Installing SSM and SD5

16.4.1 Windows

1. In the **Setup a key store** step, click the **No** radio button and click the **Next** button to continue.

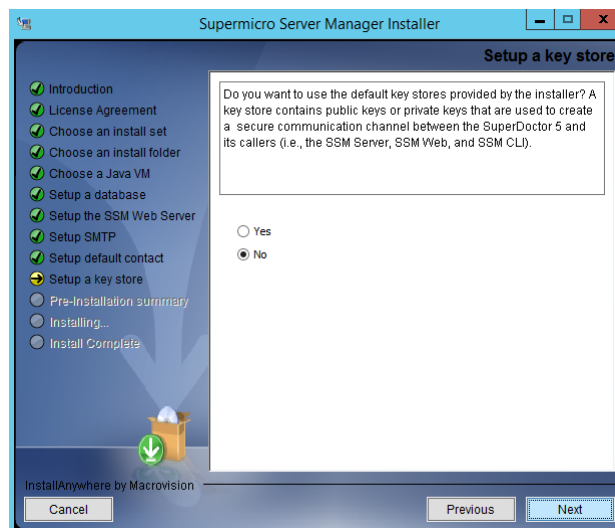


Figure 16-11

2. Provide a new SSM Server private key store (the **jchecknrpe.auth** file) and a new SSM Server public key store (the **jchecknrpe.trust** file). For SuperDoctor 5 installer, provide SuperDoctor 5 private and public key stores (the **agent.auth** and the **agent.trust** files) in the similar step.

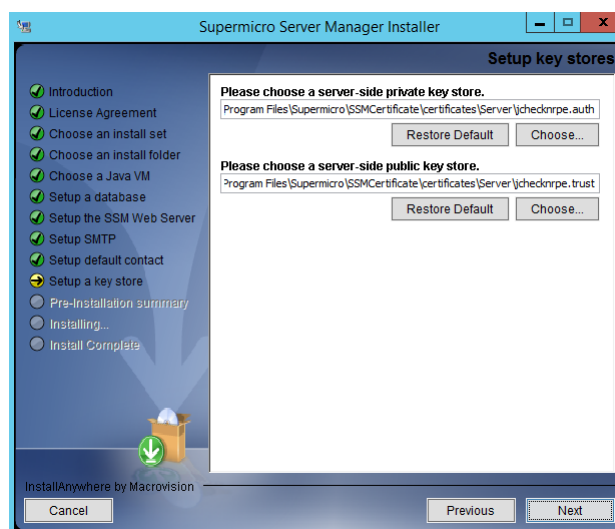


Figure 16-12

3. For SuperDoctor 5 installer, Click **Yes** and then click **Next** to continue above step. Or if you have customized password while using `ssmkeytool -ap` option, you can click **No** and provide the same password in `ssmkeytool -ap` option to continue. See *16.3.3 Overwriting Default Password for SD5* for more information.

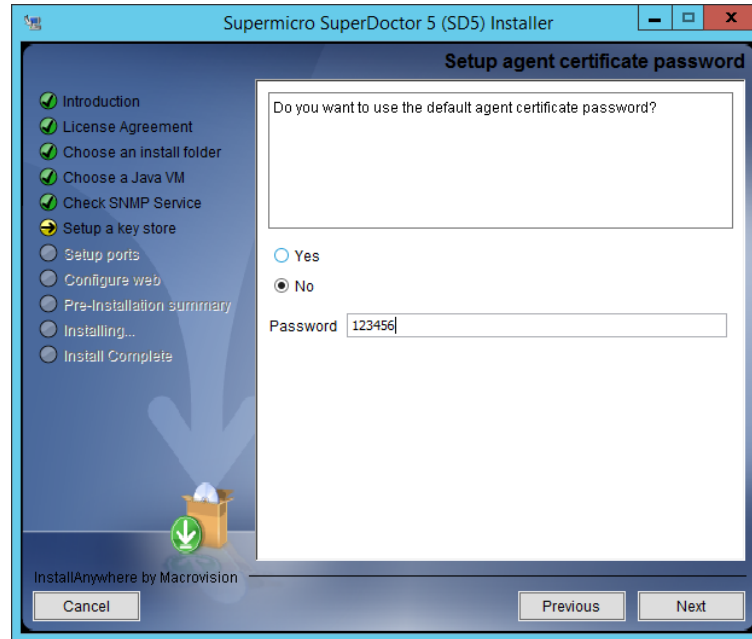


Figure 16-13

4. Please follow user's guide to complete the SSM and SuperDoctor 5 installation.

16.4.2 Linux

1. In the **Setup a key store** step, choose **No** (type 2) and press the **<Enter>** key to continue.

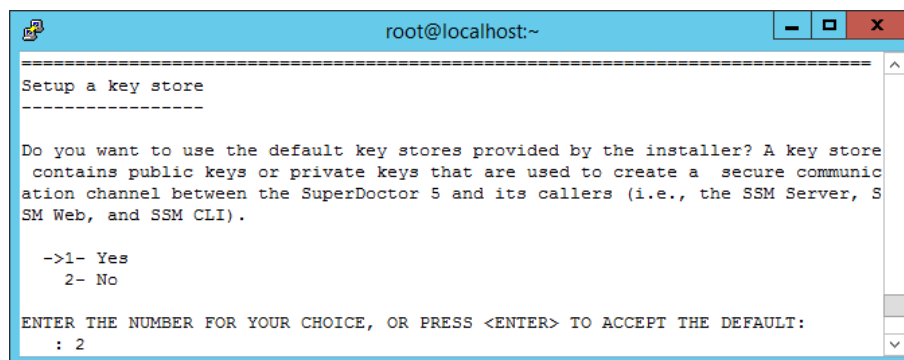


Figure 16-14

2. Provide a new SSM Server private key store (the **jchecknrpe.auth** file) and a new SSM Server public key store (the **jchecknrpe.trust** file). For SuperDoctor 5 installer, provide SuperDoctor 5 private and public key stores (the **agent.auth** and the **agent.trust** files) in the similar step.

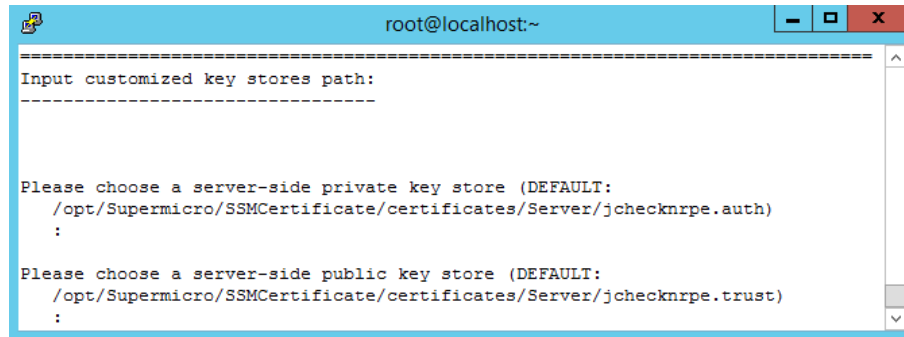


Figure 16-15

For SuperDoctor 5 installer, Choose **Yes** (type 1), and press **<Enter>**. Or, if you have the customized password while using `ssmkeytool -ap` option, click **No** (type 2) and provide the same password in `ssmkeytool -ap` option to continue. See *16.3.3 Overwriting Default Password for SD5* for more information.

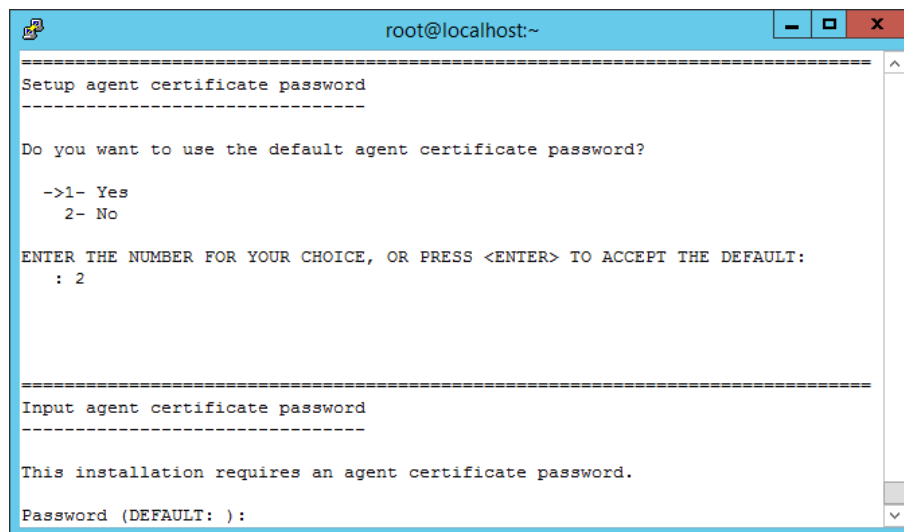


Figure 16-16

3. Please follow user's guide to complete the SSM and SuperDoctor 5 installation.

16.5 Manually Replacing SSM Server Certification

You can manually replace the default key pairs after installing SSM Server. The SSM Server key pairs, **jchecknrpe.auth** and **jchecknrpe.trust**, are located in the **[install folder]\shared\jcheck_nrpe\certificates** folder. Please use the **ssmkeytool** program to generate new key pairs and copy the generated **jchecknrpe.auth** and **jchecknrpe.trust** files in the **\certificates\Server** folder to the **[install folder]\shared\jcheck_nrpe\certificates** folder to overwrite the default key pairs.



Note: You need to restart SSM Server after replacing certifications if SSM Server has been running.

16.6 Manually Replacing the SD5 Certification

You can manually replace the default key pairs after installing SuperDoctor 5. The SuperDoctor 5 key pairs, **agent.auth** and **agent.trust**, are located in the **[install folder]\SuperDoctor5\certificates** folder. Please copy the **ssmkeytool** generated **agent.auth** and **agent.trust** files in the **\certificates\Agent** folder to the **[install folder]\SuperDoctor5\certificates** folder to overwrite the default key pairs.



Note: You need to restart SuperDoctor 5 after replacing certifications if SuperDoctor 5 has been running.

Part 6 Appendices

A. Log Settings

SSM Server and SSM Web use a log file to record runtime information and errors. By default, each SSM module backs up 10 copies of the log file when it reaches a maximum size of 8 MB. For instance, backup files are named `ssmsserver.log.1`, `ssmsserver.log.2`, `ssmsserver.log.3` . . . `ssmsserver.log.10`. You can change the maximum log file size and maximum number of backup copies.

Configuring the log properties of SSM Server:

1. Stop the SSM Server Service. Please refer to 2.4.2 *SSM Server Service* for more information.
2. Find **log4j.properties** located in the `[install folder]\SSMServer\config` folder and open it with a text editor.
3. Find the content that contains the following line:
log4j.appender.SSMSERVER_LOGFILE.MaxFileSize=8000KB
Modify the word 8000KB to an appropriate value. Allowable unit sizes are KB, MB and GB. This line may be commented out if no file size constraint is to be applied.
4. Find the content that contains the following line:
log4j.appender.WEB_LOGFILE.MaxBackupIndex=10
Modify the keyword **10** to an appropriate value.
5. Save the file and restart the SSM Server service.

Configuring the log properties of SSM CLI:

1. Find **log4j.properties** located in the `[install folder]\SSMCLI` folder and open it with a text editor.
2. Find the content that contains the following line:
log4j.appender.fileAppender.MaxFileSize=8000KB
Modify the word 8000KB to an appropriate value. Allowable units are KB, MB and GB. This line may be commented out if no file size constraint is to be applied.
3. Find the content that contains the following line:
log4j.appender.fileAppender.MaxBackupIndex=10
Modify the keyword **10** to an appropriate value.
4. Save the file.

Configuring the log properties of SSM Web:

1. Stop the SSM Web Service. Please refer to 2.4.3 *SSM Web Service* for more information.
2. Find **log4j.properties** located in `[install folder]\SSMWeb\config` folder and open it with a text editor.
3. Find the content that contains the following line:
log4j.appender.WEB_LOGFILE.MaxFileSize=8000KB

Modify the word 8000KB to an appropriate value. Allowable units are KB, MB and GB. This line may be commented out if no file size constraint is to be applied.

4. Find the content that contains the following line:
log4j.appender.WEB_LOGFILE.MaxBackupIndex=10
Modify the keyword **10** to an appropriate value.
5. Save the file and restart the SSM Web service.

Configure log properties of jcheck_nrpe:

1. Find **log4j.properties** located in **[install folder]\shared\jcheck_nrpe** and open it with a text editor.
2. Find the content that contains the following line:
log4j.appender.LOGFILE.MaxFileSize=8000KB

Modify the word 8000KB to an appropriate value. Allowable units are KB, MB and GB. This line may be commented out if no file size constraint is to be applied.

3. Find the content that contains the following line: **log4j.appender.LOGFILE.MaxBackupIndex=10**
Modify the keyword **10** to an appropriate value.
4. Save the file.

B. Third-Party Software

The following open source libraries are used by SSM:

Library	License	SSM Server	SSM Web	SSM CLI
Antlr	BSD	X	X	X
aopalliance	Public Domain	X	X	X
apache-mime4j	Apache License	X	X	X
Apache commons	Apache License	X	X	X
asm	BSD		X	
AspectJ weaver	Eclipse Public License		X	
Aspectjrt	Eclipse Public License		X	
Camel	Apache License	X	X	
cdi-api	Apache License	X	X	X
cglib	Apache License		X	
classindex	Apache License	X	X	X
dom4j	BSD	X	X	X
Ehcache-core	Apache License	X	X	X
evo-inflector	Apache License		X	
google-guice	Apache License	X	X	X
gson	Apache License	X	X	X
guava	Apache License	X	X	X
Hibernate	LGPL	X	X	X
httpClient	Apache License	X	X	X

httpcore	Apache License	X	X	X
Jackson	Apache License	X	X	✗
jandex	Apache License	X	X	X
Java Native Access	LGPL			
JavaMail (mail.jar)	CDDL	X	X	X
javassist	Apache 2.0, LGPL 2.1, Mozilla Public License 1.1	X	X	X
javax.annotation-api	GPL, CDDL	X	X	X
javax.ejb-api	GPL, CDDL	X	X	X
javax.el-api	GPL, CDDL	X	X	X
javax.inject	Apache License	X	X	X
javax.interceptor-api	GPL, CDDL	X	X	X
javax.servlet-api	GPL, CDDL	X	X	
javax.transaction-api	GPL, CDDL	X	X	X
javax.websocket	GPL, CDDL		X	
javax.ws.rs-api	GPL, CDDL	X	X	X
jboss-annotations-api	GPL, CDDL	X	X	X
jboss-jaxrs-api	GPL, CDDL	X	X	X
jboss-logging	Apache License	X	X	X
jboss-servlet-api	GPL, CDDL	X	X	X
jboss-transaction-api	GPL, CDDL	X	X	X
jcl	Apache License	X	X	X
jcommon	LGPL		X	
jetty	Apache License, Eclipse		X	

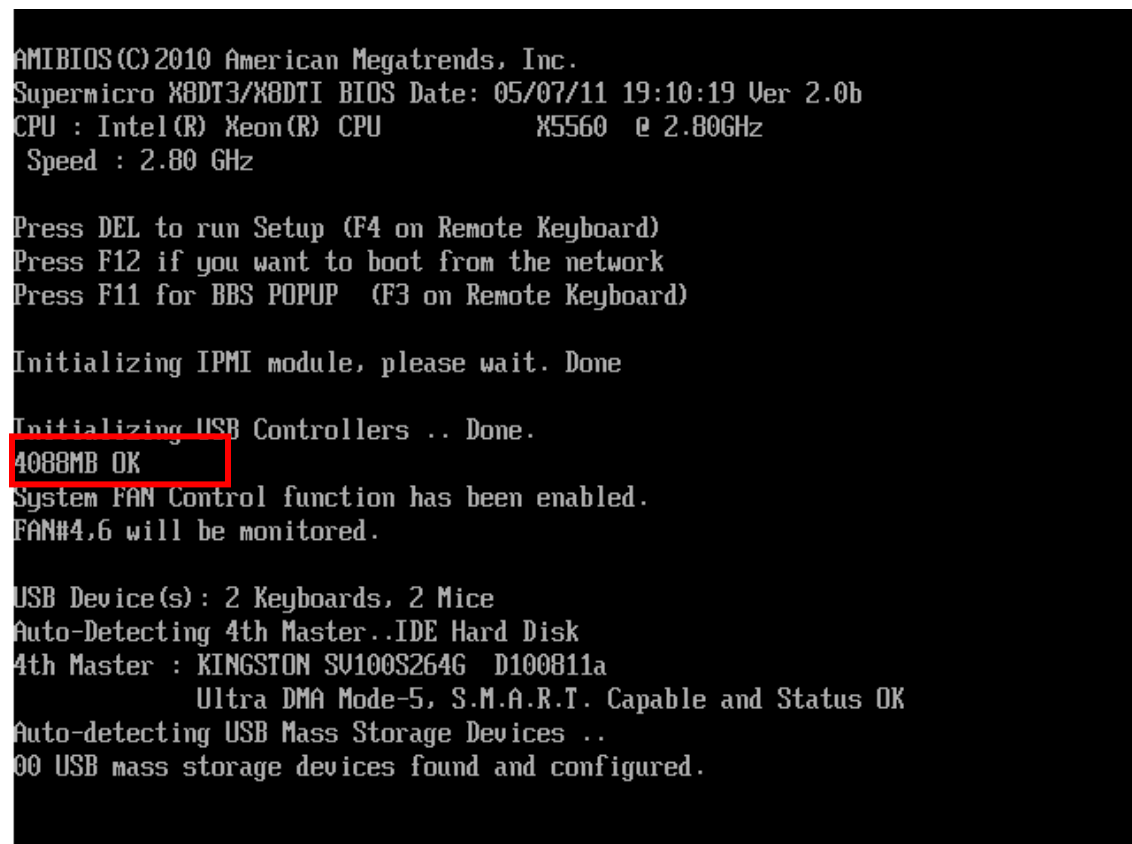
	Public License			
JFreeChart	LGPL		X	
jline	BSD			X
Jmdns	Apache License	X	X	
jna	Apache License, LGPL	X	X	X
Joda Time	Apache License		X	
jsmiparser	Apache License	X		
json-path	Apache License		X	
Log4J	Apache License	X	X	X
Netty	Apache License	X	X	
Postgresql jdbc driver	BSD	X	X	X
Quartz	Apache License	X		
reflections	BSD	X	X	X
resteasy	Apache License	X	X	X
SLF4J	MIT	X	X	X
SNMP4J	Apache License	X	X	
Spring framework	Apache License	X	X	X
stax2	BSD		X	
truelicense	Eclipse Public License	X	X	X
typetools	Apache License		X	
validation	Apache License		X	
websocket	Apache License, Eclipse Public License		X	
Wicket	Apache License		X	
WicketStuff Restannotations	Apache License		X	

woodstox	Apache License	X
xstream	BSD	X

C. Uncorrectable ECC Errors

A DIMM that has a UECC error should be regarded as unstable and may damage the entire system. In some hardware designs, a UECC error will cause a system reboot and the affected DIMM to be automatically disabled by the hardware. In such cases, SSM will not send you a UECC error since the DIMM does not exist anymore from SSM's perspective. However, if you use SSM to check the total number of DIMMs, you will be notified of a missing DIMM. The DIMM causing the UECC error can be re-enabled by power cycling.

For example, Supermicro X8DT3 and X8DTI motherboards implement the disabling function described above. The following screenshot shows a X8DT3 system with 4088 MB of RAM.



```
AMIBIOS (C) 2010 American Megatrends, Inc.  
Supermicro X8DT3/X8DTI BIOS Date: 05/07/11 19:10:19 Ver 2.0b  
CPU : Intel(R) Xeon(R) CPU           X5560 @ 2.80GHz  
Speed : 2.80 GHz  
  
Press DEL to run Setup (F4 on Remote Keyboard)  
Press F12 if you want to boot from the network  
Press F11 for BBS POPUP (F3 on Remote Keyboard)  
  
Initializing IPMI module, please wait. Done  
  
Initializing USB Controllers .. Done.  
4088MB OK  
System FAN Control function has been enabled.  
FAN#4,6 will be monitored.  
  
USB Device(s): 2 Keyboards, 2 Mice  
Auto-Detecting 4th Master..IDE Hard Disk  
4th Master : KINGSTON SU100S264G D100811a  
Ultra DMA Mode-5, S.M.A.R.T. Capable and Status OK  
Auto-detecting USB Mass Storage Devices ..  
00 USB mass storage devices found and configured.
```

Figure C-1

The total memory is 4088MB.

As shown in the following screenshot, CPU01/DIMM1A caused a UECC error and the DIMM was automatically disabled by the hardware. As a result, the total memory changed from 4088MB to 2040MB.

```
CPU : Intel(R) Xeon(R) CPU           X5560 @ 2.80GHz
Speed : 2.80 GHz

Entering SETUP...
Press F12 if you want to boot from the network
Press F11 for BBS POPUP (F3 on Remote Keyboard)

Initializing IPMI module, please wait. Done

Initializing USB Controllers .. Done.
2040MB OK
System FAN Control function has been enabled.
FAN#4,6 will be monitored.

USB Device(s) : 2 Keyboards, 2 Mice, 1 Storage Device
Auto-Detecting 4th Master..IDE Hard Disk
4th Master : KINGSTON SU100S264G D100B11a
                Ultra DMA Mode-5, S.M.A.R.T. Capable and Status OK
Auto-detecting USB Mass Storage Devices ..
Device #01 : USB Flash Disk *HiSpeed*
01 USB mass storage devices found and configured.

Un-Correctable DRAM ECC Error Detected at CPU01/DIMM1A
Press F1 to Resume
```

Figure C-2

The total memory becomes 2040MB since CPU01/DIMM1A was disabled.



Note: The above behavior is hardware-dependent and is only applicable to Intel platforms.



Contacting Supermicro

Headquarters

Address: Super Micro Computer, Inc.
980 Rock Ave.
San Jose, CA 95131 U.S.A.

Tel: +1 (408) 503-8000
Fax: +1 (408) 503-8008
Email: marketing@supermicro.com (General Information)
support@supermicro.com (Technical Support)

Website: www.supermicro.com

Europe

Address: Super Micro Computer B.V.
Het Sterrenbeeld 28, 5215 ML
's-Hertogenbosch, The Netherlands

Tel: +31 (0) 73-6400390
Fax: +31 (0) 73-6416525
Email: sales@supermicro.nl (General Information)
support@supermicro.nl (Technical Support)
rma@supermicro.nl (Customer Support)

Website: www.supermicro.nl

Asia-Pacific

Address: Super Micro Computer, Inc.
3F, No. 150, Jian 1st Rd.
Zhonghe Dist., New Taipei City 235
Taiwan (R.O.C)

Tel: +886-(2) 8226-3990
Fax: +886-(2) 8226-3992
Email: support@supermicro.com.tw

Website: www.supermicro.com.tw