Supermicro Server Manager

User's Guide

Revision 2.2

Manual Revision: 2.2
Release Date: 6/2/2023

Revision History

Date	Rev	Description
Sep-10-2014	1.0	1. Initial document.
Dec-12-2014	1.0a	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	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	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	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	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	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	1. Added limitations for ChangeJVM utility. 2. Changed some figures.
Dec-11-2015	1.3	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	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	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	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	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	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	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	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	1. Replaced SFT-OOB-LIC Activation with Node PK Activation.
Jun-22-2017	1.6e	1. Changed TPM 1.2 module to TPM module.
Aug-3-2017	1.7	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	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	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	1.	Removed the “Apply SystemInfo Data” button.
		2.	Changed the scenario for “Change Arguments” of “IPMI SEL Health.”
Dec-11-2017	1.7d	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	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	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	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	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.

		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	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	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	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.
Feb-5-2020	2.0a	1. Changed some figures. 2. Added a note for the method of using web browsers to connect to the IPv6 hosts. 3. Changed the location for the logs of SSM Installer. 4. Changed mymacs.txt to SSM_mymacs.txt.
May-25-2020	2.0b	1. Removed the SSM CLI program. 2. Changed the screenshots of the SSM installer. 3. Enhanced "E-Mail SMTP Setup" page for users to view and install their own certificates for SMTP server.

		4. Added commands for CMM_IPMI hosts. 5. Changed answer files for OS Deployment. 6. Enhanced the table of default TCP/UDP ports. 7. Changed SFT-DCMS-Single to SFT-DCMS-SINGLE.
Oct-13-2020	2.0c	1. Added HOSTLOCATION and HOSTNOTES to the pre-defined macros. 2. Added MH_SYS_SERIAL, MH_SYS_MODEL, MH_BMC_VER, and MH_BIOS_VER to the pre-defined macros. 3. Fixed typo in macros chapter.
Dec-2-2020	2.0d	1. Changed system requirements. 2. Added more redfish commands. 3. Added support for downloading troubleshooting logs in the "About SSM" section. 4. Modified the system information chapters. 5. Modified the service calls chapters. 6. Updated the 3rd party software. 7. Modified matrix in user roles chapter. 8. Refined the attributes used in template answer file for SLES.
Apr-19-2021	2.1	1. Changed system requirements and architecture. 2. Added more IPMI and redfish commands for RoT management. 3. Modified the supported types of System Information. 4. Modified matrix in user roles chapter. 5. Modified service properties chapter. 6. Modified OS Deployment chapter. 7. Added an appendix about the supported platforms of redfish command and IPMI command.
Nov-17-2021	2.1a	1. Modified OS supports for the OS Deployment function. 2. Added scheduled task chapter. 3. Modified a table in Appendix B. 4. Renamed "BMC Log" to "BMC SEL" in the command area. 5. Removed the support for IPMI/Redfish Sensor Health service. 6. Moved the SUM Integration chapter to the IPMI Commands and Updating SUM chapters. 7. Added new chapters for FW Notification, System Information Report and Component Health. 8. Modified *Chapter 2 Setting Up SSM*. 9. Removed a screenshot in *6.14 About SSM*.

Apr-19-2022	2.1b	1. Changed system requirements. 2. Modified OS support for the OS Deployment function. 3. Added the SSM Web certificate chapter. 4. Added the Memory PFA chapter. 5. Modified Appendices B and D. 6. Modified the method to install in silent mode. 7. Modified the DB Maintenance chapter. 8. Modified the Add Service Wizard chapter. 9. Added a note to the downloaded images on FW Notification View. 10. Renamed the "Update BIOS" command to "Update BIOS (Capsule) ". 11. Added the description of "Update On Next Boot" to the Update BIOS function. 12. Removed the support for software product key and ssmlicense tool.
Nov-1-2022	2.1c	1. Added Load Factory BIOS Setting to the Redfish commands. 2. Added prerequisites and examples to the AD/LDAP chapter. 3. Modified Appendices A, B, and D. 4. Changed Detect IPMI to Detect Redfish in the Discovery Argument step of the Host Discovery Wizard. 5. Changed the word e-mail to email. 6. Modified the FW Notification chapter. 7. Added commands to CMM_Redfish hosts. 8. Modified the service calls chapters. 9. Fixed typos in the innoutconfig chapter.
Jan-4-2023	2.1d	1. Added support for domain-controlled AD/LDAP servers and modified the Directory Services chapter. 2. Added Load Factory CMM Setting to the CMM_Redfish commands. 3. Added the action log chapter. 4. Changed system requirements. 5. Added support for CDU system to be monitored. 6. Added support for FW auto update on FW Notification View.
June-2-2023	2.2	1. Modified matrix in user roles chapter. 2. Modified Redfish commands chapter. 3. Added the task history chapter. 4. Modified Appendix B.

5. Removed support for VNC.
6. Modified OS support for the OS Deployment function and removed the support for legacy boot mode.
7. Changed built-in JRE to 11.0.19.
8. Added section on new support for MCU Capsule in the FW Notification chapter.
9. Added support for CMM-6 systems.
10. Removed Sync Node PK from the CMM_Redfish and CMM_IPMI commands.

Contents

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 Redfish[1] management.
- Power management via the Intel® Intelligent Power Node Manager (NM).
- BIOS and BMC firmware management via the Supermicro Update Manager (SUM) and Redfish.
- Easy to use Web-based interface and REST API[2].
- 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 installation of Linux OS (RHEL, Ubuntu, CentOS, SLES, Rocky Linux and VMware ESXi) on the managed systems.
- Manages Blade servers through CMM.
- Edits DMI (SMBIOS) information.
- Diagnoses managed systems and receives progress and results on the SSM Web.

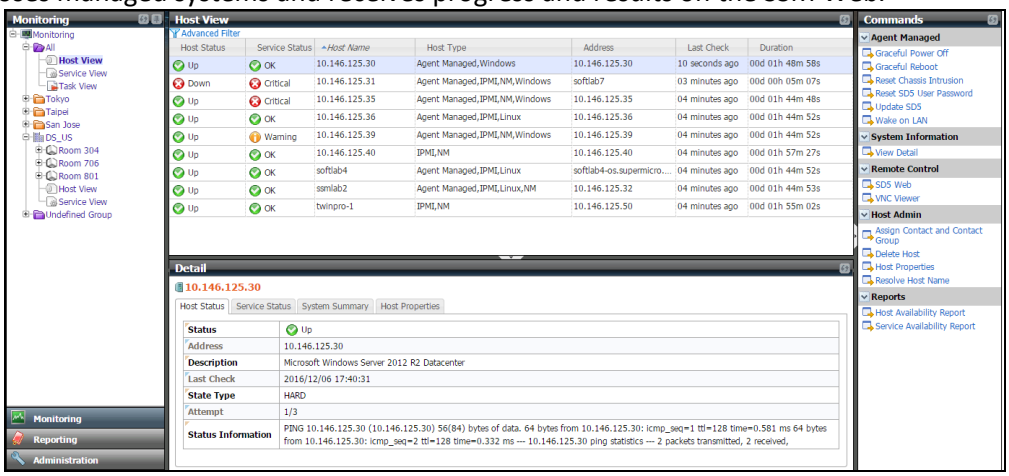


Figure 1-1: SSM Web-based Console

[1]In 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.

[2] To 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*).

1.2 Monitoring Functions

- Host Monitoring: Agent Managed, Agentless (Coolant Distribution Unit; CDU included), IPMI (CMM_IPMI included), and Redfish (CMM_Redfish included) hosts.
- Hardware Monitoring: fan speed, temperature, voltage, chassis intrusion, redundant power failure, power consumption, disk health, RAID health, memory health, and CDU health.
- Software Monitoring: HTTP, FTP, and SMTP services.
- State Control: Supports hard state and soft state to avoid false alarms.

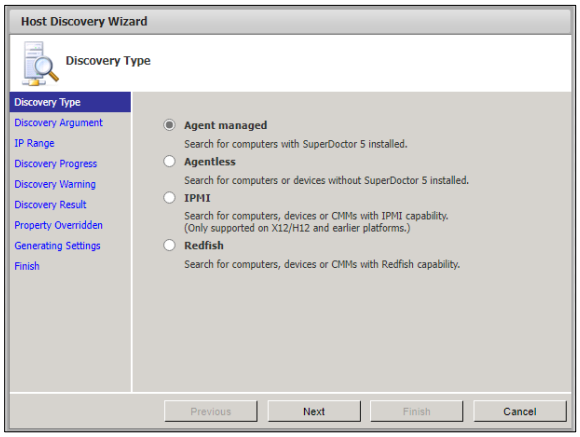


Figure 1-2: Host Discovery Wizard guides users on how to add hosts to be monitored

1.3 Control Functions

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

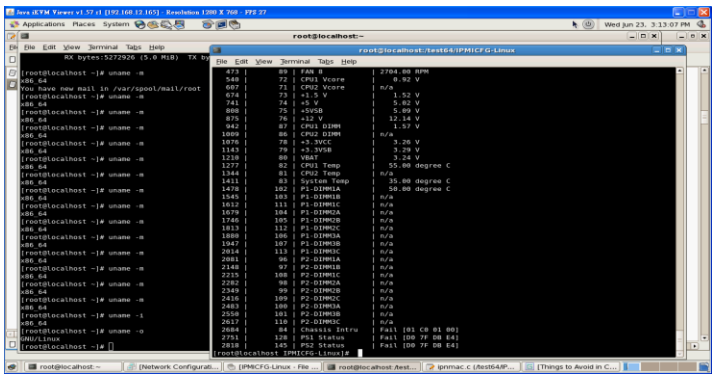


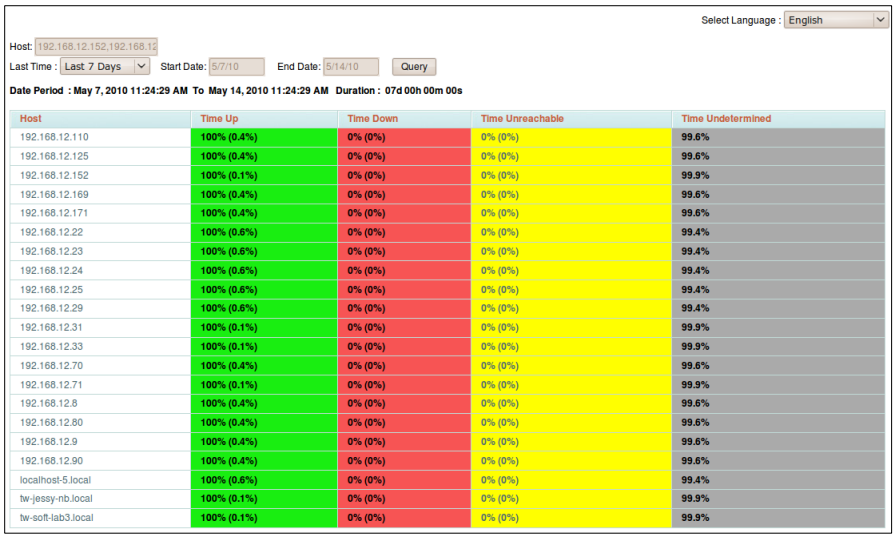
Figure 1-3: Remote Troubleshooting with iKVM via BMC Web

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, SNMP trap, or custom script.
- Notifications sent to contacts and contact groups.

1.5 System Information and Report Functions

- 20 Types of System Information[3]: 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.



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%
tw-jessy-nb.local	100% (0.1%)	0% (0%)	0% (0%)	99.9%
tw-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:

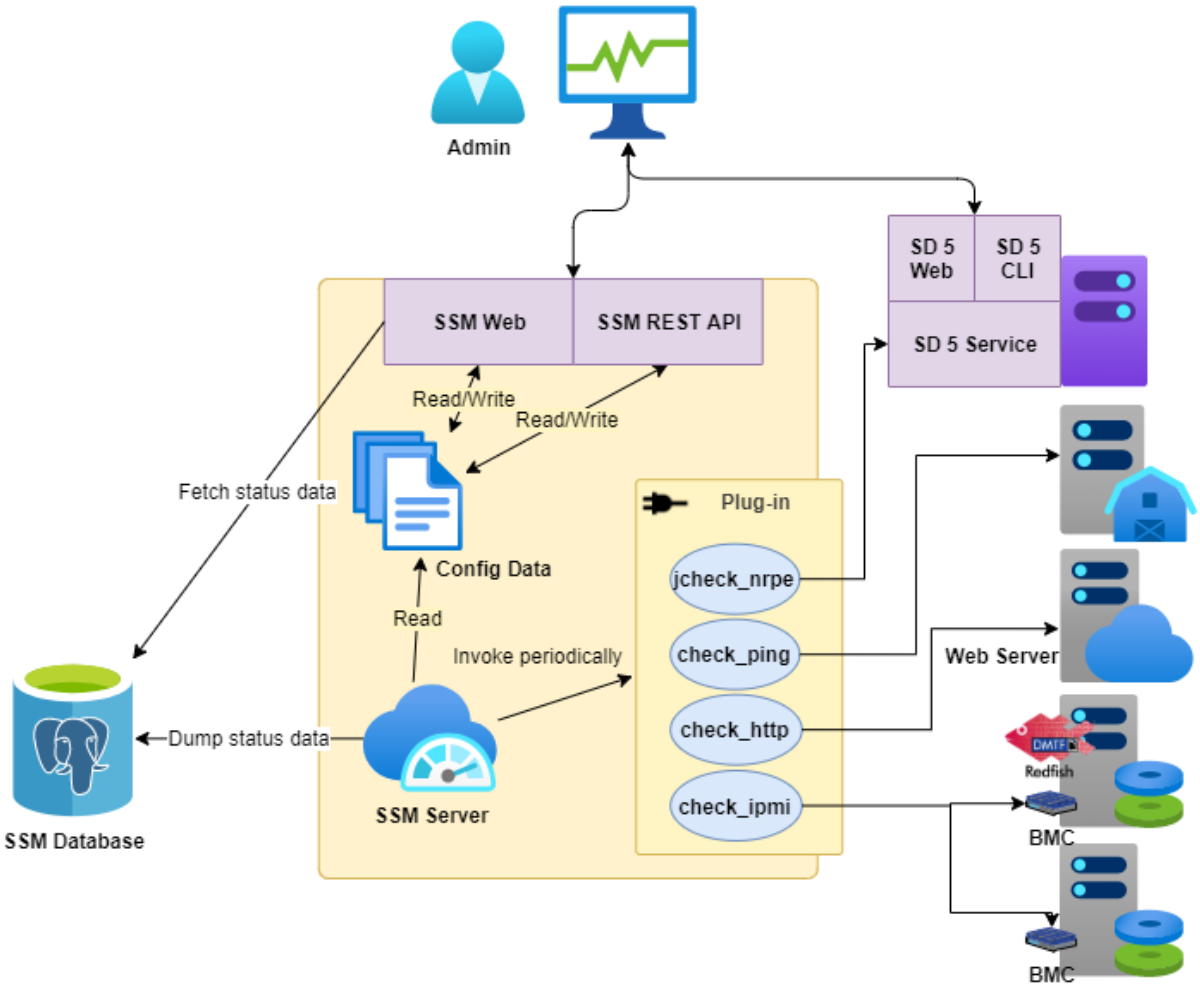


Figure 1-5: SSM System Architecture (Active Check)

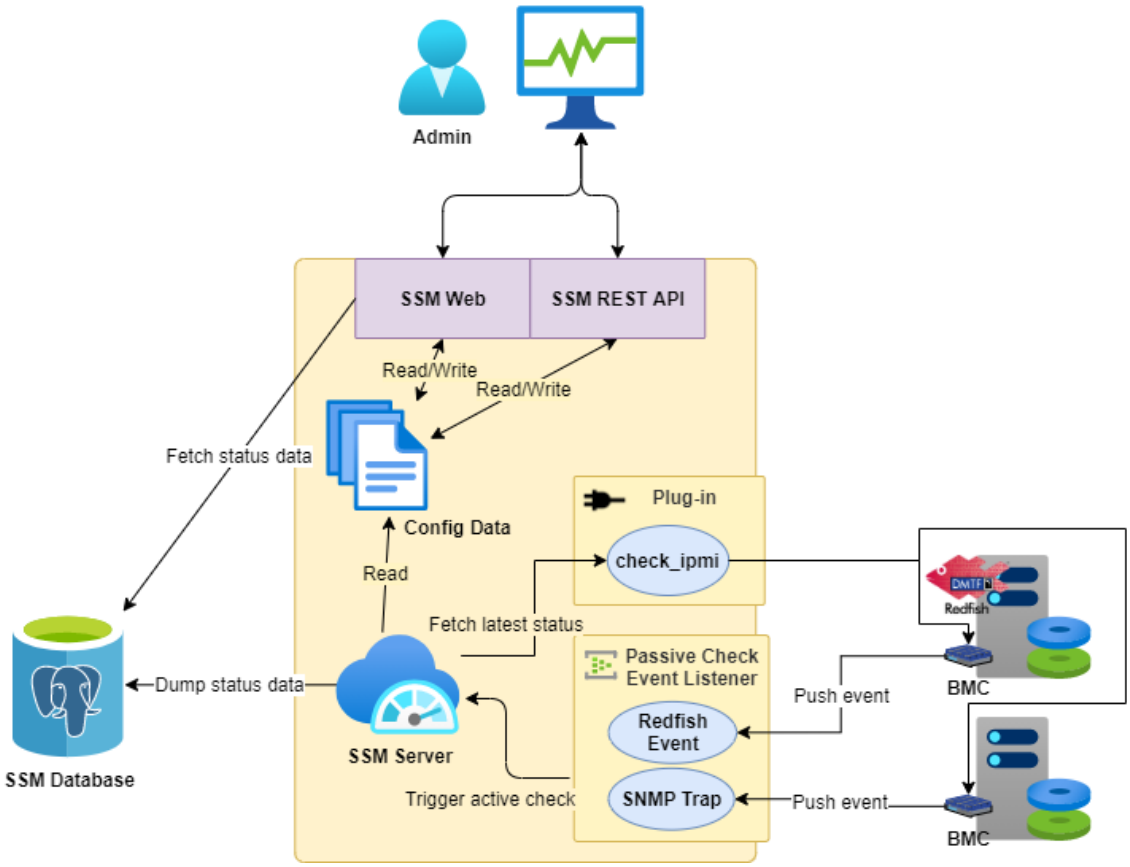


Figure 1-6: SSM System Architecture (Active Check and Passive Check)

- **SSM Server:** The SSM server is a service (a daemon) program that periodically monitors hosts and servers to check their status. It then updates the status to the SSM Database so that users can browse the information on the Web. In addition, it is able to receive SNMP traps and Redfish events sent by BMC, and then actively check BMC to reduce unnecessary active checks when BMC is not updated.
- **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 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 the data can be stored in the SSM Database and in plain text files.

1.7 System Requirements

1.7.1 Managing Up to 1,999 Hosts

1.7.1.1 SSM Server and SSM Web

- **Hardware**
  - 40.0 GB free disk space
  - 4 CPU cores
  - Available 16.0 GB RAM
  - An Ethernet network interface card

Notes:

- The system requirements must be met when SSM is used to monitor less than two thousand systems. To use SSM to monitor more than two thousand systems, please refer to *1.7.2 Managing for Over 2,000 Systems*.
- The free disk space depends on the number of OS images you will upload to SSM while using the OS deployment function.
- 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), 9.x (64-bit)
  - SUSE Linux Enterprise 12.x (64-bit), 15.x (64-bit)
  - Windows Server 2012 R2 64-bit
  - Windows Server 2016 64-bit
  - Windows Server 2019 64-bit
  - Windows Server 2022 64-bit
- **Browser**
  - Microsoft Edge 79.x or higher version
  - Firefox 68.x or higher version
  - Google Chrome 75.x or higher version
- **Screen resolution**
  - 1920 x 1080 or higher resolution

1.7.1.2 Managed System

- Any of Agent-Managed, IPMI, Redfish, or Agentless Host.

1.7.2 Managing for Over 2,000 Systems

To use SSM to monitor over 2,000 systems, make sure the following requirements for both SSM and the managed systems are met. Note that these requirements are necessary when the number of systems monitored by SSM ranges from two thousand to ten thousand.

1.7.2.1 SSM Server and SSM Web

- **Hardware**
  - 80.0 GB of free disk space
  - 12 CPU cores with Intel® Xeon® Processors or later
  - Available 32.0 GB RAM
  - An Ethernet network interface card

Note: To predict possible failures occurring on a large number of hosts, you should have at least 2 TB of free disk space to collect performance data with a sufficient data retention time.

- **Operating System**
  - Red Hat Enterprise Linux Server 7.x (64-bit), 8.x (64-bit), 9.x (64-bit)
  - SUSE Linux Enterprise 15.x (64-bit)
- **Browser**
  - Microsoft Edge 79.x or higher version
  - Firefox 68.x or higher version
  - Google Chrome 75.x or higher version
- **Screen resolution**
  - 1920 x 1080 or a higher resolution

1.7.2.2 Managed System

- **A Redfish Host is preferred.**

Note:
To manage a large number of hosts on one SSM system, you can use the passive check function for both IPMI and Redfish hosts so that a SNMP trap or Redfish event sent by BMC will be received and processed by SSM.

- The hosts added by the Host Discovery Wizard will be checked if they support the passive check function. If yes, the passive check attributes of the IPMI/Redfish SEL Health service will be set to be enabled; otherwise, those will be set as disabled.
- IPMI/Redfish SEL Health service of the hosts auto-upgraded by the SSM Installer could be set to have their passive check functions enabled all at once, see *7.3.8.1 Service Properties Command* for details.

1.7.3 Default TCP/UDP Ports

Port Number	Port Type	Direction	Description
8080	TCP	In/Out	This SSM Web listen port is used for HTTP protocol and internal communications with the SSM Server.
8443	TCP	In/Out	This SSM Web listen port is used for HTTPS protocol and internal communications with the SSM Server.
9002	TCP	In/Out	This port is used for SSM built-in database.
8555	TCP	In	This port is used to receive Redfish events from the BMC.
8556	TCP	In/Out	This port is used for SSM internal communications.
514	TCP, UDP	In	This port is used by SSM to receive the syslog when the OS deployment function is performed.
4444 and 5555	TCP	In/Out	This port is used to collect debug information when an OS deployment is performed.
25	TCP	Out	This port is used to access the SMTP server.
162	TCP	Out	This port is used to send an SNMP trap.
5333, 5666, 5999	TCP	Out	This port is used to communicate with SuperDoctor 5.
389	TCP	Out	This port is used for the LDAP/AD integration.
443	TCP	Out	This port is used for Redfish protocol and CDU communications over SSL.
623	UDP	Out	This port is used for IPMI protocol communications.

1.8 Types of Managed Systems

To discover a managed system, refer to *6.15 Host Discovery Wizard* for details. Alternatively, refer to *7.2.6 Scheduled Task Management* for details to discover IPMI hosts and Redfish hosts.

1.8.1 Agent-Managed Host

The managed system installed with SuperDoctor 5 (SD5) can provide information, including local system health. To install SD5, see *1.2 Minimum System Requirements* in *SuperDoctor 5 User's Guide* for details.

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 3108 controller (except when Windows driver version MR6.6 code is set or with higher versions) and later generations, such as 3908 and 3916. 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 available on Windows platforms.

When an agent-managed host is added, built-in services include:

- **Agent and its plug-ins versions**: Checks the health of a SuperDoctor 5 and displays 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.
- **Memory Health**: 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 the LSI MegaRAID 3108 controller (except when Windows driver MR6.6 code is set or with higher versions) and later generations, such as 3908 and 3916 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 details.

- **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.

1.8.2 IPMI Host

BMC or CMM with IPMI capability is able to communicate with SSM via IPMI protocol. To discover an IPMI host that is a managed system, it is required to activate the product key SFT-DCMS-SINGLE on the BMC first.

When an IPMI host is added, built-in services include:

- **IPMI SEL Health:** Checks the health of a host that 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 as a kind of internal mechanism. An event is automatically determined as a "Maintenance Window" in SEL when a component is replaced offline to avoid false alarms after a failed component has been repaired. After an "AC Power On" event occurs, and a "Chassis Intrusion" event occurs within an hour, this "Maintenance Window" event is determined. SSM will then verify the "Maintenance Window" event. 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.
- **IPMI System Information:** This service gathers system information via FRU, OOB Full SMBIOS, and Supermicro BMC Redfish API, and then stores them in the database. Meanwhile, the SSM also adds itself to the target BMC as an event subscriber. Besides the regular fetching frequency, SSM will then fetch system information immediately whenever BMC SEL changes. You can use the data to access system information on the SSM Web interface. If this service is added to an IPMI-managed host, the **View Details** command under the **System Information** category in the command area can be used.
- **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.

1.8.3 Redfish Host

A BMC or CMM with Redfish capability is able to communicate with SSM via Redfish protocol. To discover a Redfish host that is a managed system, the requirement below must be met.

- The managed system must have a BMC-equipped Supermicro X10 series motherboard or later.
- To access most Redfish functions, it is required to activate 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.

When a Redfish host is added, built-in services include:

- **Redfish SEL Health:** It is similar to IPMI SEL Health, but uses Redfish protocol to communicate with the BMC rather than IPMI.
- **Redfish System Information:** It is similar to IPMI System Information, but uses Redfish protocol to communicate with the BMC rather than IPMI.
- **Redfish Power Consumption** (**Detect NM** is checked)**:** It is similar to IPMI Power Consumption, but uses Redfish protocol to communicate with the BMC rather than IPMI.

1.8.4 Agentless Host

The system without SD5 can be discovered and managed as an Agentless host, e.g., a CDU system.

When a CDU host is added, built-in services include:

- **Check CDU** (**Detect CDU** is checked): Checks the health of a CDU. The service state depends on the CDU status provided by the CDU.

Note: Because the CDU system does not support the Timezone setting, the date and time on the CDU system must be set to the same as SSM to avoid false alarms. For example, the date and time on the SSM system are 2022/11/23 10:00 UTC+8, and the CDU system will be 2022/11/23 10:00.

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. In the Introduction window, click the **Next** button to continue.
3. In the License Agreement window, select **I accept the terms of the License Agreement** check box and click the **Next** button to continue.
4. In the Choose an install set window, select the **Install All** option and click the **Next** button.
5. In the Choose an install folder window, select a directory to install SSM to and click the **Next** button. It is recommended that SSM should be installed to the default folder (C:\Program Files\Supermicro\SSM).
6. In the Choose a Java VM window, use the built-in Java VM and click the **Next** button to continue. If you select the **Choose a Java VM** option instead, ensure to select a Java VM with x64 architecture so that it will be compatible with the installer. Also note that the only supported JVM versions are those later than 11.0.0 and earlier than 12.0.0.
7. In the Setup a database window, use the built-in database and click the **Next** button.
8. In the Setup user password window, you can configure the password for the built-in ADMIN account to access the SSM Web. When completed, click the **Next** button.
9. In Setup the SSM Web Server window, enter the default port numbers for HTTP and HTTPS and click the **Next** button. Normally, you should accept the default HTTP and HTTPS values of 8080 and 8443, respectively.
10. In the Setup SMTP window, enter an SMTP server, an SMTP port, a sender's email address, a user account, and the password. Check SSL (Secure Sockets Layer) or StartTLS (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. Note that you can modify the SMTP server settings later on SSM Web. See *6.10 Email SMTP Setup* for more information.
11. In the Setup default contact window, enter the email address of the default contact and click the **Next** button.
12. In the Setup a key store window, select **Yes** to use the default key store and click the **Next** button.
13. In the Pre-Installation summary window, click the **Install** button to install the SSM software on your computer.

14. In the Install Complete window, the installation is complete. Click the **Done** button to exit and restart your system to enable SSM services.

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. On the Introduction page, press the **<Enter>** key (on your keyboard) to continue.
3. On the License Agreement page, accept the license agreement and press the **<Enter>** key to continue.
4. On the Choose an install set page, select the **Install All** option and press the **<Enter>** key to continue.
5. On the Choose an install folder page, 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**).
6. On the Choose a Java VM page, use the built-in Java VM and press the **<Enter>** key to continue. If you select "Choose a Java VM" instead, ensure to select a Java VM with x64 architecture so that it will be compatible with the installer. Also note that only JVM versions later than 11.0.0 and earlier than 12.0.0 are supported.
7. On the Setup a database page, use the built-in database and press the **<Enter>** key to continue.
8. On the Set the password for built-in ADMIN user page, you can input the password for the built-in ADMIN account to access SSM Web and press the **<Enter>** key to continue.
9. On the Setup the SSM Web Server page, enter the default port numbers for HTTP and HTTPS and press the **<Enter>** key to continue. Normally you should accept the default values of 8080 and 8443 ports for HTTP and HTTPS, respectively.
10. On the Setup SMTP page, enter an SMTP server, an SMTP port, a sender's email, a user account, and the password. Enter SSL (Secure Sockets Layer) or StartTLS (Transport Layer Security) if the SMTP server uses secure connections. The data will be used by the SSM server to send notifications. When completed, press the **<Enter>** key to continue. Note that you can modify the SMTP server settings later on SSM Web. See *6.10 Email SMTP Setup* for more information.
11. On the Setup default contact page, enter the email address of the default contact and press the **<Enter>** key to continue.

12. On the Setup a key store page, use the default key store and press the **<Enter>** key to continue.
13. On the Pre-installation summary page, press the **<Enter>** key to continue.
14. On the Ready To Install page, press the **<Enter>** key to install the SSM software on your computer.
15. The Installation Complete page will show when the installation is complete. Press the **<Enter>** key to exit the installer. Note that 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 and SSM Web) 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= SSMServer,SSMWeb

#Choose a Java VM
#----------------------
USE_DEFAULT_JVM=Yes
#INSTALLED_JVM_PATH=/usr/java/jdk11.0.18/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
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.**	SSMServer,SSMWeb | SSMServer | SSMWeb
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

Attribute	Description	Option
SERVER_WEB_HTTPS_PORT	SSM Web secure listen port	8443
SERVER_EMAIL_SMTP	SMTP server location	
SERVER_EMAIL_SENDER	Sender's email	
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 email	
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 **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	

Attribute	Description	Option
	USE_SERVER_DEFAULT_DB=No	
SERVER_DB_PASSWORD	Database password if **USE_SERVER_DEFAULT_DB=No** **Note:** If the CHOSEN_INSTALL_FEATURE_LIST only has the SSMWeb component, please fill in the encoded database password by the SSM Server. You can find it in [install folder]\shared\config\datasource.properties] on the system where the SSM Server is installed.	
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_Install_MM_dd_yyyy_hh_mm_ss.log (i.e., SSM_Install_01_31_2020_09_59_31.log)** file is generated in the **[install folder]/Uninstall/Logs** 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 2021

Detect previous: 'YES'

Installation Result: Failed

Root Cause: SSM already exists, pleases 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 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

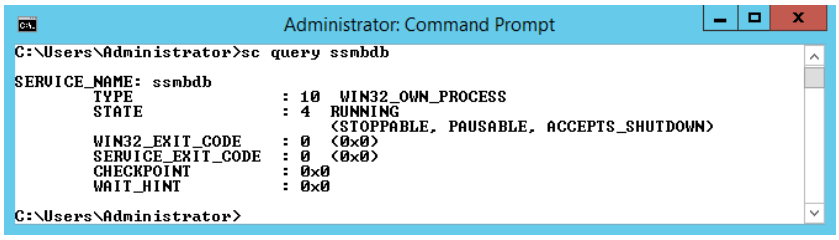


Figure 2-1

Check the SSM Server

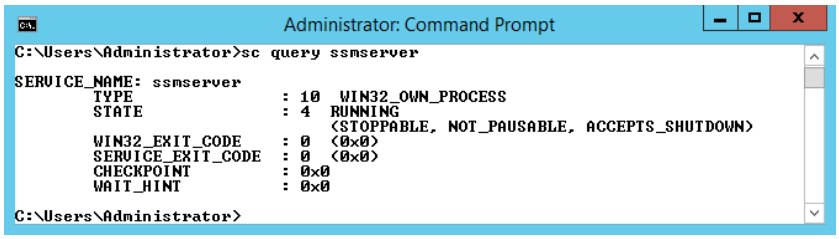


Figure 2-2

Check the SSM Web

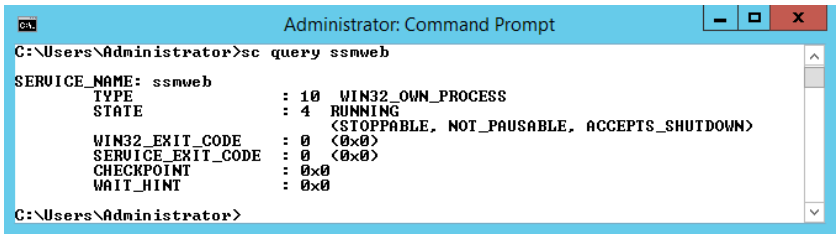


Figure 2-3

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

service ssmbdb status

service ssmserver status

service ssmweb status

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

systemctl status ssmbdb

systemctl status ssmserver

systemctl status ssmweb

2.3 Manually Controlling SSM Services

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

2.3.1 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.

2.3.2 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.

2.3.3 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.

2.4 Uninstalling SSM

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

2.4.1 Uninstalling in Windows

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

1. Execute the Uninstaller program named **Uninstall.exe** in the **[install folder]\Uninstall** folder.
2. In the Introduction window, click the **Next** button to continue.
3. In the Introduction window, select the **Complete Uninstall** option and click the **Next** button. You can also select the **Uninstall Specific Features** option to uninstall specific SSM features such as SSM Web and SSM Server.
4. In the Uninstalling… window, please wait while the program uninstalls.
5. In the Uninstall Complete window, click the **Done** button to exit the uninstaller.

2.4.2 Uninstalling in Linux

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

1. Execute the Uninstaller program named **Uninstall** 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.
2. On the Uninstall SSM page, press the **<Enter>** key (on your keyboard) to continue.
3. On the Uninstall Options page, select the **1- Completely remove all features and components** option and press the **<Enter>** key to continue. You can also choose the **2** option to uninstall specific SSM features such as SSM Web and SSM Server.
4. On the Uninstalling… page, please wait while the program uninstalls.
5. On the Uninstall Complete page, it shows that the uninstallation is complete.

2.4.3 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.

2.5 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.
- If your current version is less than v3.2.0, you must first upgrade SSM to a version between v3.2.0 and v5.1.0 in order to upgrade to v5.2.0 and later.

2.5.1 Upgrading in Windows

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

1. Execute the SSMInstaller.
2. In the Installing… window, select **Yes** to back up the data in the previous version and click the **Next** button to continue.
3. In the Installing… window, input the password of the built-in ADMIN user and click **Next** button to continue. Note that you will be forced to change the password if "ADMIN" is detected to be the password for the built-in ADMIN account.
4. Please wait until the progress bar shows that the data of the current version of SSM has been backed up completely.
5. Please wait until the progress bar shows that the data has been completely restored to the newer version of SSM.
6. The Install Complete window will show when the upgrade is complete. Click the **Done** button to exit.

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 *2.5.3 Restoring SSM after Auto-Upgrade Fails* for details.

2.5.2 Upgrading in Linux

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

1. Execute the SSMInstaller.
2. On the An old version of SSM is detected page, select **Yes** to back up the data of the current version of SSM and press the **<Enter>** key to continue. Please wait while the data of the current version of SSM is backed up.
3. On the Set the password for built-in ADMIN user page, input the password of the built-in ADMIN user and press the **<Enter>** key to continue. Note that you will be forced to change the password if "ADMIN" is detected to be the password for the built-in ADMIN account.
4. On the Installing… page, please wait while the newer version of SSM is installed and the older version is uninstalled.
5. The Installation Complete page shows when the upgrade is complete. Press the **<Enter>** key to exit.

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 *2.5.3 Restoring SSM after Auto-Upgrade Fails* for details.

2.5.3 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 *2.4 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.

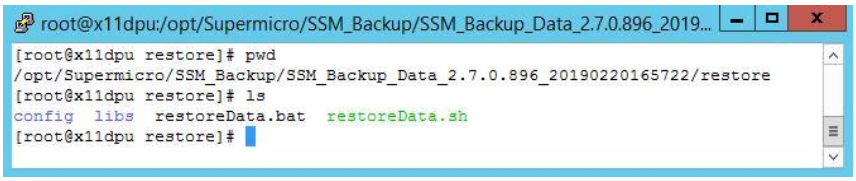


Figure 2-4

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

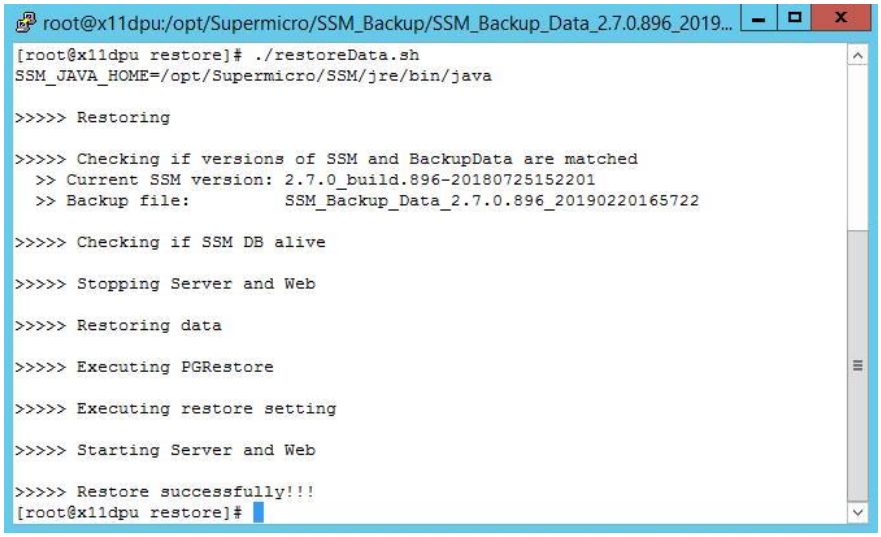


Figure 2-5

2.5.4 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).

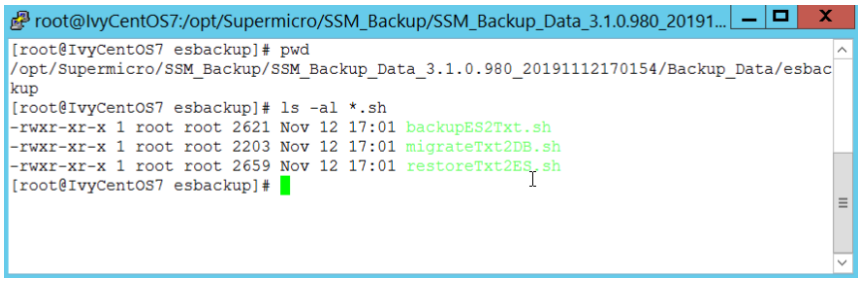


Figure 2-6

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.

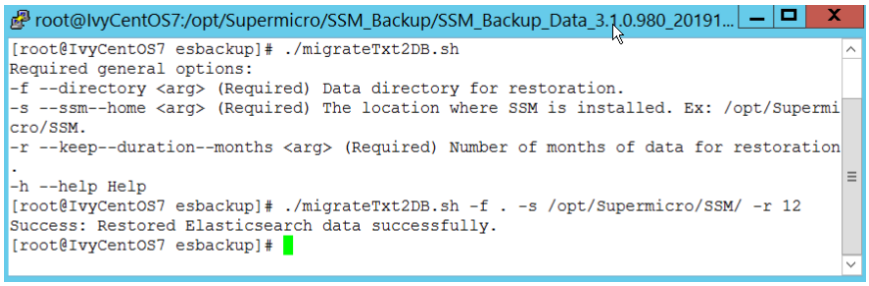


Figure 2-7

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 contain 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. 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 Exporting and Importing 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 the managed host.

ipmi_password

This attribute defines the encoded password to access the managed host. Note that when you use the innoutconfig program, use "<your- -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. 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 five built-in physical groups: datacenter, room, row, rack and enclosure. A physical group must be one of the five 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, rack, and enclosure are 5, 4, 3, 2 and 1, respectively.

Note: You are not allowed to create an enclosure on your own. When a CMM host is discovered, an enclosure group with the name *CMMModelName_HostName* will be created, and the CMM host with all related blade nodes will be added to this group.

(* 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 active checks of the service and is executed to measure its status. For IPMI/Redfish SEL Health service that supports passive checks, you could decrease the check frequency to avoid unnecessary active checks.

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.

passive_check_enabled

This attribute indicates that the check result of the service is decided by the passive check instead of the active check.

(* 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-snmptrap, 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-snmptrap,
                                        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               Everday
}
```

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
SERVICEATTEMPT	The retry count of the latest service check.
HOSTLOCATION	The location of a host.
HOSTNOTES	The additional information of a host.
MH_SYS_MODEL	The model number of a managed system. The value is retrieved at runtime. To avoid possible performance impact when SSM monitors lots of hosts, use this macro with sparingly.
MH_SYS_SERIAL	The serial number of a managed system. The value is retrieved at runtime. To avoid possible performance impact when SSM monitors lots of hosts, use this macro with sparingly.
MH_BMC_VER	The BMC version of a managed system. The value is retrieved at runtime. To avoid possible performance impact when SSM monitors lots of hosts, use this macro with sparingly.
MH_BIOS_VER	The BIOS version of a managed system. The value is retrieved at runtime. To avoid possible performance impact when SSM monitors lots of hosts, use this macro with sparingly.

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>]

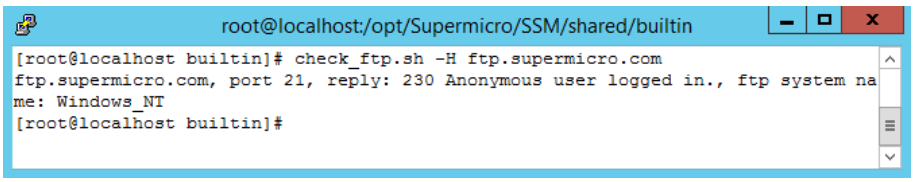
[-w | --password <arg>]

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:



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:

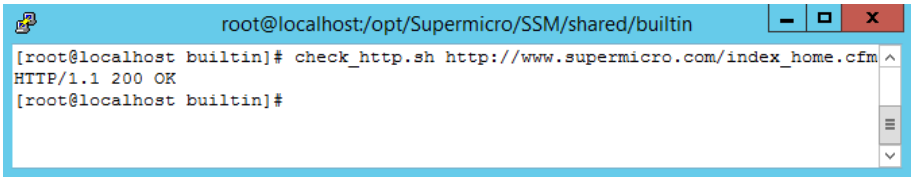
check_http URL

Options:

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

(* indicates a required attribute)

Example:



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:

-a, --account	The account to login to the BMC.
-c, --changepassword	The new password to be set.
-d, --definition	Generates definitions of monitored items.
-da, --all in one definition	Generates all-in-one definitions of monitored items.
-h, --help	Shows the help menu.
-hl, --highlimit	The up threshold for the monitored item.
-i, --ip	The IP address of the BMC.
-l, --lan	LAN Configuration
-ll, --lowlimit	The low threshold for the monitored item.
-n, --index	The number of the monitored item.
-p, --password	The password to login to the BMC.
-protocol	The protocol used to communicate with the BMC.

-t, --type

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;3
3856 FAN_4=10404RPM;0;0;784;33856 FAN_5=9216RPM;0;0;784;33856 CPU1_Vcore=0.928Vo
lts;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;3.6
48 System_Temp=33degreeC;0;0;-5;75 P1-DIMM1A=38degreeC;0;0;-5;75 P1-DIMM2A=37deg
reeC;0;0;-5;75 Chassis_Intru=0SWITCH;0;0;-1;2 PS_Status=0SWITCH;0;0;-1;2 PS2_Fan
1=8544RPM;0;0;720;10000 PS2_Temperature1=44C;0;0;-10000;10000 PS2_Temperature2=3
9C;0;0;-10000;10000 PS2_ACInputCurrent=0.156A;0;0;-10000;10000 PS2_DC12VOutputCu
rrent=4.5A;0;0;-10000;10000 PS2_ACInputPower=29W;0;0;-10000;10000 PS2_DC12VOutpu
tPower=56W;0;0;-10000;10000 PS2_ACInputVoltage=228Volts;0;0;-10000;10000 PS2_DC1
2VOutputVoltage=12.188Volts;0;0;-10000;10000 PS2_Status=0SWITCH;0;0;-1;2 PS1_Fan
1=8448RPM;0;0;720;10000 PS1_Temperature1=44C;0;0;-10000;10000 PS1_Temperature2=3
9C;0;0;-10000;10000 PS1_ACInputCurrent=0.359A;0;0;-10000;10000 PS1_DC12VOutputCu
rrent=5.75A;0;0;-10000;10000 PS1_ACInputPower=76W;0;0;-10000;10000 PS1_DC12VOutp
utPower=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>

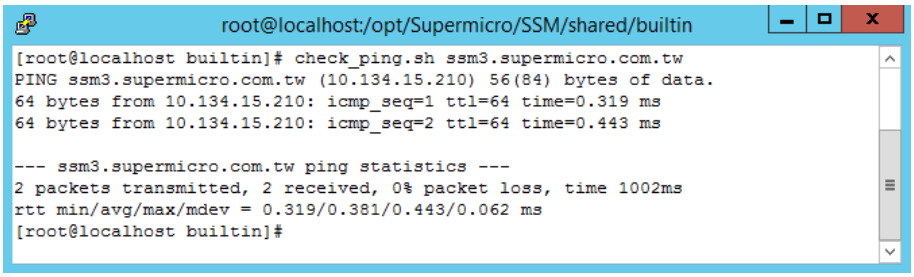
Options:

arg1 An IP address or a DNS name.

arg2 Timeout in seconds to wait for reply messages.

(* indicates a required attribute)

Example:



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:

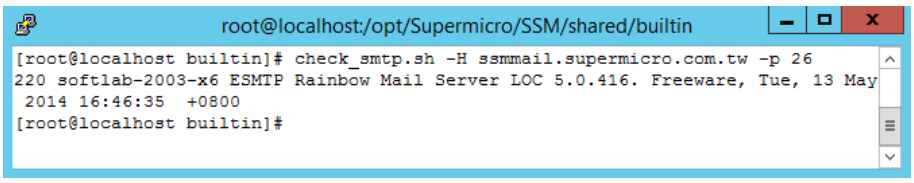
-h, --host An IP address or a DNS name.

-h, --help Shows the help menu.

-p, --port SMTP server port number. Default value is 25.

(* indicates a required attribute)

Example:



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:

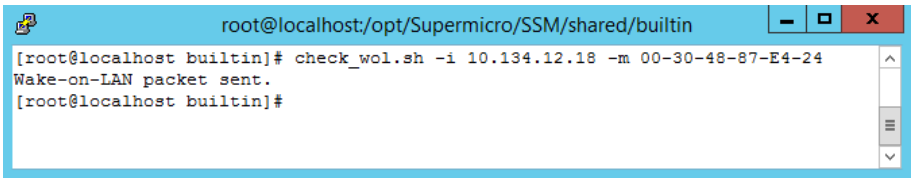
check_wol [-i | --ip <arg>] [-m | --mac <arg>]

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:



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 IObserver
-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 IObserver
-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

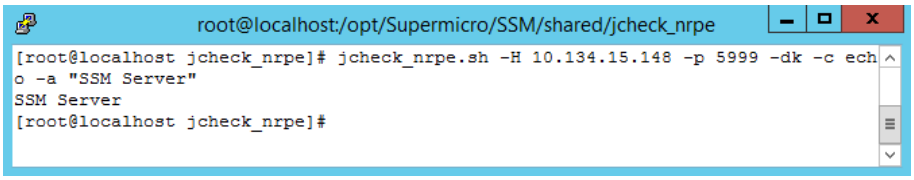
-trustKeyPassword <trustKeyStorePassword> The trust key store password

-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:



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.

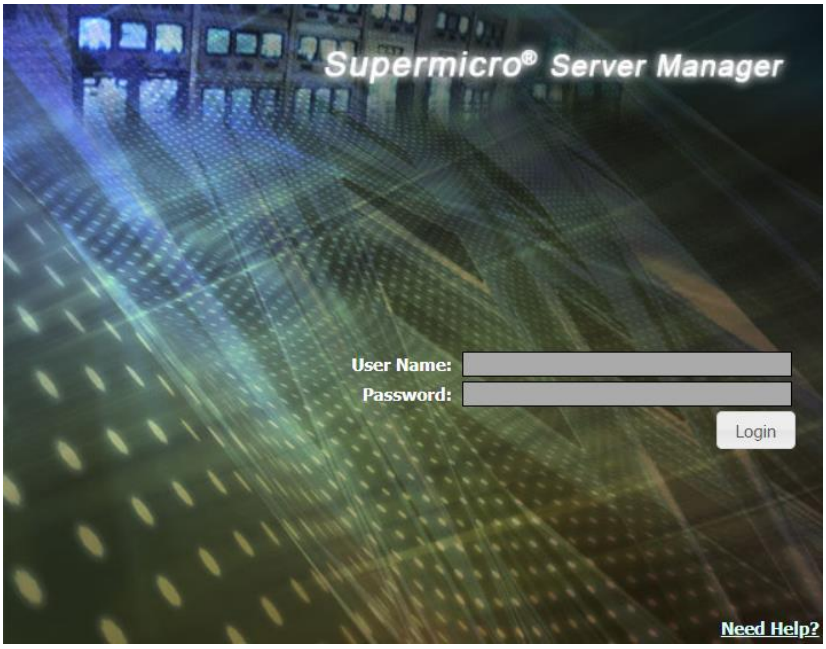


Figure 5-1

Note: When using Internet Explorer to connect to IPv6 hosts, colons are not allowed in a UNC path name format for representing an IPv6 address (i.e., fe80::f3ce:f3d5:b959:ab72). For this reason, Microsoft implemented a transcription algorithm to represent an IPv6 address in the form of domain name by replacing each colon with "-" and append .ipv6-literal.net in an IPv6 URL. (i.e., fe80--f3ce-f3d5-b959-ab72.ipv6-literal.net).

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 *6.15 Host Discovery Wizard* for more information.

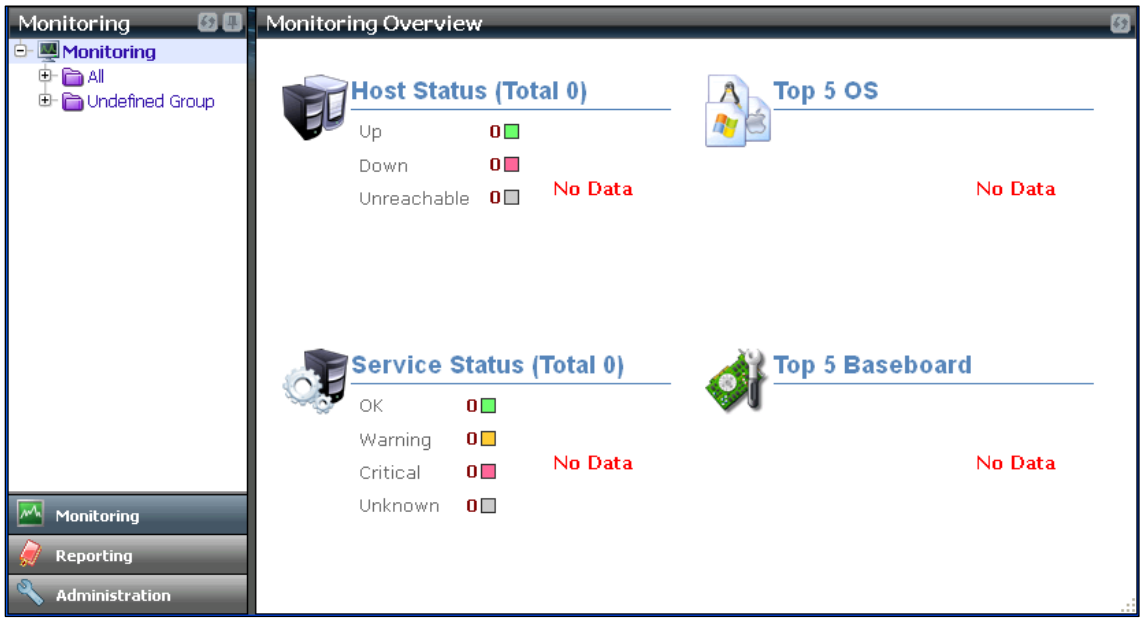


Figure 5-2

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

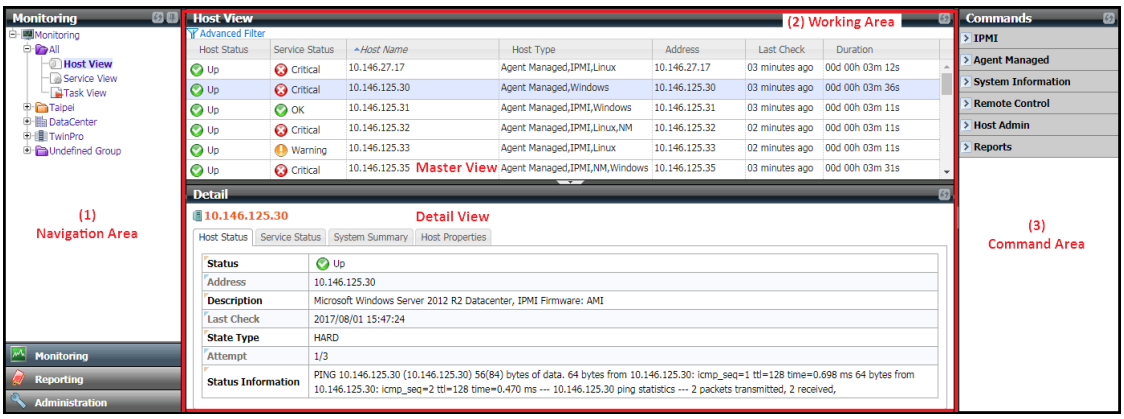


Figure 5-3

- **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.

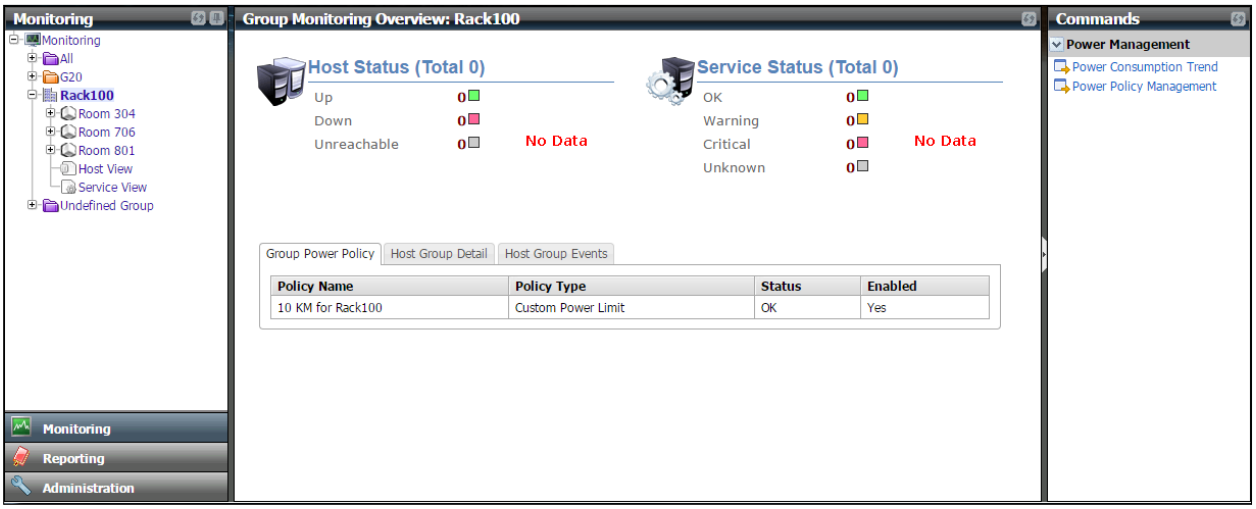


Figure 5-4

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.

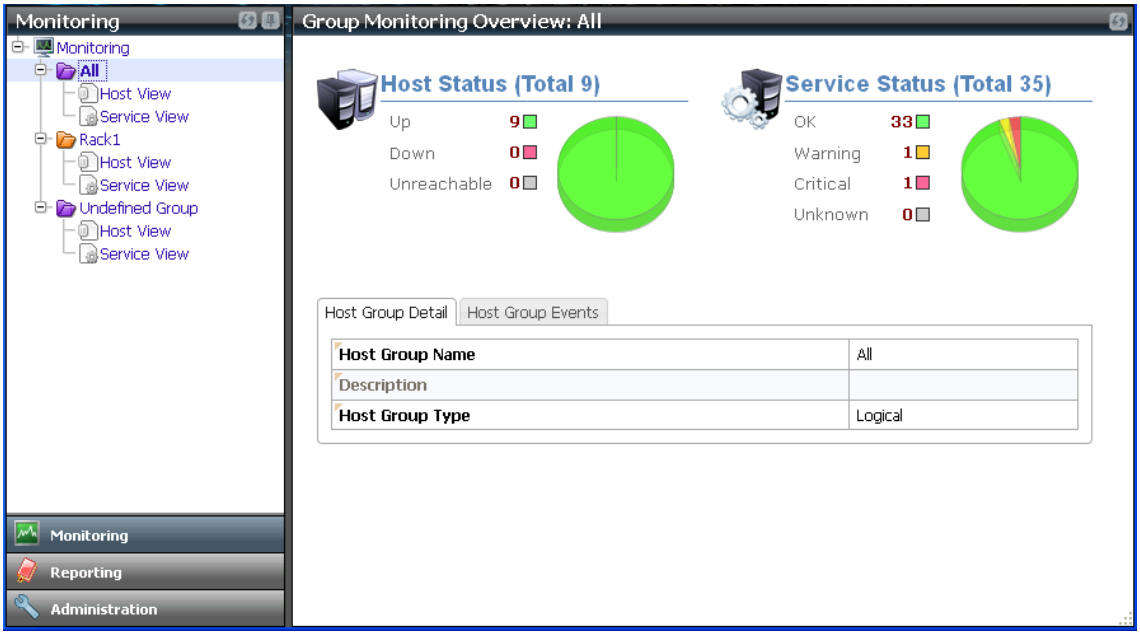

Monitoring
Monitoring
All
Host View
Service View
Rack1
Host View
Service View
Undefined Group
Host View
Service View
Monitoring
Reporting
Administration
Group Monitoring Overview: All
Host Status (Total 9)
Up 9
Down 0
Unreachable 0
Service Status (Total 35)
OK 33
Warning 1
Critical 1
Unknown 0
Host Group Detail
Host Group Events
Host Group Name All
Description
Host Group Type Logical

Figure 5-5

6 SSM Web Administration Page

6.1 Administration Page Overview

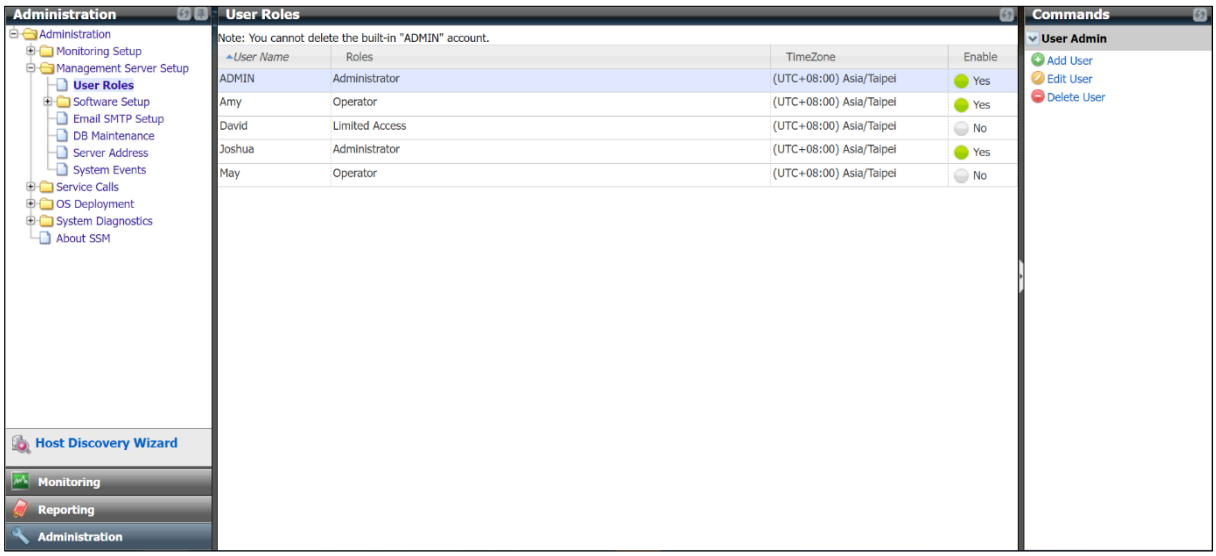


Figure 6-1

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 SUM package, and configuring the SD5 update site (4) setting up email 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 *10.3.8 FW Auto Update: Change Schedule* for details.

- **About SSM**: You can view some SSM information (i.e., **SSM version number and database information**).
- **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.

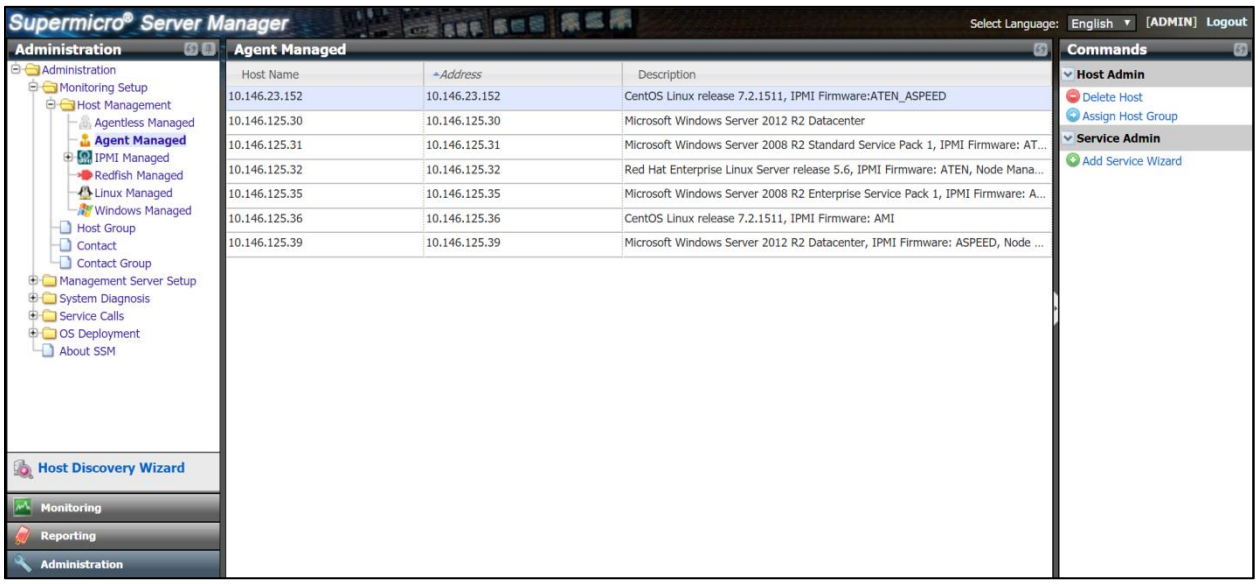


Figure 6-2

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.

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.

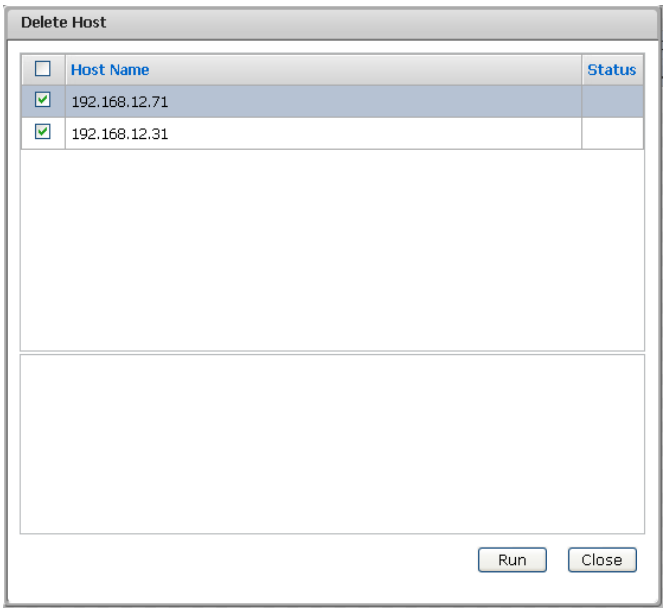


Figure 6-3

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.

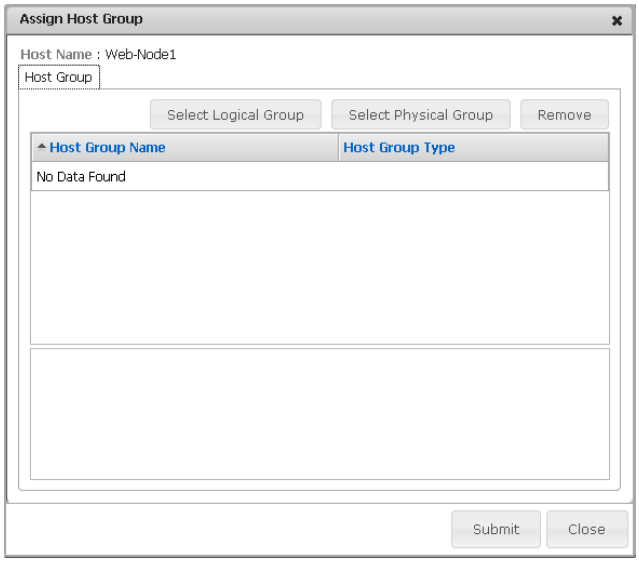


Figure 6-4

- 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.

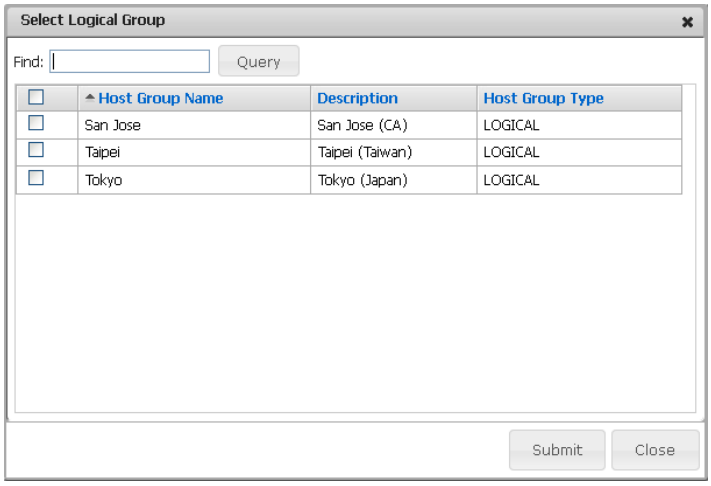


Figure 6-5

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.

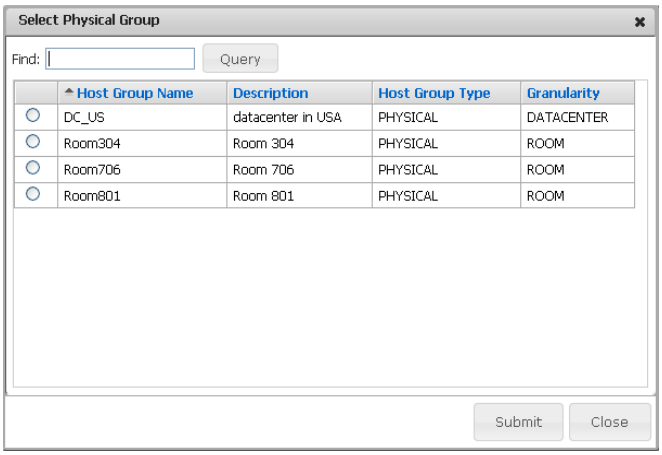


Figure 6-6

- 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.

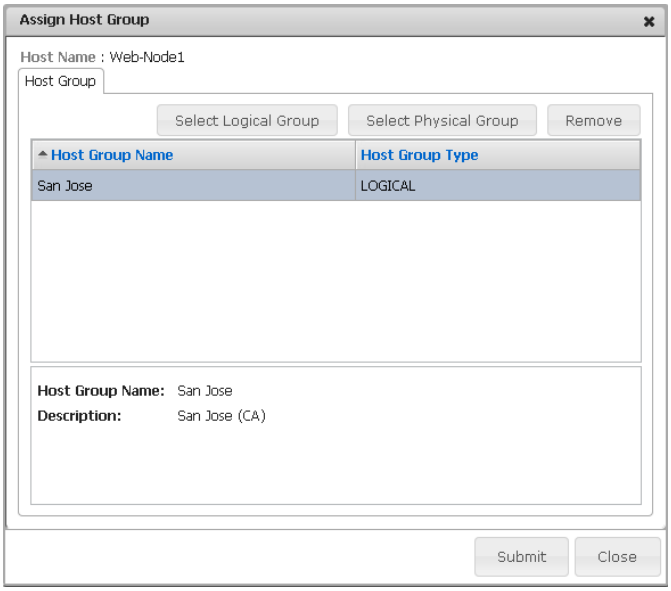


Figure 6-7

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.

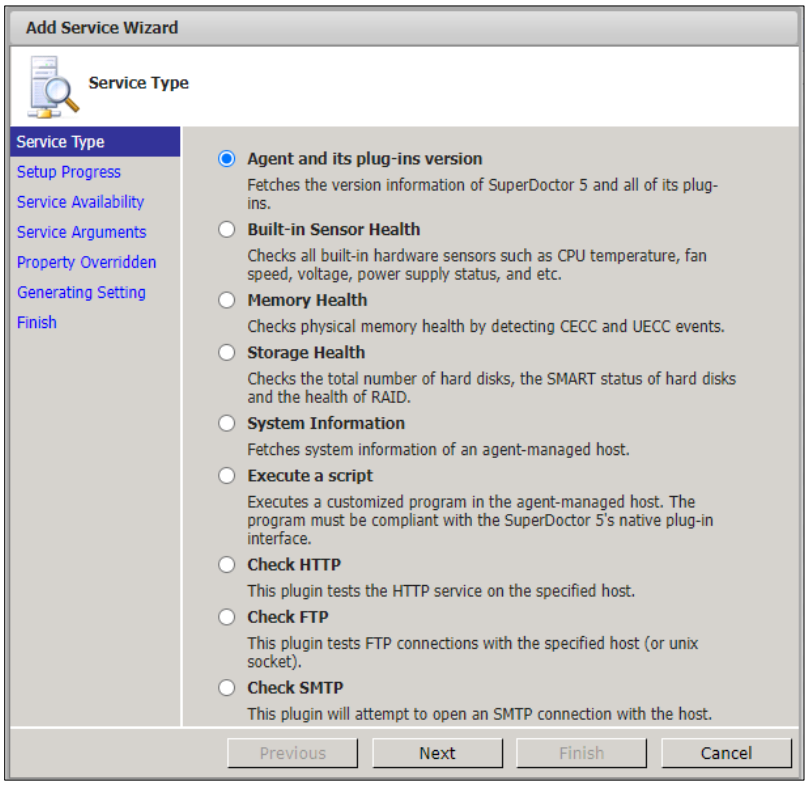


Figure 6-8

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

More additional services are listed below except built-in agent-managed services:

- **Execute a script**: Remotely executes an application (a plug-in) on the host. This service is the key to extend the monitoring features of agent-managed hosts.
- **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 (email) server.

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

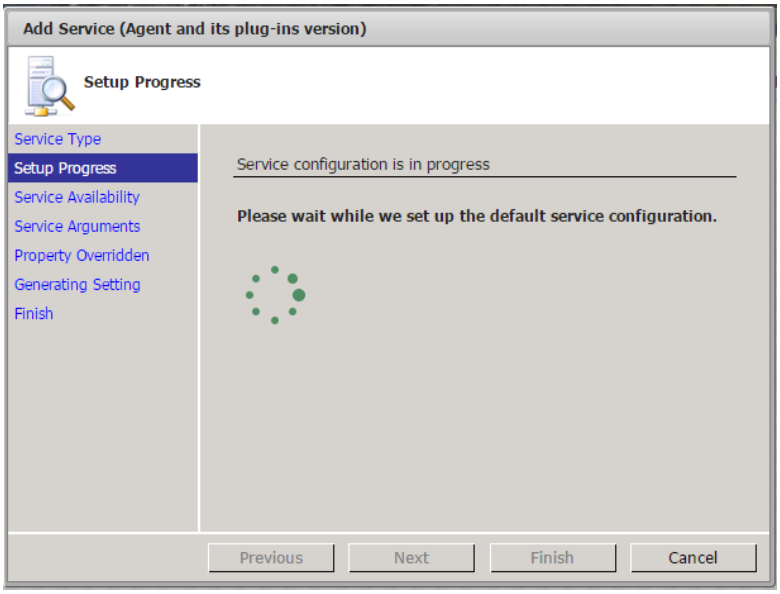


Figure 6-9

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

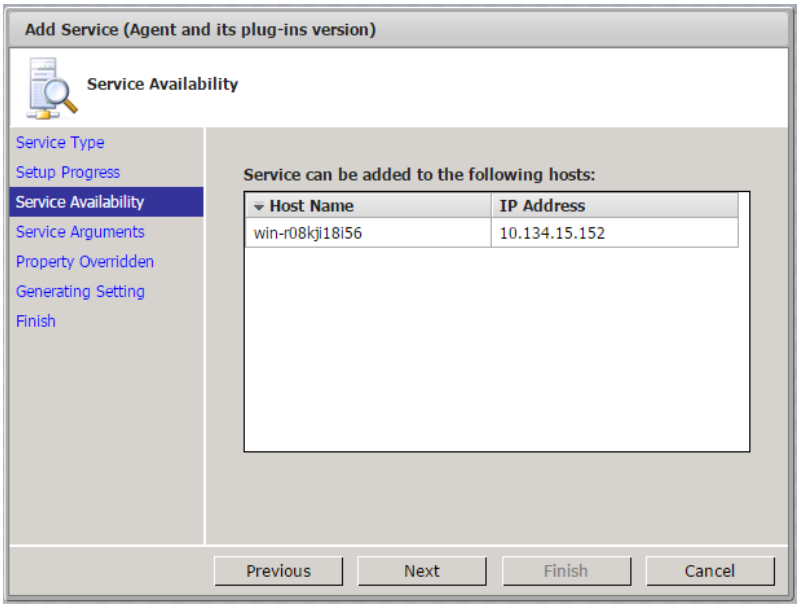


Figure 6-10

5. 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.

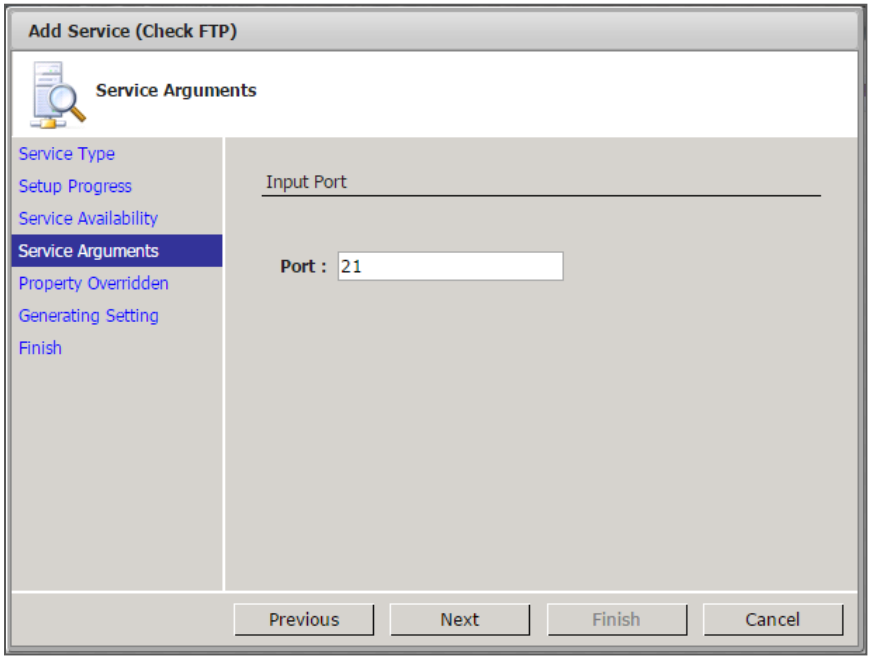


Figure 6-11

6. 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.

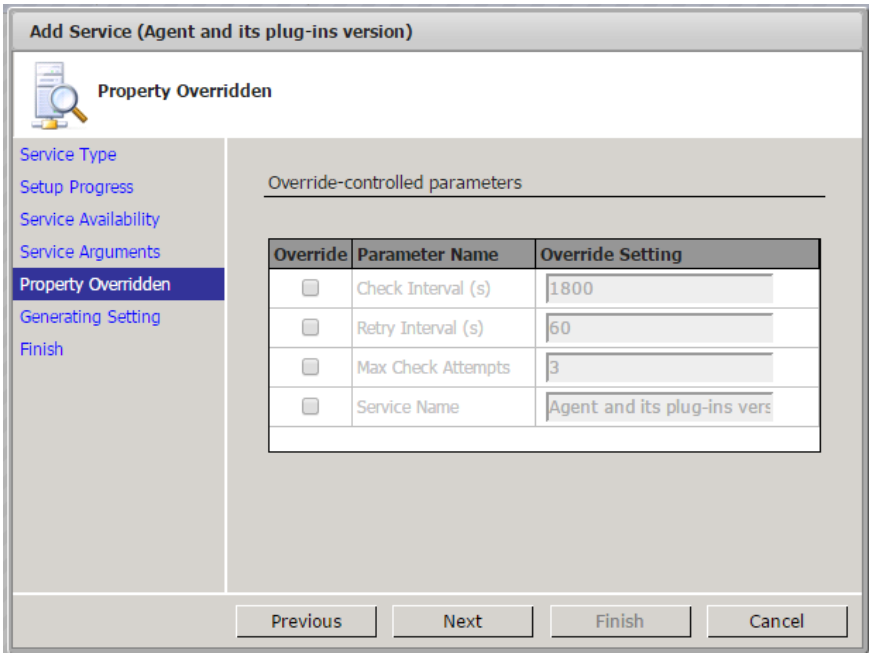


Figure 6-12

7. Please wait while SSM generates service configuration data.

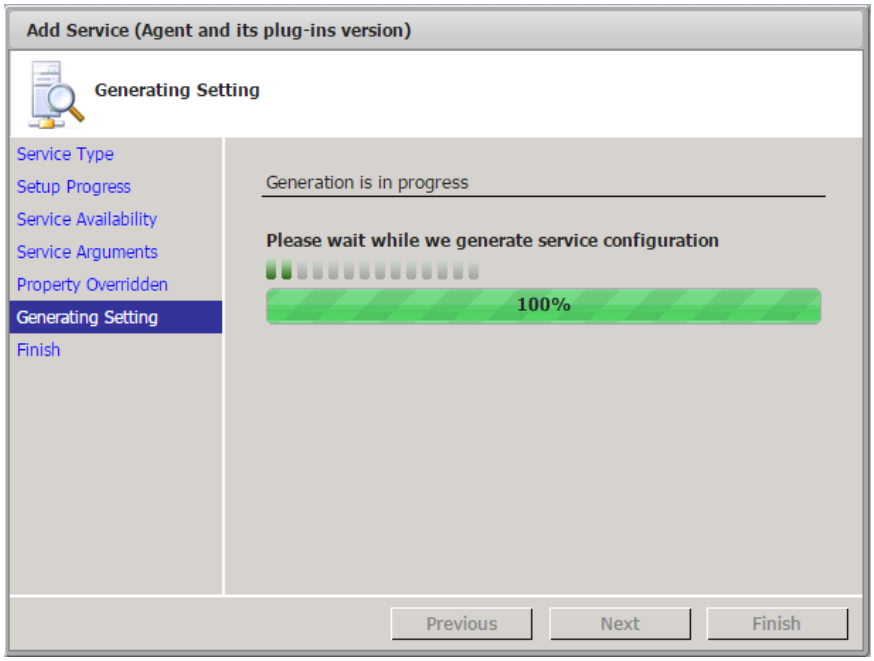


Figure 6-13

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

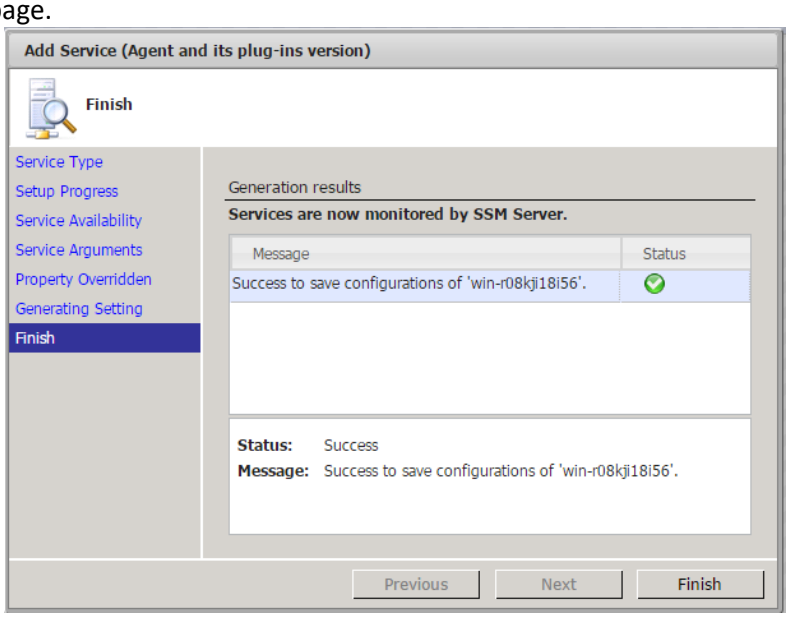


Figure 6-14

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.

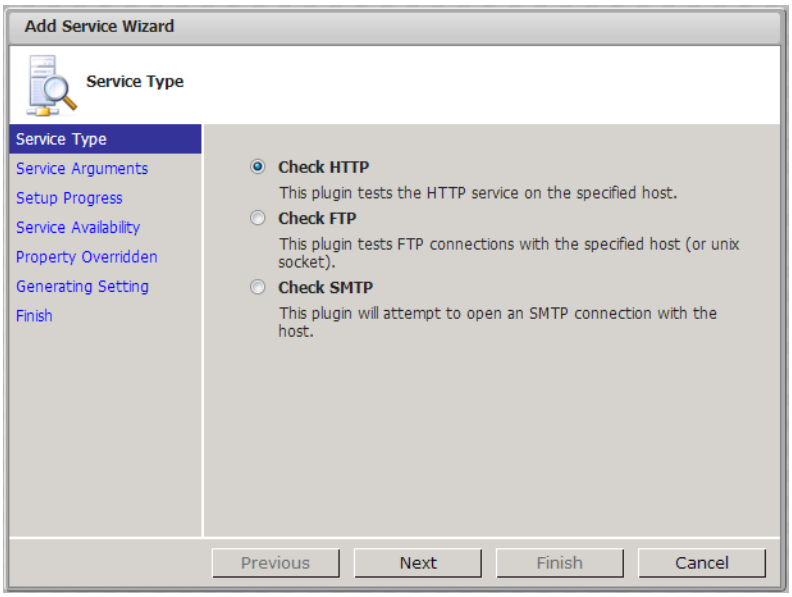


Figure 6-15

More additional services are listed below except built-in agentless services:

- **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 (email) 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.

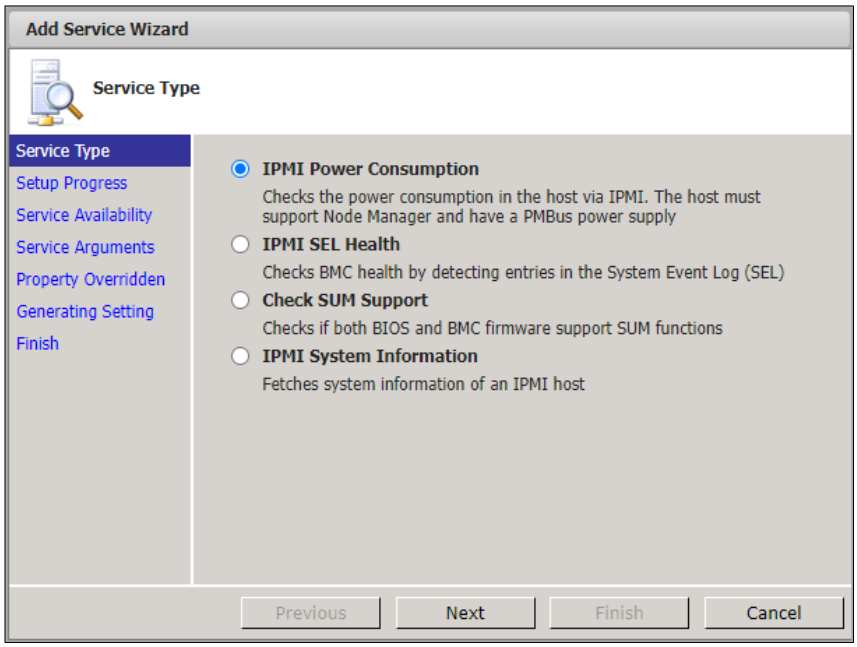


Figure 6-16

More additional services are listed below except built-in IPMI services:

- **Check SUM Support**: Checks if both BIOS and BMC firmware support SUM functions.

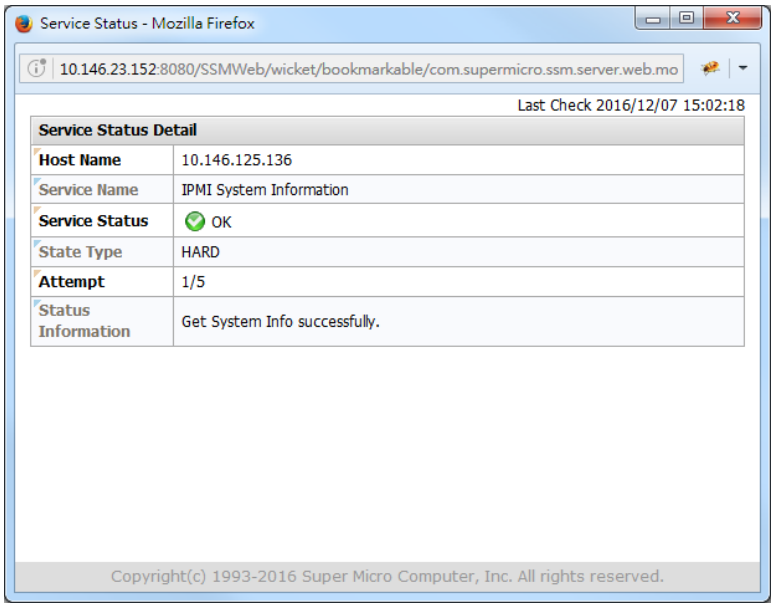


Figure 6-17

Besides the System Information command, the System Summary tab in the Detailed View also depends on the service, as shown below.

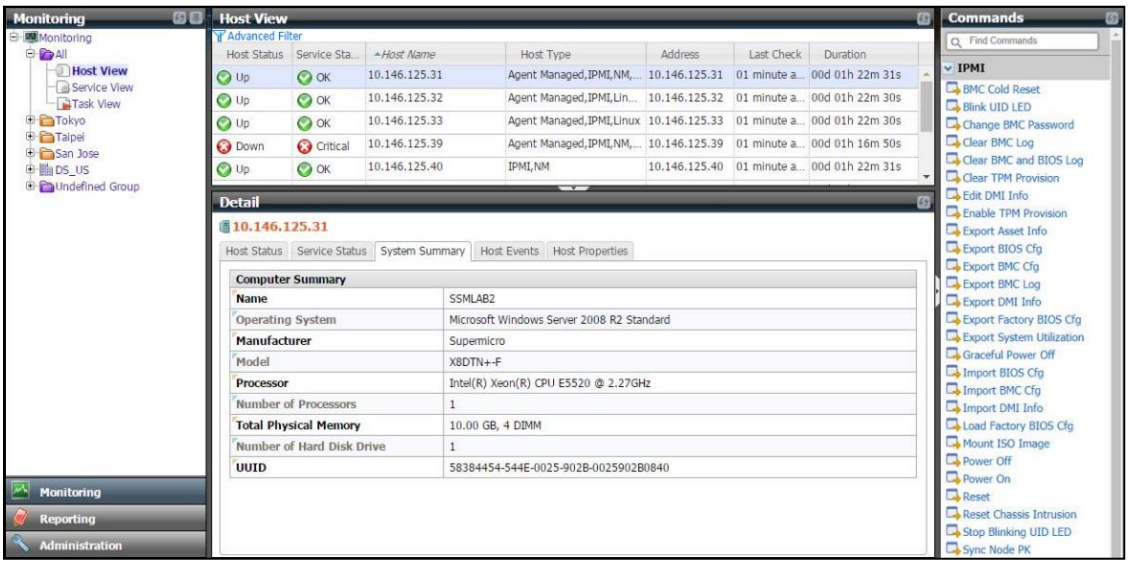


Figure 6-18

Note: The Check SUM Support service is designed for SUM. See *6.9.2 Updating SUM through SSM* for more information about SUM in SSM.

3. Select one service and click the **Next** button to continue. The subsequence 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. The Add Service Wizard dialog box will appear.

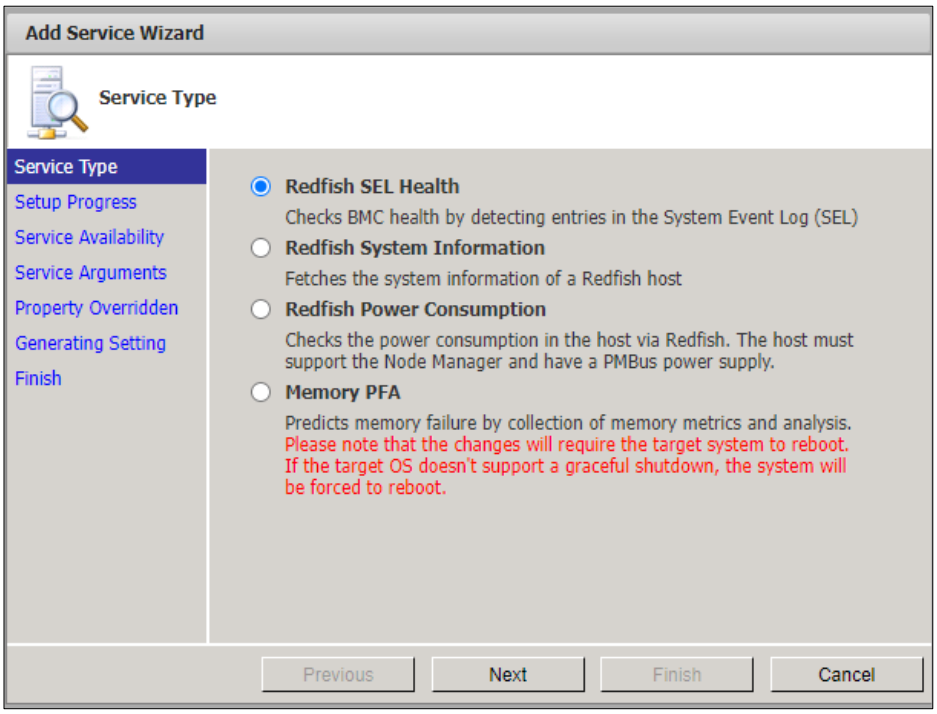


Figure 6-19

More additional services are listed below except built-in Redfish services:

- **Memory PFA**: Predicts memory failures with the collected memory metrics and analysis. Only one Memory PFA service can be enabled on a target system. Note that the system where a Memory PFA service is enabled should be rebooted immediately. If the target OS does not support a graceful shutdown, the system will be forced to be reboot. By default, the Linux OS with X Window systems do not support a graceful shutdown; it is therefore highly recommended that you change the power button setting from "Suspend" to "Power Off." See *14 Memory PFA* for more information.

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

6.2.4 Checking Activation Status

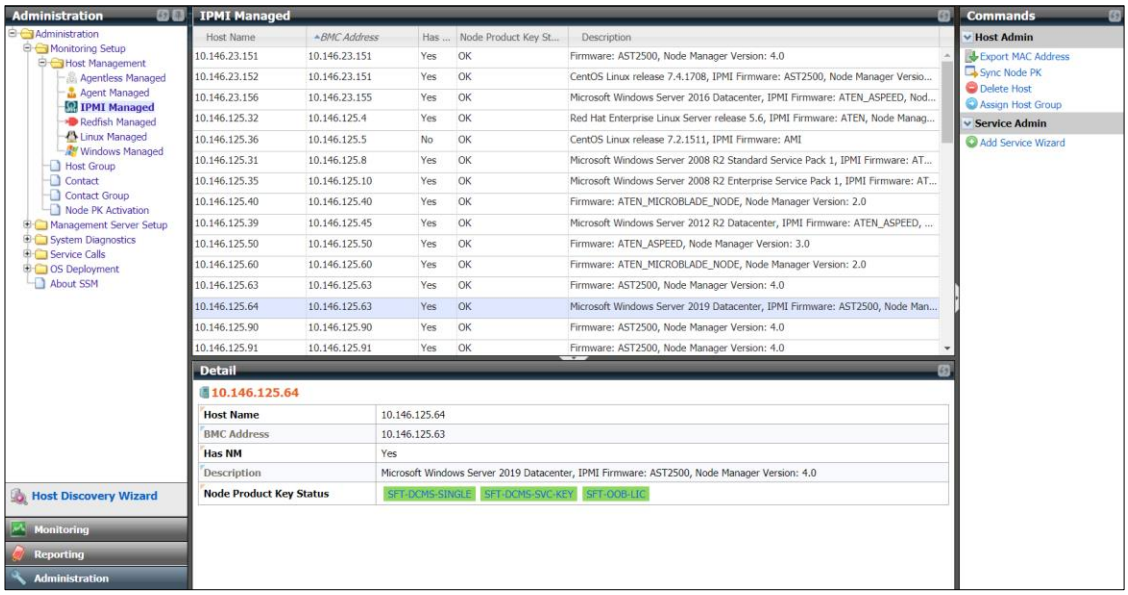


Figure 6-20

The **Node Product Key Status** of each host is shown on the **IPMI Managed** and **Redfish Managed** page under the Host Management category (see the figure above). This shows the activation status of a host.

Status Type	Description
Not Available	The IPMI host or Redfish host does not have the SFT-DCMS-SINGLE product key.
OK	The SFT-DCMS-SINGLE product key has been activated and has not yet expired.
Warning	The SFT-DCMS-SINGLE product key is going to expire in 15 days.
Critical	The SFT-DCMS-SINGLE product key has expired.

The Node Product Key Status column in the Detailed View shows additional product key information of the selected host in the master view, allowing you quickly check the key status.

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.

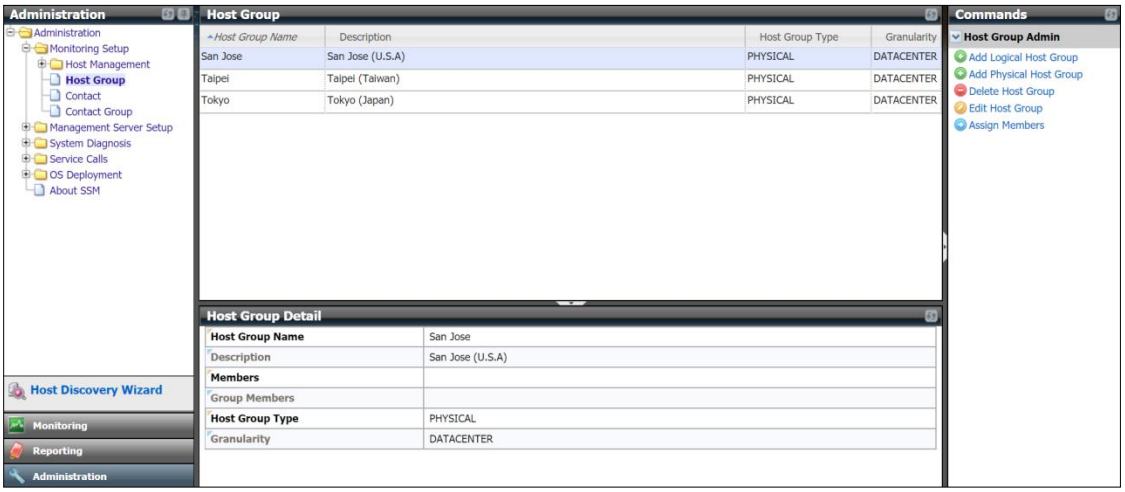


Figure 6-21

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.

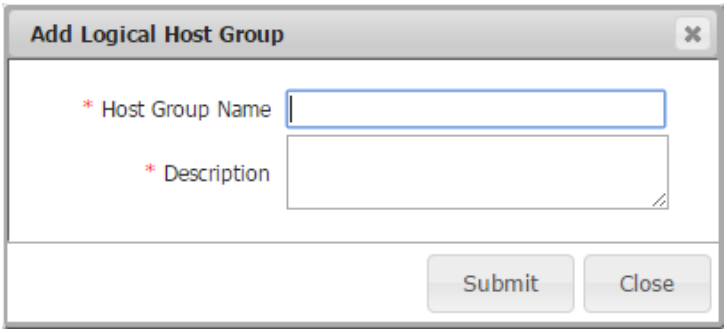


Figure 6-22

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

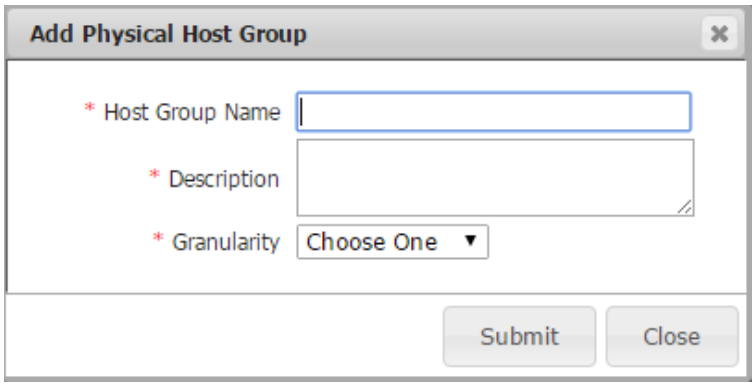


Figure 6-23

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.

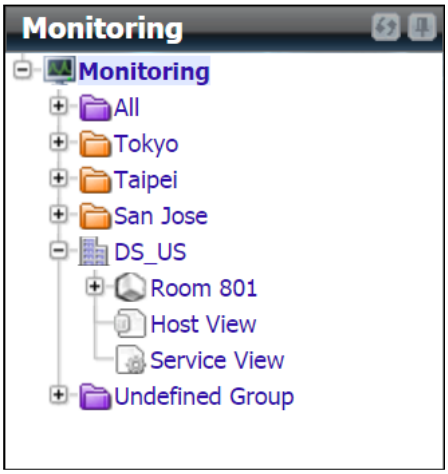


Figure 6-24

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.

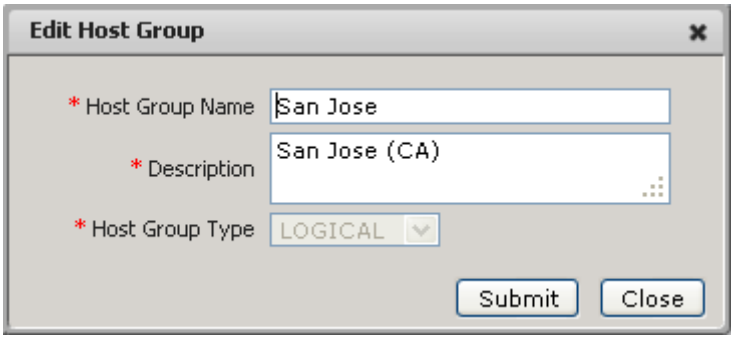


Figure 6-25

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.

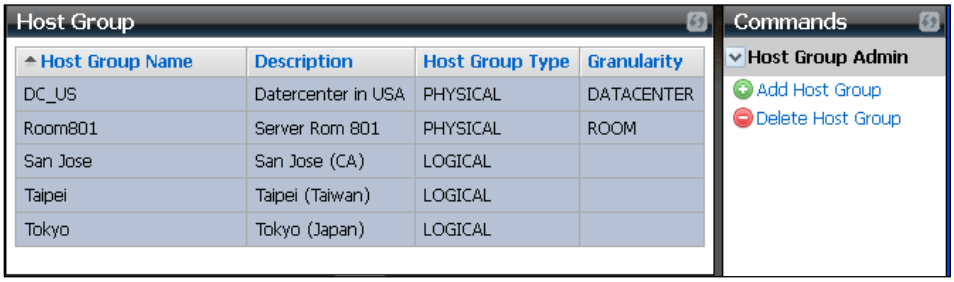


Figure 6-26

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

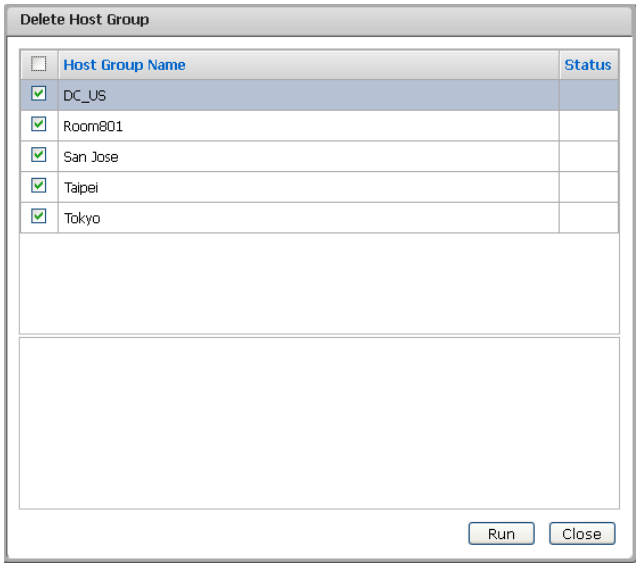


Figure 6-27

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.

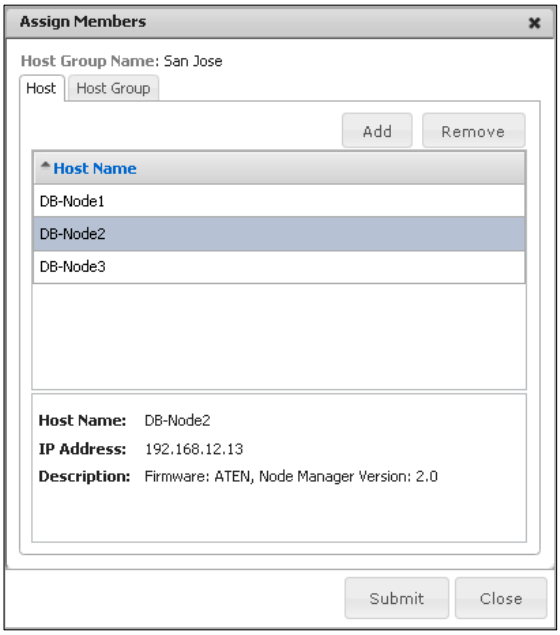


Figure 6-28

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.

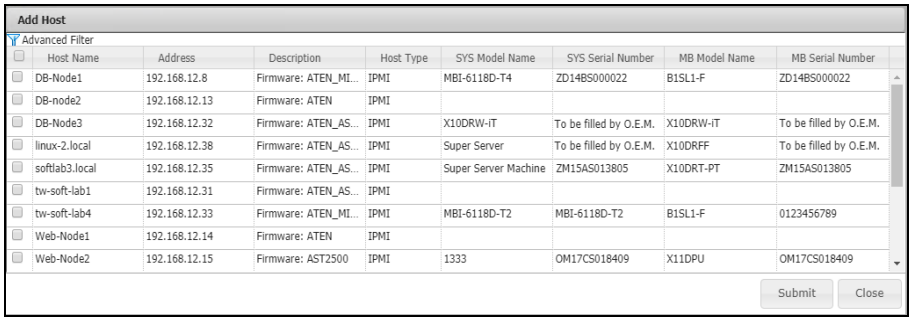


Figure 6-29

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.

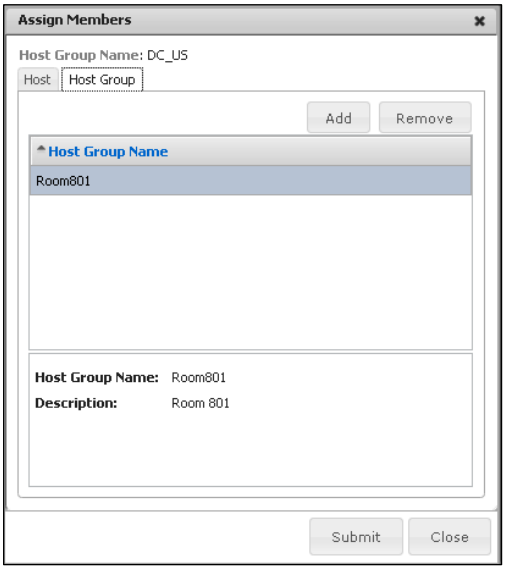


Figure 6-30

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.

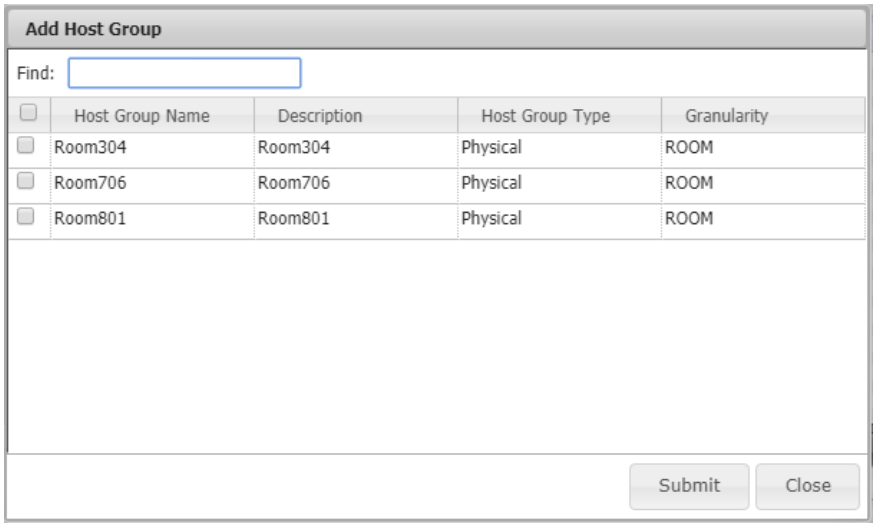


Figure 6-31

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.

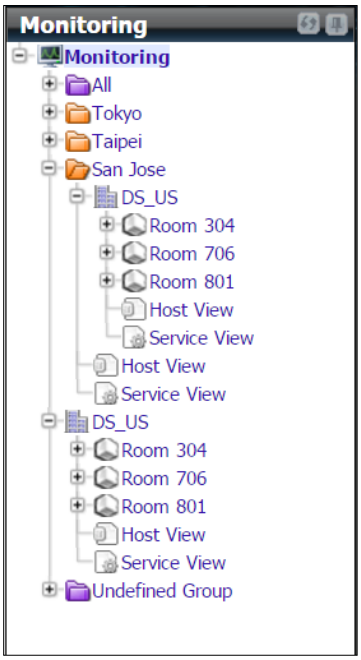


Figure 6-32

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.

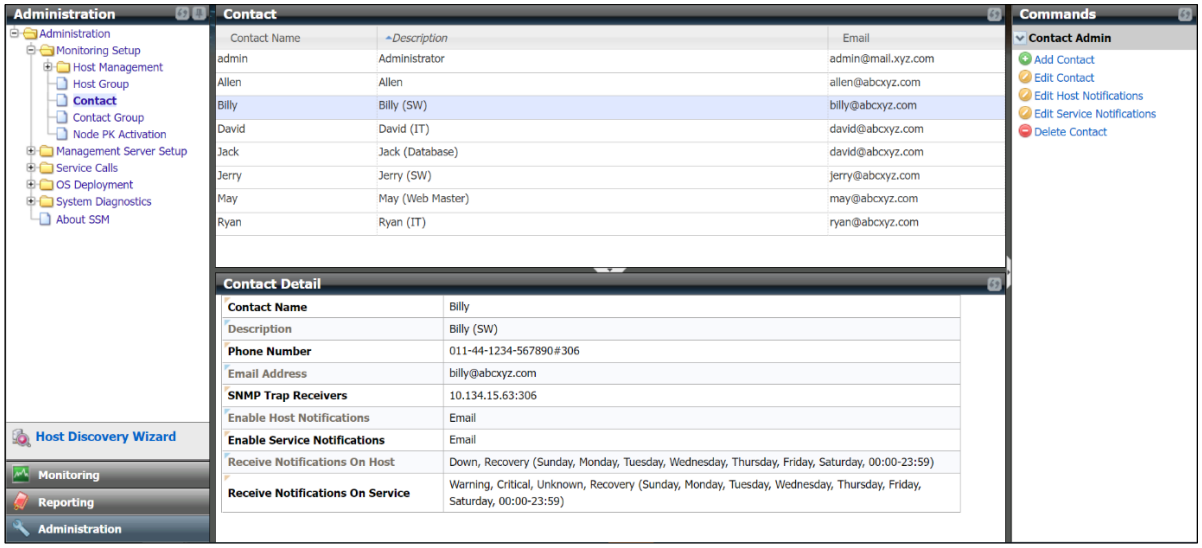


Figure 6-33

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.

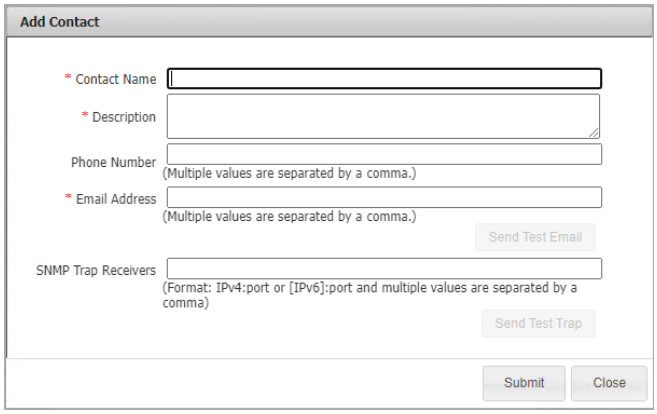


Figure 6-34

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

Notes: It is highly recommended that you click **Send Test Email** and **Send Test Trap** to ensure your email 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.

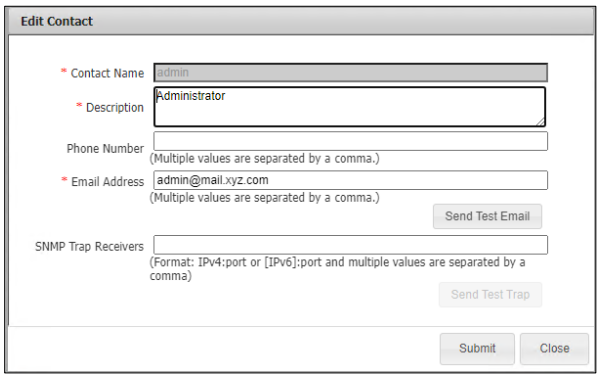


Figure 6-35

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

Notes: It is highly recommended that you click **Send Test Email** and **Send Test Trap** once you change an email 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.

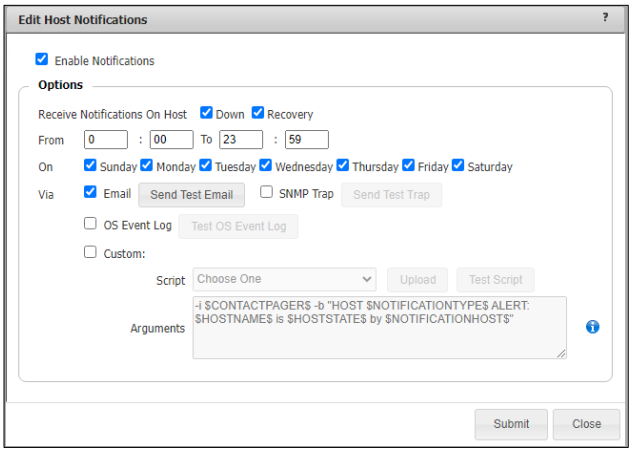


Figure 6-36

3. The **Enable Notification** checkbox is checked by default, meaning the selected contacts are able to receive notifications from hosts through email 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: Email, SNMP Trap, OS Event Log and Custom Script.
   - **Email**: Sends alerts via email. To use this function, you need to set up the email address for the contact and the Email SMTP server for SSM to send the notifications. Please refer to the *6.10 Email 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." Note that when you use a macro, it must be enclosed in double quotes if the macro is likely to include spaces.

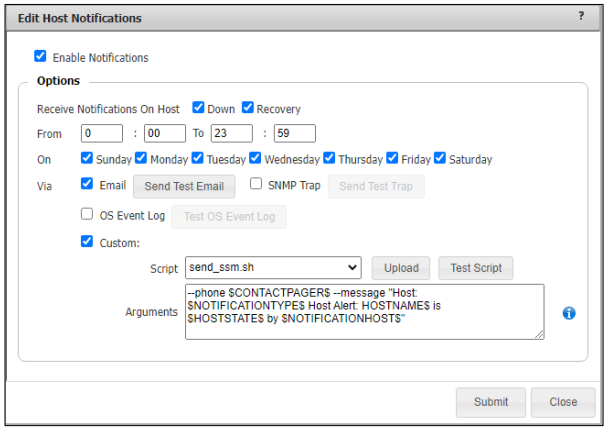


Figure 6-37

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

Notes: It is highly recommended that you click the **Send Test Email**, **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.

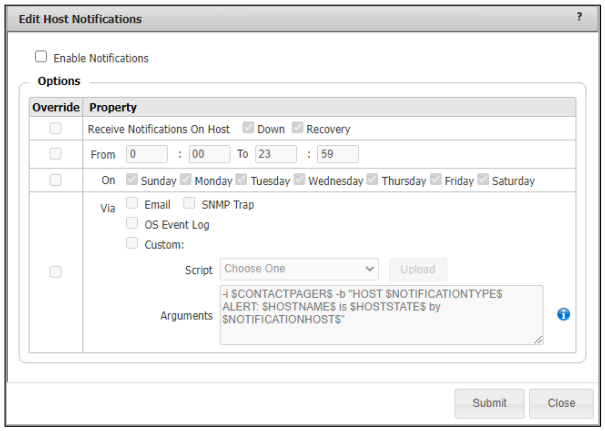


Figure 6-38

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).

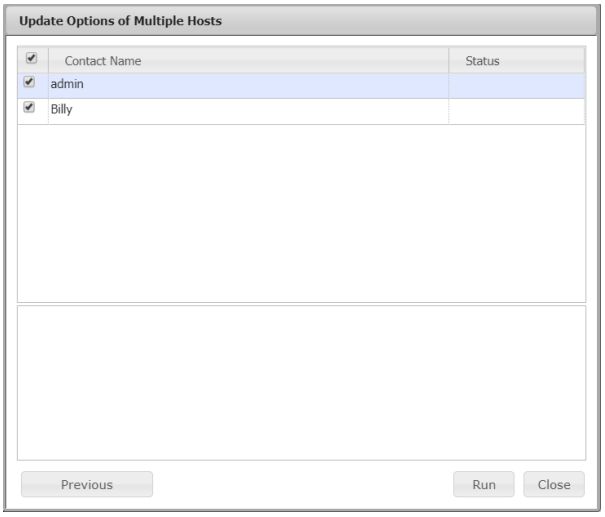


Figure 6-39

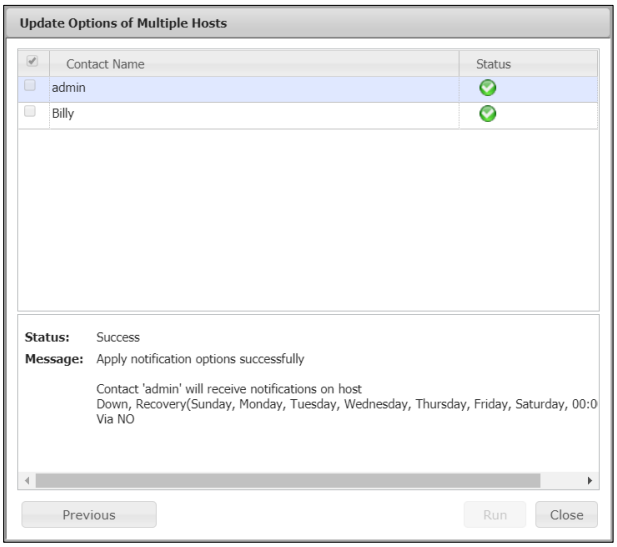


Figure 6-40

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.

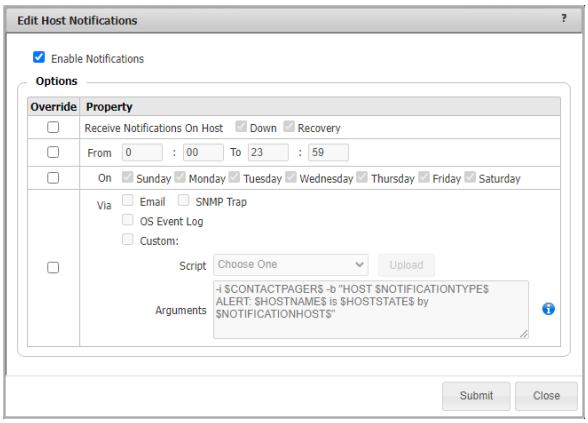


Figure 6-41

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: Email, SNMP Trap, OS Event Log and Custom Script.
   - **Email**: Sends alerts via email. To use this function, you need to set up both the email address for the contact and the email SMTP server for SSM to send email notifications. Please refer to the *6.10 Email 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."

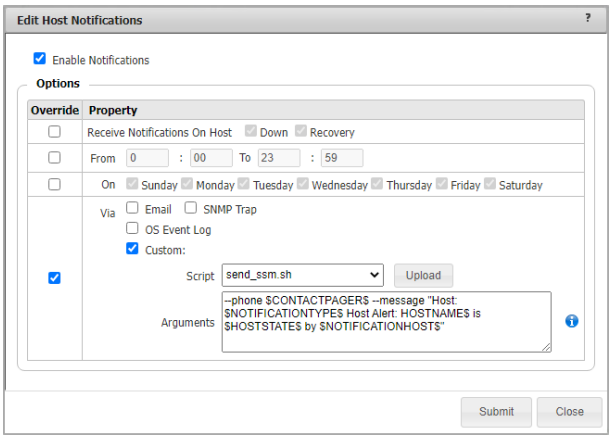


Figure 6-42

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 settings in the Override column. For the attributes in the Override column that are not selected, the original settings are kept.

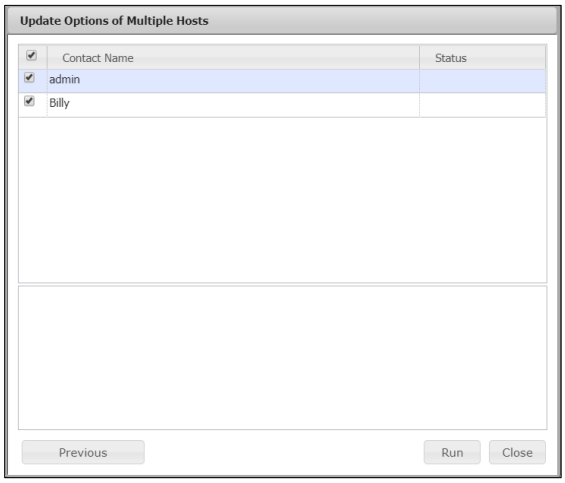


Figure 6-43

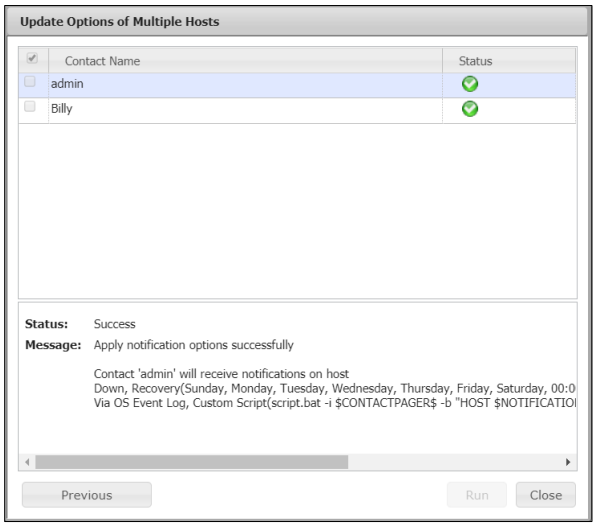


Figure 6-44

6.4.5 Editing Service Notifications for One Contact

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

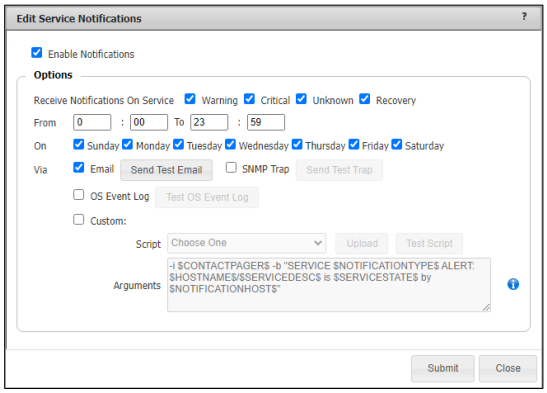


Figure 6-45

3. By default, the **Enable Notifications** checkbox is selected, meaning the selected contacts are capable of receiving notifications from services by email 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: Email, SNMP Trap, OS Event Log and Custom Script.
   - **Email**: Sends alerts via email. Note that to use this function, you need to set up both the email address for the contact and the email SMTP server for SSM to send email notifications. Please refer to the *6.10 Email 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."

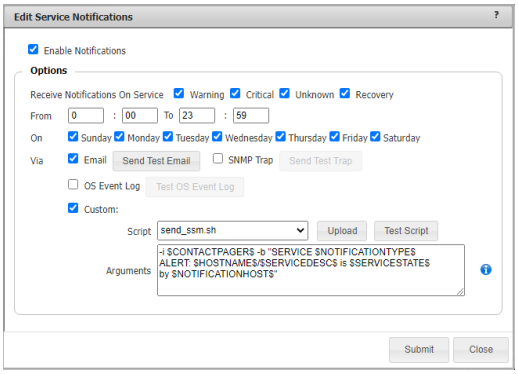


Figure 6-46

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

Note: It is highly recommended that you click the **Send Test Email**, **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.

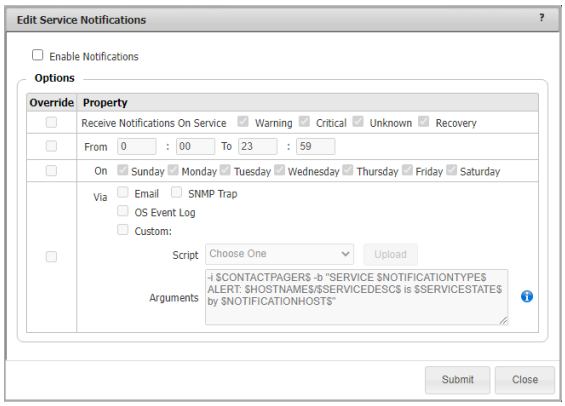


Figure 6-47

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).

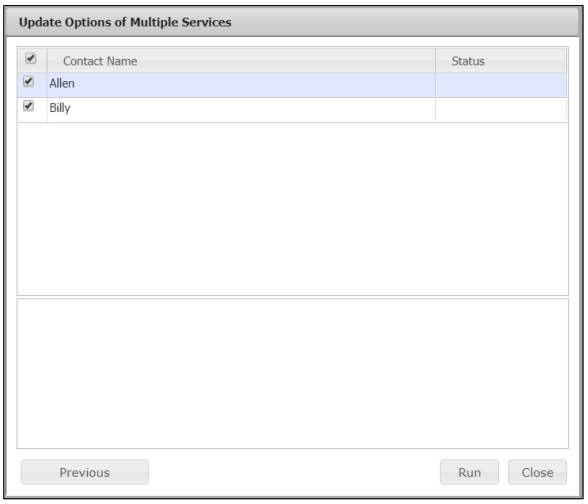


Figure 6-48

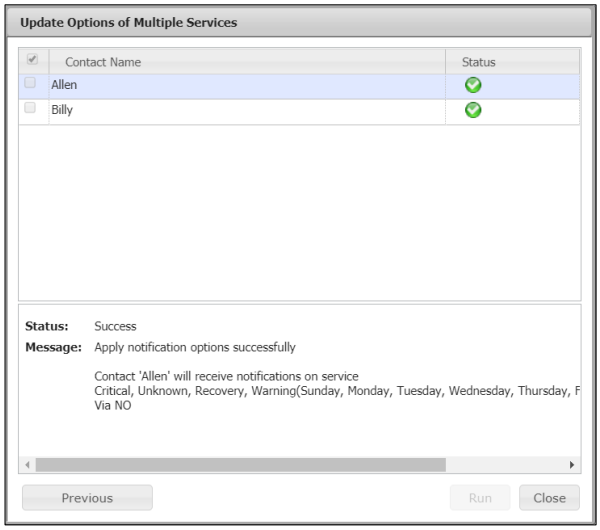


Figure 6-49

4. 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.

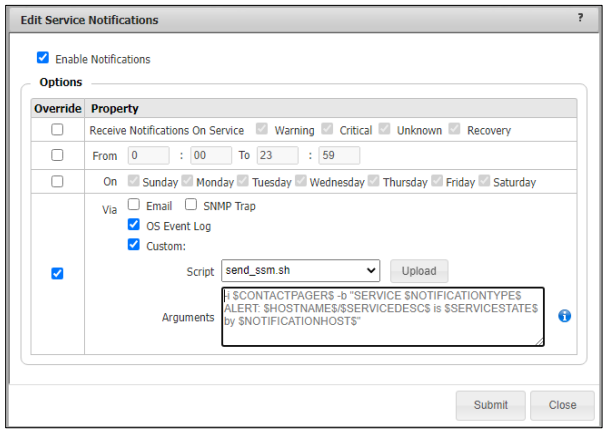


Figure 6-50

5. 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.
6. 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: Email, SNMP Trap, OS Event Log and Custom Script.
   - **Email**: Sends alerts via email. To use this function, you need to set up both the email address for the contact and the email SMTP server for SSM to send email notifications. Please refer to the *6.10 Email 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 demoSSMServer.”

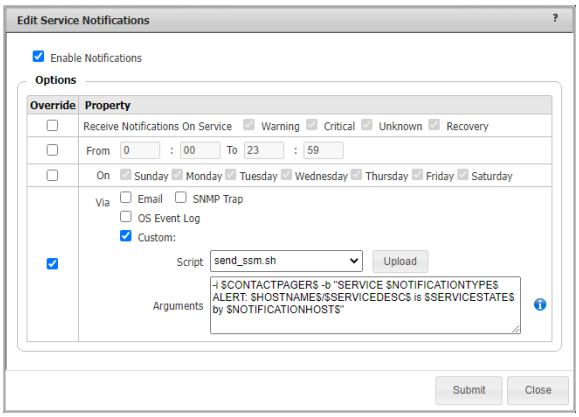


Figure 6-51

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.

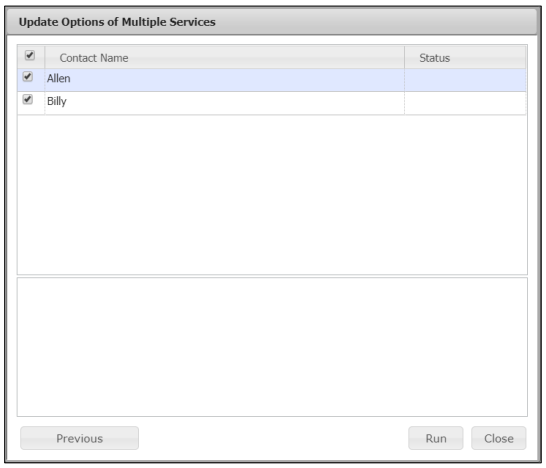


Figure 6-52

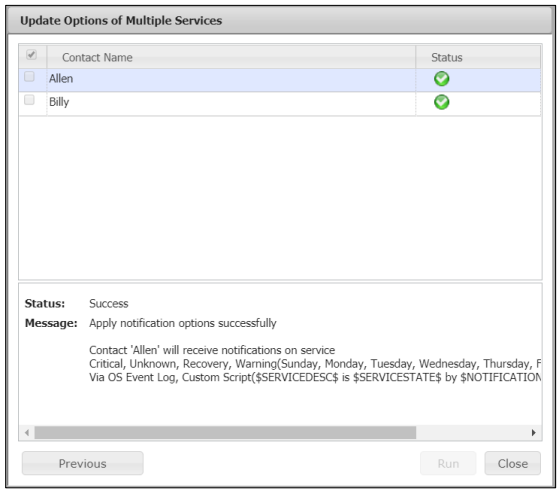


Figure 6-53

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.

Figure 6-54

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.

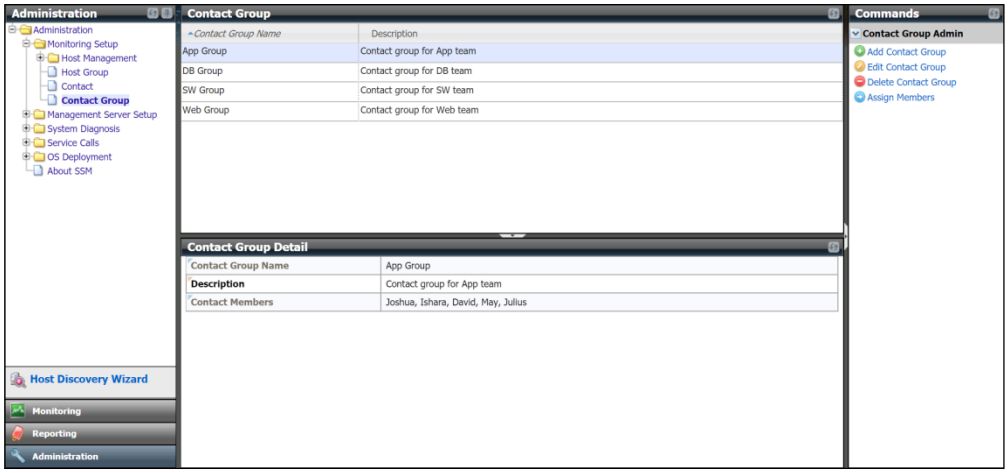


Figure 6-55

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.

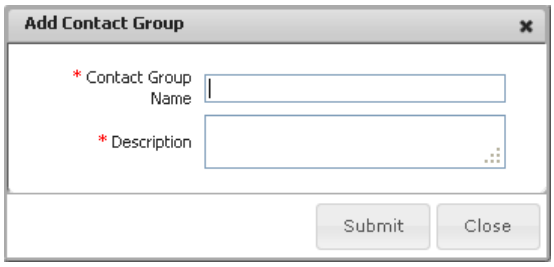


Figure 6-56

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.

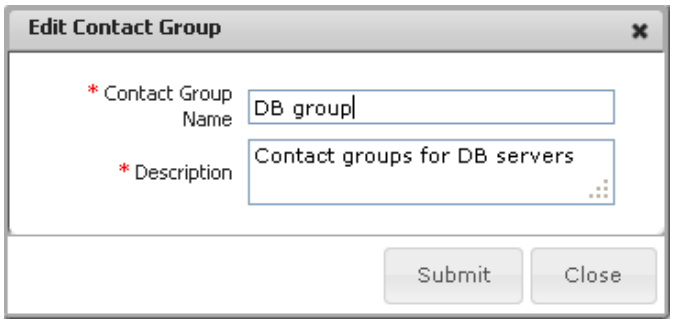


Figure 6-57

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.

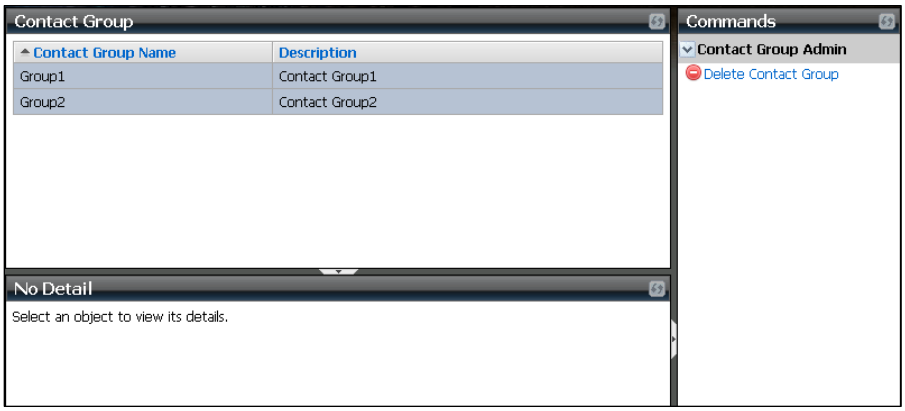


Figure 6-58

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

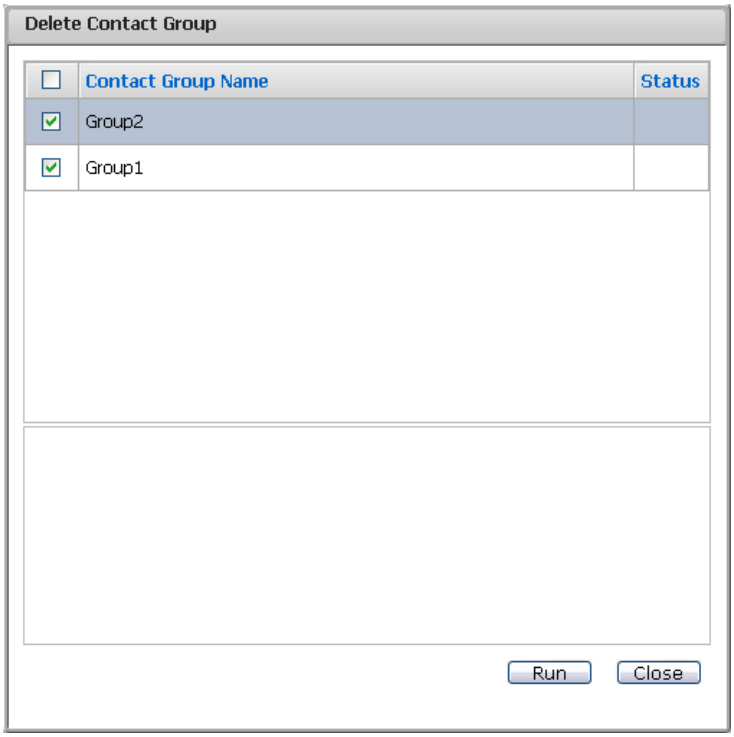


Figure 6-59

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.

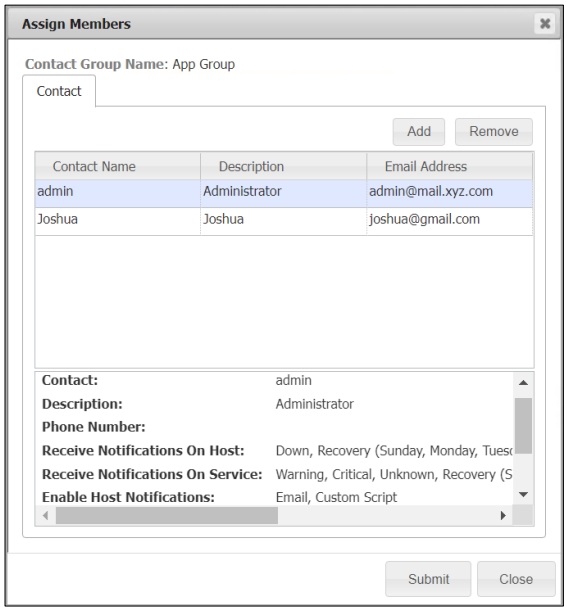


Figure 6-60

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.

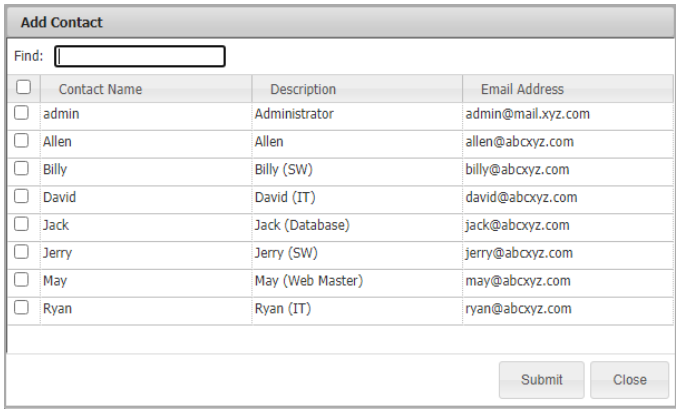


Figure 6-61

6.6 Node PK Activation

Before using SSM functions, both IPMI hosts and Redfish hosts need to be activated. You only need to activate the product key of a host once, for the product key is bound with the MAC address of the BMC LAN port. If the MAC address is changed, the product key is then void. The **Node PK Activation** page allows you to activate numerous product keys from a file. Two types of license key formats are supported:

- **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 *6.2.4 Checking Activation Status.*
- SFT-DCMS-SINGLE and SFT-SUM-LIC product keys only support X10 series and later generations of Supermicro motherboards.

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

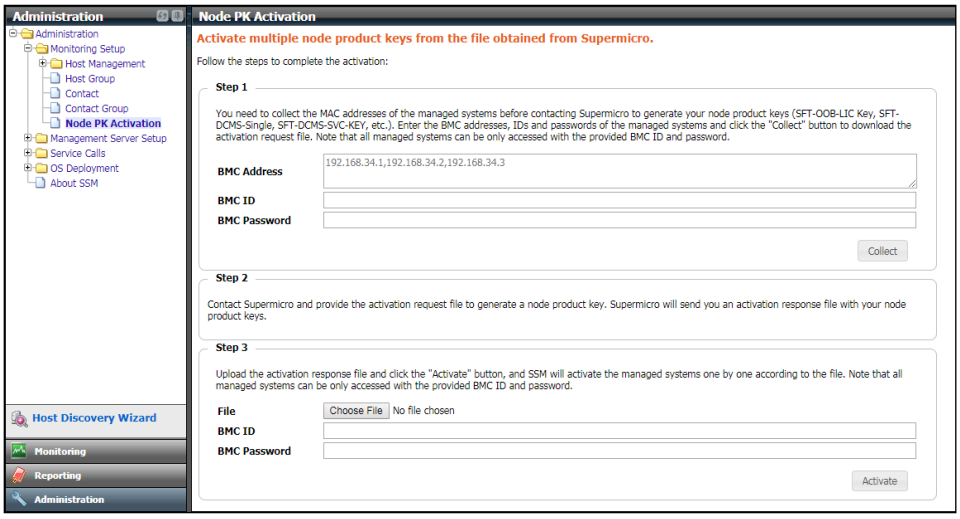


Figure 6-62

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.

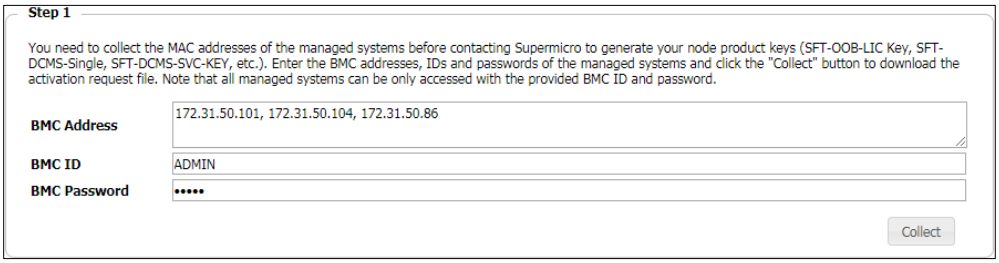


Figure 6-63

(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.

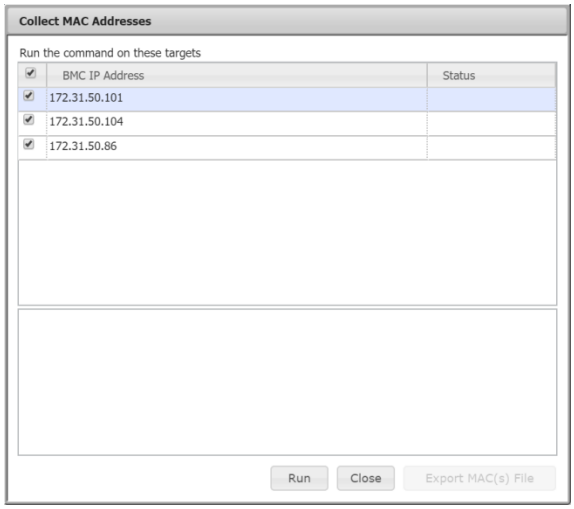


Figure 6-64

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

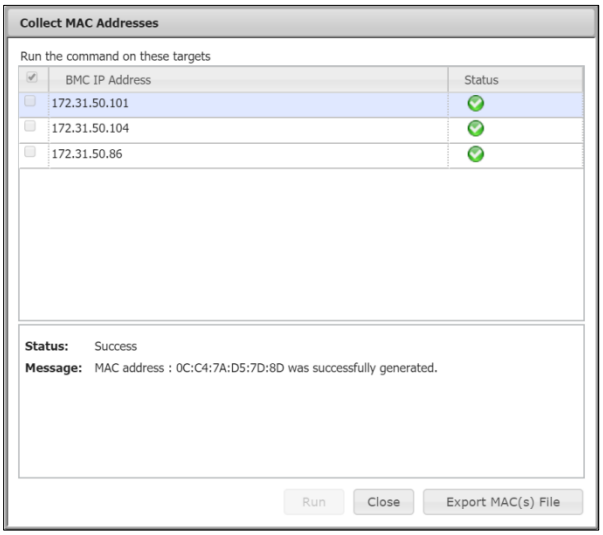


Figure 6-65

Example:

0CC47AD57D8D;172.31.50.101

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

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

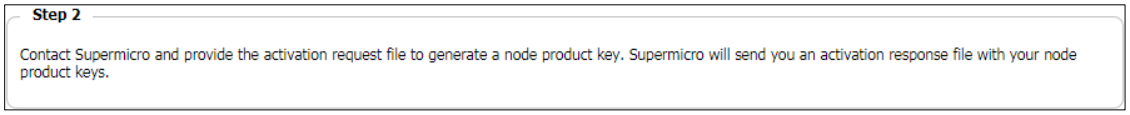


Figure 6-66

Example:

0CC47AD57D8D;172.31.50.101;AAkAAAAAAAAAAAAAAAAAMjnO7OIeNNWpc63TFto8dp6A5UrXzkBpQdkhtnMrUR/oTFKIdhLPpIi6b32lQJFaoPly7uj2OztgzUxjKy1kdMDrEEFra1KlLDrBoZC88fAWfuVXmnVBhjR7tNKSa4r29owr8M3ETun+GxqerDT8kDa+jafMEkETjDJ2Gln6sk7oRCLA7xVZhG1RfkyjcrO+qyYL4OOHH8GG8CUTDx/dlBCXH8i3TL3g5d7X8U/B2XO/z85JUWOeVgwEzUXxK0eN5l3ub/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 ("SSM_mymacs.txt"), fill in the BMC ID and BMC Password fields, and then click the **Activate** button.

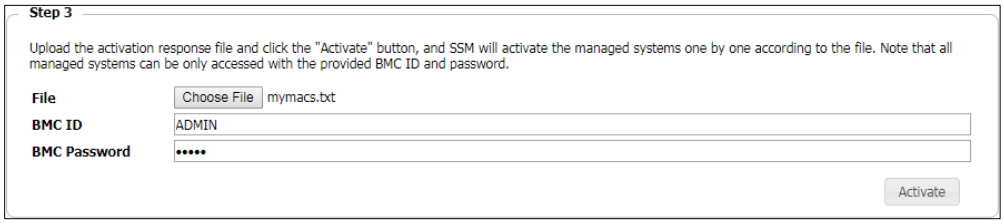


Figure 6-67

(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.

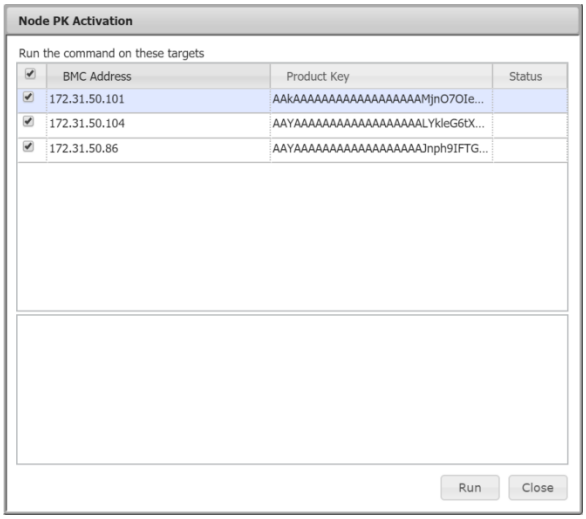


Figure 6-68

(3). Then the activation results are listed.

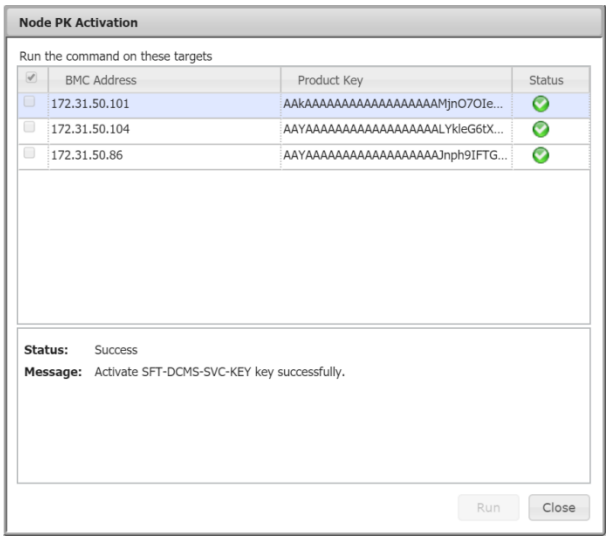


Figure 6-69

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

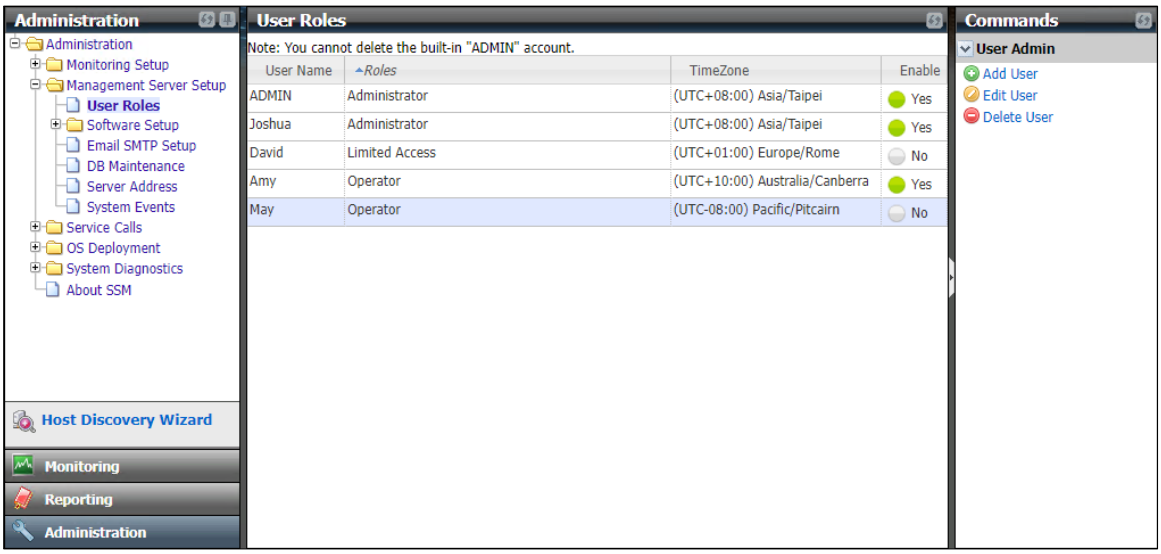


Figure 6-70

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.

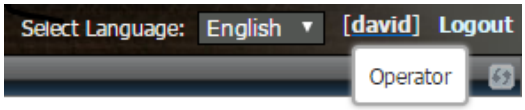


Figure 6-71

Feature	Role		
[Command category] Command	Administrator	Operator	Limited Access
[Monitoring Page] / [Agent Managed]			
Graceful Power Off	○	○	
Graceful Reboot	○	○	
Reset Chassis Intrusion	○		
Reset SD5 User Password	○	○	
Update SD5	○	○	
Wake on LAN	○	○	
[Monitoring Page] / [IPMI]			
BMC Cold Reset	○		
Blink UID LED	○		
Change BMC Password	○		
Clear BMC SEL	○		
Clear BMC SEL and BIOS Log	○		
Clear TPM Management	○		
Clear TPM Provision	○		
Deploy OS	○		
Edit DMI Info	○		
Enable TPM Management	○		
Enable TPM Provision	○		
Export Asset Info	○		
Export BIOS Cfg	○		
Export BMC Cfg	○		
Export BMC SEL	○		
Export DMI Info	○		
Export Factory BIOS Cfg	○		
Export System Utilization	○		
Graceful Power Off	○	○	
Import BIOS Cfg	○		
Import BMC Cfg	○		
Import DMI Info	○		
Load Factory BIOS Setting	○		

Feature	Role		
Load Factory BMC Setting	○		
Mount ISO Image	○		
Power Off	○	○	
Power On	○	○	
Power Reset	○	○	
Recover BIOS from Backup	○		
Recover BMC from Backup	○		
Reset Chassis Intrusion	○		
Stop Blinking UID LED	○		
Sync Node PK	○		
Unmount ISO Image	○		
Update BIOS (Capsule)	○		
Update BMC	○		
Update Golden BIOS	○		
Update Golden BMC	○		
[Monitoring Page] / [Redfish]			
BMC Cold Reset	○		
Blink UID LED	○		
Change BMC Password	○		
Clear BMC SEL	○		
Deploy OS	○		
Diagnose System	○		
Disable System Lockdown	○		
Edit BMC Setting	○		
Edit DMI Info	○		
Enable System Lockdown	○		
Export BMC SEL	○		
Export BMC MEL	○		
Graceful Power Off	○	○	
Load Factory BIOS Settings	○		
Load Factory BMC Settings	○		
Mount ISO Image	○		
Perform Memory Self-Healing	○		
Power Off	○	○	

Feature	Role		
Power On	○	○	
Power Reset	○	○	
Recover BIOS from Backup	○		
Recover BMC from Backup	○		
Reset Chassis Intrusion	○		
Secure Erase	○		
Stop Blinking UID LED	○		
Sync Node PK	○		
Unmount ISO Image	○		
Update BIOS (Capsule)	○		
Update BMC	○		
Update Golden BIOS	○		
Update Golden BMC	○		
[Monitoring Page] / [CMM IPMI]			
BMC Cold Reset	○		
Blink UID LED	○		
Change BMC Password	○		
Clear BMC SEL	○		
Export CMM Cfg	○		
Import CMM Cfg	○		
Load Factory CMM Setting	○		
Stop Blinking UID LED	○		
Turn Blade UID On/Off	○		
Update CMM	○		
[Monitoring Page] / [CMM Redfish]			
BMC Cold Reset	○		
Blink UID LED	○		
Change BMC Password	○		
Clear BMC SEL	○		
Load Factory CMM Setting	○		
Stop Blinking UID LED	○		
Turn Blade UID On/Off	○		
Update CMM	○		
[Monitoring Page] / [Power Management]			

Feature	Role		
Power Consumption Trend	○	○	○
Power Policy Management	○	○	
[Monitoring Page] / [System Information]			
View Details	○	○	○
[Monitoring Page] / [Remote Control]	○	○	
[Monitoring Page] / [Host Admin]	○		
[Monitoring Page] / [Reports]	○	○	○
[Monitoring Page] / [Service Admin]			
Service Properties	○		
Notification Properties	○		
Change Arguments	○		
Assign Contact and Contact Group	○		
Check Now	○		
Delete Service	○		
Performance Data	○	○	○
[Reporting Page]	○	○	○
[Administration Page]	○		

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.

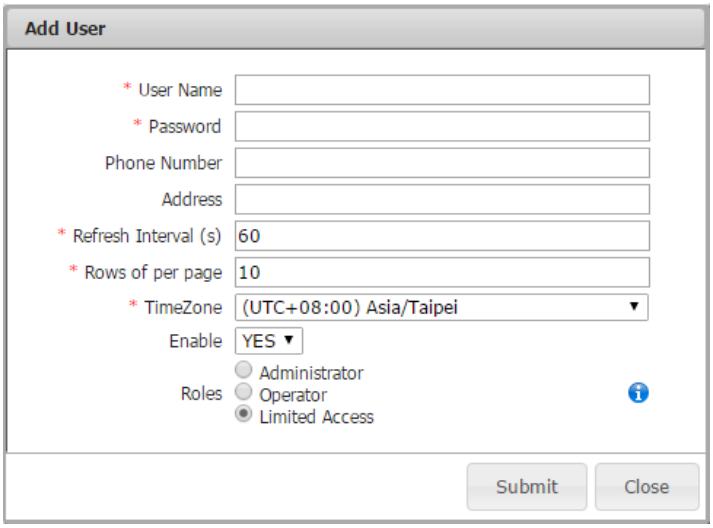


Figure 6-72

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.

Note: The maximum length of a user name is 50 characters.

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.

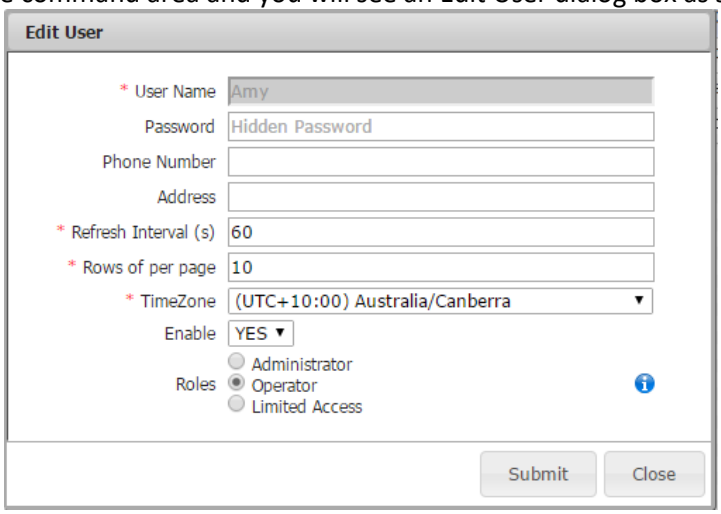


Figure 6-73

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.

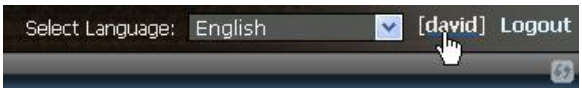


Figure 6-74

6.7.3 Deleting a User

1. Select users to be deleted in the working area. You can delete multiple users at a time[4].

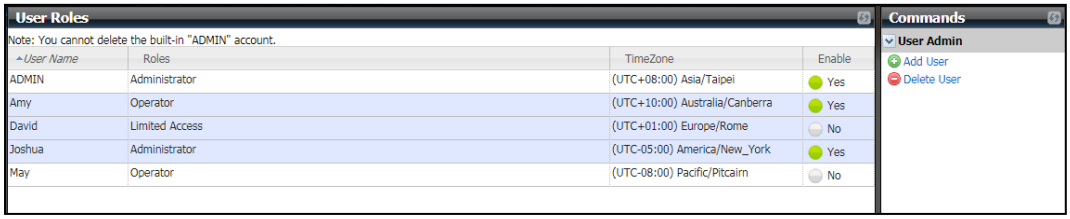


Figure 6-75

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

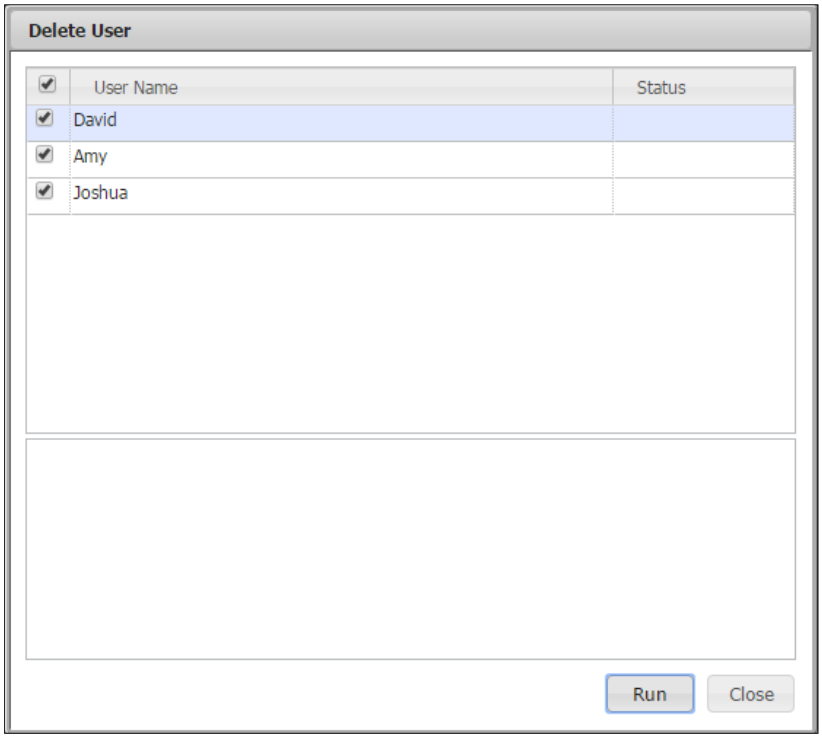


Figure 6-76

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

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

6.8 Directory Services

The **Directory Service** function allows SSM to contact Lightweight Directory Access Protocol (LDAP) services or Active Directory (AD) services to validate the user. You could click **SSM New GUI** on the top toolbar → **Configuration** → **User Account** to perform the **Directory Service** function.

The **LDAP Service** page is by default shown with four panes of settings that are: **Directory Service Setting**, **Static Server Setting / Domain Controller Setting**, **Search Options,** and **Group Mapping**. Besides the setting information, the page also provides the **LDAP Service Test** pane to test overall settings.

The **AD Service** tab is similar to the **LDAP Service** tab, it shows three panes of settings: **Directory Service Setting**, **Static Server Setting / Domain Controller Setting**, and **Group Mapping**. The **AD Service Test** pane is for testing above **AD Service** settings.

If configured, you can use your LDAP/AD accounts to log into SSM. SSM searches the account in the directory servers one at a time until the login user is found or all of the enabled servers are searched. Besides local users, only accounts found in LDAP/AD are allowed to access SSM.

6.8.1 Prerequisites

To integrate AD/LDAP in SSM, make sure your AD/LDAP server meet these requirements:

- Your LDAP server must implement LDAPv3 (LDAP version 3).
- The StartTLS (LDAP over TLS) is supported for secure connection and the port is 389 by default. Note that SSM does **NOT** support LDAPS communication. For the LDAP over SSL, the default port is 636.
- Simple Authentication method is configured for LDAP Authentication (by default).

6.8.2 Configuring Directory Services

To use LDAP, make necessary configurations on the four panes.

- **Directory Service Setting**: Shows two toggles for the DNS Lookup setting and the Local User setting.
- **Static Server Setting / Domain Controller Setting**: Shows a table of servers that are either static or domain controlled. The **Static Server Setting** pane is available when the DNS Lookup is disabled, otherwise, the **Domain Controller Setting** pane is available. In the upper right corner of the table, users are able to manage servers, such as add, edit, delete, and change search orders. The table also has the Enable column toggle for you to enable or disable a setting.
- **Search Options**: Shows the LDAP user and group search criteria. It is used to identify the login user and the group the login user belongs to.
- **Group Mapping**: Shows the mapping between the SSM role and the LDAP group. It is used to identify the role of the group the login user belongs to.

Once the above configuration is completed, you could use **LDAP Service Test** to test if an LDAP server setting is correct for a login account.

To use AD, make necessary configurations on the three panes.

- **Directory Service Setting**: Shows two toggles for the DNS Lookup setting and the Local User setting.
- **Static Server Setting / Domain Controller Setting**: Shows a table of servers that are either static or domain controlled. The **Static Server Setting** pane is available when the DNS Lookup is disabled, otherwise, the **Domain Controller Setting** pane is available. In the upper right corner of the table, users are able to manage servers, such as add, edit, delete, and change search orders. The table also has the Enable column toggle for you to enable or disable a setting.
- **Group Mapping**: Shows the mapping between the SSM role and the AD group. It is used to identify the role of the group the login user belongs to.

Once the above configuration is complete, you could use **AD Service Test** to test if an AD server setting is correct for a login account.

6.8.3 Configuring Directory Service Setting

Two fields are on the Directory Service Setting pane:

- **DNS Lookup setting**: LDAP or AD servers are either static or domain-controlled. If the DNS Lookup is enabled, users are able to manage domain-controlled servers, otherwise, only static servers are allowed. By default, the field is disabled. Note that if you disable the DNS lookup, all domain-controlled servers you have added before will be cleared immediately, and vice versa.
- **Local User setting**: By default, SSM will allow local users to log into SSM even if the directory service is configured. The field is for users to enable or disable local users. Note that if you disable local users before properly configuring directory services, you will not be able to log into SSM.

6.8.3.1 Configuring Directory Service Setting

Enabling the DNS Lookup so that directory servers could be retrieved through DNS with given domain names.

Follow these steps to enable the DNS lookup.

1. When the **DNS Lookup** is disabled, click the **Edit** icon in the upper right corner of the **Directory Service Setting** pane, then the Editing mode is switched on.

2. Toggle from Disabled to **Enabled** in the DNS Lookup field, a confirmation dialog box will appear.

3. Click **Yes** to continue or **No** to abort and close this dialog box.

4. After clicking the **Save** icon in the upper right corner, the DNS Lookup is enabled. Otherwise, click the **Cancel** icon to abort.

To disable the DNS Lookup, the procedure is similar to that of enabling DNS Lookup procedure.

Note: After enabling the DNS Lookup, all static AD/LDAP servers you have added before will be cleared immediately, and vice versa.

6.8.4 Configuring Server Setting

6.8.4.1 Adding a Domain Controller Setting for LDAP Service

1. Ensure the **DNS Lookup** field is enabled in the **Directory Service Setting** pane**.**

2. Click the **Add Domain Controller Setting** icon in the upper right corner of **Domain Controller Setting** pane and the **Add Domain Controller Setting** dialog will pop up.

3. Input the domain controller setting in this dialog box. A domain controller setting is determined by the following attributes:

Setting Name	A unique name used to identify the setting.
Domain	The domain name of the LDAP servers. Only a DNS name (FQDN) can be specified.
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 that SSL (LDAPS; LDAP over SSL) connection is not supported.**
Allow Anonymous Access	Toggles whether the Bind requires a Distinguished Name (DN) as well as a password.
Bind DN	Connects to the directory server. Note that the Bind DN user should have permission to retrieve LDAP user and group entries.
Bind Password:	Connects to the LDAP server.

4. Click the **Test Connection** button to check if the server setting is correct. If you select a TLS connection between SSM and the LDAP server, you must install the certificate first. An **Install Certificates** dialog box pops up. Read the certificate carefully and click **Install** to continue the installation or click **Cancel** to abort. Click **Next** if more than one LDAP server is registered within one domain.

5. After the certificate(s) is installed, you can view the certificate information in the **Certificate List**

area. The host in the **Issued To** field indicates the LDAP server. If the encrypted connection is not established or the certificate's hostname does not match the hostname in the dialog box, an error message will appear in the dialog box after the **Test Connection** button is clicked**.**

6. Click the **Save** button to add the setting or the **Cancel** button to abort and close this dialog box. Note that the connection status will be verified before saving the setting.

6.8.4.2 Adding a Domain Controller Setting for AD Service

1. Ensure the **DNS Lookup** field is enabled in the **Directory Service Setting** pane**.**

2. Click the **Add Domain Controller Setting** icon in the upper right corner of the **Domain Controller Setting** pane and the **Add Domain Controller Setting** dialog will appear.

3. Input the domain controller setting in this dialog box. A domain controller setting is determined by the following attributes:

Setting Name	A unique name used to identify the setting.
Domain	The domain name of the AD servers. Only a DNS name (FQDN) can be specified.
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.
Bind DN	Connects to the AD server.
Bind Password	Connects to the AD server.

4. Click the **Test Connection** button to check if the server setting is correct. If you select a TLS connection between SSM and the AD server, you must install the certificate first. An **Install Certificates** dialog box appears. Read the certificate carefully and click **Install** to continue the installation or click **Cancel** to abort. Click **Next** if more than one AD server is registered within one domain.

5. After the certificate(s) is installed, you can view the certificate information in the **Certificate List** area. The host in the **Issued To** field indicates the AD server. If the encrypted connection is not established or the certificate's hostname does not match the hostname in the dialog box, an error message appears in the dialog box after the **Test Connection** button is clicked**.**

6. Click the **Save** button to add the setting or the **Cancel** button to abort and close this dialog box. Note that the connection status will be verified before saving the setting.

6.8.4.3 Adding a Static Server Setting for LDAP Service

1. Ensure the **DNS Lookup** field is disabled in the **Directory Service Setting** pane**.**

2. Click the **Add Static Server Setting** icon in the upper right corner of **Static Server Setting** pane and the **Add Static Server Setting** dialog will pop up.

3. Input the LDAP server setting in this dialog box. A static LDAP server setting is determined by the following attributes:

Setting Name:	A unique name used to identify the LDAP 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. Usually, it's 389 as this port can be used in both unsecure (security type: NONE) and secure (security type: TLS) transmissions.
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 that SSL (LDAPS; LDAP over SSL) connection is not supported.**
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. Note that the Bind DN user should have permission to retrieve LDAP user and group entries.
Bind Password:	Used to connect to the LDAP server.

4. Click the **Test Connection** button to check if the server setting is correct. If you select a TLS connection between SSM and the LDAP server, you must install the certificate first. An **Install Certificate** dialog box pops up. Read the certificate carefully and click **Install** to continue the installation or click **Cancel** to abort.

5. After the certificate is installed, you can view the certificate information in the **Certificate** area. The host in the **Issued To** field indicates the LDAP server. If the encrypted connection is not established or the certificate's hostname does not match the hostname in the dialog box, an error message appears in the dialog box after the **Test Connection** button is clicked.

Click the **Save** button to add the setting or the **Cancel** button to abort and close this dialog box. Note that the connection status will be verified before saving the setting.

6.8.4.4 Adding a Static Server Setting for AD Service

1. Ensure the **DNS Lookup** field is disabled in the **Directory Service Setting** pane**.**

2. Click the **Add Static Server Setting** icon in the upper right corner of **Static Server Setting** pane and the **Add Static Server Setting** dialog will pop up.

3. Input the AD server setting in this dialog box. A static AD server setting is determined by the following attributes:

Setting Name:	A unique name used to identify the AD 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 AD server, only FQDN can be specified.
Domain:	The domain name of the AD server. It should be following the FQDN naming rule.
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.
Bind DN:	Connects to the AD server.
Bind Password:	Connects to the AD server.

4. Click the **Test Connection** button to check if the server setting is correct. If you select a TLS connection between SSM and the AD server, you must install the certificate first. An **Install Certificate** dialog box pops up. Read the certificate carefully and click **Install** to continue the installation.

5. After the certificate is installed, you can view the certificate information in the **Certificate** area. The host in the **Issued To** field indicates the AD server. If the encrypted connection is not established or

the certificate's hostname does not match the hostname in the dialog box, an error message appears in the dialog box after the **Test Connection** button is clicked.

6. Click the **Save** button to add the setting and close this dialog box. Note that the connection status will be verified before saving the setting.

6.8.4.5 Editing a Server Setting

Follow these steps to edit one **Static Server Setting**.

1. Select one setting in **Static Server Setting** pane.
2. Click the **Edit Static Server Setting** icon in the upper right corner and the **Edit Static Server Setting** dialog will pop up.
3. Modify the server setting in this dialog box.
4. Click the **Save** button to modify the setting and close this dialog box. Note that the connection status will be verified before saving the setting.

To edit the **Domain Controller Setting**, the procedure is similar to edit the **Static Server Setting**.

6.8.4.6 Deleting a Server Setting

Follow these steps to delete **Static Server Settings**.

1. Select one or more settings in the **Static Server Setting** pane.
2. Click the **Delete Static Server Setting** icon in the upper right corner and the **Delete Static Server Setting** dialog will pop up.
3. Click the **Run** button to delete the selected settings.

To delete the **Domain Controller Setting**, the procedure is similar to delete the **Static Server Setting**.

6.8.4.7 Changing the Enable Status of a Server Setting

The **Enable** column in the **Domain Controller Setting** or **Static Server Setting** pane indicates the enabled status of the server setting. Only enabled server settings will be used to look for the login user.

To enable or disable the server setting, click the **Enable** column toggle to change the status.

6.8.4.8 Changing the Search Order of a Server Setting

The **Search Order** column in the **Domain Controller Setting** or **Static Server Setting** pane shows the search priority of the server setting. To give a higher priority to the server setting, select one setting in the pane table, and click **Grant Higher Search Order** icon in the upper right corner. To give a lower priority to the server setting, select one setting in the pane table, and click the **Grant Lower Search Order** icon in the upper right corner. You can only select one server setting 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.

6.8.5 Configuring User and Group Search Criteria

The **Search Options** and **Group Mapping** pane in **LDAP Service** and the **Group Mapping** pane in **AD Service** tab are 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: The configuration of group mapping in AD servers is a subset of that in LDAP servers. The following setting steps are an example of Group Mapping for LDAP servers and will omit the explanation of AD.

- The **Search Options** pane is used to identify the login user and the group the login user belongs to. Note that it's necessary for you to configure the following attributes to ensure the uniqueness of the login user and the group. Otherwise, the login request may fail. Click the **Edit** icon in the upper right corner to edit the **Search Options** and then click the **Save** icon to save the configuration.

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

Below is an example of how an object user in an LDAP server can be mapped to an SSM login user. The upper half of the figure is the LDAP Admin tool for browsing user objects on the LDAP server, while the bottom half shows the configurations of User Search in SSM.

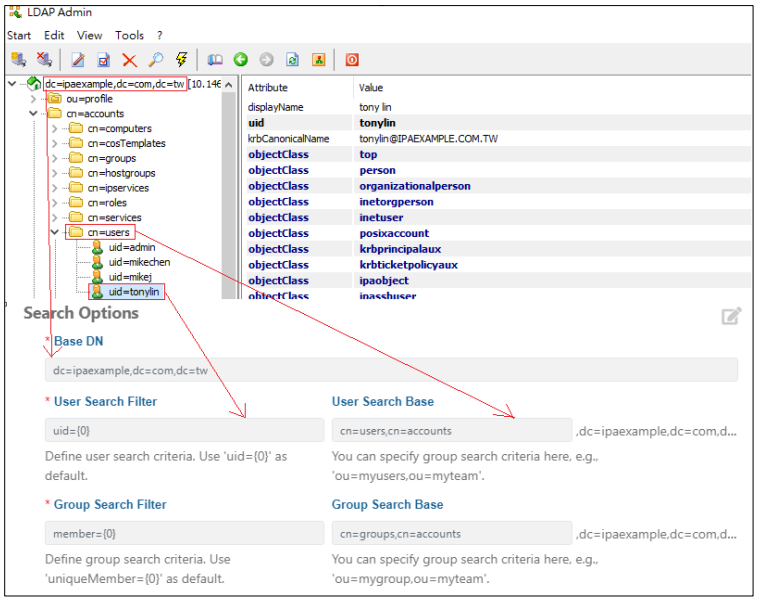


Figure 6-77

Below is an example of how a group object in an LDAP server could be mapped to an SSM login role. The upper half of the figure is the LDAP Admin tool for browsing group objects on the LDAP server, while the bottom half is the configuration of Group Search in SSM.

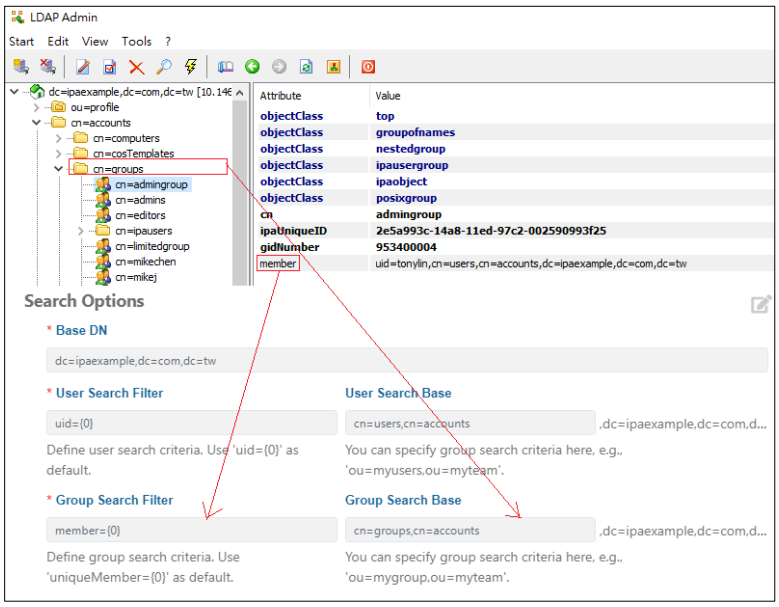


Figure 6-78

Examples of settings for some popular LDAP servers are shown below.

LDAP Servers	User Search Filter	Group Search Filter
OpenLDAP	uid={0}	uniqueMember={0}
Apache Directory	uid={0}	uniqueMember={0}
FreeIPA	uid={0}	member={0}

- The **Group Mapping** pane is used to identify the role of the group the login user belongs to. Note that you must configure the following attributes to ensure the permission a user has. Otherwise, the user may have trouble logging in. Three roles can be configured. Click the **Edit** icon in the upper right corner to edit the **Group Mapping** and then click the **Save** icon to save the configuration.

  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" 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."

6.8.5 Testing Server Settings

LDAP Service Test / **AD Service Test** pane is for a user to test a login account before using the Directory Service function. SSM will check if the user is valid and find the user's role permissions.

Follow these steps to check whether a user is able to log into SSM or not.

1. Input the username in **Login User Name** field and then click the **Test** button.
2. The test result will be displayed in the gray pane.

The following test result shows an example that the account **mike** is found in the LDAP, and it belongs to **ipausers** and **software** of the LDAP. Meanwhile, the assigned roles for **mike** allow it to access SSM as an **Operator**. (If multiple roles are assigned to one single user, the user will have the highest privilege among the other users.)

```
User mike can log in.
Assigned roles: Operator, Limited Access
Owning groups: ipausers, software
```

6.9 Software Update

6.9.1 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.

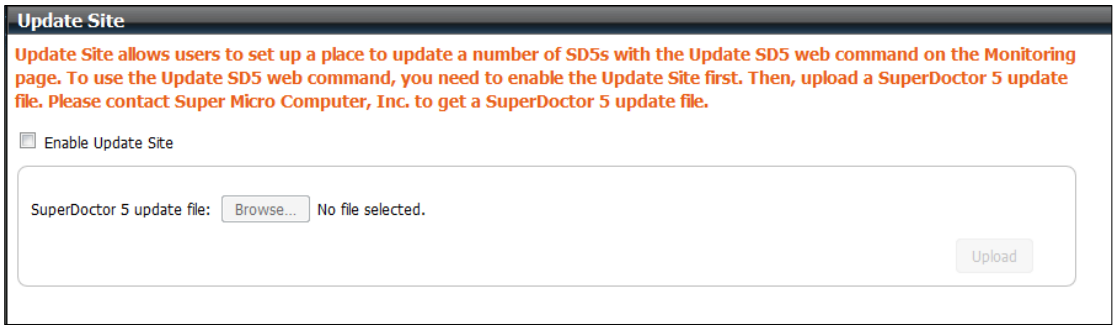


Figure 6-79

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.

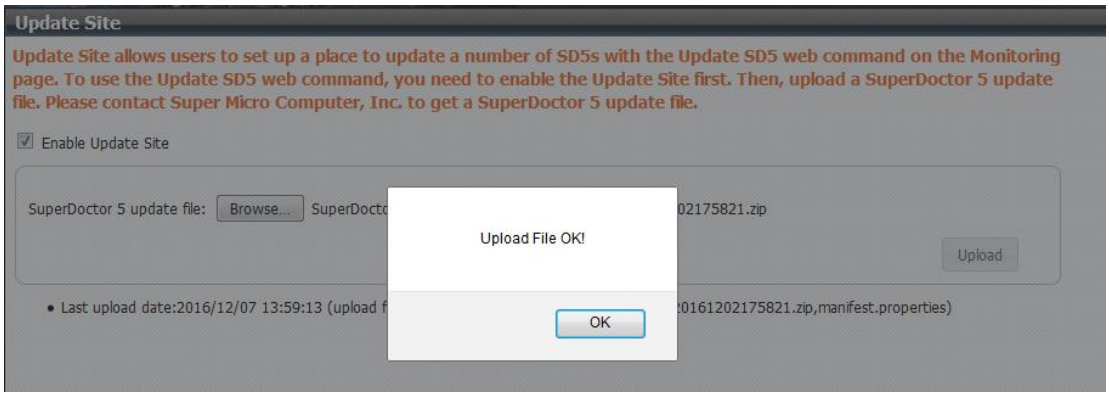


Figure 6-80

6.9.2 Updating SUM through SSM

You can integrate the Supermicro Update Manager (SUM) as check_sum plug-in to SSM to allow you to manage IPMI hosts. For more details, see *Supermicro Update Manager User's Guide* in the **[install folder]\shared\sum\sum** folder. The **Update SUM** function allows you to update the SUM package through SSM.

Currently, the SUM functions integrated to SSM include:

- 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.

Contact Supermicro to get a SUM update file before you begin.

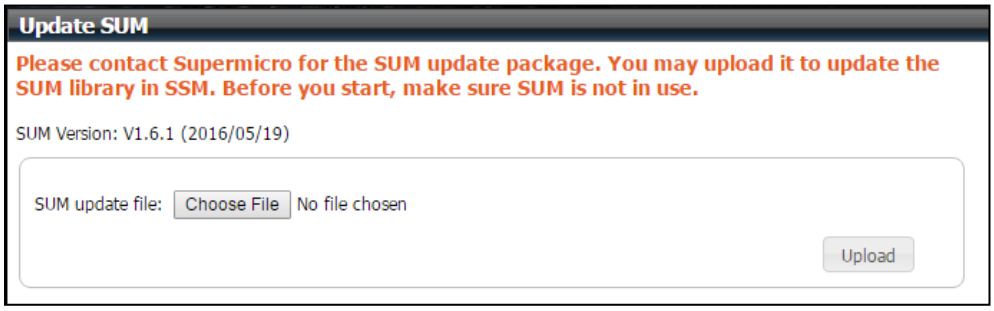


Figure 6-81

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).

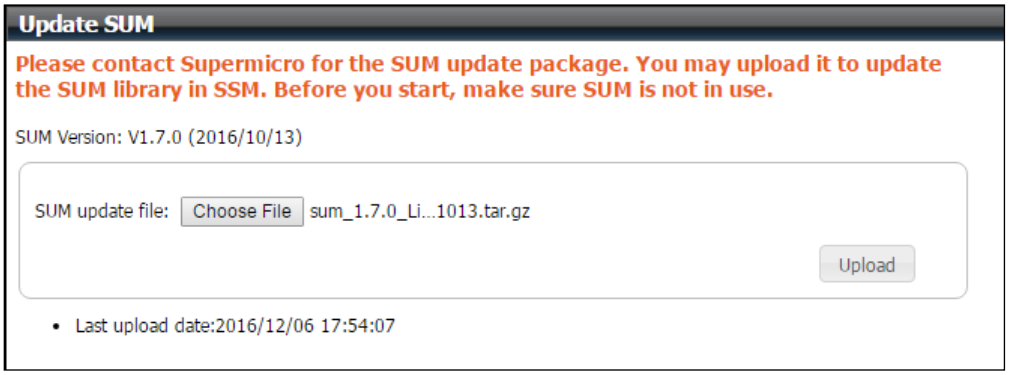


Figure 6-82

6.10 Email SMTP Setup

The **Email SMTP Setup** function allows users to modify the sender's email, 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 email notifications. Note that both SSL and StartTLS provide a secure connection for TLS1.3, 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.

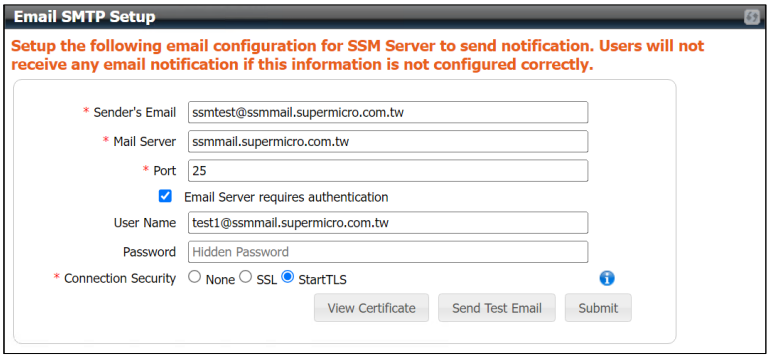


Figure 6-83

If you select an SSL or StartTLS as the type of connection security between SSM and the SMTP server, you need to install the certificate first. When you click the **Send Test Email** button or the **Submit** button, a certificate information dialog box pops up. Read the certificate carefully and click **Install Certificate** to continue the installation or click **Cancel** to abort.

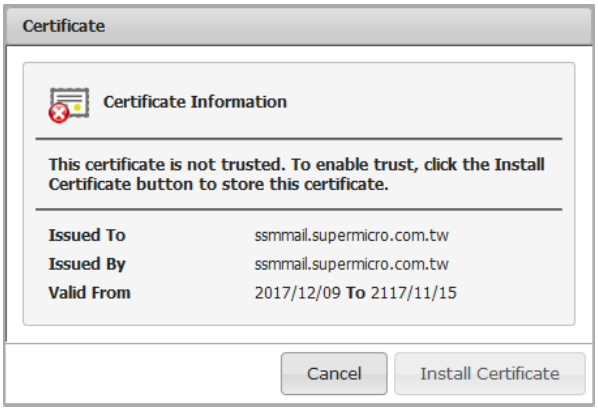


Figure 6-84

After the certificate is installed, you can click **View Certificate** to check the certificate. The host in the Issued To field indicates the SMTP server.

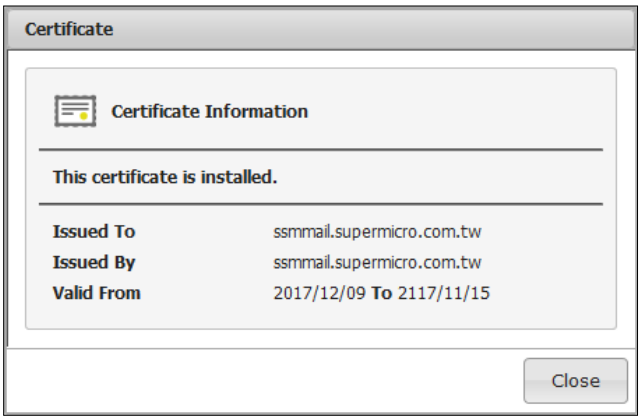


Figure 6-85

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:

- Raw performance data for individual hosts
- Aggregated hourly performance data for individual hosts
- Aggregated daily performance data for individual hosts
- Raw performance data for host groups
- Aggregated hourly performance data for host groups

The table below shows the data retention time periods that can be configured.

	RAW Data	Hourly Data	Daily Data
Retention Time Periods	1-7 day(s)	1-3 month(s)	1-12 month(s)

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.

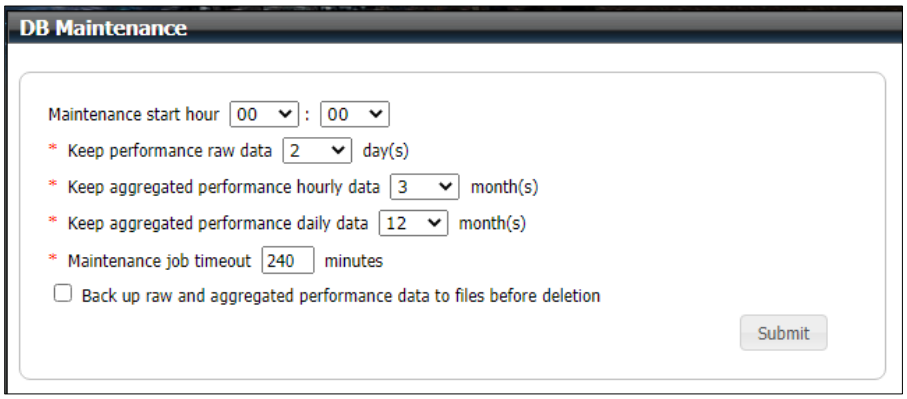


Figure 6-86

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 hourly data**: This argument specifies how many months of the aggregated hourly performance data of hosts and host groups will be kept in the SSM

Database.

- **Keep aggregated performance daily data**: This argument specifies how many months of the aggregated daily performance data of hosts 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 before it times out.

- **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_	INSTANCI	SERVICE_	SERVICEC	NAME	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

servicePerfRawData_20110916_0

Figure 6-87

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.

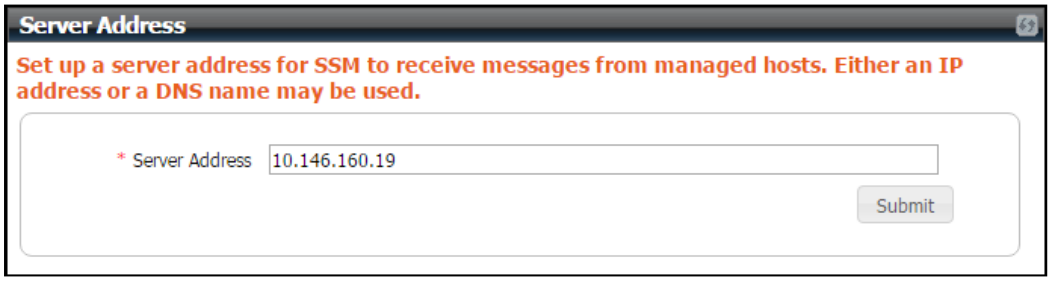


Figure 6-88

6.13 System Events

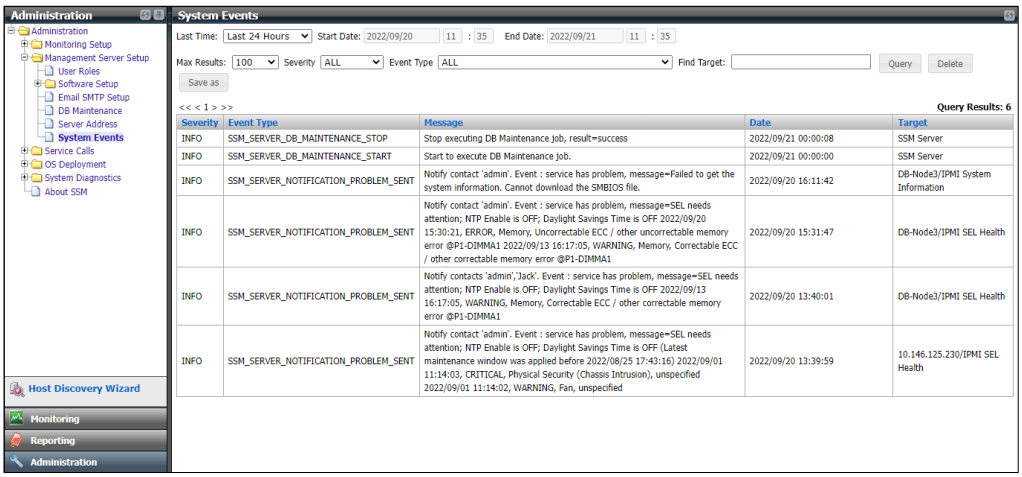


Figure 6-89

The **System Events** function is designed to display SSM system events including events of the SSM Server, and the SSM Web. 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, and the database 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 the creation date. Besides some system information, this page also provides a link for downloading all log files in an all-in-one zip file for the sole purpose of troubleshooting. It might take time to collect logs generated by SSM Web, SSM Server and those from remote BMC hosts.

6.15 Host Discovery Wizard

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

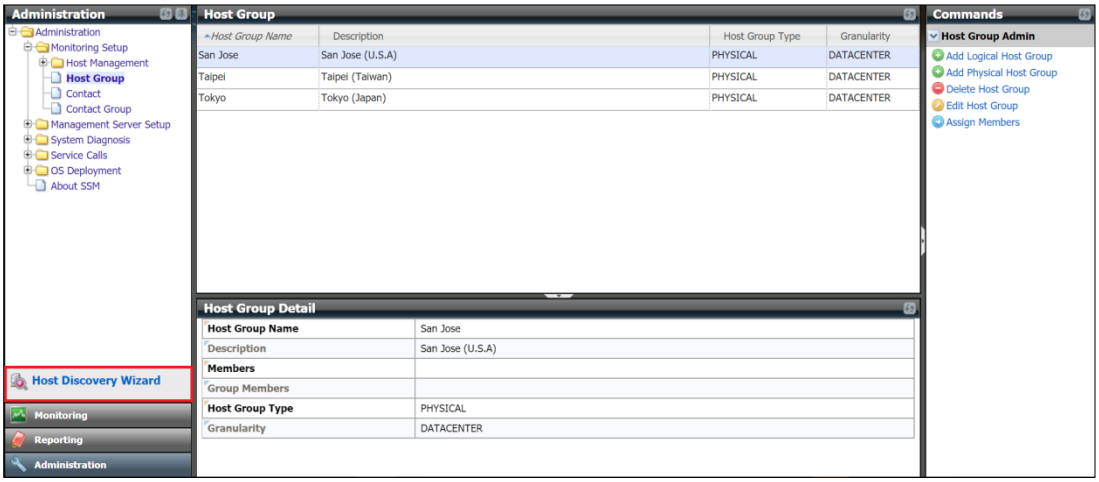


Figure 6-90

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

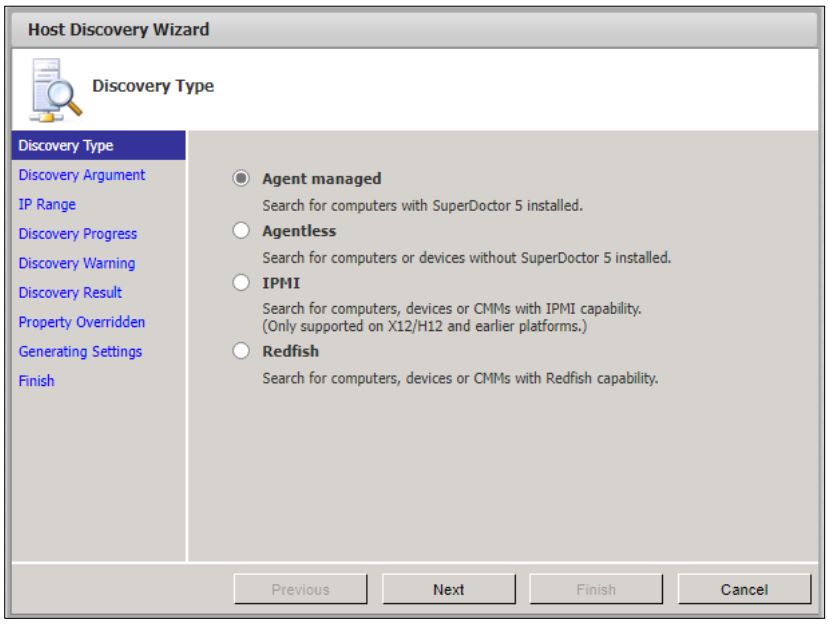


Figure 6-91

3. In the Discovery Argument step, you can set the SuperDoctor 5 port number and BMC ID as well as the password. Note that only accounts with Administrator privileges can perform all Redfish commands. Click the **Next** button to continue.

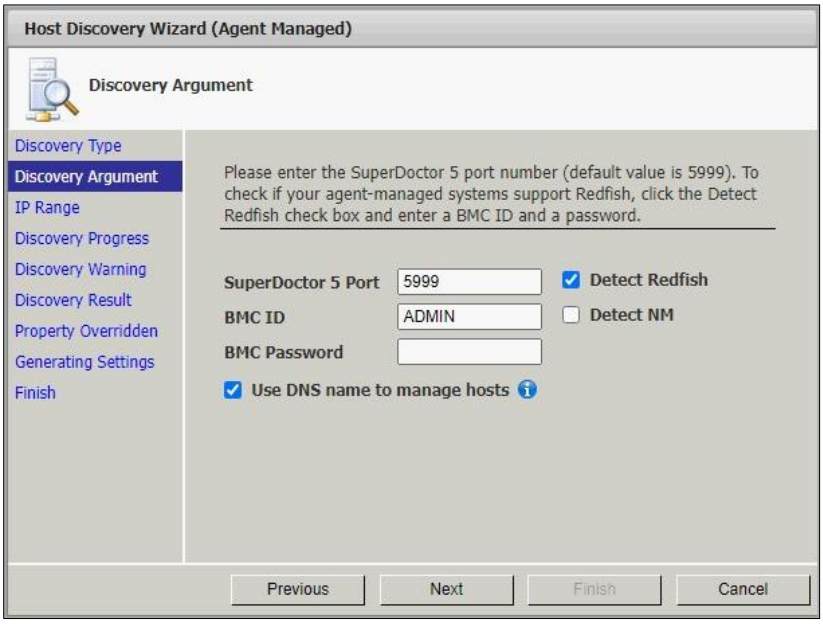


Figure 6-92

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.

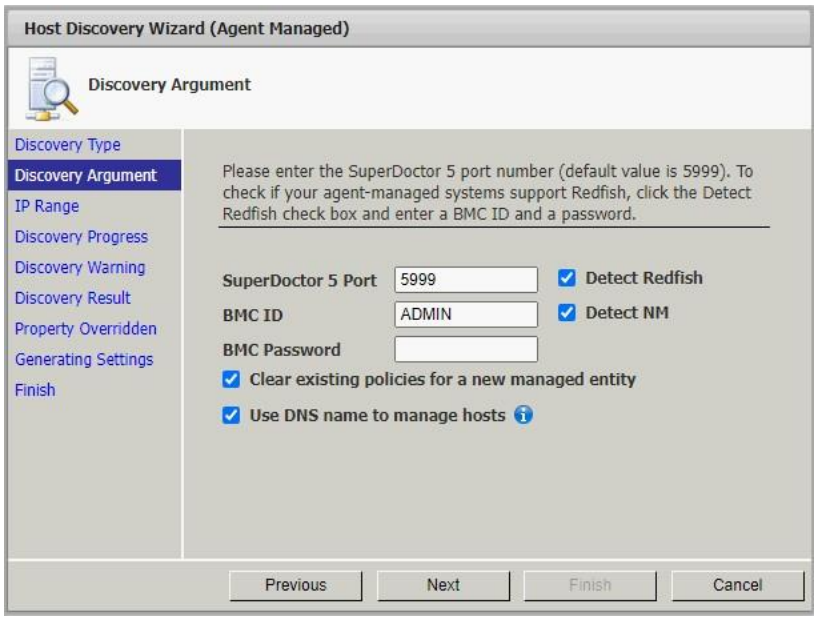


Figure 6-93

If the **Clear existing policies for a new managed entity** checkbox is selected, 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.

Note: To discover a CDU host, click the **Detect CDU** checkbox and enter the ID and Password in the Discovery Argument step of the Agentless host discovery type.

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.

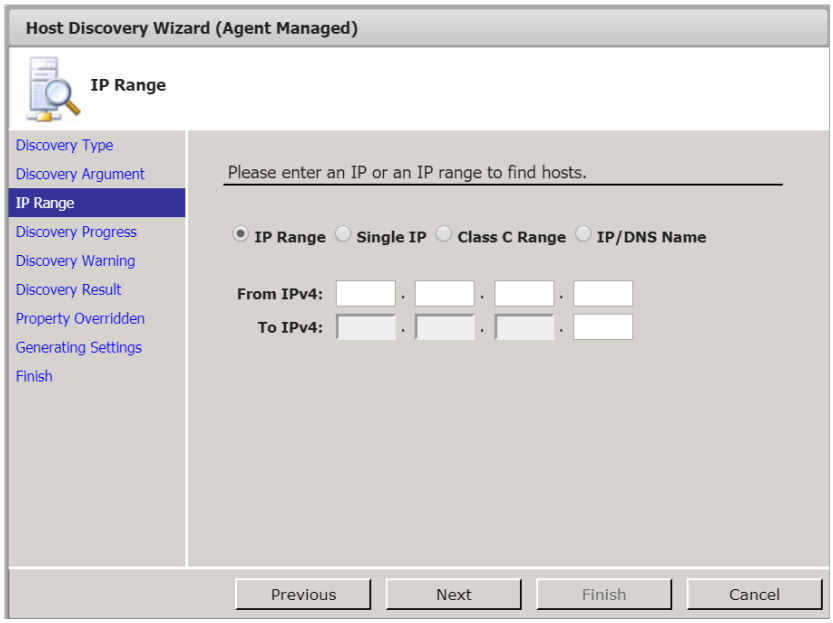


Figure 6-94

5. Please wait while the Discovery Wizard searches.

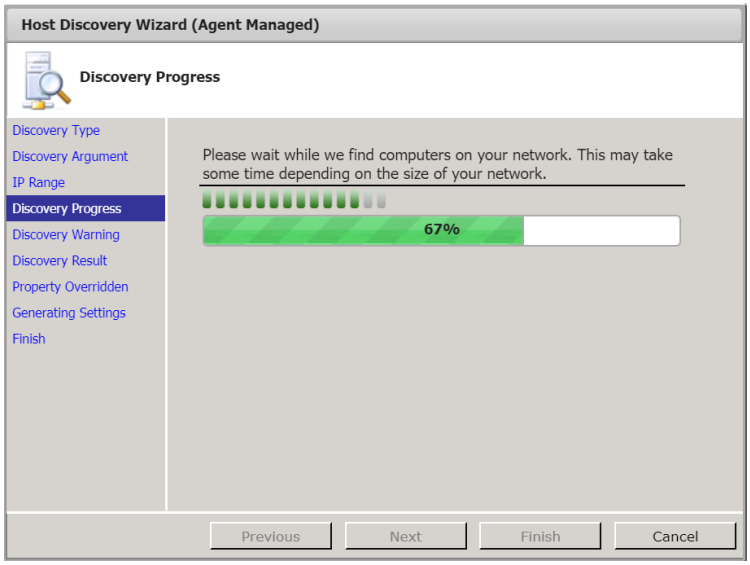


Figure 6-95

6. The currently unavailable hosts are then listed.

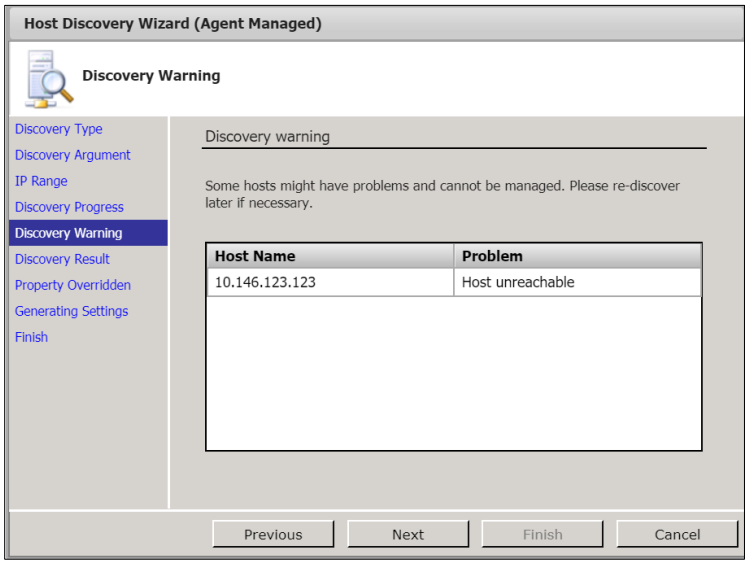


Figure 6-96

7. Select the hosts to be monitored by SSM. Note that if an agent-managed host supports Redfish, the BMC IP address is shown in the BMC column. Otherwise, “None” is shown in the BMC column. If a host with a BMC IP address supports the Node Product Key and the Node Product Key is activated, “Yes” is shown in the Node PK column. The green icon in the Valid BMC field indicates that the BMC ID and password are valid.

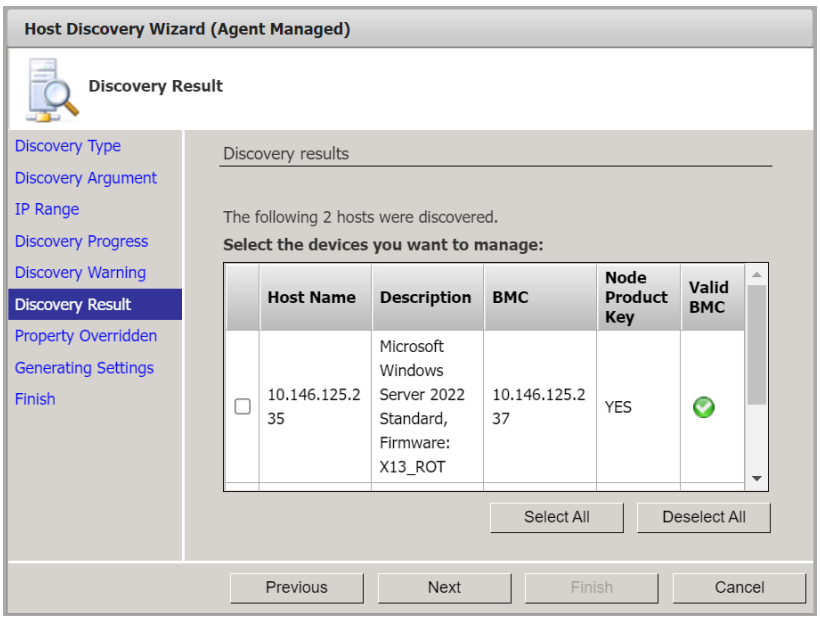


Figure 6-97

Note: In the Discovery Type step, when the IPMI or Redfish option is selected for CMM host discovery, all blade nodes managed by the CMM you provided in the IP Range step will also be automatically discovered. You do not need to specify blade nodes for host discovery. For CMM-6 and later generations, this function is only available when the Redfish option is selected.

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

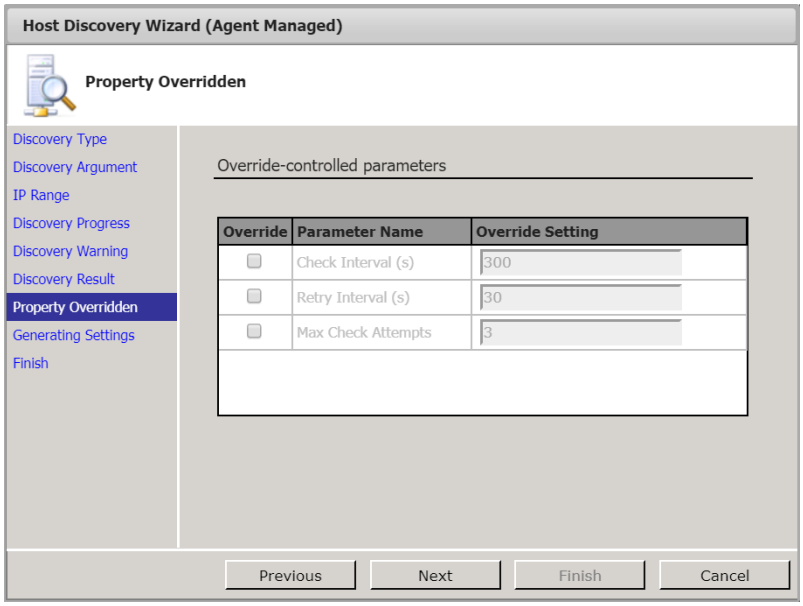


Figure 6-98

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

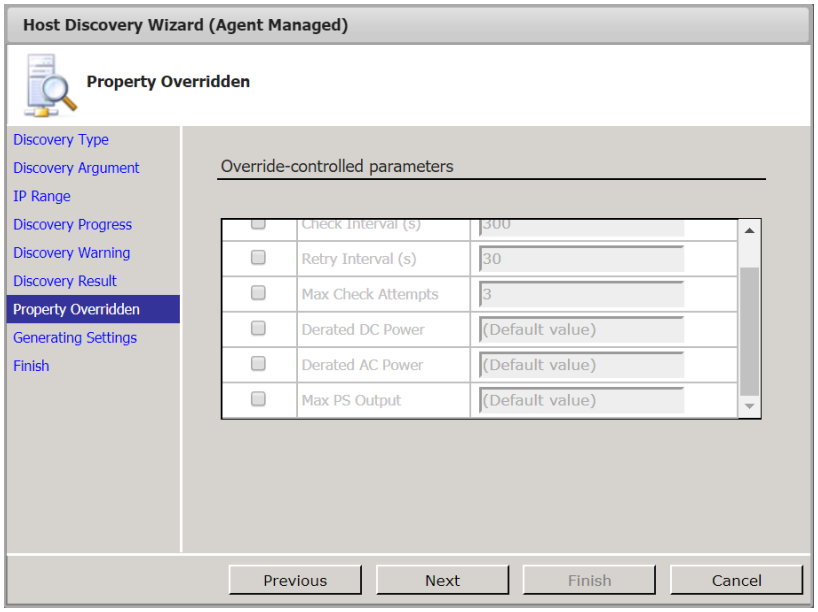


Figure 6-99

9. Please wait while SSM generates the settings.

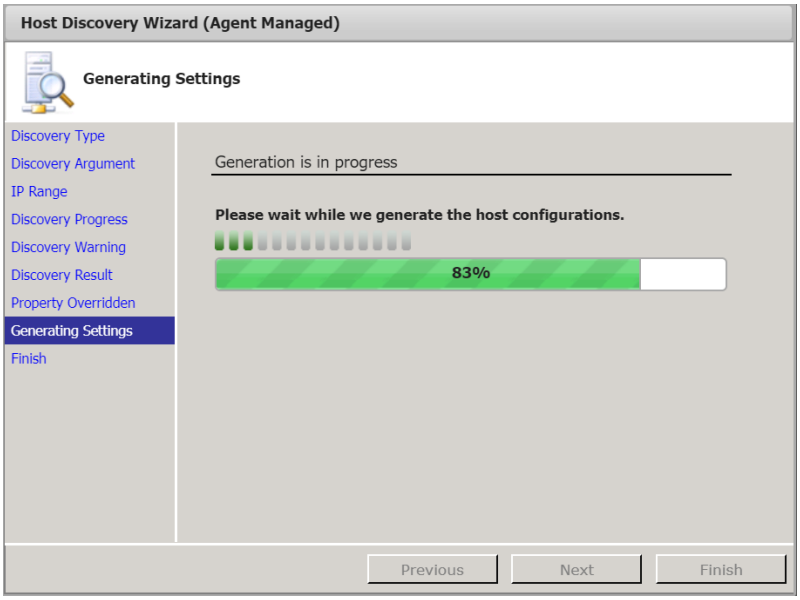


Figure 6-100

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

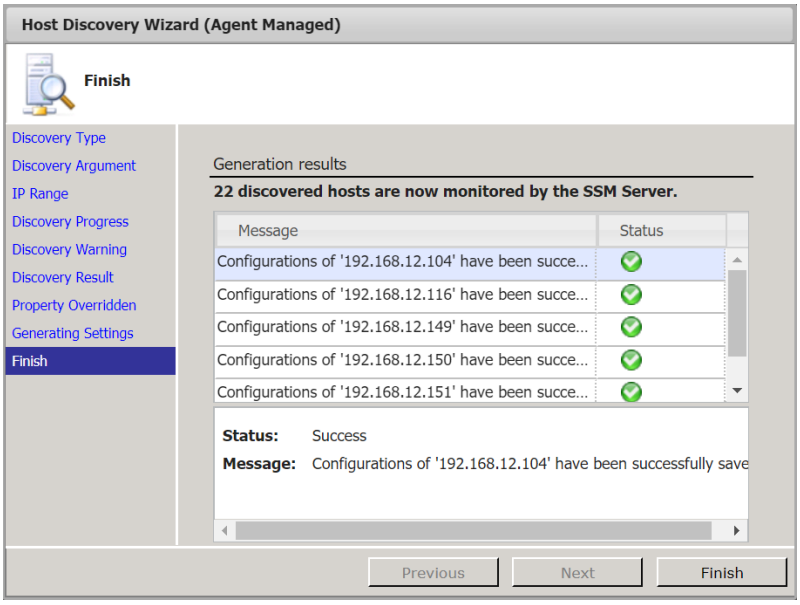


Figure 6-101

Notes:

- The **Detect IPMI** checkbox of an **Agent-managed** host discovery type is replaced with the **Detect Redfish** checkbox instead.
- You can follow similar steps to add agentless, IPMI, and Redfish hosts. If a CMM host is discovered, a new physical host group with the name *CMMModelName_HostName* will be created and the CMM host with all related blade nodes will be added to this group. The number of blade nodes to be added depends on the number of blades managed by the specified CMM host. If the "bmc_password" of a blade node is either different from the request parameter or currently unavailable, those blade nodes will not be discovered.
- An IPMI host supports motherboard generations earlier than X13/H13/CMM-6. Host Discovery Wizard disallows you to add IPMI hosts when the managed system is X13, CMM-6 or later except for some X13 non-RoT systems. For X12/H12 and later, it is recommended that you add Redfish hosts for new feature support.

6.16 SSM Web Certificate

As a SHA-256 self-signed certificate with a 2048-bit key length, the built-in SSL certificate is used for the SSM HTTPS website.

Click **SSM New GUI → Configuration → Server Setup**, and the Certificate page is shown. **Certificate Information** displays the information of the certificate installed on SSM Web.

- **Valid From:** Displays the start time of the validity period.
- **Valid To:** Displays the end time of the validity period.
- **Issued To:** Displays the subject's name of the certificate.
- **Issued By:** Displays the issuer's name of the certificate.
- **Status:** If the certificate is within the validity period, the **Status** shows **OK**. Otherwise, the **Status** shows **Critical**.

6.16.1 Replacing a SSM Web Certificate

To replace the SSM Web certificate, follow these steps:

1. On the Certificate page, enter the password for the new certificate in the SSL Key Password field.

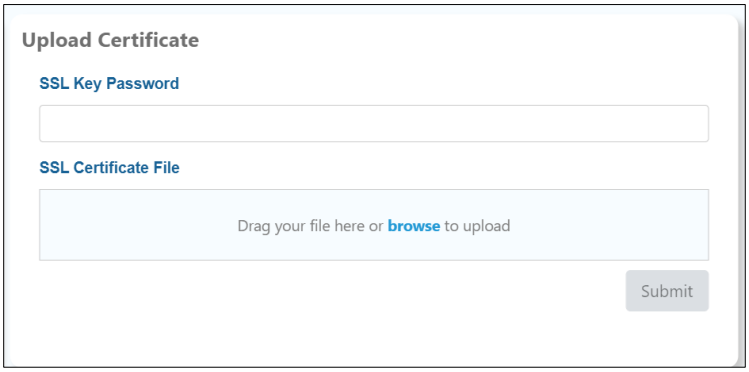


Figure 6-102

2. Either drag the new certificate file (PKC#12 format) to the SSL Certificate File area or click **Browse** to select one to upload.
3. Click the **Submit** button to upload the new certificate. Note that the Certificate Information on the left will be updated after the upload is complete.

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.

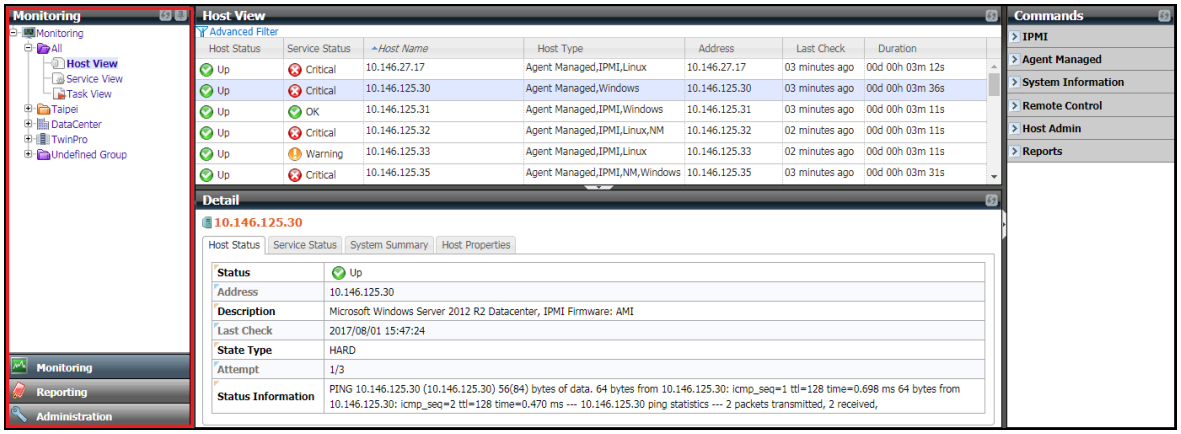


Figure 7-1

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.

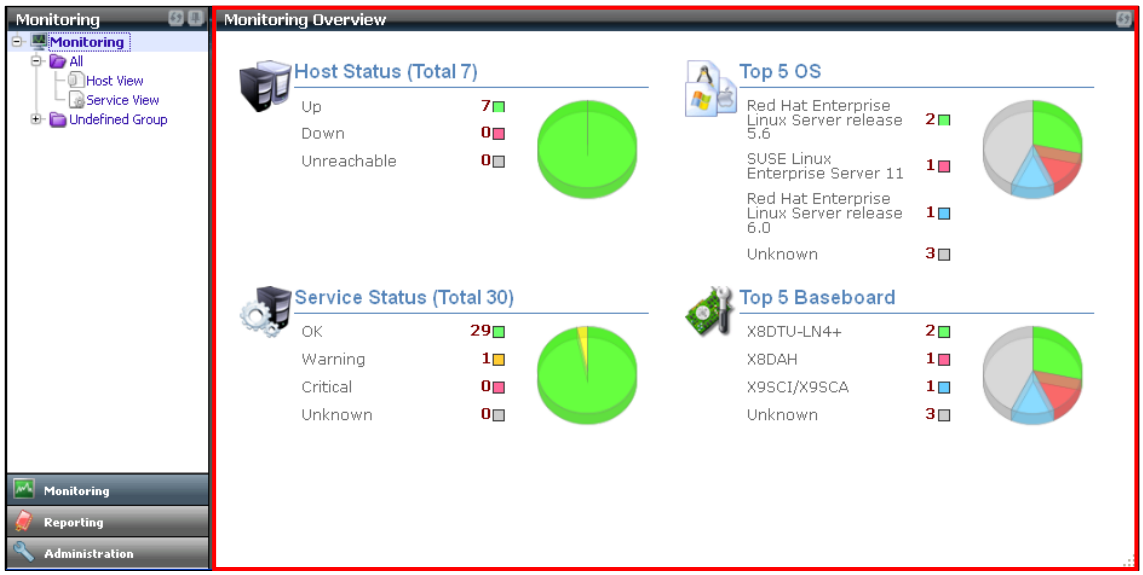


Figure 7-2

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 Agent Managed, Agentless, IPMI, Redfish, NM, Linux, Windows, CMM_IPMI, CMM_Redfish, and CDU.
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.

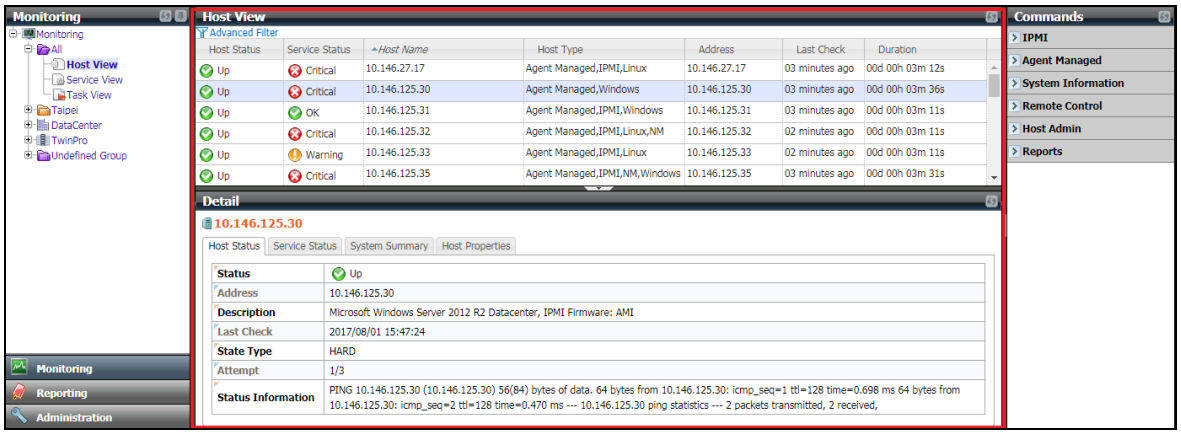


Figure 7-3

- **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.

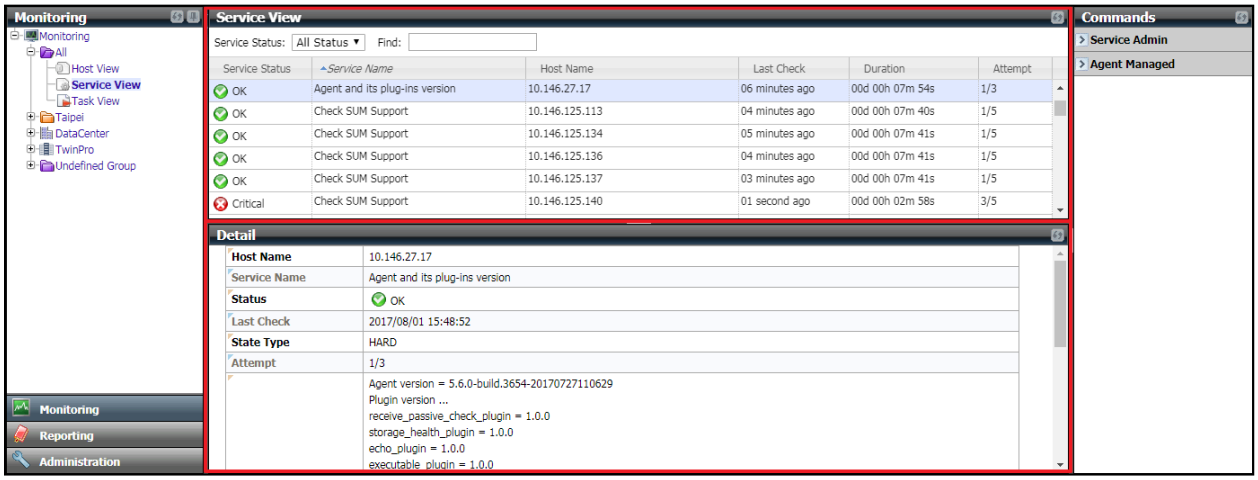


Figure 7-4

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.

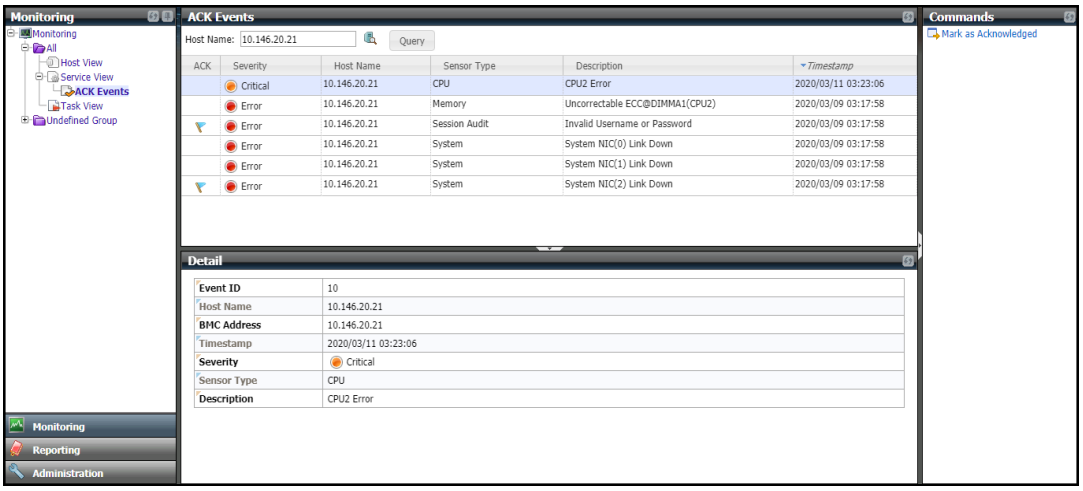


Figure 7-5

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 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.

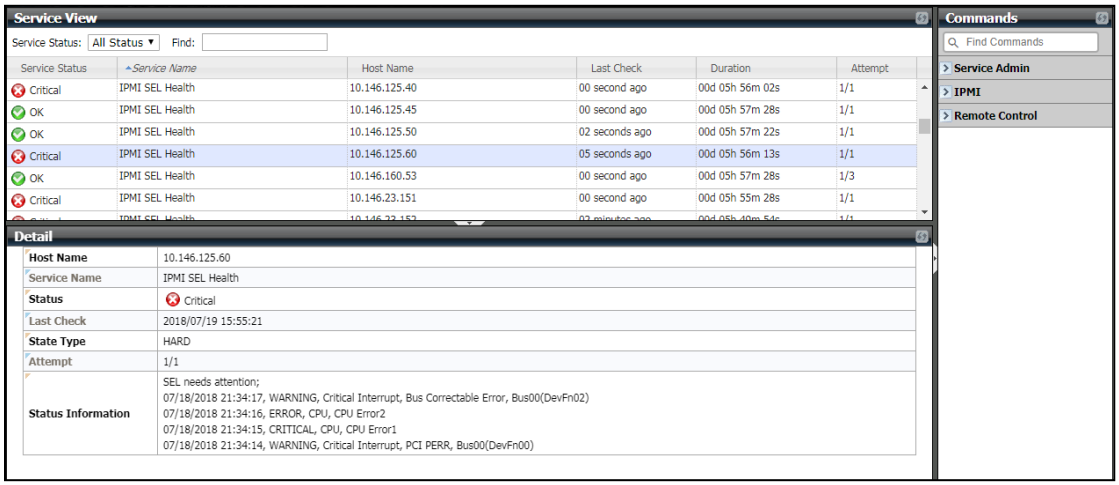


Figure 7-6

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.

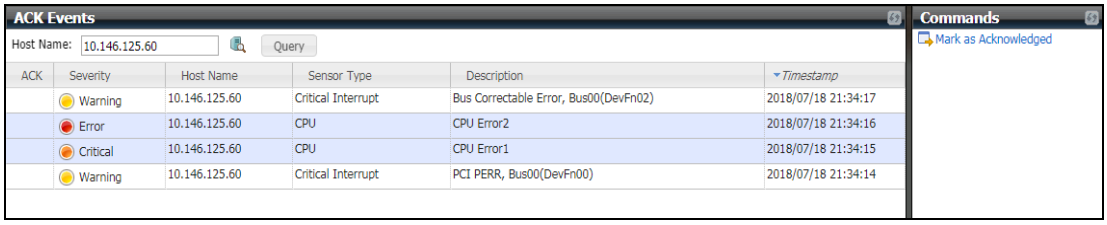


Figure 7-7

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

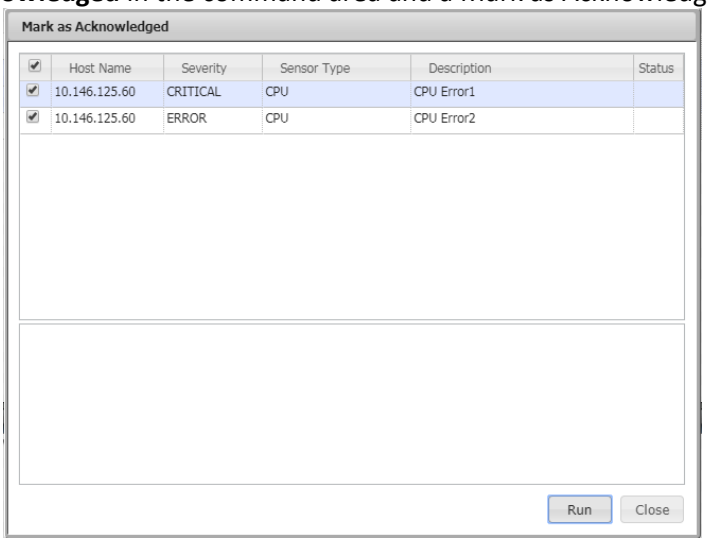


Figure 7-8

3. 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.

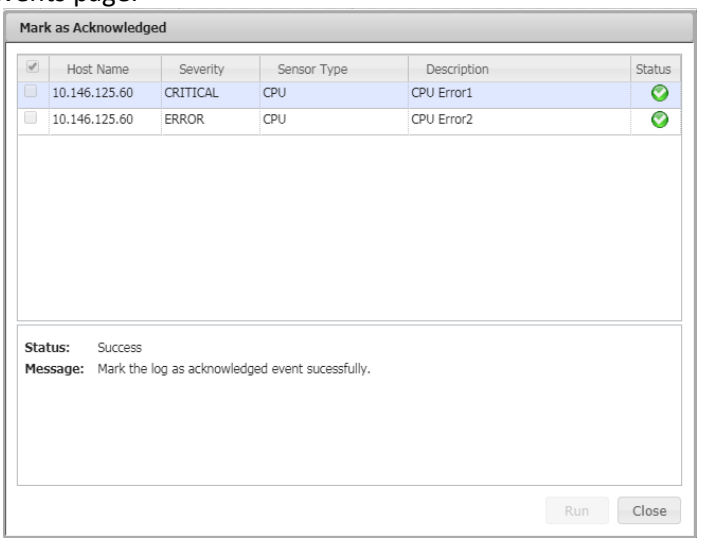
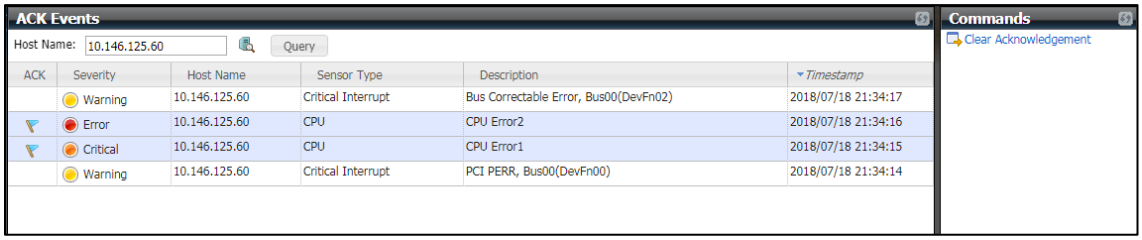


Figure 7-9

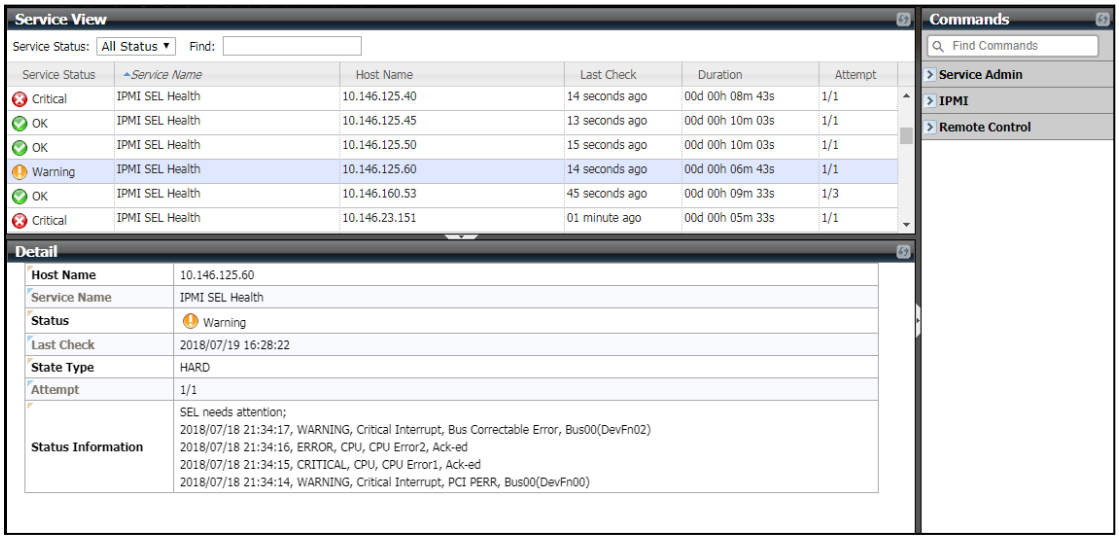
4. In ACK Events master view, the icons appear **before** the items “CPU Error2” and “CPU Error1” in the ACK column.



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

5. 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
Critical	IPMI SEL Health	10.146.125.40	14 seconds ago	00d 00h 08m 43s	1/1
OK	IPMI SEL Health	10.146.125.45	13 seconds ago	00d 00h 10m 03s	1/1
OK	IPMI SEL Health	10.146.125.50	15 seconds ago	00d 00h 10m 03s	1/1
Warning	IPMI SEL Health	10.146.125.60	14 seconds ago	00d 00h 06m 43s	1/1
OK	IPMI SEL Health	10.146.160.53	45 seconds ago	00d 00h 09m 33s	1/3
Critical	IPMI SEL Health	10.146.23.151	01 minute ago	00d 00h 05m 33s	1/1

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.

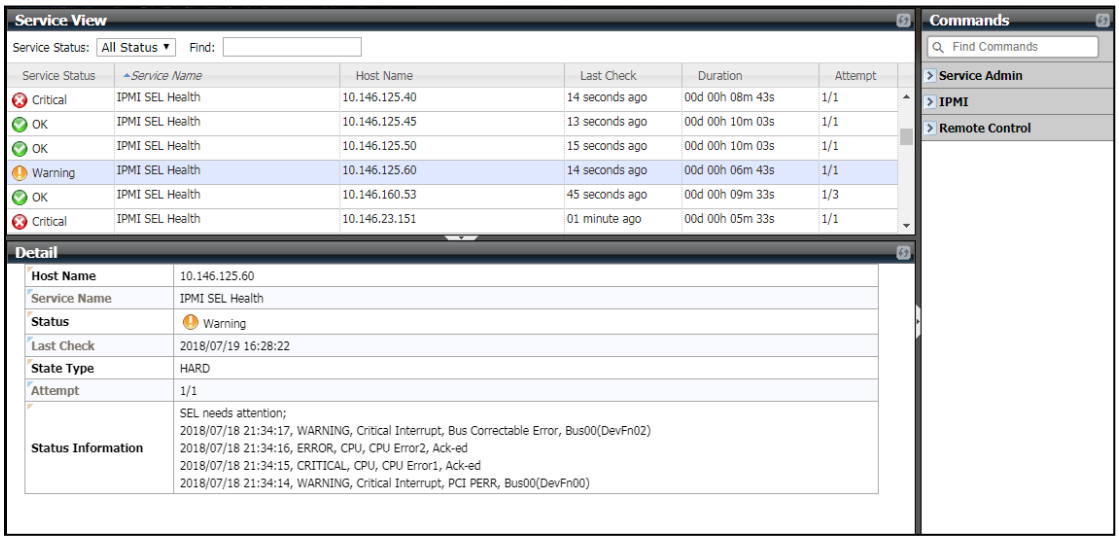


Figure 7-12

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.

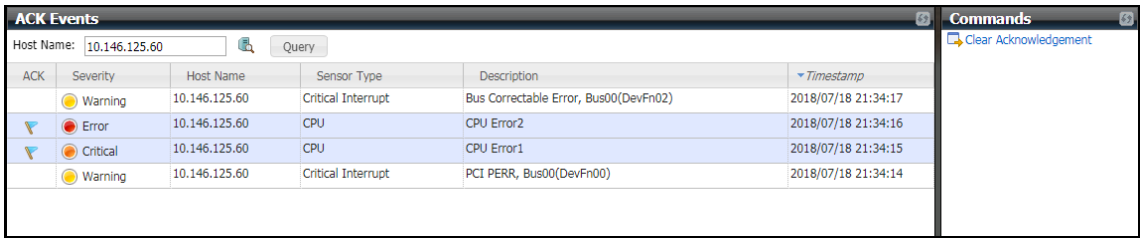


Figure 7-13

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

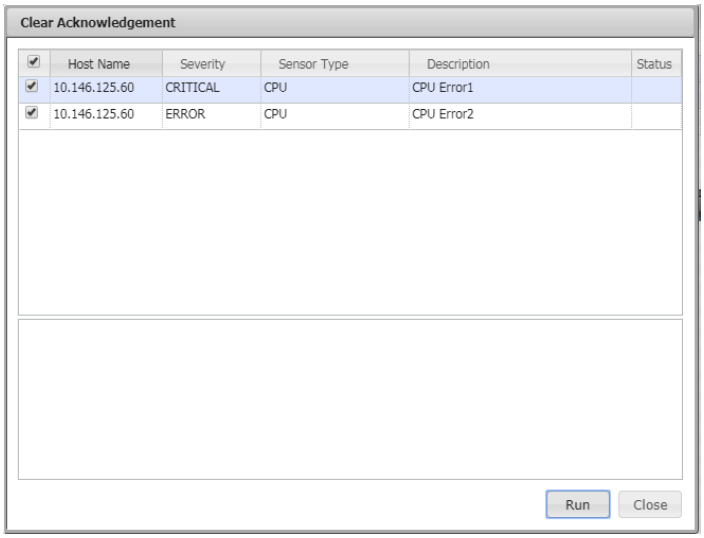


Figure 7-14

3. 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 the **Close** button and return to the ACK Events page.

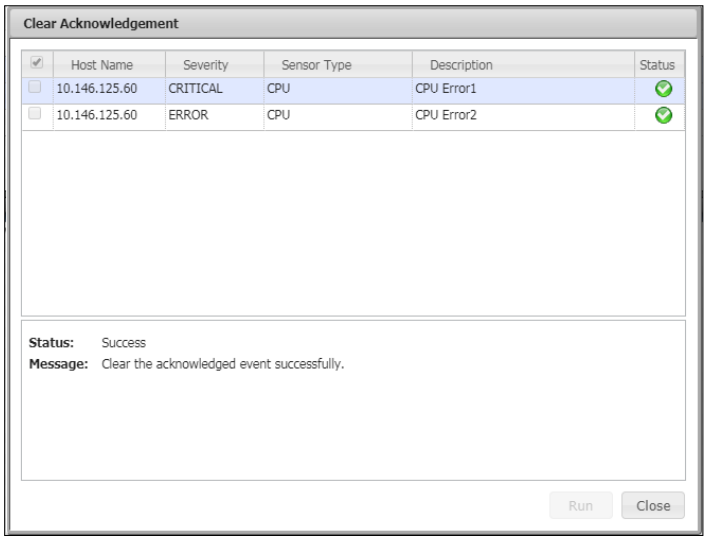
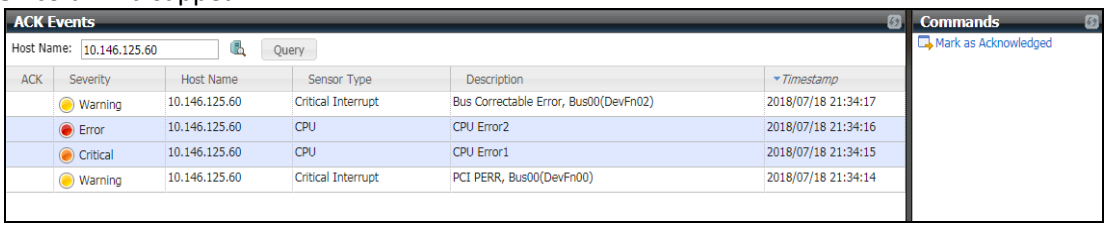


Figure 7-15

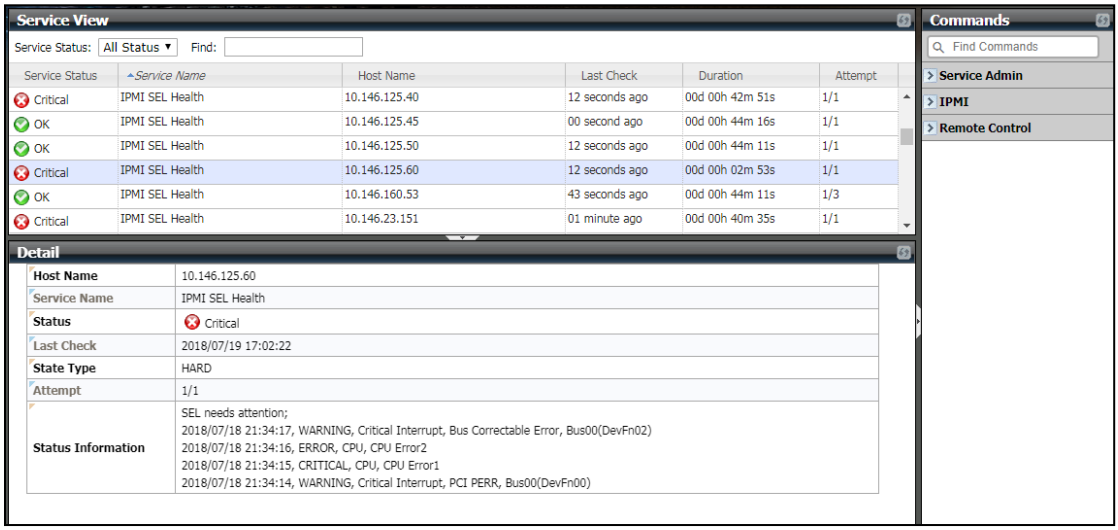
4. In the ACK Events master view, the icons before both items “CPU Error2” and “CPU Error1” in the **ACK** column disappear.



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

5. 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 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

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 or suspended but not yet processed).
Task ID:	Shows the unique key to identify the Task.
Task Name:	The asynchronous task represents a web command to a target resource. The 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.

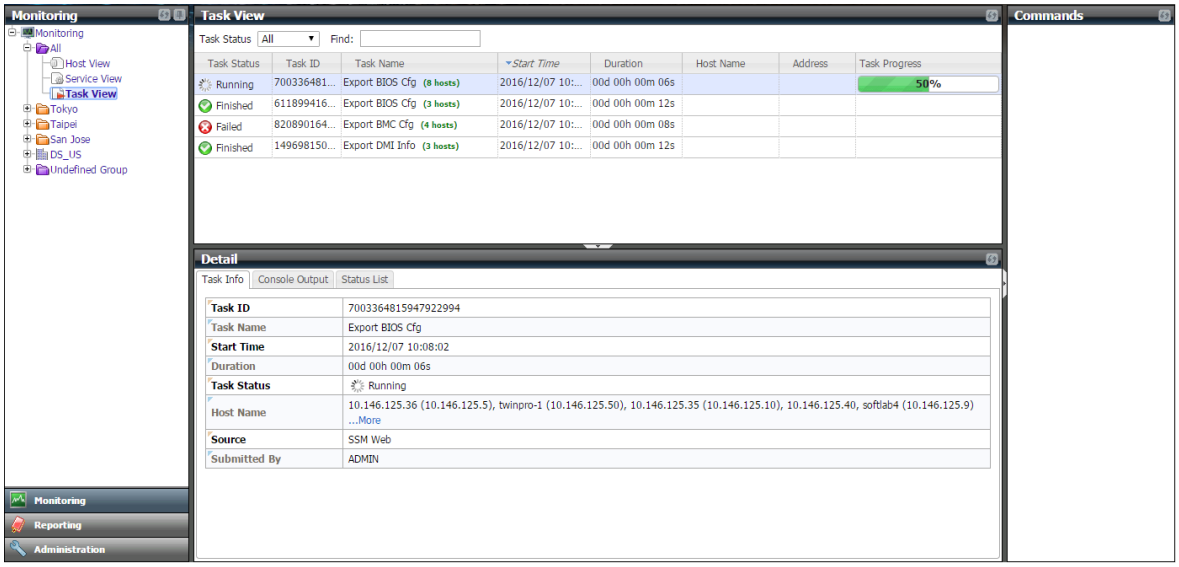


Figure 7-18

- **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 7 days.

7.2.6 Scheduled Task Management

The Scheduled Task Management command is used to create scheduled tasks. You can also use the command to discover IPMI hosts and Redfish hosts.

To create a scheduled task, follow these steps:

1. Click **Scheduled Task Management** in the Commands area of Task View.

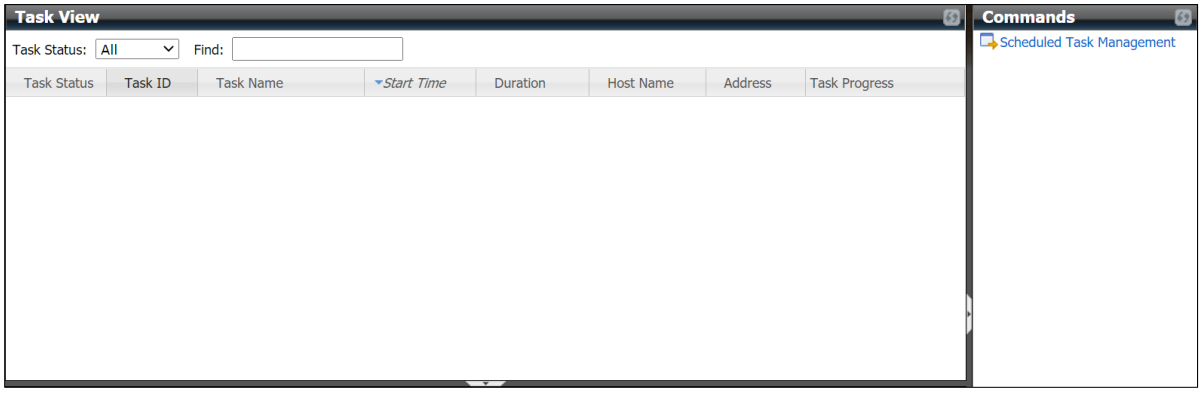


Figure 7-19

2. The Scheduled Task Management dialog box appears and displays the existing scheduled tasks. Click the **Add** button to create a new scheduled task.

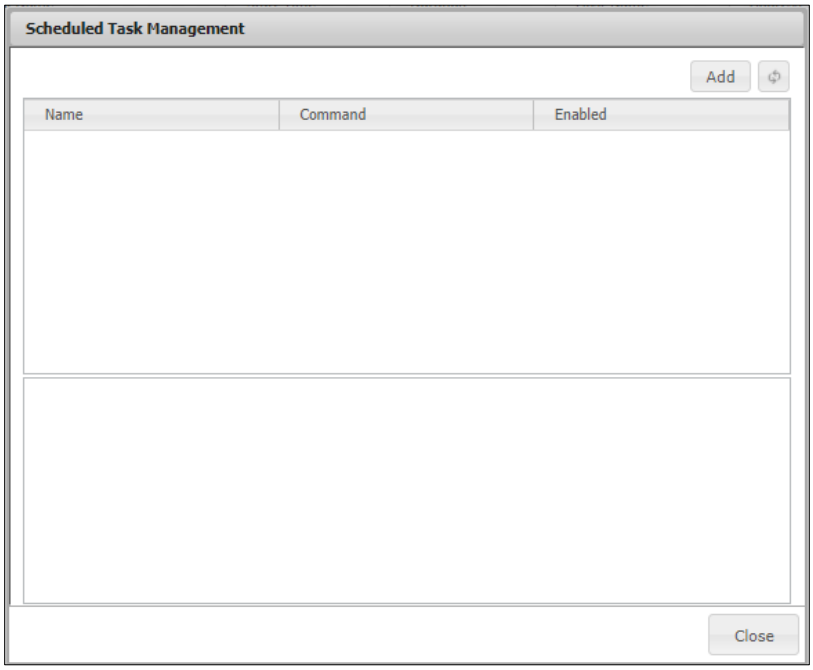


Figure 7-20

3. The Add Scheduled Task Setting dialog box appears. Both **Name** and **Command** fields in the Edit Command tab must be filled out. By default, the **Enabled** check box is checked. Note that execution will not run without this check box selected.

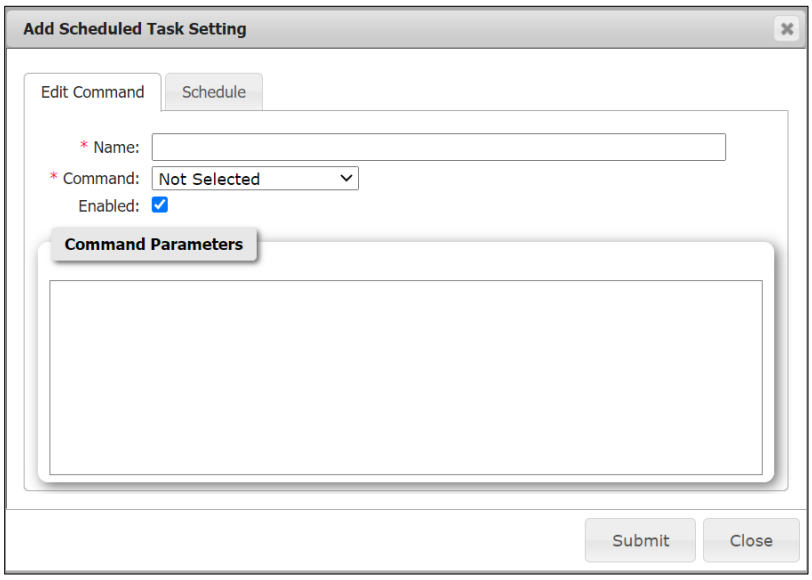


Figure 7-21

4. Click the **Command** drop-down list and select the desired type of action. The corresponding parameters appear in the Command Parameters area.

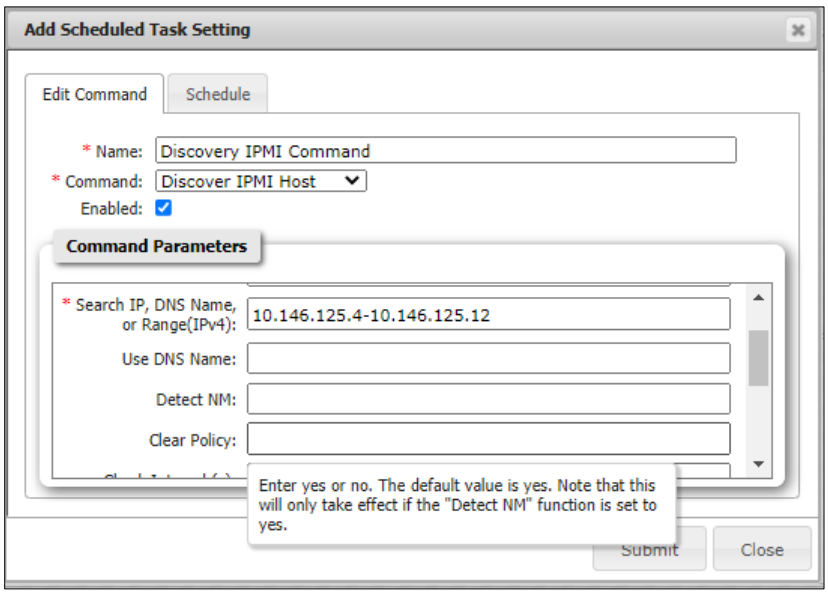


Figure 7-22

Notes:

- All fields are case-insensitive except BMC ID and BMC Password.
- A hint appears when the mouse hovers over the target field.
- If the Detect NM field is set to “yes,” settings of the rest of fields, including "Clear Policy," "Derated DC Power," "Derated AC Power," and "Max PS Output," will take effect at the same time.

5. To modify a task’s schedule attributes, click the **Schedule** tab. Use the Repeat On drop-down list to select Once or Weekly to determine the execution frequency.

- **Weekly**

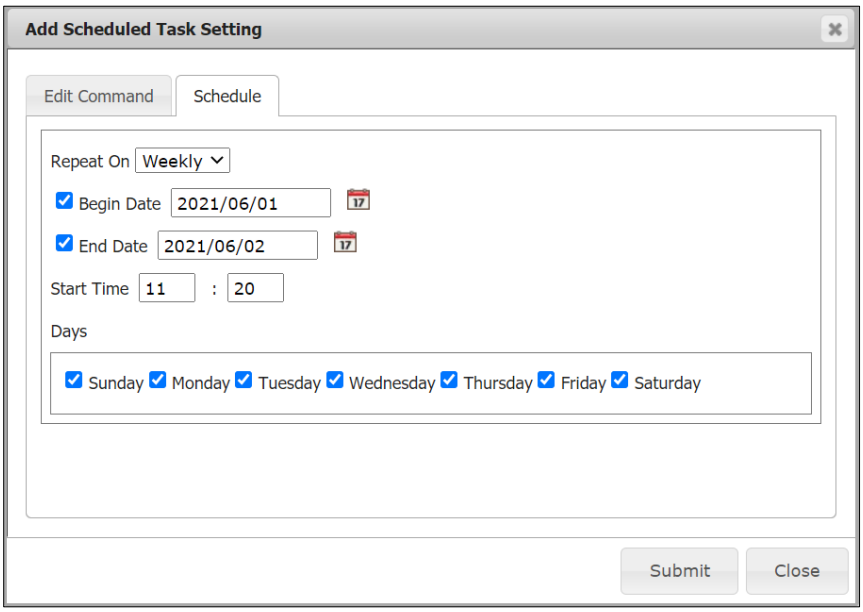


Figure 7-23

  - **Begin Date:** Specifies the date from which the execution begins. If the Begin Date is not specified, the command will be executed repeatedly from the date when the task is created.
  - **End Date:** Specifies the date on which the execution stops. If the End Date is not specified, the execution will never stop.
  - **Start Time:** Specifies the time in hours and minutes when the execution starts.
  - **Days:** Specifies the days of the week when the execution runs. Note that at least one day must be selected, e.g., Monday.

- **Once**

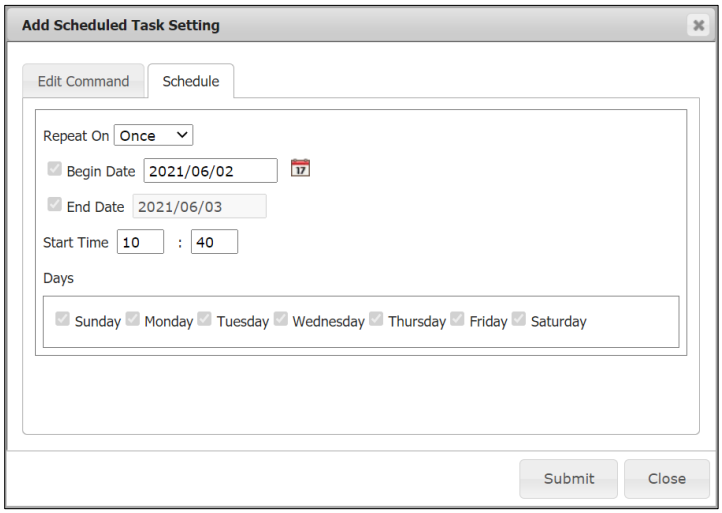


Figure 7-24

- **Begin Date:** Specifies the date on which the command execution begins.
- **End Date:** This setting is not available.
- **Start Time:** Specifies the time in hours and minutes when the execution starts.
- **Days:** This setting is not available.

6. After you finish both tabs, click the **Submit** button. The new task is now added.

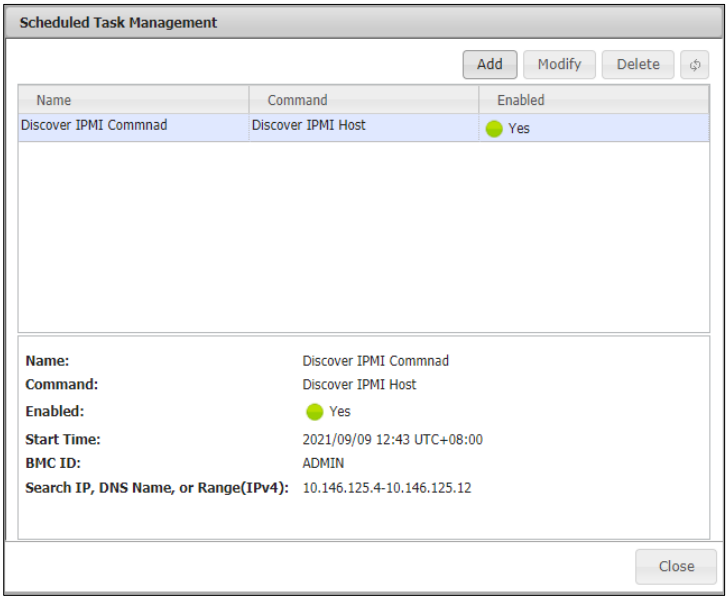


Figure 7-25

- **Add:** Adds another scheduled task.

- **Modify:** Edits the selected scheduled task setting.
- **Delete:** Deletes the selected scheduled task.
- **Refresh:** Refreshes all available scheduled tasks.

7. Click the **Close** button to finish.
8. When the scheduled task execution begins, its status is displayed in Task View. In this example, all hosts discovered are displayed on the Console Output tab.

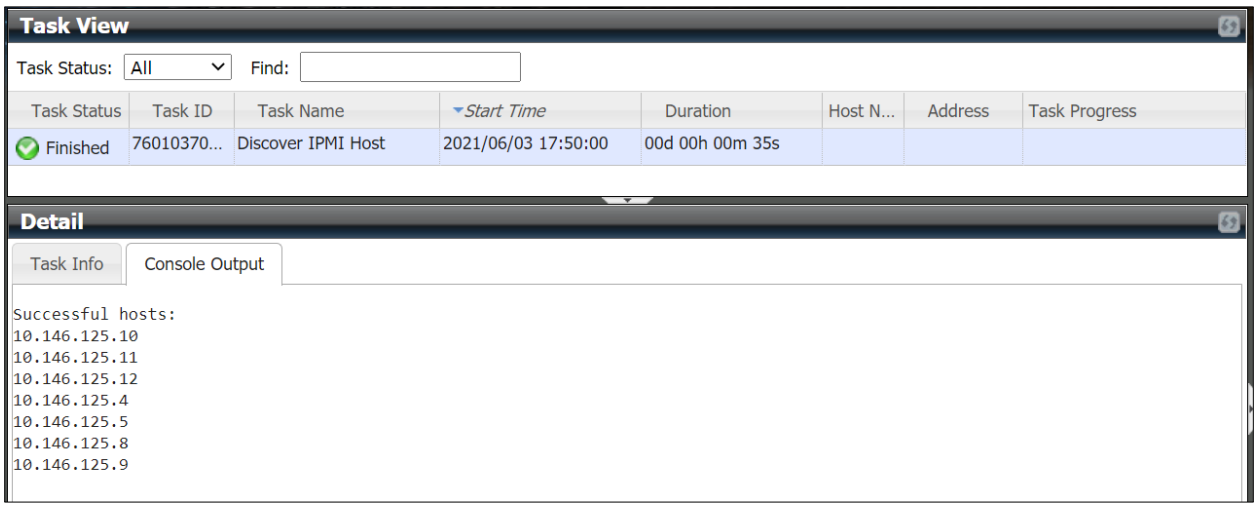


Figure 7-26

7.2.7 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).

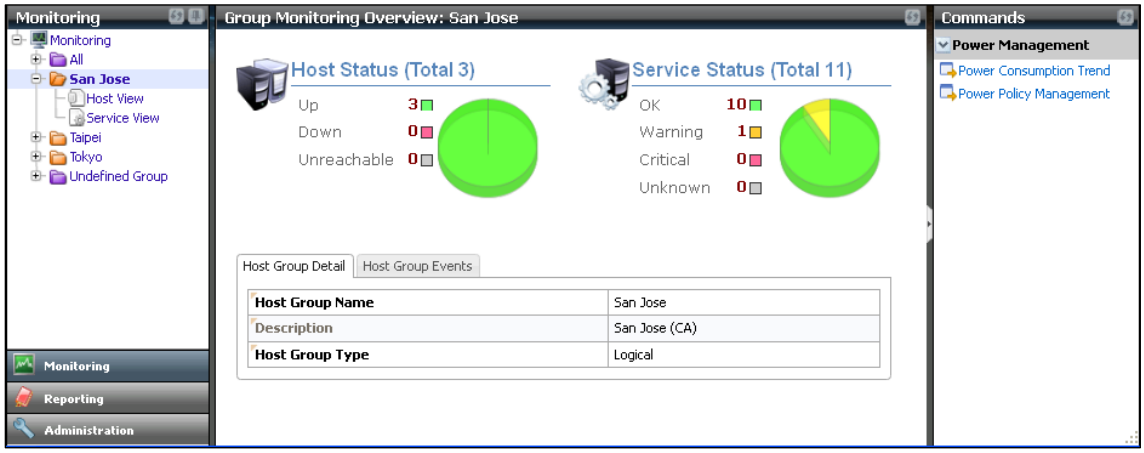


Figure 7-27

7.2.8 Action Log

An action log records the actions users and the system have taken toward a managed system. With an action log, you are able to analyze any malicious attacks during a specific period of time or troubleshoot faulty machines based on historical actions. Currently, user's logging in, user's logging out, session timed out, and web commands for IPMI and Redfish host types are supported.

To view action logs, click **SSM New GUI → Monitoring → Action Log**, and the **Action Log** page is shown.

A user in the role of Administrator can search all action logs. Otherwise, a user as Operator or with Limited Access can only search for their own action logs.

An action log is composed of the following attributes:

- **Time**: the timestamp of the action log.
- **User**: the user who executes the action.
- **Role**: the user's role. If the User field is not empty, the Role will be Administrator, Operator, or Limited Access.
- **User Type**: the type of user who executed the action, such as System (non-login user), Local User (the user is a local user), LDAP (the user is an LDAP account), and AD (the user is an AD account).
- **Target**: the target resource that was affected by an action, such as System, host's name, or user's name.

- **Category**: the category of the action log.
  - **Audit**: the log is recorded when a user logs in, logs out, or session timed out.
  - **Host Operation**: the log is recorded when a login user or the system executes a command on the managed IPMI and Redfish host.
- **Event Type**: the event type of the action log, such as BMC Cole Reset, Update BMC, or User Login.
- **Description**: the description of the action log.

If the number of action logs is more than 1500 on Action Log page, the user is required to narrow the search using the filter dialog to query again. To filter the action logs with specific criteria, click the **Filter** icon on the right side, fill in the necessary information and click the Submit button. If you want to filter the action logs with the specific hosts, click the **Search** icon in the bottom right in the **Target** field and select the desired hosts in the Select Hosts dialog box. You could also input the host name in the **Target** field and then press the **<Enter>** key directly. Note that the **User** field is available when the login user has the Administrator permission.

Note: To prevent the action logs from getting too large, the data retention period is 3 months.

7.2.9 Task History

The Task History shows a list of tasks that have been completed within three months. Unlike the tasks on the Working/Recent tab, here you can find earlier tasks (regardless of their triggers by scheduler, manual control, or REST API), and narrow your search by specific criteria.

To view task histories, click **SSM New GUI → Monitoring → Task View**, then click the **History** tab and the page is shown.

- **History**: A task history is composed of the following attributes:

Task Status:	The status values include FAILED (the task has not been completed successfully) and FINISHED (the task has been completed successfully).
Task ID:	Shows a unique key to identify the Task.
Task Name:	The asynchronous task is named after the web command executed on the target resource.
Start Time:	Shows the start time of running a Task.
Duration:	Shows the total time of running a Task.

Submitted By:	Shows the System or the user who submitted the task.
Target Resource:	Shows the resource that is affected by the task, such as System, a host name, or a plan name.

If there are more than 1500 records of tasks on the History page, the user is required to narrow the search by filters. To filter task histories by specific criteria, click the **Filter** icon on the right side, fill in necessary information, and click the **Submit** button. To find tasks for specific hosts, click the **Search** icon in the bottom right in the **Target Resource** field, and then click **Search By Hosts** from the drop-down menu. You can select hosts in the Select Hosts dialog box. Also, you can input the exact host name in the **Target Resource** field and then press the **<Enter>** key.

Note: To prevent the task histories from getting too large, the data retention period is 3 months.

- Click the right double arrow » icon to show the details of the task history, which includes **Task Information**, **Console Output**, and **Status Overview** information.

Task Information:	Includes information such as task name, start time, duration, target resource, etc.
Console Output:	The task execution message.
Status Overview:	Donut charts to present the task completion percentage and the task status.

7.3 Command Area

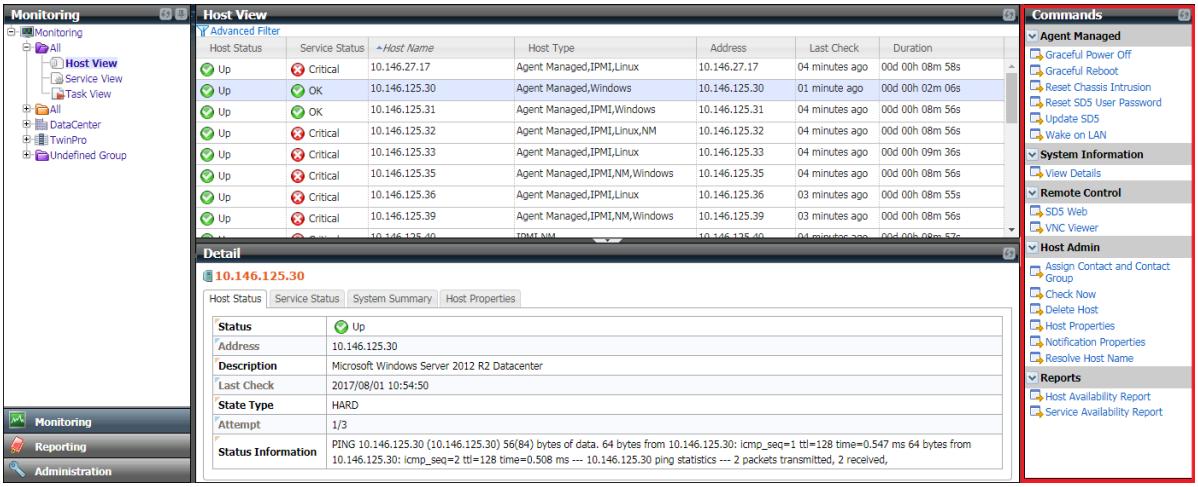


Figure 7-28

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

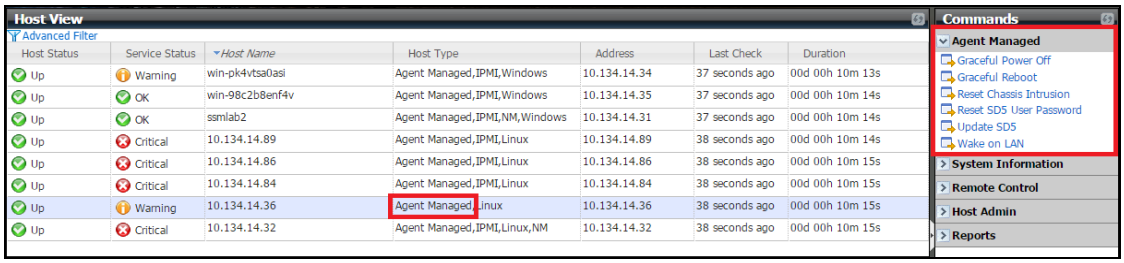


Figure 7-29

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**.

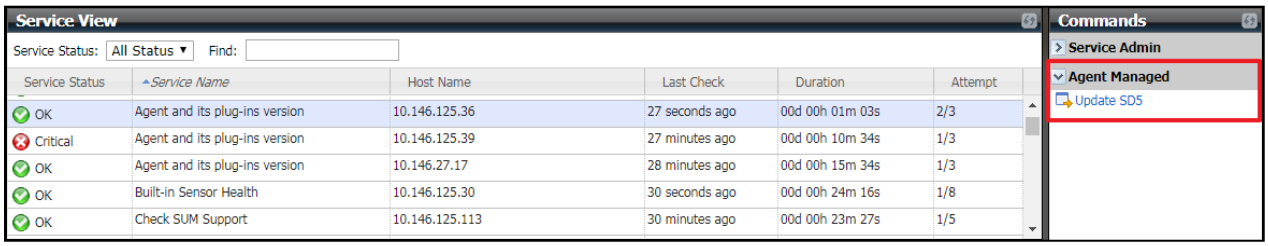


Figure 7-30

To execute a command, first select one or more hosts[5] 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.

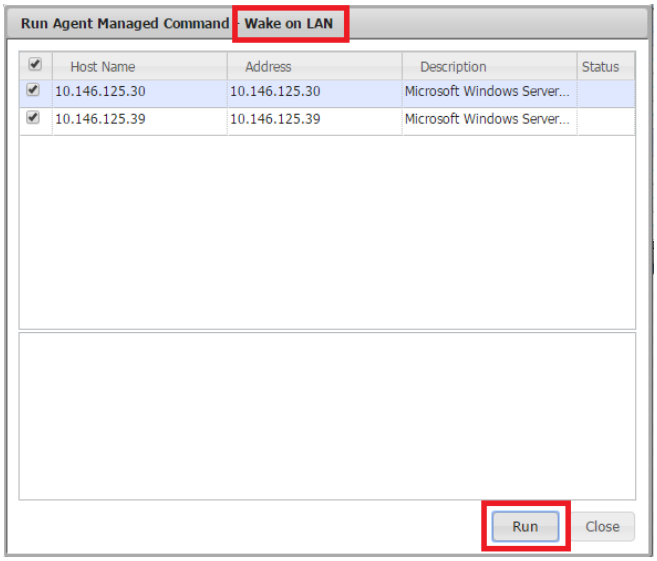


Figure 7-31

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

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

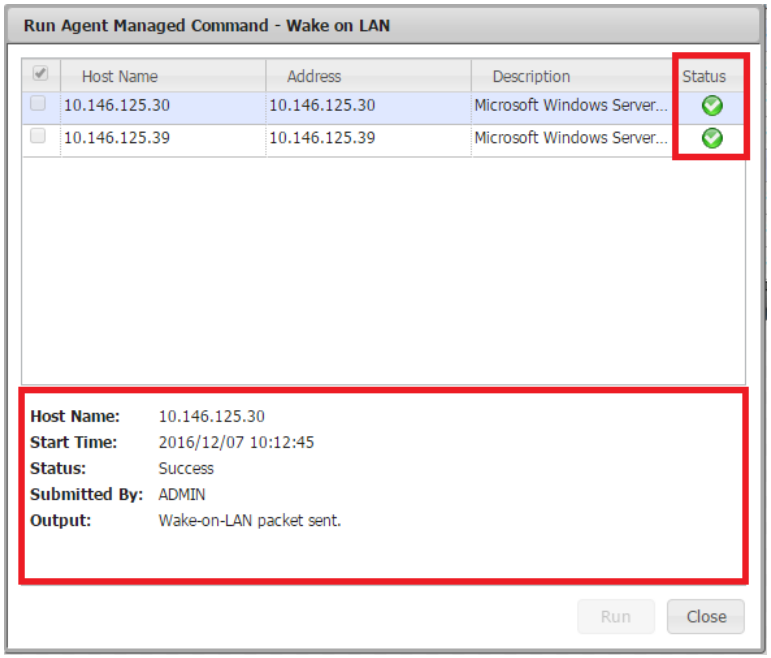

Run Agent Managed Command - Wake on LAN
Host Name
Address
Description
Status
10.146.125.30
10.146.125.30
Microsoft Windows Server...
10.146.125.39
10.146.125.39
Microsoft Windows Server...
Host Name: 10.146.125.30
Start Time: 2016/12/07 10:12:45
Status: Success
Submitted By: ADMIN
Output: Wake-on-LAN packet sent.
Run
Close

Figure 7-32

7.3.2 IPMI Commands

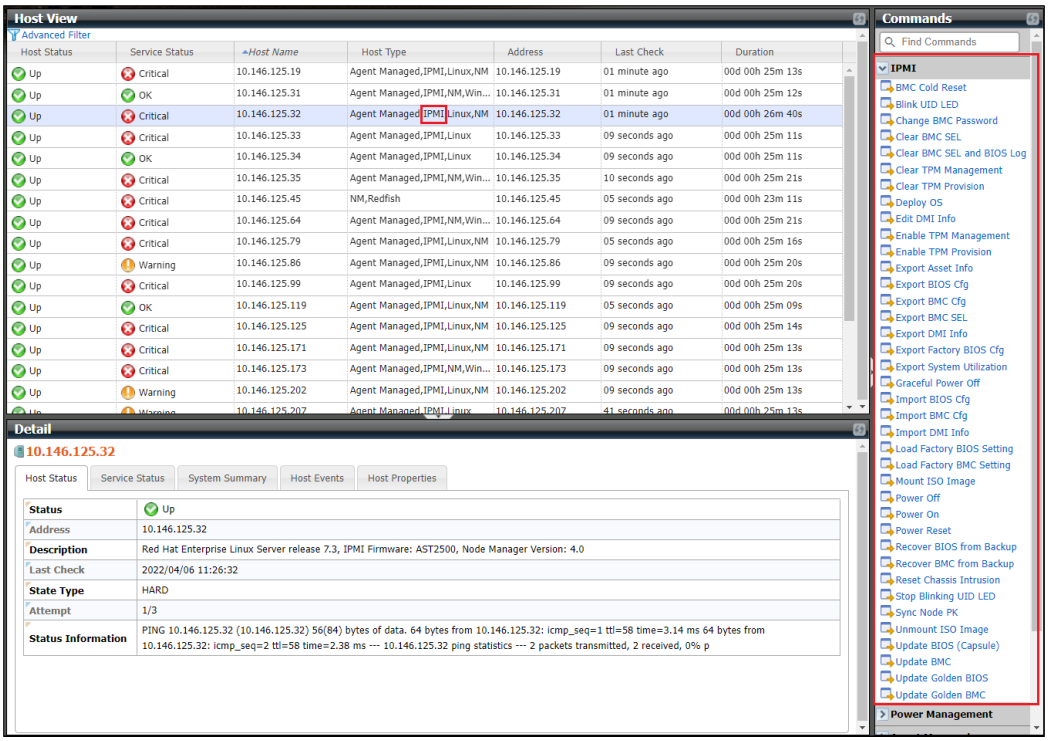


Figure 7-33

Commands in this category as shown below apply 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 SEL:** Clears the BMC health event logs.
- **Clear TPM Provision/Management:** Clears TPM module capabilities from the selected hosts.
- **Clear BMC SEL and BIOS Log:** Clears the BMC health event logs and BIOS event logs.
  - Health event logs in BMC will be cleared immediately.
  - Event logs in BIOS will be cleared only after system reboot.
- **Deploy OS**: Deploys Linux OS on a host. See *10.3.8 FW Auto Update: Change Schedule* for details.

- **Edit DMI Info:** Changes specific 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.
- **Enable TPM Provision/Management:** Enables TPM module capabilities for the selected hosts.
- **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.

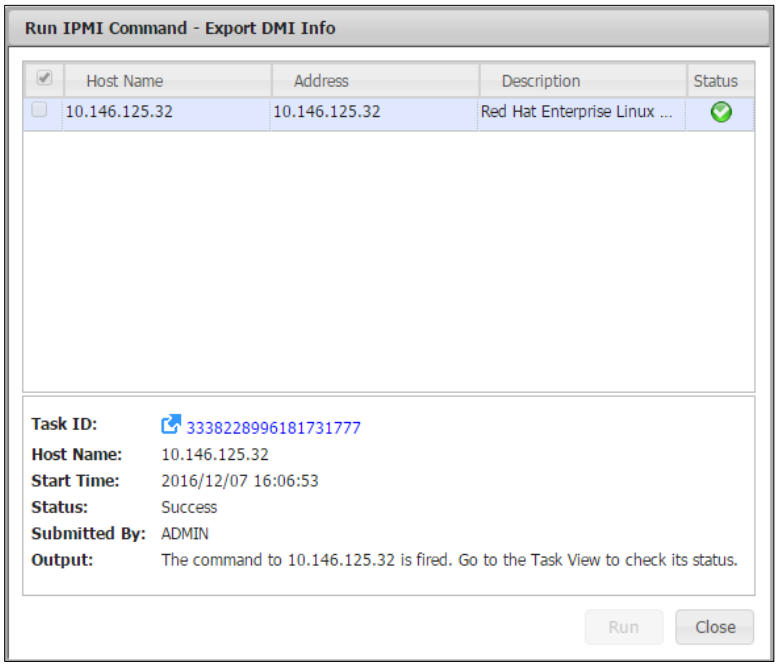


Figure 7-34

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.

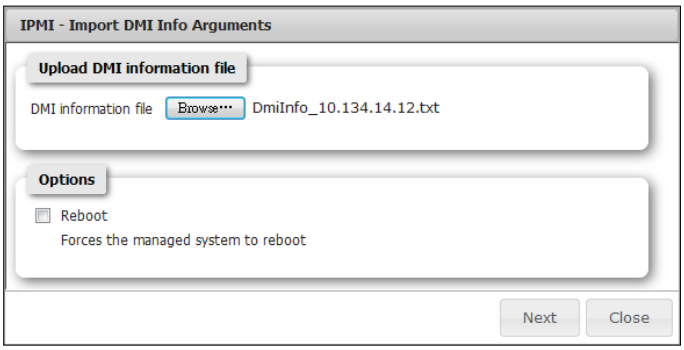


Figure 7-35

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.

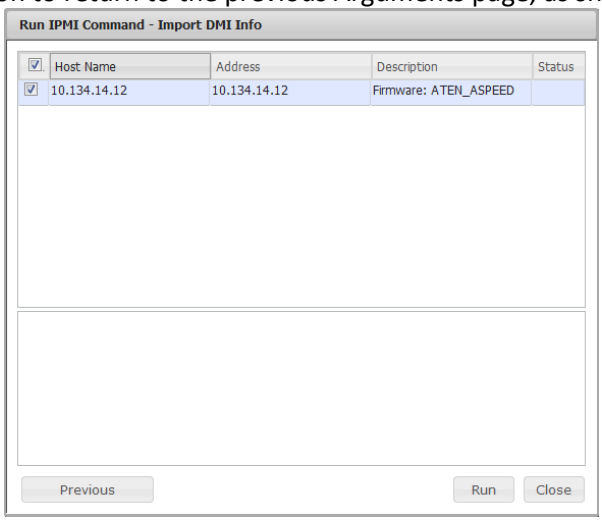


Figure 7-36

8). Click the **Run** button to update 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: Changes made in The DMI information will only take effect after a system reboots or powers up. You can select the **Reboot** option in the Arguments dialog box for rebooting after updating.

- **Graceful Power Off**: Powers off a host gracefully.
- **Power Off**: Powers off a host immediately.
- **Power On**: Powers on a host.
- **Power 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.
- **Update Golden BIOS**: Sets the current active BIOS image as a golden template. Note that the managed system must support the RoT system.
- **Update Golden BMC**: Sets the current active BMC image as a golden template. Note that the managed system must support the RoT system.
- **Recover BIOS from Backup:** Recovers BIOS from the backup firmware image. Note that the managed system must support the RoT system.
- **Recover BMC from Backup:** Recovers BMC from the backup firmware image. Note that the managed system must support the RoT system.
- **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 Setting:** 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.
- **Load Factory BMC Setting:** Restores the BMC to the default factory settings. Note that not all of the BMC settings will be set to factory default, for SSM to continue monitoring, the settings of network, FRU, and user will be retained. The operation is similar to that of the **Import BMC Cfg** command.
- **Update BIOS (Capsule):** Updates the selected hosts with an image file. In the Arguments dialog box, you need to upload a BIOS image file and choose the flash options, as shown below.

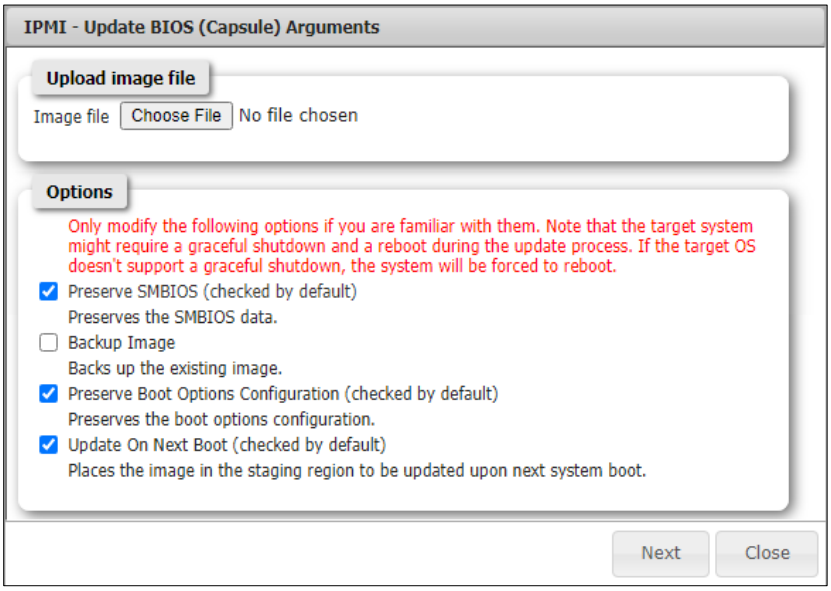


Figure 7-37

Notes:

- The options in the Update BIOS (Capsule) Arguments may vary depending on the selected motherboard or system, and they will be available while the System Information service check is being performed. To update multiple hosts all at once, the motherboards of these hosts must be from the same series.
- You can use the **Update On Next Boot** option to update BIOS on X12/H12 and later RoT systems without an immediate system reboot. If you select the option and run the command and the image file is uploaded to the staging region, the **Update BIOS** task will be in the pending status in the task view. The pending task will resume and continue the update process after the selected hosts reboot or power up. You can also abort the pending task by running the **Delete Task** command in the commands area.
- The selected hosts as non-RoT systems must be rebooted or powered up for the changes to take effect. You can use the **Reboot** option (if available) to reboot

after update.

- **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. 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.
- **Export BMC SEL:** Exports the BMC health event logs. The operation and result are similar to those of the **Export DMI Info** command.
- **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.

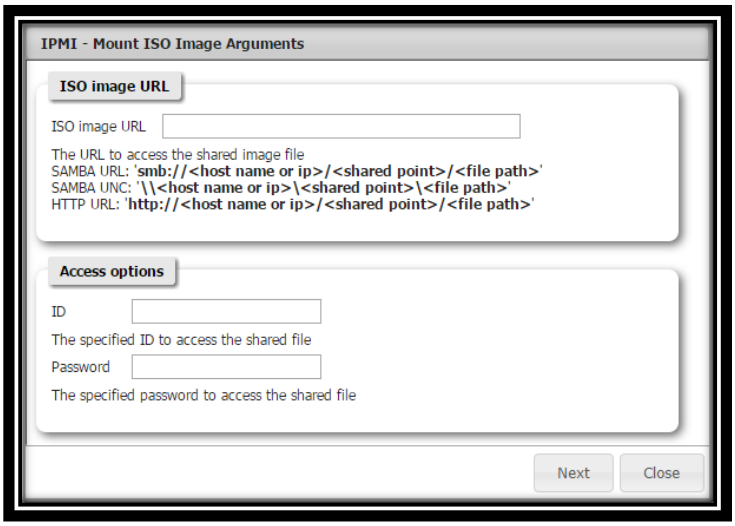


Figure 7-38

- **Unmount ISO Image:** Removes ISO image as a virtual media from the selected hosts.

Note: For the web commands that require systems to reboot, SSM performs a graceful shutdown to protect the managed systems. If the target OS does not support a graceful shutdown, the system will be forced to be reboot. The Linux OS with X Window systems do not support a graceful shutdown by default, and it is therefore highly recommended

that you change the power button setting from “Suspend” to “Power Off.” The system will then shut down after the power button is pressed.

Commands in this category as shown below apply to CMM_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 SEL:** Clears the BMC health event logs.
- **Load Factory CMM Setting:** Restores the CMM to the default factory settings. Note that not all of the CMM settings will be set to factory default. The settings of the network, FRU, and the user will be retained for SSM to continue monitoring.
  1). Click **SSM New GUI → Monitoring → Host Monitoring view** to view the status of hosts.
  2). Select hosts in the working area. You can select multiple hosts at a time of the same host type.
  3). Click the **Toolbar** icon in the upper right corner of the Host View, and click the **Load Factory CMM Setting** in the CMM IPMI commands area. The Load Factory CMM Setting dialog box will appear.
  4). Click the **Run** button to execute the command.
  5). Click the **Task ID** link to go the Task View. SSM uses an asynchronous task to represent the request that takes longer time to complete.
- **Stop Blinking UID LED**: Stops a host’s UID LED from blinking.
- **Export CMM Cfg**: Exports the CMM IPMI host settings.
- **Import CMM Cfg:** Imports the CMM host settings. The operation is similar to that of the **Import DMI Info** command. You need to upload a file of newly configured CMM host settings in the Import CMM Cfg Arguments dialog box.
- **Turn Blade UID On/Off**: Causes a CMM host’s UID LED to blink to identify a specific physical host in a data center.
- **Update CMM:** Updates the CMM firmware image. You need to upload a CMM firmware image file in the Update CMM Arguments dialog box.

Note: For IPMI or CMM_IPMI hosts, when you execute a **Load Factory BMC Setting** or a **Load Factory CMM Setting** command, it's likely that the IP address and user credentials will be restored to factory defaults. You’ll need to modify the IP address and user credentials on BMC Web first and then execute the **Host Properties** web command for SSM to add itself to the target BMC as an event subscriber.

7.3.3 Power Management Commands

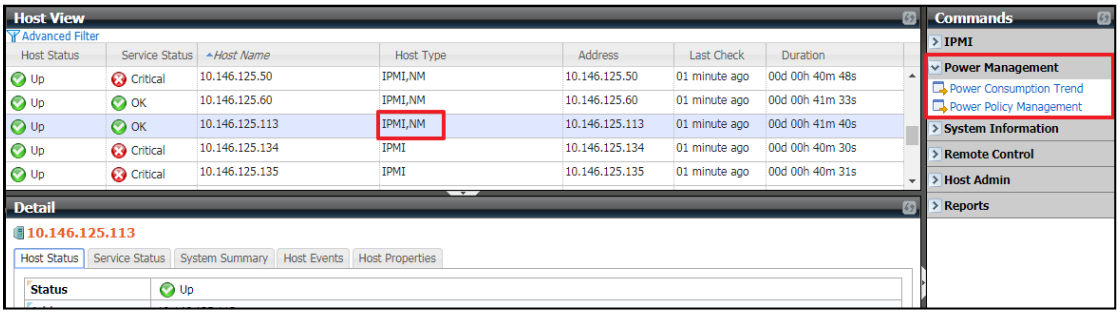


Figure 7-39

The power management commands are applicable for IPMI hosts or Redfish hosts with NM support.

- **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**.

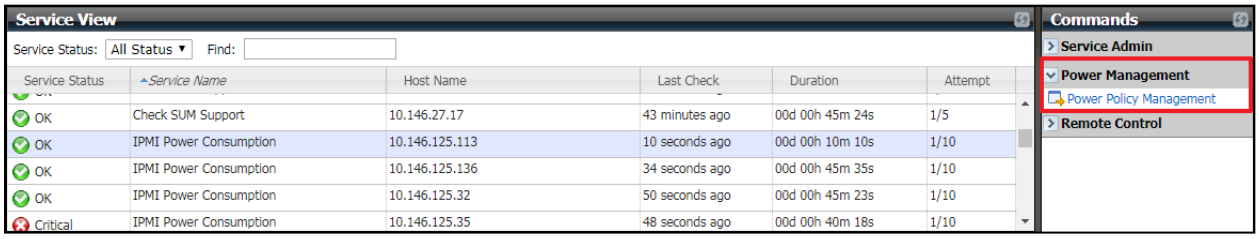


Figure 7-40

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, IPMI and Redfish 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.
- a Redfish host is selected,
- a Redfish System Information service is selected.

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

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

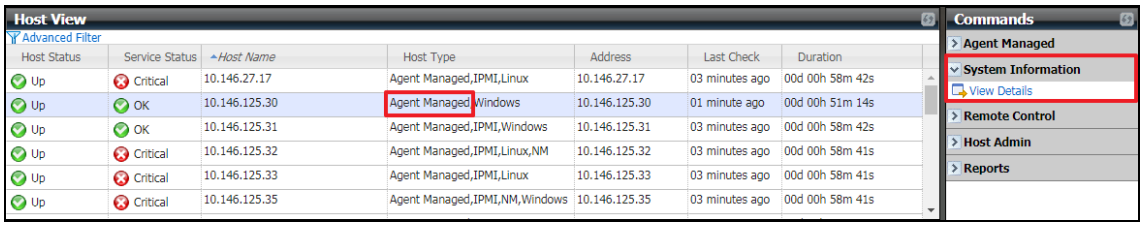


Figure 7-41

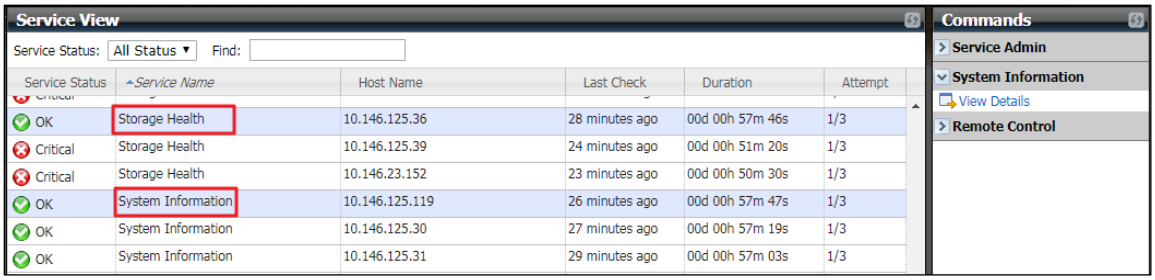


Figure 7-42

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.

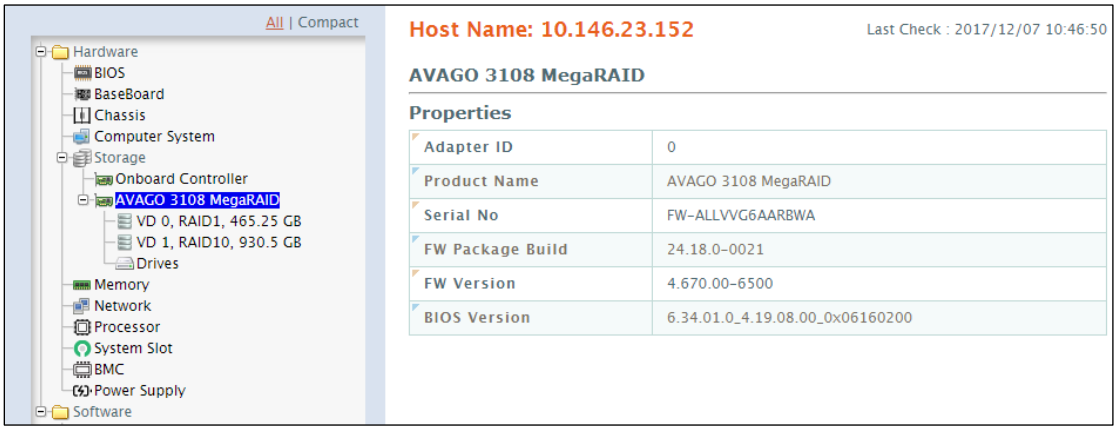


Figure 7-43

Notes:

- For Agent Managed hosts, the system information contents are platform dependent. That is, the 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 Keyboard, Port Connector, Pointing Device, Serial Port, Computer Summary, Startup Command, and Video Controller are supported on Windows platforms only.
- Besides the onboard controller, only LSI MegaRAID 3108 RAID controller and later generations such as 3908 and 3916 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 or Redfish hosts, BIOS, BaseBoard, Chassis, Computer System, Storage (onboard controller), Memory, Network, Processor, BMC, Power Supply, GPU, OEM Strings, and System Cfg Options are supported. CMM Switch is especially supported for CMM_IPMI or CMM_Redfish hosts.
- 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.

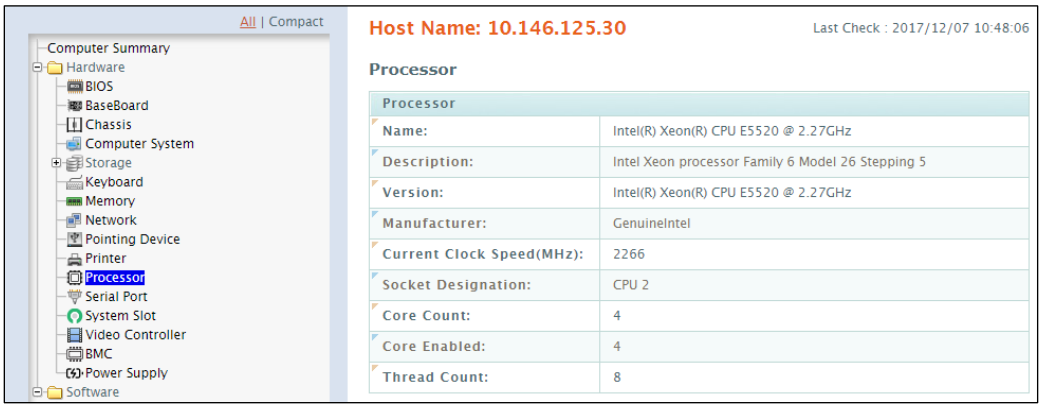


Figure 7-44

7.3.5 Remote Control Commands

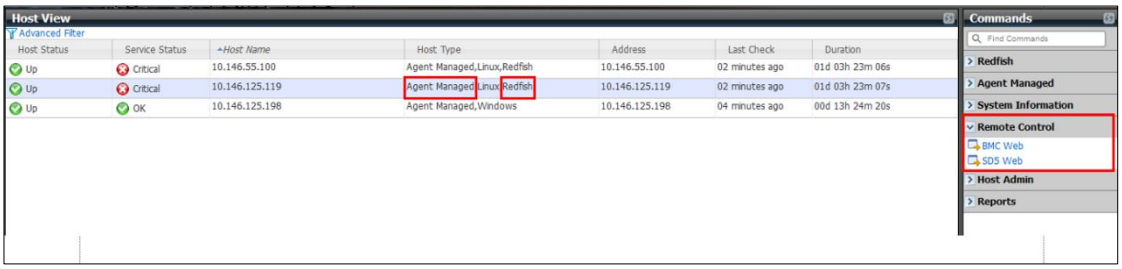


Figure 7-45

Commands in this category apply only to Agent Managed hosts, IPMI, Redfish, and CDU hosts. For Agent Managed hosts, one remote control command is available:

- **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/Redfish Managed hosts, one remote control command is available:

- **BMC Web:** This opens a Web browser to connect to a BMC Web running on a BMC. You can **use this c**ommand 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 **BMC Web** command to open a browser and connect to the BMC Web. Enter a BMC username and password to login to the BMC Web.

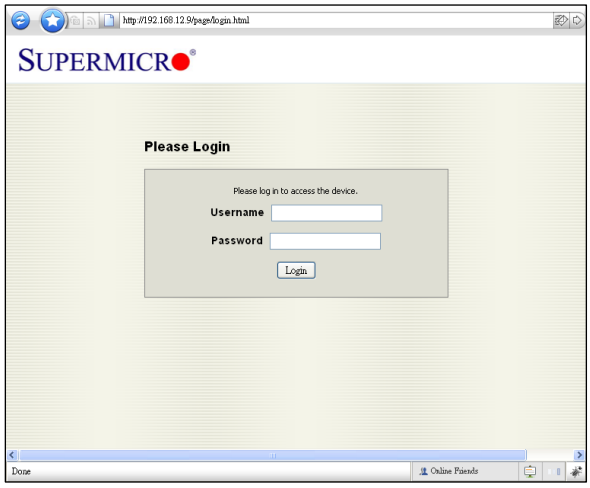


Figure 7-46

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

Figure 7-47

For CDU Managed hosts, one remote control command is available:

- **CDU Web:** This opens a Web browser to connect to a CDU Web running on a CDU system. You can

use this command to view detailed CDU device and sensor information, update device FW, and more.

7.3.6 Host Admin Commands

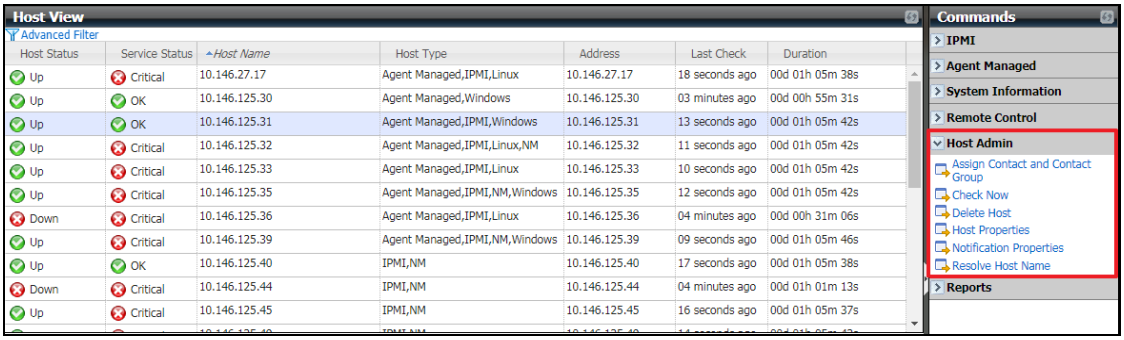


Figure 7-48

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.

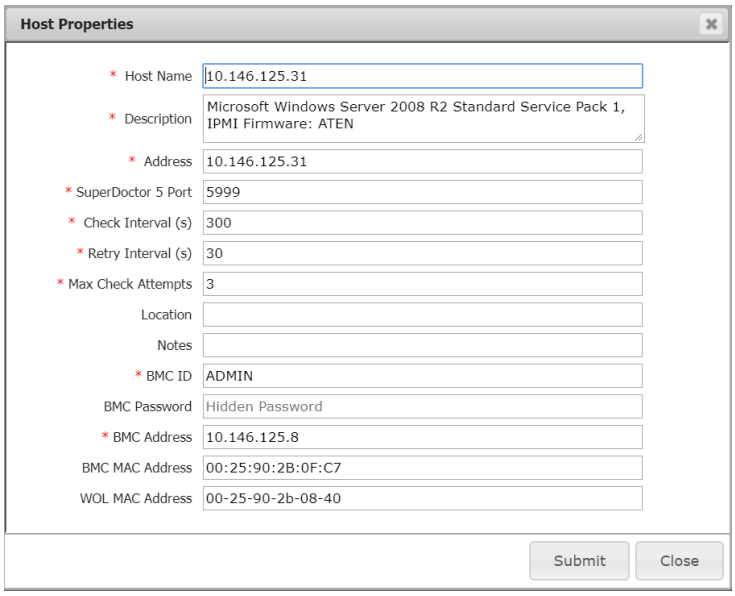


Figure 7-49

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.

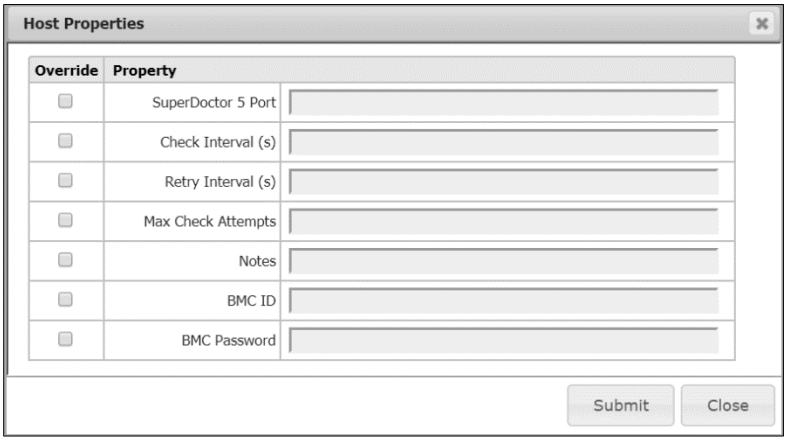


Figure 7-50

When multiple hosts[6] 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.

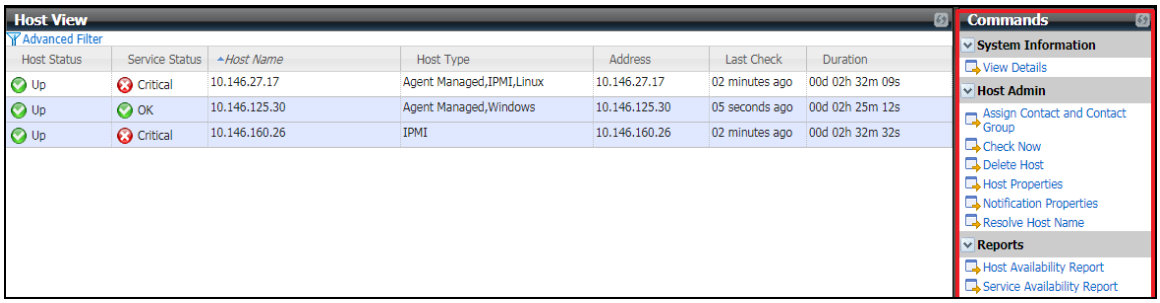


Figure 7-51

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.

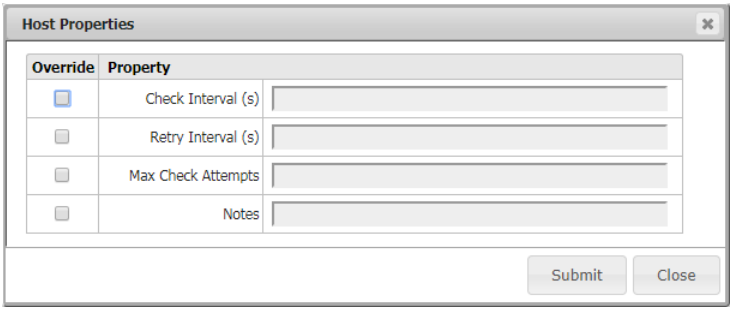


Figure 7-52

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

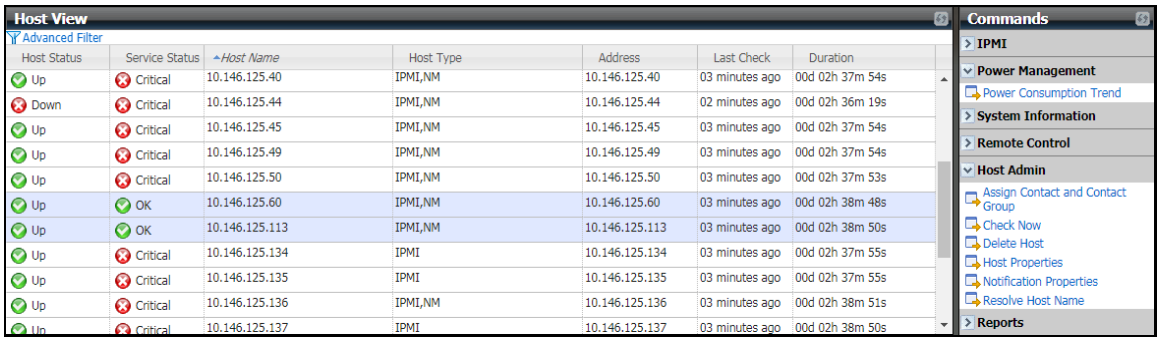


Figure 7-53

[6] 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.

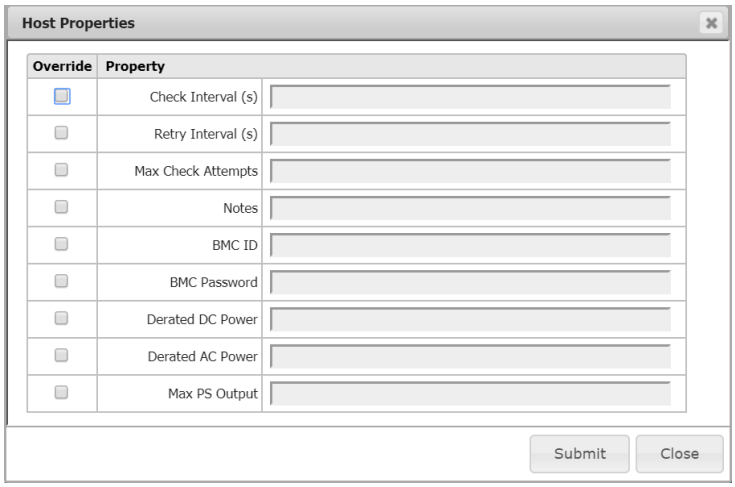


Figure 7-54

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.

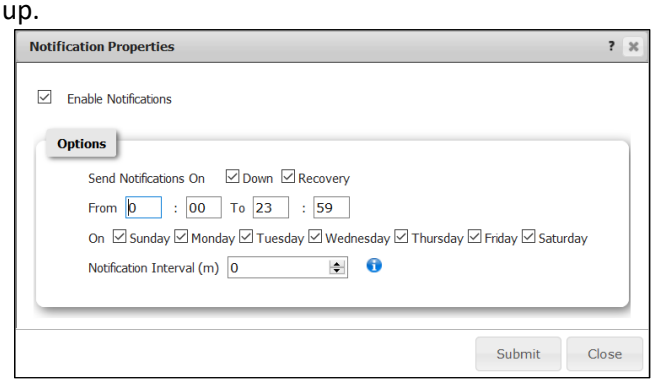


Figure 7-55

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.

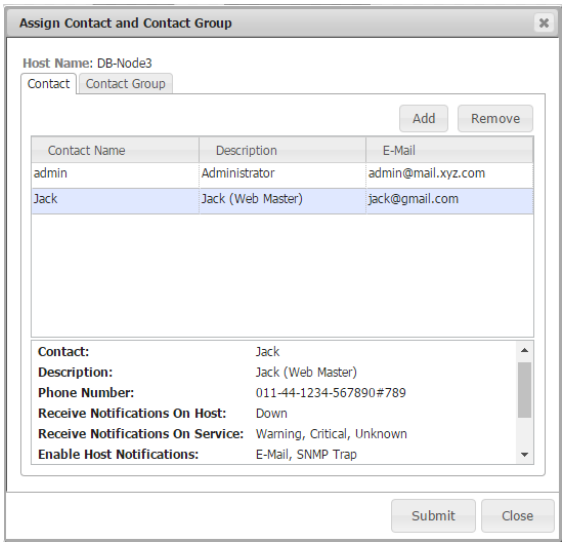


Figure 7-56

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.

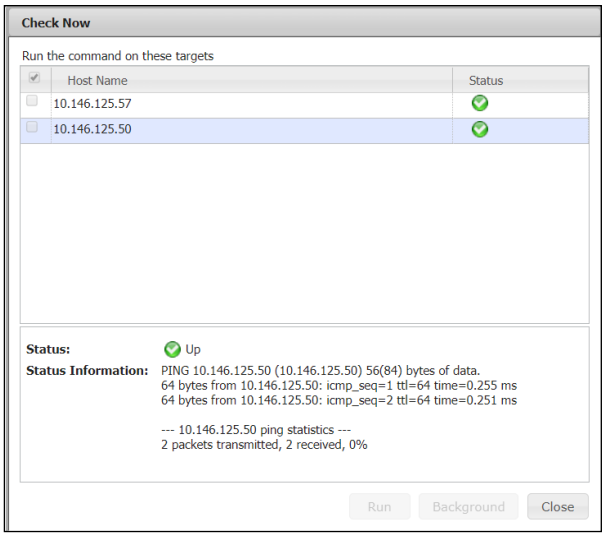


Figure 7-57

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.

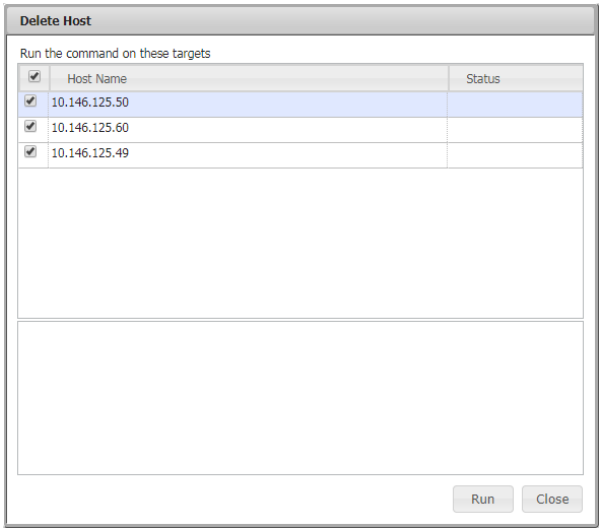


Figure 7-58

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.

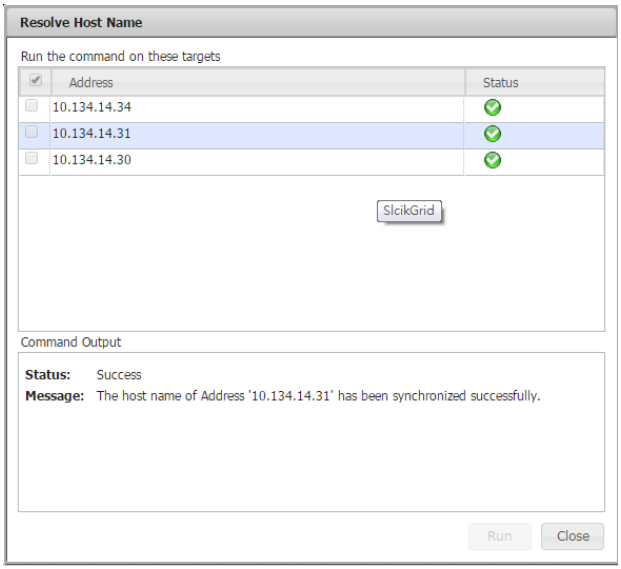


Figure 7-59

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.

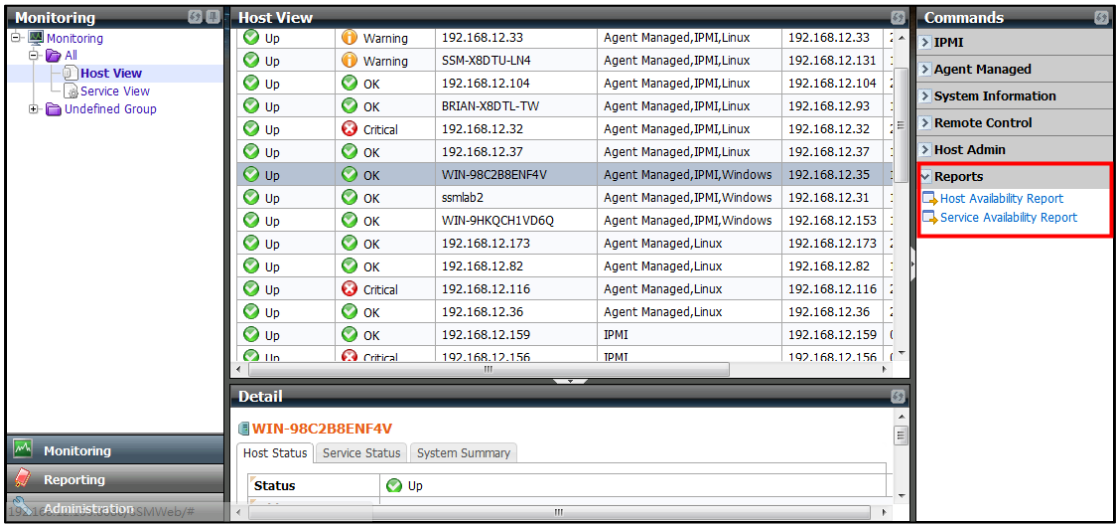


Figure 7-60

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 7-61 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 7-62 Service Availability Report (Example)

7.3.8 Service Admin Commands

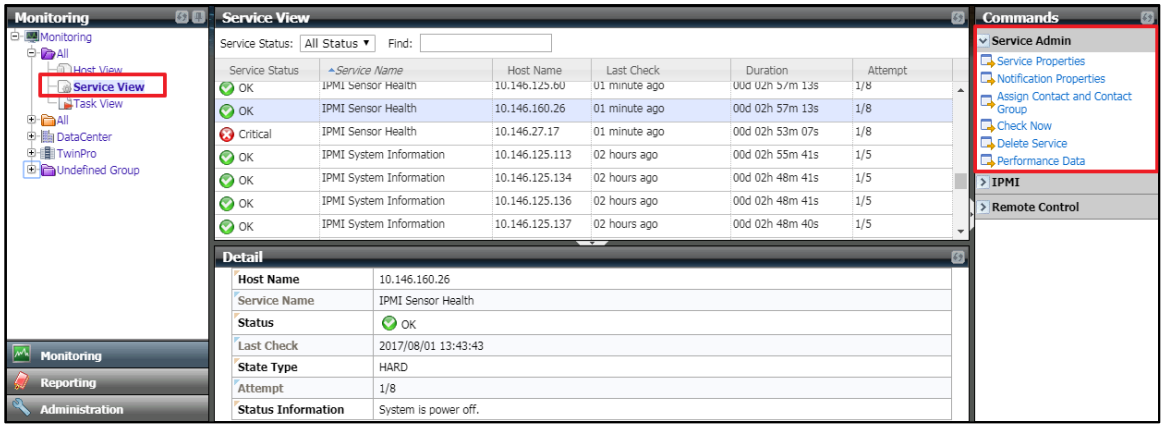


Figure 7-63

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.

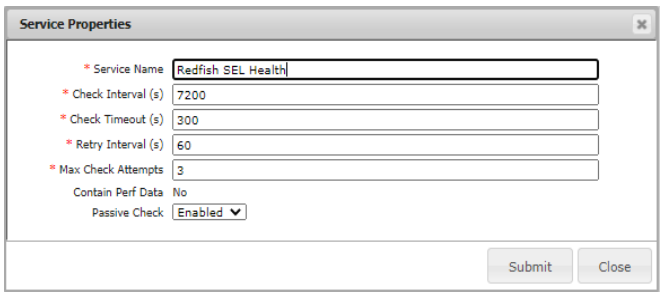


Figure 7-64

Note: You can enable or disable the passive check function in IPMI/Redfish SEL Health service where it is supported.

Also, when selecting multiple services[7] 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.

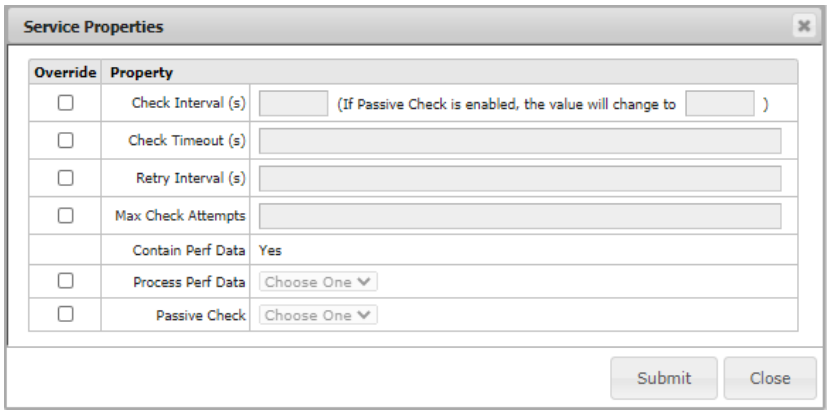


Figure 7-65

Note that not all services you select support passive checks. The check interval attribute will be decided if Passive Check is enabled.

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.

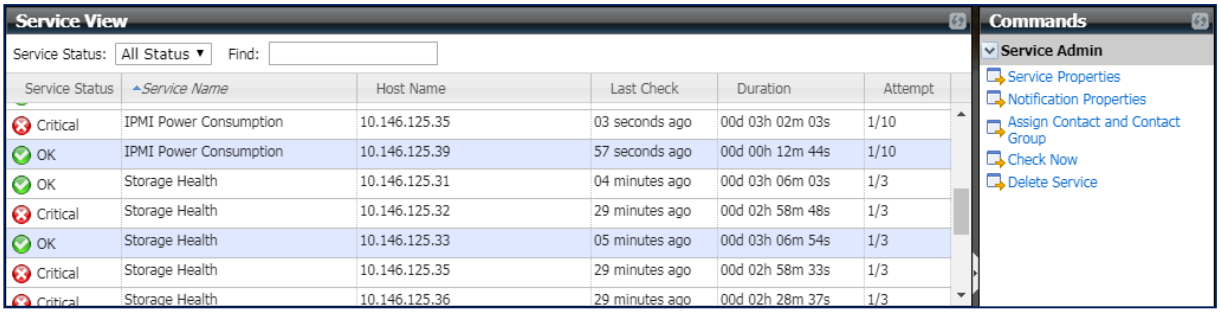


Figure 7-66

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

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.

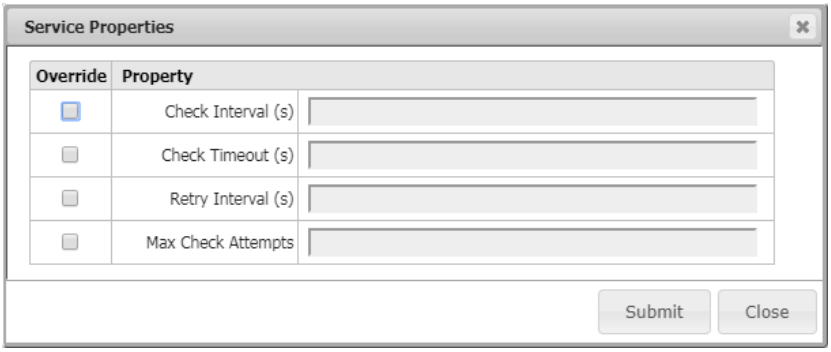


Figure 7-67

For another example, suppose that you select two IPMI Power Consumption services and execute the **Service Properties** command.

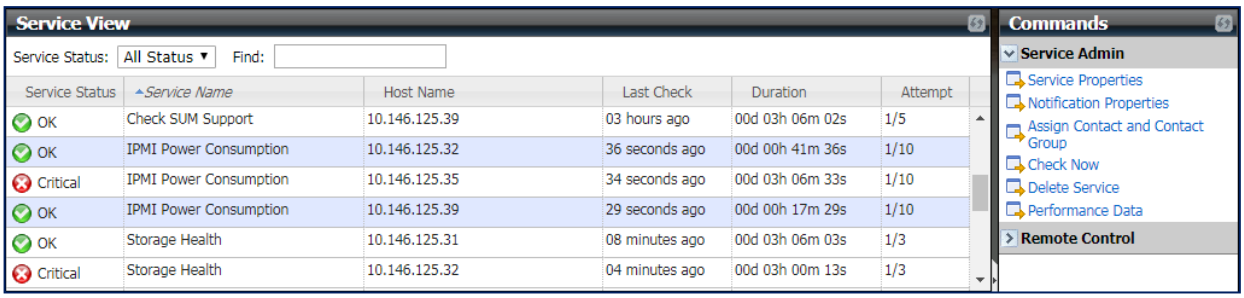


Figure 7-68

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.

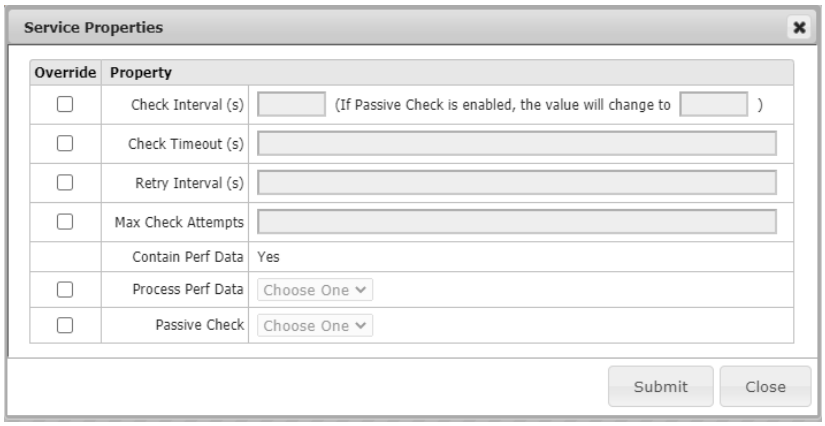


Figure 7-69

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.

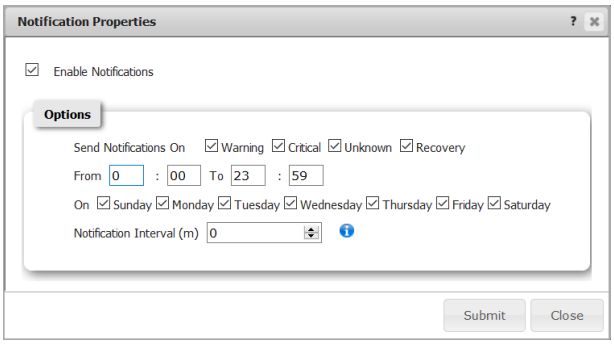


Figure 7-70

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.

Figure 7-71

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.

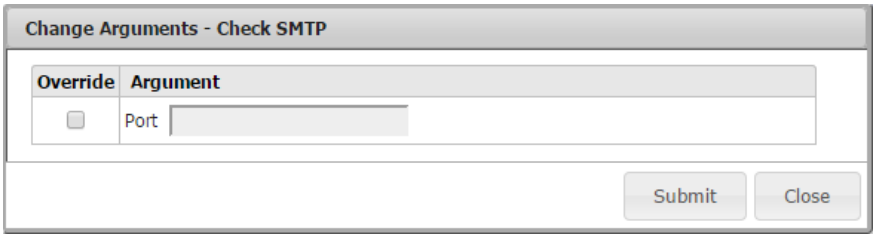


Figure 7-72

Storage Health

When you select a **Storage Health** service and execute the command, a Change Arguments dialog box will appear.

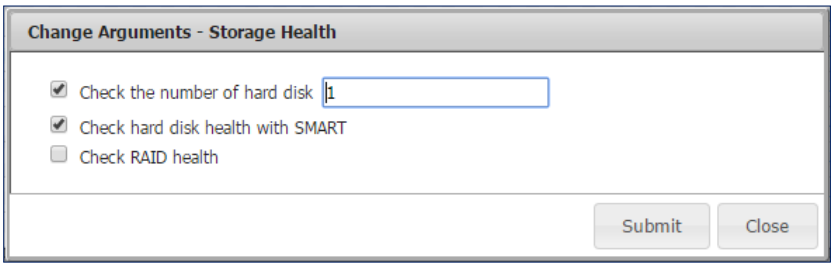


Figure 7-73

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.

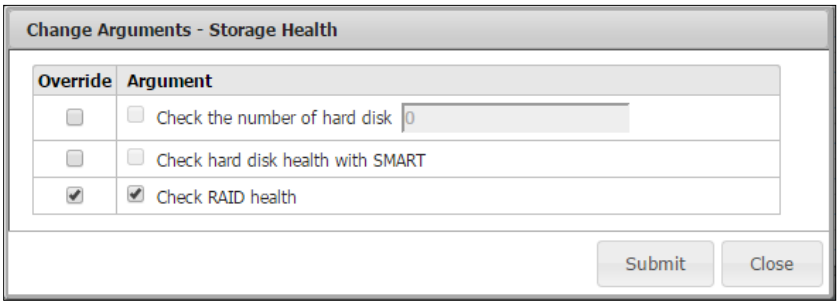


Figure 7-74

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.”

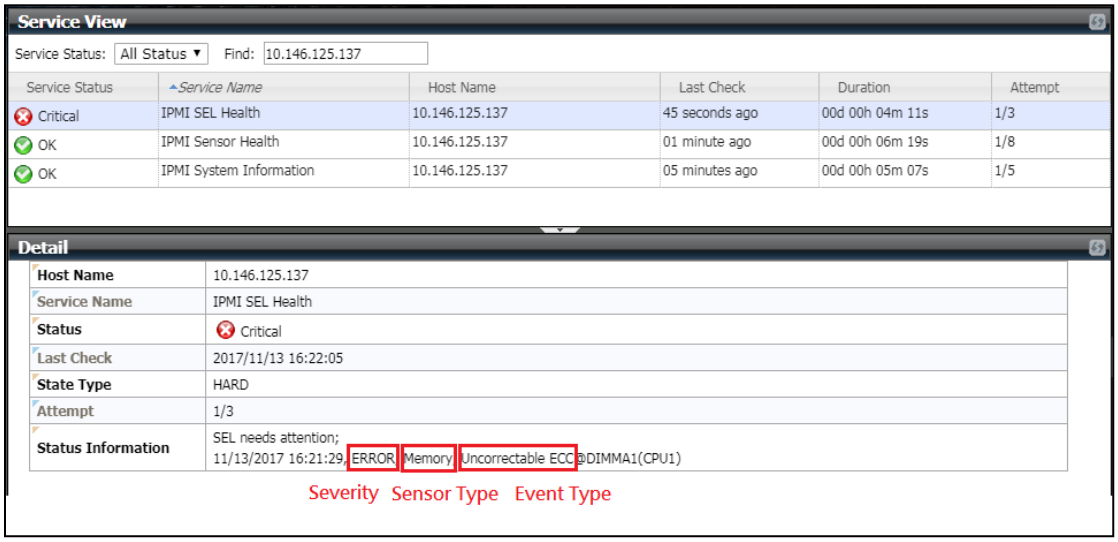


Figure 7-75

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.

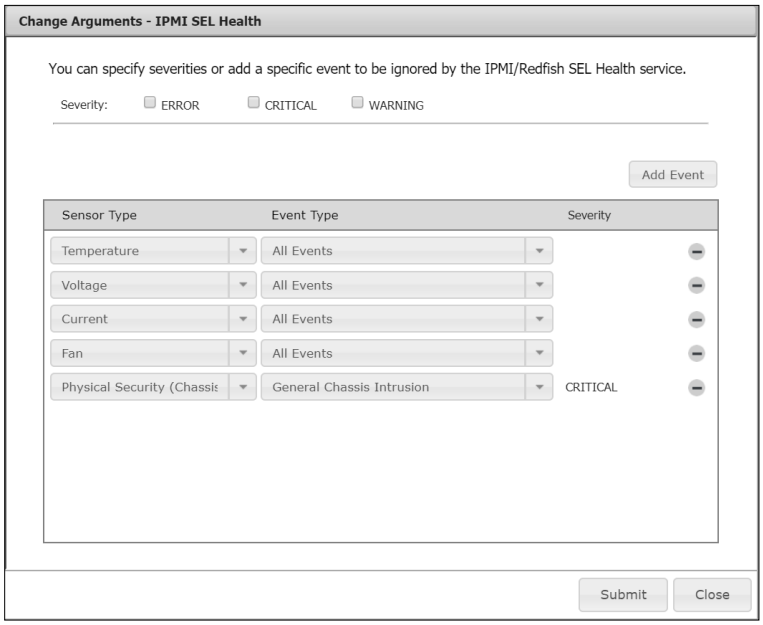


Figure 7-76

2. Click the **ERROR** check box to ignore all events with ERROR severity.

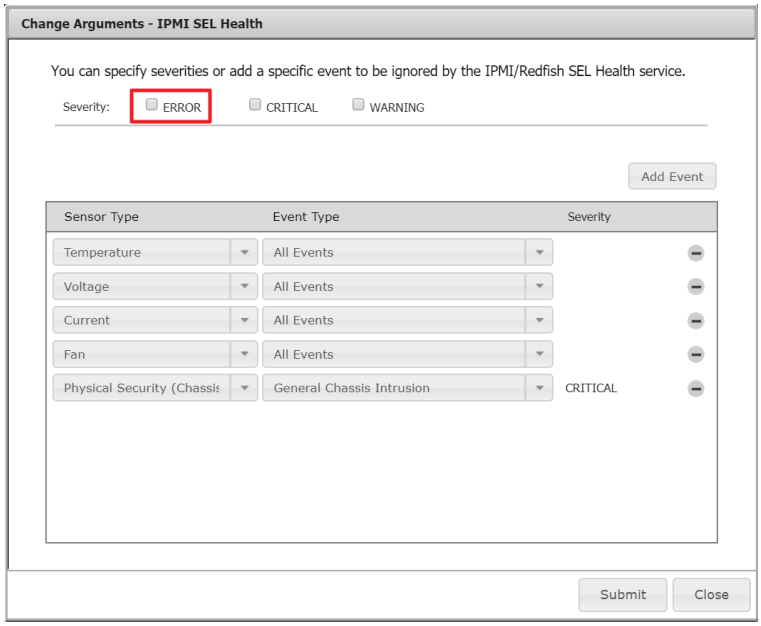


Figure 7-77

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.

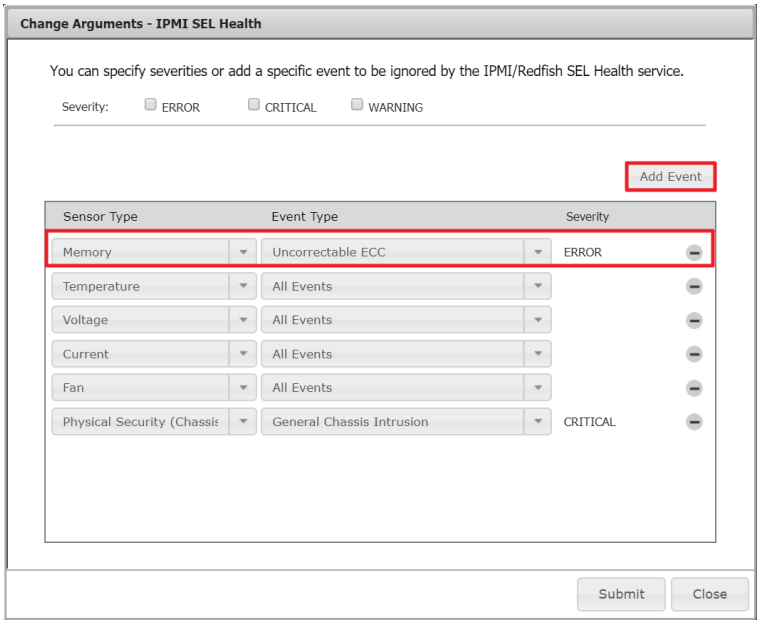


Figure 7-78

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.

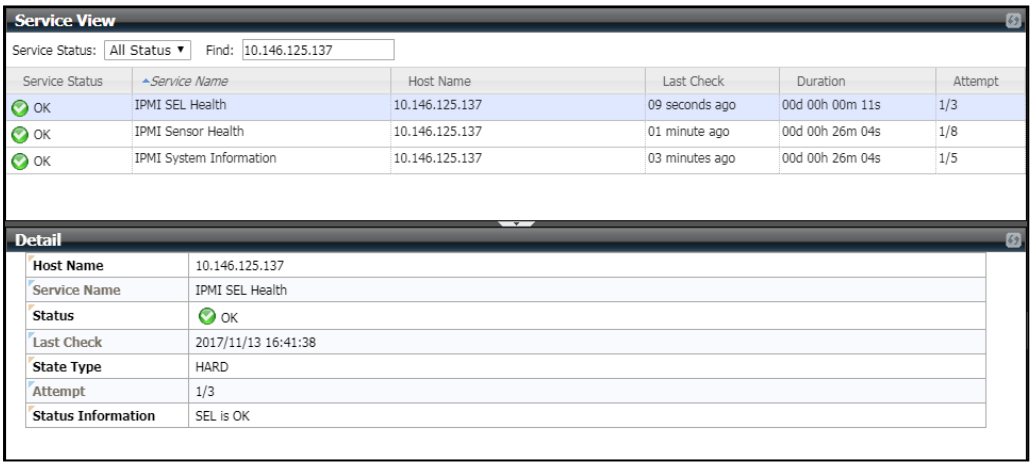


Figure 7-79

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.

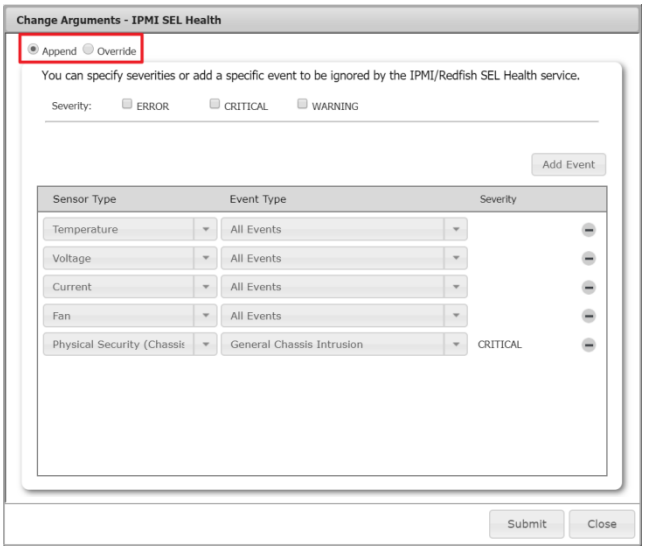


Figure 7-80

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.

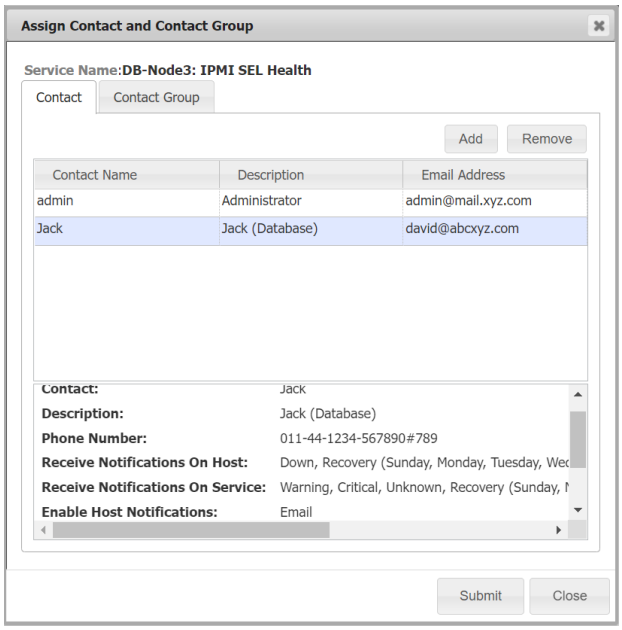


Figure 7-81

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.

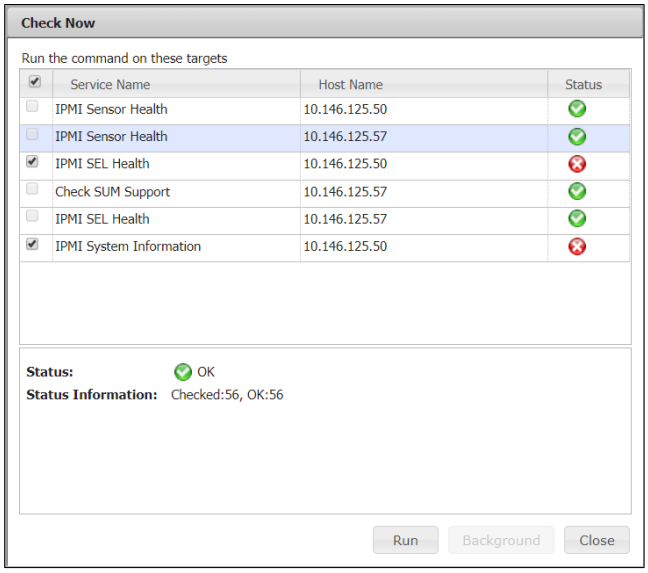


Figure 7-82

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.

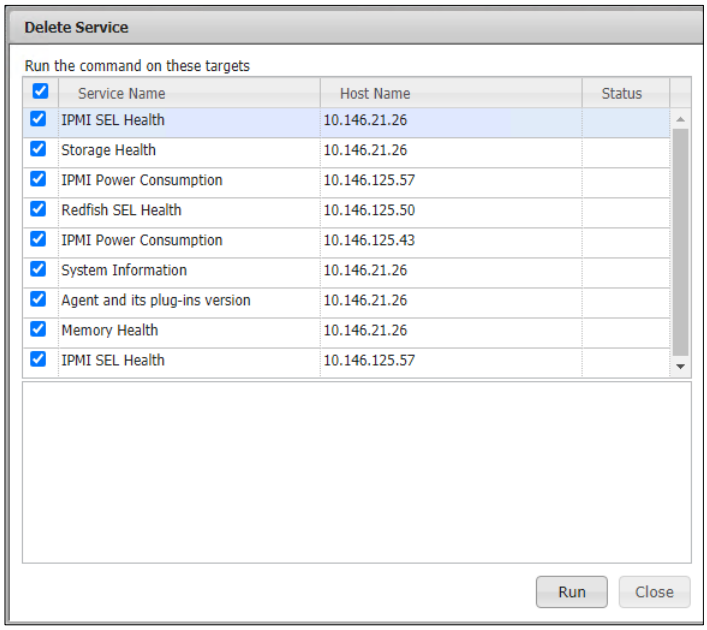


Figure 7-83

7.3.8.7 Performance Data Command

Two SSM built-in services, the **Built-in Sensor Health** and **IPMI/Redfish 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.

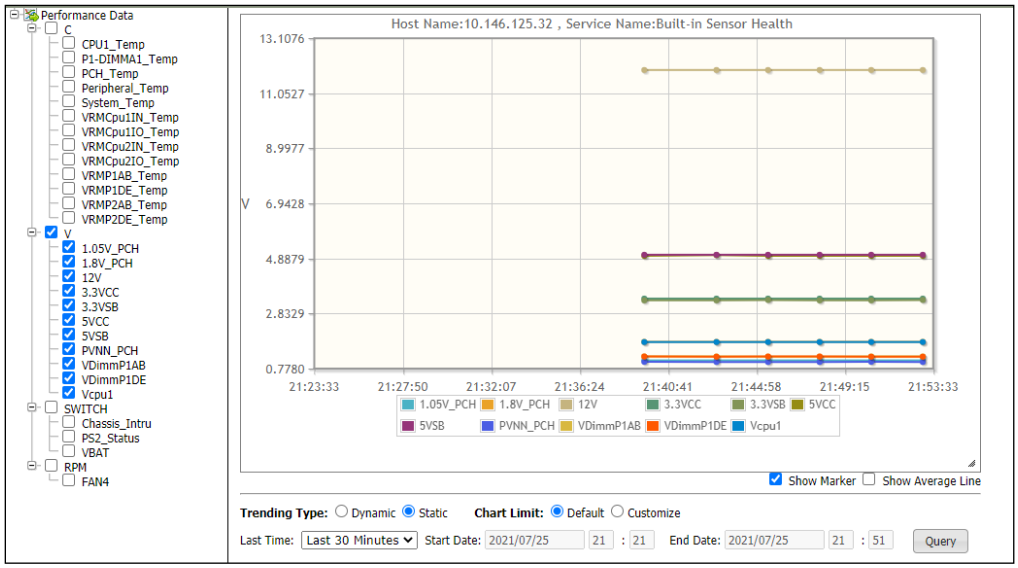


Figure 7-84: Performance Data dialog of a Built-in Sensor Health service

The performance data of an individual host stored in the SSM Database contains three different formats: raw data, aggregated hourly data and aggregated daily 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 hourly 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 daily 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 hourly 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 daily performance data is not available. In other words, The Performance Data dialog uses the aggregated hourly 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 Built-in Sensor Health service as shown above contains 28 items: **FAN4(RPM)**, **1.05V_PCH(V)**, **P1-DIMMA1_Temp(℃)** and **System_Temp(℃)**, 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 Built-in Sensor Health service is 300 seconds, which means 28 different records in the SSM Database are created every 300 seconds for a single **Built-in Sensor Health** service. If you have 100 Built-in Sensor Health services, 806,400 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

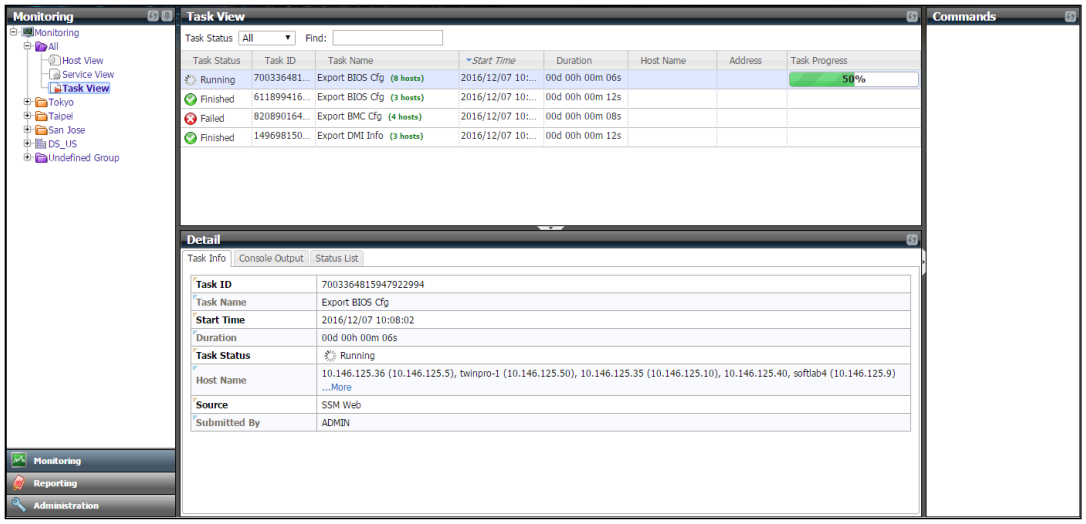


Figure 7-85

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 or pending.
- **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.

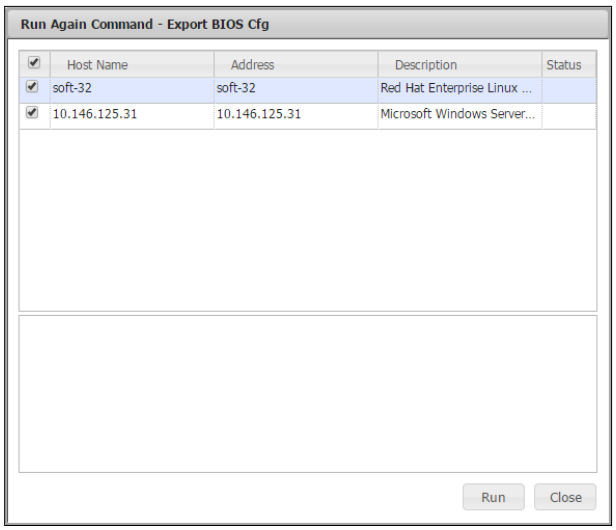


Figure 7-86

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.

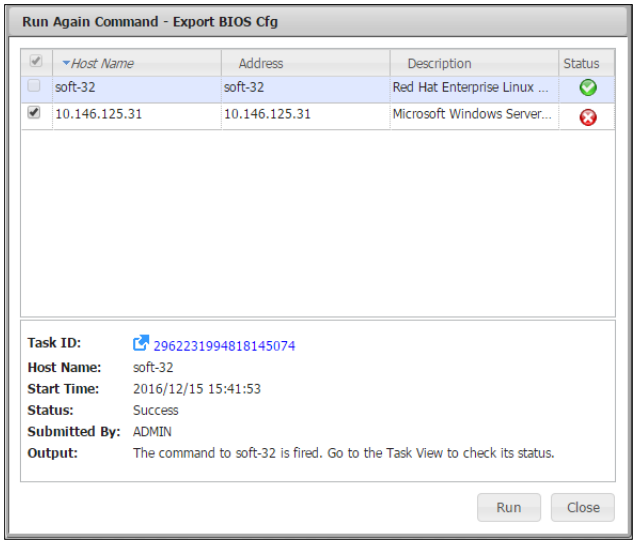


Figure 7-87

7.3.9.2 Delete Task Command

The **Delete Task** command applies to the finished, failed, or pending 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.

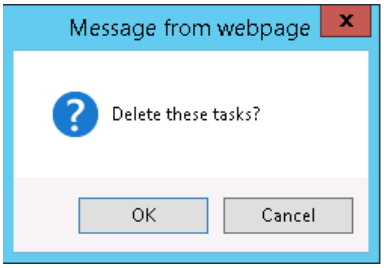


Figure 7-88

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.

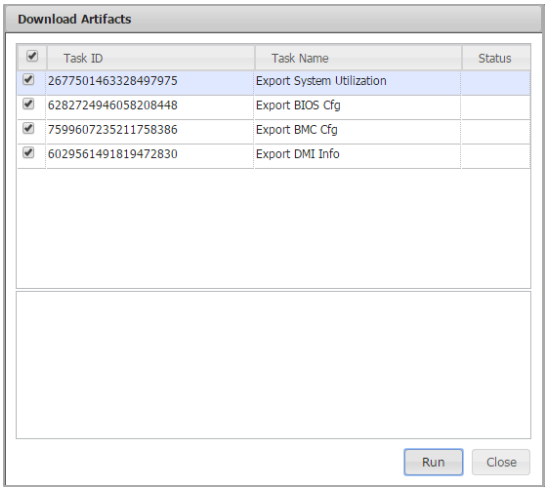


Figure 7-89

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.

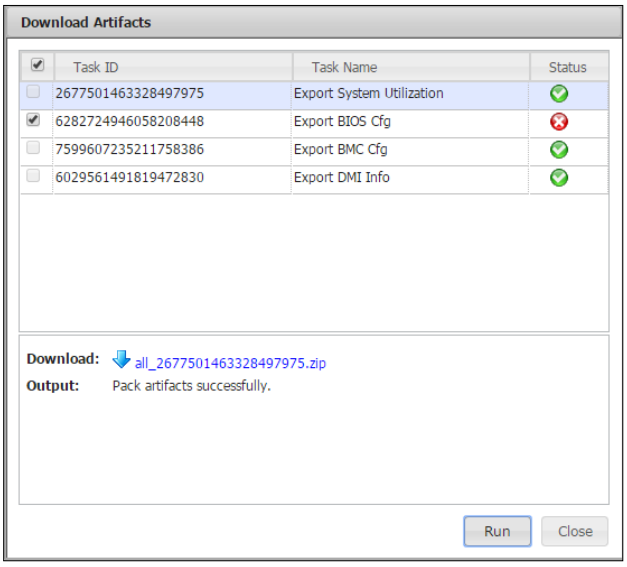


Figure 7-90

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

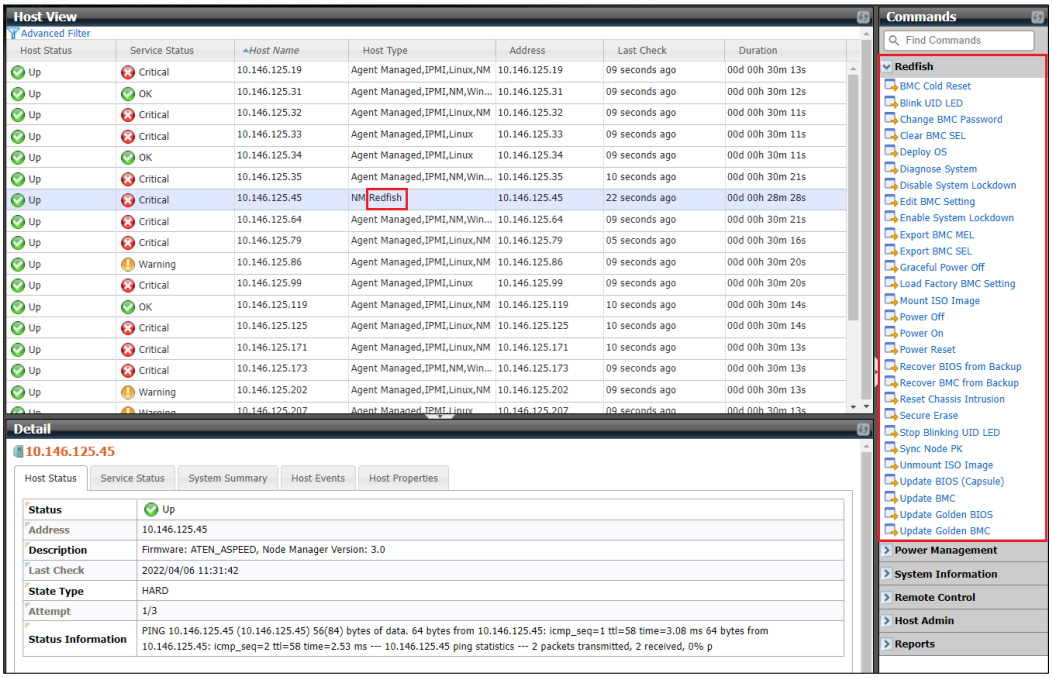


Figure 7-91

Commands in this category as shown below apply only to Redfish hosts. They are similar to those in the IPMI category, but they 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 SEL:** Clears the BMC health event logs.
- **Deploy OS**: Deploys Linux OS on a host. See *10.3.8 FW Auto Update: Change Schedule* for details.

- **Diagnose System:** Diagnoses if there are faults or problems with system boot-up. See *13 System Diagnostics* for more information.
- **Disable System Lockdown:** Disables a host's lockdown mode. Note that the managed system must be Supermicro X12/H12 series or later.
- **Edit BMC Setting:** Changes specific of BMC setting items**.** You can click the **Add Item** button to specify BMC setting items to be updated.

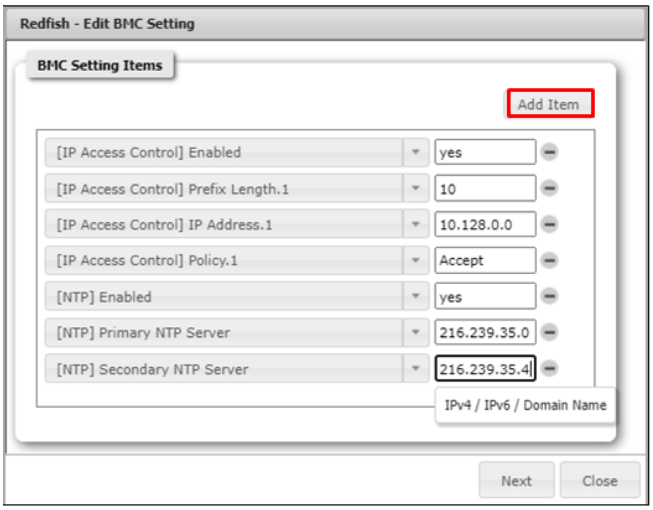


Figure 7-92

- **Edit DMI Info:** Changes specific DMI information items.
  1). Click **SSM New GUI → Monitoring → Host Monitoring view** to view the status of hosts.
  2). Select hosts in the working area. You can select multiple hosts at a time of the same host type.
  3). Click the **Toolbar** icon in the upper right corner of the Host View, then click **Edit DMI Info** in the Redfish commands area, and an Edit DMI Info - Arguments dialog box will pop up.
  4). Expand the specific DMI items and then enter the desired description in the fields.
  5). Click **Next** and then click **Run** button to execute the command.
  6). Click the **Submit** button to reboot the system.
  7). Click the **Task ID** link to go the Task View. SSM uses an asynchronous task to represent the request that takes longer time to complete.
- **Enable System Lockdown:** Enables a host's lockdown mode. Note that the managed system must be a Supermicro X12/H12 series or later.
- **Export BMC SEL**: Exports the BMC health event logs.
- **Export BMC MEL**: Exports the BMC maintenance event logs.
- **Graceful Power Off**: Powers off a host gracefully.
- **Load Factory BIOS Setting:** Restores BIOS to the default factory settings.
  1). Click **SSM New GUI → Monitoring → Host Monitoring view** to view the status of hosts.
  2). Select hosts in the working area. You can select multiple hosts at a time of the same host type.
  3). Click the **Toolbar** icon in the upper right corner of the Host View, and click the **Load Factory BIOS Setting** in the Redfish commands area. The Load Factory BIOS Setting dialog box will appear.
  4). Click the **Run** button to execute the command.
  5). Click the **Submit** button to reboot the system.
  6). Click the **Task ID** link to go the Task View. SSM uses an asynchronous task to represent the request that takes longer time to complete.
- **Load Factory BMC Setting:** Restores the BMC to the default factory settings. Note that not all of the BMC settings will be set to factory default, for SSM to continue monitoring, the settings of network, FRU, and user will be retained.

- **Mount ISO Image:** Provides the selected hosts with an ISO Image as Virtual Media through BMC and the SAMBA Server. In the Arguments dialog box, you need to designate an image URL and input the access options, as shown below. Note that the managed system must be a Supermicro X12 series or later.

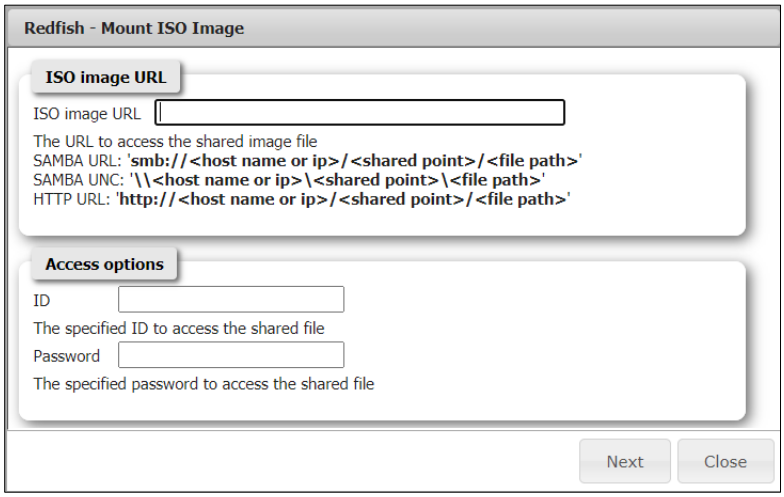


Figure 7-93

- **Power Off**: Powers off a host immediately.
- **Power On**: Powers on a host.
- **Power Reset**: Resets (reboots) a host immediately.
- **Recover BIOS from Backup:** Recovers BIOS from the backup firmware image. Note that the managed system must support the RoT system.
- **Recover BMC from Backup:** Recovers BMC from the backup firmware image. Note that the managed system must support the RoT system.
- **Reset Chassis Intrusion**: Resets a chassis intrusion flag.
- **Secure Erase**: Erases a specific drive slot connected to LSI MegaRAID 3108 and its later generations such as 3908 and 3916. In the Arguments dialog box, you need to select a drive slot. Note that the managed system must be Supermicro X12 series or later.

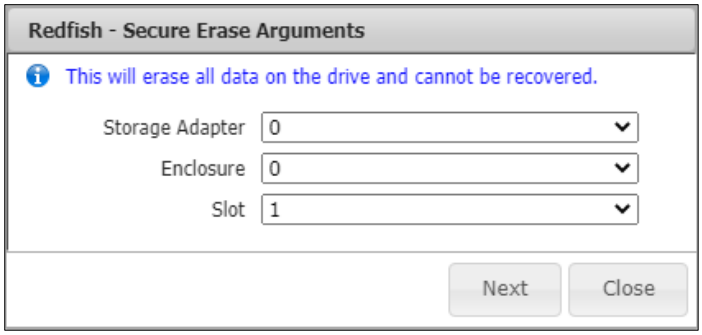


Figure 7-94

- **Stop Blinking UID LED**: Stops a host's UID LED from blinking.
- **Sync Node PK**: Syncs node product keys between SSM and BMC.
- **Unmount ISO Image:** Removes an ISO image as Virtual Media from the selected hosts. Note that the managed system must be Supermicro X12 series or later.
- **Update BIOS (Capsule):** Updates the selected hosts with an image file. In the Arguments dialog box, you need to upload a BIOS image file and choose the flash options, as shown below. Note that the managed system must be Supermicro X12 series or later.

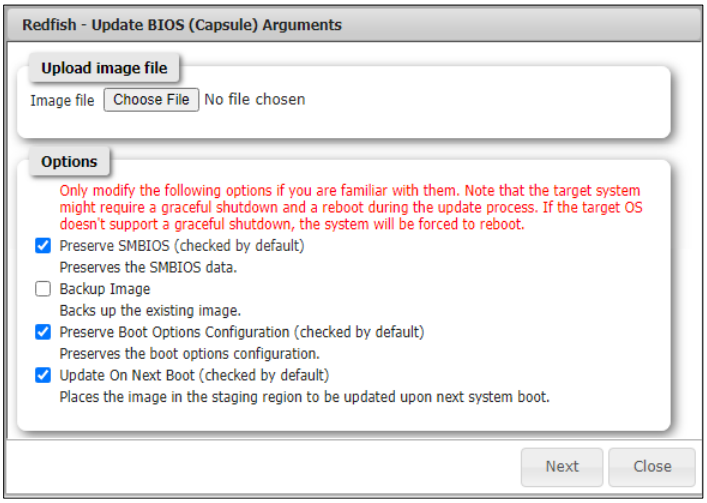


Figure 7-95

Notes:

- The options in Update BIOS (Capsule) Arguments may vary depending on the selected motherboard or system, and they will be available while the System Information service check is being performed. To update multiple hosts all at once, the motherboards of these selected hosts must be from the same series.
- You can use the **Update On Next Boot** option to update BIOS (Capsule) on X12/H12 and later RoT systems without an immediate system reboot. If you select the option and run the command, and the image file is uploaded to the staging region, the task will be in the pending status in the task view. The pending task will resume and continue the update process after the selected hosts reboot or power up. You can also abort the pending task by running the **Delete Task** command in the commands area. Note that the name of the task will be **Update BIOS** or **Update MCU Capsule**, depending on the type of BIOS image you upload.
- The selected hosts as non-RoT systems must be rebooted or powered up for the changes to take effect. You can use the **Reboot** option (if available) to reboot after update.

- **Update BMC:** Updates the selected hosts with a BMC image file. In the Arguments dialog box, you need to upload a BMC image file and choose the flash options, as shown below. Note that the managed system must be Supermicro X12 series or later.

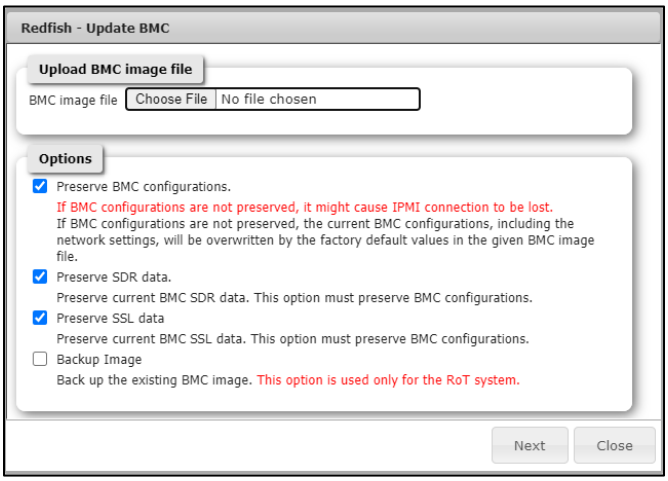


Figure 7-96

- **Update Golden BIOS**: Sets the current active BIOS image as the golden template. Note that the managed system must support the RoT system.
- **Update Golden BMC**: Sets the current active BMC image as a golden template. Note that the managed system must support the RoT system.

Note: For the web commands that require systems to reboot, SSM performs a graceful shutdown to protect the managed systems. If the target OS does not support a graceful shutdown, the system will be forced to be reboot. The Linux OS with X Window systems do not support a graceful shutdown by default, and it is therefore highly recommended that you change the power button setting from "Suspend" to "Power Off." The system will then shut down after the power button is pressed.

Commands in this category shown below apply to CMM_Redfish 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 SEL:** Clears the BMC health event logs.
- **Load Factory CMM Setting:** Restores the CMM to the default factory settings. Note that not all of the CMM settings will be set to factory default. The settings of the network, FRU, and the user will be retained for SSM to continue monitoring.
  1). Click **SSM New GUI → Monitoring → Host Monitoring view** to view the status of hosts.
  2). Select hosts in the working area. You can select multiple hosts at a time of the same host type.
  3). Click the **Toolbar** icon in the upper right corner of the Host View, and click the **Load Factory CMM Setting** in the CMM Redfish commands area. The Load Factory CMM Setting dialog box

will appear.

4). Click the **Run** button to execute the command.

5). Click the **Task ID** link to go the Task View. SSM uses an asynchronous task to represent the request that takes longer time to complete.

- **Stop Blinking UID LED**: Stops a host's UID LED from blinking.
- **Turn Blade UID On/Off**: Causes a CMM host's UID LED to blink to identify a specific physical host in a data center.
- **Update CMM:** Updates the CMM firmware image. You need to upload a CMM firmware image file in the Update CMM Arguments dialog box. Note that the managed system must be Supermicro CMM-6 or later.

Note: For Redfish or CMM_Redfish hosts, when you execute a **Load Factory BMC Setting** or a **Load Factory CMM Setting** command, it's likely that the IP address and user credentials will be restored to factory defaults. You'll need to modify the IP address and user credentials on BMC Web first and then execute the **Host Properties** web command for SSM to add itself to the target BMC as an event subscriber**.**

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 state[8] (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 state[9] (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.

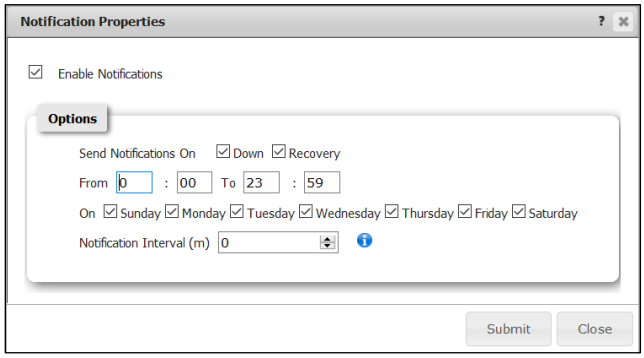


Figure 7-97

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.

[8] The status of the host changes from a non-UP state to another non-UP state will also trigger a problem alert.

[9] The status of the service changes from a non-OK state to another non-OK state will also trigger a problem alert.

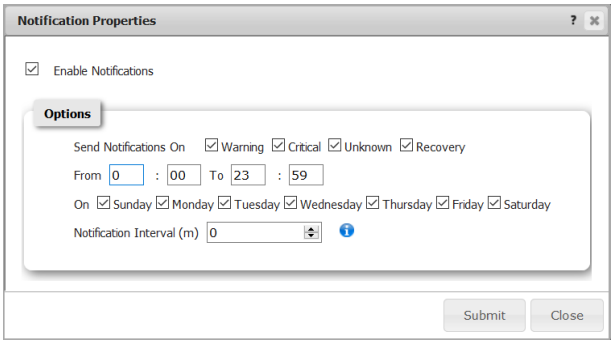


Figure 7-98

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.

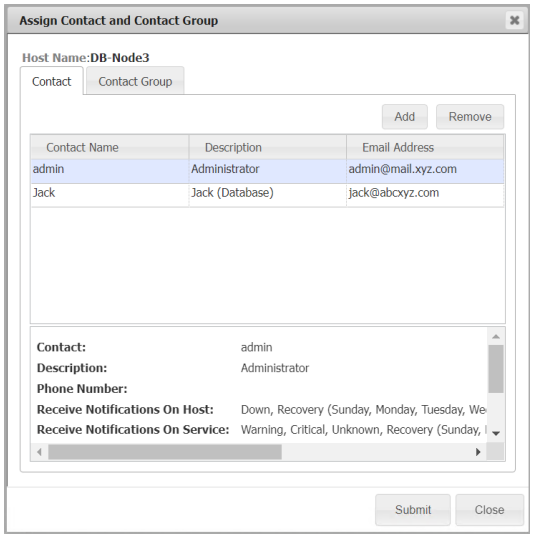


Figure 7-99

Each contact can define its time period and notification methods to receive notifications. See *6.4.1 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 Email 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.

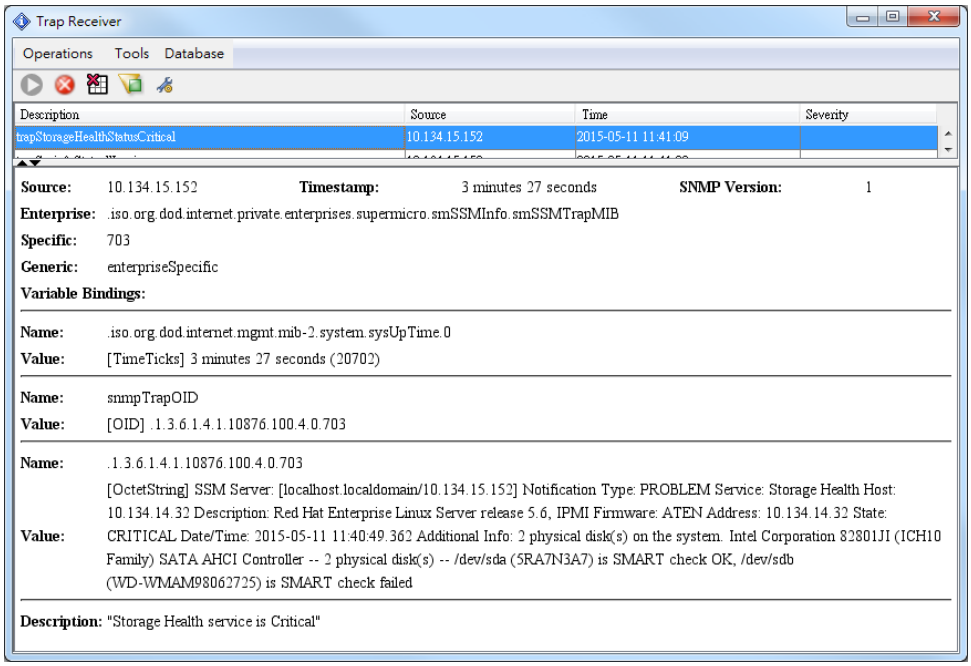


Figure 7-100

8 SSM Web Reporting Page

8.1 SSM Server Report

Three reports related to the SSM Server are supported:

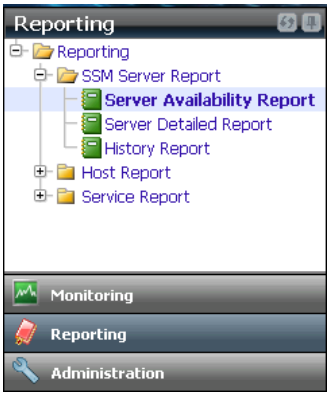
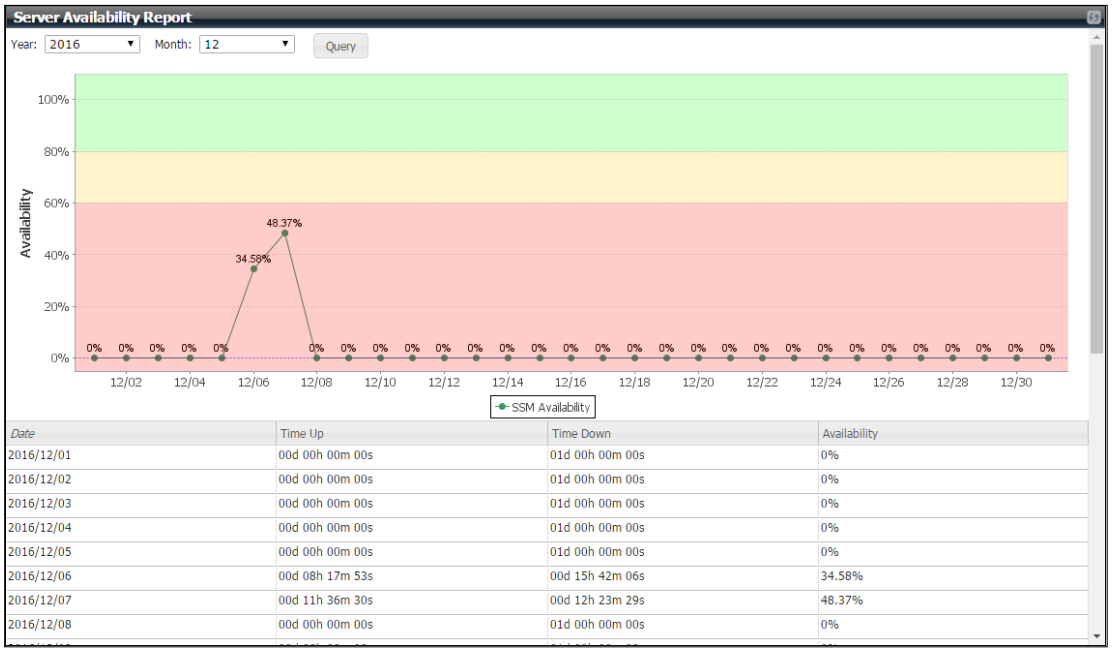


Figure 8-1

- **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.

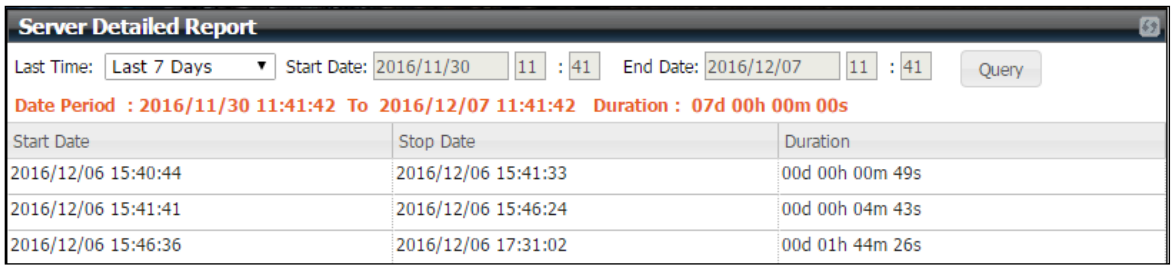


Date	Time Up	Time Down	Availability
2016/12/01	00d 00h 00m 00s	01d 00h 00m 00s	0%
2016/12/02	00d 00h 00m 00s	01d 00h 00m 00s	0%
2016/12/03	00d 00h 00m 00s	01d 00h 00m 00s	0%
2016/12/04	00d 00h 00m 00s	01d 00h 00m 00s	0%
2016/12/05	00d 00h 00m 00s	01d 00h 00m 00s	0%
2016/12/06	00d 08h 17m 53s	00d 15h 42m 06s	34.58%
2016/12/07	00d 11h 36m 30s	00d 12h 23m 29s	48.37%
2016/12/08	00d 00h 00m 00s	01d 00h 00m 00s	0%

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.



Start Date	Stop Date	Duration
2016/12/06 15:40:44	2016/12/06 15:41:33	00d 00h 00m 49s
2016/12/06 15:41:41	2016/12/06 15:46:24	00d 00h 04m 43s
2016/12/06 15:46:36	2016/12/06 17:31:02	00d 01h 44m 26s

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.

History Report

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 Query

<< < 1 2 3 4 5 6 7 8 9 10 > >>

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

Five types of host reports are supported:

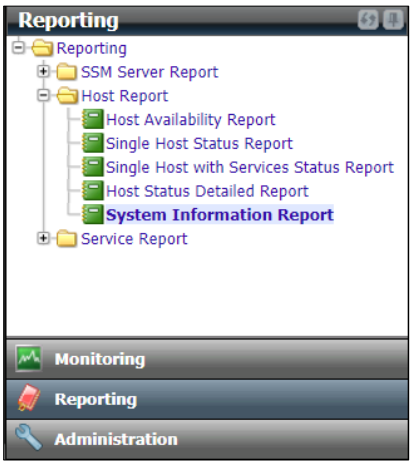


Figure 8-5

- **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.
- **System Information Report**: Shows the host's information, including name, address, BMC version, BIOS version, motherboard model, and system model.

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.

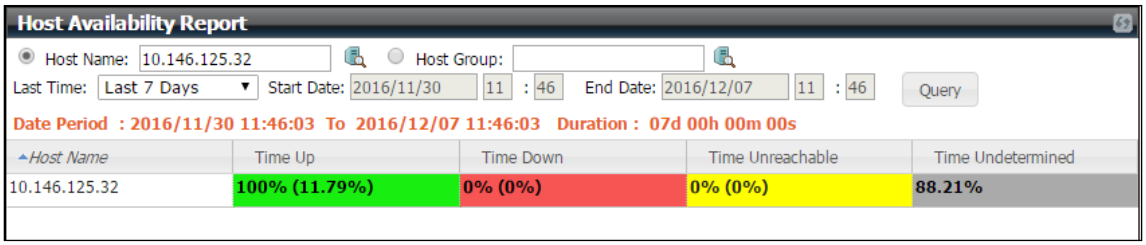


Figure 8-6

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.

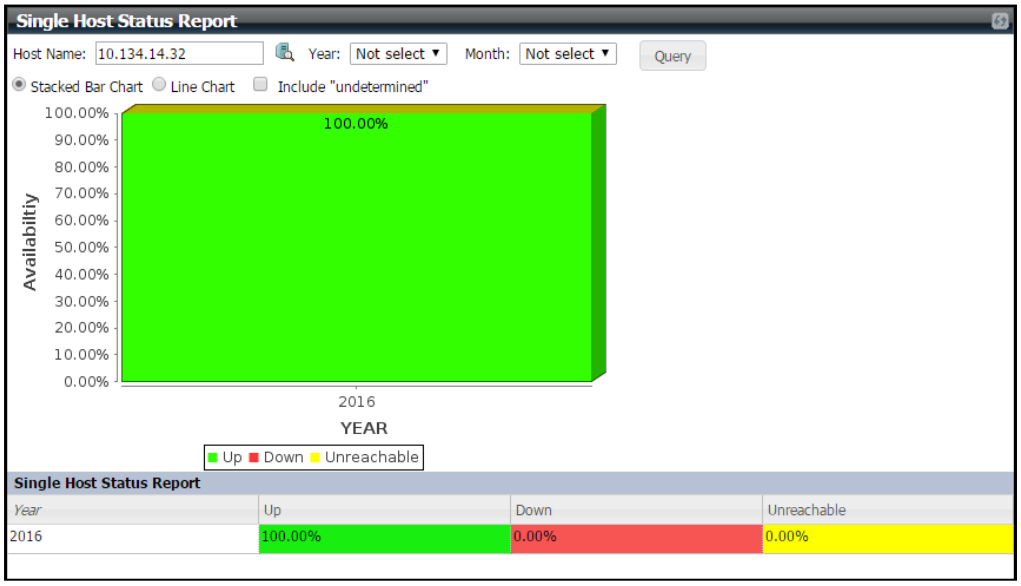


Figure 8-7

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.

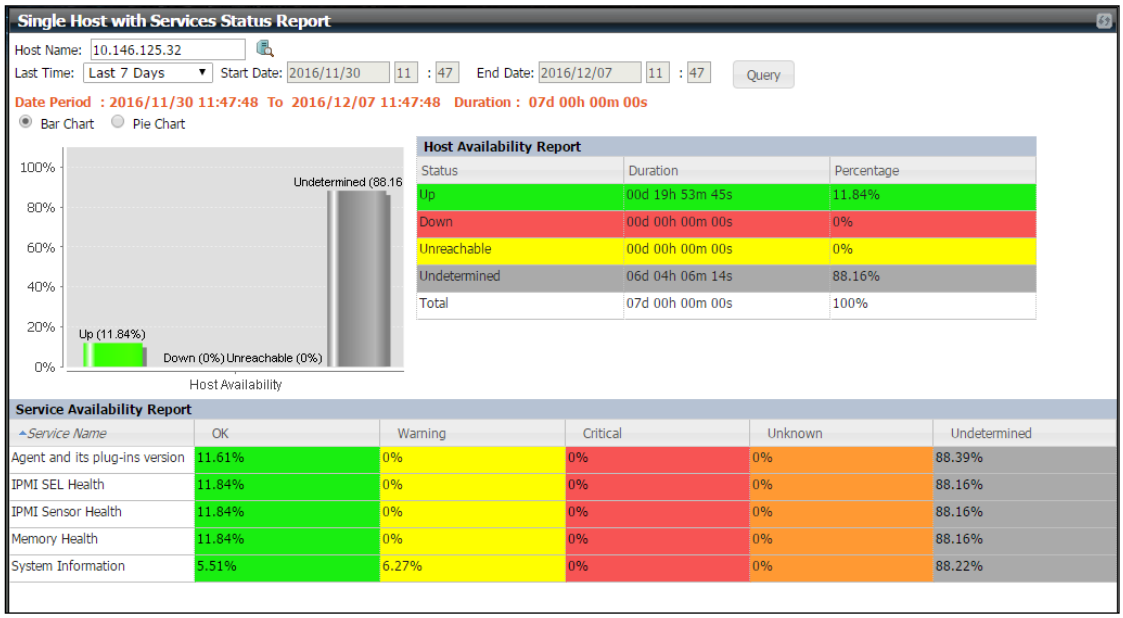


Figure 8-8

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.

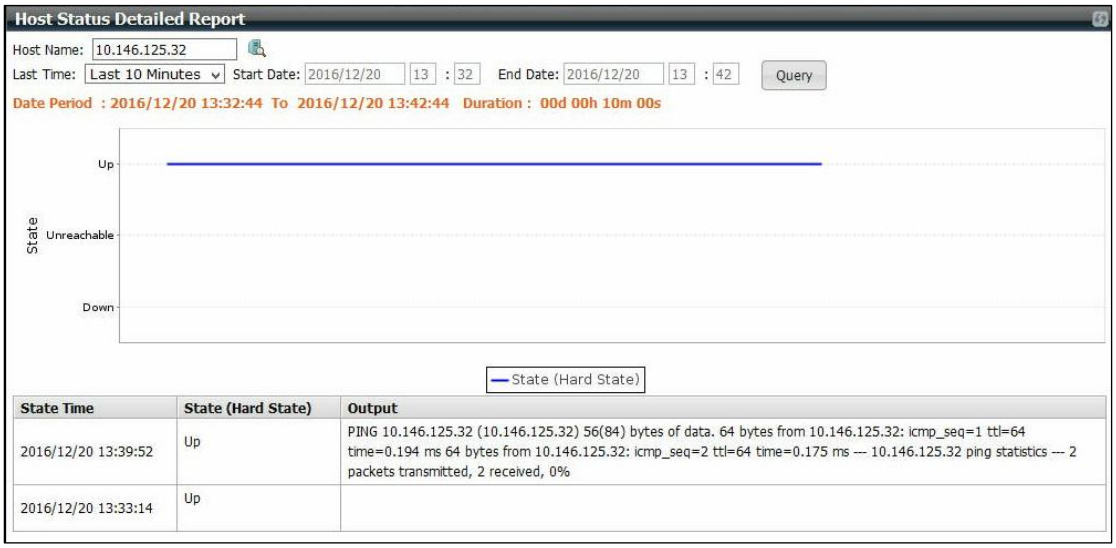


Figure 8-9

8.2.5 System Information Report

Click **Reporting → Host Report → System Information Report** to use the System Information 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 select the columns from available columns. When completed, click the **Query** button to generate the report or "Save as" button to save the results as a CSV file.

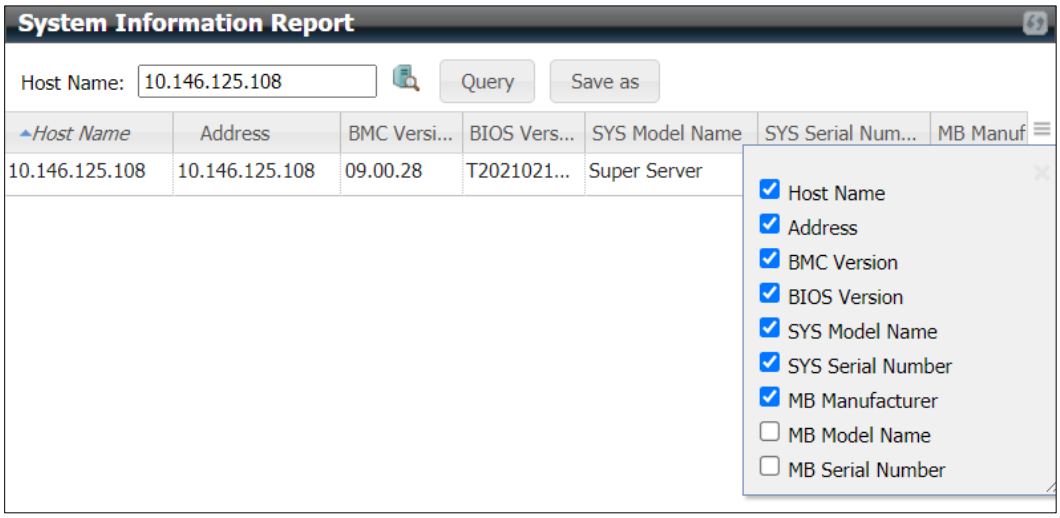


Figure 8-10

8.2.6 Component Health

Click **SSM New GUI → Monitoring → Component Health** to view status of processor and memory. SSM can display the health status of each individual IPMI or Redfish host based on components such as processor and memory. Note that most data in this function is automatically provided by System Information Service (if available).

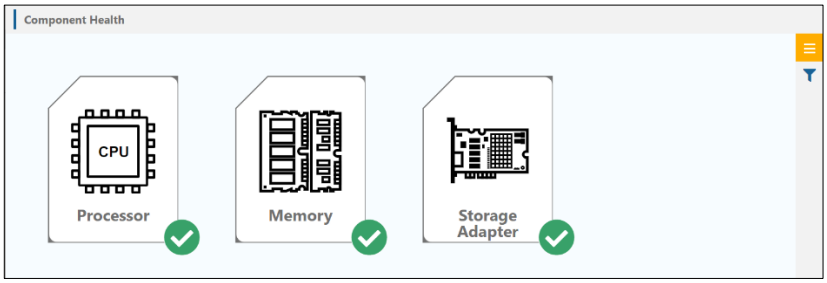


Figure 8-11

8.2.6.1 Processor

Click the **Processor** icon, the CPU status of all hosts managed by SSM management will be displayed:

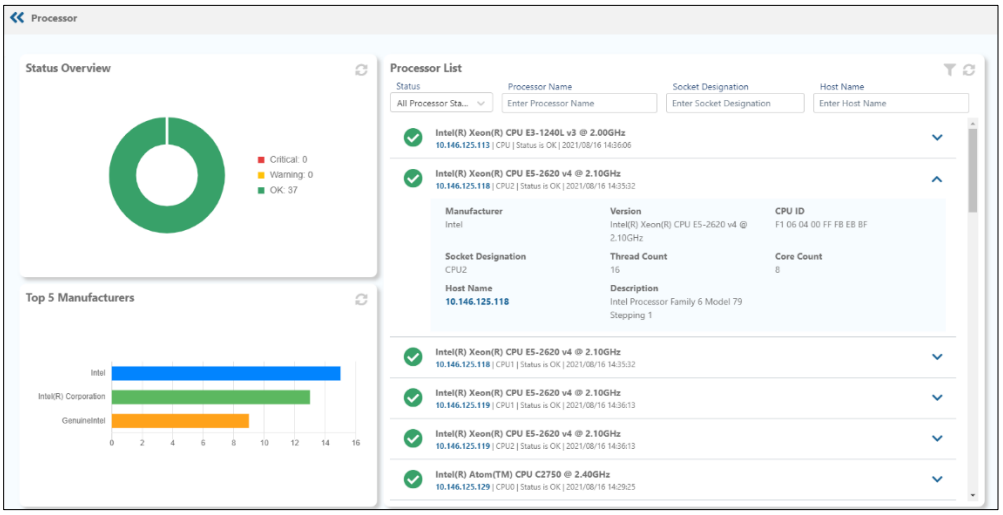


Figure 8-12

- **Status Overview:** Displays the statistics of the processor status of all managed hosts, including **Critical**, **Waring**, and **OK**. Note that the status is gathered for each processor via Supermicro BMC Redfish API.
- **Top 5 Manufacturers:** Displays the statistics of the top five manufacturers of processors of all managed hosts.
- **List of processors of managed hosts:** Accesses the default list of processors of all managed hosts. You can filter by conditions, including individual status ("Critical," "Warning," and "OK") or all status, processor name, socket designation, and host name.
- **Processor Details:** Click the arrow icon on the right side of each processor record to view the details of this processor, including Manufacturer, Socket Designation, Host Name, Version, Thread Count, Description, CPU ID and Core Count. Click **Host Name** to access the details of the individual host.

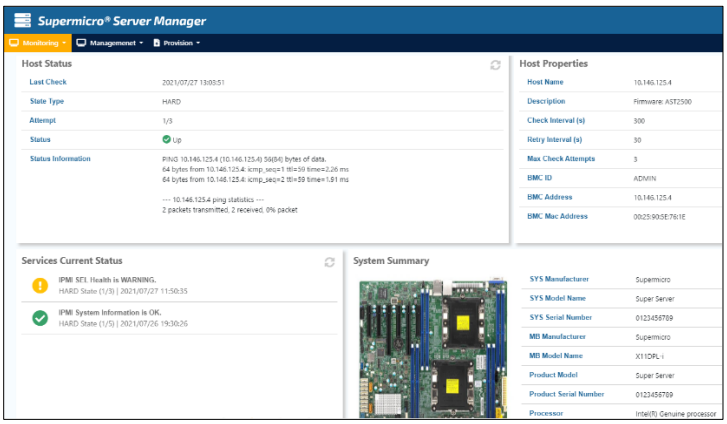


Figure 8-13

8.2.6.2 Memory

Go to the Component Health page and click the **Memory** button to display status of all SSM management hosts' memories.

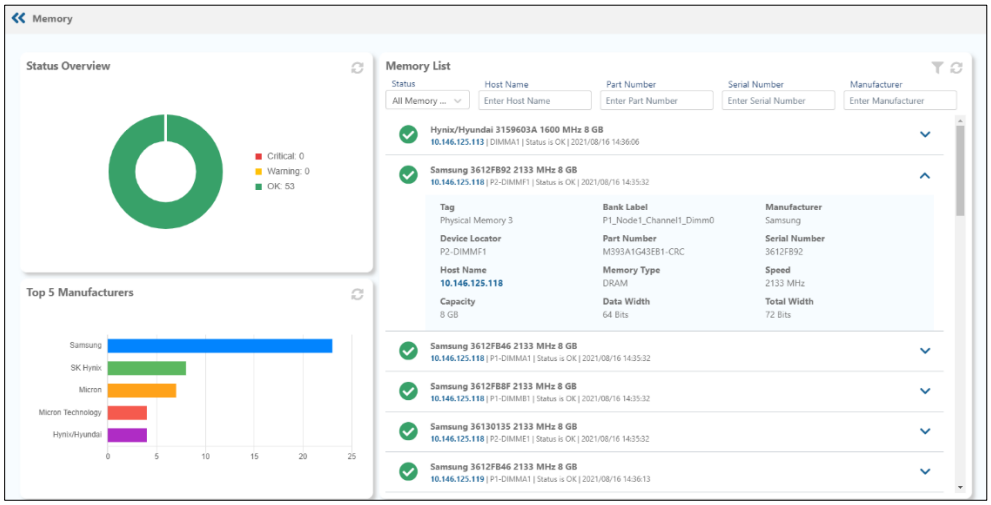


Figure 8-14

- **Status Overview** Displays the statistics of the memory status of all managed hosts, including **Critical**, **Waring**, and **OK**. Note that the status is gathered for each memory via Supermicro BMC Redfish API.
- **Top 5 Manufacturers:** Displays the statistics of the top five manufacturers of memories of all managed hosts.
- **List of memories of managed hosts:** Accesses the default list of memories of all managed hosts. You can filter by conditions, including individual status ("Critical," "Warning," and "OK") or all status, host name, part number, serial number, and manufacturer.
- **Memory Details**: Click the arrow icon on the right side of each memory record to view the details of this memory, including Tag, Device Locator, Host Name, Capacity, Bank Label, Part Number, Memory Type, Data Width, Manufacturer, Serial Number, Speed, Total Width, etc. Click **Host Name** to access the details of the individual host.

8.2.6.3 Storage Adapter

Go to the Component Health page and click the **Storage Adapter** button to display status of all SSM management hosts' storage adapters.

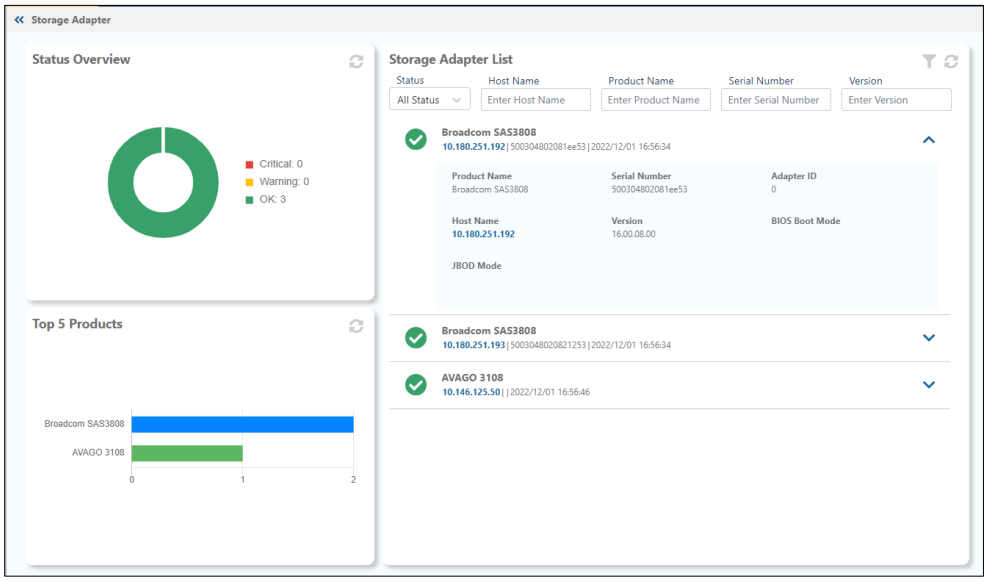


Figure 8-15

- **Status Overview:** Displays the statistics of the storage adapter status of all managed hosts, including **Critical**, **Waring**, and **OK**. Note that the status is gathered for each storage adapter via Supermicro BMC Redfish API.
- **Top 5 Products:** Displays the statistics of the top five products of storage adapters of all managed hosts.
- **List of storage adapters of managed hosts:** Accesses the default list of storage adapters of all managed hosts. You can filter by conditions, including individual status ("Critical," "Warning," and "OK") or all status, host name, product name, serial number, and version.
- **Storage Adapter Details**: Click the arrow icon on the right side of each storage adapter record to view the details of this storage adapter, including Product Name, Serial Number, Adapter ID, Host Name, Version, BIOS Boot Mode, JBOD Mode, etc. Click **Host Name** to access the details of the individual host.

8.3 Service Report

Three types of service reports are supported:

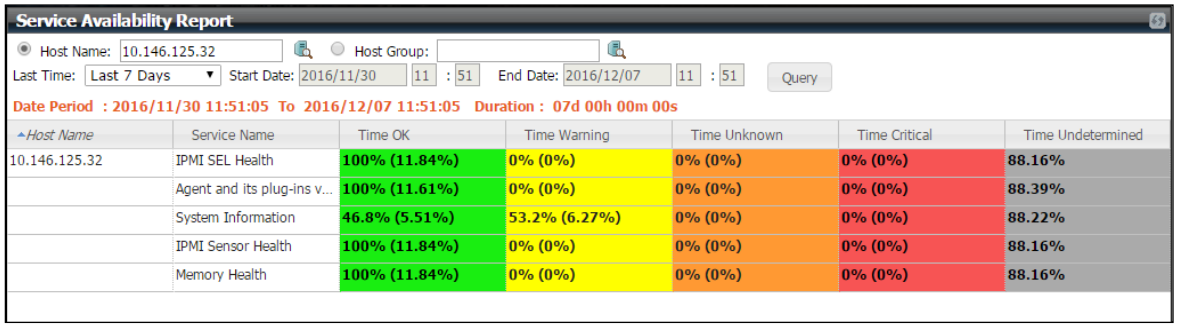
Figure 8-16

- **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.

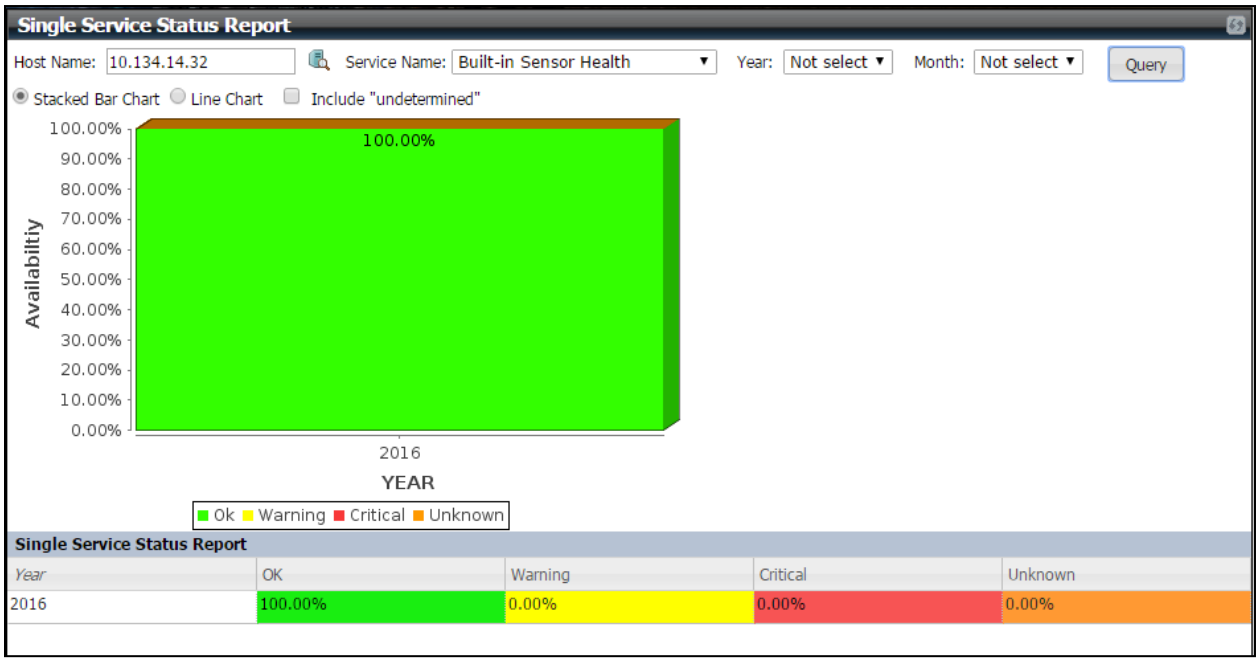


Host Name	Service Name	Time OK	Time Warning	Time Unknown	Time Critical	Time Undetermined
10.146.125.32	IPMI SEL Health	100% (11.84%)	0% (0%)	0% (0%)	0% (0%)	88.16%
	Agent and its plug-ins v...	100% (11.61%)	0% (0%)	0% (0%)	0% (0%)	88.39%
	System Information	46.8% (5.51%)	53.2% (6.27%)	0% (0%)	0% (0%)	88.22%
	IPMI Sensor Health	100% (11.84%)	0% (0%)	0% (0%)	0% (0%)	88.16%
	Memory Health	100% (11.84%)	0% (0%)	0% (0%)	0% (0%)	88.16%

Figure 8-17

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.



Single Service Status Report

Year	OK	Warning	Critical	Unknown
2016	100.00%	0.00%	0.00%	0.00%

Figure 8-18

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.

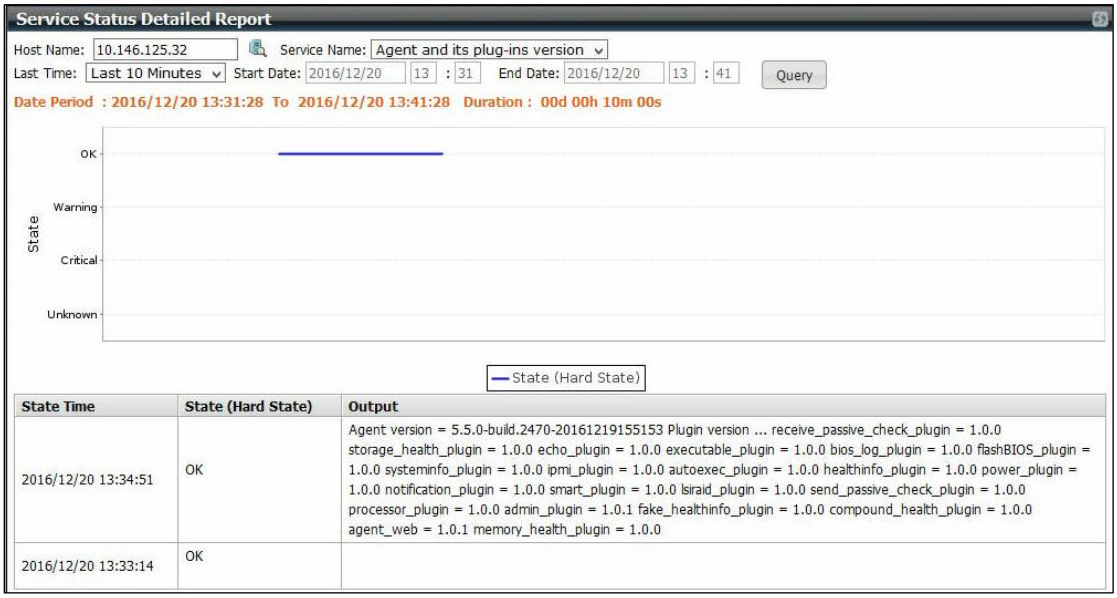


Figure 8-19

9 Power Management

9.1 Power Management in SSM

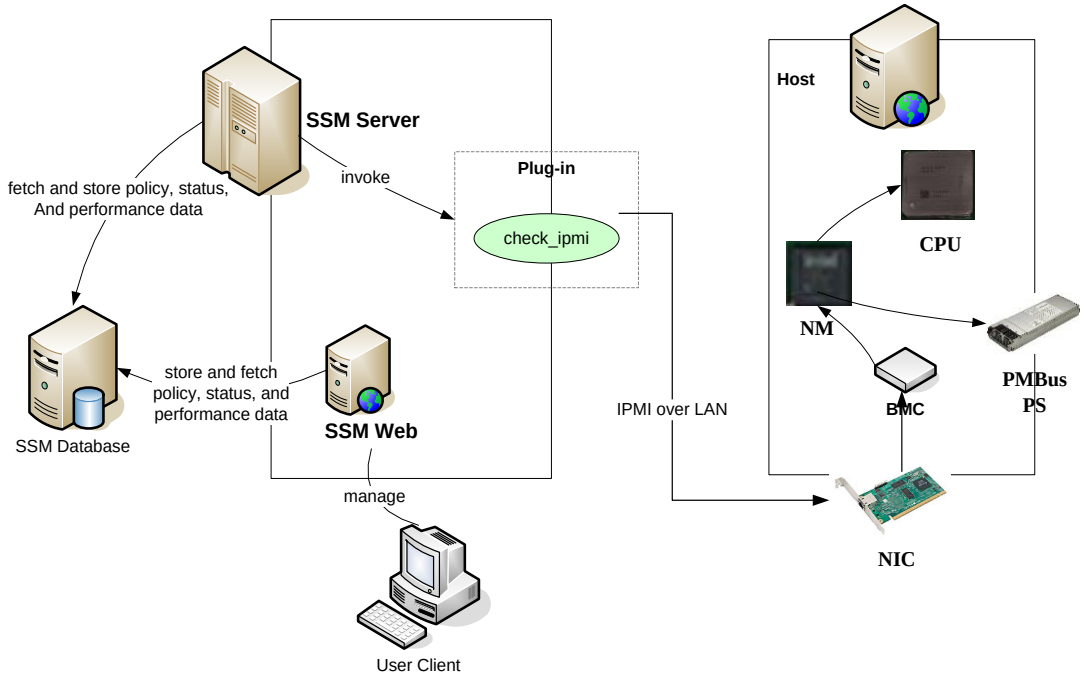


Figure 9-1

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, either using IPMI over LAN or Redfish protocol, 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 or later**. 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

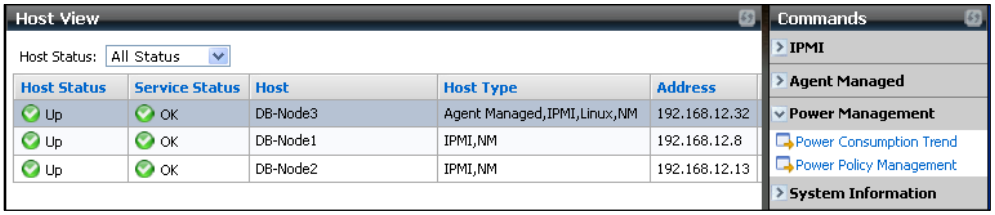


Figure 9-2

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.

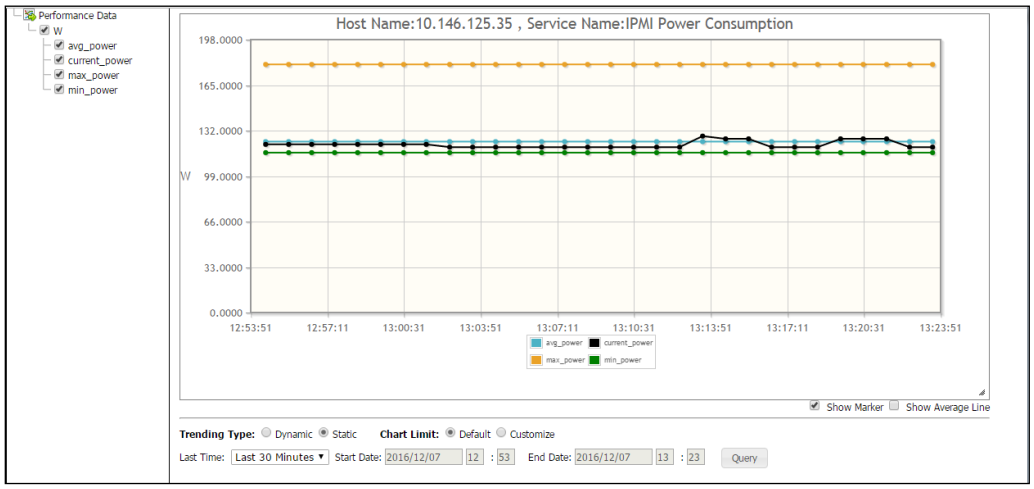


Figure 9-3

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

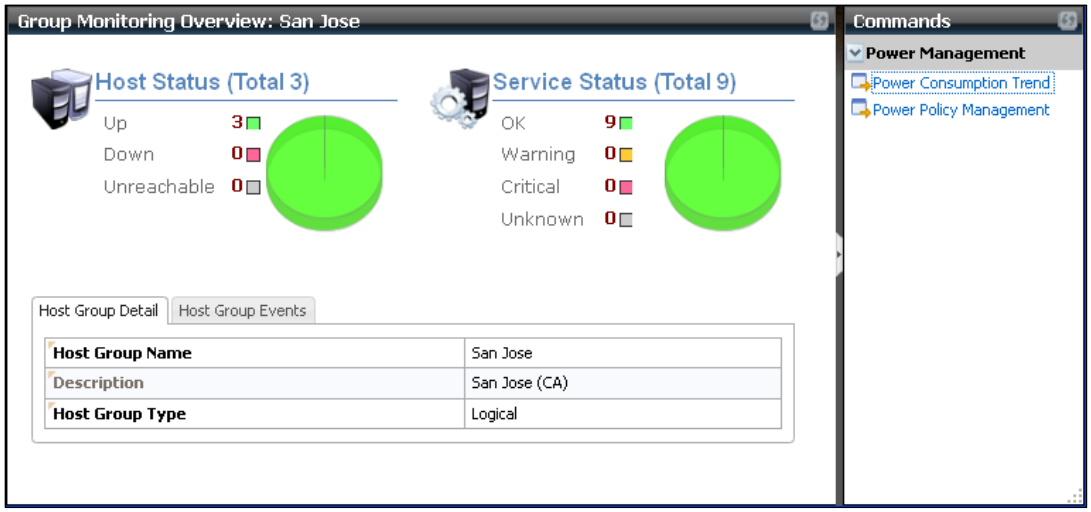


Figure 9-4

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**.**

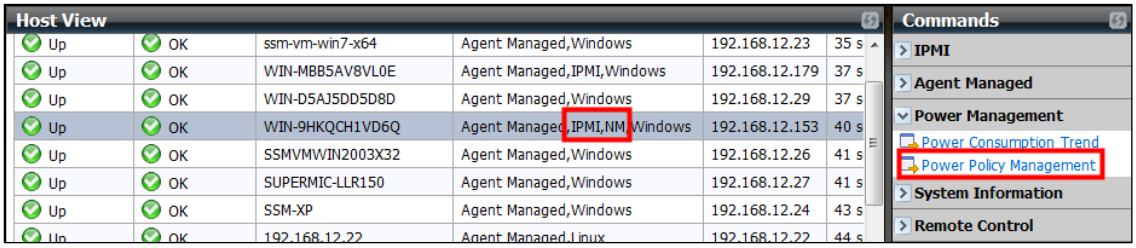


Figure 9-5

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.

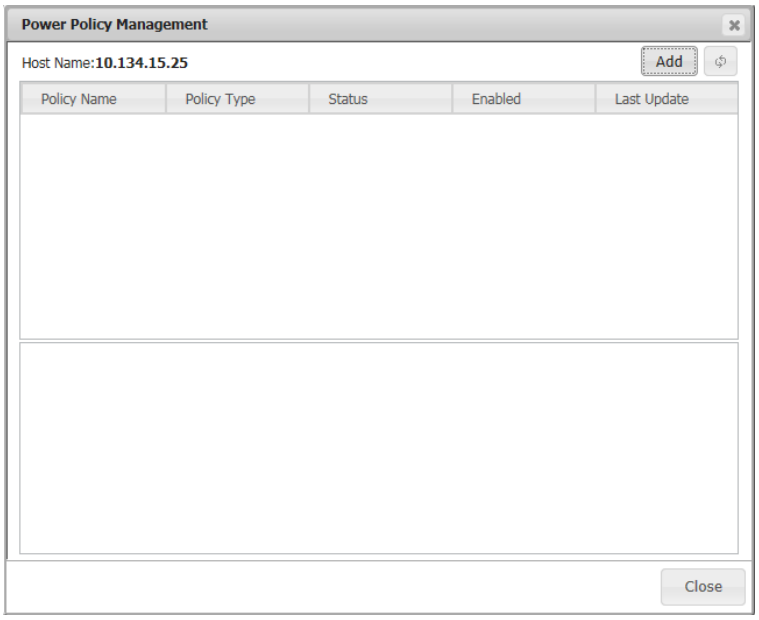


Figure 9-6

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.

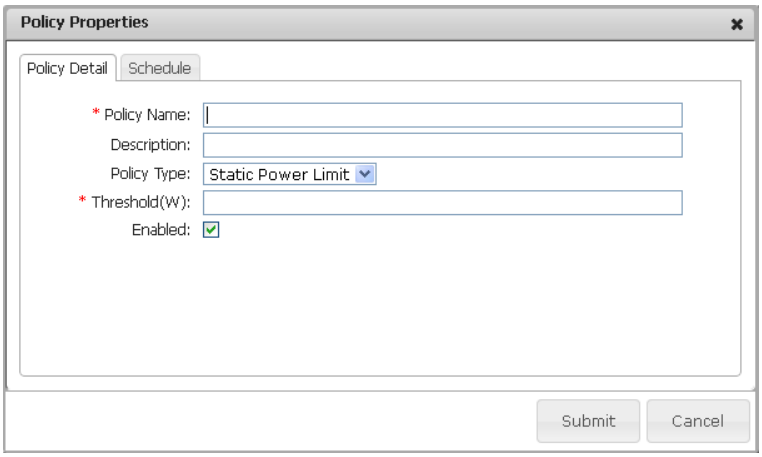


Figure 9-7

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.

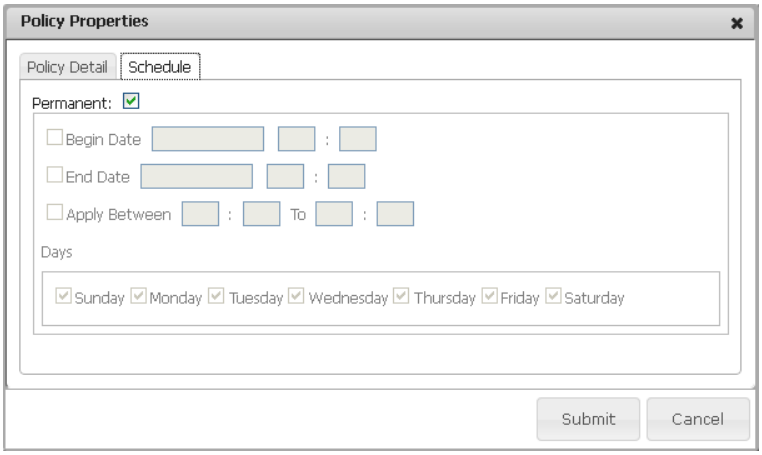


Figure 9-8

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.

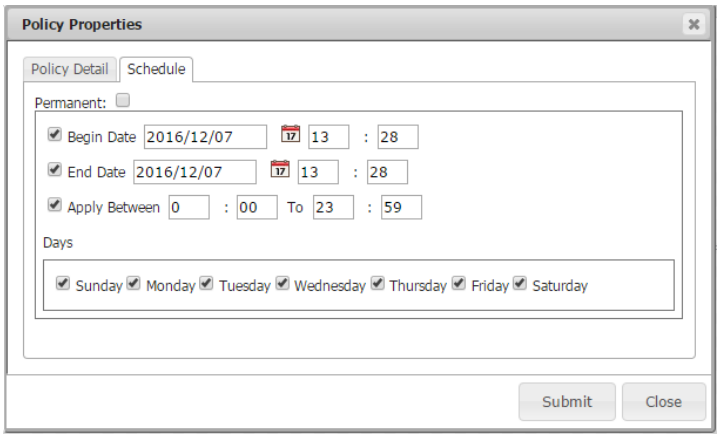


Figure 9-9

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**.

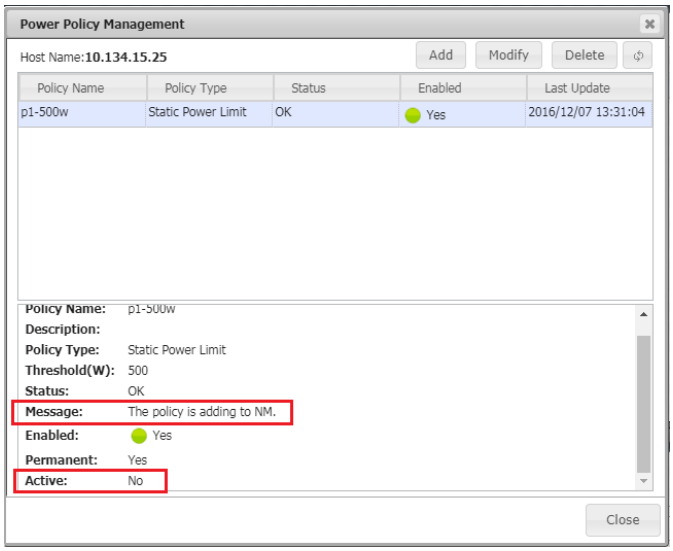


Figure 9-10

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.

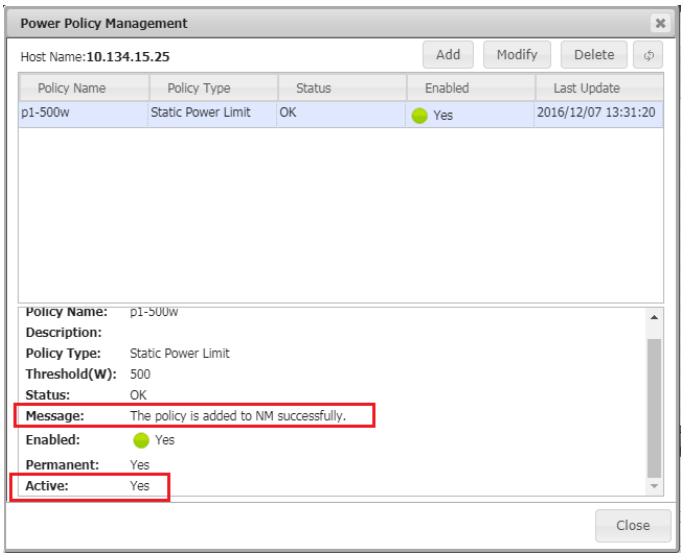


Figure 9-11

9.3.2 Host Group Policies

1. Select a host group and execute the Power Policy Management command**.**

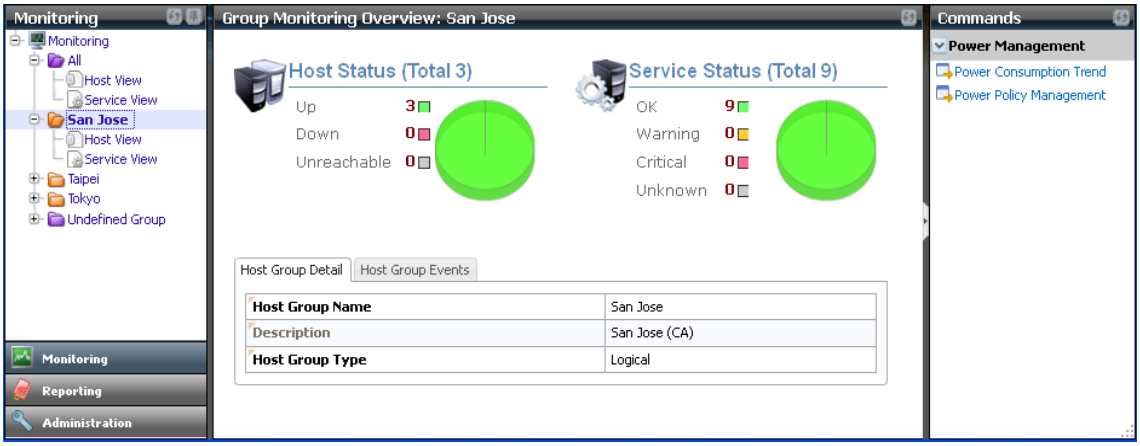


Figure 9-12

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.

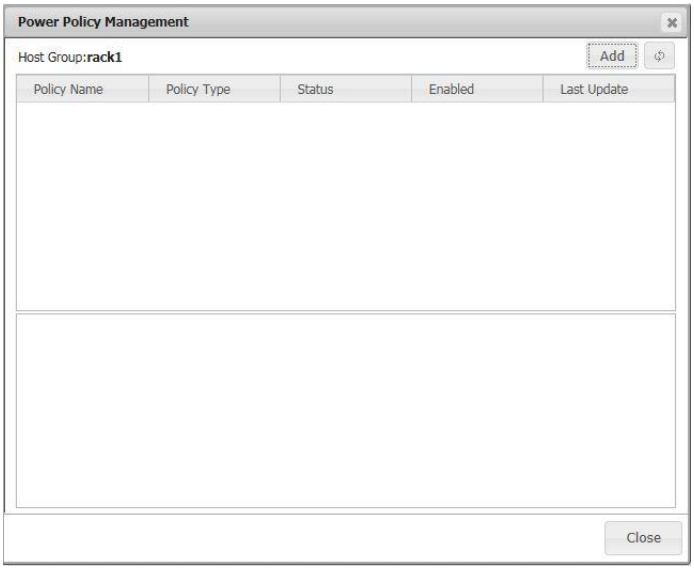


Figure 9-13

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.

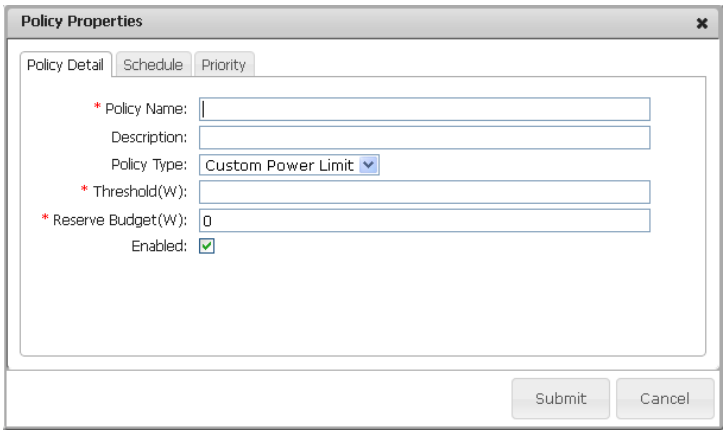


Figure 9-14

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.

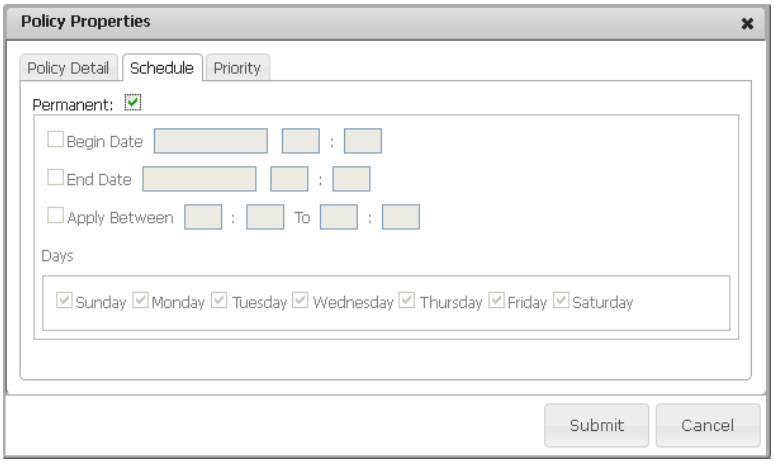


Figure 9-15

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.

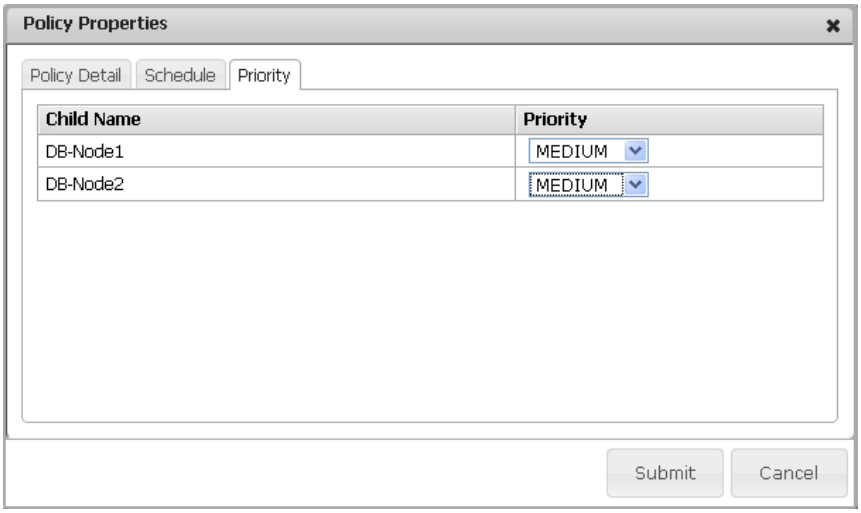


Figure 9-16

6. 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**.

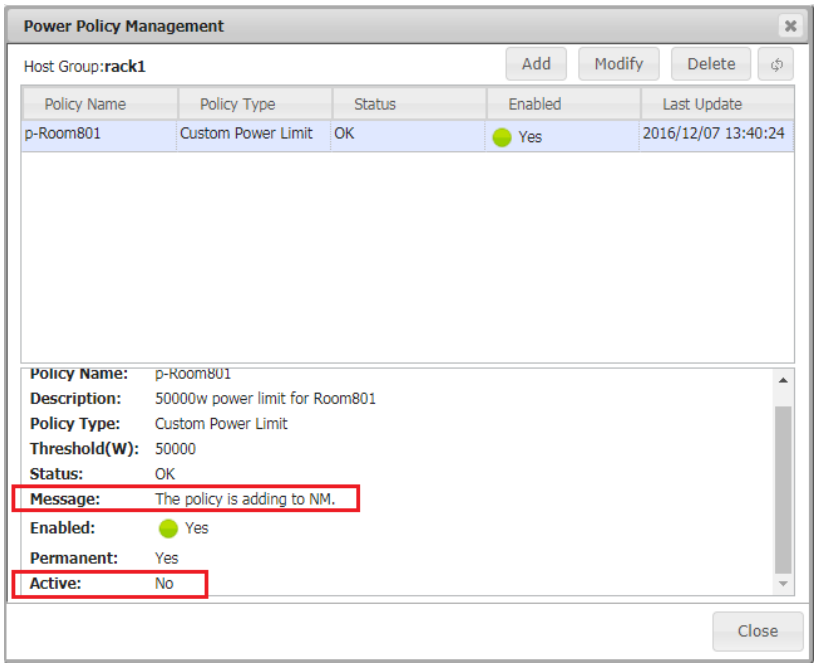


Figure 9-17

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.

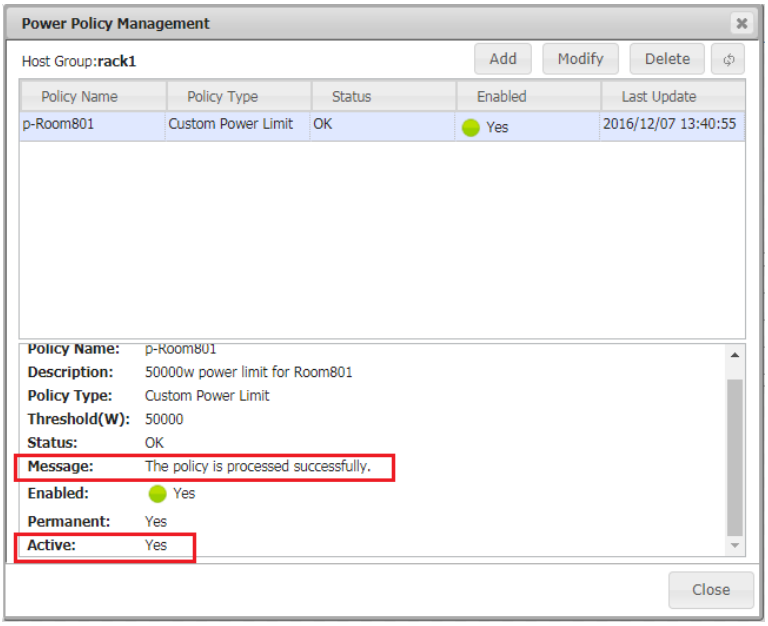


Figure 9-18

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.

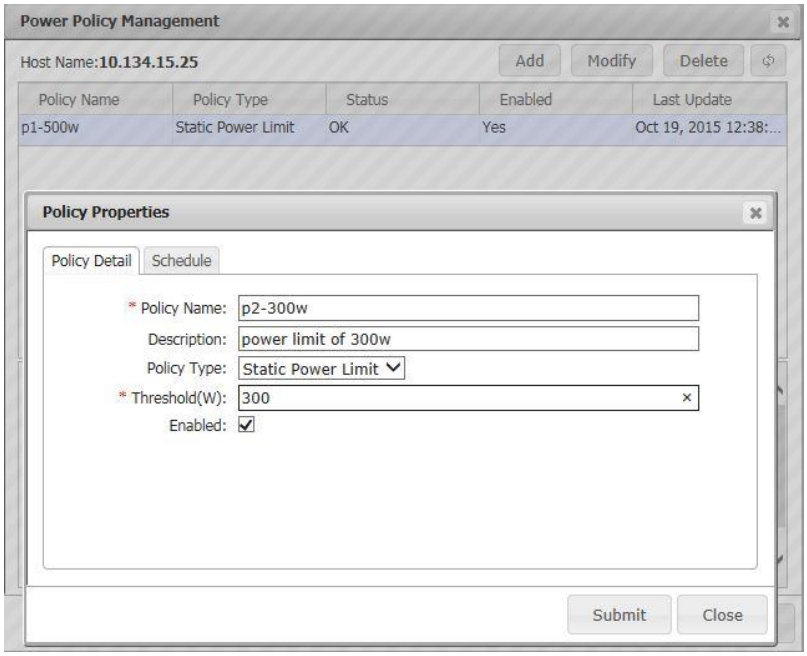


Figure 9-19

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.

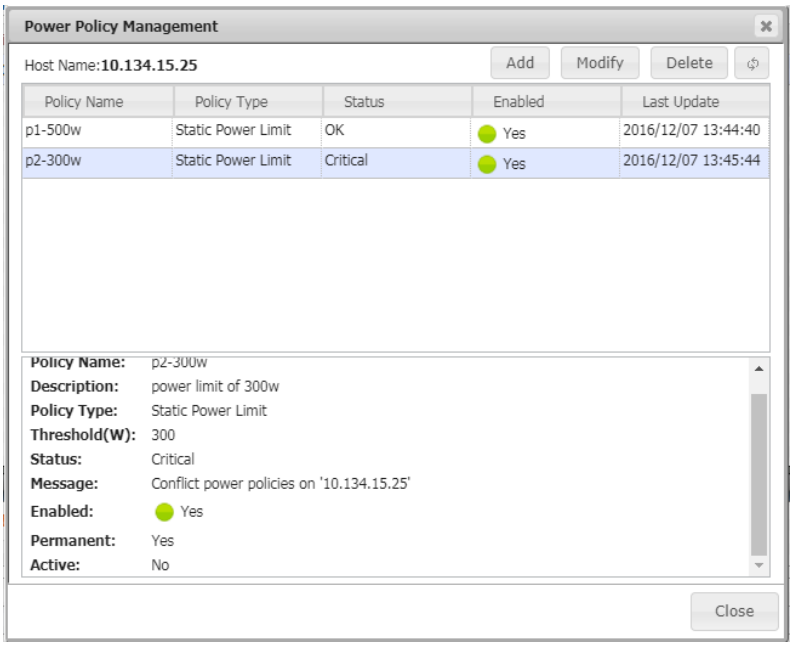


Figure 9-20

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.

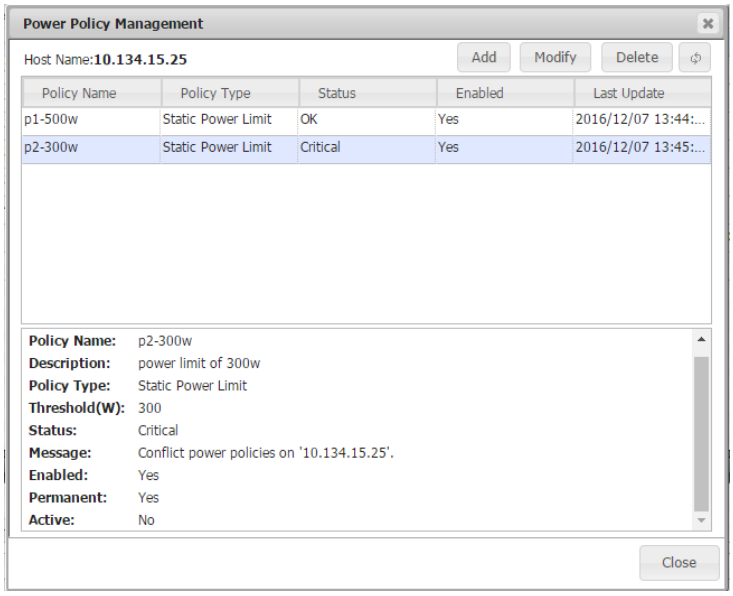


Figure 9-21

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.

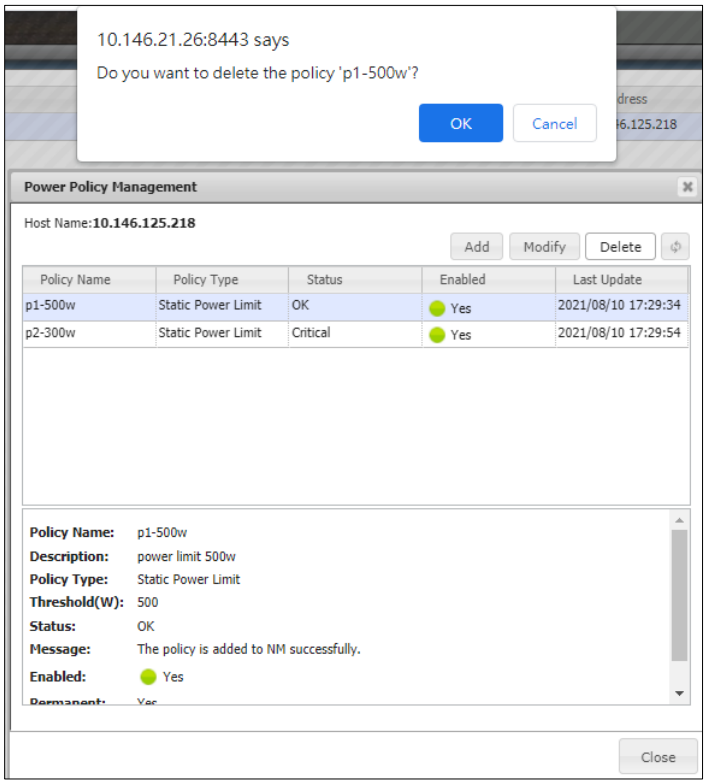


Figure 9-22

You can see that the p1-500W policy was deleted. At this time, the p2-300W policy is not in the Active state yet.

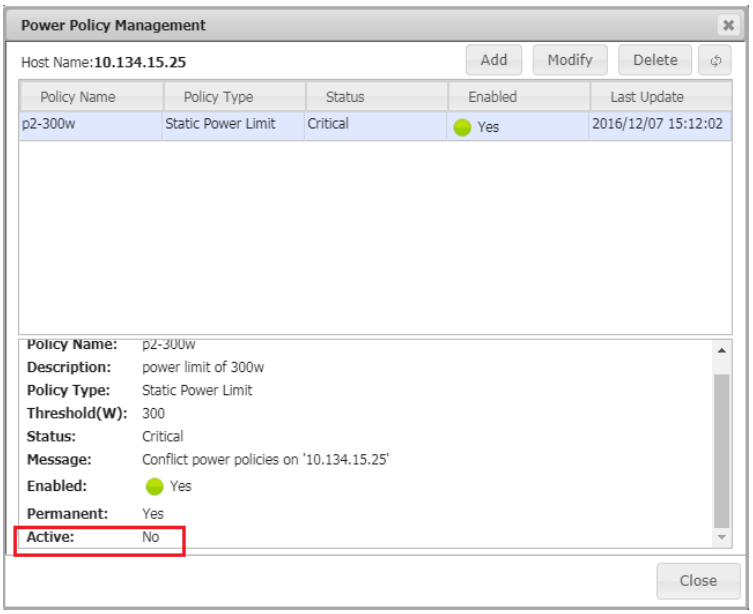


Figure 9-23

Few seconds later, the p2-300W policy is automatically activated by the SSM Server.

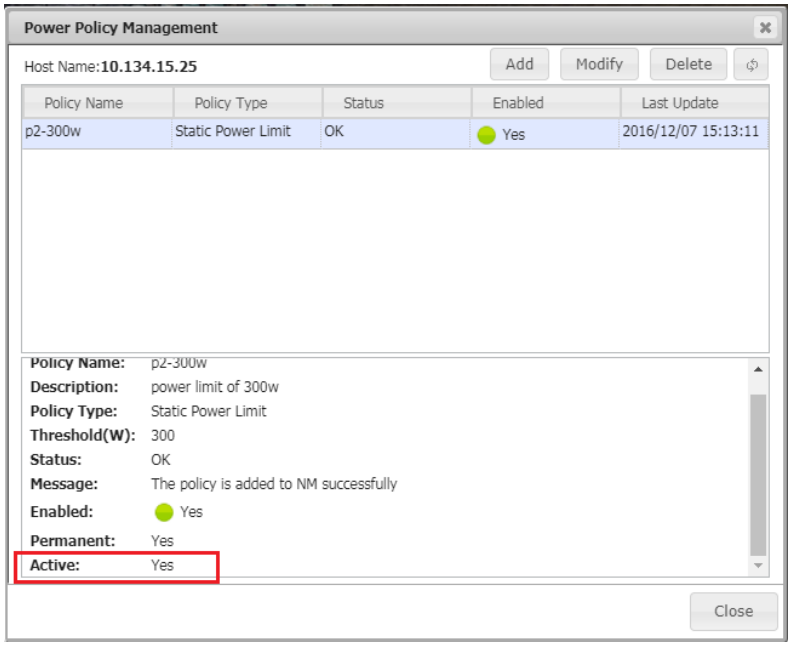


Figure 9-24

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.

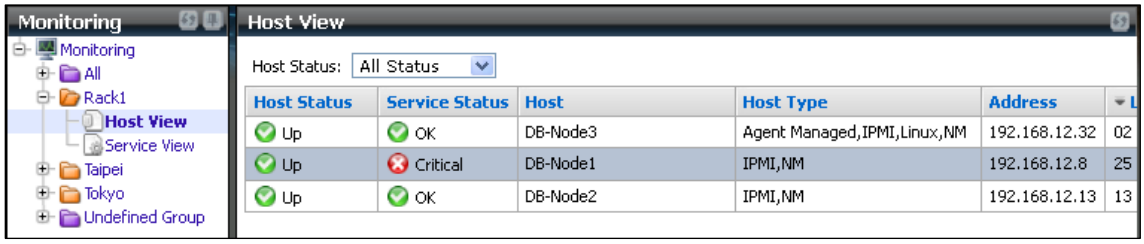


Figure 9-25

DB-Node1 has an active permanent policy named host-p-800w with a threshold of 800W.

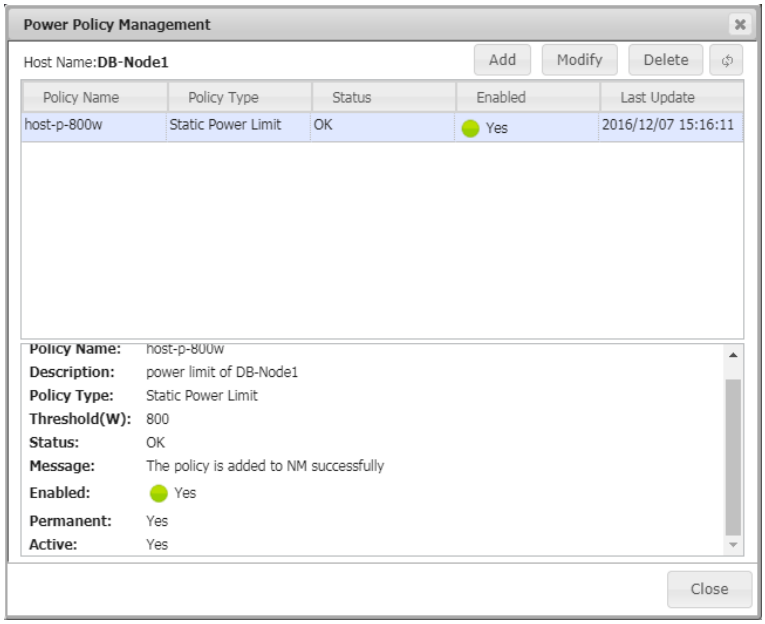


Figure 9-26

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.

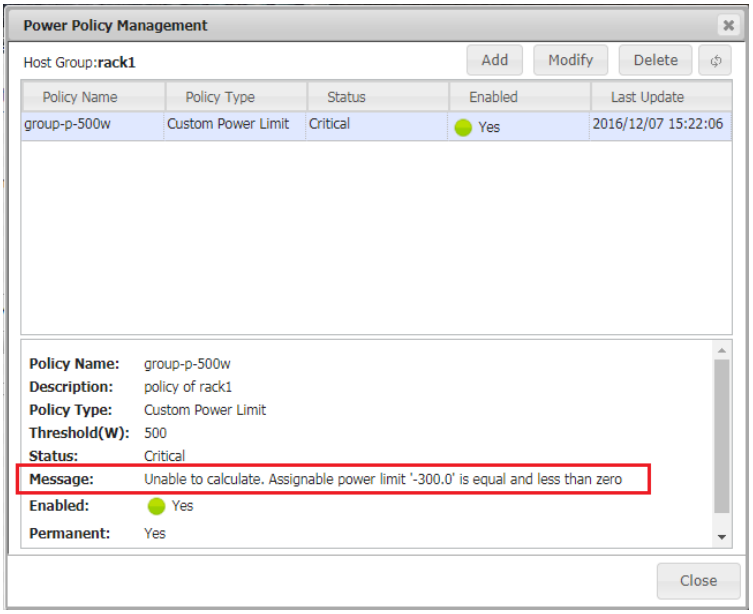


Figure 9-27

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.

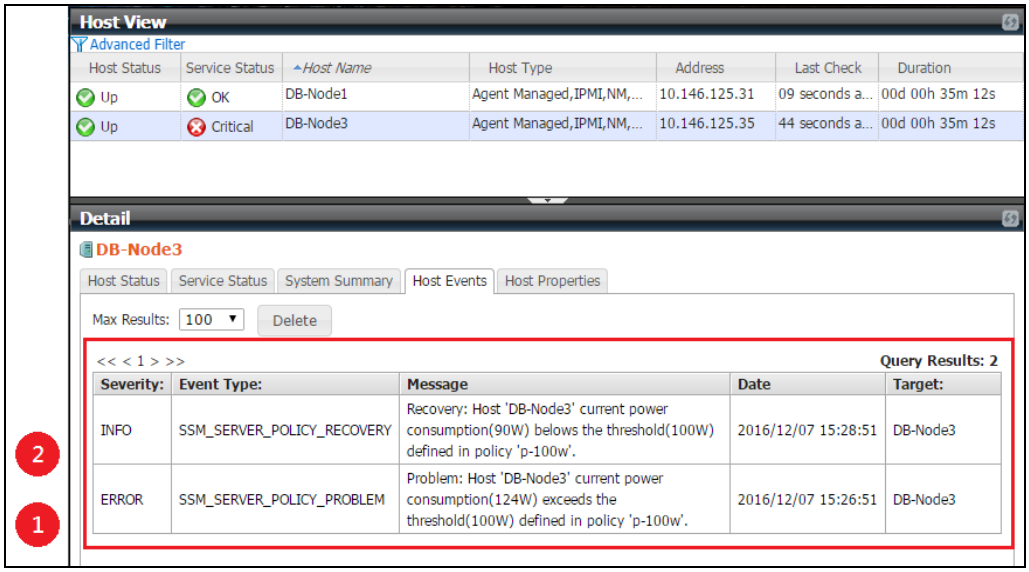


Figure 9-28

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.

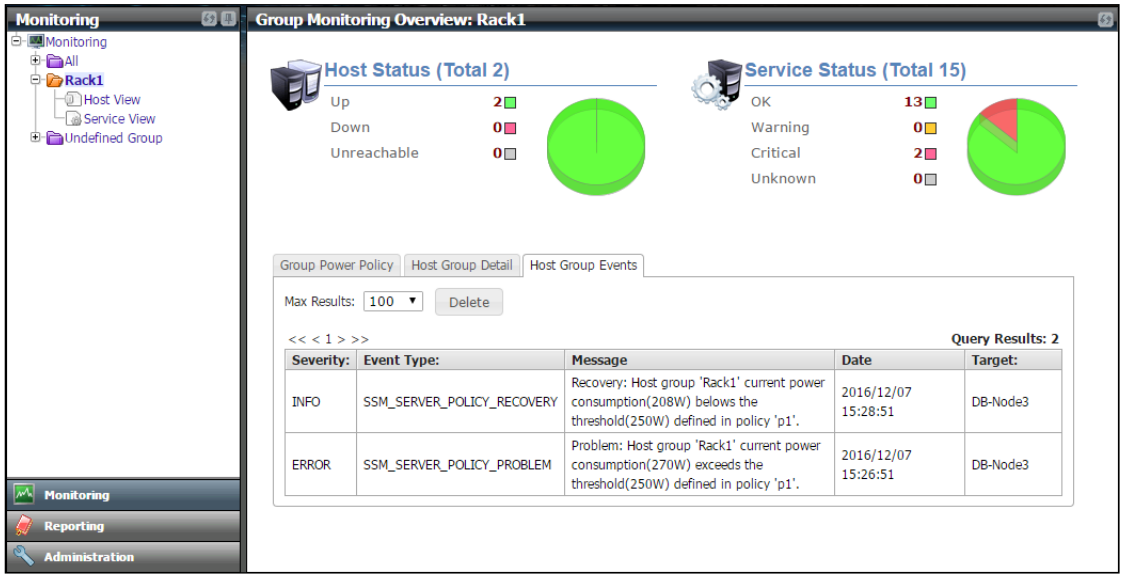


Figure 9-29

You can clear the host group events by clicking the **Delete** button and the events will be deleted from the SSM Database.

10 Firmware Notification

BIOS, Microcode Update (MCU) Capsule and BMC firmware information on SSM is synchronized with Supermicro's Firmware Repository Portal (https://fwapi.supermicro.com/api/v1/firmwares/search) to ensure that administrators get notified of the latest updates by email. To simplify the following firmware update procedure, SSM also allows firmware to be auto-updated by schedule based on the synchronization result or manually.

10.1 Prerequisites

To use the function with the BIOS and BMC firmware type, the managed hosts must meet the following requirements:

- Support for obtaining UFFN (Unique Firmware File Name) information.
- Supermicro's X12/H12 platforms and later or new released FW for mainstream platforms.

To use the function with the MCU Capsule firmware type, the managed hosts must meet the following requirements:

- Supermicro's X13 platforms and later Intel generations.
- The managed system must support the RoT system.

If you have any questions, please contact Supermicro.

10.2 FW Notification Settings

10.2.1 Setting up FW Notification

1. To set up firmware notification, click **SSM New GUI** on the top tool bar→ **Provision** → **FW Notification**, and the FW Notification View page is shown. Select **Settings** tab.

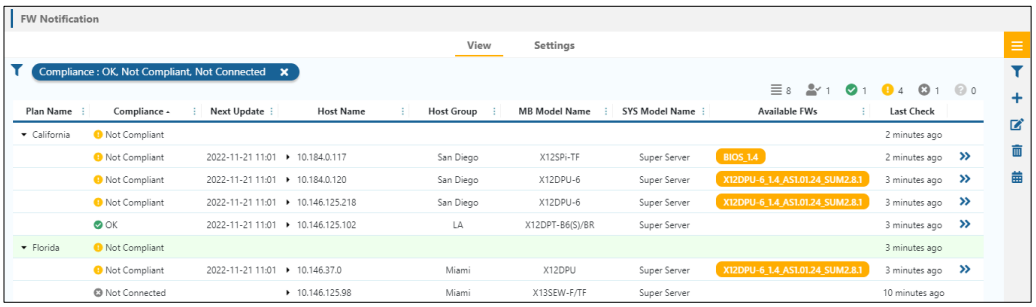


Figure 10-1

2. A dialog box appears.

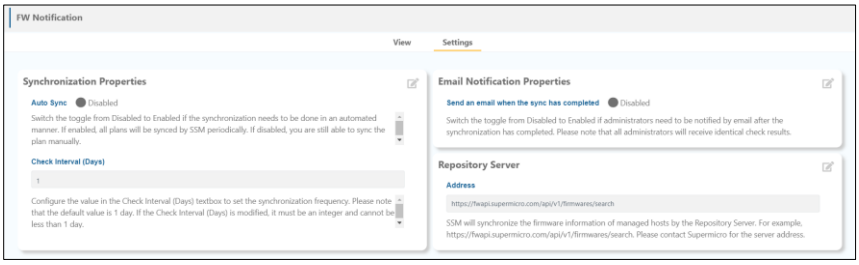


Figure 10-2

3. To enable the automatic synchronization on the selected hosts, click the **Edit** icon on the top right corner, toggle from Disabled to **Enabled** in the Auto Sync field, and click the **Save** icon. You can also set synchronization frequency by changing the value in the Check Interval (Days) field. Note that the value cannot be less than one.
4. SSM can synchronize with **Repository Server** automatically or manually, and the default address is Supermicro's Firmware Repository Portal. To change the URL, click the **Edit** icon in the top right corner to enter the new address, and then click the **Save** icon.
5. To get notified by email, click the **Edit** icon on the top right corner, toggle from Disabled to **Enabled** in the **Send an email when the sync has completed** field, and then click the **Save** icon.

10.2.2 Setting Up Email

Note: Besides built-in ADMIN account, if you need another administrator to get notified via email, refer to this section for details. Otherwise, you may skip this section.

1. In the left navigation area of Administration, expand **Administration → Management Server Setup**, and select **Email SMTP Setup**. Type in required information and click **Submit**.

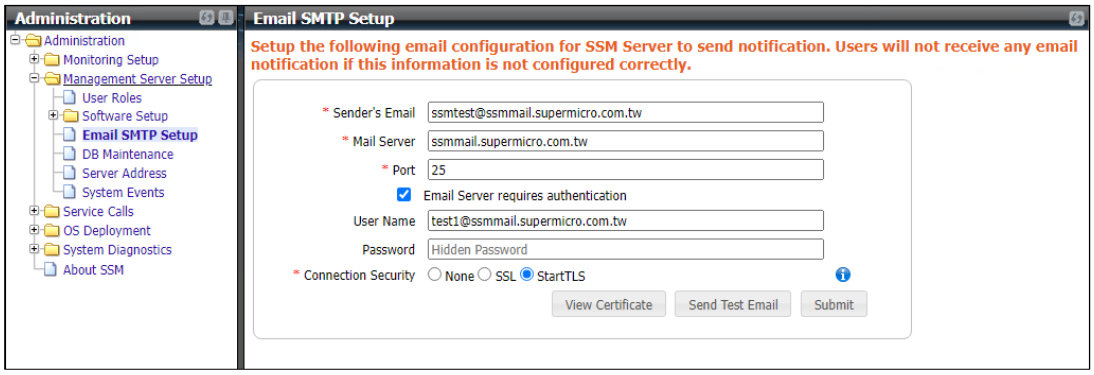


Figure 10-3

2. Select **User Roles** under Management Server Setup, and click **Add User** in the Commands area.

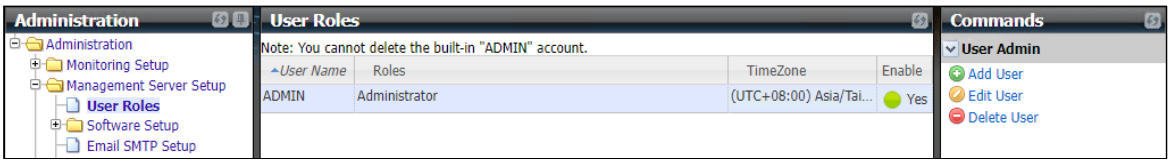


Figure 10-4

3. Note that only SSM administrators get notified by email. Type in necessary information and select **Administrator** to be the new user's role.

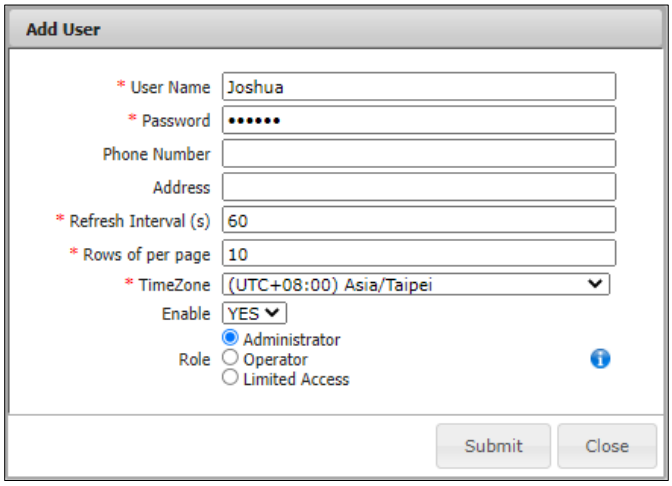


Figure 10-5

The new user appears in the list.

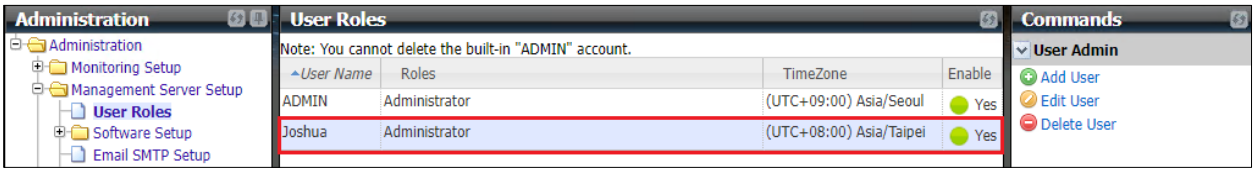


Figure 10-6

4. Expand **Administration → Monitoring Setup → Contact**, and click **Add Contact** in the Commands area.

Figure 10-7

5. Add the user in the users list as new contact, type in necessary information and click the **Submit** button.

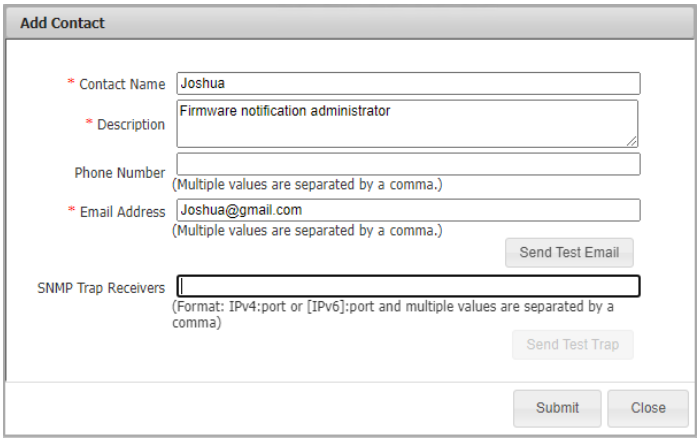


Figure 10-8

The new contact appears in the list.

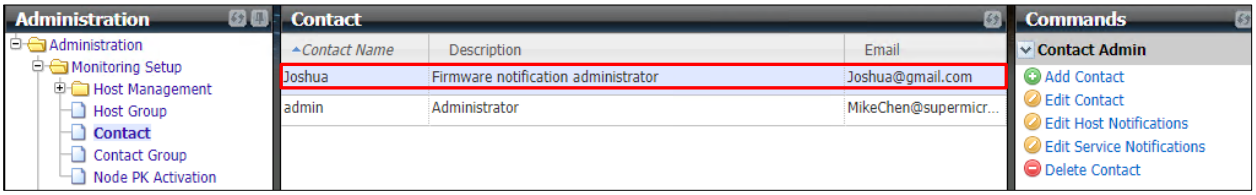


Figure 10-9

10.3 FW Notification View

After establishing a connection with Supermicro's Firmware Repository Portal website through the **Repository Server** setting, the synchronized firmware information of managed hosts can be viewed on the FW Notification View. Synchronization can be done manually as well.

10.3.1 Overview

The firmware synchronization result is displayed on the **View** page.

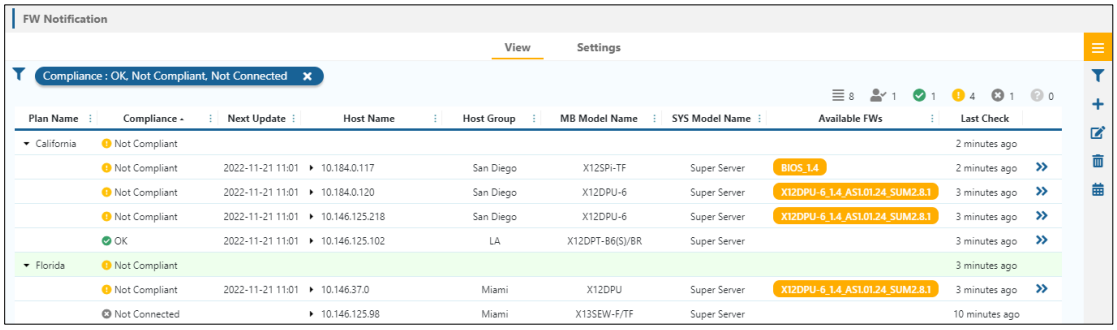


Figure 10-10

- **Filter:** Click the Filter icon on the right side, fill in the necessary information and click the Submit button. Note that Compliance has been added to the criteria by default so that users do not see the hosts with their Compliance showing “Not Supported”.

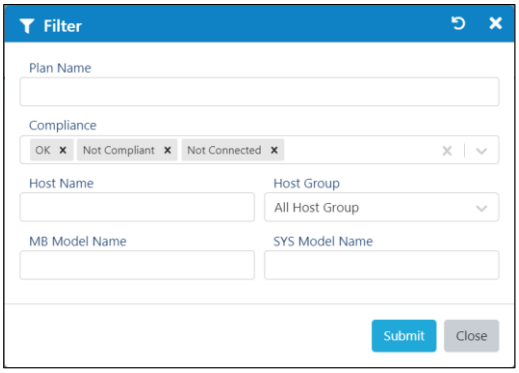


Figure 10-11

- **Compliance**: This column shows the status of Bundle, BIOS, MCU Capsule, or BMC.
  - **OK**: The BMC, MCU Capsule, and BIOS are up to date.
  - **Not Compliant**: Any one of BMC, BIOS, or MCU Capsule is not up to date.
  - **Not Connected**: Unable to connect to firmware repository portal for status check.
  - **Not Supported**: No firmware information available for this host.

If the record belongs to a specific host, the column value is the **Compliance** of each host. If the record belongs to a specific plan, the column value is the **Compliance** that summarizes firmware compliance of all hosts in the plan:

- If the plan has hosts with **Compliance** like **Not Compliant**, **Not Connected, OK,** and **Not Supported**, the **Compliance** is **Not Compliant**.
- If the plan has hosts with **Compliance** like **Not Connected**, **OK** and **Not Supported**, the **Compliance** is **Not Connected**.
- If the plan has hosts with **Compliance** like **OK**, and **Not Supported**, the **Compliance** is **OK**.
- If the plan has all hosts with the same **Compliance** and is **Not Supported**, the **Compliance** is **Not Supported**.
- If the plan has no hosts at all, the **Compliance** is **OK**.

- **Next Update**: This column shows the scheduled time to update the firmware.
  - If the host has been assigned a scheduled setting, the column value is the next scheduled time.
  - If the host's firmware is being updated, the column shows **Updating**.
  - If the host has not been assigned a scheduled setting, the column will not display any value.

Plan Name	Compliance	Next Update	Host Name	Host Group	MB Model Name	SYS Model Name	Available FWs	Last Check	
California	Not Compliant							a day ago	
	Not Compliant	Updating	10.184.0.120	Miami	X12DPU-6	Super Server	X12DPU-6_1.4_AS1.01.24_SUM2.8.	a day ago	
	Not Compliant		10.184.0.117		X12SPi-TF	Super Server	BMC_01.01.31	a day ago	
Florida	Not Compliant							a day ago	
	Not Compliant	Updating	10.184.0.120	Miami	X12DPU-6	Super Server	X12DPU-6_1.4_AS1.01.24_SUM2.8.	a day ago	
	OK	2022-11-16 17:35	10.184.25.19	Miami	X12SPi-TF	Super Server		N/A	

Figure 10-12

- **Data Statistics Bar**: displays the statistics:
  - : shows the total number of records.
  - : shows the number of the selected records.
  - : shows the number of host records of "**OK**" in Compliance column.
  - : shows the number of host records of "**Not Compliant**" in Compliance column.
  - : shows the number of host records of "**Not Connected**" in Compliance column.
  - : shows the number of host records of "**Not Supported**" in Compliance column.
- **Available FWs:** This column shows the latest and upgradable firmware (orange bar) as well as other intermediate versions (gray bars). Because the Bundle package has both highly compatible BIOS and BMC versions, its installation is prioritized over the respective BIOS and BMC versions. After clicking the orange bar or gray bar in this column, a dialog box appears and shows you all firmware release information. Note that the **Download** button only appears when you click the orange bar.

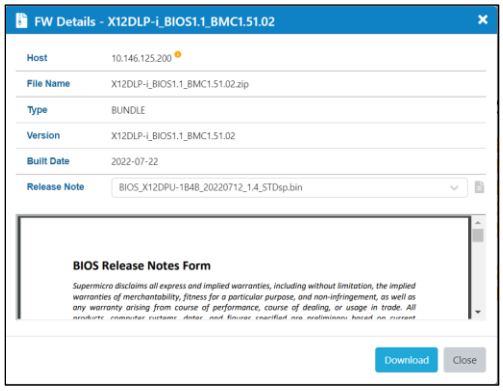


Figure 10-13

- **Last Check**: This column is used to determine the synchronization time between SSM and FW repository. If the record belongs to a specific host, the column value describes the property of this respective host. If the record belongs to a specific plan, the latest value of **Last Check** in the hosts will be used.
- Click the right double arrow » icon to show the details of the host, including **System Summary**, **BMC,** and **BIOS** information, and all **Available FWs**. If the **MCU Capsule** is supported, the **MCU Capsule Version** is displayed in the **BIOS** panel. You could also download the release notes and firmware in **Available FWs**. Note that only the first one can be downloaded.

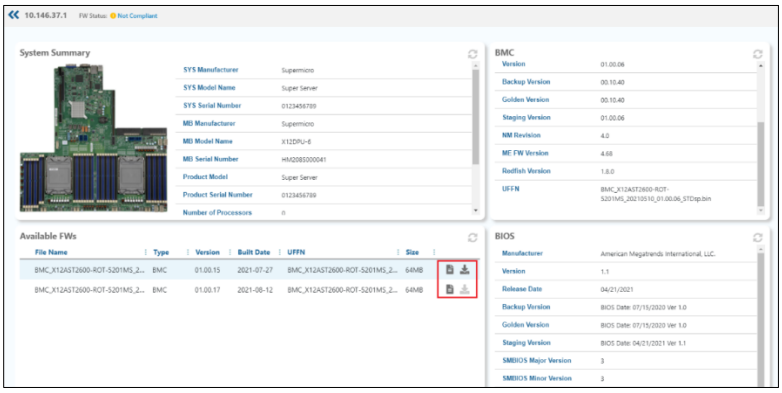


Figure 10-14

10.3.2 Creating a Plan

To view the firmware information from synchronization result, you must create firmware compliance plans first to include managed hosts. Using different plans can also help you classify managed hosts for different purposes.

1. Go to **View** page and click the **Add a Plan** icon.

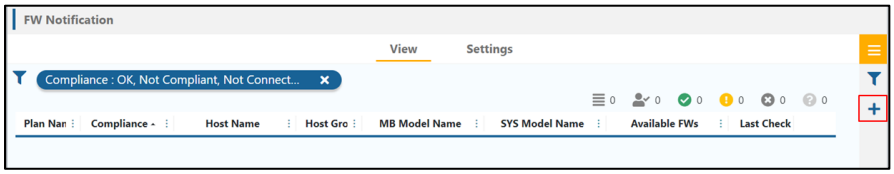


Figure 10-15

2. Fill in all necessary information, select the desired host groups or hosts. If you want to set the scheduled time to automatically update the firmware, toggle from Disabled to **Enabled** and determine the execution frequency in the **Scheduled Update Time** area, and then click the **Submit** button.

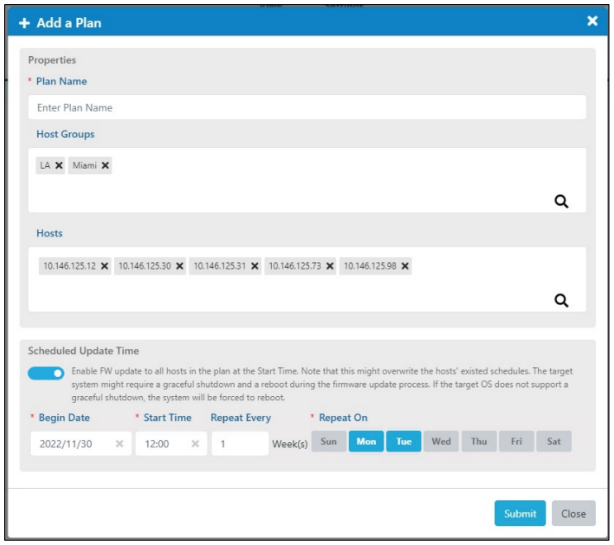


Figure 10-16

10.3.3 Editing a Plan

You can edit a plan after it is created. You can click the **Edit** icon or click the icon and click **Edit a Plan**.

To edit a plan, select a desired plan to be edited. Fill in the necessary information and click the **Submit** button.

Note that the configuration of **Scheduled Update Time** will be applied with previous scheduled setting automatically.

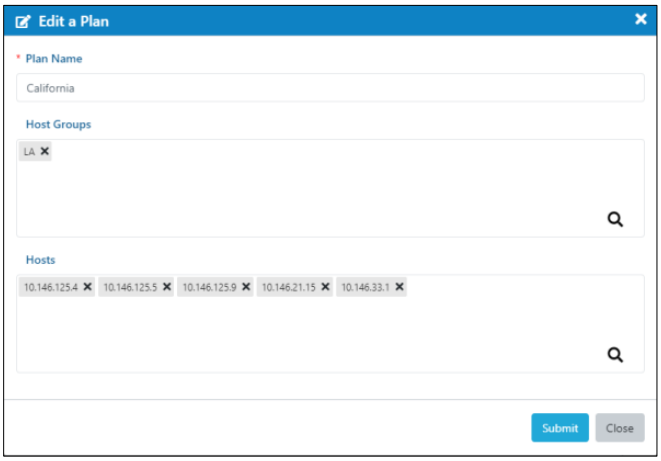


Figure 10-17

10.3.4 Deleting a Plan

You can delete a plan if it is no longer needed.

You can click the **Delete** icon or click the icon and click **Delete a Plan**.

To delete a plan, select a desired plan and then click the **Run** button.

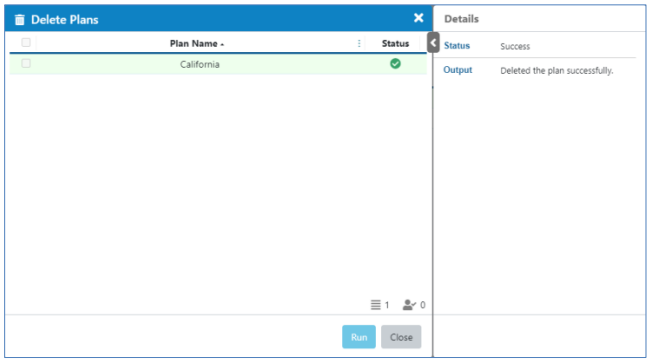


Figure 10-18

10.3.5 Checking for BMC, BIOS, and MCU Capsule

A firmware compliance plan can include many managed hosts, but acquiring firmware information requires data synchronization with Supermicro's Firmware Repository Portal. In addition to enabling the automatic synchronization mechanism in **Settings** page, you can also use **Check for BMC, Check for BIOS,** and **Check for MCU Capsule** in the **View** page to synchronize manually.

1. Click the plan and expand the **Plan Operations** on the right-hand side of the panel, then click **Check for BMC** (or **Check for BIOS** and **Check for MCU Capsule**).

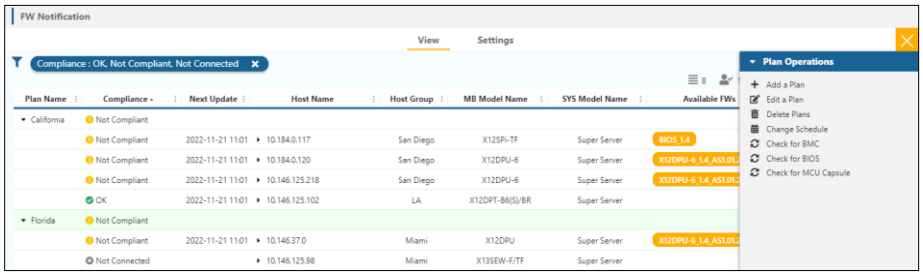


Figure 10-19

2. Click **Run** and then click the **Task ID** link to go the **Detailed Task View**. SSM uses an asynchronous task to represent the request for the long task completion.

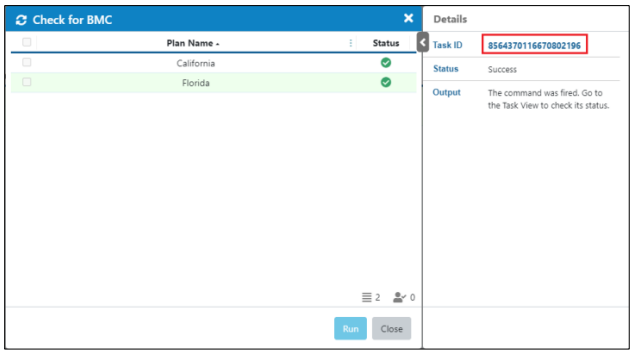


Figure 10-20

3. The firmware synchronization result will be displayed on the **View** page.

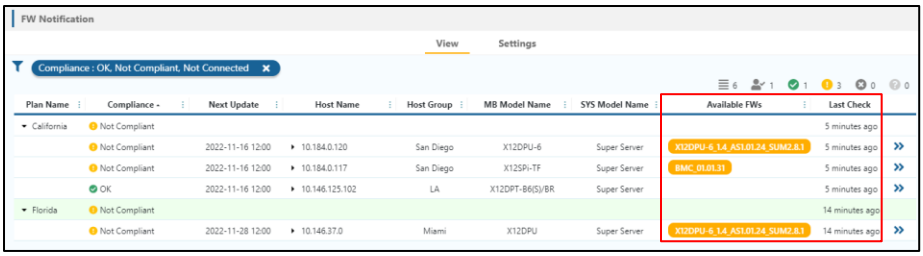


Figure 10-21

10.3.6 FW Notifications: Emails

Whether the firmware synchronization is automatic or manual, any administrators receive notifications by email. Each email summarizes the firmware information of all hosts in all selected plans at a specific time, and lists hosts by different compliance, such as “OK” and “Not Compliant.” You can go to the system for further details.

```
SSM - Check FW Compliance Result


Event Source: WIN-5T5S6R83QEC/10.146.125.225
Version: 5.1.0_build.1209-20210811165913

Executed Plan(s): Florida

Date/Time: 2021/08/13 12:33:26 UTC+08:00

[Summary]
Number of Not Compliant Hosts: 2
Number of Not Connected Hosts: 0
Number of Not Supported Hosts: 2
Number of OK Hosts: 1

[Not Compliant Host(s)]
10.146.37.1
    Available FWs: BMC_01.00.15, BMC_01.00.17
10.146.125.218
    Available FWs: X12DPU-6_BIOS1.1b_BMC00.12.98
[Not Supported Host(s)]
10.146.125.108
10.146.125.200
```

Figure 10-22

10.3.7 FW Notifications: Reminders

If the synchronization is manually done, an administrator receives a reminder. The reminder includes hyperlinks to FW Notification View and Task View. Multiple plans can be selected to be checked at the same time.

1. Go to **View** page. For each plan selected to be synchronized, a reminder is set to be sent after synchronization. Select the desired plans and click **Check for BMC**, **Check for BIOS,** or **Check for MCU Capsule** in the **Plan Operations** panel on the right side of the page. After several minutes, the reminder appears at the top of the page.

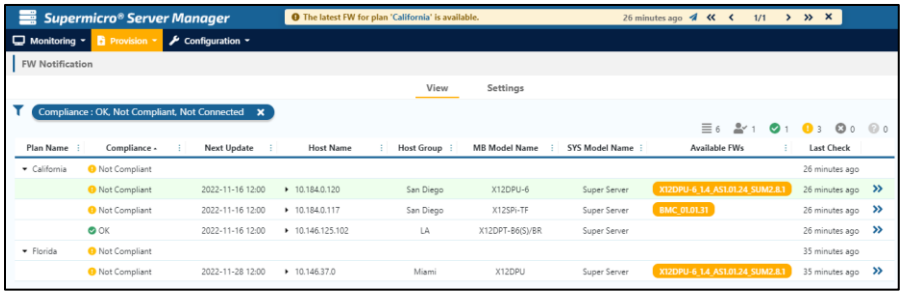


Figure 10-23

2. Use the right or left arrow buttons to view the reminders one by one if multiple plans are selected to be synchronized.
3. To view the details, click the plan name 'California' in the reminder to go to the **View** page. The filter search is automatically limited to the selected plan.
4. Clicking the arrow icon in the reminder bar to view the result.

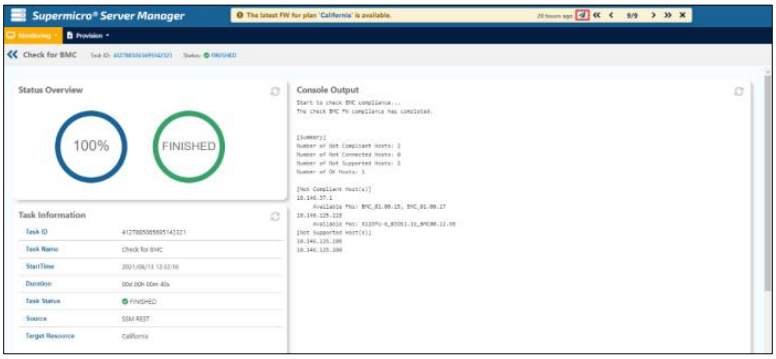


Figure 10-24

Note: The background color of the reminder bar shows different situations:

- **Yellow:** Any one of BIOS, BMC, or MCU Capsule check results in the plan is "Not Compliant," and the firmware of the hosts in the plan can be updated.
- **Red:** Any one of Check for BMC, Check for BIOS, or Check for MCU Capsule has failed.

- **Green:** Check results for BIOS, BMC, or MCU Capsule are available.

10.3.8 FW Auto Update: Change Schedule

You can change the firmware auto-update schedule of a firmware compliance plan. All hosts under the plan will be affected by this schedule setting even if the host itself has a schedule on it.

1. Click the plan and expand the **Plan Operations** on the right-hand side of the panel, and then click **Change Schedule**.

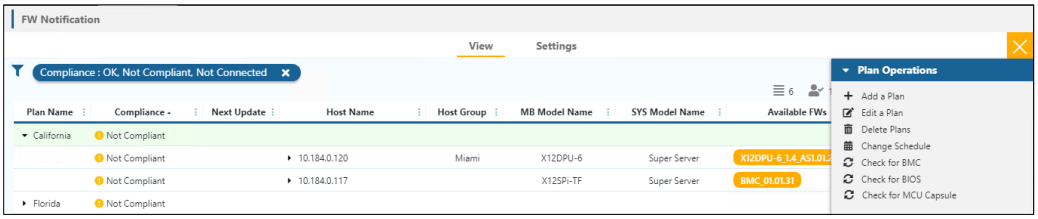


Figure 10-25

2. You can turn on the toggle and set the begin date, start time, repeat interval and day of the week and then click the **Next** button.

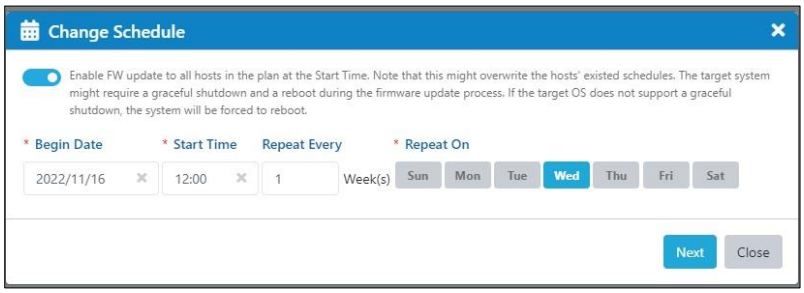


Figure 10-26

3. In the **Change Schedule** dialog box, click **Run** and retrieve success messages.

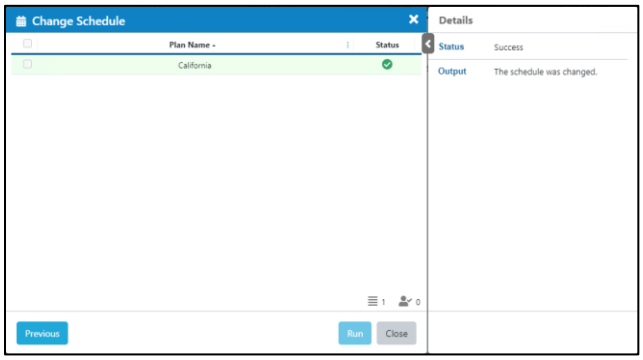


Figure 10-27

To add or change the schedules of the specific hosts, please select the hosts instead of the plans.

10.3.9 FW Auto Update: by Schedule

The **Firmware Auto Update** function makes it easy to automatically update the Bundle, BIOS, BMC, or MCU Capsule based on the firmware synchronization results. SSM will download the firmware package from the Supermicro's Firmware Repository Portal directly, verify the checksum for the package, and then update the firmware on the managed hosts. If the managed host has multiple available firmware, SSM will update the firmware from the upgradable firmware to the latest one automatically.

In the previous chapters, we show how the schedule setting to be set by the **Add a Plan** and the **Change Schedule** commands. SSM uses an asynchronous task named **Update firmware By Compliance Result** to represent the request for the long running FW update task. When the scheduled time is up, it will automatically create a task for the **Not Compliant** hosts. As for hosts of **Not Connected** and **Not Supported** compliance types, there won't be any tasks even though there are scheduled times on them.

1. To view the detailed update progress, go to **Task View** page.
2. Click the **Filter** icon on the right side, fill in the Task Name as **Update firmware By Compliance Result** and the Target Resource as the desired host name**.**

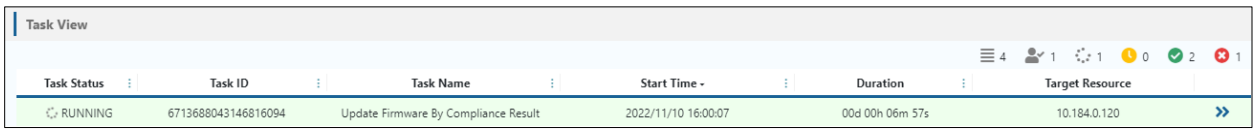


Figure 10-28

When the firmware auto-update task is complete, the **Next Update** column in **FW Notification View** page will display the next scheduled time.

Note: To enhance security, the checksum for the firmware file will be verified before downloading. If the checksum is inconsistent with the value from the Repository Server, the file will not be downloaded, and the error message will appear to show the difference between the Repository Server and the firmware file.

10.3.10 FW Auto Update: Selected Hosts

In addition to enabling the Firmware Auto Update mechanism by setting the schedule, you can also use **Update FW Now** command in **FW Notification View** page to fire firmware auto update task. Note that Update FW Now is only available when the selected host status or when the selected plan status is **Not Compliant**.

1. Select the host and click the orange bar in **Available FWs** column, a dialog box appears and shows you all firmware release information. Click the gray bar and check the release content again until all related information is reviewed completely.

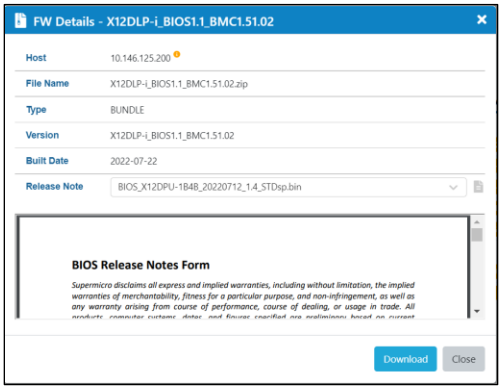


Figure 10-29

2. Expand the **Plan Operations** panel on the right, and then click **Update FW Now**.

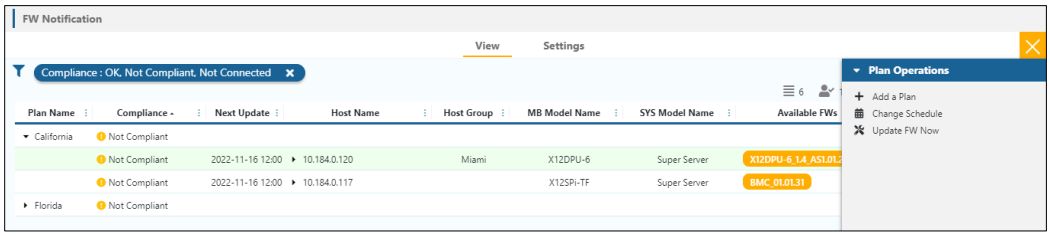


Figure 10-30

3. Click **Run** and then click the **Task ID** link to go the **Detailed Task View**. SSM uses an asynchronous task named **Update firmware By Compliance Result** to represent the request for the long task completion. Note that once you execute the command, the existed schedule setting on this host before will be cleared and SSM will update the host based on the firmware compliance check result immediately.

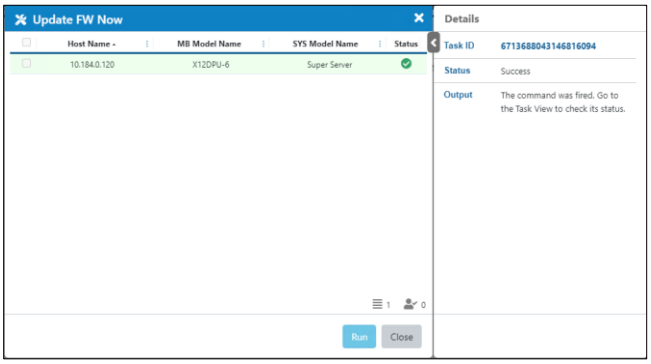


Figure 10-31

10.3.11 FW Auto Update: Reminders

If the firmware auto-update is manually triggered, an administrator receives the reminder when the task is started and the task is done. The reminder includes hyperlinks to FW Notification View and Task View.

1. Go to **FW Notification View** page. Select the desired hosts and click **Update FW Now** in the **Plan Operations** on the right-hand side of the panel. When the update firmware task is started, the reminder appears on the top of the page.

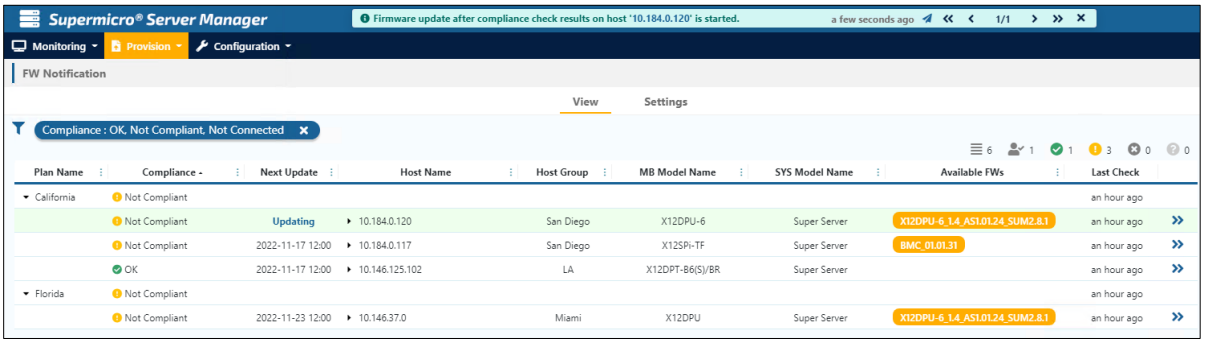


Figure 10-32

2. Use the right or left arrow buttons to view the reminders one by one while receiving the reminders.
3. To view the task execution and result, click the arrow icon in the reminder bar to go the **Detailed Task View**.

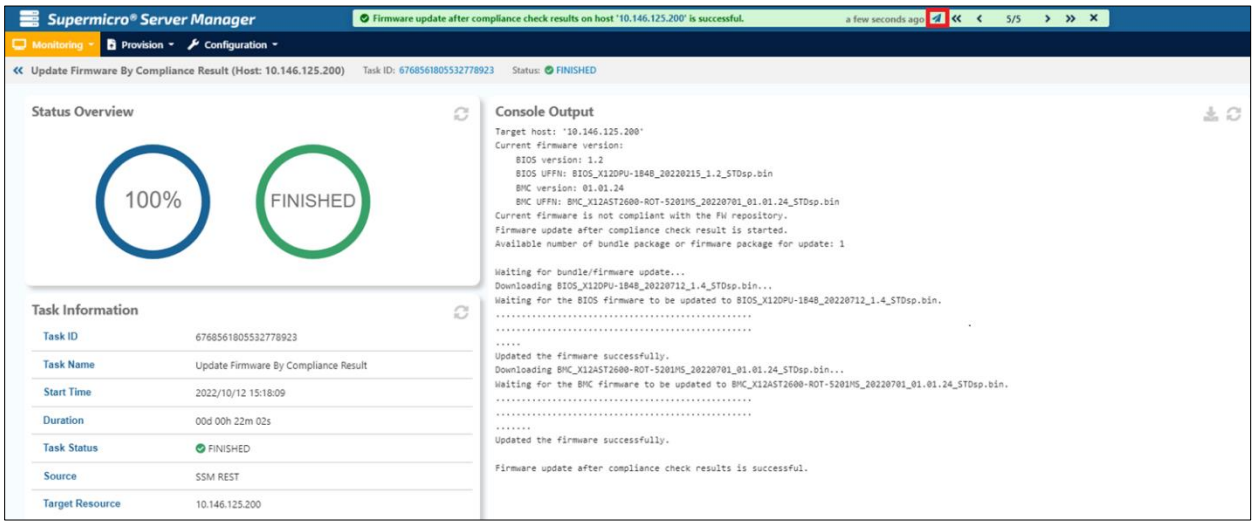


Figure 10-33

4. To view the status of the **Compliance**, click the host name (such as 10.146.125.200 in the above example) in the reminder to go to the **FW Notification View** page. If the firmware update task is successful, you will see the host of the **Compliance** showing **OK**.

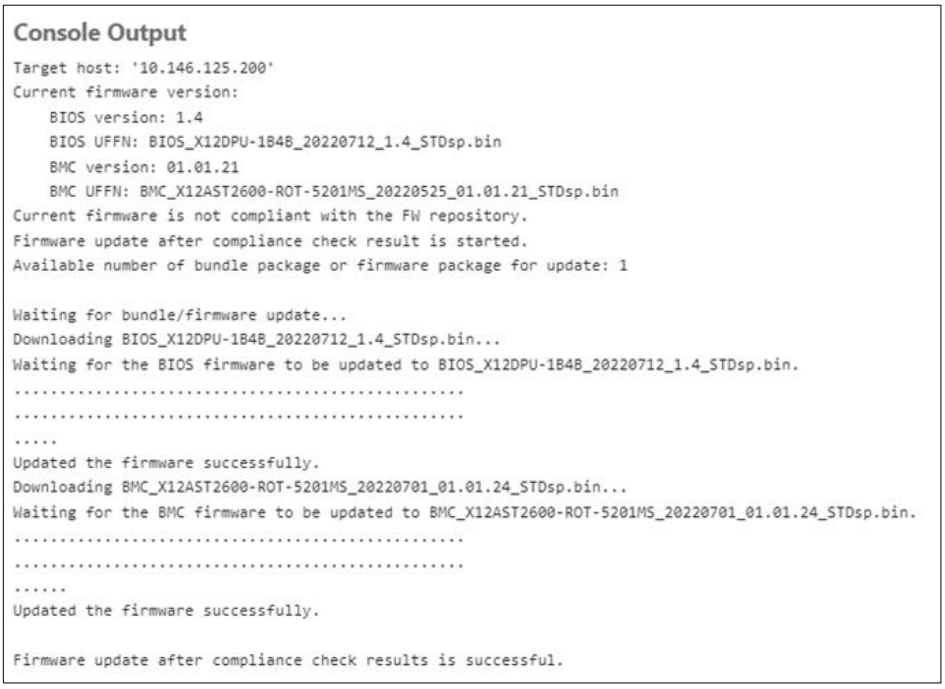
Note: The background color of the reminder bar shows different situations:

- **Light blue:** The firmware update is started.
- **Red:** The firmware update fails.
- **Green:** The firmware update is successful.

10.3.12 FW Auto Update: Progress

When the **Update firmware By Compliance Result** task begins, its status is displayed on Task View. To view the detailed update progress, select the desired task and then click the right double arrow icon to go the **Detailed Task View**.

The execution message is displayed on the Console Output panel, and a successful Firmware Auto Update with a bundle package example is shown below.



Console Output

```
Target host: '10.146.125.200'
Current firmware version:
    BIOS version: 1.4
    BIOS UFFN: BIOS_X12DPU-1B4B_20220712_1.4_STDsp.bin
    BMC version: 01.01.21
    BMC UFFN: BMC_X12AST2600-ROT-5201MS_20220525_01.01.21_STDsp.bin
Current firmware is not compliant with the FW repository.
Firmware update after compliance check result is started.
Available number of bundle package or firmware package for update: 1

Waiting for bundle/firmware update...
Downloading BIOS_X12DPU-1B4B_20220712_1.4_STDsp.bin...
Waiting for the BIOS firmware to be updated to BIOS_X12DPU-1B4B_20220712_1.4_STDsp.bin.
.................................................
.................................................
.....
Updated the firmware successfully.
Downloading BMC_X12AST2600-ROT-5201MS_20220701_01.01.24_STDsp.bin...
Waiting for the BMC firmware to be updated to BMC_X12AST2600-ROT-5201MS_20220701_01.01.24_STDsp.bin.
.................................................
.................................................
......
Updated the firmware successfully.

Firmware update after compliance check results is successful.
```

Figure 10-34

With the execution message, the user learns the current firmware version, the available number of the package for the update, the firmware package information, and the execution result.

If the firmware on a host fails to update, SSM will try to roll back the firmware to a previous version if the firmware package for the previous version and BMC are available. Note that only the firmware packages used by SSM for firmware auto-update will be preserved. If SSM is upgraded, none of the firmware packages will be reserved.

11 OS Deployment

The **Deploy OS** function allows users to deploy Linux OS on the managed IPMI/Redfish hosts. The supported versions of 64-bit Linux OS include:

- Red Hat Enterprise Linux Server 6.x, **7.x**, **8.x, 9.x**
- CentOS Server **7.x**, **8.x**
- Ubuntu Server 14.x, 15.x, 16.x, 18.04[10] LTS, 20.04 LTS
- SUSE Linux Enterprise Server 12.x, **15.x**
- VMware ESXi **6.5**, **6.7, 7.0, 8.0**
- Rocky Linux **8.x, 9.x**

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.
- If you use pure IPv6 environment, only the OS in bold is supported.

For the management server,

- Inbound TCP port and UDP port 514 need to be opened.
- Outbound TCP ports 4444 and 5555[11] need 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.
- 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 *7.3.2 IPMI Commands* and *7.3.10 Redfish Commands* for the steps to update the BMC and BIOS.

[10] SSM no longer supports unattended installation of Ubuntu with the "live-server" ISO files starting from Ubuntu 17. Please refer to *11.1* for details.
[11] SSM will collect the diagnostic information from the managed system through TCP ports 4444 and 5555 when the deployment task fails.

SSM allows users to deploy an OS in unattended mode. In this mode, users will only have to provide an answer file (e.g., Kickstart[12] in RHEL, AutoYAST[13] 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 or Redfish hosts (hosts with node product keys) on the Monitoring page for mass deployment.

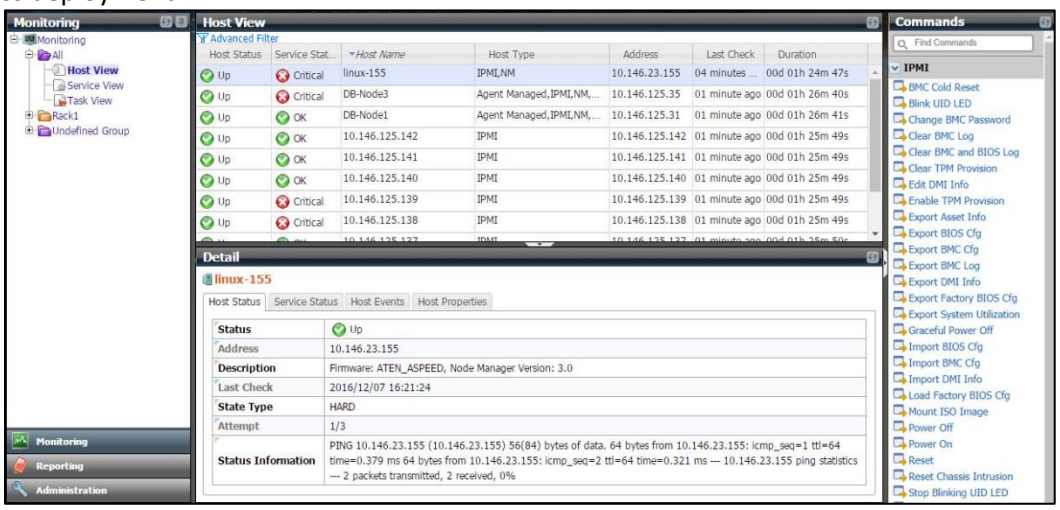


Figure 11-1

2. Click **Deploy OS** in the command area and a Deploy OS Arguments dialog box will appear.

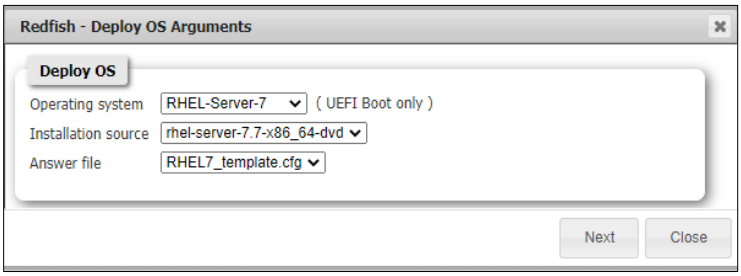


Figure 11-2

3. Use the drop-down menus and click the checkbox to select the **Operating system**, **Installation**

[12] Kickstart, a file containing the system installation information and configurations used on most Linux systems, can be used without user intervention.
[13] AutoYAST, an XML file containing the system installation information and configurations used on SLES systems, can be used without user intervention.

source and **Answer file**. Note that only Operating Systems such as RHEL Server, CentOS, Ubuntu, SLES, 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. Click the **Next** button to continue or the **Close** button to abort and close this dialog box.

- **Note:** The Deploy OS function supports installations in UEFI bootable devices only.

4. 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.

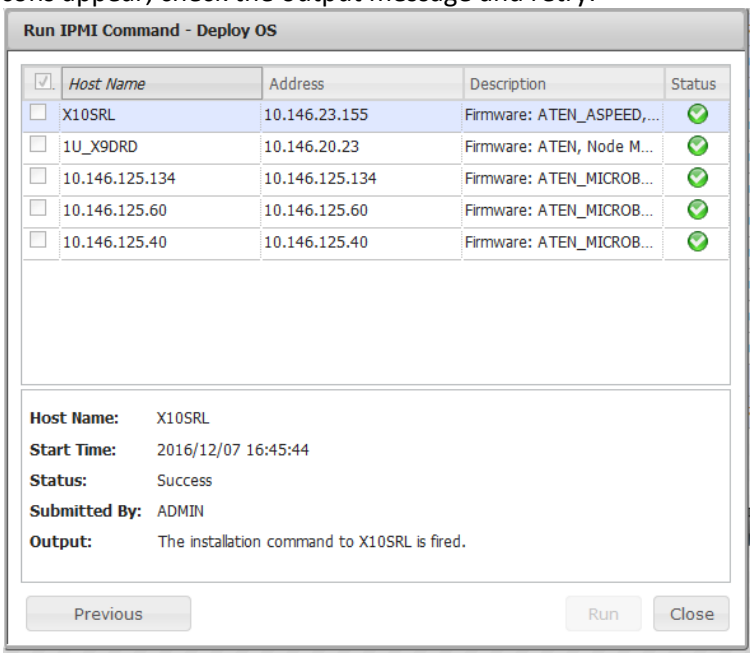


Figure 11-3

5. 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.

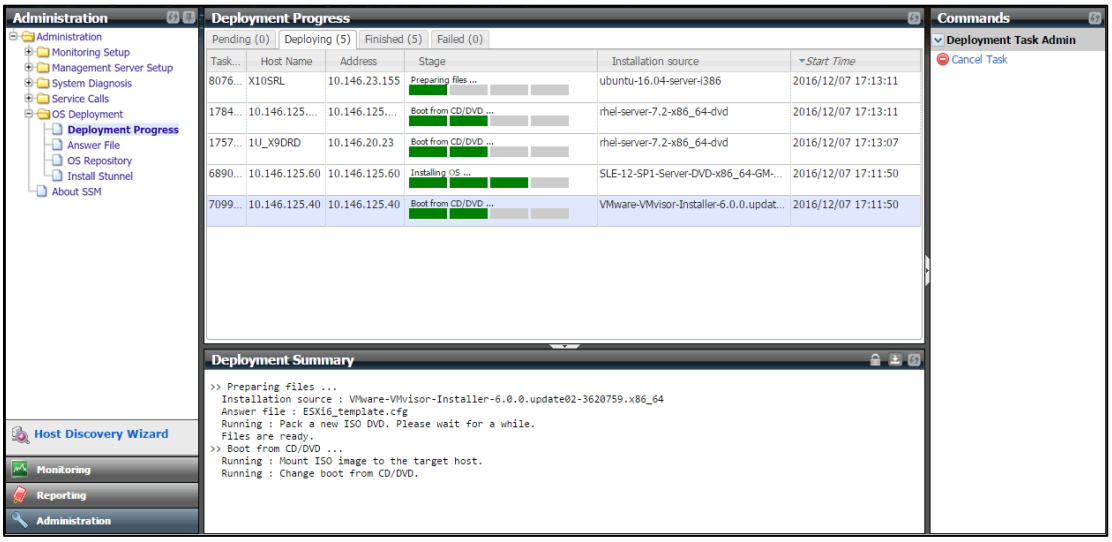


Figure 11-4

6. 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.

7. 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.

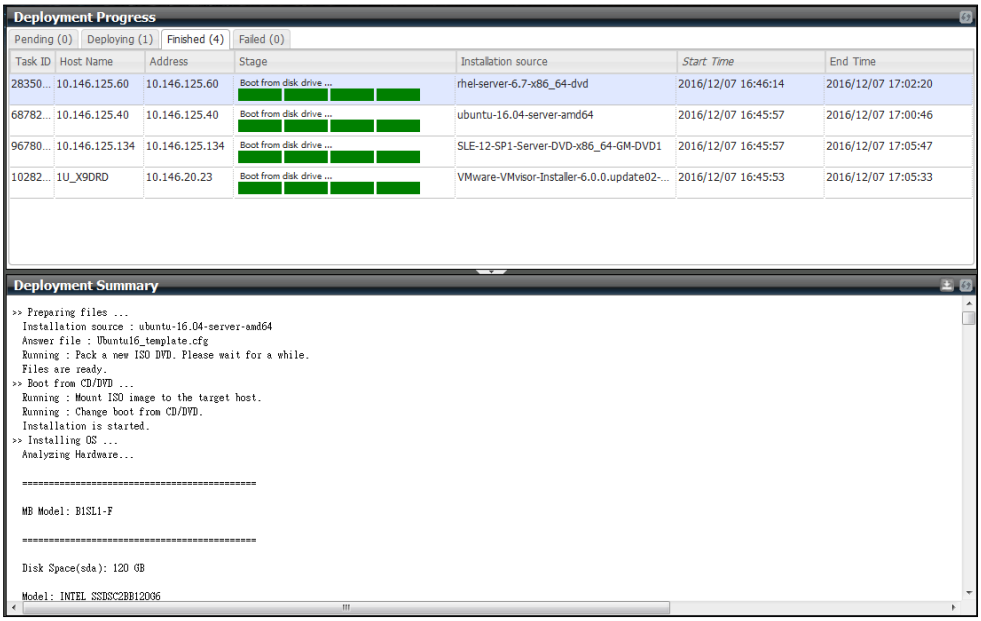


Figure 11-5

8. 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.

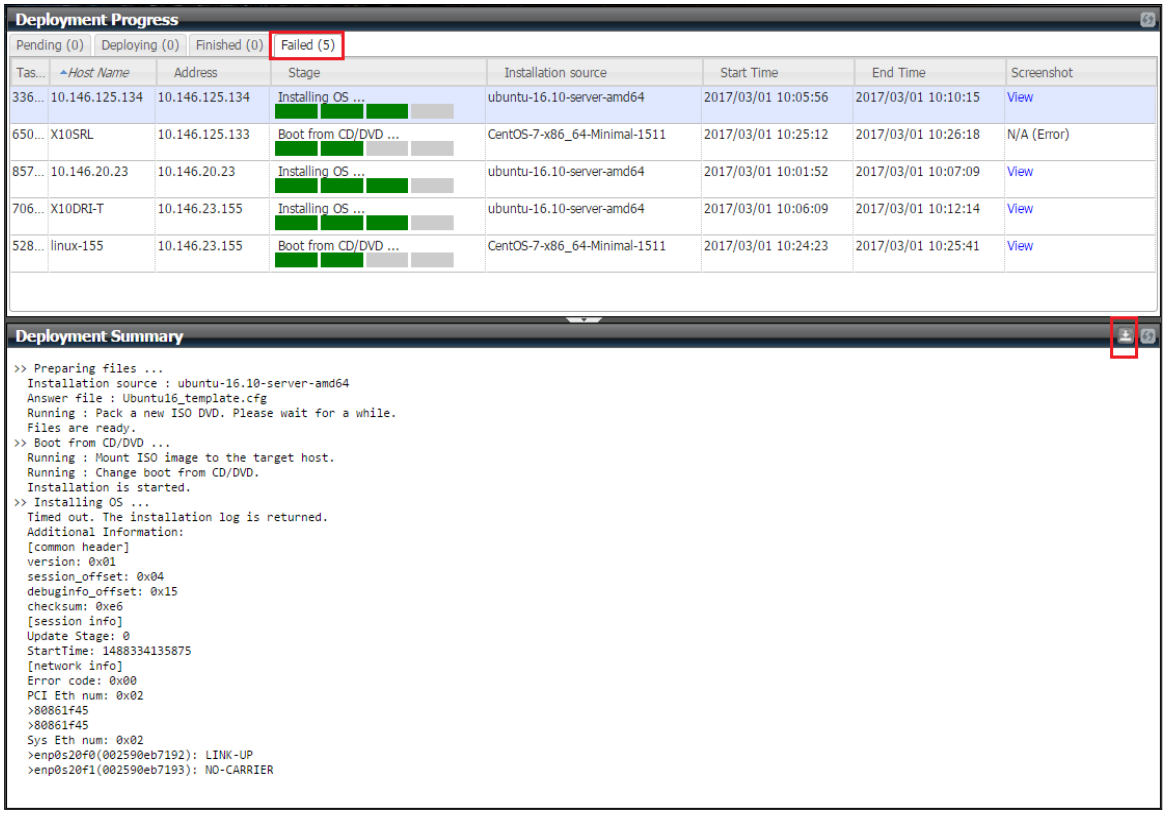


Figure 11-6

9. You can also use the BMC 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 8.3, you need to run the **Upload ISO** web command to upload an OS image (an ISO file, such as rhel-8.3-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.

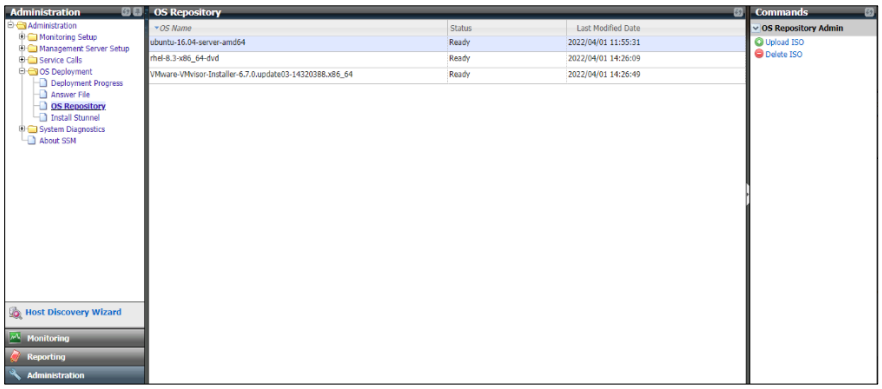


Figure 11-7

Note: In SSM, Ubuntu's feature “Kickstart” is adopted for remotely automated installation. Because of Ubuntu’s changes in their definition for images since version 17.10, SSM currently supports "non-live" images only.

Since its version 17.10, Ubuntu Server released images have been roughly categorized as "live" and "non-live" images, e.g., ubuntu-18.04.5-**live-server**-amd64.iso and ubuntu-18.04.5-**server**-amd64.iso. Starting from Ubuntu 20.04, the "non-live" server images are still available for use but renamed as "legacy" server images, e.g., ubuntu-20.04.1-**legacy-server**-amd64.iso. For more information, please refer to https://wiki.ubuntu.com/BionicBeaver/ReleaseNotes#Server_installer

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-8.3-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.

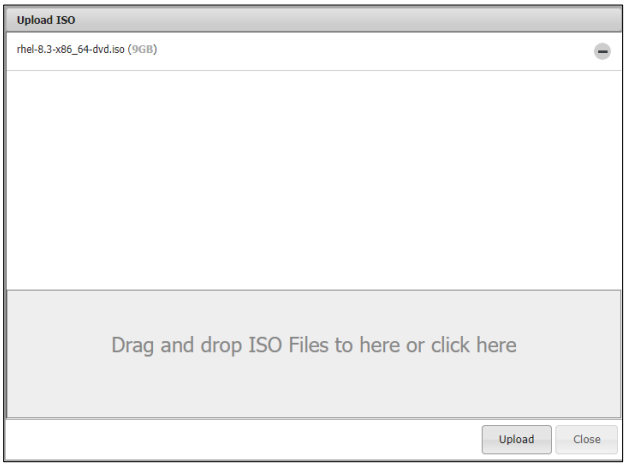


Figure 11-9

5. Click the **Upload** button to start uploading ISO files to the SSM folder. The upload progress is shown.

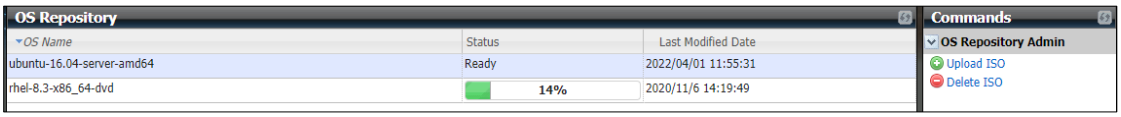


Figure 11-10

6. You may run the **Cancel Uploading ISO** web command to cancel the upload.

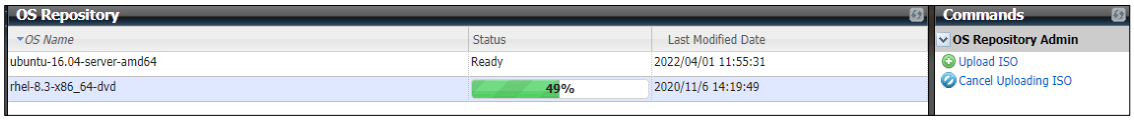


Figure 11-11

Note: The OS images uploaded for OS Deployment will not be preserved during the auto-upgrading process in Installer. You are required to upload the ISO files again when your SSM has been upgraded to a newer version.

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.

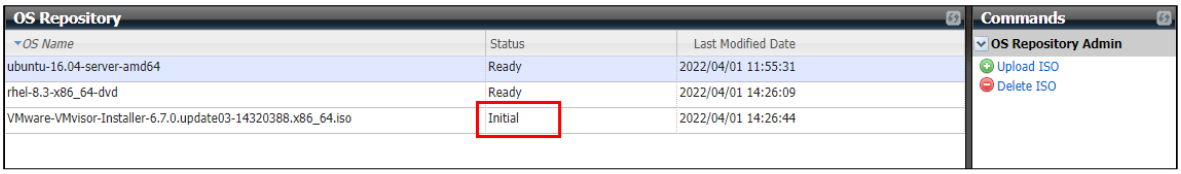


Figure 11-12

11.1.3 Deleting an ISO File

1. Select the ISO file(s) to be deleted in the working area. You can delete multiple ISO files at a time.

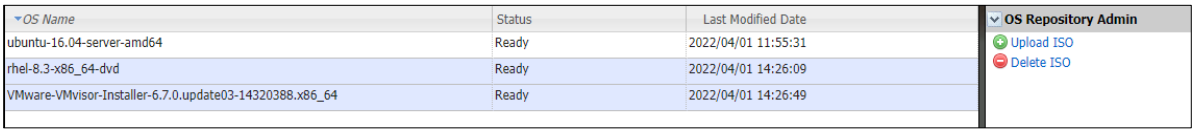


Figure 11-13

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

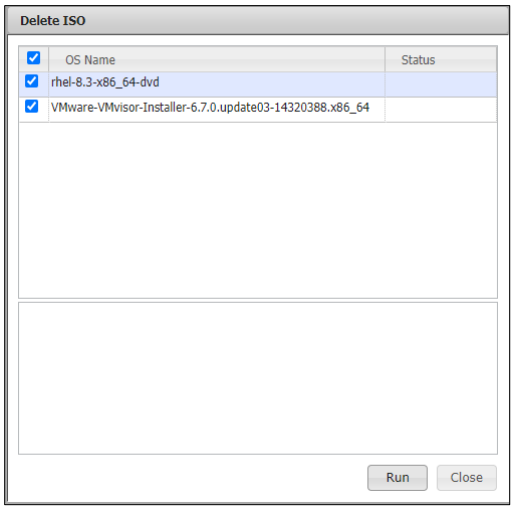


Figure 11-14

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, CentOS7_template for CentOS 7.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 RHEL6_template cannot be used for an unattended RHEL 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.

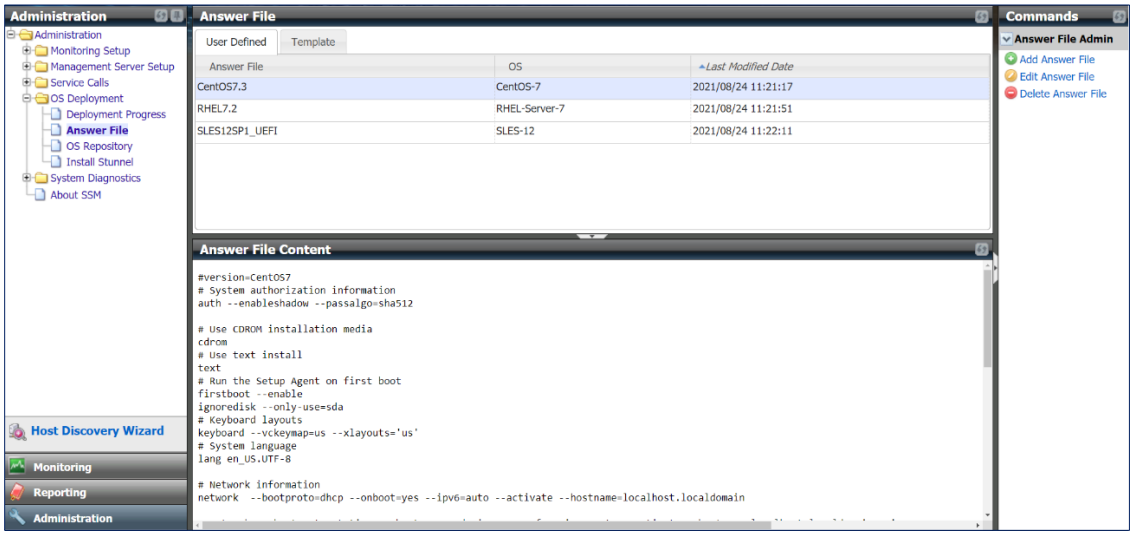


Figure 11-15

The functions of adding, editing and deleting are not supported in the **Template** tab.

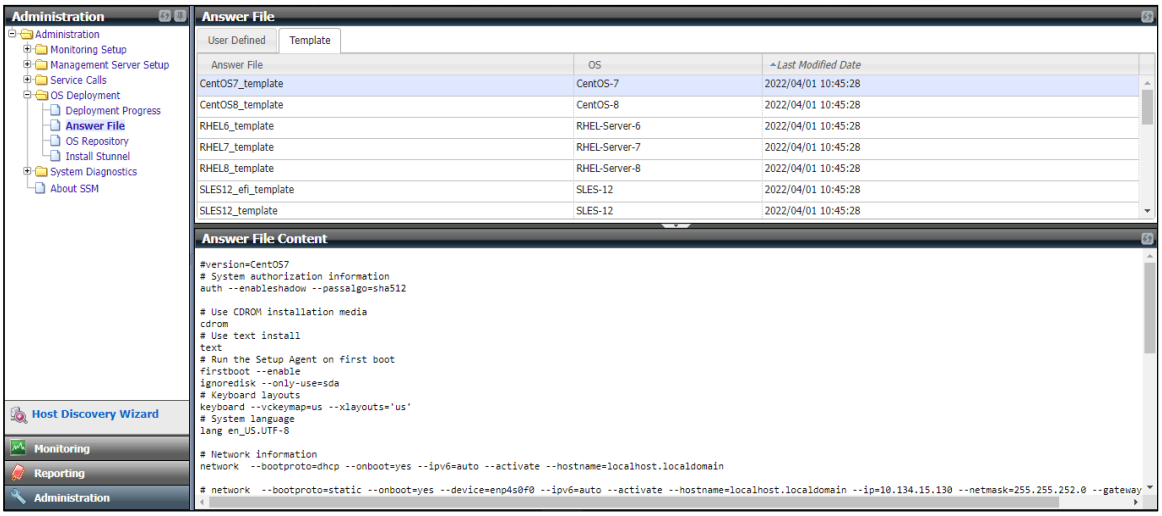


Figure 11-16

11.2.1 Attributes in Template Answer Files

Template Answer Files	Attribute	Description
CentOS/ RHEL/ Ubuntu	ignoredisk --only-use=**sda**	Specifies that only the **sda** drive is used and other disks should be ignored. 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

Template Answer Files	Attribute	Description
		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.
SLES	<enable_firewall config:type="boolean">true</enable_firewall> <start_firewall config:type="boolean">true</start_firewall>	Specifies the firewall is enabled.
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. (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>	
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. Note: It's required when performing an unattended installation on a system.
SLES	<user_password>123456</user_password> <username>root</username>	
VMware ESXi	rootpw default_PW	

Template Answer Files	Attribute	Description
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. 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. Note: It's required when performing an unattended installation on a system.
VMware ESXi	keyboard 'US Default'	
CentOS/ RHEL	authconfig --enableshadow --passalgo=sha512 auth --enableshadow --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.
SLES15 SP2+	<add-on> <add_on_products	Specifies the **Module-Basesystem** to be installed on the OS.

Template Answer Files	Attribute	Description
	config:type="list"> <listentry> <media_url><![CDATA[dvd:///?devices=/dev/sr0]]></media_url> <product>**Module-Basesystem**</product> <product_dir>Module-Basesystem</product_dir> </listentry> </add_on_products> </add-on>	Note: You can find the Software chapter in the AutoYast Guide on the SUSE web site (https://documentation.suse.com/sles/) for details.

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).

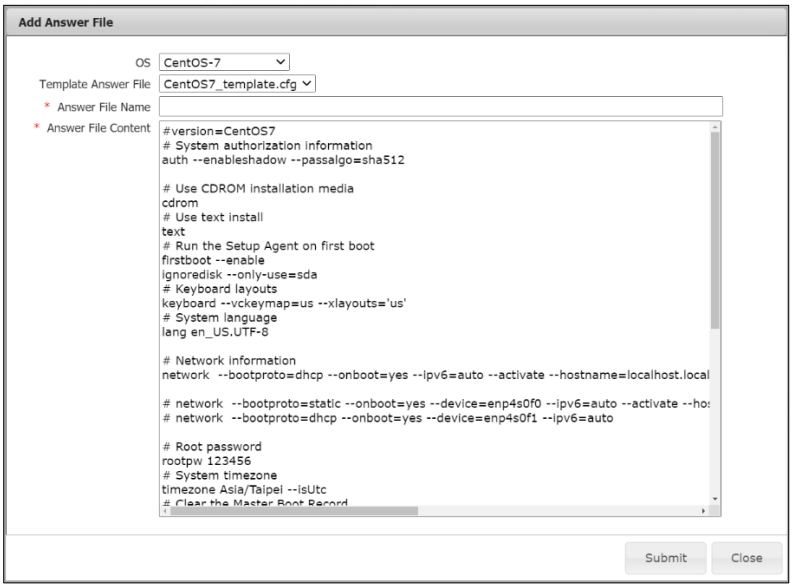


Figure 11-17

2. Select the OS type.

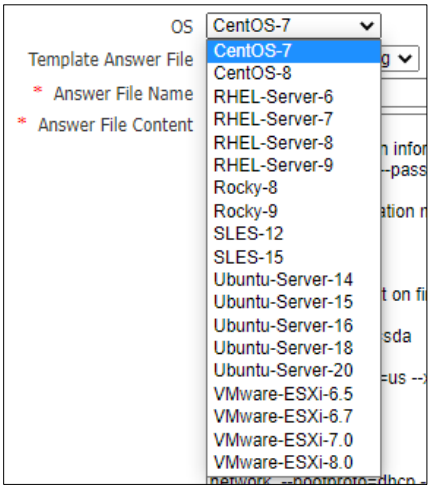


Figure 11-18

3. Select the template answer file. The drop-down list options may vary depending on the OS you selected.

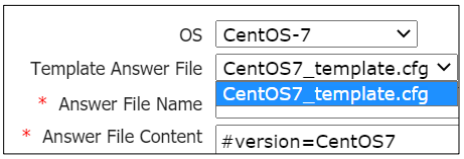


Figure 11-19

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.

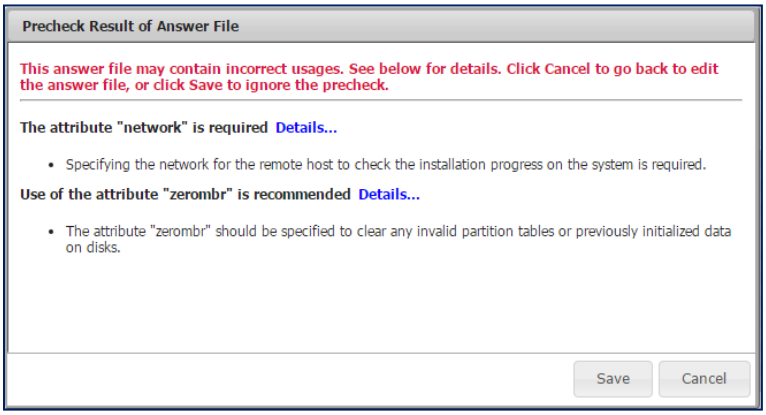


Figure 11-20

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.

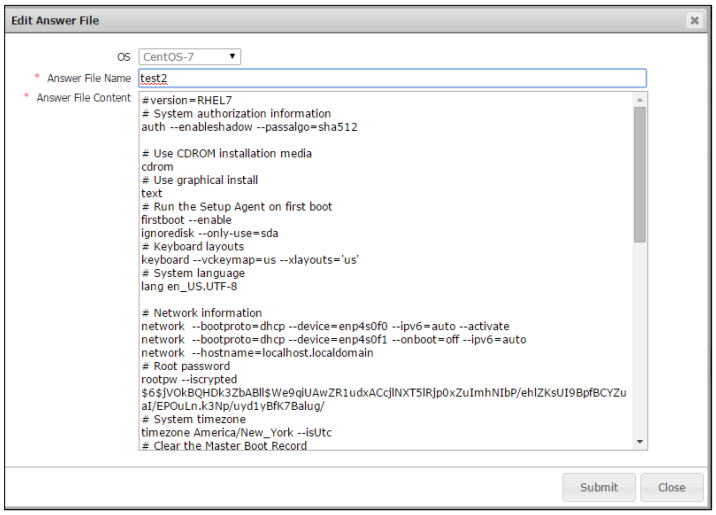


Figure 11-21

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.

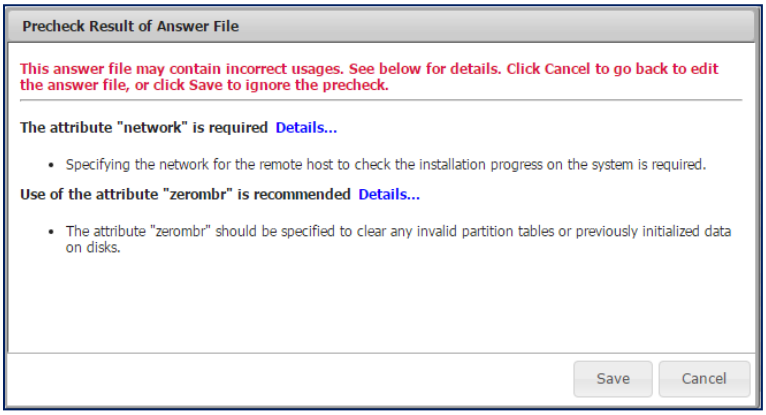


Figure 11-22

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.

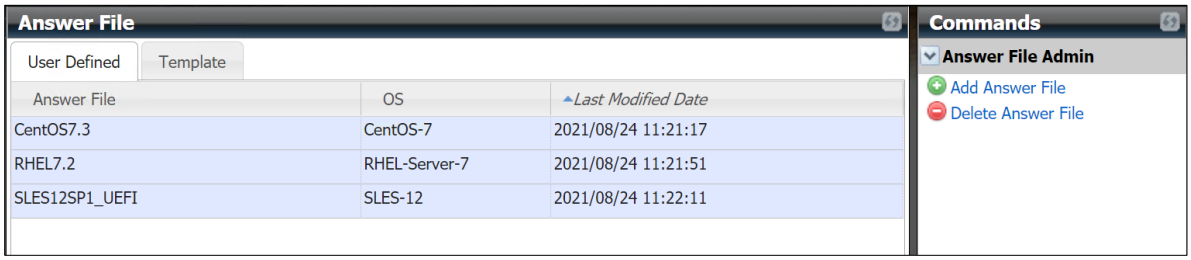


Figure 11-23

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

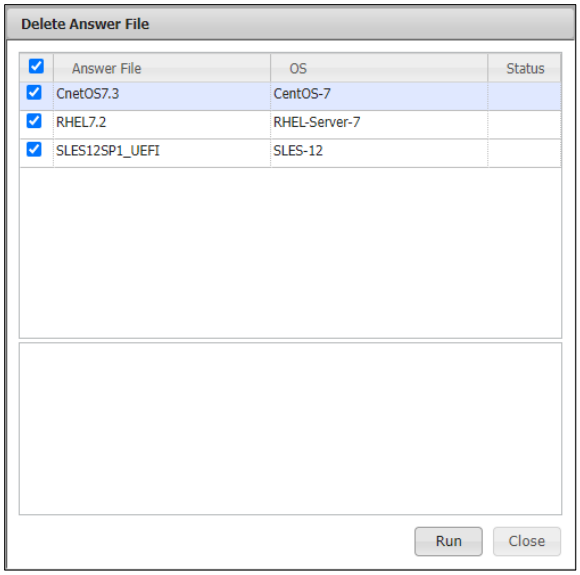


Figure 11-24

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.

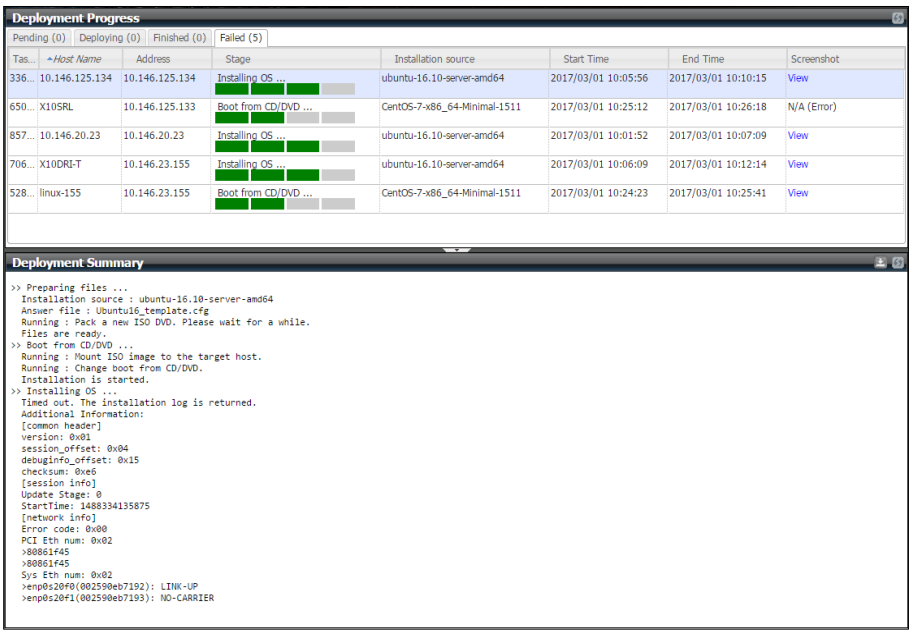


Figure 11-25

- 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/Redfish 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/Redfish 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/Redfish 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/Redfish 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/Redfish 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/Redfish host.
Tar file:	The local information from the IPMI/Redfish 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/Redfish 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.

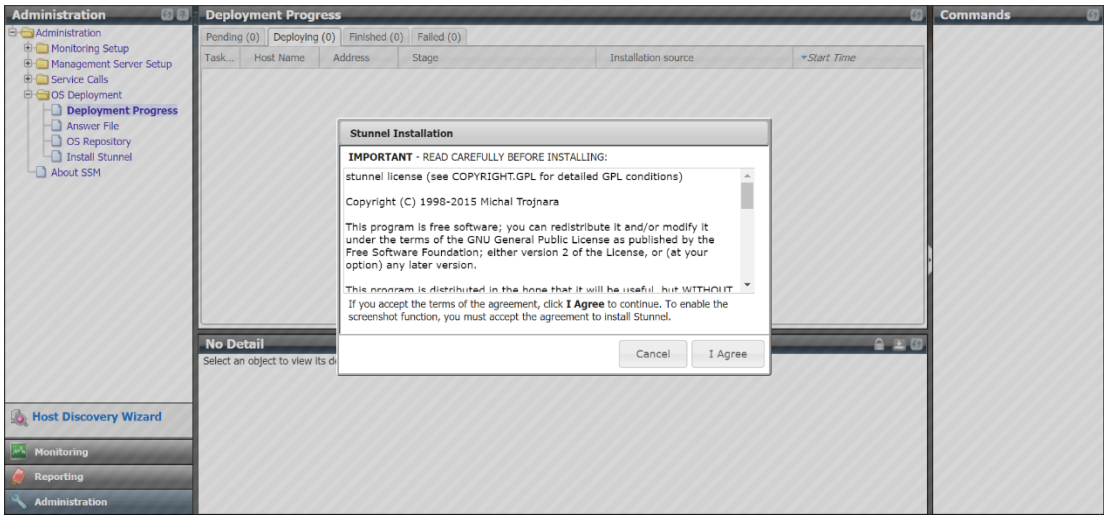


Figure 11-26

To install Stunnel, click **Install Stunnel** in the navigation area. You can either upload a Stunnel zip file or directly install from the Internet.

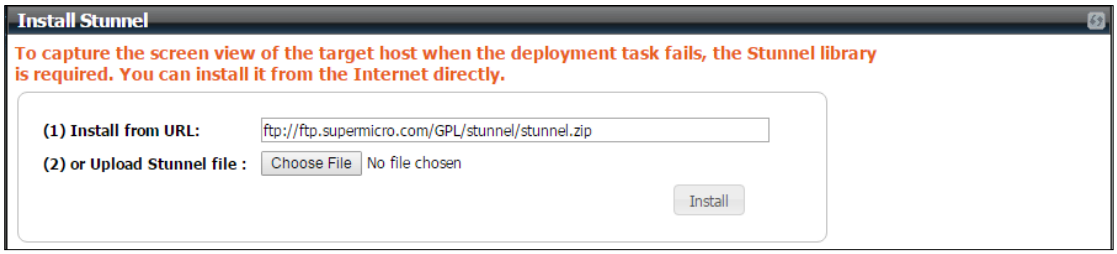


Figure 11-27

- **Install from URL**

Select this option and a license agreement dialog box appears. Read the agreement carefully and click **I Agree** to continue installation.

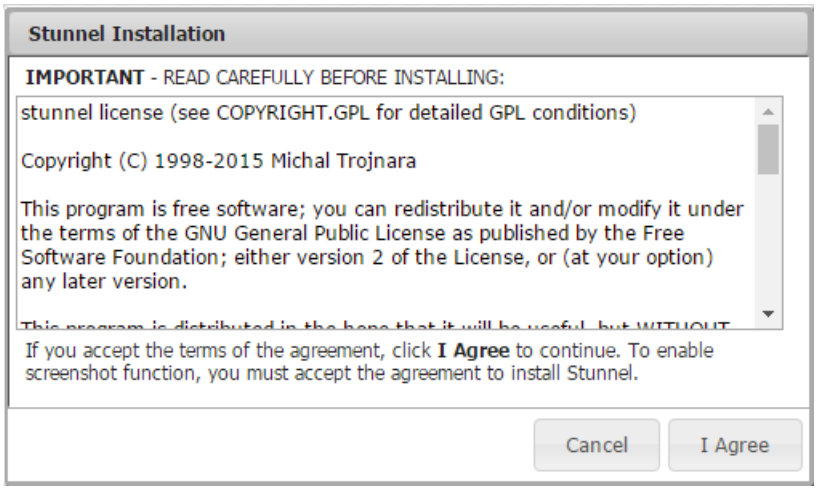


Figure 11-28

- **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:

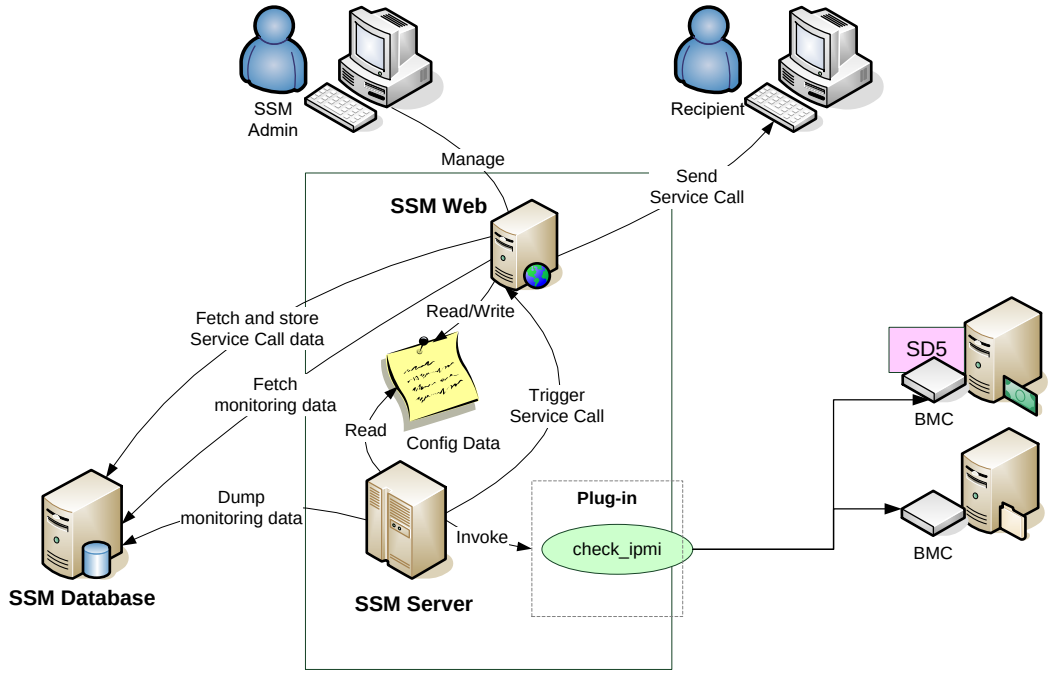


Figure 12-1

- **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 system of Supermicro X10 series and later generations 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 or a Redfish 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*, a customer (see 12.1.2.1 Adding a Customer), and a recipient (see 12.1.3.1 Adding a Recipient)* must be first added to a **Setup***; triggers (See 12.1.5.4 Editing Trigger) and a site location (See 12.1.4.1 Adding a Site Location)* are required for a **Device** defined in the Setup. Please see *12.1.5.7 Testing Service Call* for testing a Service Call after a Setup is complete or refer to a list of check items if you have trouble setting up a Service Call.

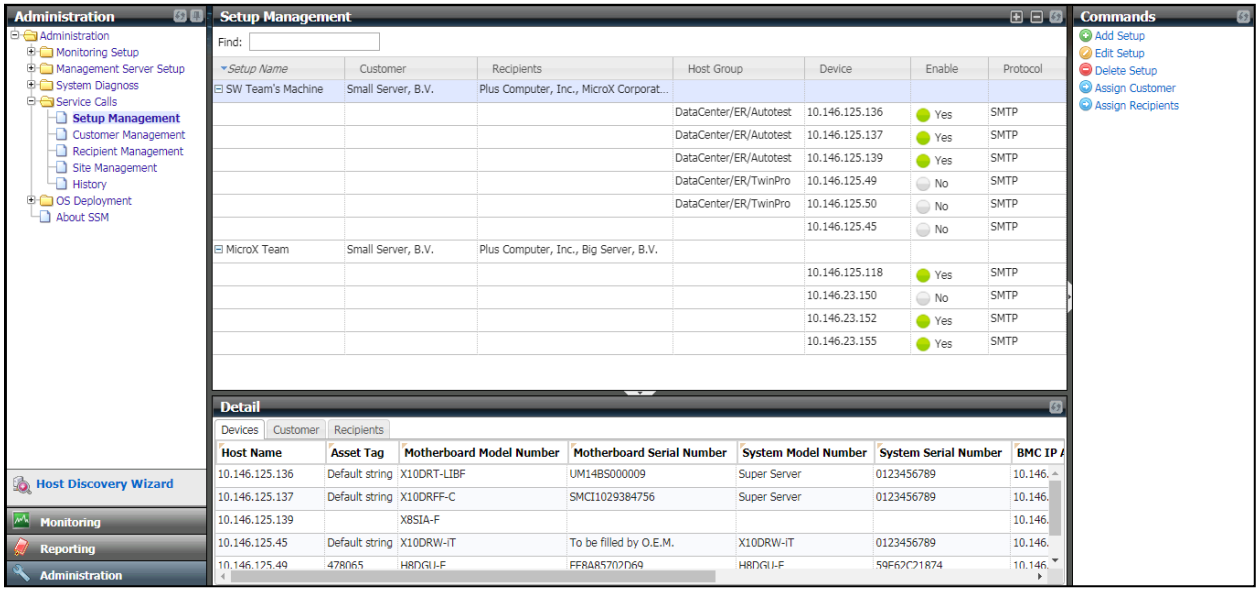


Figure 12-2

12.1.1.1 Adding a Setup

1. Click **Add Setup** in the commands area and an Add Setup dialog box appears.

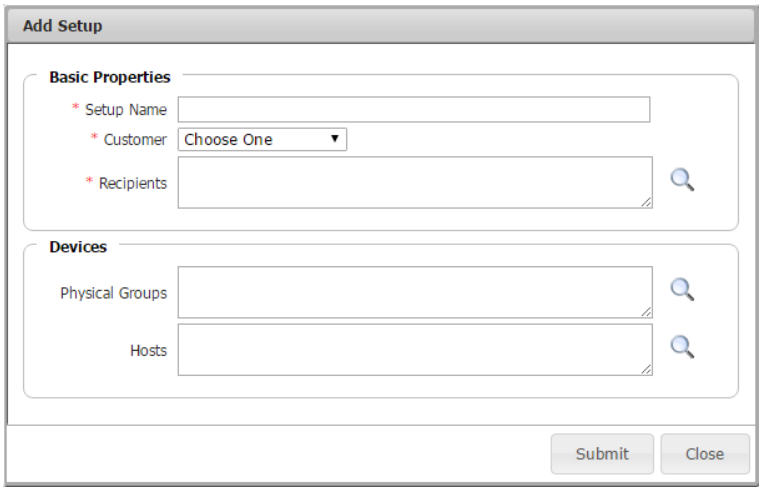


Figure 12-3

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 *12.1.2.1 Adding a Customer* 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 *12.1.3.1 Adding a Recipient* 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.

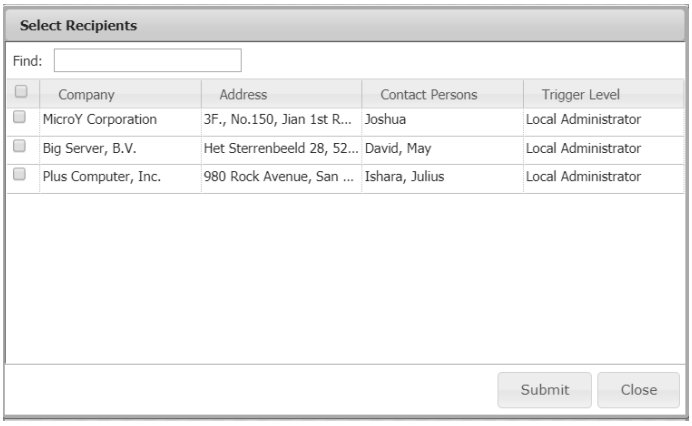


Figure 12-4

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.

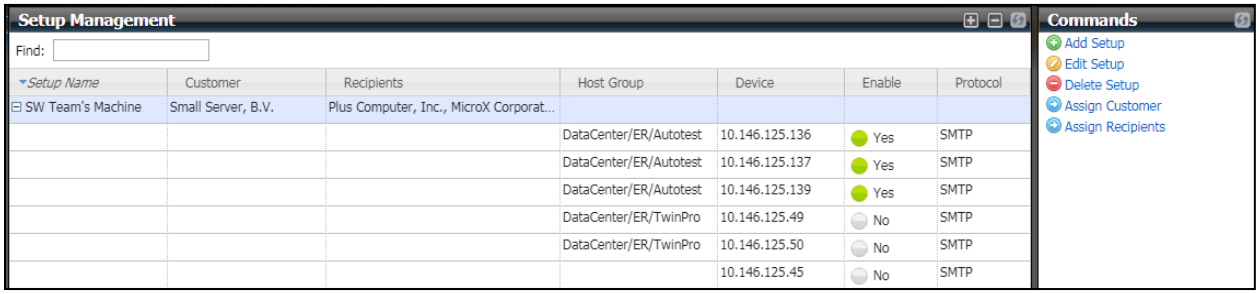


Figure 12-5

2. Click **Edit Setup** in the commands area and an Edit Setup dialog box appears.

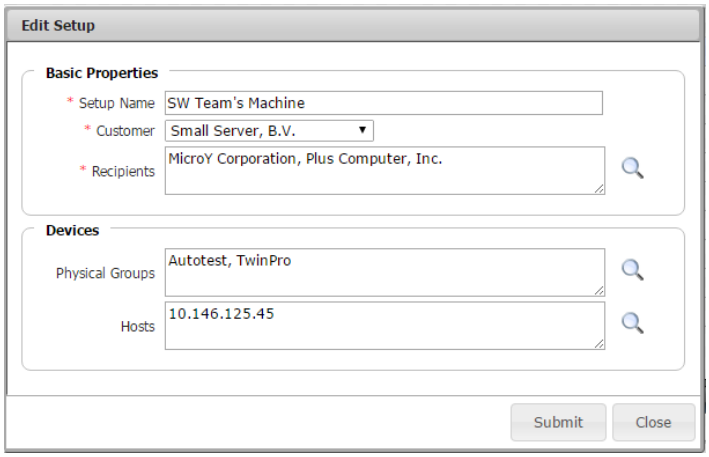


Figure 12-6

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.

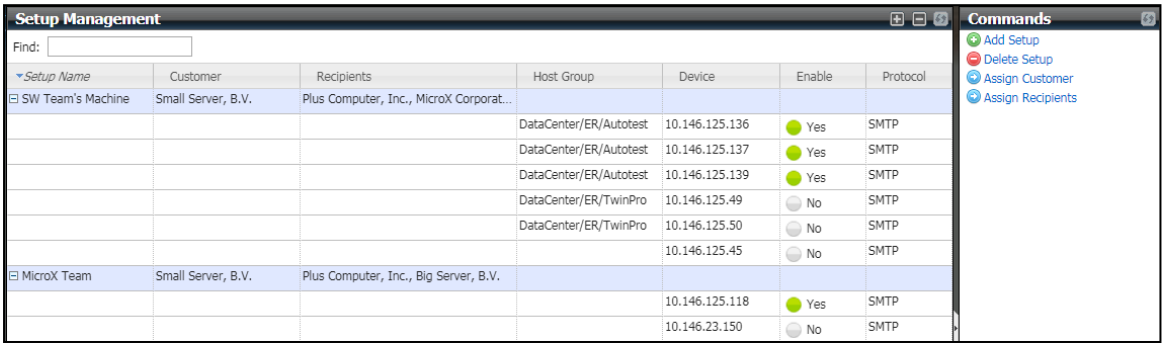


Figure 12-7

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

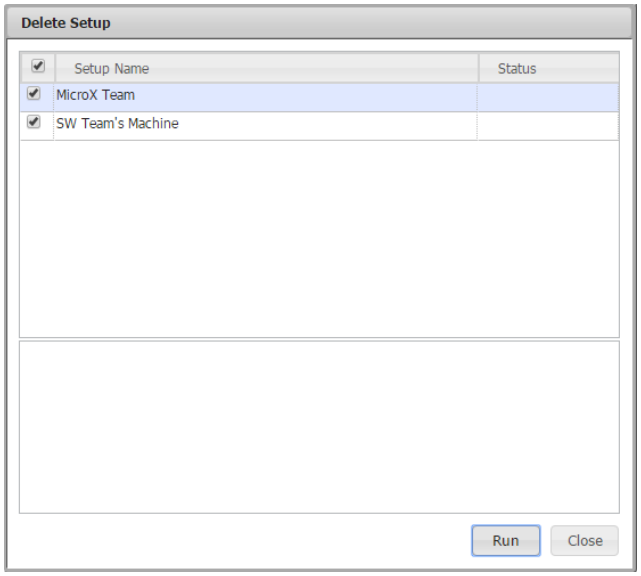


Figure 12-8

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.

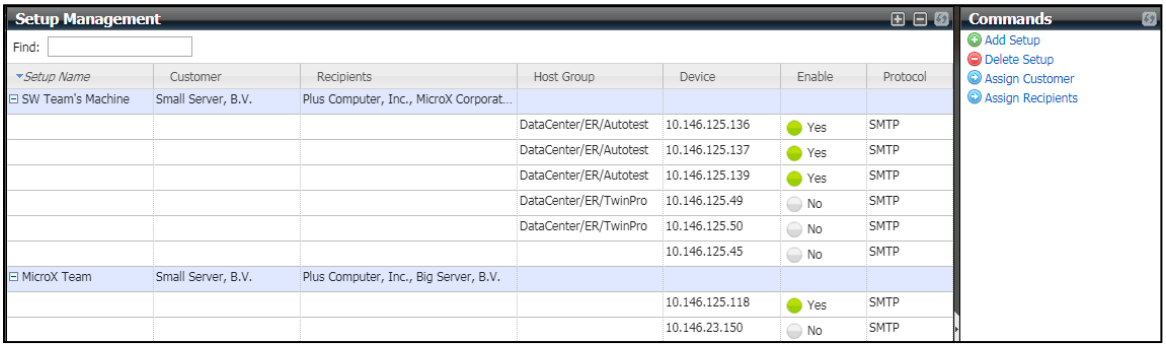


Figure 12-9

2. Click **Assign Customer** in the command area and an Assign Customer query dialog box appears.

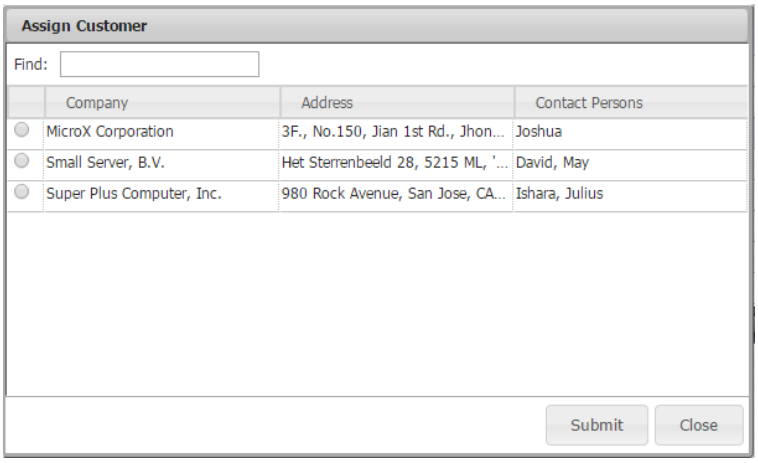


Figure 12-10

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.

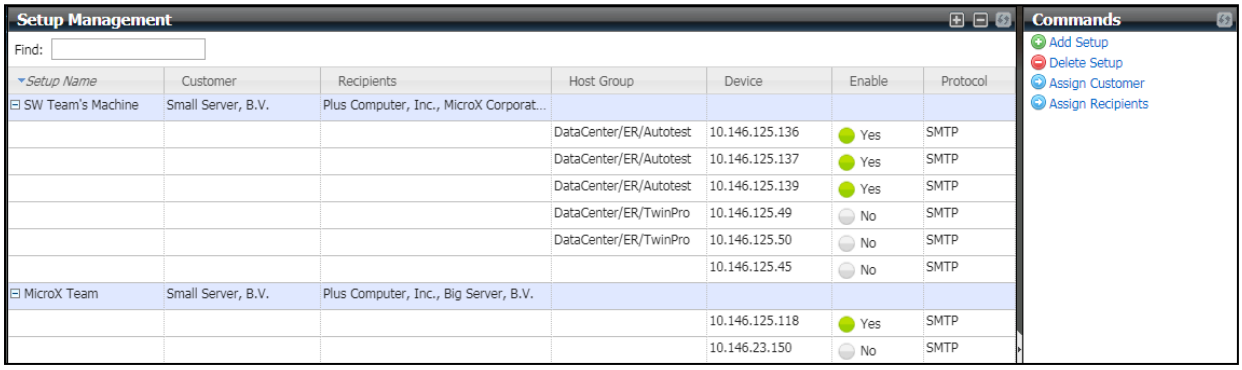


Figure 12-11

2. Click **Assign Recipients** in the command area and an Assign Recipients query dialog box appears.

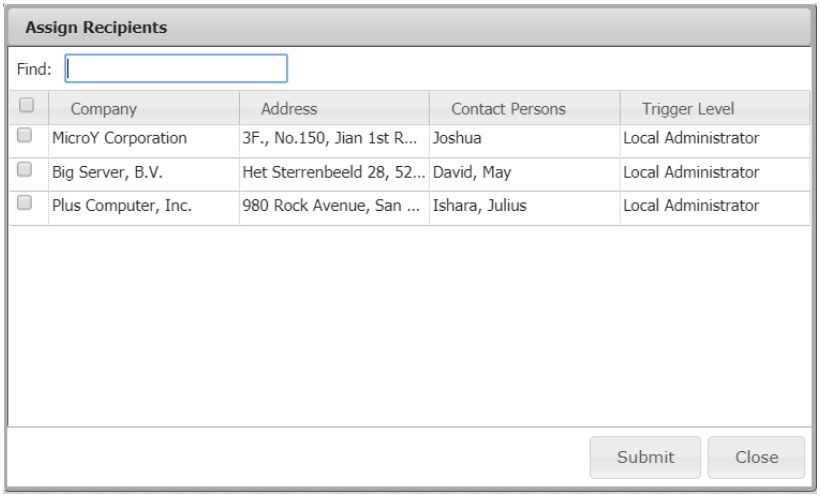


Figure 12-12

3. Select the recipients to be assigned and click the **Submit** button.

12.1.2 Customer Management

Customers will be used in Setup configurations. Click **Customer Management** in the navigation area to perform Customer Management functions.

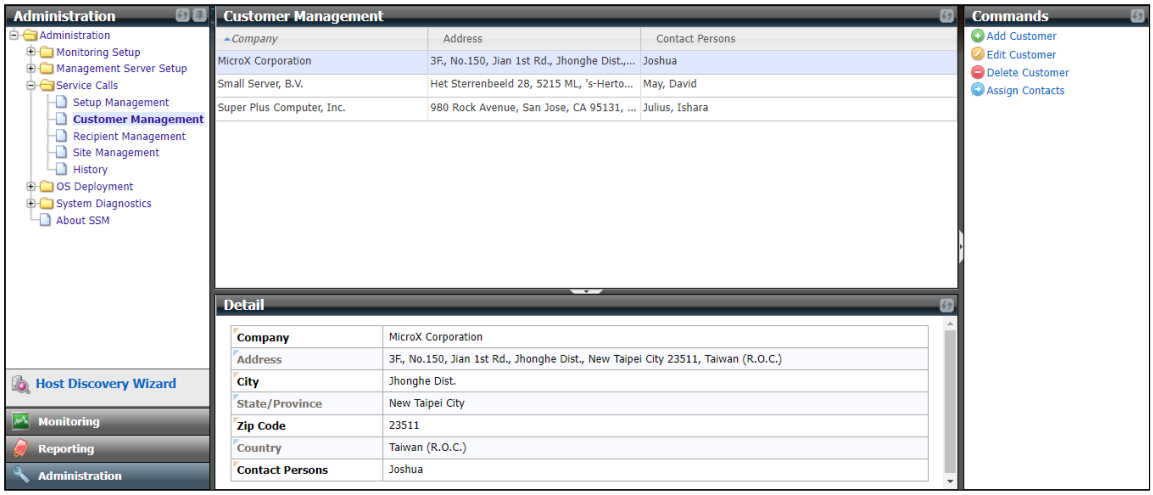


Figure 12-13

12.1.2.1 Adding a Customer

1. Click **Add Customer** in the commands area and an Add Customer dialog box appears.

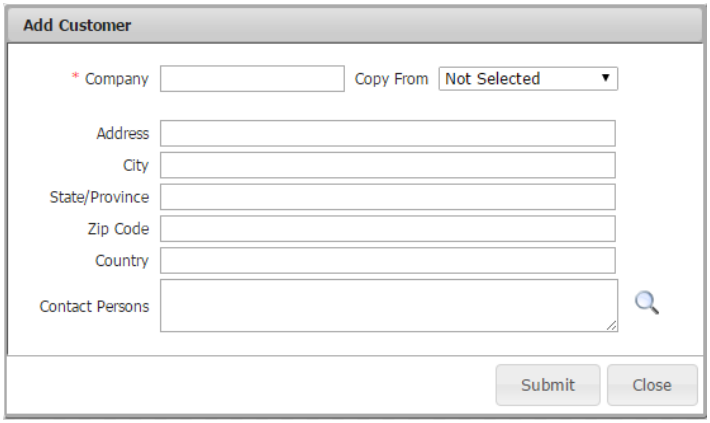


Figure 12-14

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 *6.4 Contact Management* to add contacts first.

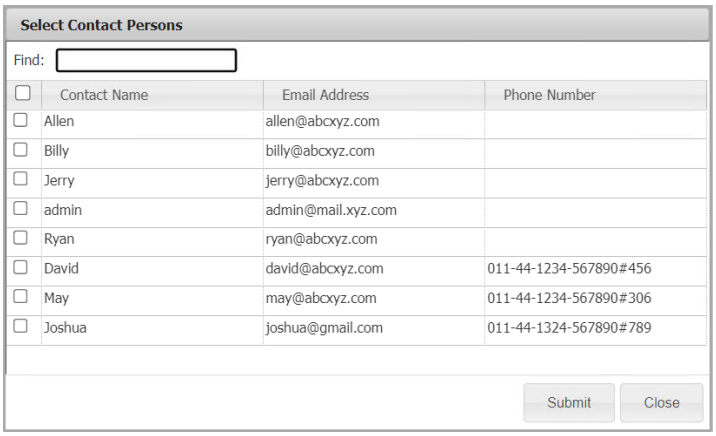


Figure 12-15

Note: You can click on the **Copy From** pull-down menu to copy the customer data from an existing customer.

3. 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.

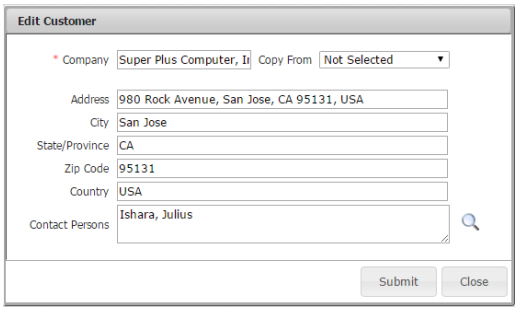


Figure 12-16

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.

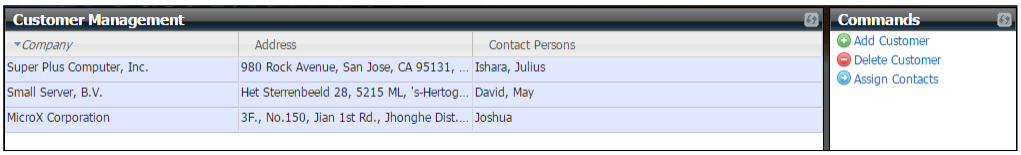


Figure 12-17

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

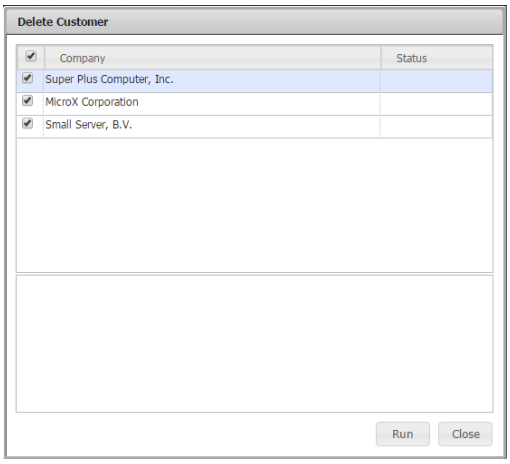


Figure 12-18

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.

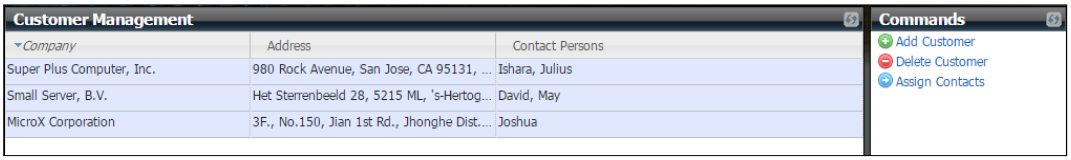


Figure 12-19

2. Click **Assign Contacts** in the command area and an Assign Contacts query dialog box appears.

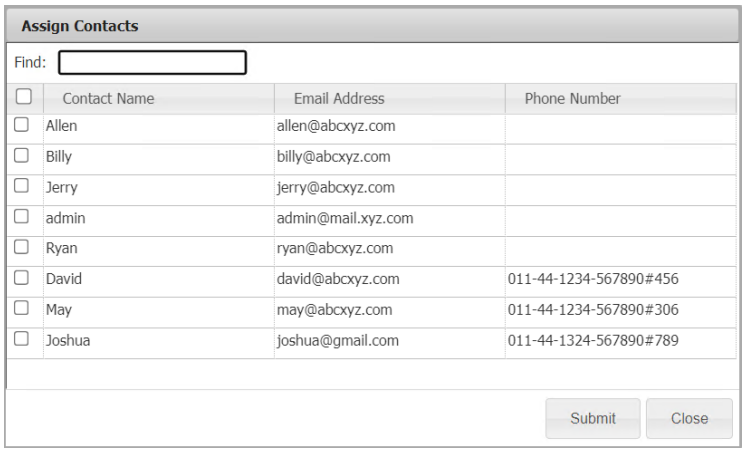


Figure 12-20

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.

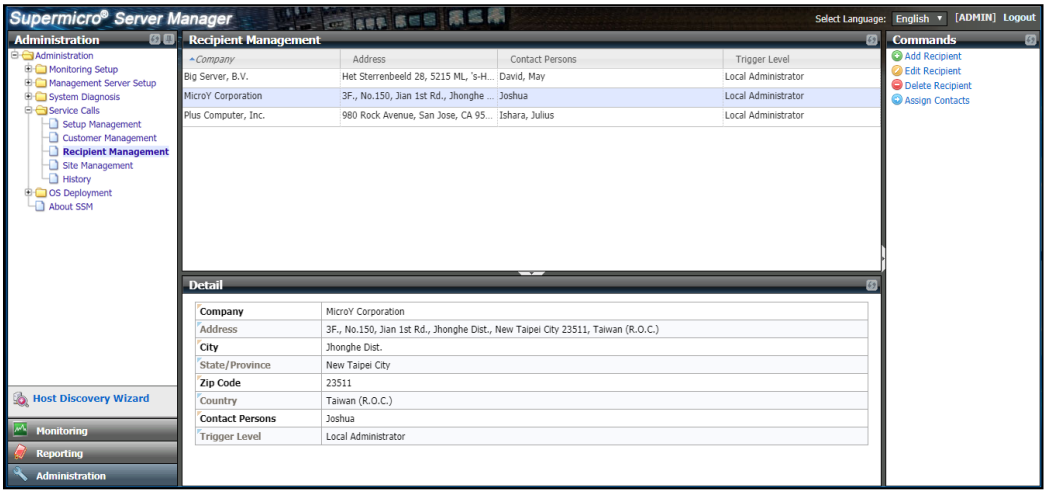


Figure 12-21

12.1.3.1 Adding a Recipient

1. Click **Add Recipient** in the commands area and an Add Recipient dialog box appears.

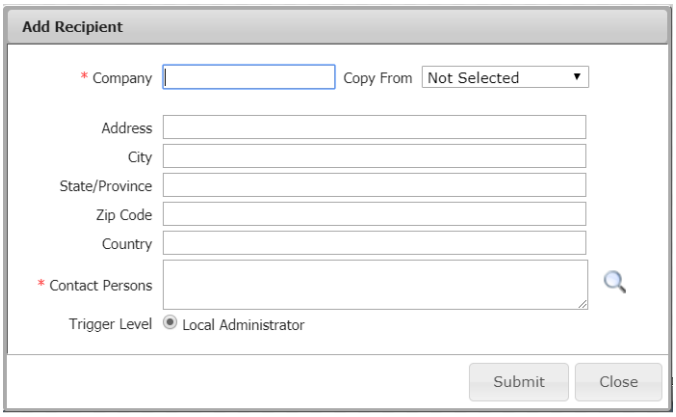


Figure 12-22

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 *6.4 Contact Management* 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.

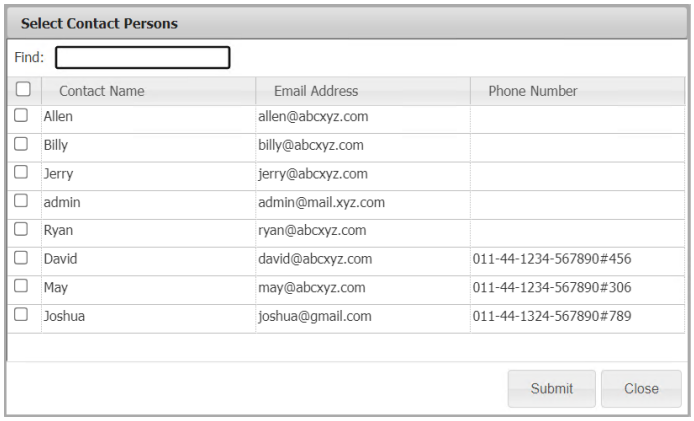


Figure 12-23

Note: You can click on the **Copy From** pull-down menu to copy the recipient data from an existing recipient.

3. 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.

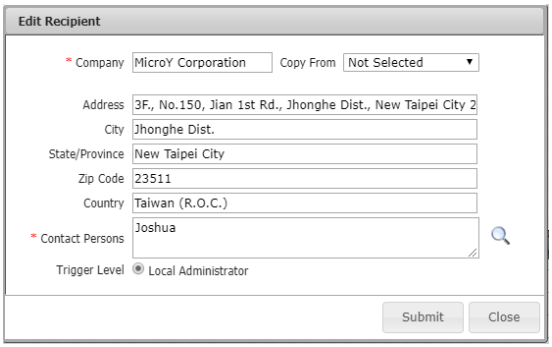


Figure 12-24

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.

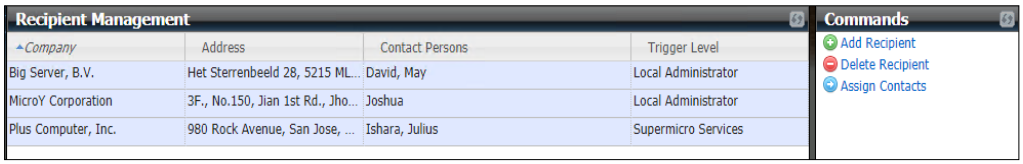


Figure 12-25

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

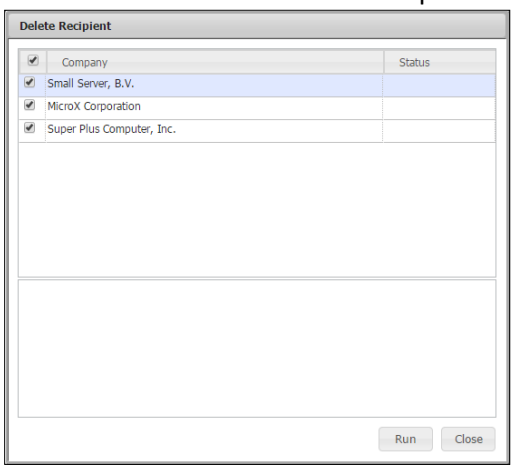


Figure 12-26

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.

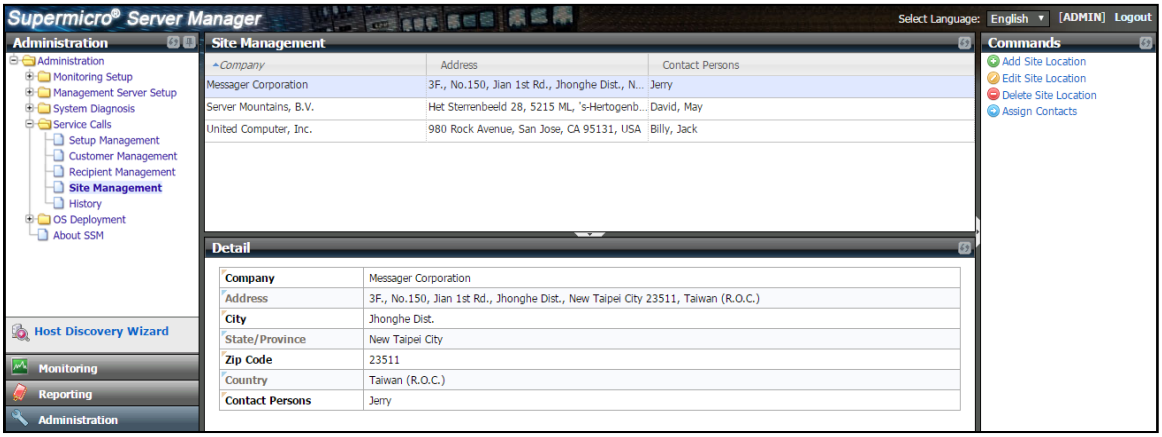


Figure 12-27

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.

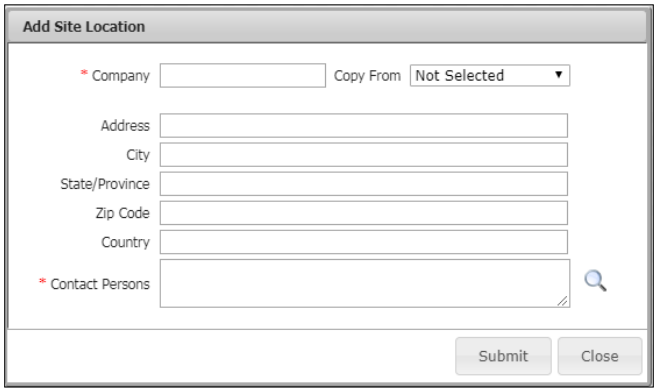


Figure 12-28

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.

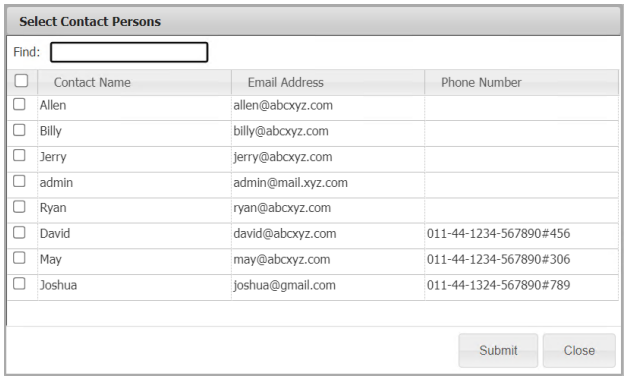


Figure 12-29

Note: You can click on the **Copy From** pull-down menu to copy the site location data from an existing site location.

3. 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.

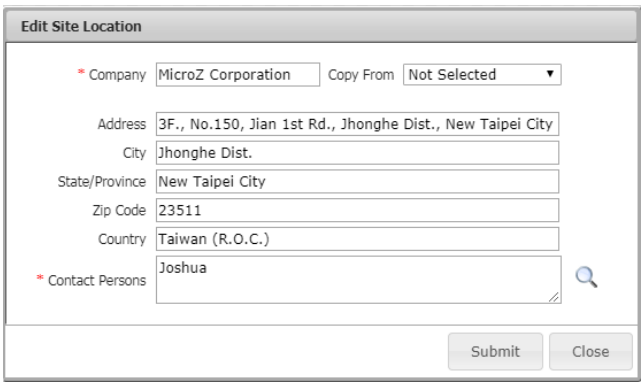


Figure 12-30

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.

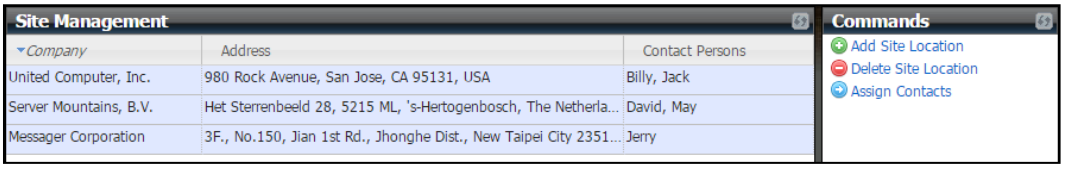


Figure 12-31

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

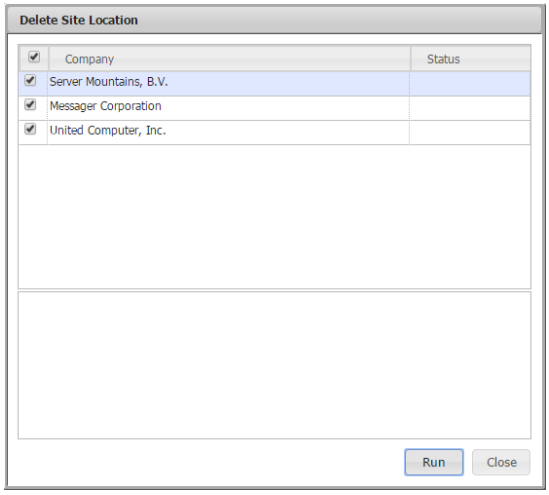


Figure 12-32

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.*

12.1.5 Device Management

12.1.5.1 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 hosts with the SFT-DCMS-SVC-KEY product key activated**.** You can only edit one device at a time.

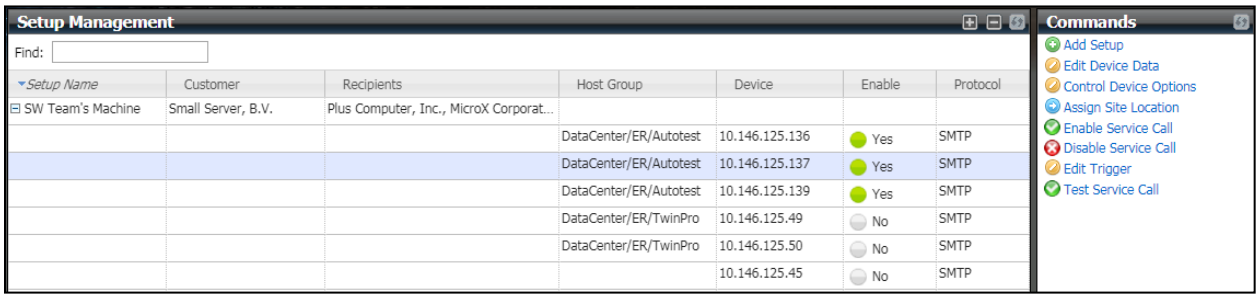


Figure 12-33

2. Click **Edit Device Data** in the commands area and an Edit Device Data dialog box appears.

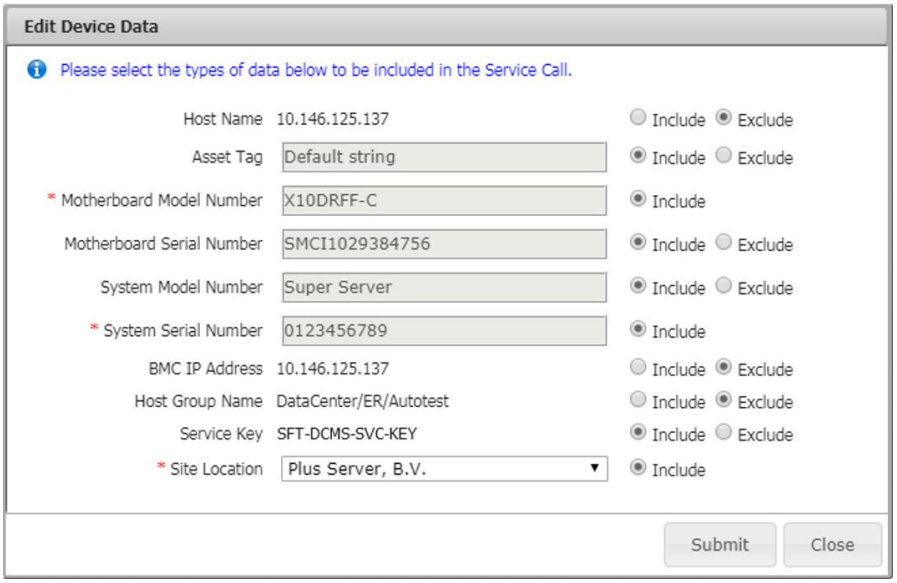


Figure 12-34

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).
BMC IP Address	The IP address of the BMC 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 *12.1.4.1 Adding a Site Location* 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/Redfish 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.

12.1.5.2 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.

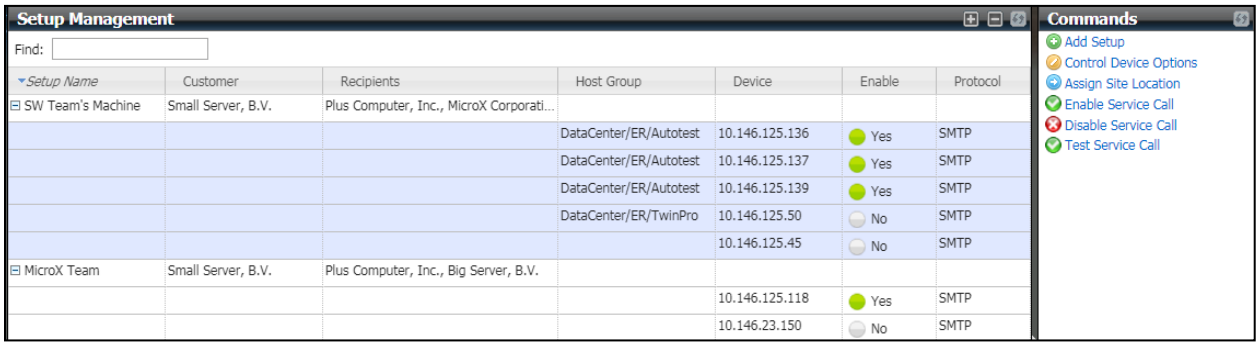


Figure 12-35

2. Click **Control Device Options** in the command area and a Control Device Options query dialog box appears.

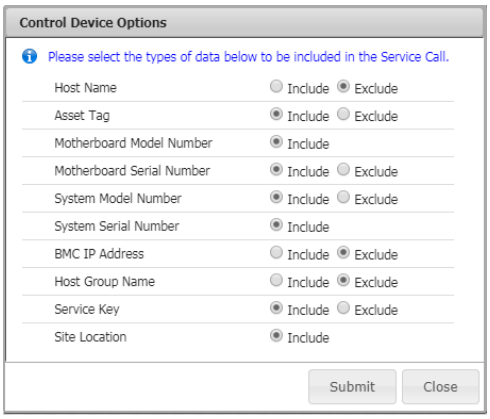


Figure 12-36

3. Select the attributes to be included in Service Call alert and click the **Submit** button.

12.1.5.3 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.

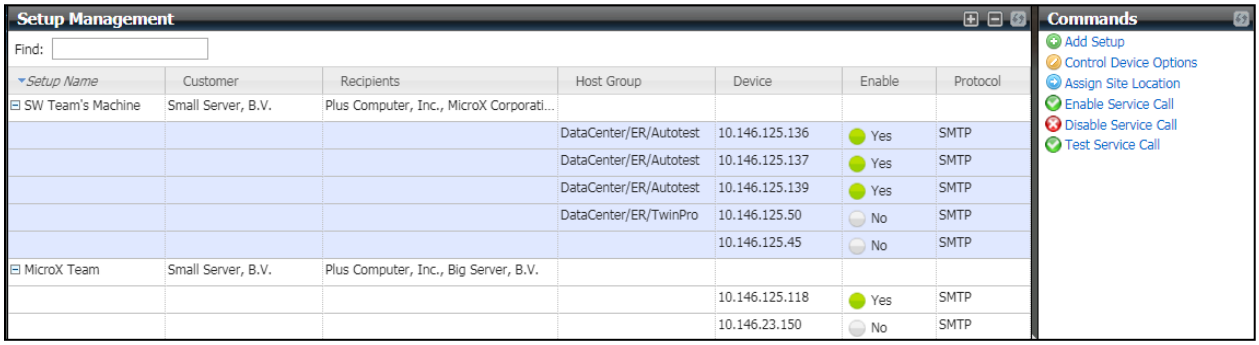


Figure 12-37

2. Click **Assign Site Location** in the command area and an Assign Site Location query dialog box appears.

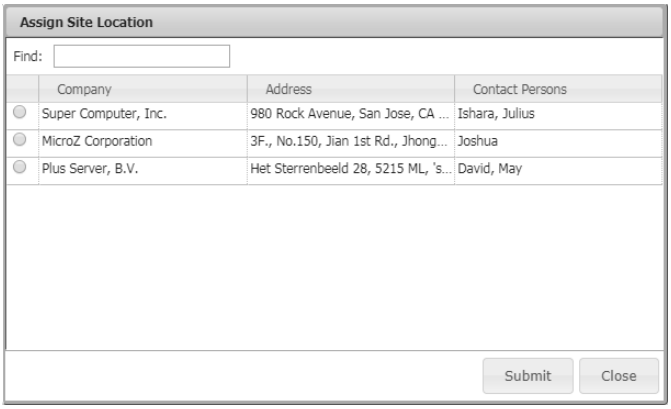


Figure 12-38

3. Select the site location to be assigned and click the **Submit** button.

12.1.5.4 Editing Trigger

SSM fetches the trigger items based on the last check results from the IPMI/Redfish SEL Health service. Trigger items include the present BMC sensors with the corresponding severity level and the SEL definition in the BMC. SSM will collect all trigger items and store them into a cache. After initialization, the trigger items will be loaded from the cache. The cache is changed while the service check of IPMI/Redfish SEL 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.

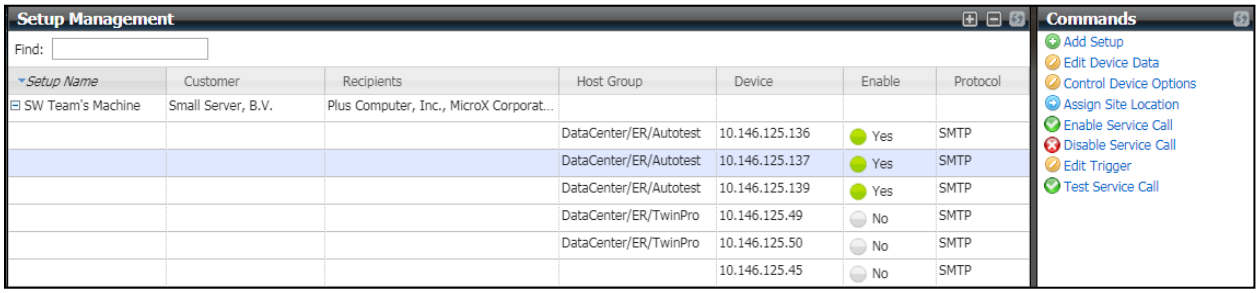


Figure 12-39

2. Click **Edit Trigger** in the command area and the Edit Trigger dialog box appears.

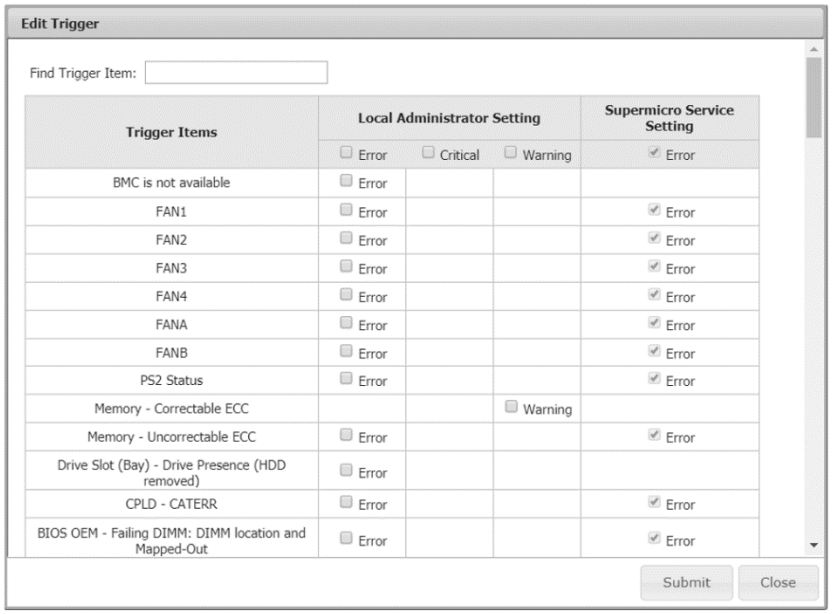


Figure 12-40

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.

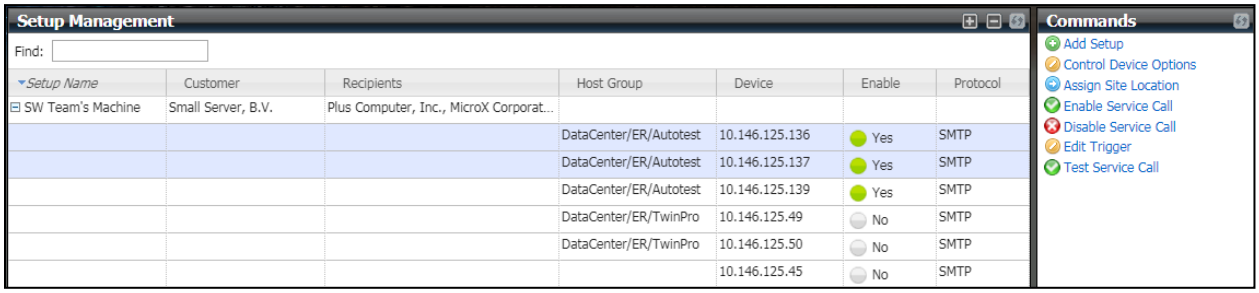


Figure 12-41

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, all of their available trigger items, even with different severity levels, are all shown in the Edit Trigger dialog box.

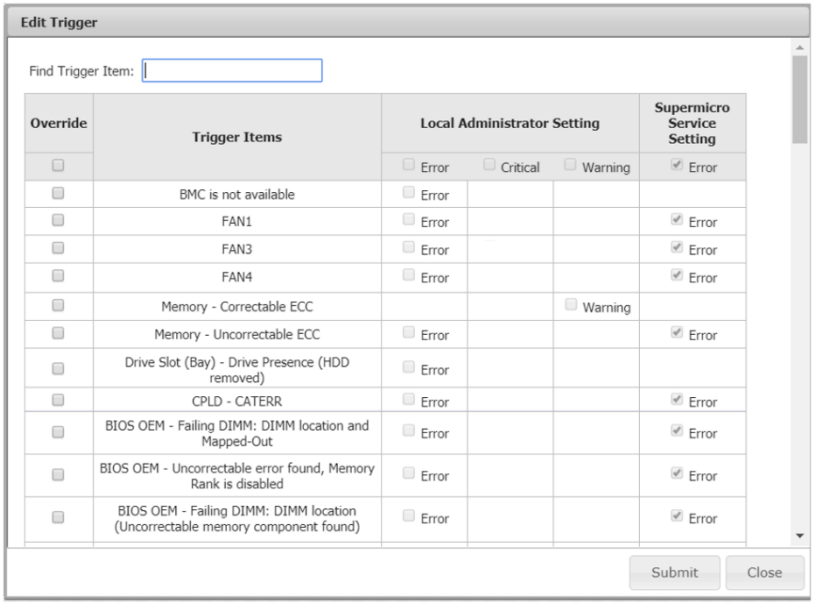


Figure 12-42

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.

12.1.5.5 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/Redfish 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:

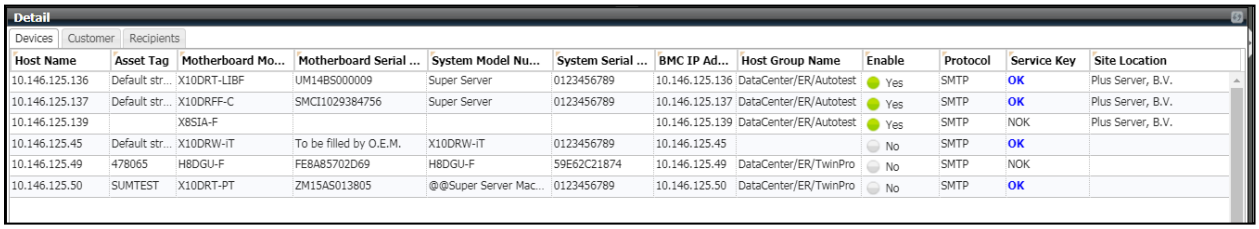


Figure 12-43

1. Select one or more devices to be enabled in the working area. You can enable multiple devices simultaneously.

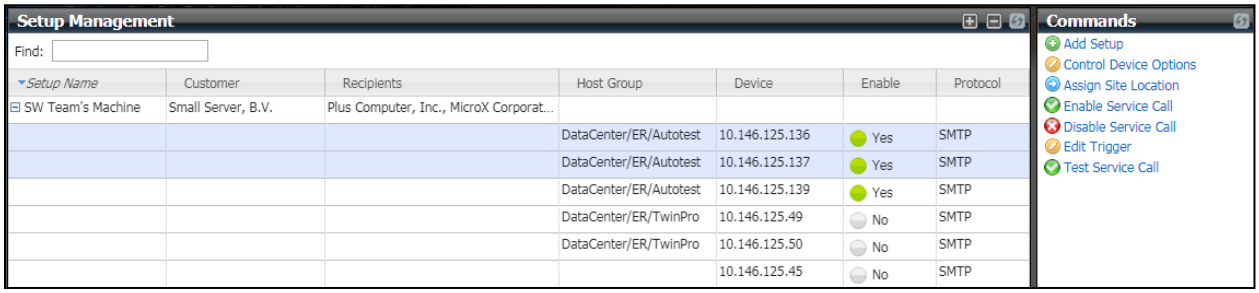


Figure 12-44

2. Click **Enable Service Call** in the command area and an Enable Service Call dialog box appears.

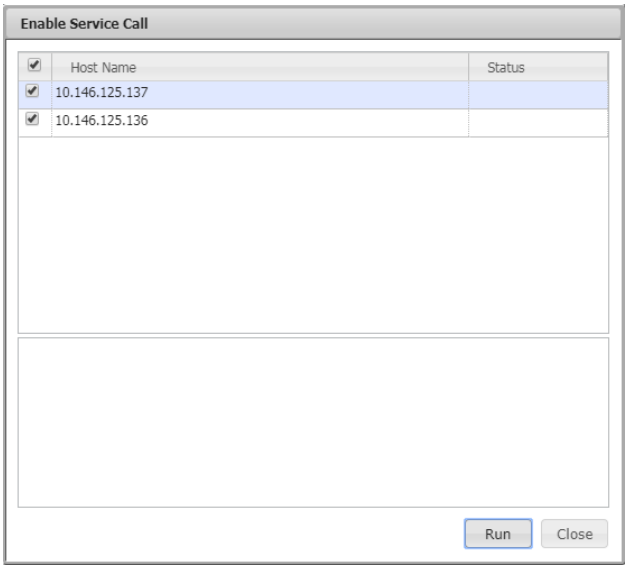


Figure 12-45

Note: Since the IPMI SEL Health[14] service is used to check the health status of a device, if the service is unavailable, the IPMI host will fail to be enabled. Similar to IPMI, Redfish SEL Health service should be available for enabling service call for a Redfish host.

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

[14] Currently, only hardware failure sensors support Service Calls. When a non-hardware sensor item in IPMI SEL Health becomes critical, no alert will be sent.

12.1.5.6 Disabling a Service Call

1. Select one or more devices to be disabled in the working area. You can disable multiple devices simultaneously.

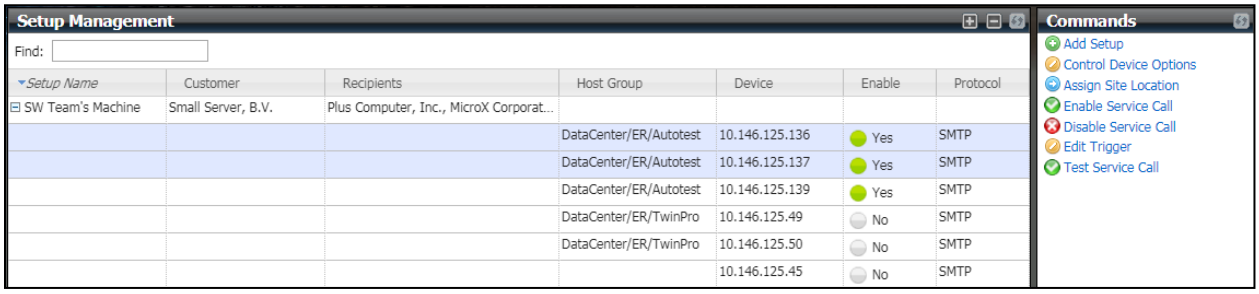


Figure 12-46

2. Click **Disable Service Call** in the command area and a Disable Service Call dialog box appears.

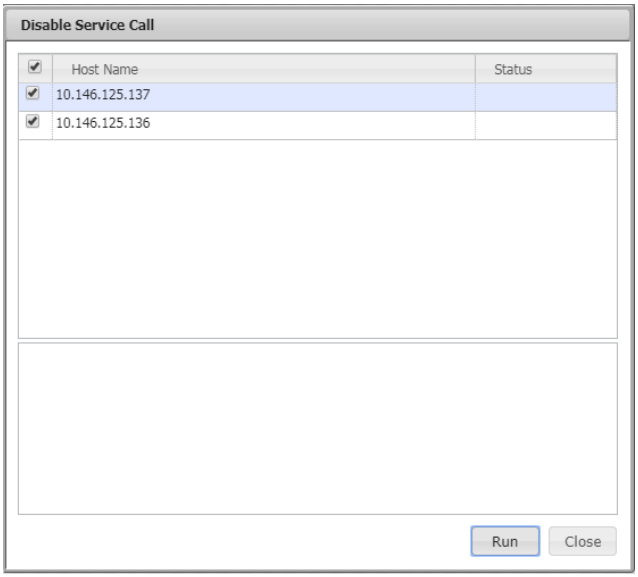


Figure 12-47

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

12.1.5.7 Testing Service Call

1. Select one or more devices to be tested in the working area. You can test multiple devices simultaneously.

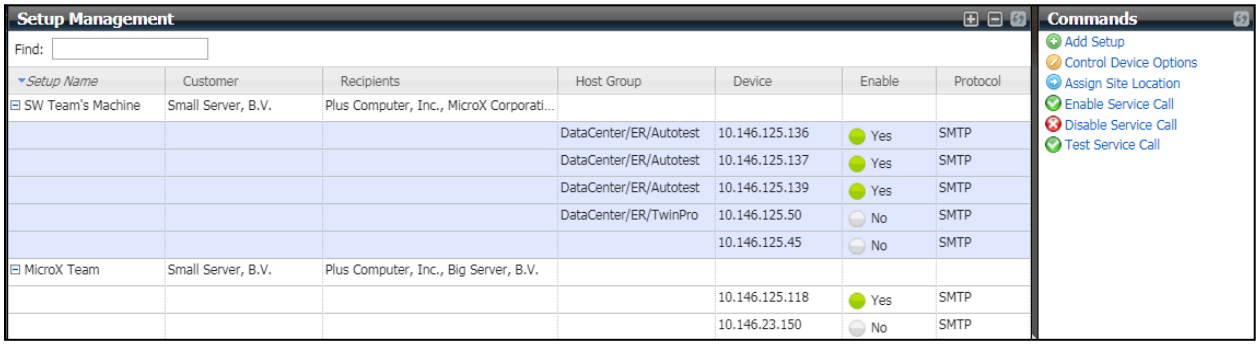


Figure 12-48

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 email address.	You should review the email addresses of the contacts in recipient(s) field since Service Call alerts are delivered via email. See *12.1.3.2 Editing a Recipient, 12.1.2.4 Assigning a Contact, and 6.4 Contact Management* 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 *12.1.5.4 Editing Trigger*.
Local Administrator triggers should have their recipients.	Service Call alerts are delivered to Local Administrator recipients by their designations.
The service used to check the health status of the device should be available.	If IPMI/Redfish SEL Health service used to check the health status of a device is not available, you should use the Add Service Wizard to add services. See *6.2.3 Add* Service Wizard.
Attributes for device data cannot be left blank.	To identify the problematic devices, it's required to provide the necessary device data. See *12.1.5.1 Editing a Device*.
The device is enabled.	To enable Service Call, see *12.1.5.5 Enabling a Service Call* for details.

2. Click **Test Service Call** in the command area and a Test Service Call dialog box appears.

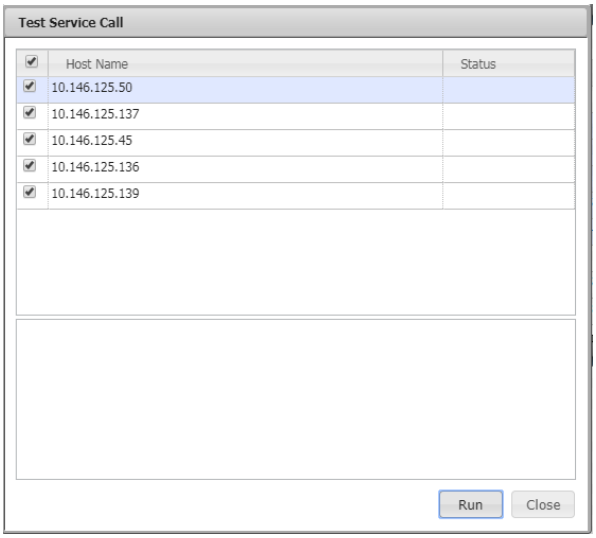


Figure 12-49

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.

12.2 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 and later generations is equipped with a dedicated network interface and a BMC with the **SFT-DCMS-SVC-KEY** product key activated.
- The IPMI/Redfish host defined in a setup is enabled. See *12.1.5.5 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/Redfish SEL Health[15] service goes into a **HARD** problem 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/Redfish service goes into a **HARD** state.
- Recovery items are triggered in the current HARD state.

[15] Currently, only hardware failure sensor items support Service Calls. When a non-hardware sensor item in IPMI/Redfish SEL Health becomes critical, no alert will be sent.

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 your SSM has been upgraded from an older version, you can enable the passive check attribute of the IPMI/Redfish SEL Health service. Once the passive check function is enabled in the service, the check result will be decided by the SNMPv1 trap or any Redfish events the SSM Server receives. By receiving a trap or an event sent by BMC, SSM can show the latest real-time health status of the managed host.

- If active check is still preferred, you can change the check interval attributes of the host and its IPMI/Redfish SEL Health service to shorten/extend the frequency of checking the monitored items when necessary.

- Each sensor item is tracked in a Service Call so that an alert could contain both problem and recovery messages. For example, the subject line of an email 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.

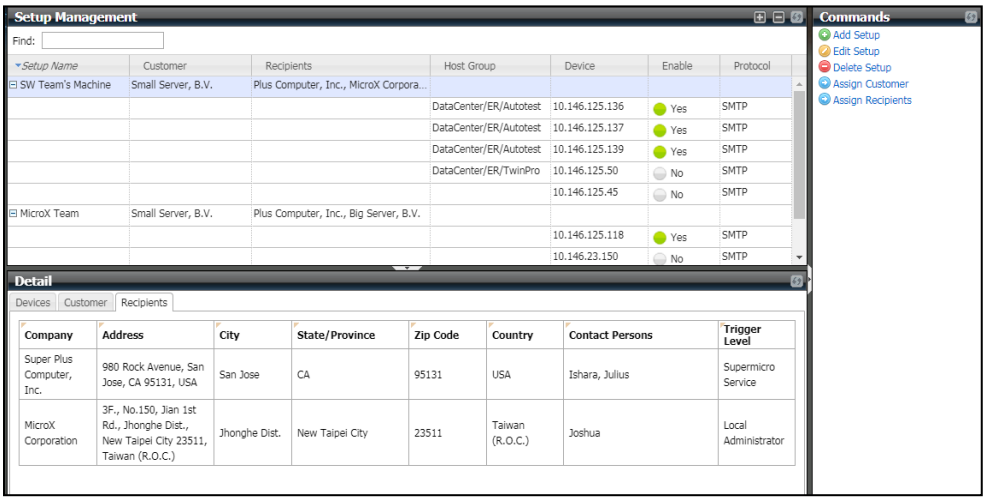


Figure 12-50

12.2.3 Alert Format

The message format in email is defined by the following attributes:

- Email 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

- Email 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 [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.

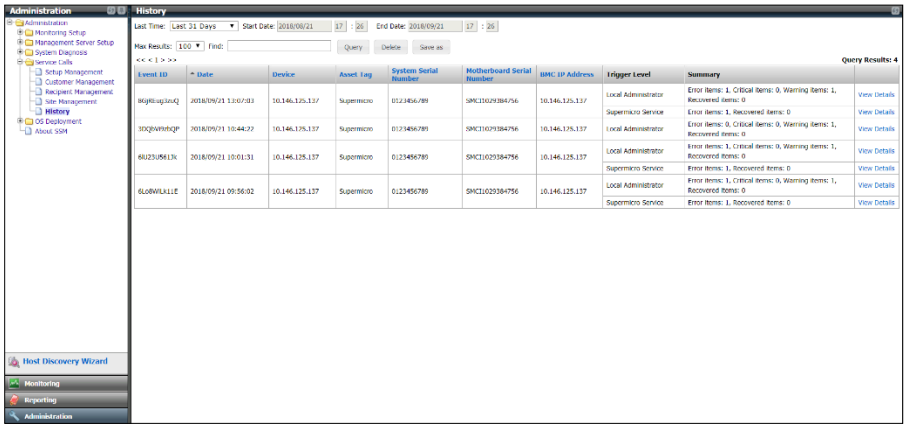


Figure 12-51

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 5 tabs: **Problematic Items**, **Recovered Items, Setup Configuration**, **Device Info** and **Trigger Setting**.

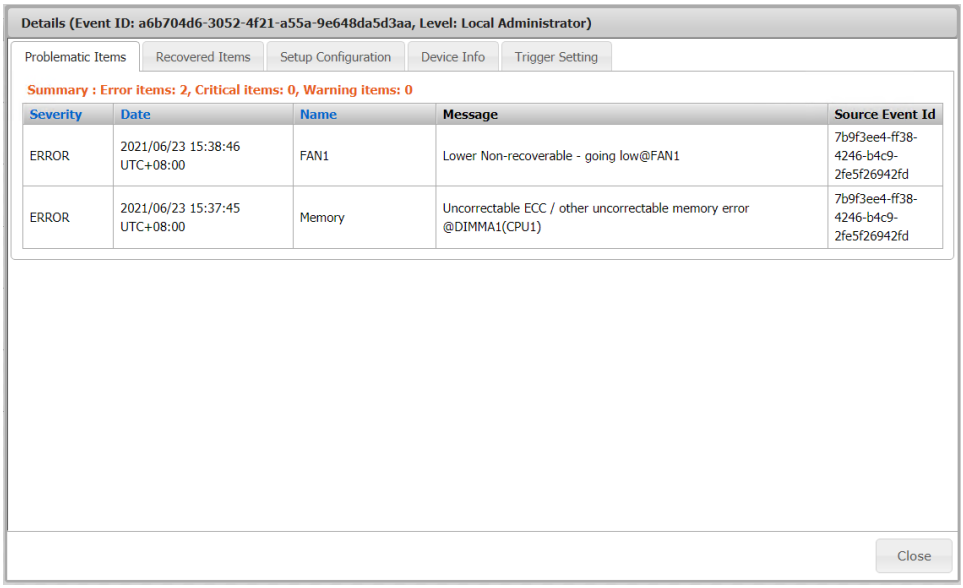
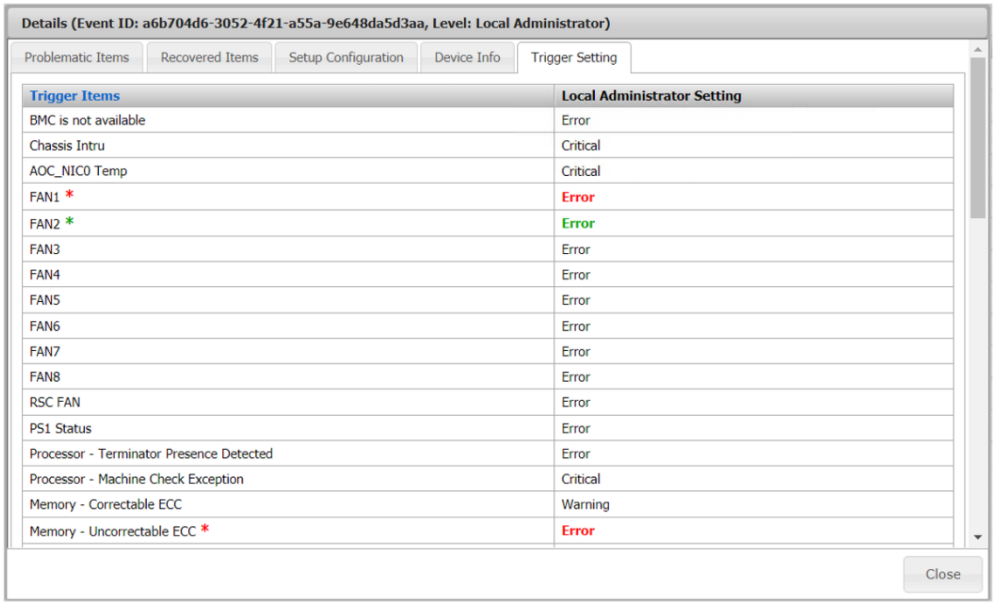


Figure 12-52

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.
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 *12.1.5.1 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.



Trigger Items	Local Administrator Setting
BMC is not available	Error
Chassis Intru	Critical
AOC_NIC0 Temp	Critical
FAN1 *	Error
FAN2 *	Error
FAN3	Error
FAN4	Error
FAN5	Error
FAN6	Error
FAN7	Error
FAN8	Error
RSC FAN	Error
PS1 Status	Error
Processor - Terminator Presence Detected	Error
Processor - Machine Check Exception	Critical
Memory - Correctable ECC	Warning
Memory - Uncorrectable ECC *	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 CSV file.

	A	B	C	D	E	F	G	H	I
1	Event ID	Date	Device	Asset Tag	System Model Number	System Serial Number	Motherboard Model Number	Motherboard Serial Number	BMC IP Address
2	29a601b4-	2020/10/05 15:07:58 UTC+08:00	10.146.125.136	1FDSFKQE	X10DRT-LIBF	S180103X5111610	X10DRT-LIBF	UM14BS000009	10.146.125.136
3	aae4ae99-	2020/10/05 14:58:54 UTC+08:00	win-7dks8c2cp8r	2FSDFQWER	X12SCZ	S192210X2213733	X12SCZ	AD42AS5787H6	10.146.40.87
4	477b9447-	2020/10/05 14:38:01 UTC+08:00	10.146.125.136	1FDSFKQE	X10DRT-LIBF	S180103X5111610	X10DRT-LIBF	UM14BS000009	10.146.125.136

Figure 12-54

In chronological order by default, each row indicates an event including the Setup data (Customer and Recipients), Device Info (Device Data and Site Location) and Trigger Setting.

Q	R	S	T	U	V
Setup	Customer	Recipients	Site Location	Local Administrator.Trigger Setting	Supermicro Service.Trigger Setting
SW Team's Machine	Small Server, B.V.	MicroY Corporation	Plus Server, B.V.	BMC is not available: Error Processor - Thermal Trip: Error Processor - FRB1/BIST failure:	FAN1: Error PS Status: Error NVMe - Drive Fault: Error
MicroX Team	Super Plus Computer, Inc.	Big Server, B.V.	Super Computer, Inc.	BMC is not available: Error Chassis Intru: Critical 12V: Error, Critical, Warning	FANA: Error FANB: Error CPLD - CATERR: Error

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.
- 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.

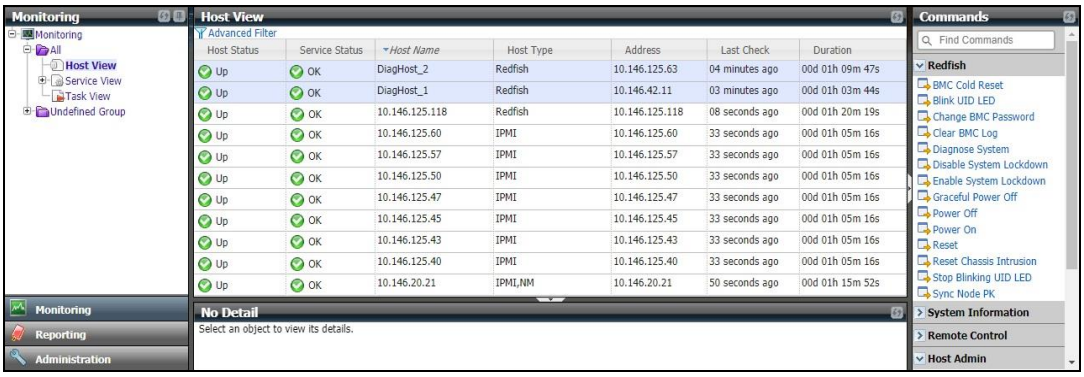


Figure 13-1

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.

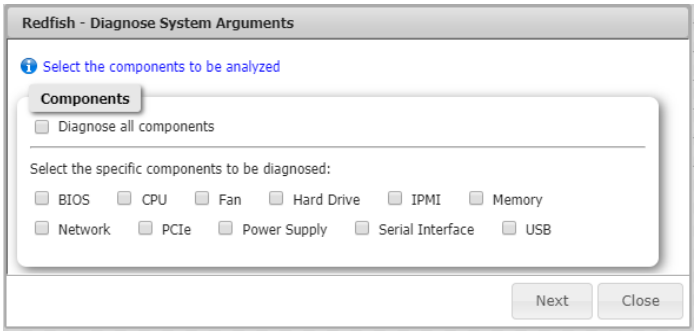


Figure 13-2

3. Click the **Run** button to start the diagnostic process.

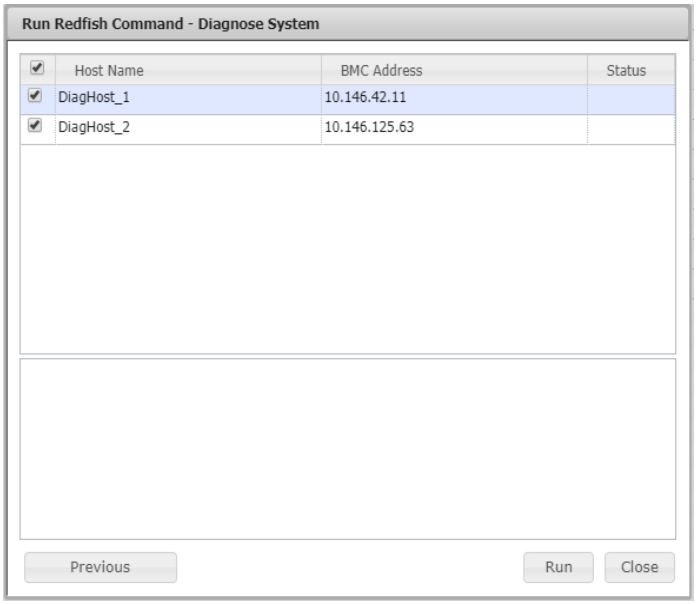


Figure 13-3

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.

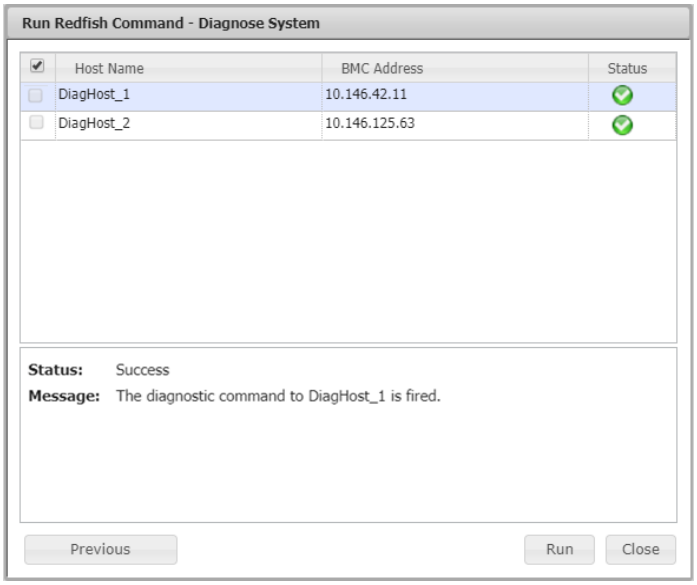


Figure 13-4

5. 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.

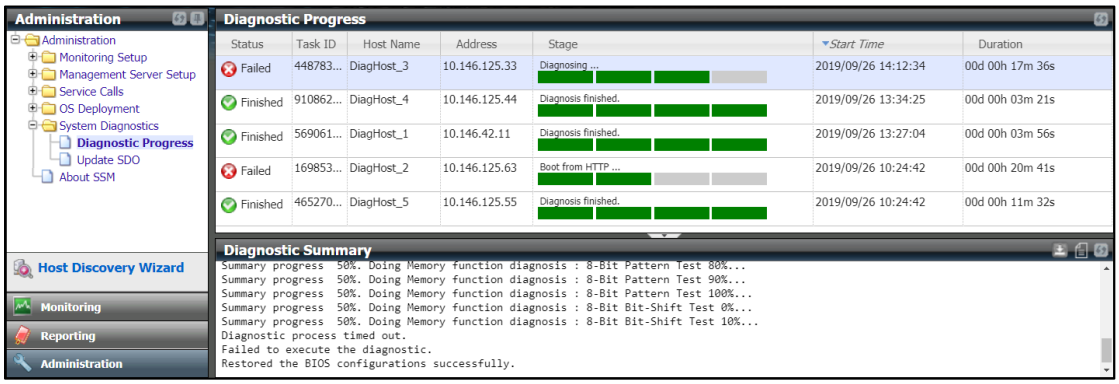


Figure 13-5

6. If the diagnostics fail, view the **Diagnostic Summary** pane below to get the detailed messages.

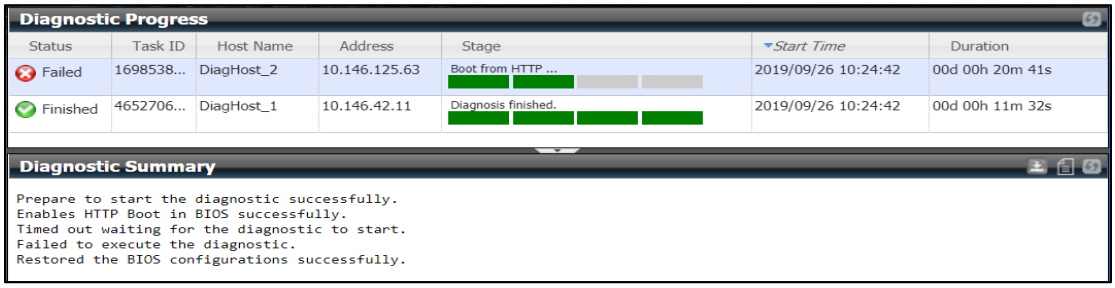


Figure 13-6

7. If the diagnostics finish successfully, click the **View Report** icon in the top right corner of Diagnosis Summary toolbar to view the diagnostic report.

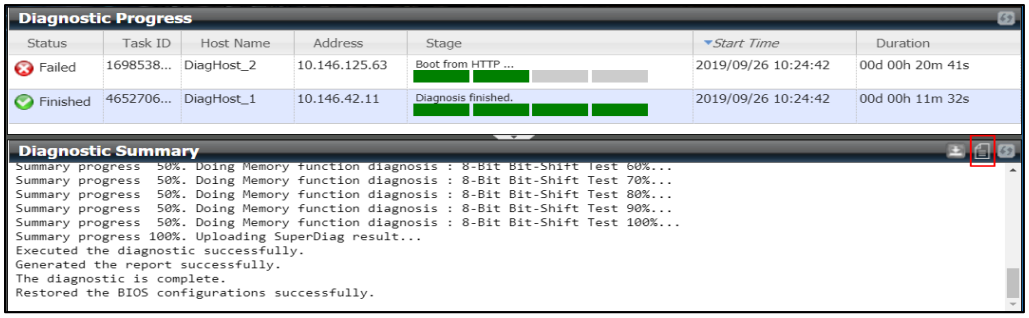


Figure 13-7

8. The diagnostic report is summarized and shown in graphic display in Hypertext (.html) for easier access.

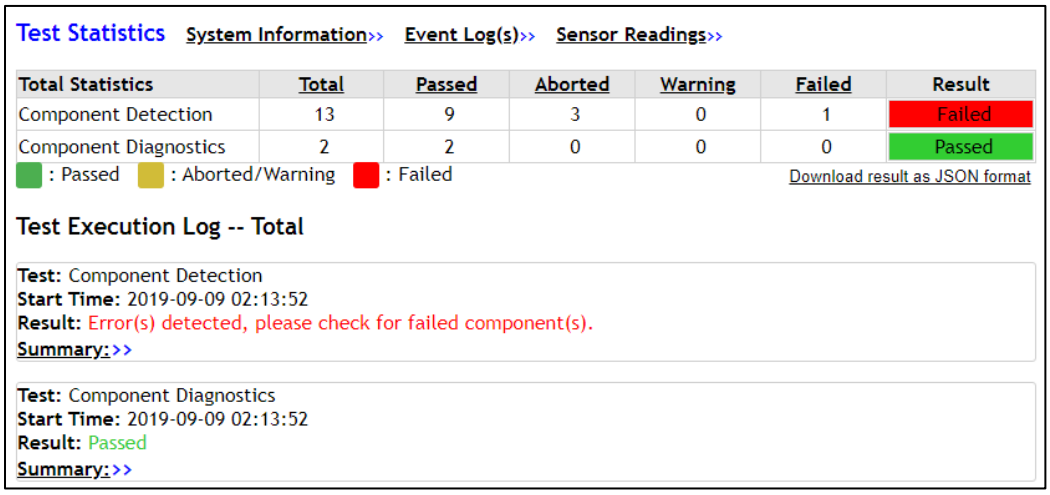


Figure 13-8

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 30 diagnostic tasks to run simultaneously. When that threshold is reached, the rest of the diagnostic tasks will be queued.

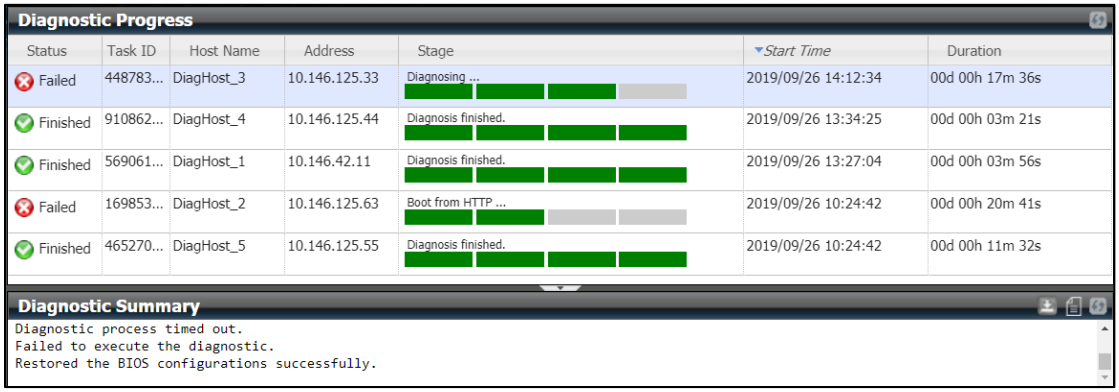


Figure 13-9

- **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.

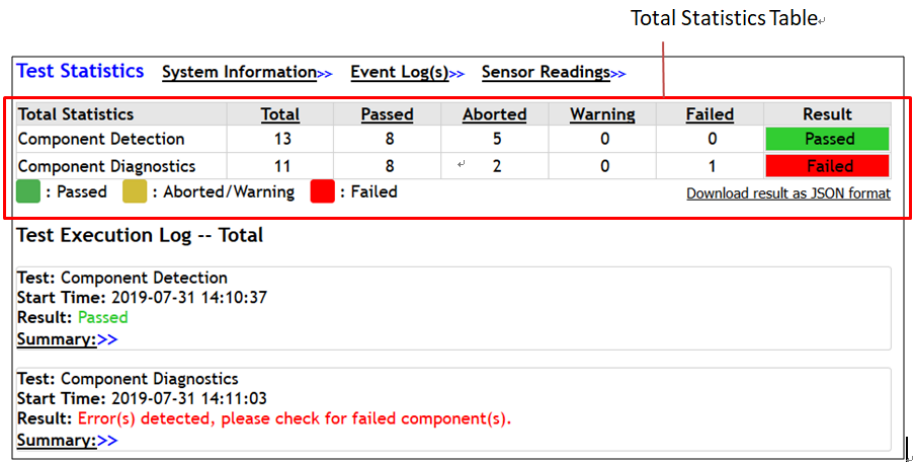


Figure 13-10

Here we use the Total results as an example to illustrate the process. To access the Total results, click the column title **Total**.

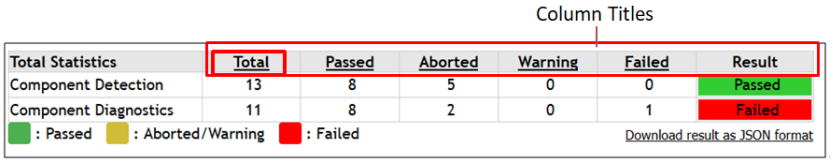


Figure 13-11

The summary of the selected type of test result then appears. To view a summary of each log record, click **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.

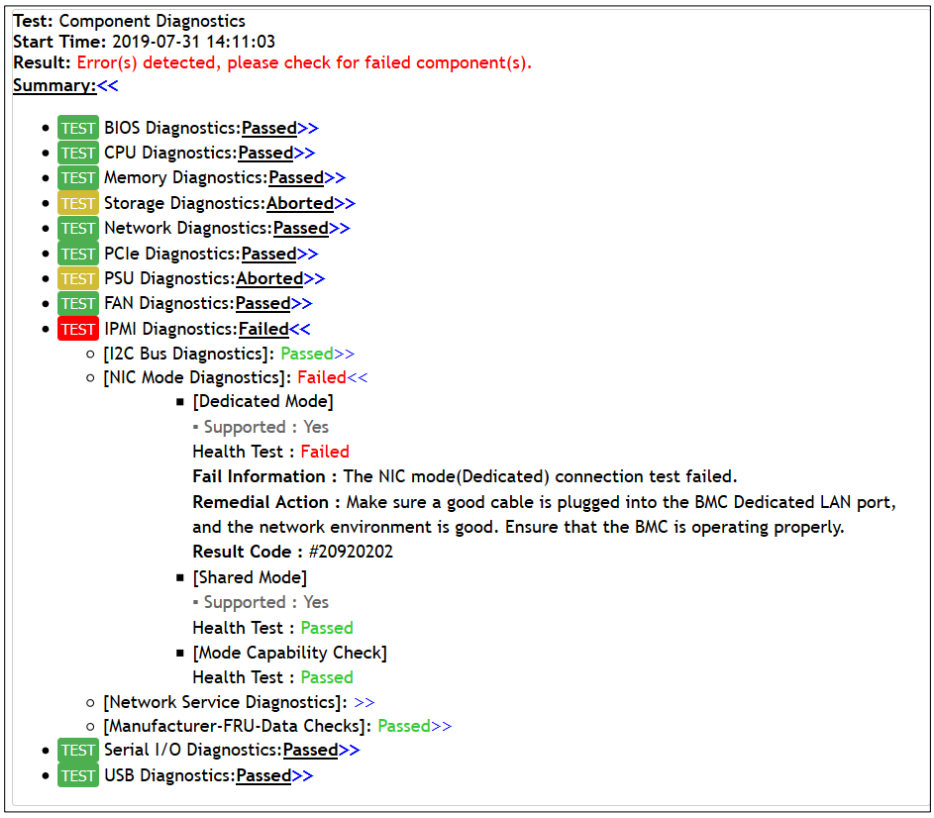


Figure 13-13

13.3.1.2 System Information

A list of system components can be viewed in the diagnostic report. Click **System Information** beside Test Statistics.

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 13-14

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

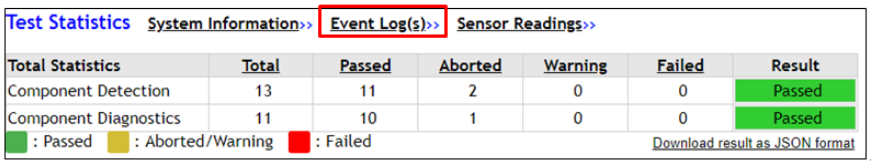
SMBIOS Information	
System	
Manufacturer	Supermicro
Product Name	Super Server
Board	
Manufacturer	Supermicro
Product Name	X11DPU
Version	1.10
Serial Number	OM173S033970

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)**.



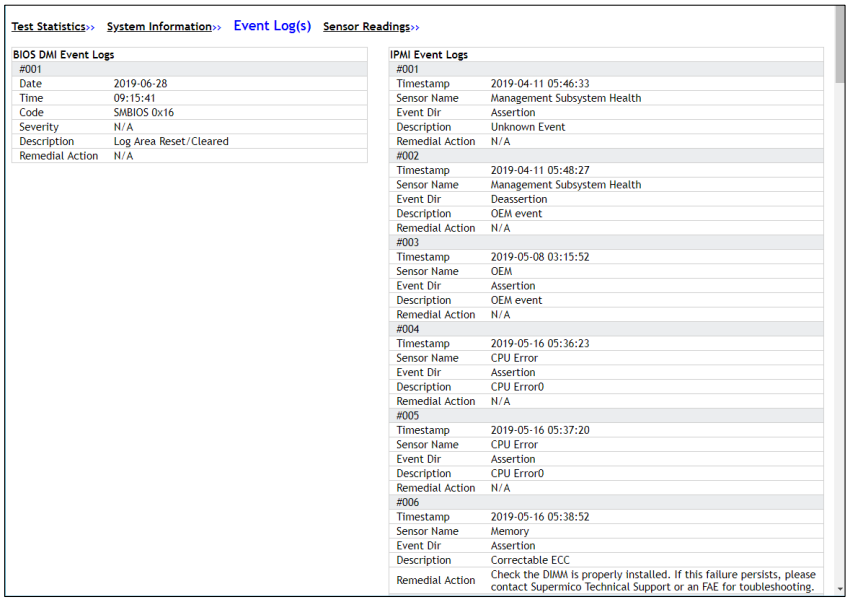
Test Statistics System Information›› Event Log(s)›› Sensor Readings››

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.



Test Statistics›› System Information›› Event Log(s) Sensor Readings››

BIOS DMI Event Logs

#001	
Date	2019-06-28
Time	09:15:41
Code	SMBIOS 0x16
Severity	N/A
Description	Log Area Reset/Cleared
Remedial Action	N/A

IPMI Event Logs

#001	
Timestamp	2019-04-11 05:46:33
Sensor Name	Management Subsystem Health
Event Dir	Assertion
Description	Unknown Event
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 toubleshooting.

Figure 13-17

13.3.1.4Sensor 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

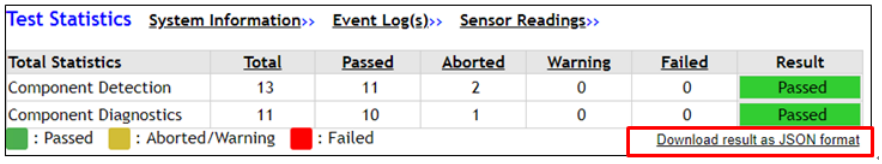
IPMI Sensor Reasings

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.



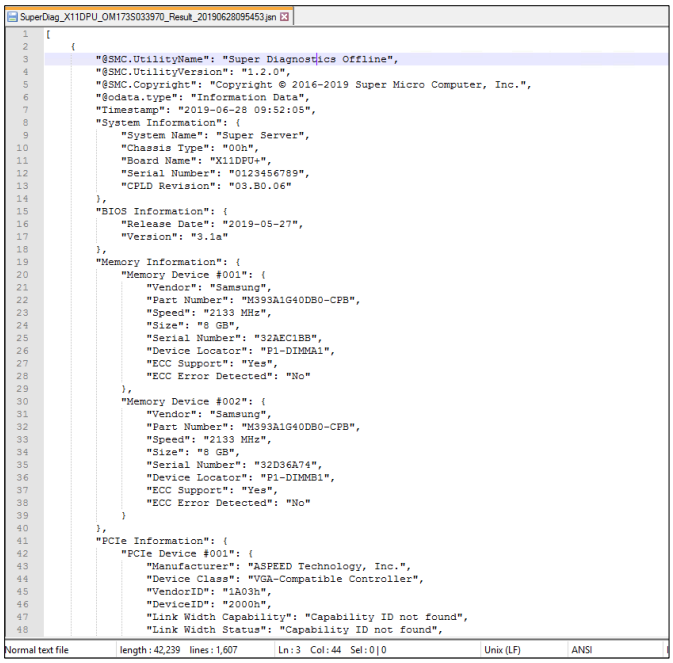
Test Statistics System Information>> Event Log(s)>> Sensor Readings>>

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.



SuperDiag_X11DPU_OM173S033970_Result_20190628095453.jsn


```
[
    {
        "@SMC.UtilityName": "Super Diagnostics Offline",
        "@SMC.UtilityVersion": "1.2.0",
        "@SMC.Copyright": "Copyright © 2016-2019 Super Micro Computer, Inc.",
        "@odata.type": "Information Data",
        "Timestamp": "2019-06-28 09:52:05",
        "System Information": {
            "System Name": "Super Server",
            "Chassis Type": "00h",
            "Board Name": "X11DPU+",
            "Serial Number": "0123456789",
            "CPLD Revision": "03.B0.06"
        },
        "BIOS Information": {
            "Release Date": "2019-05-27",
            "Version": "3.1a"
        },
        "Memory Information": {
            "Memory Device #001": {
                "Vendor": "Samsung",
                "Part Number": "M393A1G40DB0-CPB",
                "Speed": "2133 MHz",
                "Size": "8 GB",
                "Serial Number": "32AEC1BB",
                "Device Locator": "P1-DIMMA1",
                "ECC Support": "Yes",
                "ECC Error Detected": "No"
            },
            "Memory Device #002": {
                "Vendor": "Samsung",
                "Part Number": "M393A1G40DB0-CPB",
                "Speed": "2133 MHz",
                "Size": "8 GB",
                "Serial Number": "32D36A74",
                "Device Locator": "P1-DIMMB1",
                "ECC Support": "Yes",
                "ECC Error Detected": "No"
            }
        },
        "PCIe Information": {
            "PCIe Device #001": {
                "Manufacturer": "ASPEED Technology, Inc.",
                "Device Class": "VGA-Compatible Controller",
                "VendorID": "1A03h",
                "DeviceID": "2000h",
                "Link Width Capability": "Capability ID not found",
                "Link Width Status": "Capability ID not found",
```


Normal text file | length : 42,239 lines : 1,607 | Ln : 3 Col : 44 Sel : 0 | 0 | Unix (LF) | ANSI

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**.

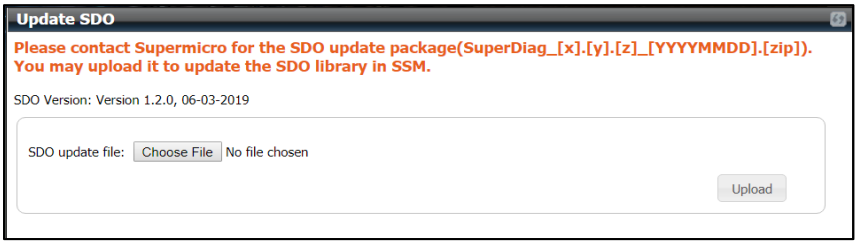


Figure 13-22

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.

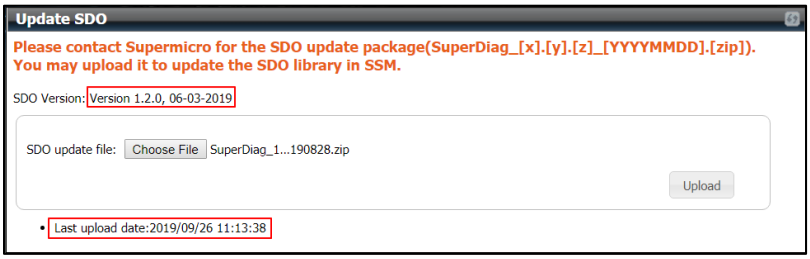


Figure 13-23

14 Memory PFA

The **Memory Predictive Failure Analysis (Memory PFA)** function allows you to predict if any DIMM slots on managed Redfish hosts might fail in the future. SSM starts to collect and store the memory events from BMC as performance data when the Memory PFA service is added on managed hosts. SSM will analyze the data to indicate any potential failure. Once a possible imminent memory failure is detected, it's highly recommended that you execute the Perform Memory Self-Healing web command to scan and repair the potentially bad memory module.

14.1 Prerequisites

To use the Memory PFA function in SSM, make sure your systems meet these requirements:

- Only available on Supermicro X13 series with 4th Gen Intel® Xeon® Processor Scalable Family-based Platform.
- Must have the newest versions of both BIOS and BMC firmware on the managed hosts.
- At least 2 TB of free disk space must be saved for a large number of hosts.

14.2 Collecting Performance Data

SSM collects and stores the metrics of performance data from each DIMM via BMC, including DIMM temperature, ECC events, and the execution results of Post Package Repair (PPR). SSM also stores the lifetime metric for each DIMM for Memory PFA. For details on performance data, see *7.3.8.7 Performance Data Command*. For Data Retention Time, refer to *6.11 DB Maintenance*.

14.2.1 DIMM Temperature Metric

When a memory module is used in a high temperature environment for a long time, memory errors or damage are likely to occur. SSM collects the metrics in order to analyze the temperature abnormalities and offers suggestions.

Note: A DIMM cannot exceed 60 degrees Celsius for more than one day.

14.2.2 DIMM ECC Event Metric

The DIMM Error Correcting Code (ECC) metric is the main indicator determining the health of memory and predicting failures. The DIMM ECC event metrics that SSM collects include Correctable ECC (CECC) events and Uncorrectable ECC (UECC) events.

Note: Only four CECC events per four GB in one day can be allowed. No UECC events are allowed at all.

14.2.3 DIMM PPR Status Metric

When you execute the Perform Memory Self-Healing web command on the selected Redfish host on SSM Web, Post Package Repair (PPR) is automatically executed on any DIMM slots found with errors. The execution results will be stored.

14.2.4 DIMM Lifetime Metric

DIMM lifetime might affect the performance of memory. SSM stores the lifetime for each DIMM when the system is managed by SSM with the first service check of Redfish System Information. The part number and serial number are also stored to identify an individual DIMM slot.

Note: DIMMs more than three years old will be shown onscreen as additional information for the Memory PFA Service.

14.3 Memory PFA Service

To use this function, your managed hosts must meet the requirements listed in *14.1 Prerequisites*. When you use the Add Service Wizard to add a Memory PFA service, the SSM Web will enable the **Memory PFA Support** feature on the managed systems. If a managed system supports Memory PFA, SSM will start to collect the metric data and determine the state of Memory PFA service. Onscreen messages suggest how you could reduce occurrences of memory failures.

14.3.1 Adding a Service

Note that only one Memory PFA service can be added to a Redfish host. Please refer to *6.2.3.4 Add Redfish Services* for more information.

14.3.2 Service Status

The prediction results include three types of status.

- **OK**: All DIMMs on the managed system are well or possible DIMM failures do not yet meet the criteria.
- **Warning**: When one DIMM experiences one of these situations: (1) the CECC or UECC event criteria is reached without a failed PPR attempt (either there is no PPR or there is a successful PPR attempt), (2) the temperature limit is reached.

- **Critical**: The CECC or UECC event criteria for one DIMM is reached, and the last execution of PPR has failed.

When a DIMM is more than three years old and the status shows either Warning or Critical, a message appears.

14.3.3 Executing the Memory Self-Healing Command

The Memory Self-Healing command integrates with the Post Package Repair (PPR), part of Intel® Reliability, Availability, and Serviceability (RAS), for BIOS to scan memory with the Advanced Memory Test (AMT). If it detects errors, and PPR is then executed.

There are two ways to execute the Memory Self-Healing web command.

- **Method 1**

1. Click **SSM New GUI** on the top tool bar→**Monitoring** → **Host Monitoring View** to view the status of the hosts.
2. Select Hosts in the working area. You can select multiple hosts with same host type at a time.
3. Click the **Toolbar** icon in the upper right corner of the Host View, then click **Perform Memory Self-Healing** in the Redfish commands area, and a Perform Memory Self-Healing dialog box will pop up.

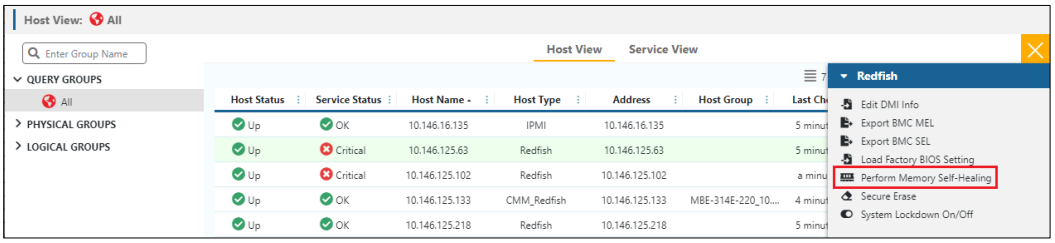


Figure 14-1

4. Click the **Run** button to execute the command.
5. Click the **Submit** button to accept the prompt so that a system reboot will be forced for the action to take effect on the target system.
6. Click the **Task ID** link to go the Task View for execution results.

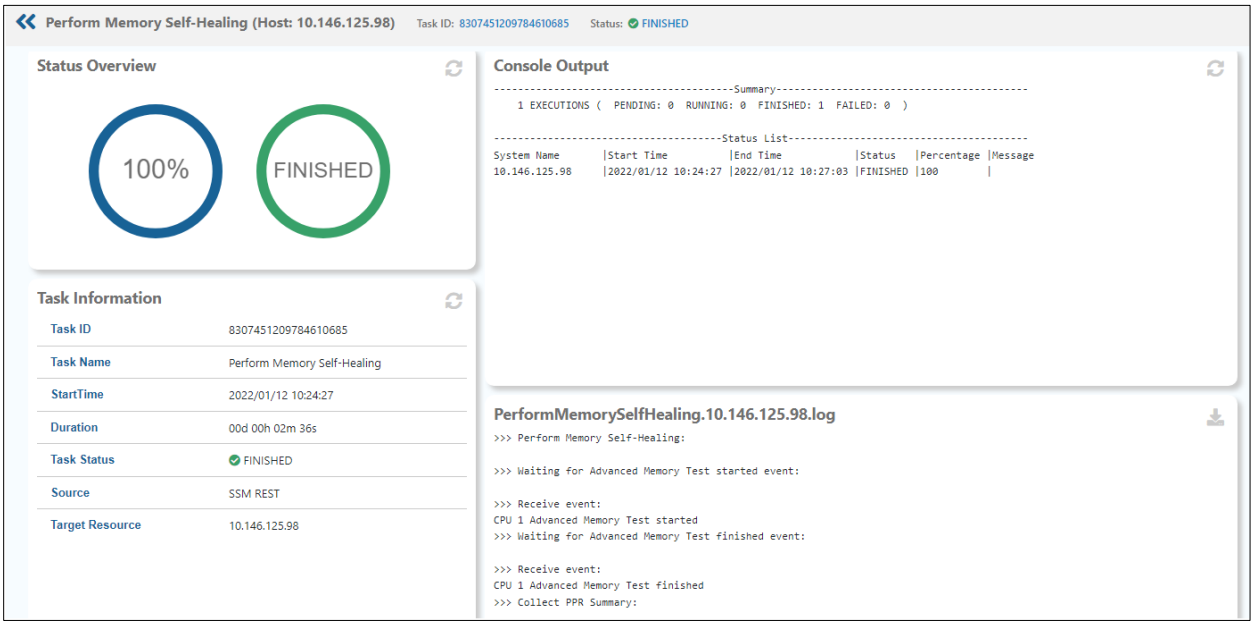


Figure 14-2

- **Method 2**

1. Click **SSM New GUI →Monitoring → Host Monitoring View → Service View** to view the status of services.
2. Select the **Memory PFA** service in the working area.
3. Click the **Angle-Double-Right** icon to view the details of the Memory PFA service.
4. You can also click the **Memory** icon in the upper right corner of the **Monitoring Overview** pane to execute this command.

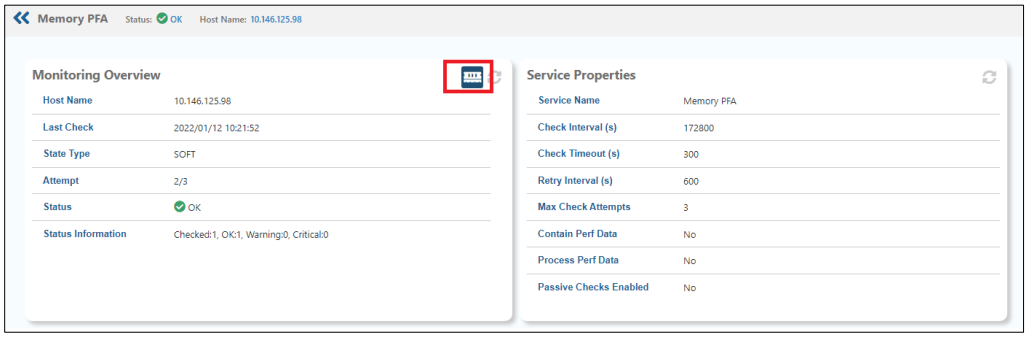


Figure 14-3

Part 4 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 Exporting and Importing 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 database[16].

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

[16] 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.

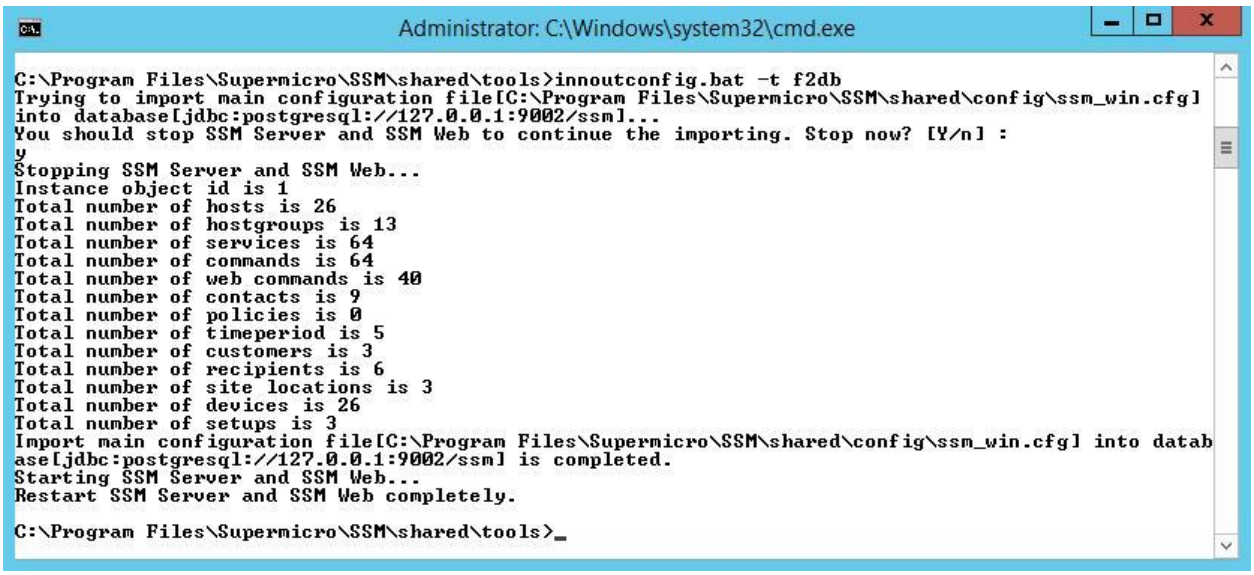


Figure 14-2

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\CallHomeData 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\CallHomeData** 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.

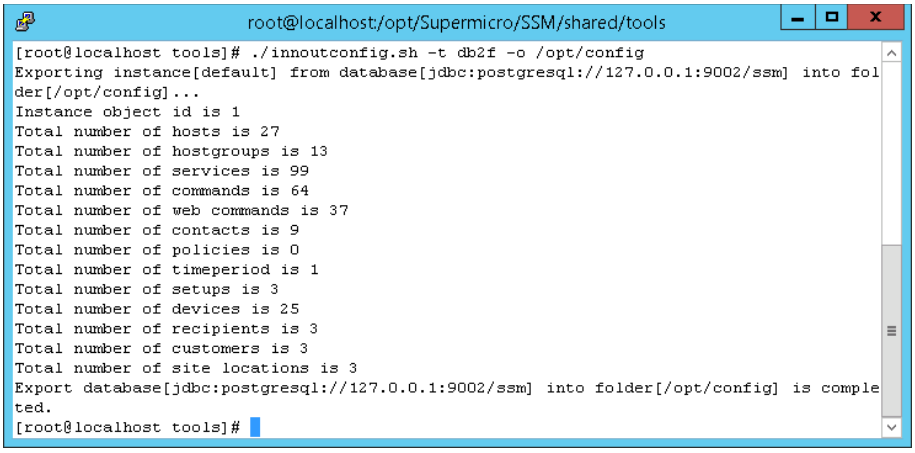


Figure 14-3

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.

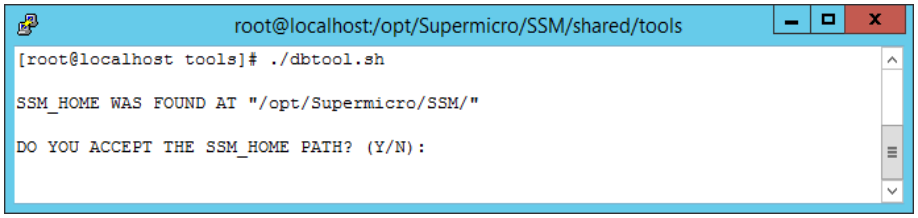


Figure 14-4

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.

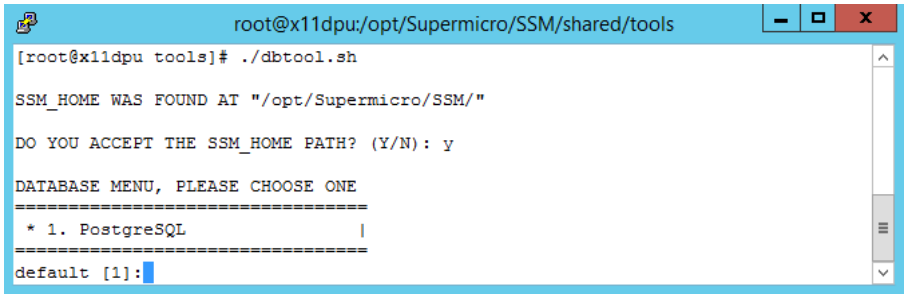


Figure 14-5

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 14-6

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 14-7

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 14-8

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 14-9

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 14-10

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 14-11

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 14-12

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 14-13

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 14-14

12. Type **Y** to save the database settings to the property files that are used by SSM Web and SSM Server.

```
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 14-15

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 14-16

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/jdk11.0.18/jre/bin/java.
-h, --help	Shows the help menu.

The following figure shows how the command **changejvm.bat -j "C:\Java\jdk-11.0.18+10-jre\bin\java.exe" -p "C:\Program Files\Supermicro\SSM"** is used to change to another version of Java VM (JRE 11.0.18+10).

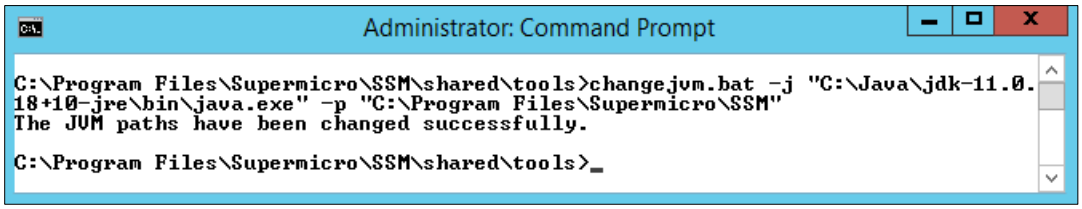


Figure 14-17

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.

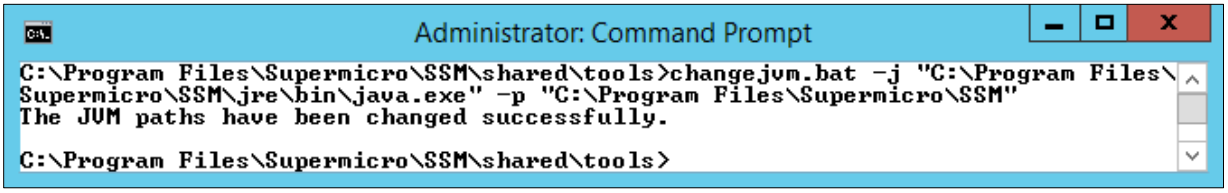


Figure 14-18

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 11 in SSM. Other Oracle JREs (i.e., JRE 8, and JRE 19+) and Non-Oracle Java VMs (i.e., OpenJDK 8, and OpenJDK 19+) are not supported in this version.

16 SSM Certification

When server-side applications (i.e., SSM Server and SSM Web) 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 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

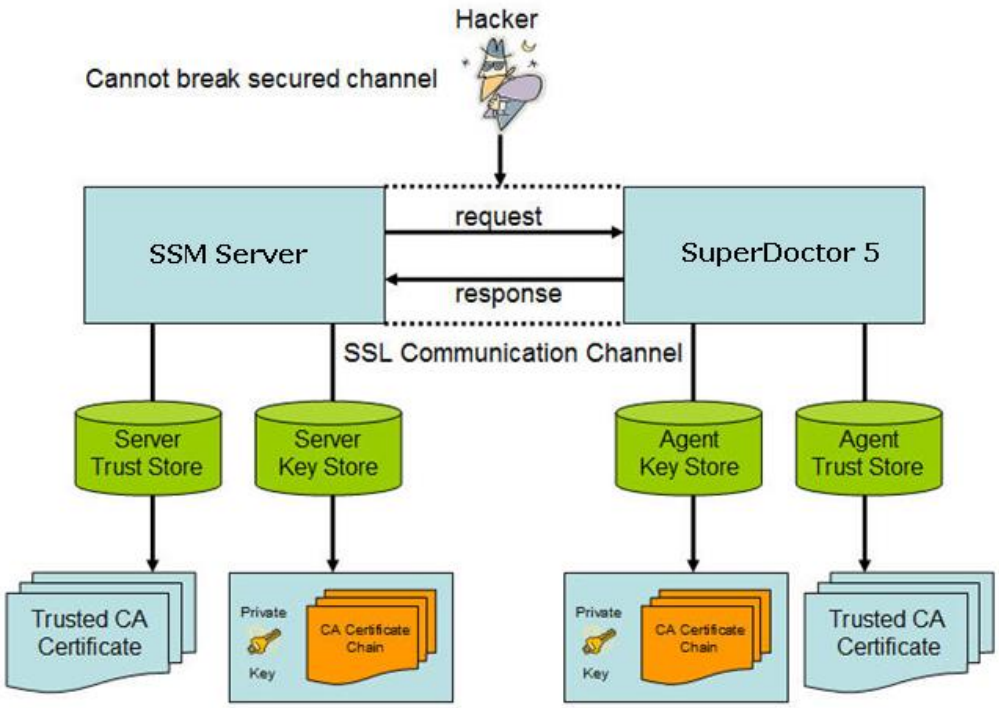


Figure 15-1

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 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.

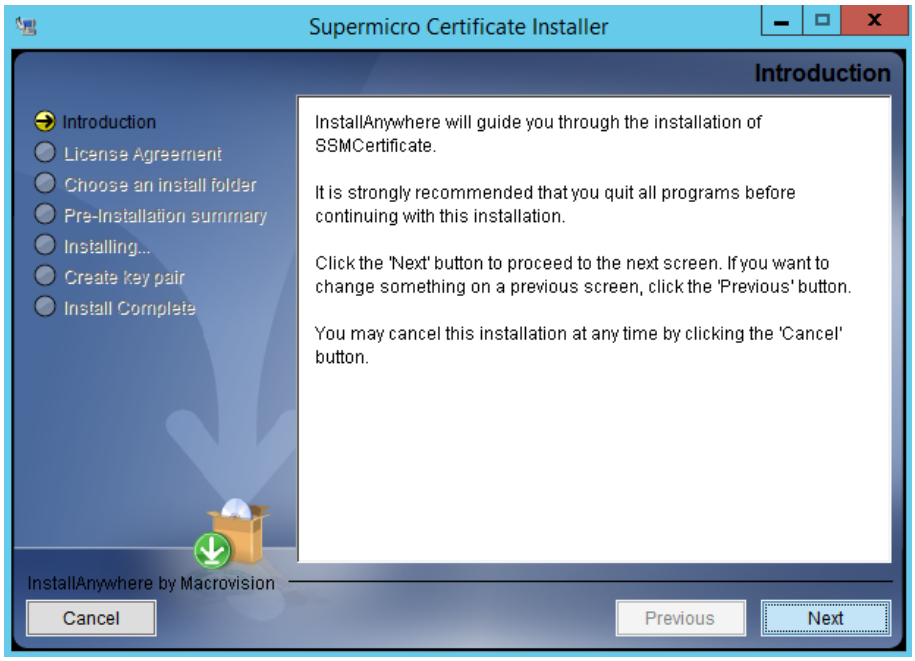


Figure 15-2

4. Accept the copyright and click the **Next** button to continue.

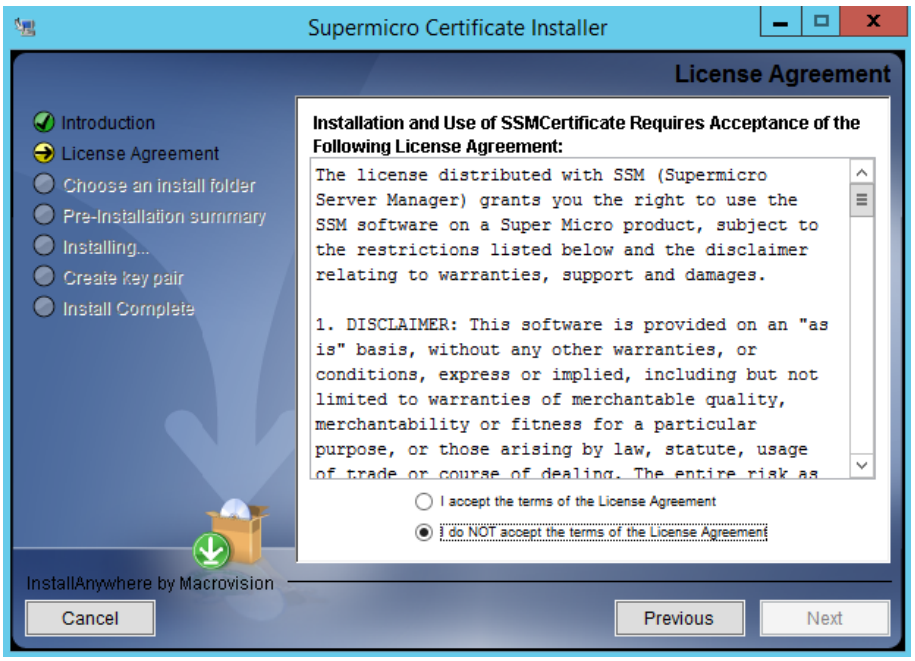


Figure 15-3

5. Choose an installation folder. The default folder is **C:\Program Files\Supermicro\SSMCertificate**.

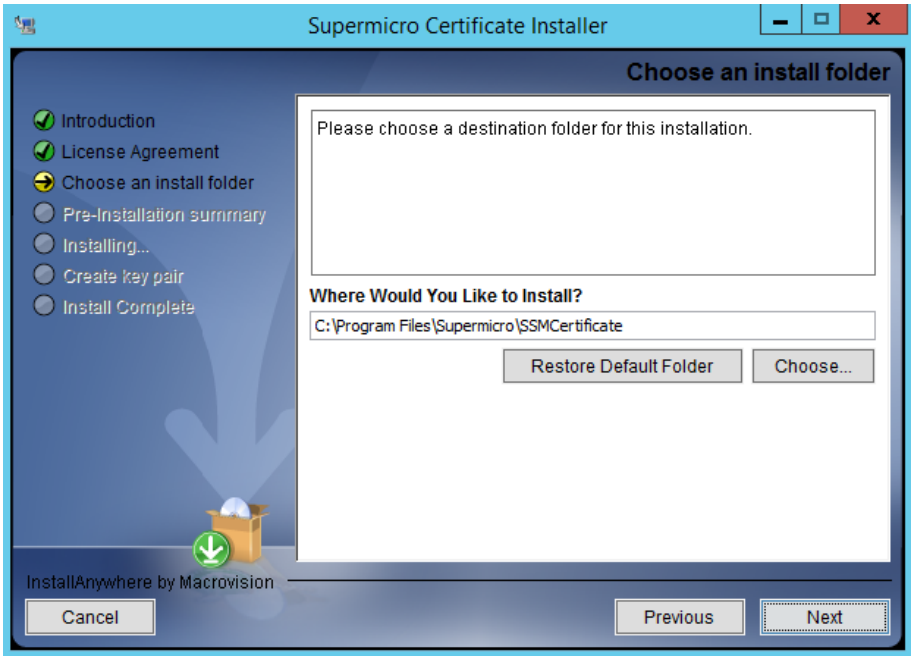


Figure 15-4

6. The figure shown below is the pre-installation summary. Click the **Install** button to install the program.

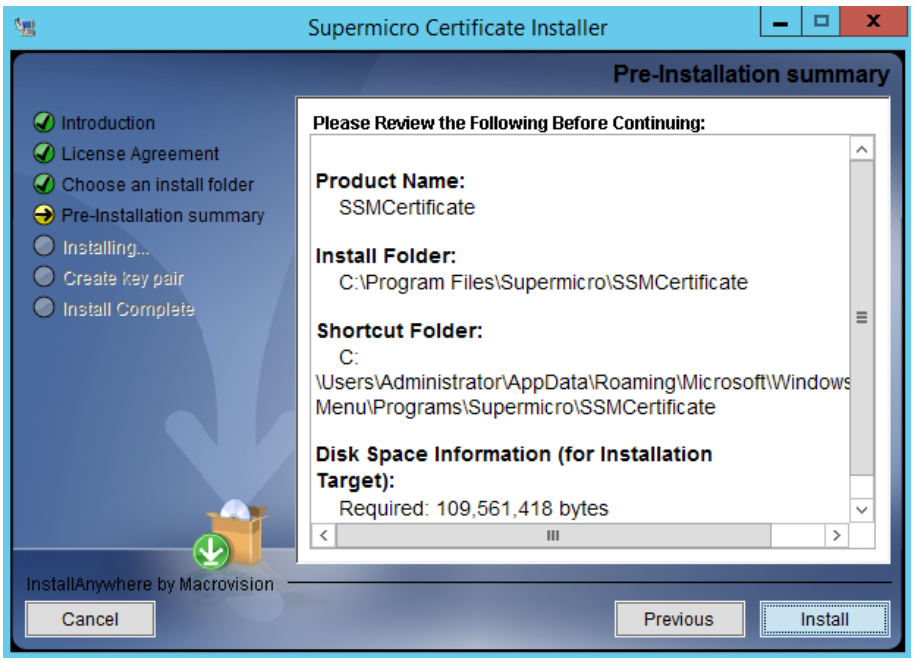


Figure 15-5

7. Please wait while the installation is in progress.

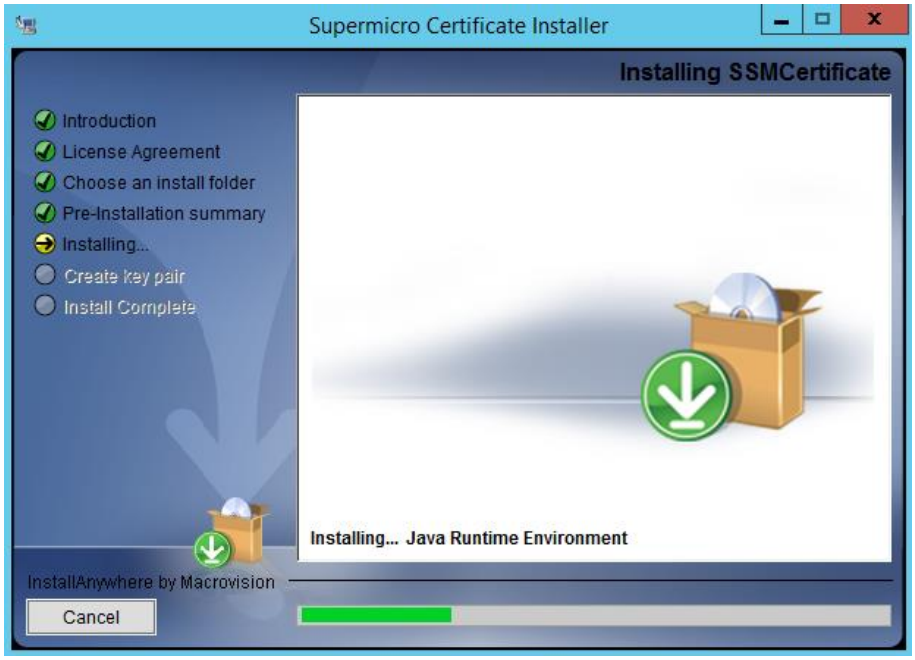


Figure 15-6

8. 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.

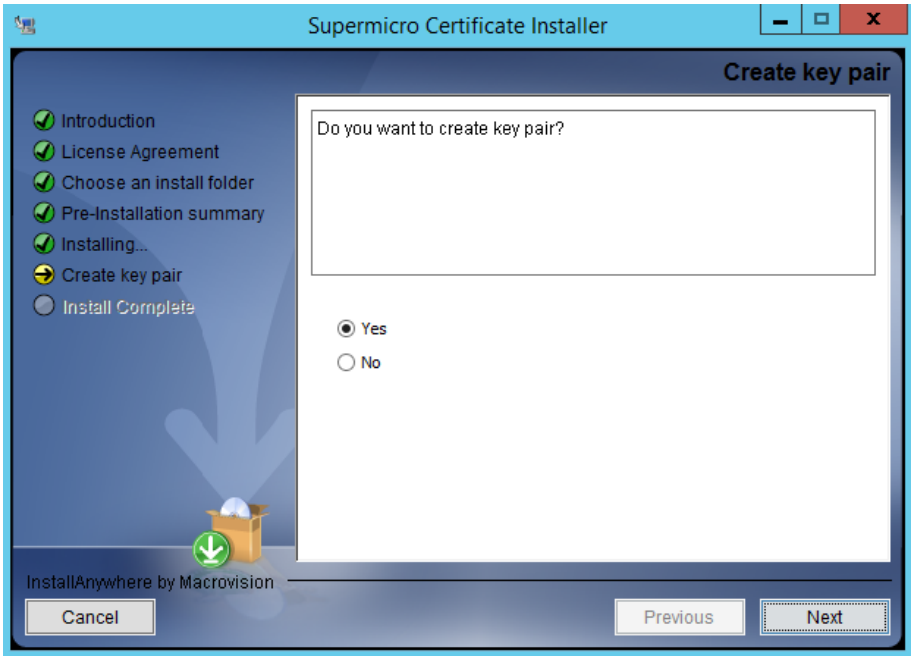


Figure 15-7

9. The installation is complete. Click the **Done** button to close the installation program.

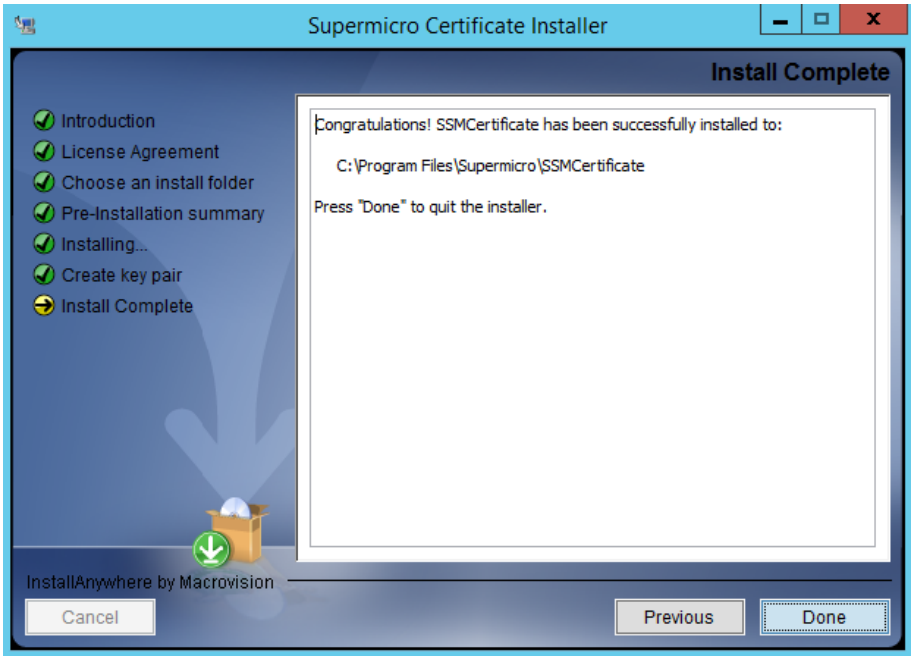


Figure 15-8

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.

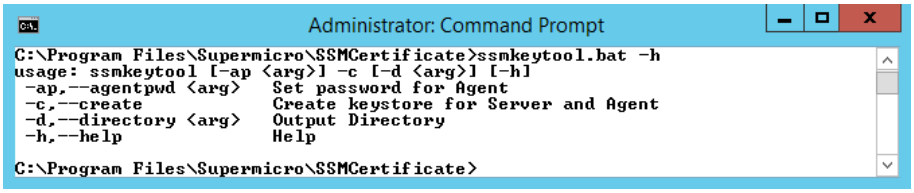


Figure 15-9

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 and SSM Web) 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.

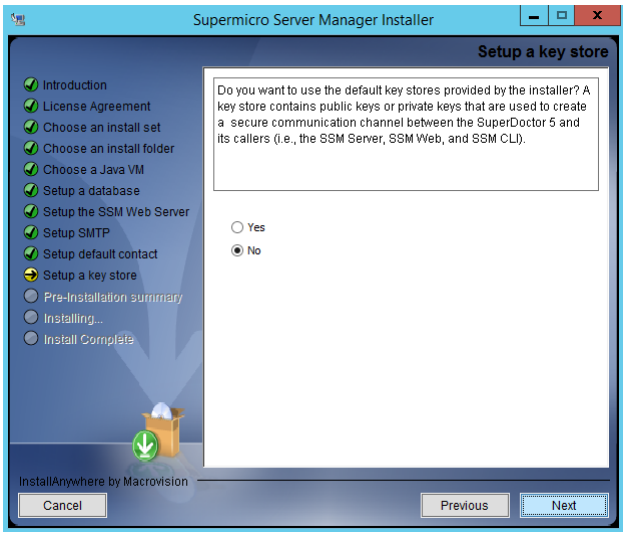


Figure 15-10

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.

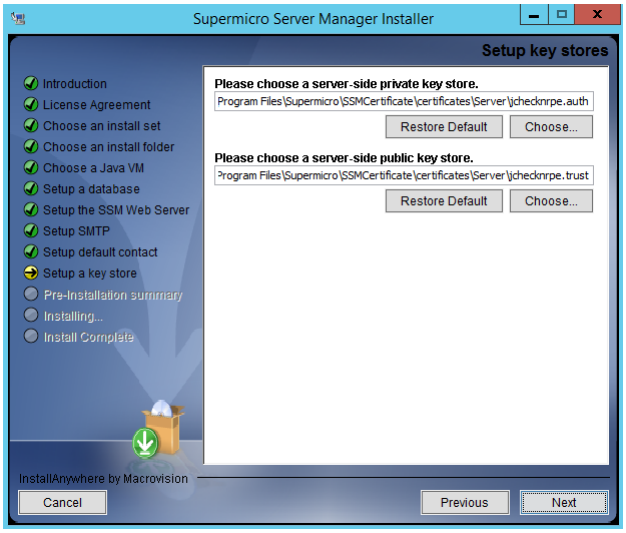


Figure 15-11

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.

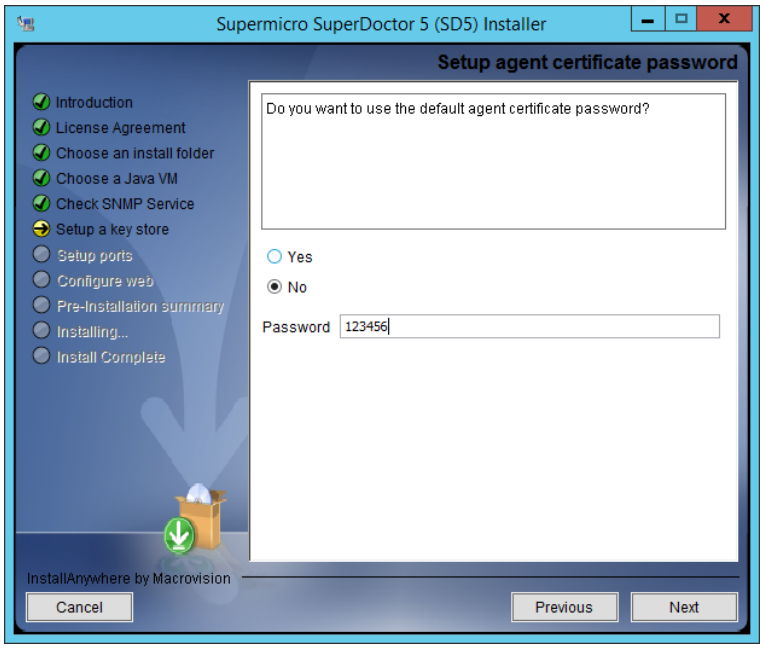


Figure 15-12

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.

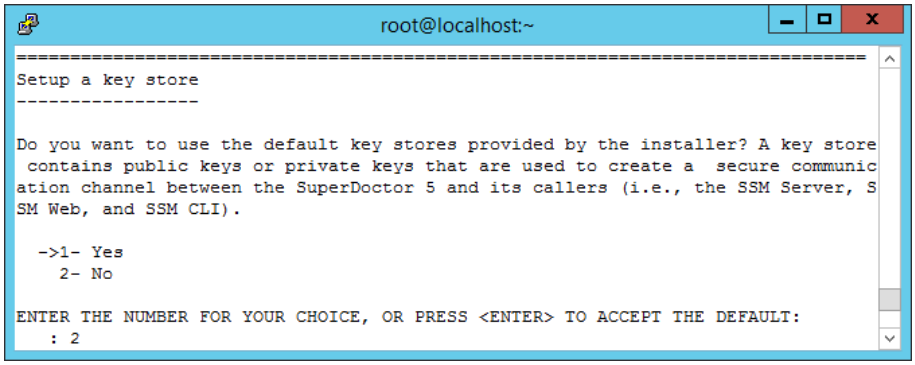


Figure 15-13

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.

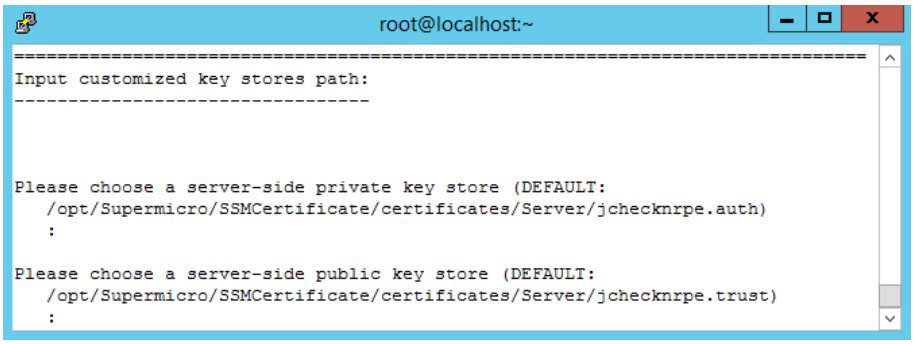


Figure 15-14

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 15-15

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 5 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 ssmserver.log.1, ssmserver.log.2, ssmserver.log.3 . . . ssmserver.log.10. You can change the maximum log file size and maximum number of backup copies.

Configuring the log properties of SSM Server:

1. Find **log4j2.properites** located in the **[install folder]\SSMServer\config** folder and open it with a text editor.

2. Find the content that contains the following line: **appender.ssmserver.policies.size.size=8192KB**
   Modify the word 8192KB 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.

3. Find the content that contains the following line: **appender.ssmserver.strategy.max=10**
   Modify the keyword **10** to an appropriate value.

4. Save the file.

Configuring the log properties of SSM Web:

1. Find **log4j2.properties** located in **[install folder]\SSMWeb\config** folder and open it with a text editor.

2. Find the content that contains the following line:
   appender.web.policies.size.size=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:
   appender.web.strategy.max=10
   Modify the keyword **10** to an appropriate value.

4. Save the file.

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:
   appender.logfile.policies.size.size=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: **appender.logfile.strategy.max=10**
   Modify the keyword **10** to an appropriate value.

4. Save the file.

B. Third-Party Software

The open source libraries used by SSM are as follows:

Name	License	Component Source URL	Note
activation	CDDL	http://java.sun.com/javase/technologies/desktop/javabeans/jaf/index.jsp	SSM Server, SSM Web
Antlr	BSD	https://repo1.maven.org/maven2/org/antlr/antlr-complete	SSM Server, SSM Web
aopalliance	Public Domain	http://aopalliance.sourceforge.net	SSM Server, SSM Web
Apache commons	Apache License	https://commons.apache.org/	SSM Server, SSM Web
asm	BSD	https://repo1.maven.org/maven2/org/ow2/asm/asm	SSM Web
AspectJ weaver	Eclipse Public License	https://repo1.maven.org/maven2/org/aspectj/aspectjweaver	SSM Web
Aspectjrt	Eclipse Public License	https://repo1.maven.org/maven2/org/aspectj/aspectjrt	SSM Web
byte-buddy	Apache License	https://repo1.maven.org/maven2/net/bytebuddy/byte-buddy/	SSM Server, SSM Web
BVal	Apache License	https://bval.apache.org/	SSM Web
Camel	Apache License	https://camel.apache.org/	SSM Server, SSM Web
cdi-api	Apache License	https://repo1.maven.org/maven2/javax/enterprise/cdi-api	SSM Server, SSM Web
cglib	Apache License	https://repo1.maven.org/maven2/cglib/cglib	SSM Web
classindex	Apache License	https://repo1.maven.org/maven2/org/atteo/classindex/classindex	SSM Server, SSM Web
classmate	Apache License	https://repo1.maven.org/maven2/com/fasterxml/classmate	SSM Server, SSM Web
dom4j	BSD	https://repo1.maven.org/maven2/org/dom4j/dom4j	SSM Server, SSM Web
Ehcache-core	Apache License	https://repo1.maven.org/maven2/net/sf/ehcache/ehcache	SSM Server, SSM Web
fat32	LGPL	https://mvnrepository.com/artifact/de.waldheinz/fat32-lib	SSM Web
evo-inflector	Apache License	https://repo1.maven.org/maven2/org/atteo/evo-inflector	SSM Web
gson	Apache License	https://repo1.maven.org/maven2/com/google/code/gson/gson	SSM Server, SSM Web

Name	License	Component Source URL	Note
guice	Apache License	https://repo1.maven.org/maven2/com/google/inject/guice	SSM Server, SSM Web
guava	Apache License	https://repo1.maven.org/maven2/com/google/guava/guava	SSM Server, SSM Web
Hibernate	LGPL	https://repo1.maven.org/maven2/org/hibernate/	SSM Server, SSM Web
httpclient	Apache License	https://repo1.maven.org/maven2/org/apache/httpcomponents/httpclient	SSM Server, SSM Web
httpcore	Apache License	https://repo1.maven.org/maven2/org/apache/httpcomponents/httpcore	SSM Server, SSM Web
httpmime	Apache License	https://repo1.maven.org/maven2/org/apache/httpcomponents/httpmime	SSM Server, SSM Web
istack-commons-runtime	CDDL, GPL	https://repo1.maven.org/maven2/com/sun/istack/istack-commons-runtime	SSM Server, SSM Web
Jackson	Apache License	https://repo1.maven.org/maven2/com/fasterxml/jackson/	SSM Server, SSM Web
jandex	Apache License	https://repo1.maven.org/maven2/org/jboss/jandex	SSM Server, SSM Web
Java Native Access	Apache License, LGPL	https://repo1.maven.org/maven2/net/java/dev/jna/jna	SSM Server, SSM Web
JavaMail (mail.jar)	CDDL	https://repo1.maven.org/maven2/javax/mail/mail	SSM Server, SSM Web
javassist	Apache 2.0, LGPL 2.1, Mozilla Public License 1.1	https://repo1.maven.org/maven2/org/javassist/javassist	SSM Server, SSM Web
javax.activation-api	CDDL, GPL	https://repo1.maven.org/maven2/javax/activation/javax.activation-api	SSM Server, SSM Web
javax.annotation-api	GPL, CDDL	https://repo1.maven.org/maven2/javax/annotation/javax.annotation-api	SSM Server, SSM Web
javax-ejb-api	GPL, CDDL	https://repo1.maven.org/maven2/javax/ejb/javax.ejb-api	SSM Server, SSM Web
javax-el-api	GPL, CDDL	https://repo1.maven.org/maven2/javax/el/javax.el-api	SSM Server, SSM Web
javax.inject	Apache License	https://mvnrepository.com/artifact/javax.inject/javax.inject	SSM Server, SSM Web
javax.interceptor-api	GPL, CDDL	https://repo1.maven.org/maven2/javax/interceptor/javax.interceptor-api	SSM Server, SSM Web
Javax.persistence-api	EDL, EPL	https://repo1.maven.org/maven2/javax/persistence/javax.persistence-api	SSM Server, SSM Web
javax.servlet-api	GPL, CDDL	https://repo1.maven.org/maven2/javax/servlet/javax.servlet-api	SSM Server, SSM Web
javax.transaction-api	GPL, CDDL	https://repo1.maven.org/maven2/javax/transaction/javax.transaction-api	SSM Server, SSM Web
javax.websocket	GPL, CDDL	https://repo1.maven.org/maven2/javax	SSM Web

Name	License	Component Source URL	Note
		/websocket/javax.websocket-api	
javax.ws.rs-api	GPL, CDDL	https://repo1.maven.org/maven2/javax/ws/rs/javax.ws.rs-api	SSM Server, SSM Web
jaxb-api	CDDL	https://mvnrepository.com/artifact/javax.xml.bind/jaxb-api	SSM Server, SSM Web
Jaxb-runtime	CDDL, GPL	https://repo1.maven.org/maven2/org/glassfish/jaxb/jaxb-runtime	SSM Server, SSM Web
jboss-annotations-api	GPL, CDDL	https://repo1.maven.org/maven2/org/jboss/spec/javax/annotation/jboss-annotations-api_1.2_spec	SSM Server, SSM Web
jboss-jaxrs-api	GPL, CDDL	https://repo1.maven.org/maven2/org/jboss/spec/javax/ws/rs/jboss-jaxrs-api_2.0_spec	SSM Server, SSM Web
jboss-logging	Apache License	https://repo1.maven.org/maven2/org/jboss/logging/jboss-logging	SSM Server, SSM Web
jboss-servlet-api	GPL, CDDL	https://repo1.maven.org/maven2/org/jboss/spec/javax/servlet/jboss-servlet-api_3.1_spec	SSM Server, SSM Web
jboss-transaction-api	GPL, CDDL	https://repo1.maven.org/maven2/org/jboss/spec/javax/transaction/jboss-transaction-api_1.2_spec	SSM Server, SSM Web
jcl	Apache License	https://repo1.maven.org/maven2/org/slf4j/jcl-over-slf4j	SSM Server, SSM Web
jcommon	LGPL	https://repo1.maven.org/maven2/jfree/jcommon	SSM Web
jetty	Apache License, Eclipse Public License	https://repo1.maven.org/maven2/org/eclipse/jetty/	SSM Web
JFreeChart	LGPL	http://sourceforge.net/projects/jfreechart	SSM Web
Jmdns	Apache License	https://repo1.maven.org/maven2/org/jmdns/jmdns	SSM Server, SSM Web
Joda Time	Apache License	https://repo1.maven.org/maven2/joda-time/joda-time	SSM Web
jsmiparser	Apache License	https://github.com/dverstap/jsmiparser	SSM Server
json-path	Apache License	https://repo1.maven.org/maven2/com/jayway/jsonpath/json-path	SSM Web
jsoup	MIT	https://jsoup.org/	SSM Web
liquibase	Apache License	https://repo1.maven.org/maven2/org/liquibase/liquibase-core	SSM Server
Log4J	Apache License	http://logging.apache.org/log4j	SSM Server, SSM Web
openjson	Apache License	https://github.com/openjson/openjson	SSM Web
Netty	Apache License	https://repo1.maven.org/maven2/io/netty/netty	SSM Server, SSM Web

Name	License	Component Source URL	Note
Postgresql jdbc driver	BSD	https://repo1.maven.org/maven2/org/postgresql/postgresql	SSM Server, SSM Web
Quartz	Apache License	https://repo1.maven.org/maven2/org/quartz-scheduler/quartz	SSM Server
reflections	BSD	https://repo1.maven.org/maven2/org/reflections/reflections	SSM Server, SSM Web
resteasy	Apache License	https://repo1.maven.org/maven2/org/jboss/resteasy	SSM Server, SSM Web
sabre	LGPL	https://repo1.maven.org/maven2/com/github/stephenc/java-iso-tools/sabre	SSM Web
SLF4J	MIT	https://repo1.maven.org/maven2/org/slf4j	SSM Server, SSM Web
snakeyaml	Apache License	https://repo1.maven.org/maven2/org/yaml/snakeyaml	SSM Server
SNMP4J	Apache License	https://repo1.maven.org/maven2/org/apache/servicemix/bundles/org.apache.servicemix.bundles.snmp4j	SSM Server, SSM Web
Spring framework	Apache License	https://repo1.maven.org/maven2/org/springframework	SSM Server, SSM Web
stax2	BSD	https://repo1.maven.org/maven2/org/codehaus/woodstox/stax2-api	SSM Web
trimou-core	Apache License	https://repo1.maven.org/maven2/org/trimou/trimou-core	SSM Server, SSM Web
truelicense	Eclipse Public License	https://repo1.maven.org/maven2/de/schlichtherle/truelicense/	SSM Server, SSM Web
typetools	Apache License	https://repo1.maven.org/maven2/net/jodah/typetools	SSM Web
validation	Apache License	https://repo1.maven.org/maven2/javax/validation/validation-api	SSM Web
websocket	Apache License, Eclipse Public License	https://repo1.maven.org/maven2/org/eclipse/jetty/websocket	SSM Web
Wicket	Apache License	https://repo1.maven.org/maven2/org/apache/wicket	SSM Web
WicketStuff Restannotations	Apache License	https://mvnrepository.com/artifact/org.wicketstuff/wicketstuff-restannotations	SSM Web
woodstox	Apache License	https://repo1.maven.org/maven2/com/fasterxml/woodstox/woodstox-core	SSM Web
@coreui/coreui	MIT	https://www.npmjs.com/package/@coreui/coreui	SSM Web
@coreui/icons	MIT	https://www.npmjs.com/package/@coreui/icons	SSM Web
@coreui/react	MIT	https://www.npmjs.com/package/@cor	SSM Web

Name	License	Component Source URL	Note
		eui/react	
@fortawesome/fontawesome-svg-core	MIT	https://www.npmjs.com/package/@fortawesome/fontawesome-svg-core	SSM Web
@fortawesome/free-solid-svg-icons	CC-BY-4.0 and MIT	https://www.npmjs.com/package/@fortawesome/free-solid-svg-icons	SSM Web
@fortawesome/react-fontawesome	MIT	https://www.npmjs.com/package/@fortawesome/react-fontawesome	SSM Web
classnames	MIT	https://www.npmjs.com/package/classnames	SSM Web
core-js	MIT	https://www.npmjs.com/package/core-js	SSM Web
excanvas	Apache License	https://mvnrepository.com/artifact/org.webjars/excanvas	SSM Web
font-awesome	OFL-1.1 and MIT	https://fontawesome.com/	SSM Web
i18next	MIT	https://www.npmjs.com/package/i18next	SSM Web
i18next-browser-languagedetector	MIT	https://www.npmjs.com/package/i18next-browser-languagedetector	SSM Web
i18next-xhr-backend	MIT	https://www.npmjs.com/package/i18next-xhr-backend	SSM Web
json-smart	Apache License	http://www.minidev.net/	SSM Web
lodash	MIT	https://www.npmjs.com/package/lodash	SSM Web
moment-timezone	MIT	https://www.npmjs.com/package/moment-timezone	SSM Web
nimbus-jose-jwt	Apache License	https://bitbucket.org/connect2id/nimbus-jose-jwt	SSM Web
prop-types	MIT	https://www.npmjs.com/package/prop-types	SSM Web
react	MIT	https://www.npmjs.com/package/react	SSM Web
react-bootstrap	MIT	https://www.npmjs.com/package/react-bootstrap	SSM Web
react-dom	MIT	https://www.npmjs.com/package/react-dom	SSM Web
react-i18next	MIT	https://www.npmjs.com/package/react-i18next	SSM Web
react-loadable	MIT	https://www.npmjs.com/package/react-loadable	SSM Web
react-moment	MIT	https://www.npmjs.com/package/react-moment	SSM Web
react-redux	MIT	https://www.npmjs.com/package/react-redux	SSM Web
react-router-config	MIT	https://www.npmjs.com/package/react-router-config	SSM Web

Name	License	Component Source URL	Note
react-router-dom	MIT	https://www.npmjs.com/package/react-router-dom	SSM Web
react-select	MIT	https://www.npmjs.com/package/react-select	SSM Web
react-sliding-pane	MIT	https://www.npmjs.com/package/react-sliding-pane	SSM Web
react-table	MIT	https://react-table.tanstack.com/	SSM Web
reactstrap	MIT	https://www.npmjs.com/package/reactstrap	SSM Web
react-virtualized	MIT	https://www.npmjs.com/package/react-virtualized	SSM Web
react-draggable	MIT	https://www.npmjs.com/package/react-draggable	SSM Web
redux	MIT	https://www.npmjs.com/package/redux	SSM Web
redux-logger	MIT	https://www.npmjs.com/package/redux-logger	SSM Web
redux-thunk	MIT	https://www.npmjs.com/package/redux-thunk	SSM Web
styled-components	MIT	https://www.npmjs.com/package/styled-components	SSM Web

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.

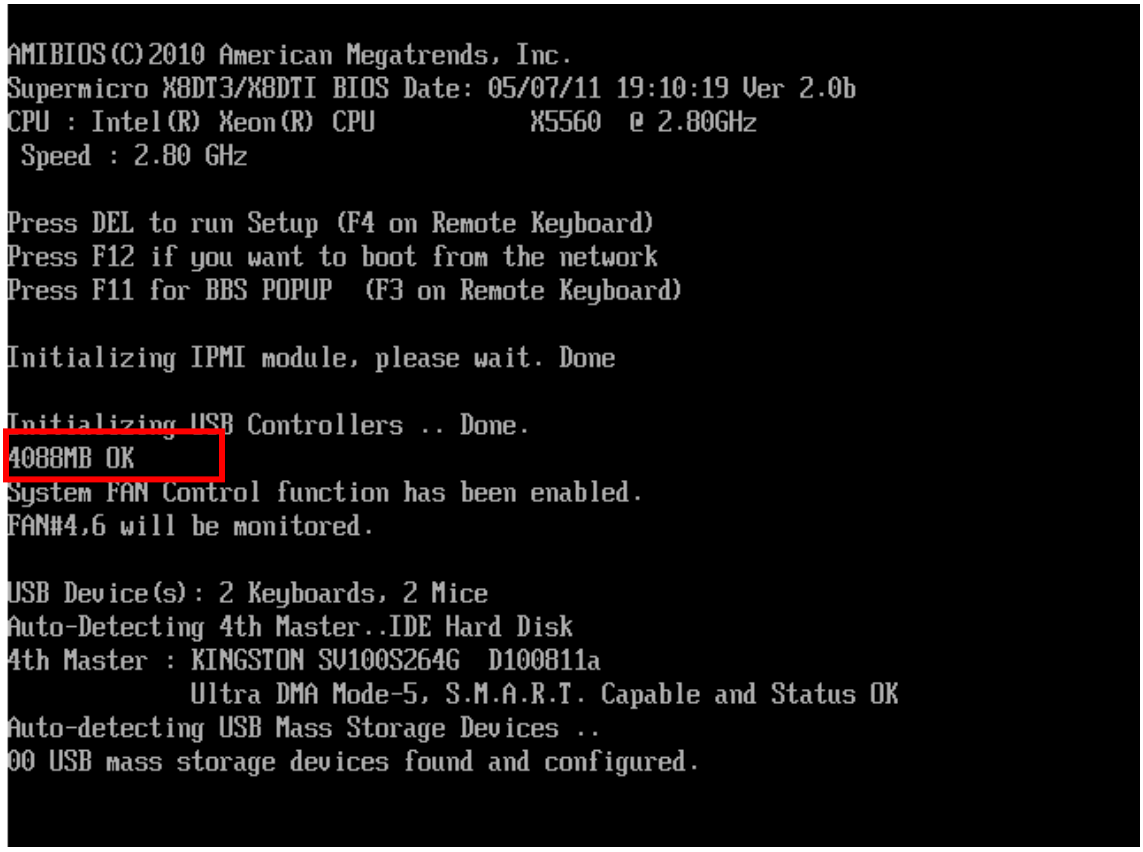


Figure C-1

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 SV100S264G  D100811a
             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.

D. Supported Platforms for IPMI and Redfish Commands

In the table below, ● shows availability of support by SSM, while ○ stands for not available. Note that each generation of both AMD and Intel platforms supposedly shares the same codebase.

Command	SSM Host Type	Intel MB	AMD MB	CMM	Blade
BMC Cold Reset	IPMI	X10, X11, X12	H11, H12	●	●
	Redfish	X10+	H11+	●	●
Blink UID LED	IPMI	X10, X11, X12	H11, H12	●	●
	Redfish	X10+	H11+	●	●
Change BMC Password	IPMI	X10, X11, X12	H11, H12	●	●
	Redfish	X10+	H11+	●	●
Clear BMC SEL	IPMI	X10, X11, X12	H11, H12	●	●
	Redfish	X10+	H11+	●	●
Clear BMC SEL and BIOS Log	IPMI	X10, X11, X12	H11, H12	○	●
Clear TPM Management	IPMI	X11(after C620s), X12	○	○	○
Clear TPM Provision	IPMI	X10, X11(before C620s), X12	○	○	●
Deploy OS	IPMI	X10, X11, X12	H11, H12	○	●
	Redfish	X12+	H12+	○	●
Diagnose System	Redfish	X12+	H12+	○	●
Disable System Lockdown	Redfish	X12+	H12+	○	●
Edit BMC Setting	Redfish	X10+	H11+	○	●
Edit DMI Info	IPMI	X10, X11, X12	H11, H12	○	●
	Redfish	X12+	H12+	○	B12+/BH12+
Enable System Lockdown	Redfish	X12+	H12+	○	●
Enable TPM Management	IPMI	X11(after C620s), X12	○	○	○
Enable TPM Provision	IPMI	X10, X11 (before C620s), X12	○	○	●
Export Asset Info	IPMI	X10, X11, X12	H11, H12	○	●
Export BIOS Cfg	IPMI	X10, X11, X12	H11, H12	○	●

Command	SSM Host Type	Intel MB	AMD MB	CMM	Blade
Export BMC Cfg	IPMI	X10, X11, X12	H11, H12	○	●
Export BMC SEL	IPMI	X10, X11, X12	H11, H12	○	●
	Redfish	X10+	H11+	○	●
Export BMC MEL	Redfish	X11+	H11+	○	●
Export DMI Info	IPMI	X10, X11, X12	H11, H12	○	●
Export Factory BIOS Cfg	IPMI	X10, X11, X12	H11, H12	○	●
Export System Utilization	IPMI	X10, X11, X12	H11, H12	○	●
Graceful Power Off	IPMI	X10, X11, X12	H11, H12	○	●
	Redfish	X10+	H11+	○	●
Import BIOS Cfg	IPMI	X10, X11, X12	H11, H12	○	●
Import BMC Cfg	IPMI	X10, X11, X12	H11, H12	○	●
Import DMI Info	IPMI	X10, X11, X12	H11, H12	○	●
Load Factory BIOS Setting	IPMI	X10, X11, X12	H11, H12	○	●
	Redfish	X12+	H12+	○	B12+/BH12+
Load Factory BMC Setting	IPMI	X10, X11, X12	H11, H12	○	●
	Redfish	X10+	H11+	○	●
Mount ISO Image	IPMI	X10, X11, X12	H11, H12	○	●
	Redfish	X12+	H12+	○	●
Power Off	IPMI	X10, X11, X12	H11, H12	○	●
	Redfish	X10+	H11+	○	●
Power On	IPMI	X10, X11, X12	H11, H12	○	●
	Redfish	X10+	H11+	○	●
Recover BIOS from Backup	IPMI	X12	H12	○	B12+/BH12+
	Redfish	X12+	H12+	○	B12+/BH12+
Recover BMC from Backup	IPMI	X12	H12	○	B12+/BH12+
	Redfish	X12+	H12+	○	B12+/BH12+
Power Reset	IPMI	X10, X11, X12	H11, H12	○	●
	Redfish	X10+	H11+	○	●
Reset Chassis Intrusion	IPMI	X10, X11, X12	H11, H12	○	●
	Redfish	X10+	H11+	○	●
Secure Erase	Redfish	X12+	○	○	○
Stop Blinking UID LED	IPMI	X10, X11, X12	H11, H12	●	●
	Redfish	X10+	H11+	●	●
Sync Node PK	IPMI	X10, X11, X12	H11, H12	○	●
	Redfish	X10+	H11+	○	●
Unmount ISO Image	IPMI	X10, X11, X12	H11, H12	○	●
	Redfish	X12+	H12+	○	●
Update BIOS	IPMI	X10, X11, X12	H11, H12	○	●

Command	SSM Host Type	Intel MB	AMD MB	CMM	Blade
(Capsule)	Redfish	X12+	H12+	○	●
Update BMC	IPMI	X10, X11, X12	H11, H12	○	●
	Redfish	X12+	H12+	○	●
Update Golden BIOS	IPMI	X12	H12	○	B12+/BH12+
	Redfish	X12+	H12+	○	B12+/BH12+
Update Golden BMC	IPMI	X12	H12	○	B12+/BH12+
	Redfish	X12+	H12+	○	B12+/BH12+
Update CMM	IPMI	○	○	●	○
	Redfish	○	○	CMM-6+	○
Turn Blade UID On/Off	IPMI	○	○	●	○
	Redfish	○	○	●	○
Export CMM Cfg	IPMI	○	○	●	○
Import CMM Cfg	IPMI	○	○	●	○
Load Factory CMM Setting	IPMI	○	○	●	○
	Redfish	○	○	●	○

E. Backing Up and Restoring SSM in a New System

In this appendix you'll learn how to use the built-in scheduler in the OS to back up SSM data and then restore it in a new SSM. Note that the backup script that SSM provides will overwrite the backup copies.

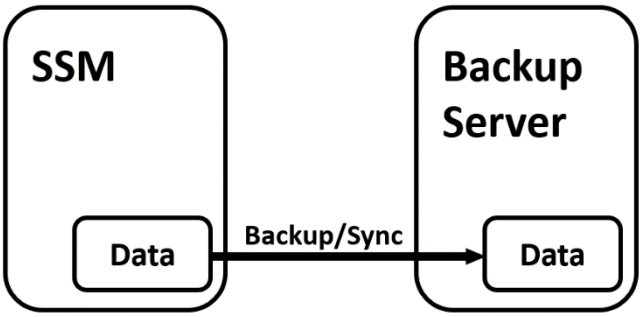


Figure E-1

Regardless of how often SSM data has been backed up, only the latest backup will be kept. To prevent the SSM system from suddenly crashing, it's recommended that backup data be kept in another system, which is named "Backup Server" in the following examples. The backup process is shown below.

Backing Up on Linux

To back up SSM configurations and database data on Linux, follow these steps.

1. Generate your RSA SSH key and put the public key in the Backup Server. For example, the SSM IP address is 10.146.40.43, and the Backup Server IP address is 10.146.42.3. Generate an RSA SSH key in 10.146.40.43, and copy the ID to 10.146.42.3.

```
[root@localhost backup]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
/root/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:+3R1kSi9I1K0K+Q7YXvaH5Lz4T18g0WXdSl9R2LRcqk root@localhost.localdomain
The key's randomart image is:
+---[RSA 2048]----+
|          .    =++|
|         . . .oo=O|
|        . o . oo=*|
|       o . . .E.oo|
|        *So . .o o|
|       . *.o .. o |
|        +.=.oo o  |
|         =o=.++ o |
|        . .o+ .o .|
+----[SHA256]-----+
[root@localhost backup]# ssh-copy-id -i /root/.ssh/id_rsa root@10.146.42.3
```

Figure E-2

2. Edit the backup.sh script in [install folder]/shared/tools/backupAndRestore/backup.sh], and modify "**restoreIP**" in the third line [Backup Server IP address].
3. Create a cron job to execute the backup.sh script to backup both the SSM configurations and the database data, and then copy the backup files to the Backup Server. You can use the crontab to specify time periods for the backup script. For example, you can run the backup.sh script at 8:30 AM every day.

```
30 08 * * * /opt/Supermicro/SSM/shared/tools/backupAndRestore/backup.sh
```

Figure E-3

Restoring on Linux

To use the backup data to set up a new SSM, please follow these steps. Note that the Backup Server and the new SSM is on the same host so that the new SSM can access to the backup data directly.

1. Install SSM. Note that system environment requirements should be the same as the original SSM.
2. Execute the restore.sh script in **[install folder]/shared/tools/backupAndRestore/restore.sh.** Note that while restoring data, SSM services will be stopped by the restore.sh script.
3. Revise the server's address if the IP address of your new system has been changed. See *6.12 Server Address* for details.
4. Restart the SSM services.
   1). service ssmweb restart.
   2). service ssmserver restart

Backing Up on Windows

To back up SSM configurations and database data in Windows, follow these steps.

1. Set the SSM Server to share network with the Backup Server and transfer the backup files to the Backup Server. For example, the SSM Server IP address is 10.146.40.43, and the Backup Server System name is "WIN-5T5S6R83QEC". Make sure you can copy files to the network space without a password. Note that you need to turn off password protected sharing when using the shared network function.

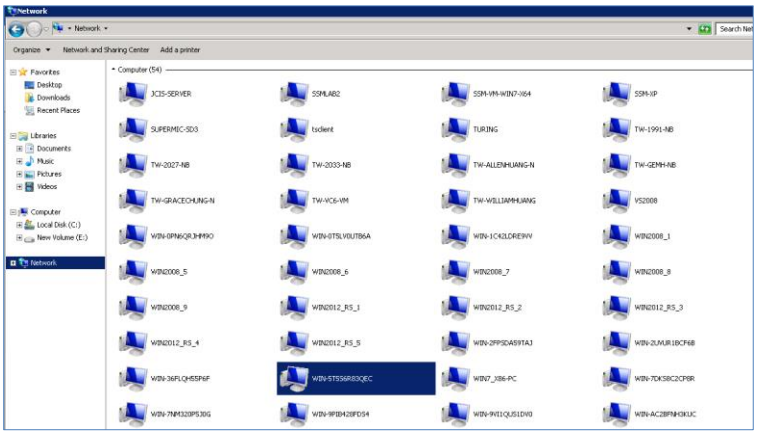


Figure E-4

2. Edit the backup.bat file in **[install folder]/shared/tools/backupAndRestore/backup.bat**, and modify

"**targetPath**" in the third line of the Backup Server shared folder named "backup." In this example, Backup Server "WIN-5T5S6R83QEC" shares the "backup" folder with SSM to output backup data so the targetPath should be set to "\\WIN-5T5S6R83QEC\backup."

3. Set the task scheduler to run the backup.bat file at the specified time. The backup.bat file backs up both SSM configurations and database data and copies the backup file to the Backup Server. For example, you can run the backup.bat file at 7:20 AM every day.

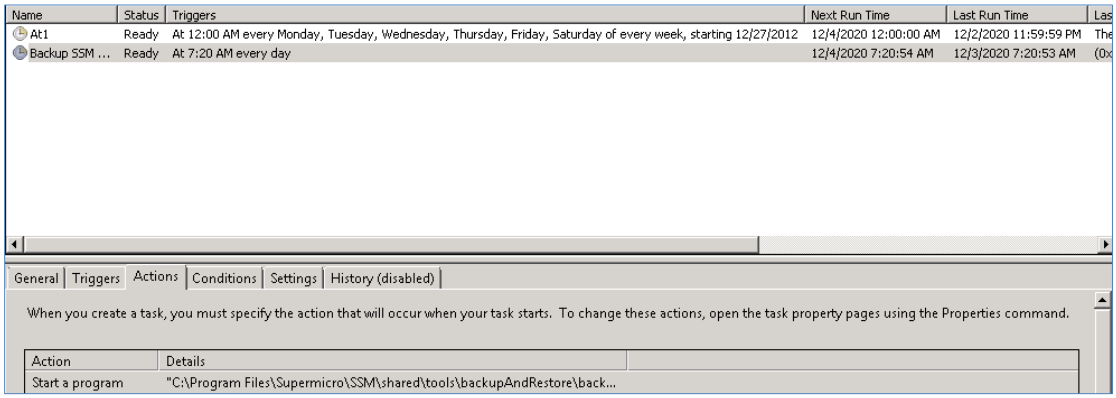


Figure E-5

Restoring on Windows

To use the backup data to set up a new SSM, please follow the steps below. Note that the Backup Server and the new SSM is on the same host so that the new SSM can access to the backup data directly.

1. Install SSM. Note the system environment requirements should be the same as the original SSM.
2. Modify "**targetPath**" in the third line in the Backup Server shared folder and then execute the restore.bat file. Note that while restoring data, SSM services will be stopped by the restore.bat script. Following the example in the *Restoring on Windows* section above, to use the existing backup file to restore, set the targetPath to "\\WIN-5T5S6R83QEC\backup."
3. Revise the server's address if the IP address of your new system has been changed. See *6.12 Server Address* for details.
4. Restart the SSM services.
   1). sc stop ssmweb
   2). sc start ssmweb
   3). sc stop ssmserver
   4). sc start ssmserver

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)
Sales-USA@supermicro.com (Sales Inquiries)
Government_Sales-USA@supermicro.com (Gov. Sales Inquiries)
support@supermicro.com (Technical Support)
RMA@supermicro.com (RMA 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_Europe@supermicro.com (Sales Inquiries)
Support_Europe@supermicro.com (Technical Support)
RMA_Europe@supermicro.com (RMA 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: Sales-Asia@supermicro.com.tw (Sales Inquiries)
Support@supermicro.com.tw (Technical Support)
RMA@supermicro.com.tw (RMA Support)
Website: www.supermicro.com.tw