Set up hardware

StorageGRID

NetApp
November 04, 2025

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

Table of Contents

Set up hardware . . . 1
- Set up hardware: Overview . . . 1
  - Configure required network connections . . . 1
  - Additional configuration that might be required . . . 1
  - Optional configuration . . . 1
- Configure StorageGRID connections . . . 1
  - Access StorageGRID Appliance Installer . . . 2
  - Verify and upgrade StorageGRID Appliance Installer version . . . 8
  - Configure network links . . . 9
  - Configure StorageGRID IP addresses . . . 20
  - Verify network connections . . . 25
  - Verify port-level network connections . . . 26
  - Configure SANtricity System Manager (SG6000 and SG5700) . . . 29
- Configure BMC interface (SGF6112, SG6000, SG100, and SG1000) . . . 36
  - BMC interface: Overview (SGF6112, SG6000, SG100, and SG1000) . . . 36
  - Change admin or root password for BMC interface . . . 36
  - Set IP address for BMC management port . . . 37
  - Access BMC interface . . . 40
  - Configure SNMP settings for BMC . . . 41
  - Set up email notifications for BMC alerts . . . 42
- Optional: Enable node encryption . . . 44
- Optional: Change RAID mode . . . 46
- Optional: Remap network ports for appliance . . . 47

Set up hardware

Set up hardware: Overview

After applying power to the appliance, you configure the network connections that will be used by StorageGRID.

Configure required network connections

For all appliances, you perform several tasks to configure required network connections such as:

- Access the Appliance Installer
- Configure network links
- Verify port-level network connections

Additional configuration that might be required

Depending upon which appliance types you are configuring, additional hardware configuration might be required.

SANtricity System Manager

For SG6000 and SG5700, you configure SANtricity System Manager. The SANtricity software is used to monitor the hardware for these appliances.

BMC interface

The following appliances have a BMC interface that must be configured:

- SGF6112
- SG6000
- SG1000
- SG100

Optional configuration

- Storage appliances
  - Configure SANtricity System Manager (SG6000 and SG5700) the software you will use to monitor the hardware
  - Change the RAID mode
- Services appliances
  - Access the BMC interface for the SG100 and SG1000 and the SG6000-CN controller

Configure StorageGRID connections

Access StorageGRID Appliance Installer

You must access the StorageGRID Appliance Installer to verify the installer version and configure the connections between the appliance and the three StorageGRID networks: the Grid Network, the Admin Network (optional), and the Client Network (optional).

Before you begin

- You are using any management client that can connect to the StorageGRID Admin Network, or you have a service laptop.
- The client or service laptop has a supported web browser.
- The services appliance or storage appliance controller is connected to all of the StorageGRID networks you plan to use.
- You know the IP address, gateway, and subnet for the services appliance or storage appliance controller on these networks.
- You have configured the network switches you plan to use.

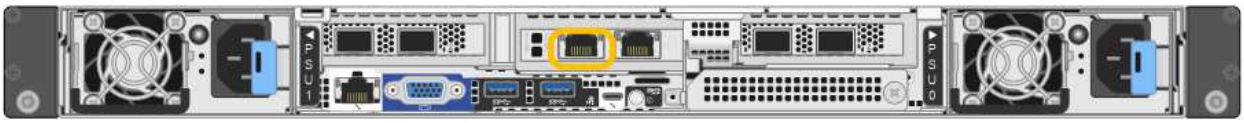
About this task

To initially access the StorageGRID Appliance Installer, you can use the DHCP-assigned IP address for the Admin Network port on the services appliance or storage appliance controller (assuming it is connected to the Admin Network), or you can connect a service laptop directly to the services appliance or storage appliance controller.

Steps

1. If possible, use the DHCP address for the Admin Network port on the services appliance or storage appliance controller. The Admin Network port is highlighted in the following figure. (Use the IP address on the Grid Network if the Admin Network is not connected.)

SGF6112



SG6000-CN

E5700SG

For the E5700SG, you can do either of the following:

- Look at the seven-segment display on the E5700SG controller. If management port 1 and 10/25-GbE ports 2 and 4 on the E5700SG controller are connected to networks with DHCP servers, the controller attempts to obtain dynamically assigned IP addresses when you power on the enclosure. After the controller has completed the power-on process, its seven-segment display shows **HO**, followed by a repeating sequence of two numbers.

  ```
  HO -- IP address for Admin Network -- IP address for Grid Network
  HO
  ```

  In the sequence:

  - The first set of numbers is the DHCP address for the appliance Storage Node on the Admin Network, if it is connected. This IP address is assigned to management port 1 on the E5700SG controller.
  - The second set of numbers is the DHCP address for the appliance Storage Node on the Grid Network. This IP address is assigned to 10/25-GbE ports 2 and 4 when you first apply power to the appliance.

    If an IP address could not be assigned using DHCP, 0.0.0.0 is displayed.

SG100

SG1000

a. Locate the MAC address label on the front of the services appliance or storage appliance, and determine the MAC address for the Admin Network port.

The MAC address label lists the MAC address for the BMC management port.

To determine the MAC address for the Admin Network port, add **2** to the hexadecimal number on the label. For example, if the MAC address on the label ends in **09**, the MAC address for the Admin Port would end in **0B**. If the MAC address on the label ends in **(*y*)FF**, the MAC address for the Admin Port would end in **(*y*+1)01**. You can easily make this calculation by opening Calculator in Windows, setting it to Programmer mode, selecting Hex, typing the MAC address, then typing **+ 2 =**.

b. Provide the MAC address to your network administrator, so they can look up the DHCP address for the appliance on the Admin Network.

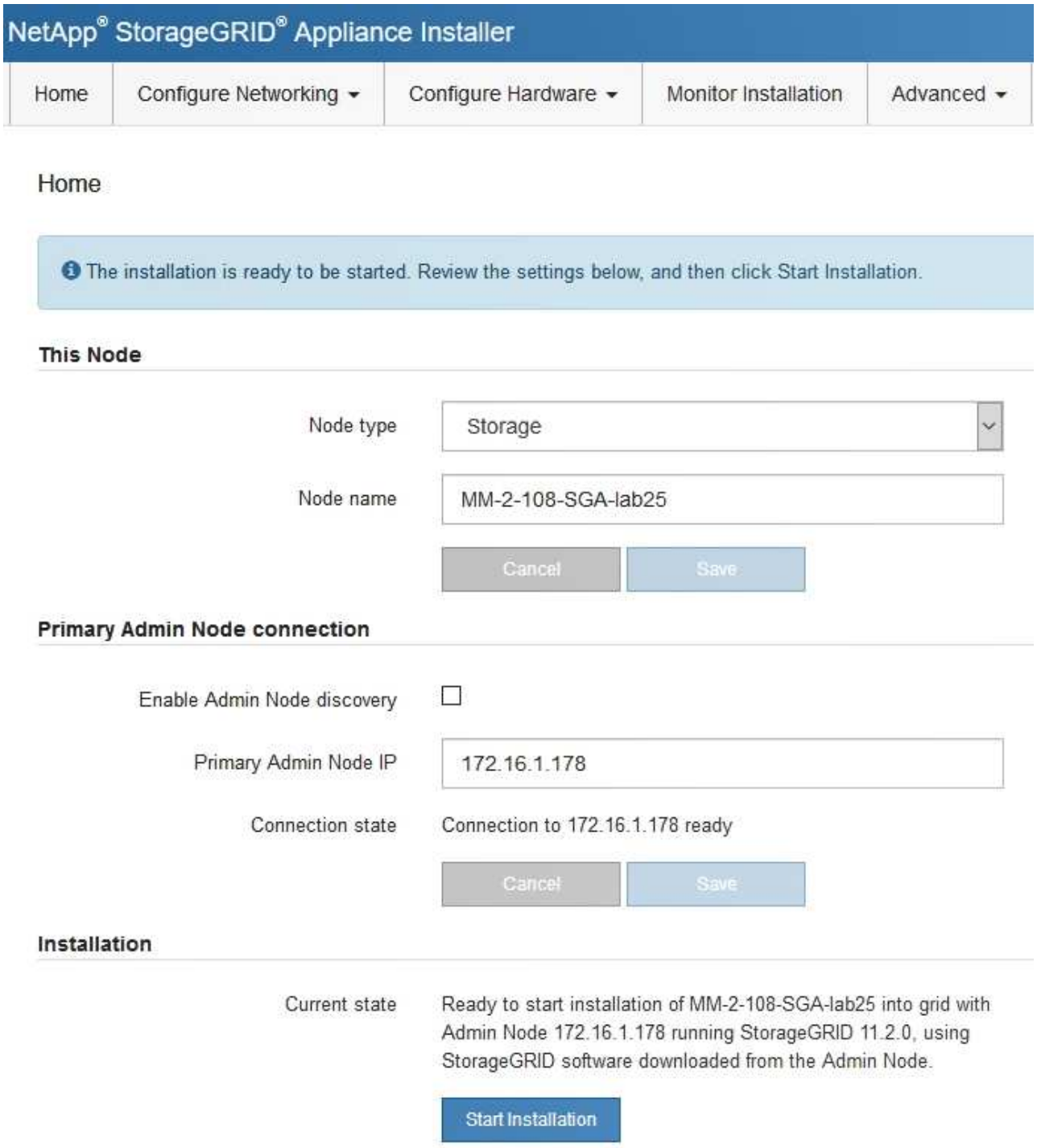
c. From the client, enter this URL for the StorageGRID Appliance Installer:
`https://Appliance_IP:8443`

For *`Appliance_IP`*, use the DHCP address (use the IP address for the Admin Network if you have it).

d. If you are prompted with a security alert, view and install the certificate using the browser's installation wizard.

The alert will not appear the next time you access this URL.

The StorageGRID Appliance Installer Home page appears. The information and messages shown when you first access this page depend on how your appliance is currently connected to StorageGRID networks. Error messages might appear that will be resolved in later steps.



2. If you can't obtain an IP address using DHCP, you can use a link-local connection.

SGF6112

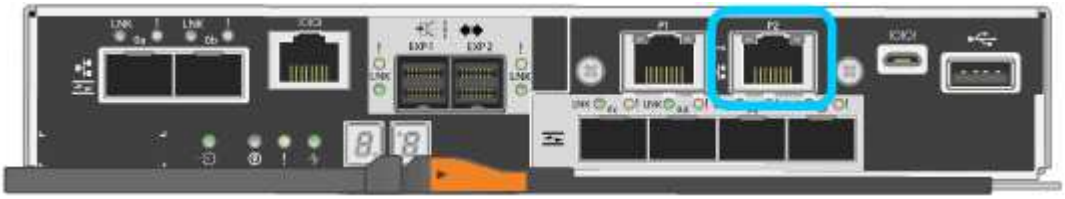
Connect a service laptop directly to the rightmost RJ-45 port on the appliance, using an Ethernet cable.

SG6000-CN

Connect a service laptop directly to the rightmost RJ-45 port on the SG6000-CN controller, using an Ethernet cable.

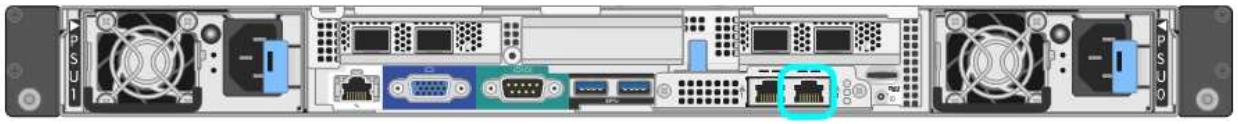
E5700SG

Connect the service laptop to management port 2 on the E5700SG controller, using an Ethernet cable.



SG100

Connect a service laptop directly to the rightmost RJ-45 port on the services appliance, using an Ethernet cable.



SG1000

Connect a service laptop directly to the rightmost RJ-45 port on the services appliance, using an Ethernet cable.

a. Open a web browser on the service laptop.

b. Enter this URL for the StorageGRID Appliance Installer:
`https://169.254.0.1:8443`

The StorageGRID Appliance Installer Home page appears. The information and messages shown when you first access this page depend on how your appliance is currently connected to StorageGRID networks. Error messages might appear that will be resolved in later steps.

If you can't access the Home page over a link-local connection, configure the service laptop IP address as `169.254.0.2`, and try again.

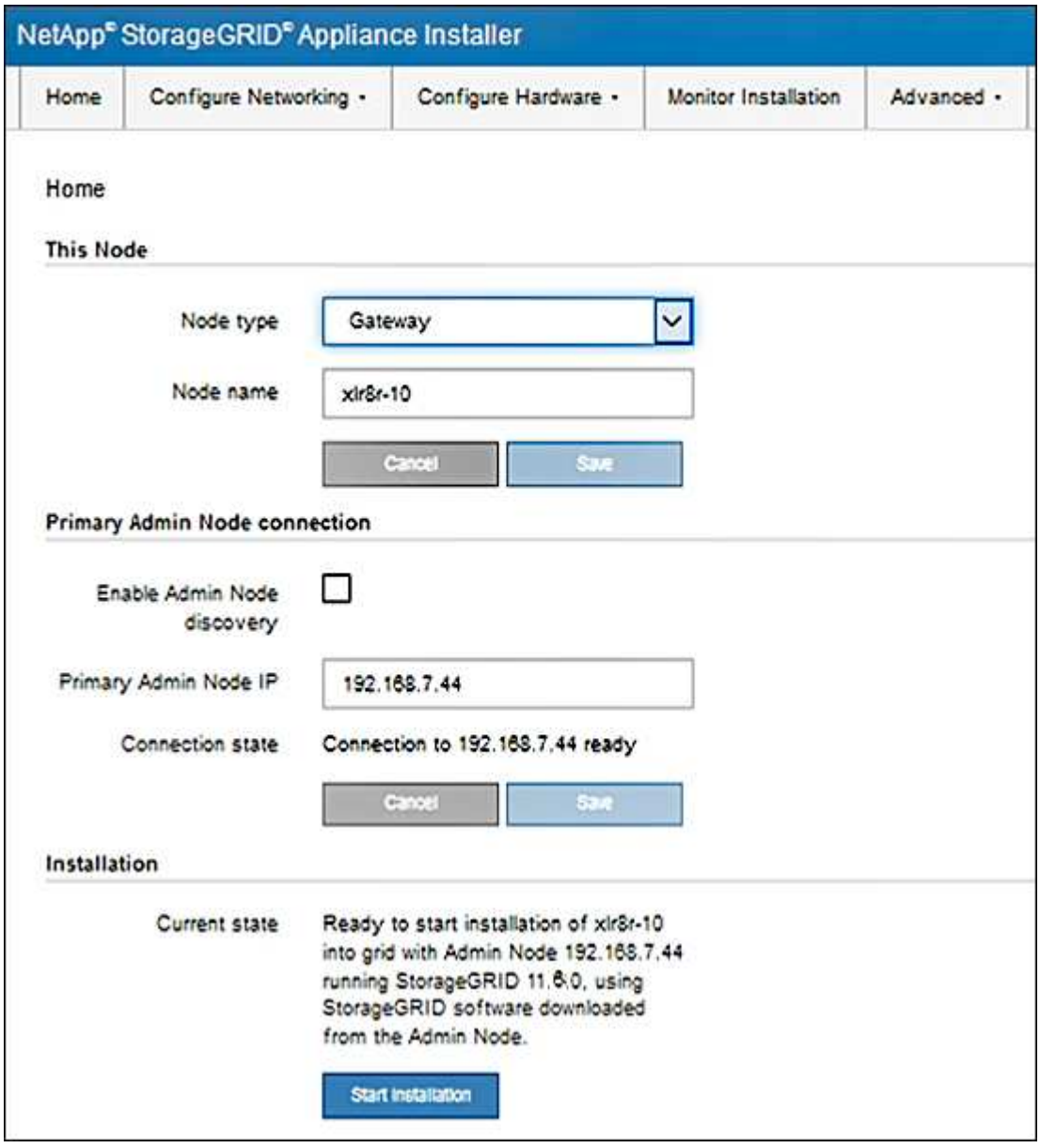
After you finish

After accessing the StorageGRID Appliance Installer:

- Verify that the StorageGRID Appliance Installer version on the appliance matches the software version installed on your StorageGRID system. Upgrade StorageGRID Appliance Installer, if necessary.

  Verify and upgrade StorageGRID Appliance Installer version

- Review any messages displayed on the StorageGRID Appliance Installer Home page and configure the link configuration and the IP configuration, as required.



Verify and upgrade StorageGRID Appliance Installer version

The StorageGRID Appliance Installer version on the appliance must match the software version installed on your StorageGRID system to ensure that all StorageGRID features are supported.

Before you begin

You have accessed the StorageGRID Appliance Installer.

About this task

StorageGRID appliances come from the factory preinstalled with the StorageGRID Appliance Installer. If you are adding an appliance to a recently upgraded StorageGRID system, you might need to manually upgrade the StorageGRID Appliance Installer before installing the appliance as a new node.

The StorageGRID Appliance Installer automatically upgrades when you upgrade to a new StorageGRID version. You don't need to upgrade the StorageGRID Appliance Installer on installed appliance nodes. This procedure is only required when you are installing an appliance that contains an earlier version of the StorageGRID Appliance Installer.

Steps

1. From the StorageGRID Appliance Installer, select **Advanced** > **Upgrade Firmware**.
2. Compare the Current Firmware version to the software version installed on your StorageGRID system. (From the top of the Grid Manager, select the help icon and select **About**.)

   The second digit in the two versions should match. For example, if your StorageGRID system is running version 11.**6**.*x*.*y*, the StorageGRID Appliance Installer version should be 3.**6**.*z*.

3. If the appliance has a down-level version of the StorageGRID Appliance Installer, go to NetApp Downloads: StorageGRID Appliance.

   Sign in with the username and password for your NetApp account.

4. Download the appropriate version of the **Support file for StorageGRID Appliances** and the corresponding checksum file.

   The Support file for StorageGRID appliances is a `.zip` archive that contains the current and previous firmware versions for all StorageGRID appliance models.

   After downloading the Support file for StorageGRID appliances, extract the `.zip` archive and see the README file for important information about installing the StorageGRID Appliance Installer.

5. Follow the instructions on the Upgrade Firmware page of your StorageGRID Appliance Installer to perform these steps:
   a. Upload the appropriate support file (firmware image) for your controller type. Some firmware versions also require uploading a checksum file. If you are prompted for a checksum file, it can also be found in the Support file for StorageGRID Appliances.
   b. Upgrade the inactive partition.
   c. Reboot and swap partitions.
   d. Upload the appropriate support file (firmware image) again for your controller type. Some firmware versions also require uploading a checksum file. If you are prompted for a checksum file, it can also be found in the Support file for StorageGRID Appliances.

e. Upgrade the second (inactive) partition.

Related information

Accessing StorageGRID Appliance Installer

Configure network links

You can configure network links for the ports used to connect the appliance to the Grid Network, the Client Network, and the Admin Network. You can set the link speed as well as the port and network bond modes.

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

Before you begin

- You have obtained the additional equipment required for your cable type and link speed.
- You have installed the correct transceivers in the ports, based on the link speed you plan to use.
- You have connected the network ports to switches that support your chosen speed.

If you plan to use Aggregate port bond mode, LACP network bond mode, or VLAN tagging:

- You have connected the network ports on the appliance to switches that can support VLAN and LACP.
- If multiple switches are participating in the LACP bond, the switches support multi-chassis link aggregation groups (MLAG), or equivalent.
- You understand how to configure the switches to use VLAN, LACP, and MLAG or equivalent.
- You know the unique VLAN tag to use for each network. This VLAN tag will be added to each network packet to ensure that network traffic is routed to the correct network.

About this task

You only need to configure the settings on the Link Configuration page if you want to use a non-default setting.

The LACP transmit hash policy is layer2+3.

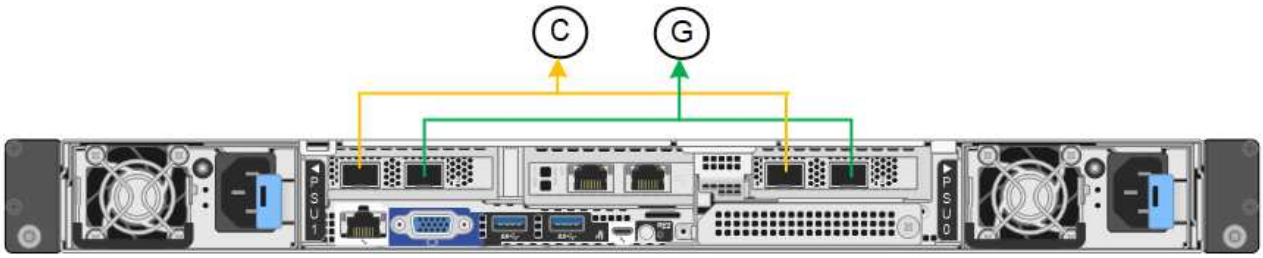
The figures and tables summarize the options for the port bond mode and network bond mode for each appliance. See the following for more information:

- Port bond modes (SGF6112)
- Port bond modes (SG6000-CN)
- Port bond modes (E5700SG)
- Port bond modes (SG1000 and SG100)

SGF6112

Fixed port bond mode (default)

The figure shows how the four network ports are bonded in fixed port bond mode (default configuration).



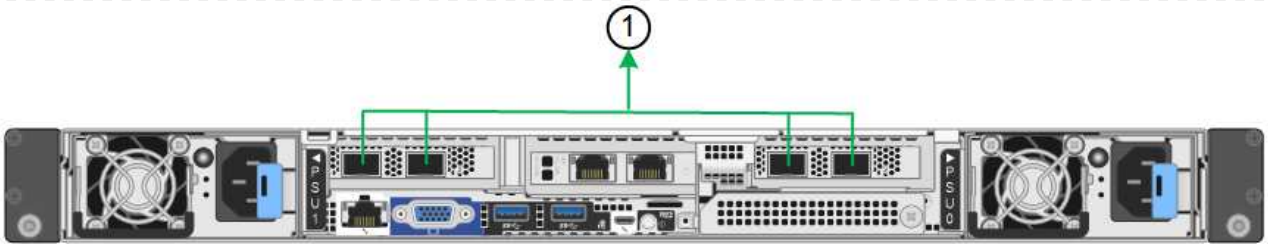
Callout	Which ports are bonded
C	Ports 1 and 3 are bonded together for the Client Network, if this network is used.
G	Ports 2 and 4 are bonded together for the Grid Network.

The table summarizes the options for configuring the network ports. You only need to configure the settings on the Link Configuration page if you want to use a non-default setting.

Network bond mode	Client Network disabled (default)	Client Network enabled
Active-Backup (default)	• Ports 2 and 4 use an active-backup bond for the Grid Network. • Ports 1 and 3 aren't used. • A VLAN tag is optional.	• Ports 2 and 4 use an active-backup bond for the Grid Network. • Ports 1 and 3 use an active-backup bond for the Client Network. • VLAN tags can be specified for both networks for the convenience of the network administrator.
LACP (802.3ad)	• Ports 2 and 4 use an LACP bond for the Grid Network. • Ports 1 and 3 aren't used. • A VLAN tag is optional.	• Ports 2 and 4 use an LACP bond for the Grid Network. • Ports 1 and 3 use an LACP bond for the Client Network. • VLAN tags can be specified for both networks for the convenience of the network administrator.

Aggregate port bond mode

The figure shows how the four network ports are bonded in aggregate port bond mode.



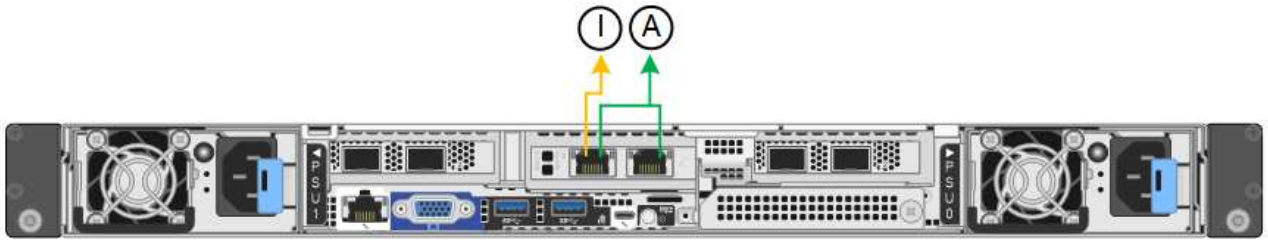
Callout	Which ports are bonded
1	All four ports are grouped in a single LACP bond, allowing all ports to be used for Grid Network and Client Network traffic.

The table summarizes the options for configuring the network ports. You only need to configure the settings on the Link Configuration page if you want to use a non-default setting.

Network bond mode	Client Network disabled (default)	Client Network enabled
LACP (802.3ad) only	• Ports 1-4 use a single LACP bond for the Grid Network. • A single VLAN tag identifies Grid Network packets.	• Ports 1-4 use a single LACP bond for the Grid Network and the Client Network. • Two VLAN tags allow Grid Network packets to be segregated from Client Network packets.

Active-Backup network bond mode for management ports

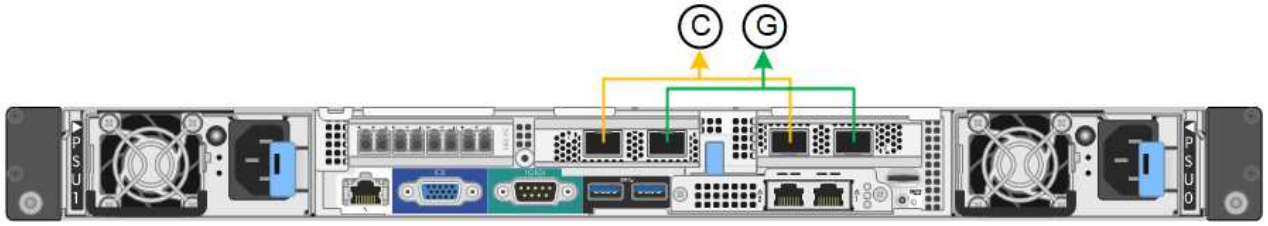
This figure shows how the two 1-GbE management ports on the SGF6112 are bonded in Active-Backup network bond mode for the Admin Network.



SG6000

Fixed port bond mode (default)

This figure shows how the four network ports are bonded in fixed port bond mode (default configuration)



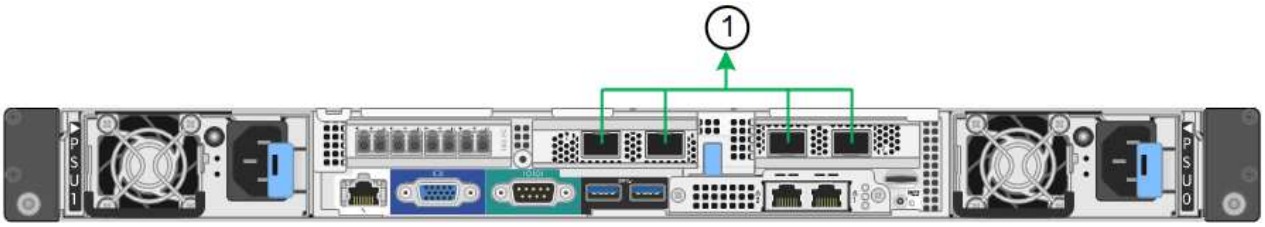
Callout	Which ports are bonded
C	Ports 1 and 3 are bonded together for the Client Network, if this network is used.
G	Ports 2 and 4 are bonded together for the Grid Network.

The table summarizes the options for configuring the network ports. You only need to configure the settings on the Link Configuration page if you want to use a non-default setting.

Network bond mode	Client Network disabled (default)	Client Network enabled
Active-Backup (default)	• Ports 2 and 4 use an active-backup bond for the Grid Network. • Ports 1 and 3 aren't used. • A VLAN tag is optional.	• Ports 2 and 4 use an active-backup bond for the Grid Network. • Ports 1 and 3 use an active-backup bond for the Client Network. • VLAN tags can be specified for both networks for the convenience of the network administrator.
LACP (802.3ad)	• Ports 2 and 4 use an LACP bond for the Grid Network. • Ports 1 and 3 aren't used. • A VLAN tag is optional.	• Ports 2 and 4 use an LACP bond for the Grid Network. • Ports 1 and 3 use an LACP bond for the Client Network. • VLAN tags can be specified for both networks for the convenience of the network administrator.

Aggregate port bond mode

This figure shows how the four network ports are bonded in aggregate port bond mode.



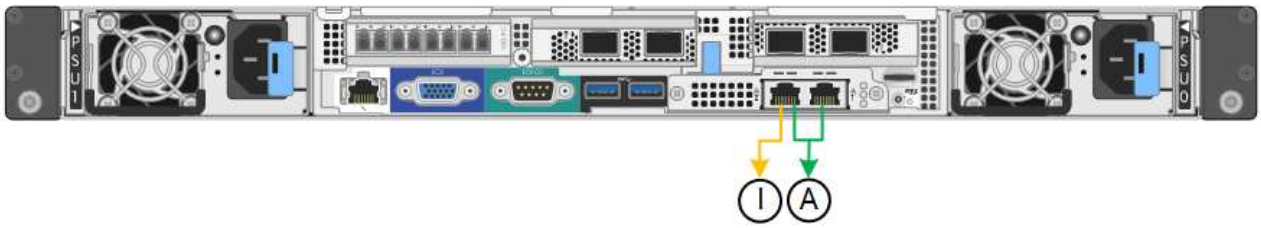
Callout	Which ports are bonded
1	All four ports are grouped in a single LACP bond, allowing all ports to be used for Grid Network and Client Network traffic.

The table summarizes the options for configuring the network ports. You only need to configure the settings on the Link Configuration page if you want to use a non-default setting.

Network bond mode	Client Network disabled (default)	Client Network enabled
LACP (802.3ad) only	• Ports 1-4 use a single LACP bond for the Grid Network. • A single VLAN tag identifies Grid Network packets.	• Ports 1-4 use a single LACP bond for the Grid Network and the Client Network. • Two VLAN tags allow Grid Network packets to be segregated from Client Network packets.

Active-Backup network bond mode for management ports

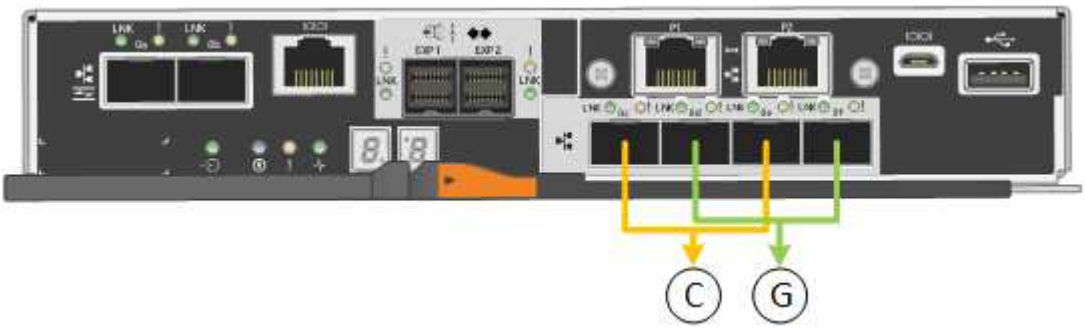
This figure shows how the two 1-GbE management ports on the SG6000-CN controller are bonded in Active-Backup network bond mode for the Admin Network.



SG5700

Fixed port bond mode (default)

This figure shows how the four 10/25-GbE ports are bonded in Fixed port bond mode (default configuration).



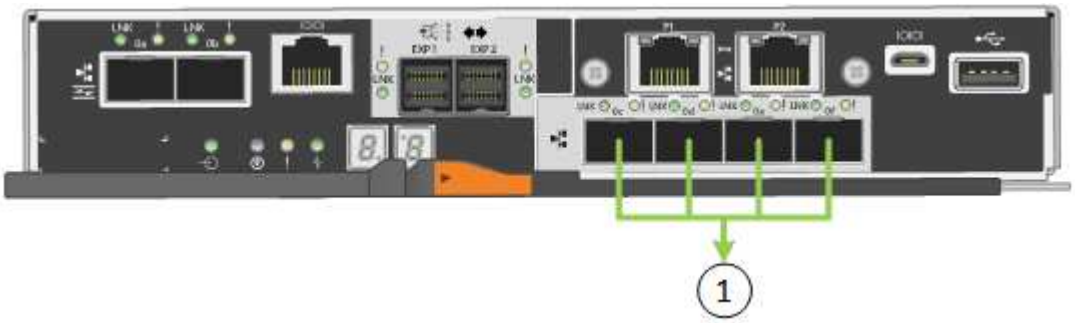
Callout	Which ports are bonded
C	Ports 1 and 3 are bonded together for the Client Network, if this network is used.
G	Ports 2 and 4 are bonded together for the Grid Network.

The table summarizes the options for configuring the four 10/25-GbE ports. You only need to configure the settings on the Link Configuration page if you want to use a non-default setting.

Network bond mode	Client Network disabled (default)	Client Network enabled
Active-Backup (default)	• Ports 2 and 4 use an active-backup bond for the Grid Network. • Ports 1 and 3 aren't used. • A VLAN tag is optional.	• Ports 2 and 4 use an active-backup bond for the Grid Network. • Ports 1 and 3 use an active-backup bond for the Client Network. • VLAN tags can be specified for both networks for the convenience of the network administrator.
LACP (802.3ad)	• Ports 2 and 4 use an LACP bond for the Grid Network. • Ports 1 and 3 aren't used. • A VLAN tag is optional.	• Ports 2 and 4 use an LACP bond for the Grid Network. • Ports 1 and 3 use an LACP bond for the Client Network. • VLAN tags can be specified for both networks for the convenience of the network administrator.

Aggregate port bond mode

This figure shows how the four 10/25-GbE ports are bonded in Aggregate port bond mode.



Callout	Which ports are bonded
1	All four ports are grouped in a single LACP bond, allowing all ports to be used for Grid Network and Client Network traffic.

The table summarizes the options for configuring the four 10/25-GbE ports. You only need to configure the settings on the Link Configuration page if you want to use a non-default setting.

Network bond mode	Client Network disabled (default)	Client Network enabled
LACP (802.3ad) only	• Ports 1-4 use a single LACP bond for the Grid Network. • A single VLAN tag identifies Grid Network packets.	• Ports 1-4 use a single LACP bond for the Grid Network and the Client Network. • Two VLAN tags allow Grid Network packets to be segregated from Client Network packets.

Active-Backup network bond mode for management ports

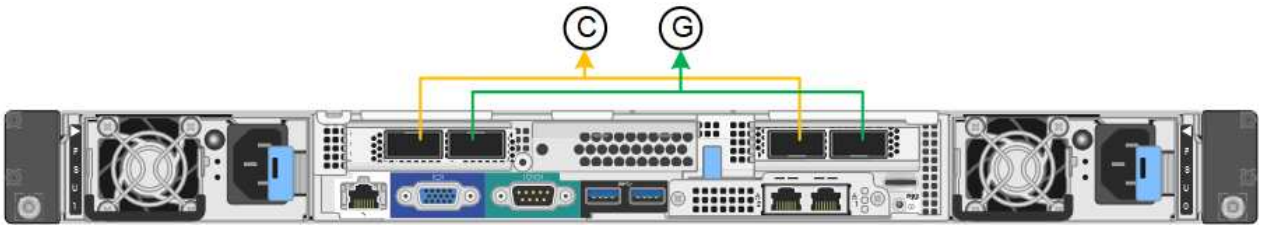
This figure shows how the two 1-GbE management ports on the E5700SG controller are bonded in Active-Backup network bond mode for the Admin Network.

SG100 and SG1000

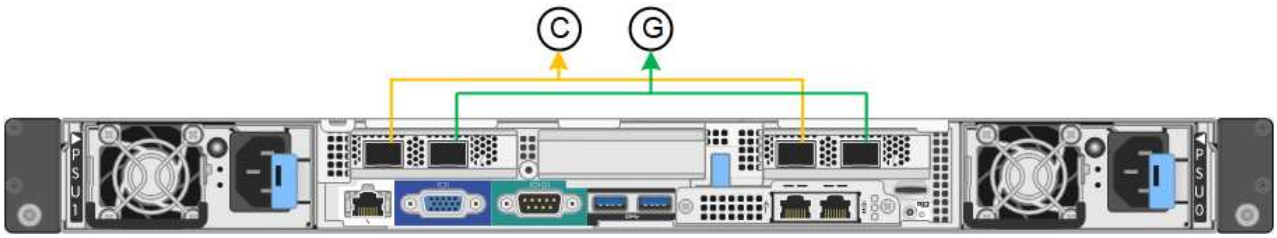
Fixed port bond mode (default)

The figures show how the four network ports on the SG1000 or SG100 are bonded in fixed port bond mode (default configuration).

SG1000:



SG100:



Callout	Which ports are bonded
C	Ports 1 and 3 are bonded together for the Client Network, if this network is used.
G	Ports 2 and 4 are bonded together for the Grid Network.

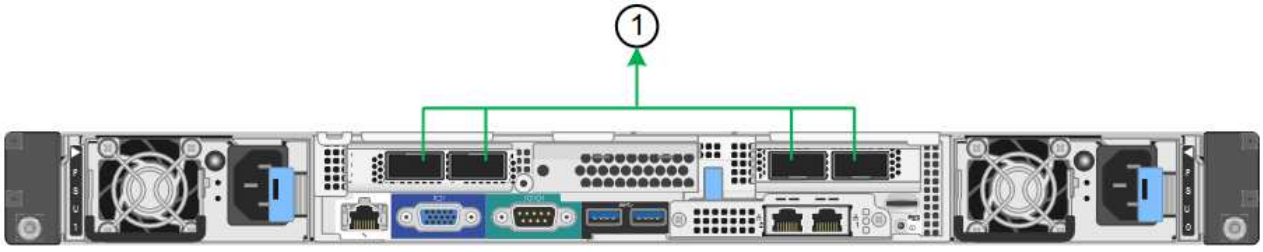
The table summarizes the options for configuring the four network ports. You only need to configure the settings on the Link Configuration page if you want to use a non-default setting.

Network bond mode	Client Network disabled (default)	Client Network enabled
Active-Backup (default)	• Ports 2 and 4 use an active-backup bond for the Grid Network. • Ports 1 and 3 aren't used. • A VLAN tag is optional.	• Ports 2 and 4 use an active-backup bond for the Grid Network. • Ports 1 and 3 use an active-backup bond for the Client Network. • VLAN tags can be specified for both networks for the convenience of the network administrator.
LACP (802.3ad)	• Ports 2 and 4 use an LACP bond for the Grid Network. • Ports 1 and 3 aren't used. • A VLAN tag is optional.	• Ports 2 and 4 use an LACP bond for the Grid Network. • Ports 1 and 3 use an LACP bond for the Client Network. • VLAN tags can be specified for both networks for the convenience of the network administrator.

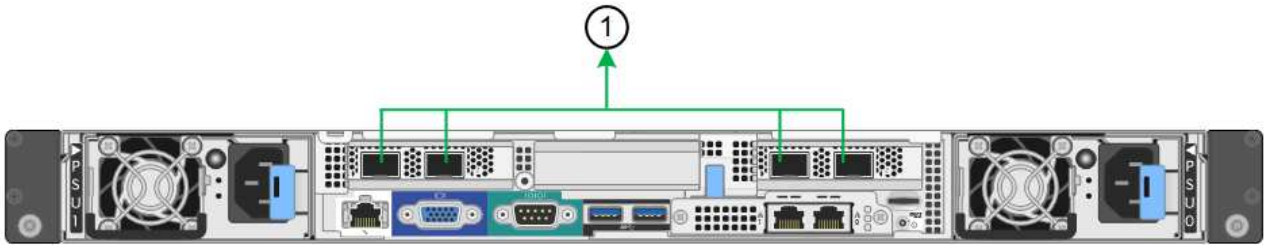
Aggregate port bond mode

These figures show how the four network ports are bonded in aggregate port bond mode.

SG1000:



SG100:



Callout	Which ports are bonded
1	All four ports are grouped in a single LACP bond, allowing all ports to be used for Grid Network and Client Network traffic.

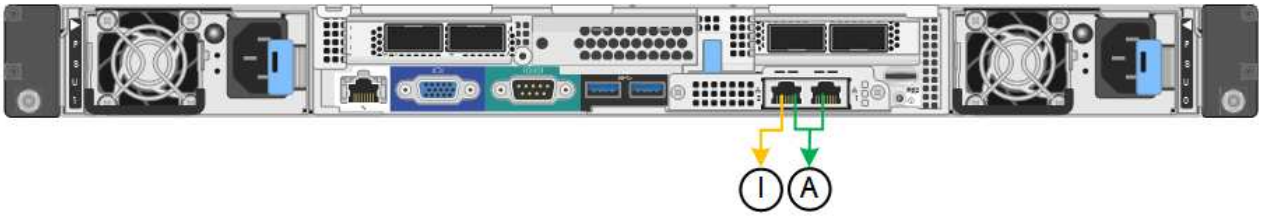
The table summarizes the options for configuring the four network ports. You only need to configure the settings on the Link Configuration page if you want to use a non-default setting.

Network bond mode	Client Network disabled (default)	Client Network enabled
LACP (802.3ad) only	• Ports 1-4 use a single LACP bond for the Grid Network. • A single VLAN tag identifies Grid Network packets.	• Ports 1-4 use a single LACP bond for the Grid Network and the Client Network. • Two VLAN tags allow Grid Network packets to be segregated from Client Network packets.

Active-Backup network bond mode for management ports

These figures show how the two 1-GbE management ports on the appliances are bonded in Active-Backup network bond mode for the Admin Network.

SG1000:



SG100:

Steps

1. From the menu bar of the StorageGRID Appliance Installer, click **Configure Networking** > **Link Configuration**.

   The Network Link Configuration page displays a diagram of your appliance with the network and management ports numbered.

   The Link Status table lists the link state, link speed, and other statistics of the numbered ports.

   The first time you access this page:

   - **Link Speed** is set to **Auto**.
   - **Port bond mode** is set to **Fixed**.
   - **Network bond mode** is set to **Active-Backup** for the Grid Network.
   - The **Admin Network** is enabled, and the network bond mode is set to **Independent**.

- The **Client Network** is disabled.

2. Select the link speed for the network ports from the **Link speed** drop-down list.

   The network switches you are using for the Grid Network and the Client Network must also support and be configured for this speed. You must use the appropriate adapters or transceivers for the configured link speed. Use Auto link speed when possible because this option negotiates both link speed and Forward Error Correction (FEC) mode with the link partner.

   If you plan to use the 25-GbE link speed for the SG6000 or SG5700 network ports:

   - Use SFP28 transceivers and SFP28 TwinAx cables or optical cables.
   - For the SG6000, select **Auto** from the **Link speed** drop-down list.
   - For the SG5700, select **25GbE** from the **Link speed** drop-down list.

3. Enable or disable the StorageGRID networks you plan to use.

   The Grid Network is required. You can't disable this network.

   a. If the appliance is not connected to the Admin Network, clear the **Enable network** checkbox for the Admin Network.
   b. If the appliance is connected to the Client Network, select the **Enable network** checkbox for the Client Network.

      The Client Network settings for the data NIC ports are now shown.

4. Refer to the table, and configure the port bond mode and the network bond mode.

   This example shows:

   - **Aggregate** and **LACP** selected for the Grid and the Client Networks. You must specify a unique VLAN tag for each network. You can select values between 0 and 4095.
   - **Active-Backup** selected for the Admin Network.

5. When you are satisfied with your selections, click **Save**.

You might lose your connection if you made changes to the network or link you are connected through. If you aren't reconnected within 1 minute, re-enter the URL for the StorageGRID Appliance Installer using one of the other IP addresses assigned to the appliance:
`https://appliance_IP:8443`

Configure StorageGRID IP addresses

You use the StorageGRID Appliance Installer to configure the IP addresses and routing information used for the services appliance or appliance Storage Node on the StorageGRID Grid, Admin, and Client Networks.

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

About this task

You must either assign a static IP for the appliance on each connected network or assign a permanent lease for the address on the DHCP server.

To change the link configuration, see the following instructions:

- Change link configuration of the SGF6112 appliance
- Change link configuration of the SG6000-CN controller
- Change link configuration of the E5700SG controller
- Change link configuration of the SG100 or SG1000 services appliance

Steps

1. In the StorageGRID Appliance Installer, select **Configure Networking** > **IP Configuration**.

   The IP Configuration page appears.

2. To configure the Grid Network, select either **Static** or **DHCP** in the **Grid Network** section of the page.
3. If you selected **Static**, follow these steps to configure the Grid Network:
   a. Enter the static IPv4 address, using CIDR notation.
   b. Enter the gateway.

      If your network does not have a gateway, re-enter the same static IPv4 address.

   c. If you want to use jumbo frames, change the MTU field to a value suitable for jumbo frames, such as 9000. Otherwise, keep the default value of 1500.

      The MTU value of the network must match the value configured on the switch port the node is connected to. Otherwise, network performance issues or packet loss might occur.

> For the best network performance, all nodes should be configured with similar MTU values on their Grid Network interfaces. The **Grid Network MTU mismatch** alert is triggered if there is a significant difference in MTU settings for the Grid Network on individual nodes. The MTU values don't have to be the same for all network types.

d. Click **Save**.

When you change the IP address, the gateway and list of subnets might also change.

If you lose your connection to the StorageGRID Appliance Installer, re-enter the URL using the new static IP address you just assigned. For example,
`https://appliance_IP:8443`

e. Confirm that the list of Grid Network subnets is correct.

If you have grid subnets, the Grid Network gateway is required. All grid subnets specified must be reachable through this gateway. These Grid Network subnets must also be defined in the Grid Network Subnet List on the primary Admin Node when you start StorageGRID installation.

> The default route is not listed. If the Client Network is not enabled, the default route will use the Grid Network gateway.

- To add a subnet, click the insert icon ➕ to the right of the last entry.
- To remove an unused subnet, click the delete icon ✖.

f. Click **Save**.

4. If you selected **DHCP**, follow these steps to configure the Grid Network:

a. After you select the **DHCP** radio button, click **Save**.

The **IPv4 Address**, **Gateway**, and **Subnets** fields are automatically populated. If the DHCP server is set up to assign an MTU value, the **MTU** field is populated with that value, and the field becomes read-only.

Your web browser is automatically redirected to the new IP address for the StorageGRID Appliance Installer.

b. Confirm that the list of Grid Network subnets is correct.

If you have grid subnets, the Grid Network gateway is required. All grid subnets specified must be reachable through this gateway. These Grid Network subnets must also be defined in the Grid Network Subnet List on the primary Admin Node when you start StorageGRID installation.

> The default route is not listed. If the Client Network is not enabled, the default route will use the Grid Network gateway.

- To add a subnet, click the insert icon ➕ to the right of the last entry.
- To remove an unused subnet, click the delete icon ✖.

c. If you want to use jumbo frames, change the MTU field to a value suitable for jumbo frames, such as 9000. Otherwise, keep the default value of 1500.

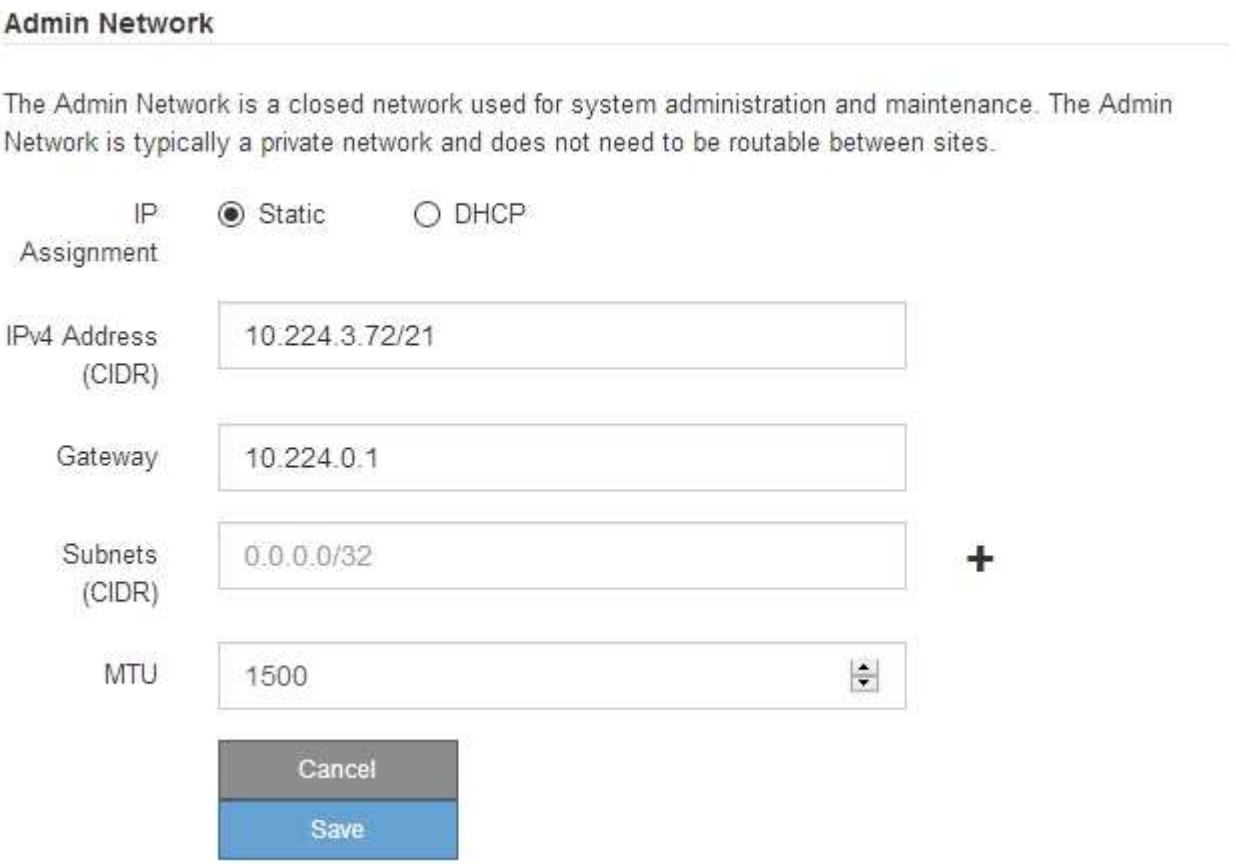
The MTU value of the network must match the value configured on the switch port the node is connected to. Otherwise, network performance issues or packet loss might occur.

For the best network performance, all nodes should be configured with similar MTU values on their Grid Network interfaces. The **Grid Network MTU mismatch** alert is triggered if there is a significant difference in MTU settings for the Grid Network on individual nodes. The MTU values don't have to be the same for all network types.

d. Click **Save**.

5. To configure the Admin Network, select either **Static** or **DHCP** in the **Admin Network** section of the page.

To configure the Admin Network, you enable the Admin Network on the Link Configuration page.



6. If you selected **Static**, follow these steps to configure the Admin Network:

a. Enter the static IPv4 address, using CIDR notation, for Management Port 1 on the appliance.

Management Port 1 is the left of the two 1-GbE RJ45 ports on the right end of the appliance.

b. Enter the gateway.

If your network does not have a gateway, re-enter the same static IPv4 address.

c. If you want to use jumbo frames, change the MTU field to a value suitable for jumbo frames, such as

9000. Otherwise, keep the default value of 1500.

> The MTU value of the network must match the value configured on the switch port the node is connected to. Otherwise, network performance issues or packet loss might occur.

d. Click **Save**.

When you change the IP address, the gateway and list of subnets might also change.

If you lose your connection to the StorageGRID Appliance Installer, re-enter the URL using the new static IP address you just assigned. For example,
`https://appliance:8443`

e. Confirm that the list of Admin Network subnets is correct.

You must verify that all subnets can be reached using the gateway you provided.

> The default route can't be made to use the Admin Network gateway.

- To add a subnet, click the insert icon ➕ to the right of the last entry.
- To remove an unused subnet, click the delete icon ✖.

f. Click **Save**.

7. If you selected **DHCP**, follow these steps to configure the Admin Network:

a. After you select the **DHCP** radio button, click **Save**.

The **IPv4 Address**, **Gateway**, and **Subnets** fields are automatically populated. If the DHCP server is set up to assign an MTU value, the **MTU** field is populated with that value, and the field becomes read-only.

Your web browser is automatically redirected to the new IP address for the StorageGRID Appliance Installer.

b. Confirm that the list of Admin Network subnets is correct.

You must verify that all subnets can be reached using the gateway you provided.

> The default route can't be made to use the Admin Network gateway.

- To add a subnet, click the insert icon ➕ to the right of the last entry.
- To remove an unused subnet, click the delete icon ✖.

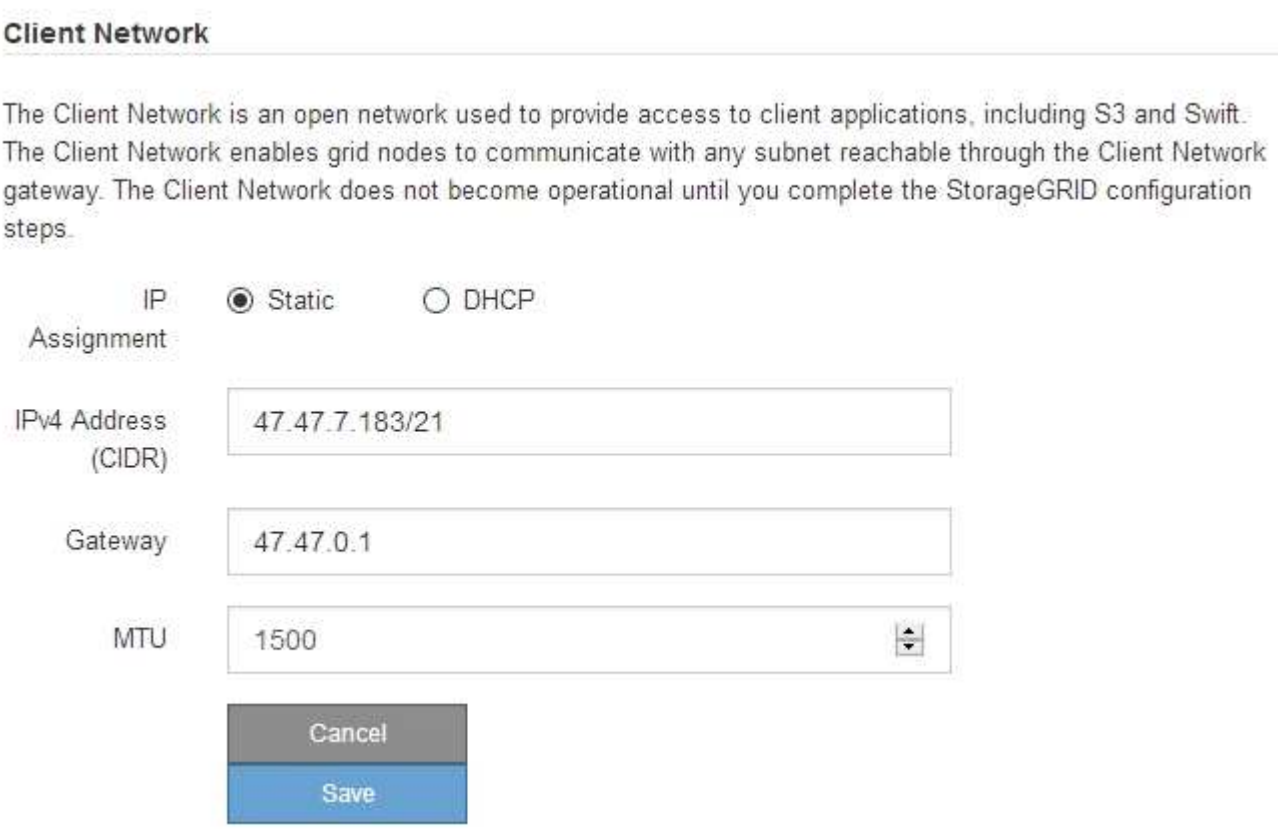
c. If you want to use jumbo frames, change the MTU field to a value suitable for jumbo frames, such as 9000. Otherwise, keep the default value of 1500.

> The MTU value of the network must match the value configured on the switch port the node is connected to. Otherwise, network performance issues or packet loss might occur.

d. Click **Save**.

8. To configure the Client Network, select either **Static** or **DHCP** in the **Client Network** section of the page.

To configure the Client Network, you enable the Client Network on the Link Configuration page.



9. If you selected **Static**, follow these steps to configure the Client Network:
   a. Enter the static IPv4 address, using CIDR notation.
   b. Click **Save**.
   c. Confirm that the IP address for the Client Network gateway is correct.

      If the Client Network is enabled, the default route is displayed. The default route uses the Client Network gateway and can't be moved to another interface while the Client Network is enabled.

   d. If you want to use jumbo frames, change the MTU field to a value suitable for jumbo frames, such as 9000. Otherwise, keep the default value of 1500.

      The MTU value of the network must match the value configured on the switch port the node is connected to. Otherwise, network performance issues or packet loss might occur.

   e. Click **Save**.
10. If you selected **DHCP**, follow these steps to configure the Client Network:
    a. After you select the **DHCP** radio button, click **Save**.

       The **IPv4 Address** and **Gateway** fields are automatically populated. If the DHCP server is set up to assign an MTU value, the **MTU** field is populated with that value, and the field becomes read-only.

Your web browser is automatically redirected to the new IP address for the StorageGRID Appliance Installer.

b. Confirm that the gateway is correct.

> If the Client Network is enabled, the default route is displayed. The default route uses the Client Network gateway and can't be moved to another interface while the Client Network is enabled.

c. If you want to use jumbo frames, change the MTU field to a value suitable for jumbo frames, such as 9000. Otherwise, keep the default value of 1500.

> The MTU value of the network must match the value configured on the switch port the node is connected to. Otherwise, network performance issues or packet loss might occur.

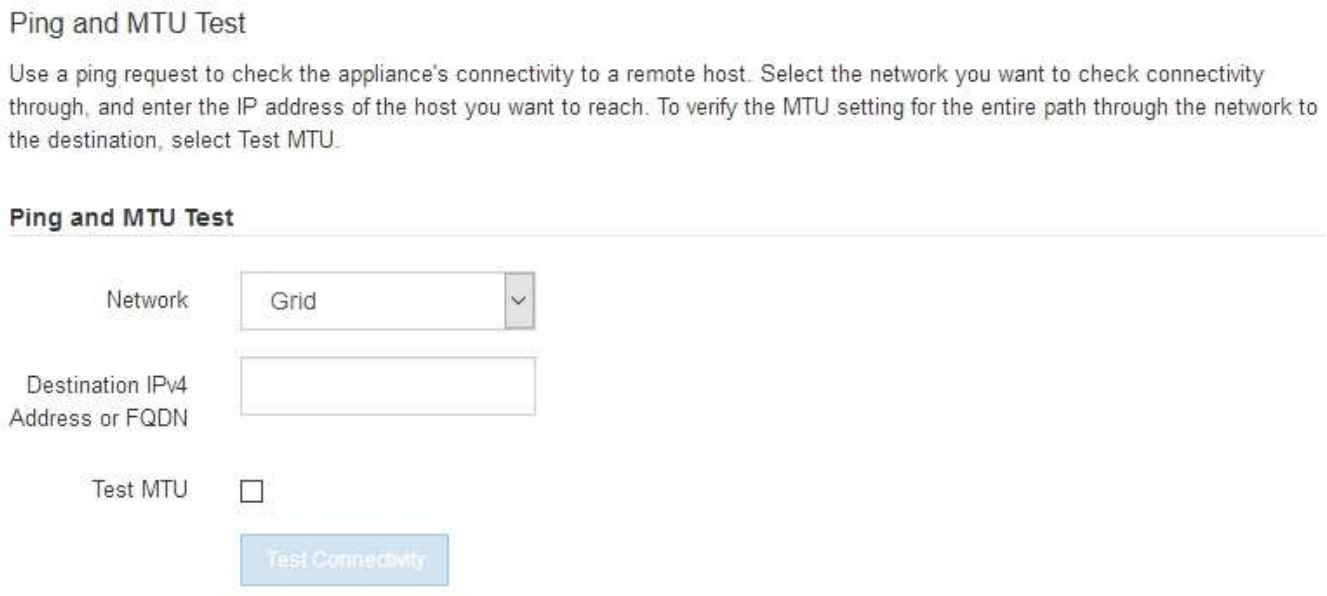
Verify network connections

You should confirm you can access the StorageGRID networks you are using from the appliance. To validate routing through network gateways, you should test connectivity between the StorageGRID Appliance Installer and IP addresses on different subnets. You can also verify the MTU setting.

Steps

1. From the menu bar of the StorageGRID Appliance Installer, click **Configure Networking** > **Ping and MTU Test**.

   The Ping and MTU Test page appears.



2. From the **Network** drop-down box, select the network you want to test: Grid, Admin, or Client.
3. Enter the IPv4 address or fully qualified domain name (FQDN) for a host on that network.

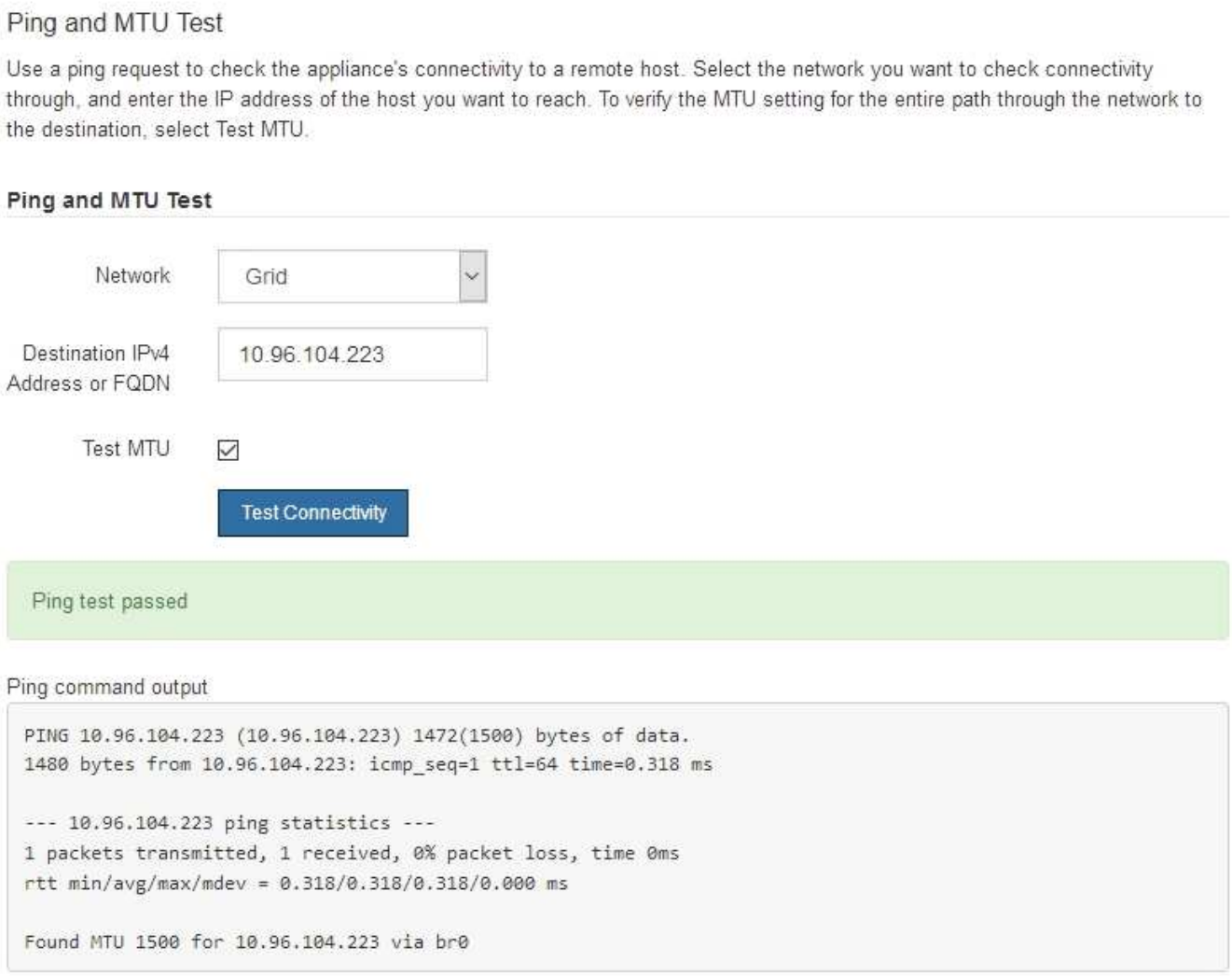
For example, you might want to ping the gateway on the network or the primary Admin Node.

4. Optionally, select the **Test MTU** checkbox to verify the MTU setting for the entire path through the network to the destination.

   For example, you can test the path between the appliance node and a node at a different site.

5. Click **Test Connectivity**.

   If the network connection is valid, the "Ping test passed" message appears, with the ping command output listed.



Related information

- Configure network links
- Change MTU setting

Verify port-level network connections

To ensure that access between the StorageGRID Appliance Installer and other nodes is not obstructed by firewalls, confirm that the StorageGRID Appliance Installer can connect to a specific TCP port or set of ports at the specified IP address or range of addresses.

About this task

Using the list of ports provided in the StorageGRID Appliance Installer, you can test the connectivity between the appliance and the other nodes in your Grid Network.

Additionally, you can test connectivity on the Admin and Client Networks and on UDP ports, such as those used for external NFS or DNS servers. For a list of these ports, see the network port reference.

> The Grid Network ports listed in the port connectivity table are valid only for StorageGRID version 11.7.0. To verify which ports are correct for each node type, you should always consult the networking guidelines for your version of StorageGRID.

Steps

1. From the StorageGRID Appliance Installer, click **Configure Networking** > **Port Connectivity Test (nmap)**.

   The Port Connectivity Test page appears.

   The port connectivity table lists node types that require TCP connectivity on the Grid Network. For each node type, the table lists the Grid Network ports that should be accessible to your appliance.

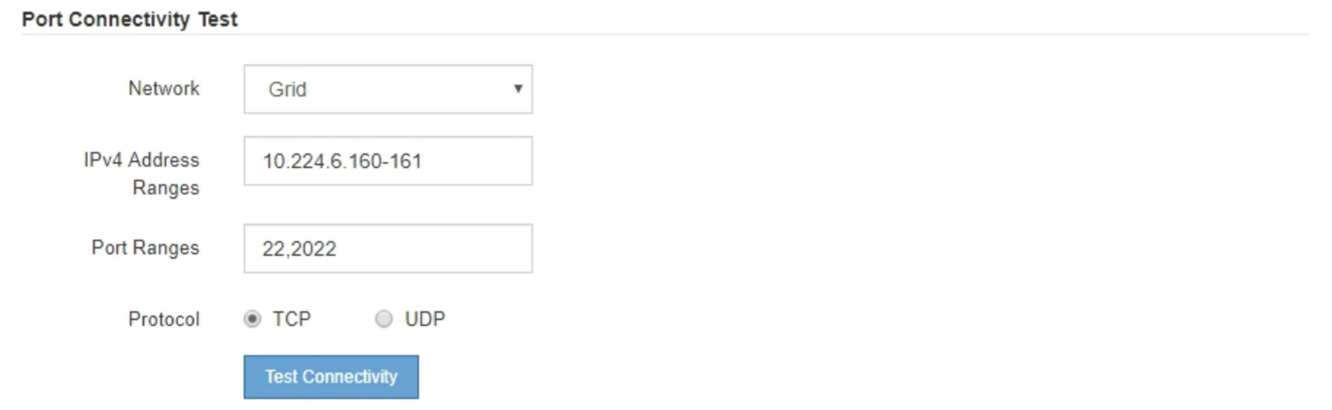
   You can test the connectivity between the appliance ports listed in the table and the other nodes in your Grid Network.

2. From the **Network** drop-down, select the network you want to test: **Grid**, **Admin**, or **Client**.
3. Specify a range of IPv4 addresses for the hosts on that network.

   For example, you might want to probe the gateway on the network or the primary Admin Node.

   Specify a range using a hyphen, as shown in the example.

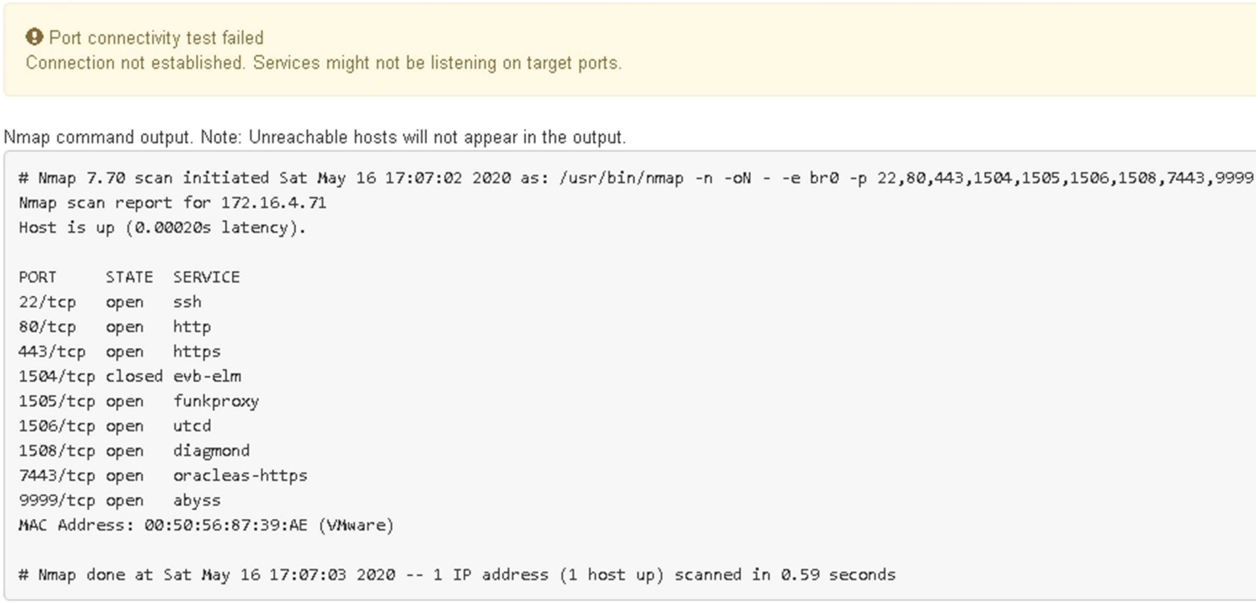
4. Enter a TCP port number, a list of ports separated by commas, or a range of ports.



5. Click **Test Connectivity**.
   - If the selected port-level network connections are valid, the “Port connectivity test passed” message appears in a green banner. The nmap command output is listed below the banner.

- If a port-level network connection is made to the remote host, but the host is not listening on one or more of the selected ports, the “Port connectivity test failed” message appears in a yellow banner. The nmap command output is listed below the banner.

  Any remote port the host is not listening to has a state of “closed.” For example, you might see this yellow banner when the node you are trying to connect to is in a pre-installed state and the StorageGRID NMS service is not yet running on that node.



- If a port-level network connection can’t be made for one or more selected ports, the “Port connectivity test failed” message appears in a red banner. The nmap command output is listed below the banner.

  The red banner indicates that a TCP connection attempt to a port on the remote host was made, but nothing was returned to the sender. When no response is returned, the port has a state of "filtered" and is likely blocked by a firewall.

  Ports with “closed” are also listed.

Configure SANtricity System Manager (SG6000 and SG5700)

You can use SANtricity System Manager to monitor the status of the storage controllers, storage disks, and other hardware components in the storage controller shelf. You can also configure a proxy for E-Series AutoSupport that enables you to send AutoSupport messages from the appliance without the use of the management port.

Set up and access SANtricity System Manager

You might need to access SANtricity System Manager on the storage controller to monitor the hardware in the storage controller shelf or to configure E-Series AutoSupport.

Before you begin

- You are using a supported web browser.
- To access SANtricity System Manager through Grid Manager, you have installed StorageGRID, and you have the Storage appliance administrator permission or Root access permission.
- To access SANtricity System Manager using the StorageGRID Appliance Installer, you have the SANtricity System Manager administrator username and password.
- To access SANtricity System Manager directly using a web browser, you have the SANtricity System Manager administrator username and password.

> You must have SANtricity firmware 8.70 or higher to access SANtricity System Manager using the Grid Manager or the StorageGRID Appliance Installer. You can check your firmware version by using the StorageGRID Appliance Installer and selecting **Help** > **About**.

> Accessing SANtricity System Manager from the Grid Manager or from the Appliance Installer is generally meant only for monitoring your hardware and configuring E-Series AutoSupport. Many features and operations within SANtricity System Manager such as upgrading firmware don't apply to monitoring your StorageGRID appliance. To avoid issues, always follow the hardware installation and maintenance instructions for your appliance.

About this task

There are three ways to access SANtricity System Manager, depending upon what stage of the installation and configuration process you are in:

- If the appliance has not yet been deployed as a node in your StorageGRID system, you should use the Advanced tab in the StorageGRID Appliance Installer.

  > Once the node is deployed, you can no longer use the StorageGRID Appliance Installer to access SANtricity System Manager.

- If the appliance has been deployed as a node in your StorageGRID system, use the SANtricity System Manager tab on the Nodes page in Grid Manager.
- If you can't use the StorageGRID Appliance Installer or Grid Manager, you can access SANtricity System Manager directly using a web browser connected to the management port.

This procedure includes steps for your initial access to SANtricity System Manager. If you have already set up SANtricity System Manager, go to the configure hardware alerts step.

> Using either the Grid Manager or the StorageGRID Appliance Installer enables you to access SANtricity System Manager without having to configure or connect the management port of the appliance.

You use SANtricity System Manager to monitor the following:

- Performance data such as storage array level performance, I/O latency, CPU utilization, and throughput
- Hardware component status
- Support functions including viewing diagnostic data

You can use SANtricity System Manager to configure the following settings:

- Email alerts, SNMP alerts, or syslog alerts for the components in the storage controller shelf
- E-Series AutoSupport settings for the components in the storage controller shelf.

  For additional details on E-Series AutoSupport, see the NetApp E-Series Systems Documentation Site.

- Drive Security keys, which are needed to unlock secured drives (this step is required if the Drive Security feature is enabled)
- Administrator password for accessing SANtricity System Manager

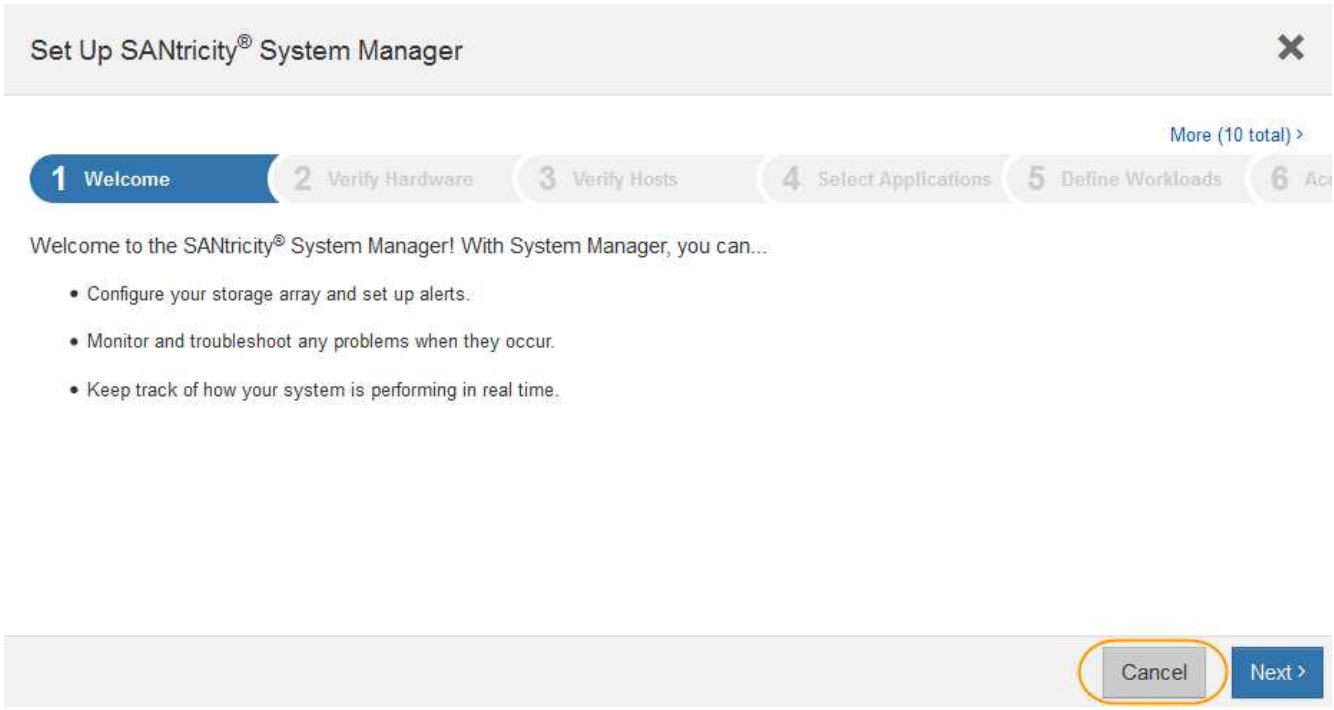
Steps

1. Do one of the following:
   - Use the StorageGRID Appliance Installer and select **Advanced** > **SANtricity System Manager**
   - Use the Grid Manager and select **NODES** > ***appliance Storage Node*** > **SANtricity System Manager**

     > If these options aren't available or the login page does not appear, use the IP addresses for the storage controllers. Access SANtricity System Manager by browsing to the storage controller IP.

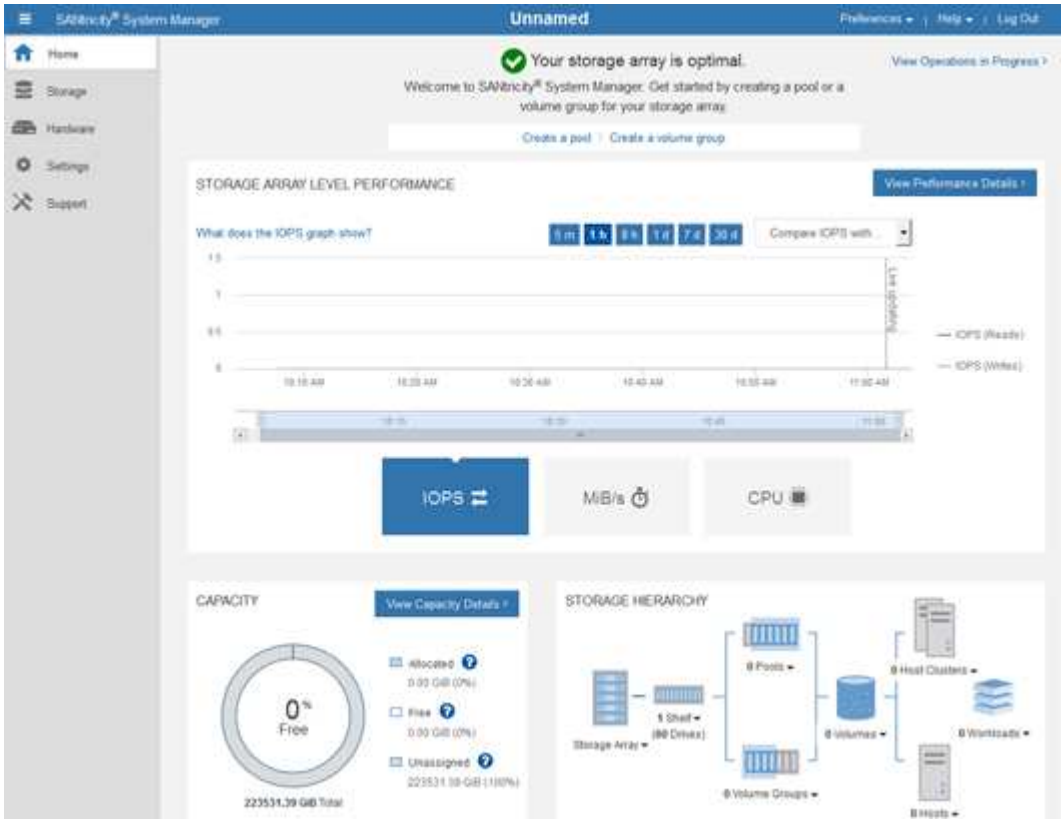
2. Set or enter the administrator password.

SANtricity System Manager uses a single administrator password that is shared among all users.



3. Select **Cancel** to close the wizard.

> Don’t complete the Set Up wizard for a StorageGRID appliance.



4. Configure hardware alerts.

a. Select **Help** to access the online help for SANtricity System Manager.
b. Use the **Settings** > **Alerts** section of the online help to learn about alerts.
c. Follow the “How To” instructions to set up email alerts, SNMP alerts, or syslog alerts.

5. Manage AutoSupport for the components in the storage controller shelf.
   a. Select **Help** to access the online help for SANtricity System Manager.
   b. Use the **SUPPORT** > **Support Center** section of the online help to learn about the AutoSupport feature.
   c. Follow the “How To” instructions to manage AutoSupport.

      For specific instructions on configuring a StorageGRID proxy for sending E-Series AutoSupport messages without using the management port, go to the instructions for configuring storage proxy settings.

6. If the Drive Security feature is enabled for the appliance, create and manage the security key.
   a. Select **Help** to access the online help for SANtricity System Manager.
   b. Use the **Settings** > **System** > **Security key management** section of the online help to learn about Drive Security.
   c. Follow the “How To” instructions to create and manage the security key.
7. Optionally, change the administrator password.
   a. Select **Help** to access the online help for SANtricity System Manager.
   b. Use the **Home** > **Storage array administration** section of the online help to learn about the administrator password.
   c. Follow the “How To” instructions to change the password.

Review hardware status in SANtricity System Manager

You can use SANtricity System Manager to monitor and manage the individual hardware components in the storage controller shelf and to review hardware diagnostic and environmental information, such as component temperatures, as well as issues related to the drives.

Before you begin

- You are using a supported web browser.
- To access SANtricity System Manager through Grid Manager, you have the Storage appliance administrator permission or Root access permission.
- To access SANtricity System Manager using the StorageGRID Appliance Installer, you have the SANtricity System Manager administrator username and password.
- To access SANtricity System Manager directly using a web browser, you have the SANtricity System Manager administrator username and password.

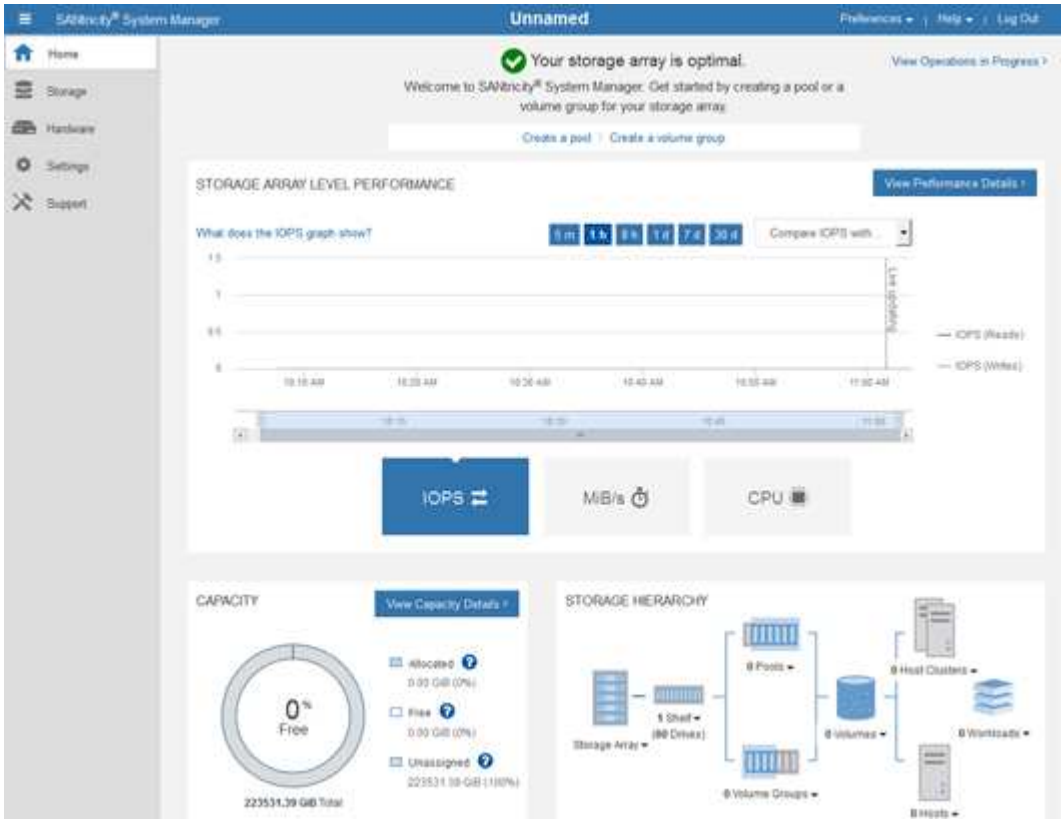
> ⓘ You must have SANtricity firmware 8.70 or higher to access SANtricity System Manager using the Grid Manager or the StorageGRID Appliance Installer.

Accessing SANtricity System Manager from the Grid Manager or from the Appliance Installer is generally meant only for monitoring your hardware and configuring E-Series AutoSupport. Many features and operations within SANtricity System Manager such as upgrading firmware don't apply to monitoring your StorageGRID appliance. To avoid issues, always follow the hardware installation and maintenance instructions for your appliance.

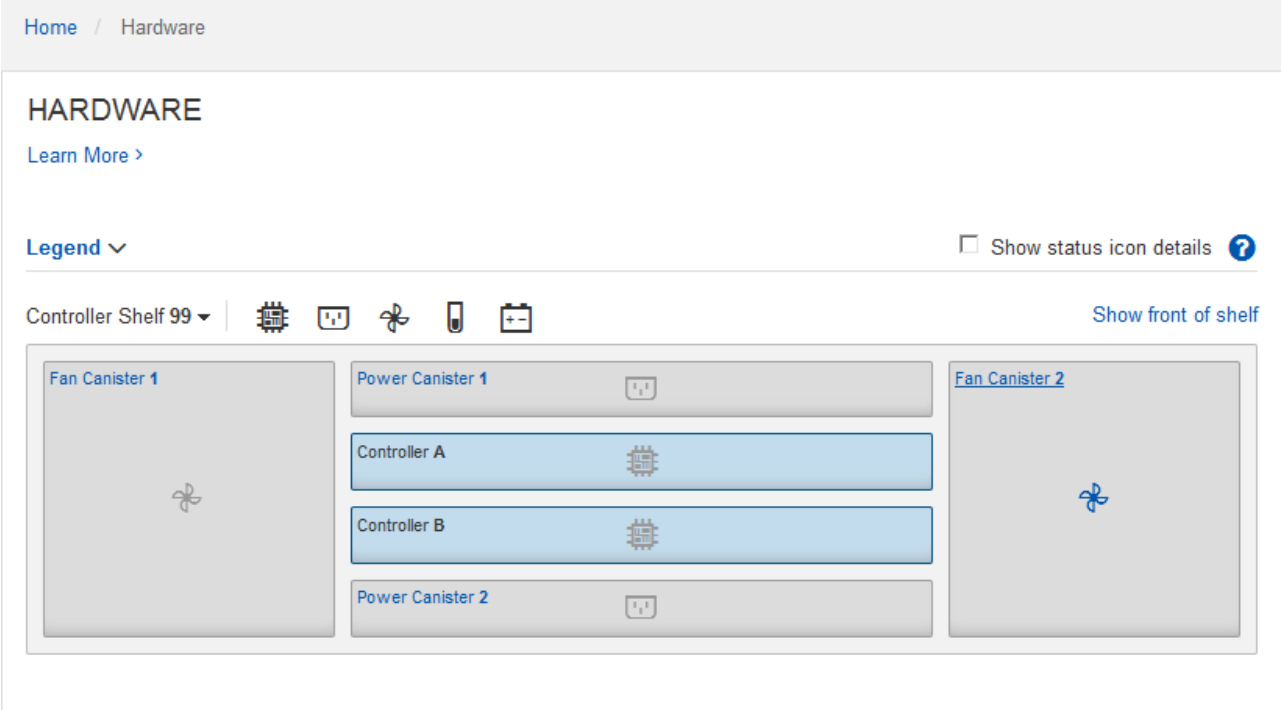
Steps

1. Access SANtricity System Manager.
2. Enter the administrator username and password if required.
3. Click **Cancel** to close the Set Up wizard and to display the SANtricity System Manager home page.

   The SANtricity System Manager home page appears. In SANtricity System Manager, the controller shelf is referred to as a storage array.



4. Review the information displayed for appliance hardware and confirm that all hardware components have a status of Optimal.
   a. Click the **Hardware** tab.
   b. Click **Show back of shelf**.



From the back of the shelf, you can view both storage controllers, the battery in each storage controller, the two power canisters, the two fan canisters, and expansion shelves (if any). You can also view component temperatures.

c. To see the settings for each storage controller, select the controller, and select **View settings** from the context menu.

d. To see the settings for other components in the back of the shelf, select the component you want to view.

e. Click **Show front of shelf**, and select the component you want to view.

   From the front of the shelf, you can view the drives and the drive drawers for the storage controller shelf or the expansion shelves (if any).

If the status of any component is Needs Attention, follow the steps in the Recovery Guru to resolve the issue or contact technical support.

Set IP addresses for storage controllers using StorageGRID Appliance Installer

Management port 1 on each storage controller connects the appliance to the management network for SANtricity System Manager. If you can't access SANtricity System Manager from the StorageGRID Appliance Installer, set a static IP address for each storage controller to ensure that you don't lose your management connection to the hardware and the controller firmware in the controller shelf.

Before you begin

- You are using any management client that can connect to the StorageGRID Admin Network, or you have a service laptop.
- The client or service laptop has a supported web browser.

About this task

DHCP-assigned addresses can change at any time. Assign static IP addresses to the controllers to ensure consistent accessibility.

Follow this procedure only if you don't have access to SANtricity System Manager from the StorageGRID Appliance Installer (**Advanced** > **SANtricity System Manager**) or Grid Manager (**NODES** > **SANtricity System Manager**).

Steps

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

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

   The StorageGRID Appliance Installer Home page appears.

2. Select **Configure Hardware** > **Storage Controller Network Configuration**.

   The Storage Controller Network Configuration page appears.

3. Depending on your network configuration, select **Enabled** for IPv4, IPv6, or both.
4. Make a note of the IPv4 address that is automatically displayed.

   DHCP is the default method for assigning an IP address to the storage controller management port.

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

5. Optionally, set a static IP address for the storage controller management port.

   You should either assign a static IP for the 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.

When you connect to SANtricity System Manager, you will use the new static IP address as the URL:
https://*Storage_Controller_IP*

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.

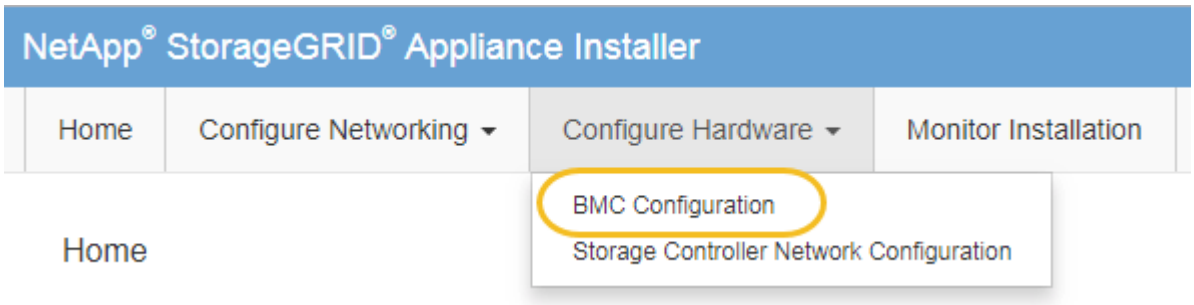
Steps

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.

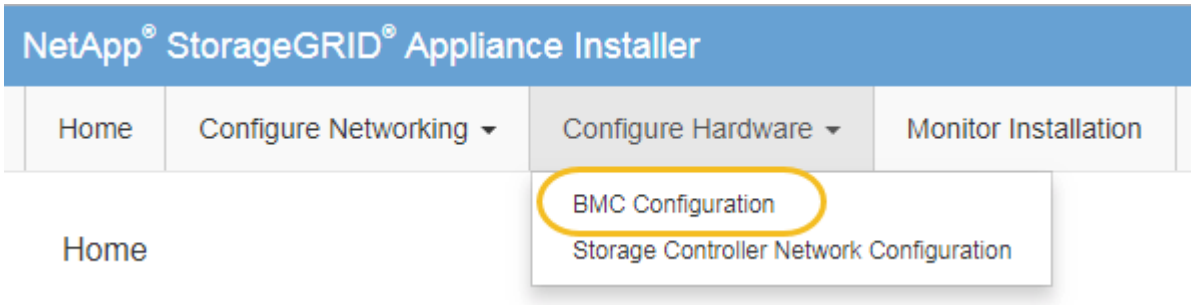
Steps

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**.

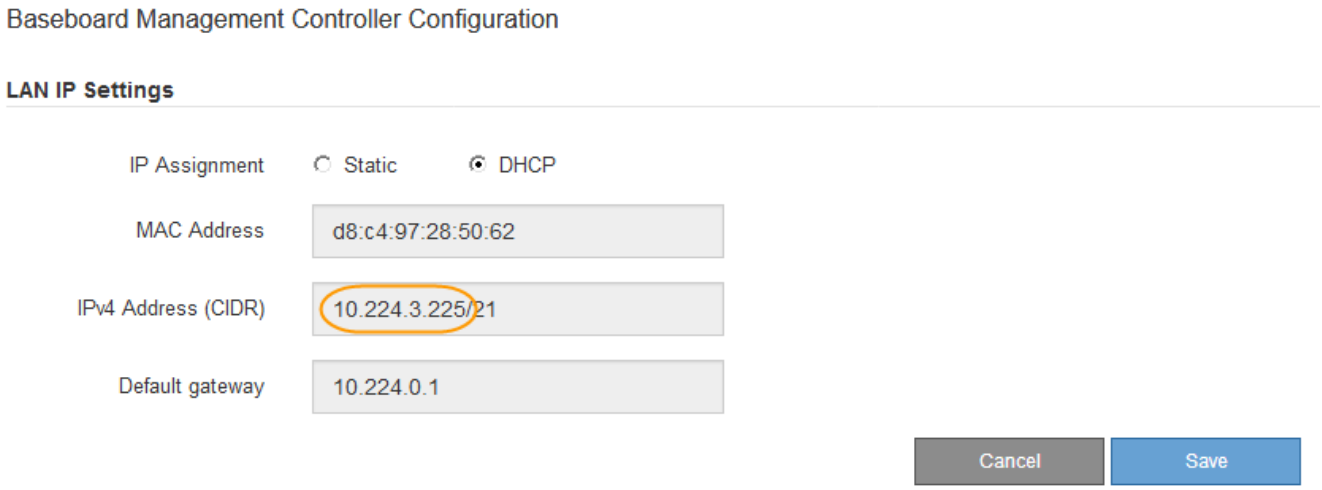


   The Baseboard Management Controller Configuration page appears.

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.

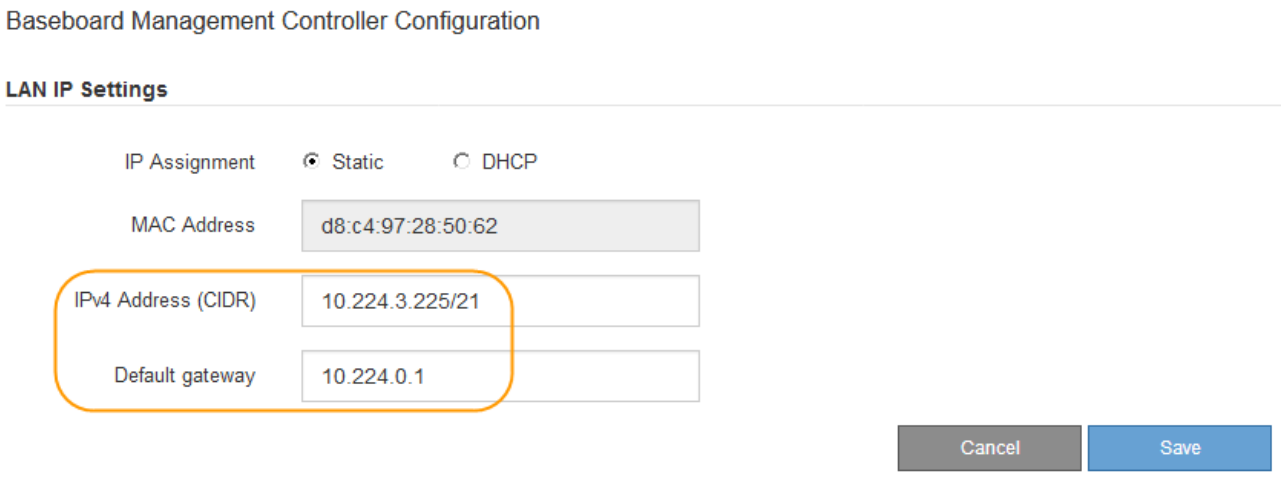
   > It might take a few minutes for the DHCP values to appear.



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

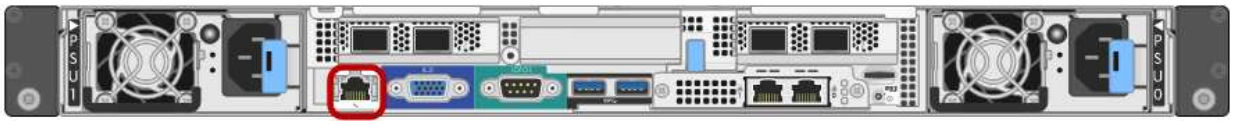
- The management client is using a supported web browser.
- The BMC management port on the appliance is connected to the management network you plan to use.

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.

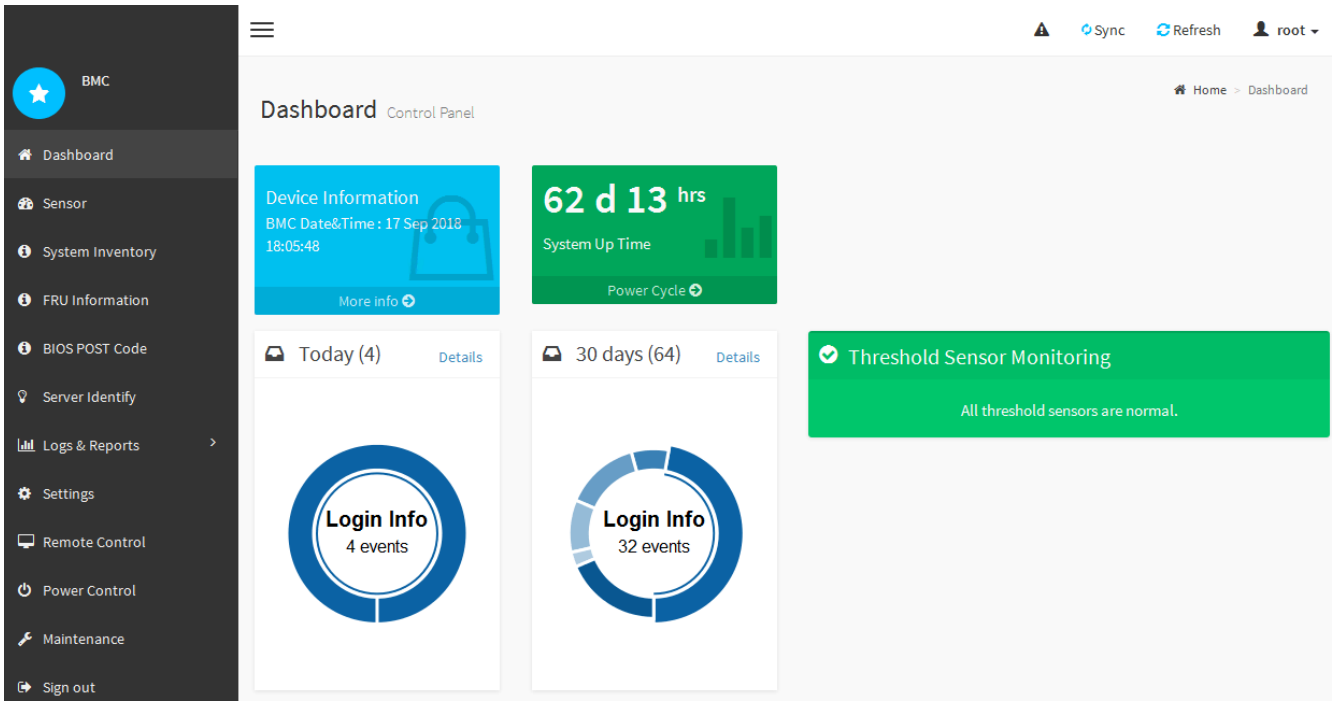
   The BMC sign-in page appears.

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.

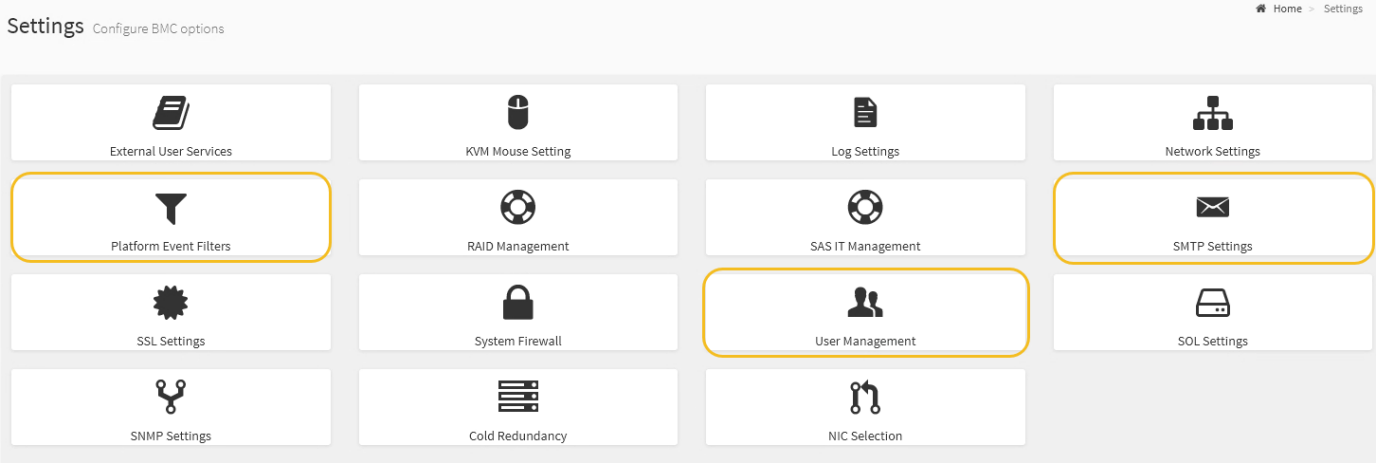
> BMC settings made by this procedure might not be preserved if the SG6000-CN controller or services appliance fails and has to be replaced. Make sure you have a record of all settings you have applied, so they can be easily reapplied after a hardware replacement if necessary.

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.

Optional: Enable node encryption

If you enable node encryption, the disks in your appliance can be protected by secure key management server (KMS) encryption against physical loss or removal from the site. You must select and enable node encryption during appliance installation. You can't disable node encryption after the KMS encryption process starts.

If you are using ConfigBuilder to generate a JSON file, you can enable node encryption automatically. See Automate appliance installation and configuration.

Before you begin

Review the information about configuring KMS.

About this task

An appliance that has node encryption enabled connects to the external key management server (KMS) that is configured for the StorageGRID site. Each KMS (or KMS cluster) manages the encryption keys for all appliance nodes at the site. These keys encrypt and decrypt the data on each disk in an appliance that has node encryption enabled.

A KMS can be set up in Grid Manager before or after the appliance is installed in StorageGRID. See the information about KMS and appliance configuration in the instructions for administering StorageGRID for additional details.

- If a KMS is set up before installing the appliance, KMS-controlled encryption begins when you enable node encryption on the appliance and add it to a StorageGRID site where KMS is configured.
- If a KMS is not set up before you install the appliance, KMS-controlled encryption is performed on each appliance that has node encryption enabled as soon as a KMS is configured and available for the site that contains the appliance node.

> When an appliance is installed with node encryption enabled, a temporary key is assigned. The data on the appliance is not protected until the appliance is connected to the Key Management System (KMS) and a KMS security key is set. See the KMS appliance configuration overview for additional information.

Without the KMS key needed to decrypt the disk, data on the appliance can't be retrieved and is effectively lost. This is the case whenever the decryption key can't be retrieved from the KMS. The key becomes inaccessible if a customer clears the KMS configuration, a KMS key expires, connection to the KMS is lost, or the appliance is removed from the StorageGRID system where its KMS keys are installed.

Steps

1. Open a browser, and enter one of the IP addresses for the appliance's compute controller.

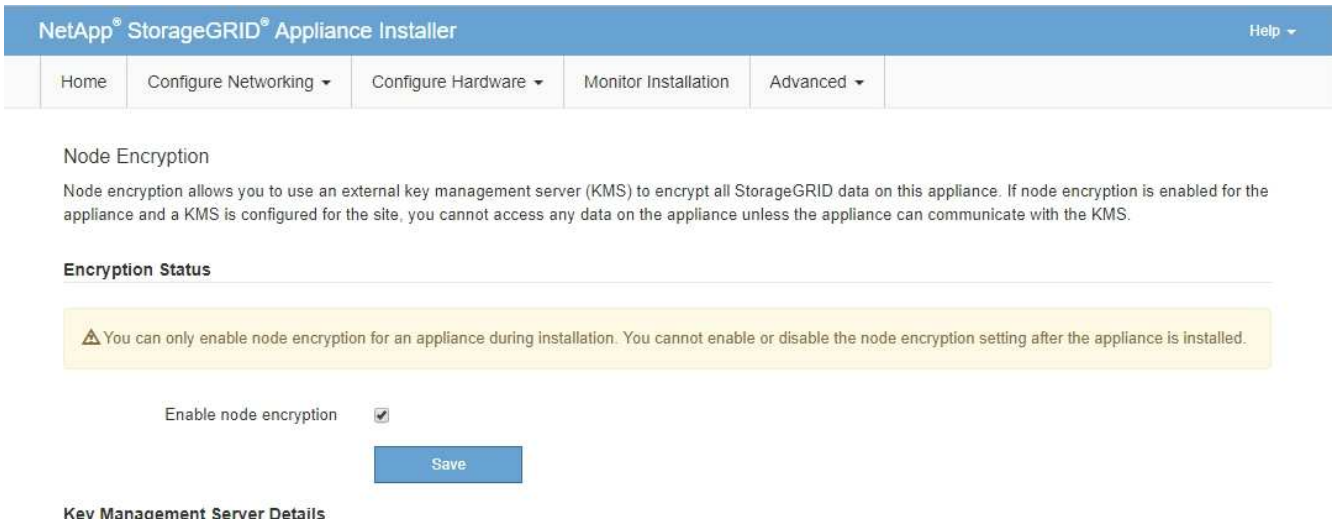
   `https://Controller_IP:8443`

Controller_IP is the IP address of the compute controller (not the storage controller) on any of the three StorageGRID networks.

The StorageGRID Appliance Installer Home page appears.

> After the appliance has been encrypted with a KMS key, the appliance disks can't be decrypted without using the same KMS key.

2. Select **Configure Hardware** > **Node Encryption**.



3. Select **Enable node encryption**.

   Before appliance installation, you can clear **Enable node encryption** without risk of data loss. When the installation begins, the appliance node accesses the KMS encryption keys in your StorageGRID system and begins disk encryption. You can't disable node encryption after the appliance is installed.

> After you add an appliance that has node encryption enabled to a StorageGRID site that has a KMS, you can't stop using KMS encryption for the node.

4. Select **Save**.
5. Deploy the appliance as a node in your StorageGRID system.

   KMS-controlled encryption begins when the appliance accesses the KMS keys configured for your StorageGRID site. The installer displays progress messages during the KMS encryption process, which might take a few minutes depending on the number of disk volumes in the appliance.

> Appliances are initially configured with a random non-KMS encryption key assigned to each disk volume. The disks are encrypted using this temporary encryption key, that is not secure, until the appliance that has node encryption enabled accesses the KMS keys configured for your StorageGRID site.

After you finish

You can view node-encryption status, KMS details, and the certificates in use when the appliance node is in maintenance mode. See Monitor node encryption in maintenance mode for information.

Optional: Change RAID mode

On some appliance models, you can change to a different RAID mode on the appliance to accommodate your storage and recovery requirements. You can only change the mode before deploying the appliance Storage Node.

If you are using ConfigBuilder to generate a JSON file, you can change the RAID mode automatically. See Automate appliance installation and configuration.

About this task

If supported by your appliance, you can choose one of the following volume configuration options:

- **Dynamic Disk Pools (DDP)**: This mode uses two parity drives for every eight data drives. This is the default and recommended mode for all appliances. When compared to RAID 6, DDP delivers better system performance, reduced rebuild times after drive failures, and ease of management. DDP also provides drawer loss protection in SG5760 appliances.

  > DDP does not provide drawer loss protection in SG6060 appliances because of the two SSDs. Drawer loss protection is effective in any expansion shelves that are added to an SG6060.

- **DDP16**: This mode uses two parity drives for every 16 data drives, which results in higher storage efficiency compared to DDP. When compared to RAID 6, DDP16 delivers better system performance, reduced rebuild times after drive failures, ease of management, and comparable storage efficiency. To use DDP16 mode, your configuration must contain at least 20 drives. DDP16 does not provide drawer loss protection.
- **RAID6**: This mode uses two parity drives for every 16 or more data drives. It is a hardware protection scheme that uses parity stripes on each disk, and allows for two disk failures within the RAID set before any data is lost. To use RAID 6 mode, your configuration must contain at least 20 drives. Although RAID 6 can increase storage efficiency of the appliance when compared to DDP, it is not recommended for most StorageGRID environments.

> If any volumes have already been configured or if StorageGRID was previously installed, changing the RAID mode causes the volumes to be removed and replaced. Any data on those volumes will be lost.

SG6000

Before you begin

- You are using any client that can connect to StorageGRID.
- The client has a supported web browser.

Steps

1. Open a browser, and enter one of the IP addresses for the appliance's compute controller.

   `https://Controller_IP:8443`

   `Controller_IP` is the IP address of the compute controller (not the storage controller) on any of the three StorageGRID networks.

   The StorageGRID Appliance Installer Home page appears.

2. Select **Advanced** > **RAID Mode**.
3. On the **Configure RAID Mode** page, select the desired RAID mode from the Mode drop-down list.
4. Click **Save**.

SG5760

Before you begin

- You have an SG5760 with 60 drives. If you have an SG5712, you must use the default DDP mode.
- You are using any client that can connect to StorageGRID.
- The client has a supported web browser.

Steps

1. Using the service laptop, open a web browser and access the StorageGRID Appliance Installer:
   `https://E5700SG_Controller_IP:8443`

   Where *`E5700SG_Controller_IP`* is any of the IP addresses for the E5700SG controller.

2. Select **Advanced** > **RAID Mode**.
3. On the **Configure RAID Mode** page, select the desired RAID mode from the Mode drop-down list.
4. Click **Save**.

Related information

NetApp E-Series Systems Documentation Site

Optional: Remap network ports for appliance

You can optionally remap the internal ports on an appliance node to different external ports. For example, you might need to remap ports because of a firewall issue.

Before you begin

- You have previously accessed the StorageGRID Appliance Installer.

About this task

You can't use remapped ports for load balancer endpoints. If you need to remove a remapped port, follow the steps in Remove port remaps.

Steps

1. From the StorageGRID Appliance Installer, select **Configure Networking** > **Remap Ports**.

   The Remap Port page appears.

2. From the **Network** drop-down box, select the network for the port you want to remap: Grid, Admin, or Client.
3. From the **Protocol** drop-down box, select the IP protocol: TCP or UDP.
4. From the **Remap Direction** drop-down box, select which traffic direction you want to remap for this port: Inbound, Outbound, or Bi-directional.
5. For **Original Port**, enter the number of the port you want to remap.
6. For **Mapped-To Port**, enter the number of the port you want to use instead.
7. Select **Add Rule**.

   The new port mapping is added to the table, and the remapping takes effect immediately.

8. To remove a port mapping, select the radio button for the rule you want to remove, and select **Remove Selected Rule**.

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.