Configure BMC interface (SGF6112, SG6000, SG100, and SG1000)

StorageGRID

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/us-en/storagegrid-117/installconfig/configuring-bmc-interface.html on November 04, 2025. Always check docs.netapp.com for the latest.

Table of Contents

Configure BMC interface (SGF6112, SG6000, SG100, and SG1000) . . . 1
- BMC interface: Overview (SGF6112, SG6000, SG100, and SG1000) . . . 1
- Change admin or root password for BMC interface . . . 1
- Set IP address for BMC management port . . . 2
- Access BMC interface . . . 5
- Configure SNMP settings for BMC . . . 6
- Set up email notifications for BMC alerts . . . 7

Configure BMC interface (SGF6112, SG6000, SG100, and SG1000)

BMC interface: Overview (SGF6112, SG6000, SG100, and SG1000)

The user interface for the baseboard management controller (BMC) on the SGF6112, SG6000, or services appliance provides status information about the hardware and allows you to configure SNMP settings and other options for the appliances.

Use the following procedures in this section to configure the BMC when you install the appliance:

- Change admin or root password for BMC interface
- Set IP address for BMC management port
- Access BMC interface
- Configure SNMP settings
- Set up email notifications for BMC alerts

> If the appliance has already been installed into a grid and is running StorageGRID software, use the following procedures:
>
> - Place the appliance into maintenance mode to access the StorageGRID appliance installer.
> - See Set IP address for BMC management port for information about accessing the BMC interface using the StorageGRID Appliance Installer.

Change admin or root password for BMC interface

For security, you must change the password for the BMC's admin or root user.

Before you begin

The management client is using a supported web browser.

About this task

When you first install the appliance, the BMC uses a default password for the admin or root user. You must change the password for the admin or root user to secure your system.

The default user depends on when you installed your StorageGRID appliance. The default user is **admin** for new installations and **root** for older installations.

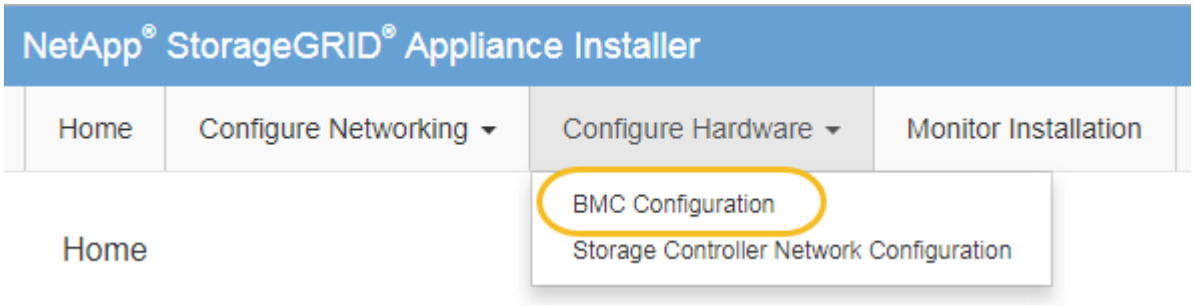
Steps

1. From the client, enter the URL for the StorageGRID Appliance Installer:
   `https://Appliance_IP:8443`

   For *`Appliance_IP`*, use the IP address for the appliance on any StorageGRID network.

   The StorageGRID Appliance Installer Home page appears.

2. Select **Configure Hardware** > **BMC Configuration**.



   The Baseboard Management Controller Configuration page appears.

3. Enter a new password for the admin or root account in the two fields provided.
4. Click **Save**.

Set IP address for BMC management port

Before you can access the BMC interface, configure the IP address for the BMC management port on the SGF6112, SG6000-CN controller, or services appliances.

If you are using ConfigBuilder to generate a JSON file, you can configure IP addresses automatically. See Automate appliance installation and configuration.

Before you begin

- The management client is using a supported web browser.
- You are using any management client that can connect to a StorageGRID network.
- The BMC management port is connected to the management network you plan to use.

SG6112

SG6000

SG1000

SG100

About this task

For support purposes, the BMC management port allows low-level hardware access.

> You should only connect this port to a secure, trusted, internal management network. If no such network is available, leave the BMC port unconnected or blocked, unless a BMC connection is requested by technical support.

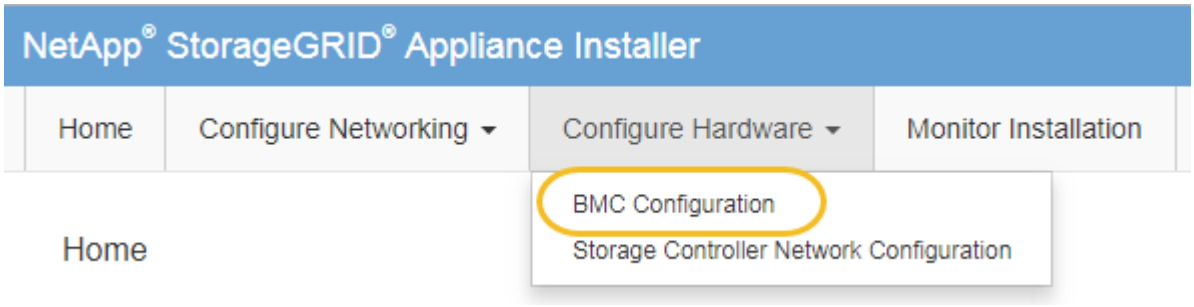
Steps

1. From the client, enter the URL for the StorageGRID Appliance Installer:
   `https://Appliance_IP:8443`

   For `Appliance_IP`, use the IP address for the appliance on any StorageGRID network.

   The StorageGRID Appliance Installer Home page appears.

2. Select **Configure Hardware** > **BMC Configuration**.

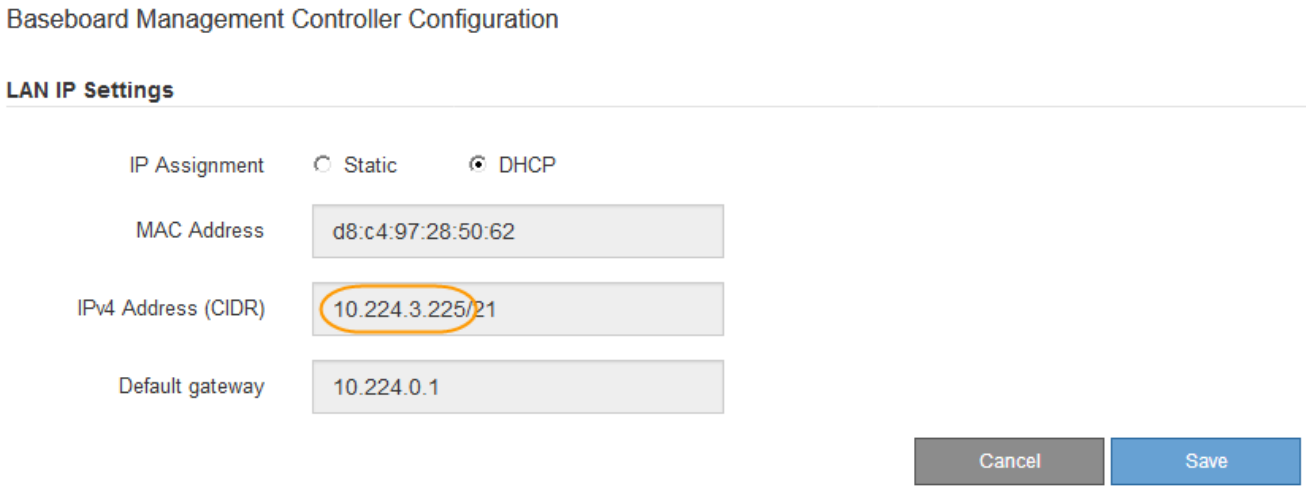


   The Baseboard Management Controller Configuration page appears.

3. Make a note of the IPv4 address that is automatically displayed.

   DHCP is the default method for assigning an IP address to this port.

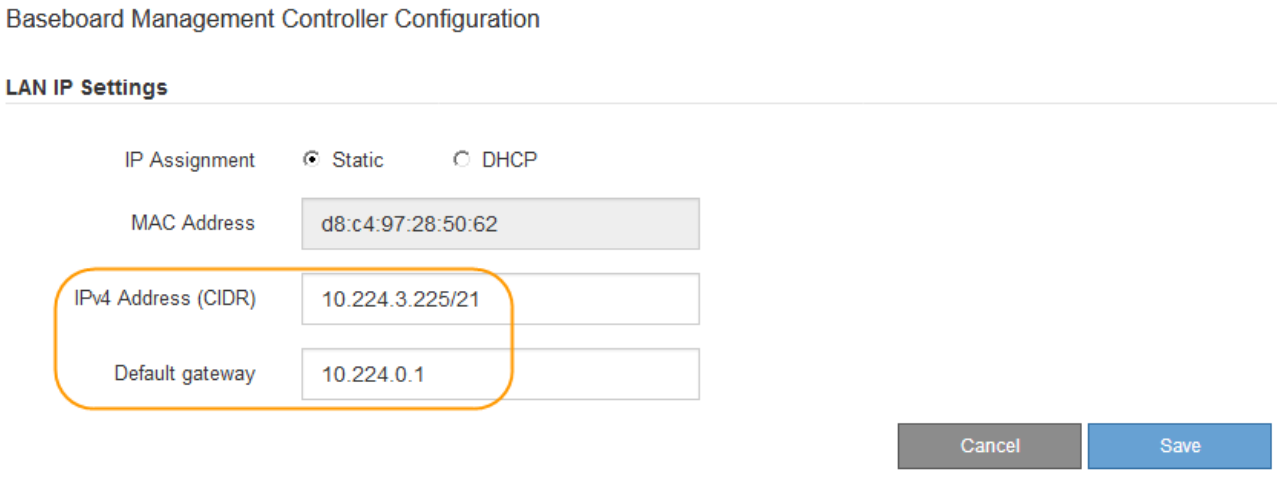
   > It might take a few minutes for the DHCP values to appear.



4. Optionally, set a static IP address for the BMC management port.

   > You should either assign a static IP for the BMC management port or assign a permanent lease for the address on the DHCP server.

   a. Select **Static**.
   b. Enter the IPv4 address, using CIDR notation.
   c. Enter the default gateway.



   d. Click **Save**.

      It might take a few minutes for your changes to be applied.

Access BMC interface

You can access the BMC interface using the DHCP or static IP address for the BMC management port on the following appliance models:

- SGF6112
- SG6000
- SG1000
- SG100

Before you begin

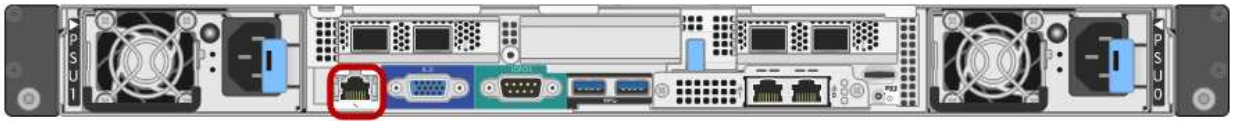
- The management client is using a supported web browser.
- The BMC management port on the appliance is connected to the management network you plan to use.

SGF6112

SG6000

SG1000

SG100



Steps

1. Enter the URL for the BMC interface:
   `https://BMC_Port_IP`

   For *`BMC_Port_IP`*, use the DHCP or static IP address for the BMC management port.

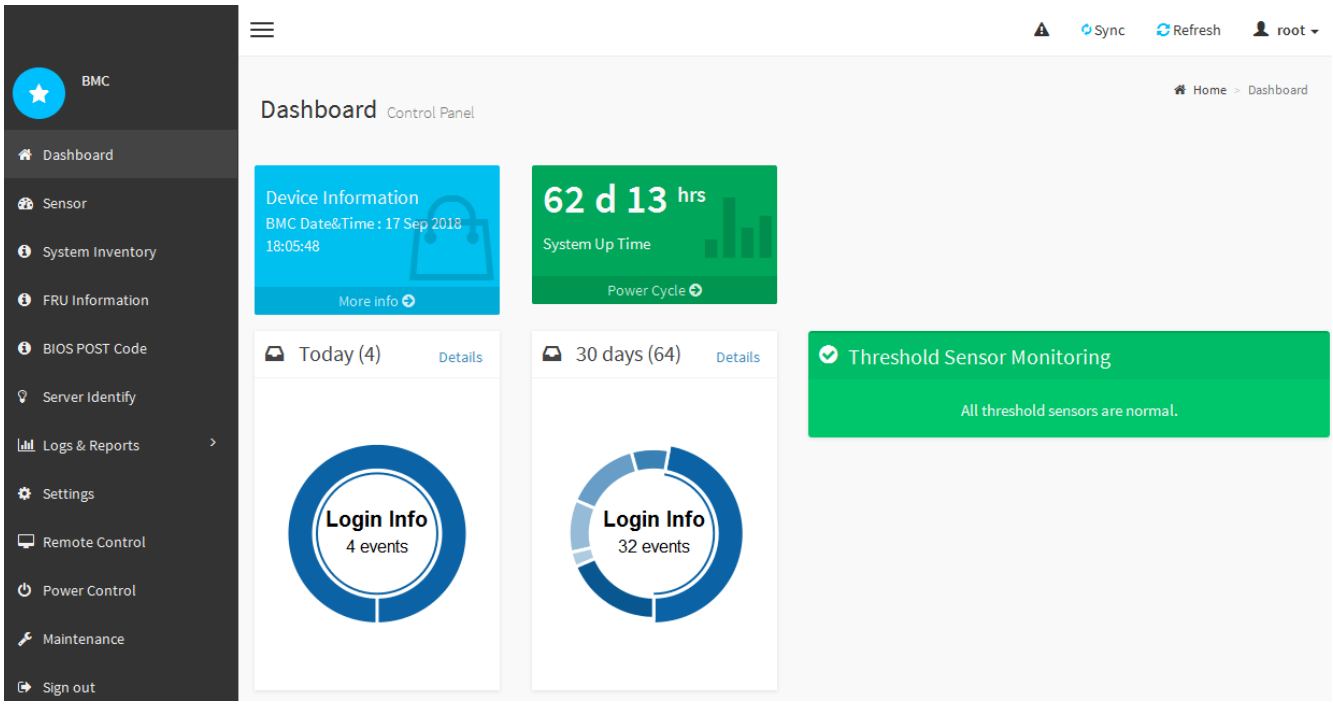
   The BMC sign-in page appears.

If you haven't yet configured `BMC_Port_IP`, follow the instructions in Configure BMC interface. If you are unable to follow that procedure due to a hardware problem, and have not yet configured a BMC IP address, you might still be able to access the BMC. By default, the BMC obtains an IP address using DHCP. If DHCP is enabled on the BMC network, your network administrator can provide the IP address assigned to the BMC MAC, which is printed on the label on the front of the appliance. If DHCP is not enabled on the BMC network, the BMC will not respond after a few minutes and assign itself the default static IP `192.168.0.120`. You might need to connect your laptop directly to the BMC port, and change the networking setting to assign your laptop an IP such as `192.168.0.200/24`, in order to browse to `192.168.0.120`.

2. Enter the admin or root username and password, using the password you set when you changed the default root password:

The default user depends on when you installed your StorageGRID appliance. The default user is **admin** for new installations and **root** for older installations.

3. Select **Sign me in**.



4. Optionally, create additional users by selecting **Settings** > **User Management** and clicking on any "disabled" user.

When users sign in for the first time, they might be prompted to change their password for increased security.

Configure SNMP settings for BMC

If you are familiar with configuring SNMP for hardware, you can use the BMC interface to configure the SNMP settings for the SGF6112, SG6000, and services appliances. You can provide secure community strings, enable SNMP Trap, and specify up to five SNMP

destinations.

Before you begin

- You know how to access the BMC dashboard.
- You have experience in configuring SNMP settings for SNMPv1-v2c equipment.

> BMC settings made by this procedure might not be preserved if the appliance fails and has to be replaced. Make sure you have a record of all settings you have applied, so they can be easily reapplied after a hardware replacement if necessary.

Steps

1. From the BMC dashboard, select **Settings** > **SNMP Settings**.
2. On the SNMP Settings page, select **Enable SNMP V1/V2**, and then provide a Read-Only Community String and a Read-Write Community String.

   The Read-Only Community String is like a user ID or password. You should change this value to prevent intruders from getting information about your network setup. The Read-Write Community String protects the device against unauthorized changes.

3. Optionally, select **Enable Trap**, and enter the required information.

   > Enter the Destination IP for each SNMP trap using an IP address. Fully qualified domain names aren’t supported.

   Enable traps if you want the appliance to send immediate notifications to an SNMP console when it is in an unusual state. Depending on the device, traps might indicate hardware failures of various components, link up/down conditions, temperature thresholds being exceeded, or high traffic.

4. Optionally, click **Send Test Trap** to test your settings.
5. If the settings are correct, click **Save**.

Set up email notifications for BMC alerts

If you want email notifications to be sent when alerts occur, use the BMC interface to configure SMTP settings, users, LAN destinations, alert policies, and event filters.

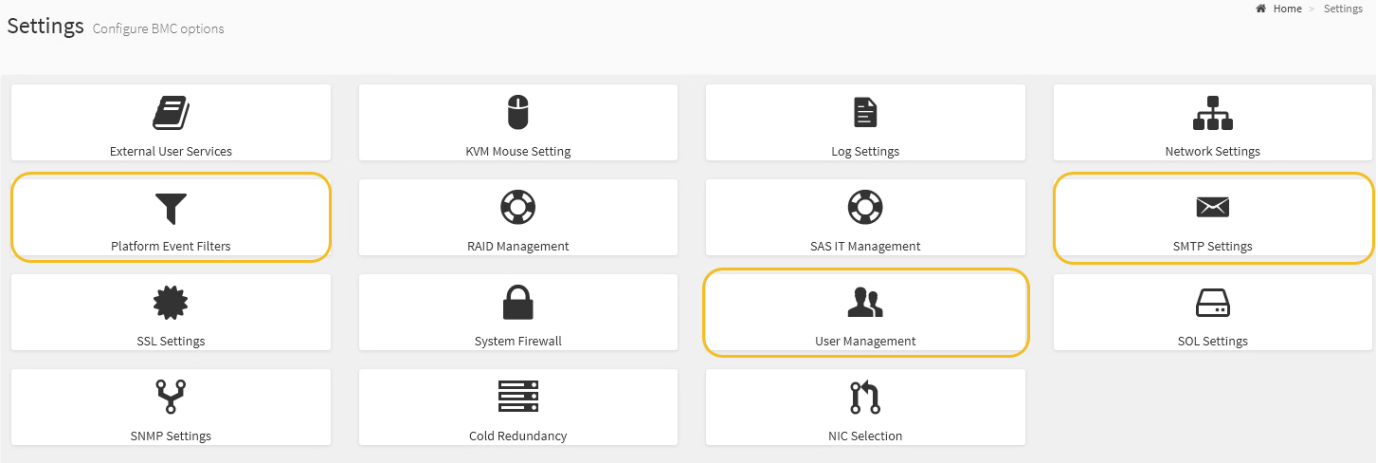
> BMC settings made by this procedure might not be preserved if the SG6000-CN controller or services appliance fails and has to be replaced. Make sure you have a record of all settings you have applied, so they can be easily reapplied after a hardware replacement if necessary.

Before you begin

You know how to access the BMC dashboard.

About this task

In the BMC interface, you use the **SMTP Settings**, **User Management**, and **Platform Event Filters** options on the Settings page to configure email notifications.



Steps

1. Configure SNMP settings for BMC.
   a. Select **Settings** > **SMTP Settings**.
   b. For Sender Email ID, enter a valid email address.

      This email address is provided as the From address when the BMC sends email.

2. Set up users to receive alerts.
   a. From the BMC dashboard, select **Settings** > **User Management**.
   b. Add at least one user to receive alert notifications.

      The email address you configure for a user is the address the BMC sends alert notifications to. For example, you could add a generic user, such as “notification-user,” and use the email address of a technical support team email distribution list.

3. Configure the LAN destination for alerts.
   a. Select **Settings** > **Platform Event Filters** > **LAN Destinations**.
   b. Configure at least one LAN destination.
      - Select **Email** as the Destination Type.
      - For BMC Username, select a user name that you added earlier.
      - If you added multiple users and want all of them to receive notification emails, add a LAN Destination for each user.
   c. Send a test alert.
4. Configure alert policies so you can define when and where the BMC sends alerts.
   a. Select **Settings** > **Platform Event Filters** > **Alert Policies**.
   b. Configure at least one alert policy for each LAN destination.
      - For Policy Group Number, select **1**.
      - For Policy Action, select **Always send alert to this destination**.
      - For LAN Channel, select **1**.
      - In the Destination Selector, select the LAN destination for the policy.
5. Configure event filters to direct alerts for different event types to the appropriate users.

a. Select **Settings** > **Platform Event Filters** > **Event Filters**.

b. For Alert Policy Group Number, enter **1**.

c. Create filters for every event you want the Alert Policy Group to be notified about.

   - You can create event filters for power actions, specific sensor events, or all events.
   - If you are uncertain which events to monitor, select **All Sensors** for Sensor Type and **All Events** for Event Options. If you receive unwanted notifications, you can change your selections later.

Copyright information

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.