Supermicro Server Manager

Quick Start Guide

Revision 1.0

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

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

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

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

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

Manual Revision: 1.0
Release Date: 5/12/2022

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

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

Copyright © 2022 Super Micro Computer, Inc.
All rights reserved.
Printed in the United States of America

Revision History

Date	Rev	Description
May-12-2022	1.0	1. Initial document.

Contents

Part 1 Preparation

1 Requirements for Target BMCs

- Each target host's BMC must be activated with an SFT-DCMS-SINGLE product key. To use the Service Calls, another SFT-DCMS-SVC product key is required as well.
- Redfish protocol is the preferred communication method between SSM[1] and its managed BMC hosts.
- To avoid any security vulnerabilities, it is strongly suggested that you should modify and not use the default port (623) of RMCP protocol.

2 Resetting All Passwords of Target BMCs

In SSM, to add a Supermicro server with BMC as either an IPMI or Redfish host, you must reset the password for the administrator account. Please follow these steps:

1. Go to https://www.supermicro.com/en/support/BMC_Unique_Password, click **click here** and then click the **ACCEPT** button to agree to the End User License Agreement.
2. Download and unzip "ResetBMCPasswordToADMIN.zip."
3. Locate the *Reset Password to "ADMIN" Using Raw Command Script* document and refer to the *Prerequisites* section to prepare a Python environment.
4. Execute the "python reset_bmc_password_to_admin [your_supermicro_mapping_file] [your_start_ip] [your_end_ip]" script to reset the BMC unique password to "ADMIN."

The "ADMIN" password can only be used temporarily. To change all BMC passwords on SSM hosts at once, refer to *10 Changing BMC Passwords for All Managed Redfish Hosts*.

[1] SSM v5.1.0 and its *SSM User Guide* are referenced in this document.

3 System Requirements for Management Server

3.1 Managing Up to 1,999 Hosts

Hardware Requirements

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

Operating System Requirements

- Red Hat Enterprise Linux Server 6.x (64-bit), 7.x (64-bit), 8.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

Note: To run SSM on a virtual machine, more CPU cores and RAMs may be needed depending on the number of managed systems.

For SSM to communicate with BMCs, open ports in your firewall. See *1.7.3 Default TCP/UDP Ports* in the *SSM User Guide* for details.

3.2 Managing 2,000 Hosts or More

Hardware Requirements

- 80.0 GB free disk space
- 12 CPU cores with Intel® Xeon® or AMD EPYC™ Processor or later
- Available 32.0 GB RAM
- An Ethernet network interface card

Operating System Requirements

- Red Hat Enterprise Linux Server 7.x (64-bit), 8.x (64-bit)
- SUSE Linux Enterprise 15.x (64-bit)

4 Downloading and Installing SSM

1. Go to https://www.supermicro.com/en/support/resources/downloadcenter/smsdownload?category=SSM, download and unzip the file of the latest version of SSM.
2. Execute the SSM installer and follow the prompts to complete the installation.
   - Windows users: You should log in with administrator privileges.
   - Linux users: Make sure you have root privileges.
3. When prompted to *Set the password for built-in ADMIN user*, configure the password for the administrator account to access the SSM Web.
4. When prompted to *Setup SMTP*, configure 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.

Note: The data will be used by the SSM server to send notifications.

5. When complete, a message "Install Completed Successfully" appears. You are now ready to use SSM.

Part 2 Usage

5 Activating SFT-DCMS-Single and SFT-DCMS-SVC-KEY Keys

The SFT-DCMS-SINGLE product keys for BMCs on your systems must be activated. If not, target BMCs are not able to be added into SSM for management. The SFT-DCMS-SVC key is required for SSM Service Calls functions. If you have bought the license keys for systems, you can skip this chapter; otherwise, follow the steps below or refer to *6.6 Node PK Activation* in the *SSM User Guide* for details.

1. Open a web browser and type https://[SSM Web address]:8443/SSMWeb.
2. Log into SSM Web with the built-in ADMIN account ID and the password you configured while installing SSM.
3. Go to SSM Main Page > Administration > Monitoring Setup > Node PK Activation **Step 1** Area.
4. Fill out the BMC Address, BMC ID, and BMC Password fields and then click the **Collect** button.
5. Click the **Export MAC(s) File** button to export all MAC addresses to a file. The output file ("SSM_mymacs.txt") includes a list of MAC address and BMC address.

Note: The BMC passwords of the managed systems were reset to "ADMIN" in the previous step.

6. Contact Supermicro to generate an activation file with the exported MAC file.
7. Go to SSM Main Page > Administration > Monitoring Setup > Node PK Activation **Step 3** Area.
8. Click the Choose File button, select the activation file from Supermicro, fill in the BMC ID and BMC Password fields, and then click the Activate button.

Note: 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.

6 Setting Up a Server Address

For a Supermicro server equipped with multiple network interfaces, you must configure a valid address for SSM to receive messages from the managed hosts. Refer to *6.12 Server Address* in the *SSM User Guide* for details.

1. Log into SSM Web with the ID and password of the built-in ADMIN account.
2. Go to SSM Main Page > Administration > Management Server Setup > Server Address.
3. Fill out the Server Address field and then click the **Submit** button.

7 Setting Up Contact Addresses for the Admin Account

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. You could refer to *6.4 Contact Management* in the *SSM User Guide* for details.

1. Log into SSM Web with the ID and password of the built-in ADMIN account.
2. Go to SSM Main Page > Administration > Monitoring Setup > Contact.
3. Select the admin contact in the working area and use the **Edit Contact** command in the **Commands** area to edit it.
4. Fill in the E-Mail Address or SNMP Trap Receivers field and then click the **Submit** button.

Note: It is highly recommended that you click the **Send Test E-Mail** and **Send Test Trap** buttons to ensure your email and trap receiver addresses are both accessible.

8 Discovering and Adding a Host

You could either add Redfish hosts manually or set a scheduler to discover them automatically.

8.1 Discovering Hosts with the Host Discovery Wizard

1. Log into SSM Web with the ID and password of the built-in ADMIN account.
2. Go to SSM Main Page > Administration > Host Discovery Wizard.
3. Select the **Redfish** option and click the **Next** button.
4. Set the BMC ID with the Administrator privileges and the password. Click the **Next** button.
5. 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.
6. In the Discovery Result setup, select the hosts to be monitored and click the **Next** button to continue.
7. When the Host Discovery Wizard is complete, click the **Finish** button to close the wizard. See *6.15* in the *SSM User Guide* for details.

8.2 Discovering Hosts by Scheduled Tasks

1. Log into SSM Web with the ID and password of the built-in ADMIN account.
2. Go to SSM Main Page > Monitoring > All > Task View > Scheduled Task Management.
3. The Scheduled Task Management dialog box appears and displays the existing scheduled tasks. Click the **Add** button to create a new scheduled task. The Add Scheduled Task Setting dialog box appears. Fill out **Name** and select **Discover Redfish Host** in the **Command** field. The corresponding parameters appear in the Command Parameters area.

Notes:

- The **Enabled** check box must be selected for the commands to be executed.
- All fields are case-insensitive except the BMC ID and BMC Password fields.
- 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.
- It is highly recommended that you click the **Send Test E-Mail** and **Send Test Trap** buttons to ensure your e-mail and trap receiver addresses are respectively accessible.

4. Click the **Schedule** tab, use the Repeat On drop-down list to select **Once** or **Weekly** to determine the execution frequency. Click the **Submit** button. The new task is now added.
5. When the scheduled task execution begins, its status is displayed in Task View. See *7.2.6* in the *SSM User Guide* for details.

9 Changing Date, Time and NTP for All Managed Redfish Hosts

To keep all clocks on the managed system synchronized, you can enable Network Time Protocol (NTP) on the BMCs and assign an NTP server at once.

1. Log into SSM Web with the ID and password of the built-in ADMIN account.
2. Go to SSM Main Page > Monitoring > All > Host View > Edit BMC Setting.
3. Press and hold both **[Ctrl] and [left mouse click]** to select multiple hosts in the Host View table, and then click **Edit BMC Setting** in the **Commands** area.
4. In the Edit BMC Setting dialog box, use the drop-down list to select **[NTP] Enabled** and set the value to **yes.** Click the **Add Item** button to create a new drop-down list, select **[NTP] Primary NTP Server**, and set the value to **0.us.pool.ntp.org** or the IP address where the NTP server also works. Click the **Next** button to continue.
5. Click the **Run** button, and then click the **Task ID** link to check for results.

10 Changing BMC Passwords for All Managed Redfish Hosts

The Change BMC password command allows users to update the BMC password saved by the BMC and SSM.

1. Log into SSM Web with the ID and password of the built-in ADMIN account.
2. Go to SSM Main Page > Monitoring > All > Host View > Change BMC Password.
3. Use **[Ctrl]** and **[left mouse click]** to select multiple hosts in the Host View table then click **Change BMC Password** in the **Commands** area and the Change BMC Password dialog box appears.
4. Fill out the fields and then click the **Next** button to change password and close this dialog box.

11 Checking Host Status and Service Status

Host Status in the Host View shows the current status of hosts while Service Status displays the combined service status. When services are problematic, you should first check the host status to see if the host is online or offline. The Redfish SEL Health service is used to check the health of a managed system *based on the System Event Log*, and Redfish System Information is used to gather system information.

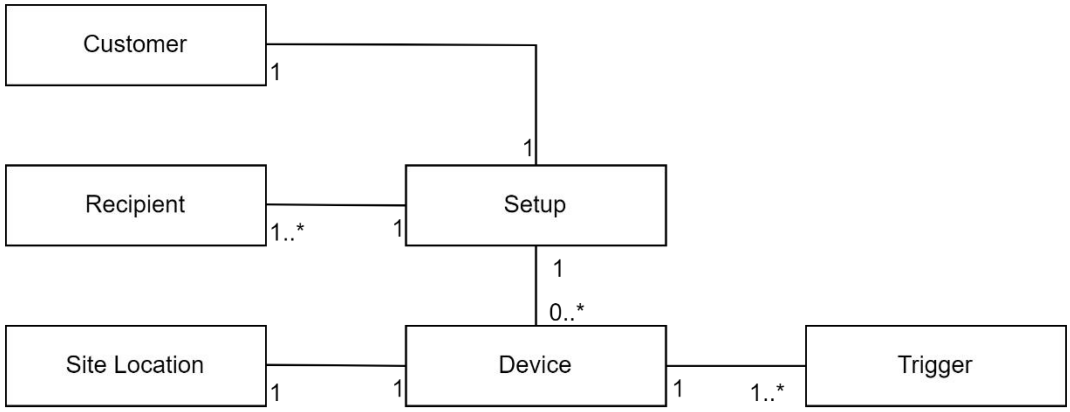
1. Log into SSM Web with the ID and password of the built-in ADMIN account.
2. Go to SSM Main Page > Monitoring > All > Host View.
3. The host status shows “Up” indicating the host is running.
4. Click the **service status** tab in the **Detail** View, the Redfish SEL Health and Redfish System Information should be available and displayed in green.

Notes:

- The **View Details** command under the **System Information** category in the **Commands** area is available for viewing all types of the system information objects.
- To run SSM on a virtual machine, more CPU cores and RAMs may be needed depending on the number of managed systems.

12 Enabling Service Calls

The Service Calls function aims to promptly respond to a host's urgent problems. Service calls are delivered via email with messages to help the recipient diagnose the issue. Refer to *12 Service Calls* in the *SSM User Guide* for reference. The diagram shown below indicates that a Setup can include only one Customer, but many Recipients, and any positive or null number of Devices.



12.1 Creating a New Customer

1. Log into SSM Web with the ID and password of the built-in ADMIN account.
2. Go to SSM Main Page > Administration > Service Calls > Customer Management.
3. Click **Add Customer** in the **Commands** area and an Add Customer dialog box appears.
4. Fill in the fields and then click the **Submit** button to add the customer and close this dialog box.

12.2 Creating a New Recipient

1. Log into SSM Web with the ID and password of the built-in ADMIN account.
2. Go to SSM Main Page > Administration > Service Calls > Recipient Management.
3. Click **Add Recipient** in the **Commands** area and an Add Recipient dialog box appears.
4. Fill in the fields and then click the Submit button to add the recipient and close this dialog box.

12.3 Creating a New Site Location

1. Log into SSM Web with the ID and password of the built-in ADMIN account.
2. Go to SSM Main Page > Administration > Service Calls > Site Management.
3. Click **Add Site Location** in the **Commands** area and an Add Site Location dialog box appears.
4. Fill in the fields and then click the **Submit** button to add the site location and close this dialog box.

12.4 Creating a New Setup

1. Log into SSM Web with the ID and password of the built-in ADMIN account.
2. Go to SSM Main Page > Administration > Service Calls > Setup Management.
3. Click **Add Setup** in the **Commands** area and an Add Setup dialog box appears.
4. Fill out the fields and then click the **Submit** button to add the setup and close this dialog box.

12.5 Assigning a Site Location

1. Login to SSM Web with the ID and password of the built-in ADMIN account.
2. Go to SSM Main Page > Administration > Service Calls > Setup Management.
3. Use **[Ctrl]** and **[left mouse click]** to select multiple devices in the working area then click Assign Site Location in the **Commands** area and an Assign Site Location query dialog box appears.
4. Select the site location to be assigned and click the **Submit** button.

12.6 Editing the Triggers

Edit the trigger for devices in a setup, and choose the desired trigger items. When a trigger item is problematic, recipients in the setup are able to receive alerts for it.

1. Log into SSM Web with the ID and password of the built-in ADMIN account.
2. Go to SSM Main Page > Administration > Service Calls > Setup Management.
3. Use **[Ctrl]** and **[left mouse click]** to select multiple devices in the working area then click Edit Trigger in the **Commands** area and the Edit Trigger dialog box appears.
4. Select the boxes in the Override column to apply the current settings to all selected devices.
5. Click the **Submit** button to edit the trigger items.

Note: For Supermicro Service recipients, the trigger types are limited: only Error items are available. Also, all triggers for a device are locked and checked by default.

12.7 Enabling Service Calls

Enable Service Calls when the device is ready to trigger alerts whenever it encounters an error.

1. Log into SSM Web with the ID and password of the built-in ADMIN account.
2. Go to SSM Main Page > Administration > Service Calls > Setup Management.
3. Use **[Ctrl]** and **[left mouse click]** to select multiple devices in the working area then click Enable Service Call in the **Commands** area and an Enable Service Call dialog box appears.
4. Click the Run button to enable the selected devices and close this dialog box.

Note: Enable Service Call only supports the Redfish hosts with the SFT-DCMS-SVC-KEY product key activated.

12.8 Testing the Service Calls function

Test the Service Calls function to pre-check if all settings are complete for a service call.

1. Log into SSM Web with the ID and password of the built-in ADMIN account.
2. Go to SSM Main Page > Administration > Service Calls > Setup Management.
3. Select one or more devices to be tested in the working area.
4. Click Test Service Call in the **Commands** area and a Test Service Call dialog box appears.
5. Click the Run button to test the selected devices and close this dialog box.

Note: It is highly recommended that you click **Test Service Call** to ensure Service Calls settings are complete.

Contacting Supermicro

Headquarters

Address: Super Micro Computer, Inc.
980 Rock Ave.
San Jose, CA 95131 U.S.A.
Tel: +1 (408) 503-8000
Fax: +1 (408) 503-8008
Email: marketing@supermicro.com (General Information)
support@supermicro.com (Technical Support)
Website: www.supermicro.com

Europe

Address: Super Micro Computer B.V.
Het Sterrenbeeld 28, 5215 ML
's-Hertogenbosch, The Netherlands
Tel: +31 (0) 73-6400390
Fax: +31 (0) 73-6416525
Email: sales@supermicro.nl (General Information)
support@supermicro.nl (Technical Support)
rma@supermicro.nl (Customer Support)
Website: www.supermicro.nl

Asia-Pacific

Address: Super Micro Computer, Inc.
3F, No. 150, Jian 1st Rd.
Zhonghe Dist., New Taipei City 235
Taiwan (R.O.C)
Tel: +886-(2) 8226-3990
Fax: +886-(2) 8226-3992
Email: support@supermicro.com.tw
Website: www.supermicro.com.tw