



# **StorageGRID Appliance Documentation**

## **StorageGRID Appliances**

NetApp  
April 11, 2024

# Table of Contents

- StorageGRID Appliance Documentation ..... 1
- StorageGRID software documentation ..... 2
  - Other versions ..... 2
- Get started with StorageGRID appliances ..... 3
  - What's new for appliances ..... 3
  - Learn about StorageGRID appliances ..... 3
- Install StorageGRID appliance hardware ..... 30
  - Quick start for appliance installation ..... 30
  - Prepare for StorageGRID installation ..... 31
  - Automate appliance installation and configuration ..... 71
  - Automate StorageGRID configuration ..... 77
  - Overview of installation REST APIs ..... 79
  - Install appliance hardware ..... 80
    - Set up hardware ..... 119
    - Deploy an appliance node ..... 168
- Maintain appliance hardware ..... 201
  - Maintain appliance configuration ..... 201
  - Appliance node cloning ..... 212
  - Maintain SG1000 and SG100 services appliance hardware ..... 219
  - Maintain SG5600 hardware ..... 232
  - Maintain SG5700 storage appliance hardware ..... 232
  - Maintain SG6000 storage appliance hardware ..... 265
  - Maintain SG6100 storage appliance hardware ..... 320
- How to enable StorageGRID in your environment ..... 360
- Legal notices ..... 361
  - Copyright ..... 361
  - Trademarks ..... 361
  - Patents ..... 361
  - Privacy policy ..... 361
  - Open source ..... 361

# StorageGRID Appliance Documentation

# StorageGRID software documentation

Go to [StorageGRID 11.8 Documentation](#) to learn how to configure and use a StorageGRID 11.8 system.

The StorageGRID doc site includes information such as:

- Networking guidelines.
- Installation instructions for Linux and VMware nodes.
- StorageGRID upgrade and hotfix instructions.
- Administration instructions for configuring your system, including using information lifecycle management (ILM) to protect object data.
- Instructions for using StorageGRID tenant accounts and the S3 REST API.
- Monitoring and troubleshooting instructions, including information about alerts, audit messages, and system logs.
- Instructions for maintaining a StorageGRID system, which includes adding new StorageGRID volumes, nodes, or site; recovering failed nodes and volumes; decommissioning nodes or sites; and performing other maintenance on your grid.

## Other versions

You can find documentation for other versions of NetApp StorageGRID software here:

- [StorageGRID 11.7 documentation](#)
- [StorageGRID 11.6 documentation](#)
- [StorageGRID 11.5 documentation](#)
- [StorageGRID 11.4 documentation](#)

# Get started with StorageGRID appliances

## What's new for appliances

Learn what's new for StorageGRID appliances.

### SGF6112 all-flash appliance

The new StorageGRID SGF6112 storage appliance features a compact design with compute controller and storage controller integrated into a 1U chassis. The appliance supports 12 SSD NVMe drives with a storage capacity of up to 15.3 TB per drive. The SSD drives are in a RAID that provides resilient object storage. See [SGF6112 appliance: Overview](#).

## Learn about StorageGRID appliances

### SG100 and SG1000 appliances: Overview

The StorageGRID SG100 services appliance and the SG1000 services appliance can operate as a Gateway Node and as an Admin Node to provide high availability load balancing services in a StorageGRID system. Both appliances can operate as Gateway Nodes and Admin Nodes (primary or non-primary) at the same time.

#### Appliance features

Both models of the services appliance provide the following features:

- Gateway Node or Admin Node functions for a StorageGRID system.
- The StorageGRID Appliance Installer to simplify node deployment and configuration.
- When deployed, can access StorageGRID software from an existing Admin Node or from software downloaded to a local drive. To further simplify the deployment process, a recent version of the software is preloaded onto the appliance during manufacturing.
- A baseboard management controller (BMC) for monitoring and diagnosing some of the appliance hardware.
- The ability to connect to all three StorageGRID networks, including the Grid Network, the Admin Network, and the Client Network:
  - The SG100 supports up to four 10- or 25-GbE connections to the Grid Network and Client Network.
  - The SG1000 supports up to four 10-, 25-, 40-, or 100-GbE connections to the Grid Network and Client Network.

#### SG100 and SG1000 diagrams

This figure shows the front of the SG100 and the SG1000 with the bezel removed. From the front, the two appliances are identical except for the product name on the bezel.

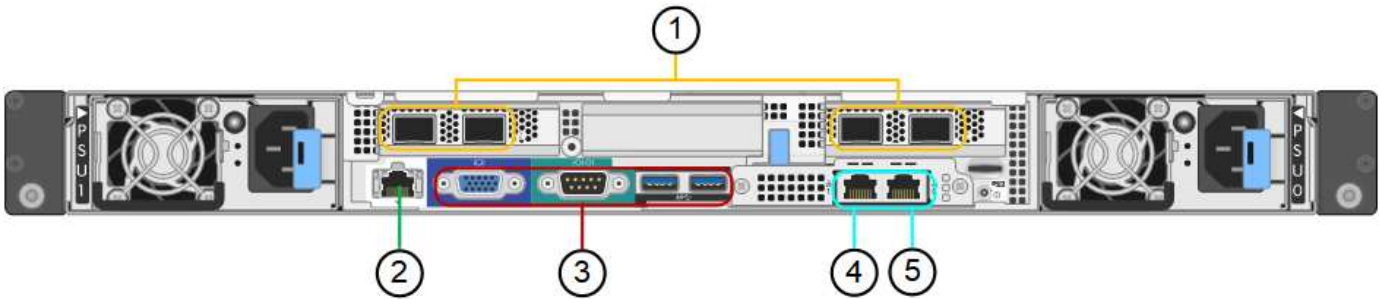


The two solid-state drives (SSDs), indicated by the orange outline, might be used for storing the StorageGRID operating system and are mirrored using RAID 1 for redundancy. When the SG100 or SG1000 services appliance is configured as an Admin Node, these drives are used to store audit logs, metrics, and database tables.

The remaining drive slots are blank.

### SG100 connectors

This figure shows the connectors on the back of the SG100.

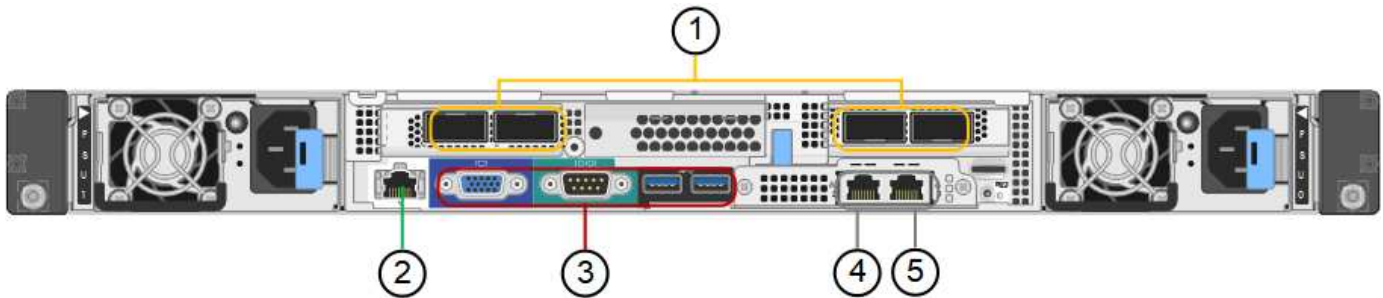


Callout	Port	Type	Use
1	Network ports 1-4	10/25-GbE, based on cable or SFP transceiver type (SFP28 and SFP+ modules are supported), switch speed, and configured link speed	Connect to the Grid Network and the Client Network for StorageGRID.
2	BMC management port	1-GbE (RJ-45)	Connect to the appliance baseboard management controller.
3	Diagnostic and support ports	<ul style="list-style-type: none"> <li>• VGA</li> <li>• Serial, 115200 8-N-1</li> <li>• USB</li> </ul>	Reserved for technical support use.
4	Admin Network port 1	1-GbE (RJ-45)	Connect the appliance to the Admin Network for StorageGRID.

Callout	Port	Type	Use
5	Admin Network port 2	1-GbE (RJ-45)	Options: <ul style="list-style-type: none"> <li>• Bond with management port 1 for a redundant connection to the Admin Network for StorageGRID.</li> <li>• Leave disconnected and available for temporary local access (IP 169.254.0.1).</li> <li>• During installation, use port 2 for IP configuration if DHCP-assigned IP addresses aren't available.</li> </ul>

### SG1000 connectors

This figure shows the connectors on the back of the SG1000.



Callout	Port	Type	Use
1	Network ports 1-4	10/25/40/100-GbE, based on cable or transceiver type, switch speed, and configured link speed. QSFP28 and QSFP+ (40/100GbE) are supported natively and SFP28/SFP+ transceivers can be used with a QSA (sold separately) to use 10/25GbE speeds.	Connect to the Grid Network and the Client Network for StorageGRID.
2	BMC management port	1-GbE (RJ-45)	Connect to the appliance baseboard management controller.

Callout	Port	Type	Use
3	Diagnostic and support ports	<ul style="list-style-type: none"> <li>• VGA</li> <li>• Serial, 115200 8-N-1</li> <li>• USB</li> </ul>	Reserved for technical support use.
4	Admin Network port 1	1-GbE (RJ-45)	Connect the appliance to the Admin Network for StorageGRID.
5	Admin Network port 2	1-GbE (RJ-45)	Options: <ul style="list-style-type: none"> <li>• Bond with management port 1 for a redundant connection to the Admin Network for StorageGRID.</li> <li>• Leave disconnected and available for temporary local access (IP 169.254.0.1).</li> <li>• During installation, use port 2 for IP configuration if DHCP-assigned IP addresses aren't available.</li> </ul>

### SG100 and SG1000 applications

You can configure the StorageGRID services appliances in various ways to provide gateway services as well as redundancy of some grid administration services.

Appliances can be deployed in the following ways:

- Add to a new or existing grid as a Gateway Node
- Add to a new grid as a primary or non-primary Admin Node, or to an existing grid as a non-primary Admin Node
- Operate as a Gateway Node and Admin Node (primary or non-primary) at the same time

The appliance facilitates the use of high availability (HA) groups and intelligent load balancing for S3 or Swift data path connections.

The following examples describe how you can maximize the capabilities of the appliance:

- Use two SG100 or two SG1000 appliances to provide gateway services by configuring them as Gateway Nodes.



Don't deploy the SG100 and SG1000 service appliances in the same site. Unpredictable performance might result.



- Use two SG100 or two SG1000 appliances to provide redundancy of some grid administration services. Do this by configuring each appliance as Admin Nodes.
- Use two SG100 or two SG1000 appliances to provide highly available load balancing and traffic shaping services accessed through one or more virtual IP addresses. Do this by configuring the appliances as any combination of Admin Nodes or Gateway Nodes and adding both nodes to the same HA group.



If you use Admin Nodes and Gateway Nodes in the same HA group, Admin Node-only port will not fail over. See the instructions for [configuring HA groups](#).

When used with StorageGRID storage appliances, both the SG100 and the SG1000 services appliances enable deployment of appliance-only grids with no dependencies on external hypervisors or compute hardware.

## SG5700 appliances: Overview

The SG5700 StorageGRID appliance is an integrated storage and computing platform that operates as a Storage Node in a StorageGRID grid. The appliance can be used in a hybrid grid environment that combines appliance Storage Nodes and virtual (software-based) Storage Nodes.

StorageGRID SG5700 series appliance provides the following features:

- Integrate the storage and computing elements for a StorageGRID Storage Node.
- Include the StorageGRID Appliance Installer to simplify Storage Node deployment and configuration.
- Includes E-Series SANtricity System Manager for hardware management and monitoring.
- Support up to four 10-GbE or 25-GbE connections to the StorageGRID Grid Network and Client Network.
- Support Full Disk Encryption (FDE) drives or FIPS drives. When these drives are used with the Drive Security feature in SANtricity System Manager, unauthorized access to data is prevented.

The SG5700 appliance is available in four models: the SG5712 and SG5712X, and the SG5760 and SG5760X. There are no specification or functional differences between the SG5712 and SG5712X except for the location of the interconnect ports on the storage controller. Similarly, there are no specification or functional differences between the SG5760 and SG5760X except for the location of the interconnect ports on the storage controller.

## SG5700 components

The SG5700 models include the following components:

**SG5712****Compute controller**

E5700SG controller

**Storage controller**

E2800A controller

**Chassis**

E-Series DE212C enclosure, a two rack-unit (2U) enclosure

**Drives**

12 NL-SAS drives (3.5-inch)

**Redundant power supplies and fans**

Two power-fan canisters

**SG5712X****Compute controller**

E5700SG controller

**Storage controller**

E2800B controller

**Chassis**

E-Series DE212C enclosure, a two rack-unit (2U) enclosure

**Drives**

12 NL-SAS drives (3.5-inch)

**Redundant power supplies and fans**

Two power-fan canisters

**SG5760****Compute controller**

E5700SG controller

**Storage controller**

E2800A controller

**Chassis**

E-Series DE460C enclosure, a four rack-unit (4U) enclosure

**Drives**

60 NL-SAS drives (3.5-inch)

**Redundant power supplies and fans**

Two power canisters and two fan canisters

**SG5760X**

**Compute controller**

E5700SG controller

**Storage controller**

E2800B controller

**Chassis**

E-Series DE460C enclosure, a four rack-unit (4U) enclosure

**Drives**

60 NL-SAS drives (3.5-inch)

**Redundant power supplies and fans**

Two power canisters and two fan canisters

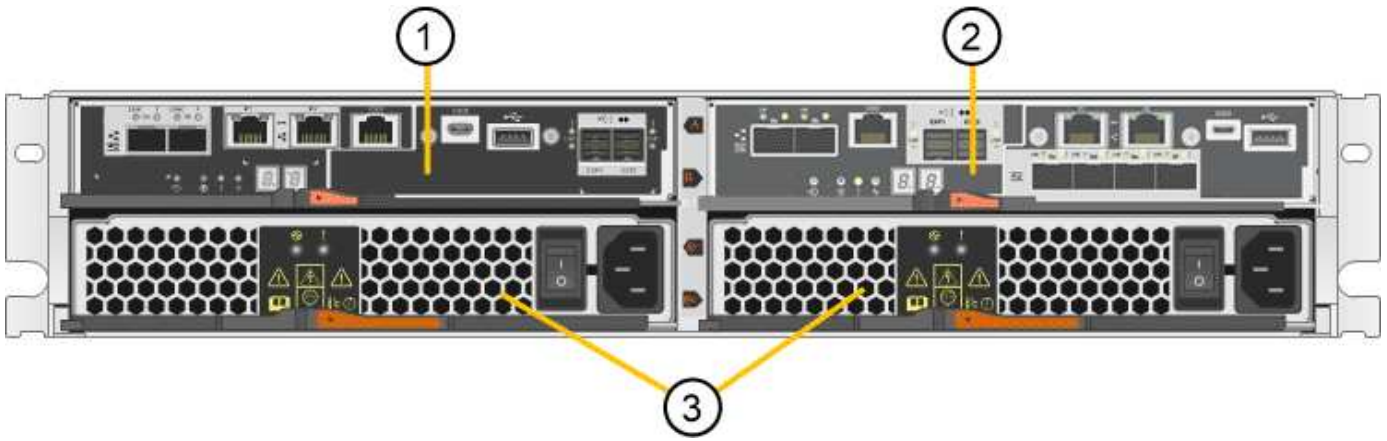
The maximum raw storage available in the StorageGRID appliance is fixed, based on the number of drives in each enclosure. You can't expand the available storage by adding a shelf with additional drives.

**SG5700 diagrams****SG5712 front and rear views**

The figures show the front and back of the SG5712, a 2U enclosure that holds 12 drives.

**SG5712 components**

The SG5712 includes two controllers and two power-fan canisters.



Callout	Description
1	E2800A controller (storage controller)
2	E5700SG controller (compute controller)
3	Power-fan canisters

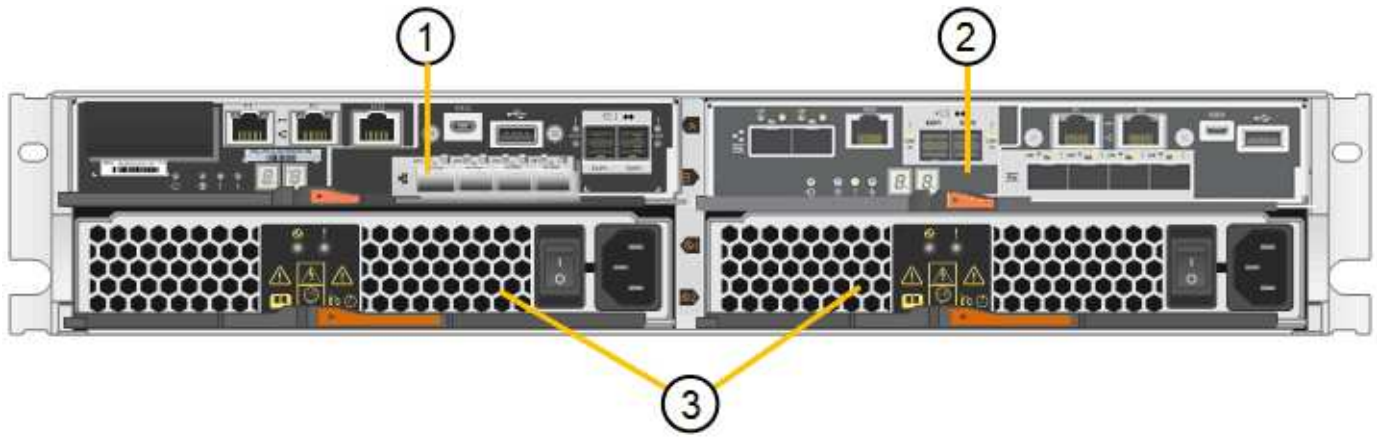
### SG5712X front and rear views

The figures show the front and back of the SG5712X, a 2U enclosure that holds 12 drives.



### SG5712X components

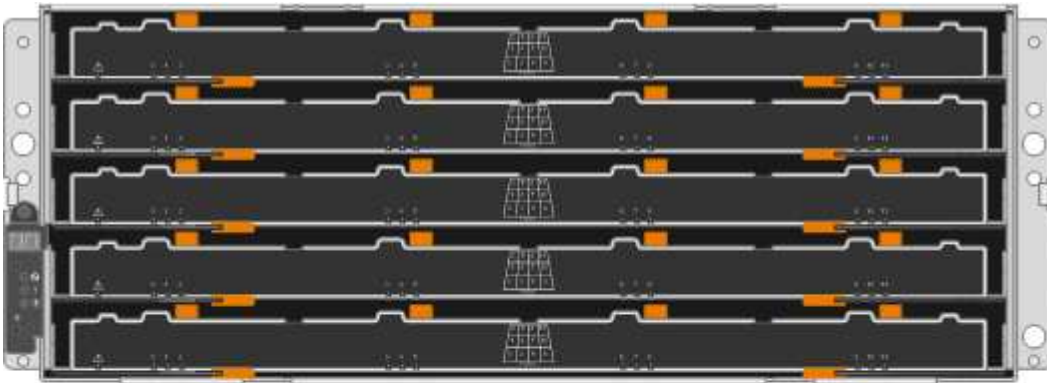
The SG5712X includes two controllers and two power-fan canisters.



Callout	Description
1	E2800B controller (storage controller)
2	E5700SG controller (compute controller)
3	Power-fan canisters

#### SG5760 front and rear views

The figures show the front and back of the SG5760 model, a 4U enclosure that holds 60 drives in 5 drive drawers.



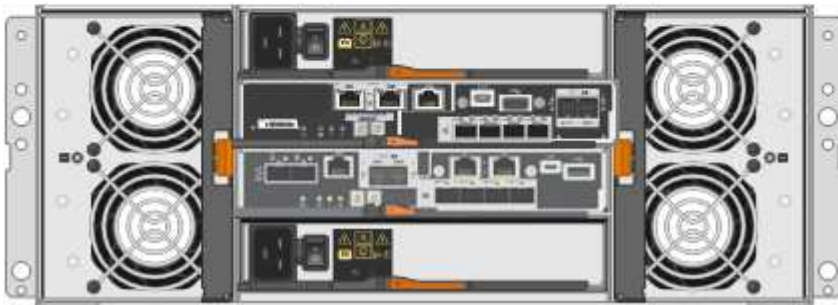
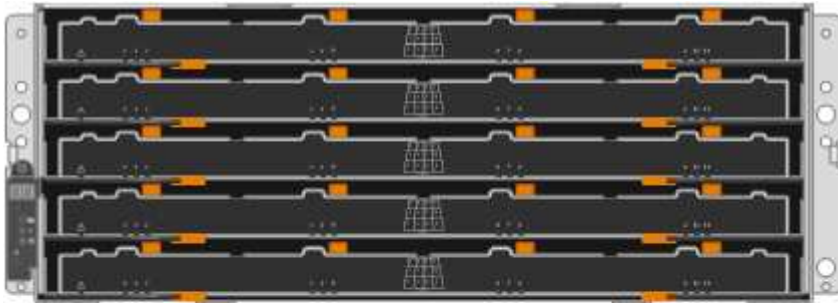
### SG5760 components

The SG5760 includes two controllers, two fan canisters, and two power canisters.

Callout	Description
1	E2800A controller (storage controller)
2	E5700SG controller (compute controller)
3	Fan canister (1 of 2)
4	Power canister (1 of 2)

### SG5760X front and rear views

The figures show the front and back of the SG5760X model, a 4U enclosure that holds 60 drives in 5 drive drawers.



### SG5760X components

The SG5760X includes two controllers, two fan canisters, and two power canisters.

Callout	Description
1	E2800B controller (storage controller)
2	E5700SG controller (compute controller)

Callout	Description
3	Fan canister (1 of 2)
4	Power canister (1 of 2)

### SG5700 controllers

Both the 12-drive SG5712 and SG5712X and the 60-drive SG5760 and SG5760X models of the StorageGRID appliance include an E5700SG compute controller and an E-Series E2800 storage controller.

- The SG5712 and SG5760 use a E2800A controller.
- The SG5712X and the SG5760X use a E2800B controller.

The E2800A and E2800B controllers are identical in specification and function except for the location of the interconnect ports.

### E5700SG compute controller

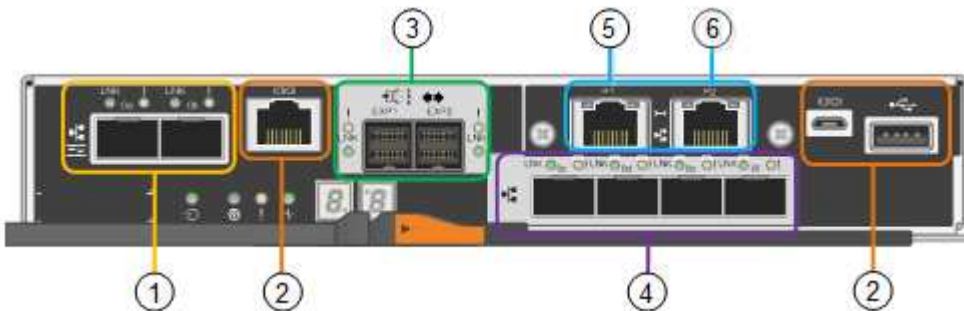
- Operates as the compute server for the appliance.
- Includes the StorageGRID Appliance Installer.



StorageGRID software is not preinstalled on the appliance. This software is accessed from the Admin Node when you deploy the appliance.

- Can connect to all three StorageGRID networks, including the Grid Network, the Admin Network, and the Client Network.
- Connects to the E2800 controller and operates as the initiator.

### E5700SG connectors



Callout	Port	Type	Use
1	Interconnect ports 1 and 2	16Gb/s Fibre Channel (FC), optical SFP	Connect the E5700SG controller to the E2800 controller.

Callout	Port	Type	Use
2	Diagnostic and support ports	<ul style="list-style-type: none"> <li>• RJ-45 serial port</li> <li>• Micro USB serial port</li> <li>• USB port</li> </ul>	Reserved for technical support.
3	Drive expansion ports	12Gb/s SAS	Not used. StorageGRID appliances don't support expansion drive shelves.
4	Network ports 1-4	10-GbE or 25-GbE, based on SFP transceiver type, switch speed, and configured link speed	Connect to the Grid Network and the Client Network for StorageGRID.
5	Management port 1	1-Gb (RJ-45) Ethernet	Connect to the Admin Network for StorageGRID.
6	Management port 2	1-Gb (RJ-45) Ethernet	Options: <ul style="list-style-type: none"> <li>• Bond with management port 1 for a redundant connection to the Admin Network for StorageGRID.</li> <li>• Leave unwired and available for temporary local access (IP 169.254.0.1).</li> <li>• During installation, use port 2 for IP configuration if DHCP-assigned IP addresses aren't available.</li> </ul>

### E2800 storage controller

There are two versions of the E2800 storage controller used in the SG5700 appliances: E2800A and E2800B. The E2800A does not have a HIC, and the E2800B has a four-port HIC. The two controller versions have identical specifications and function except for the location of the interconnect ports.

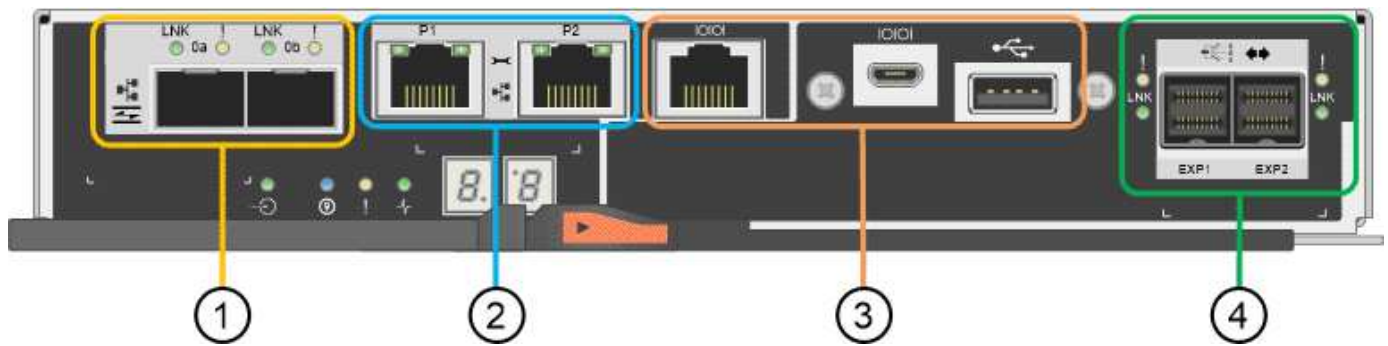
The E2800 series storage controller has the following specifications:

- Operates as the storage controller for the appliance.
- Manages the storage of data on the drives.
- Functions as a standard E-Series controller in simplex mode.
- Includes SANtricity OS Software (controller firmware).
- Includes SANtricity System Manager for monitoring appliance hardware and for managing alerts, the AutoSupport feature, and the Drive Security feature.

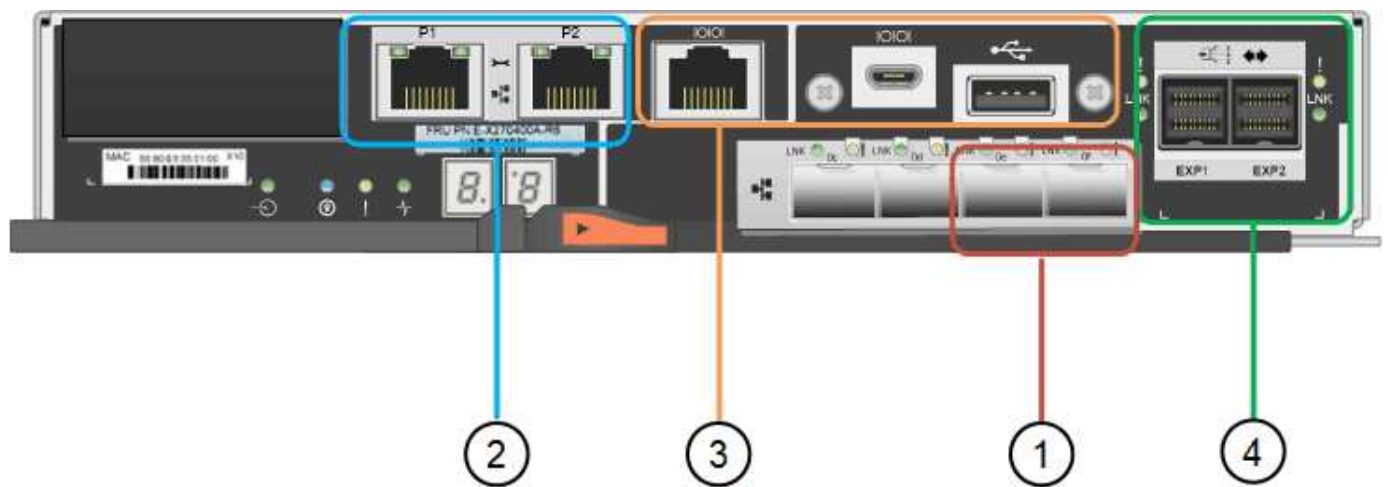


- Connects to the E5700SG controller and operates as the target.

### E2800A connectors



### E2800B connectors



Callout	Port	Type	Use
1	Interconnect ports 1 and 2	16Gb/s FC optical SFP	Connect the E2800 controller to the E5700SG controller.

Callout	Port	Type	Use
2	Management ports 1 and 2	1-Gb (RJ-45) Ethernet	<ul style="list-style-type: none"> <li>• Port 1 Options: <ul style="list-style-type: none"> <li>◦ Connect to a management network to enable direct TCP/IP access to SANtricity System Manager</li> <li>◦ Leave unwired to save a switch port and IP address. Access SANtricity System Manager using the Grid Manager or Storage Grid Appliance Installer UIs.</li> </ul> </li> </ul> <p><b>Note:</b> some optional SANtricity functionality, such as NTP sync for accurate log timestamps, is not available when you choose to leave Port 1 unwired.</p> <p><b>Note:</b> StorageGRID 11.5 or greater, and SANtricity 11.70 or greater, are required when you leave Port 1 unwired.</p> <ul style="list-style-type: none"> <li>• Port 2 is reserved for technical support use.</li> </ul>
3	Diagnostic and support ports	<ul style="list-style-type: none"> <li>• RJ-45 serial port</li> <li>• Micro USB serial port</li> <li>• USB port</li> </ul>	Reserved for technical support use.
4	Drive expansion ports.	12Gb/s SAS	Not used.

#### Related information

[NetApp E-Series Systems Documentation Site](#)

### SG6060 and SG6060X appliances: Overview

The StorageGRID SG6060 and SG6060X appliances each include a compute controller and a storage controller shelf that contains two storage controllers and 60 drives.

Optionally, 60-drive expansion shelves can be added to both appliances. There are no specification or functional differences between the SG6060 and SG6060X except for the location of the interconnect ports on

the storage controller.

## **SG6060 and SG6060X components**

The SG6060 and SG6060X appliances include the following components:

### **Compute controller**

The SG6000-CN controller is a one-rack unit (1U) server that includes:

- 40 cores (80 threads)
- 192 GB RAM
- Up to 4 × 25 Gbps aggregate Ethernet bandwidth
- 4 × 16 Gbps Fibre Channel (FC) interconnect
- Baseboard management controller (BMC) that simplifies hardware management
- Redundant power supplies

### **Storage controller shelf**

The E-Series E2860 controller shelf (storage array) is a 4U shelf that includes:

- Two E2800 series controllers (duplex configuration) to provide storage controller failover support
  - The SG6060 contains E2800A storage controllers
  - The SG6060X contains E2800B storage controllers
- Five-drawer drive shelf that holds sixty 3.5-inch drives (2 solid-state drives, or SSDs, and 58 NL-SAS drives)
- Redundant power supplies and fans

### **Optional: Storage expansion shelves**

Each SG6060 and SG6060X appliance can have one or two expansion shelves for a total of 180 drives (two of these drives are reserved for E-Series read cache).

**Note:** Expansion shelves can be installed during initial deployment or added later.

The E-Series DE460C enclosure is a 4U shelf that includes:

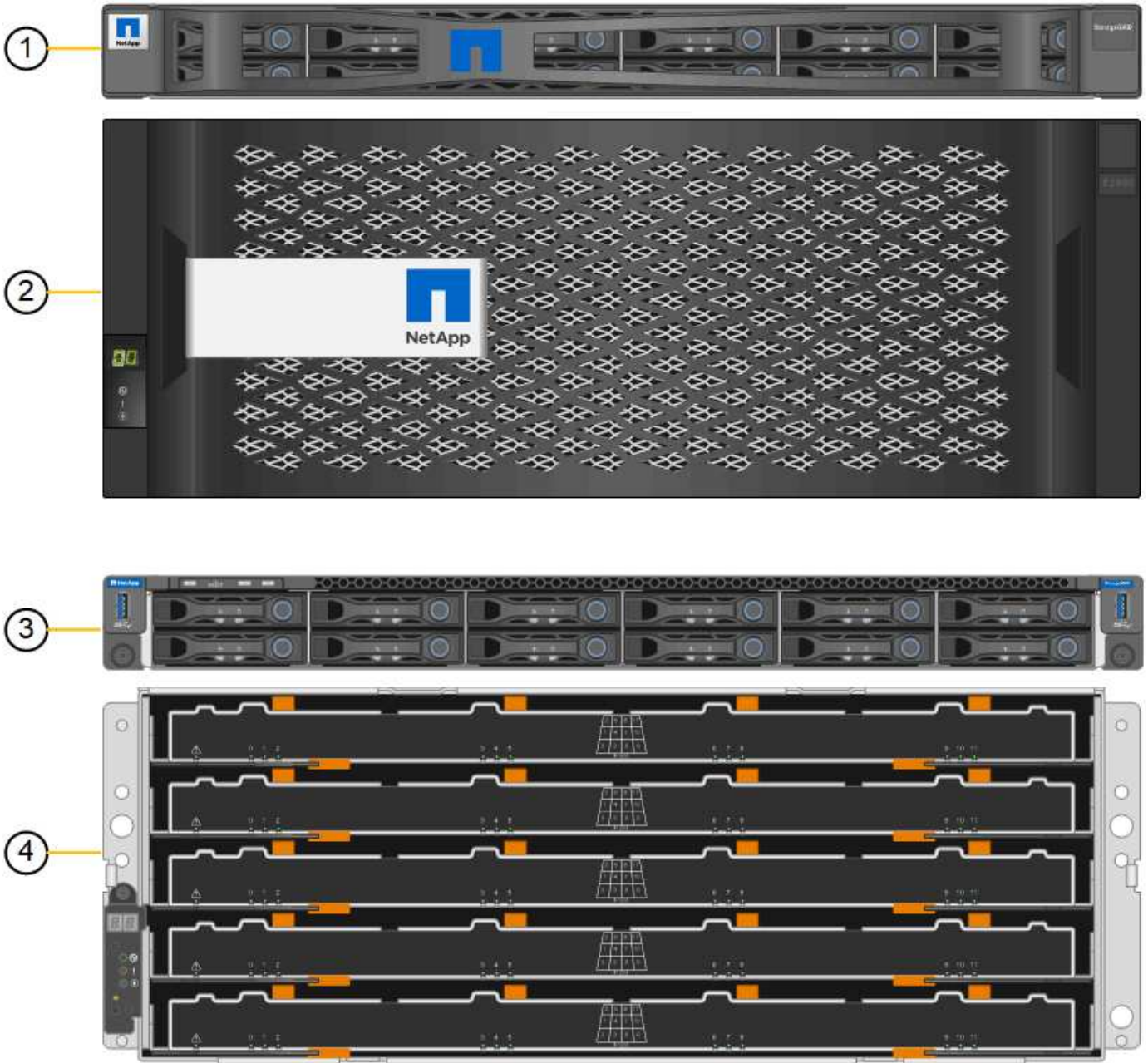
- Two input/output modules (IOMs)
- Five drawers, each holding 12 NL-SAS drives, for a total of 60 drives
- Redundant power supplies and fans

## **SG6060 and SG6060X diagrams**

The fronts of the SG6060 and SG6060X are identical.

### **SG6060 or SG6060X front view**

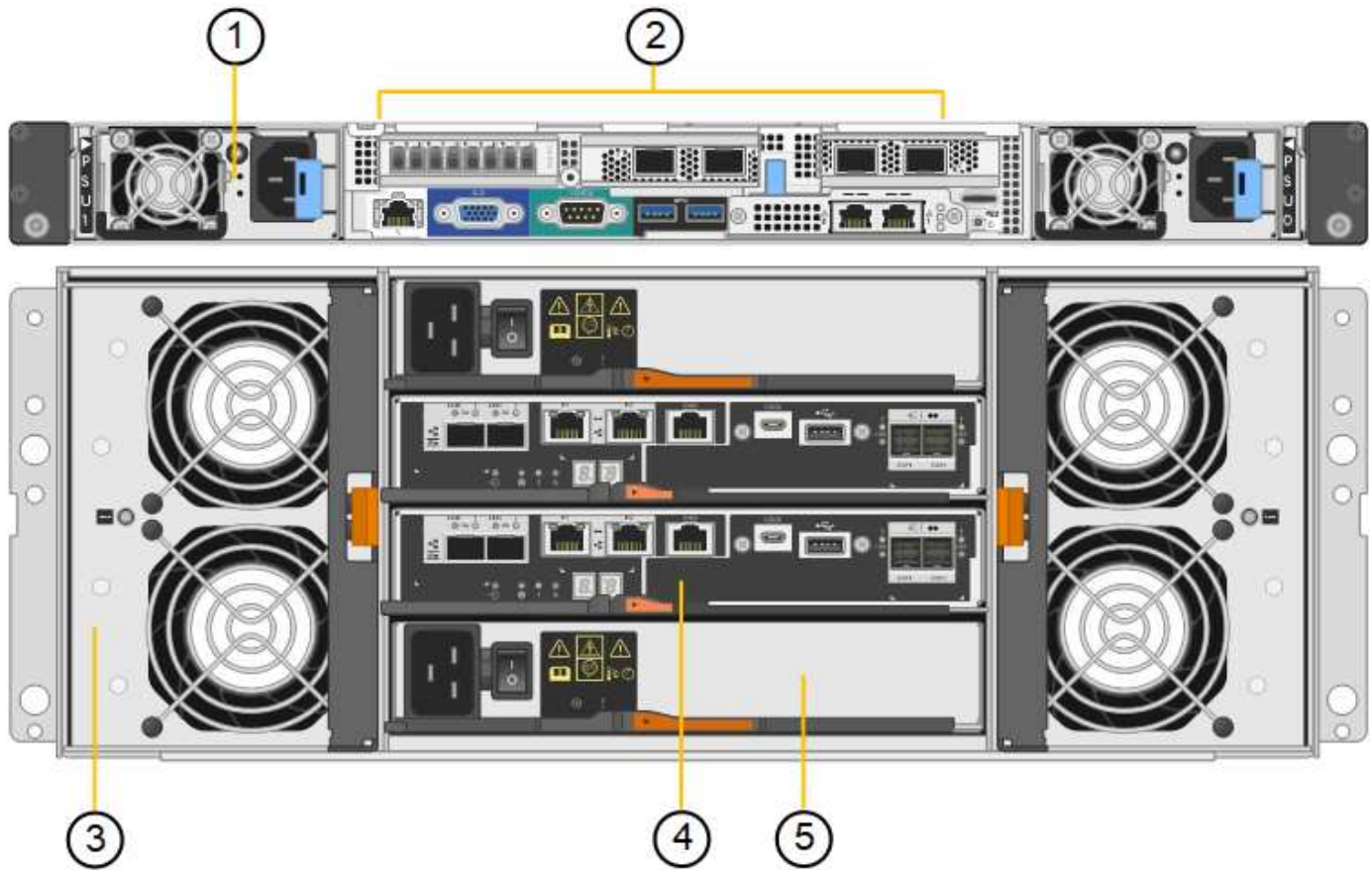
This figure shows the front of the SG6060 or SG6060X, which includes a 1U compute controller and a 4U shelf containing two storage controllers and 60 drives in five drive drawers.



Callout	Description
1	SG6000-CN compute controller with front bezel
2	E2860 controller shelf with front bezel (optional expansion shelf appears identical)
3	SG6000-CN compute controller with front bezel removed
4	E2860 controller shelf with front bezel removed (optional expansion shelf appears identical)

### SG6060 rear view

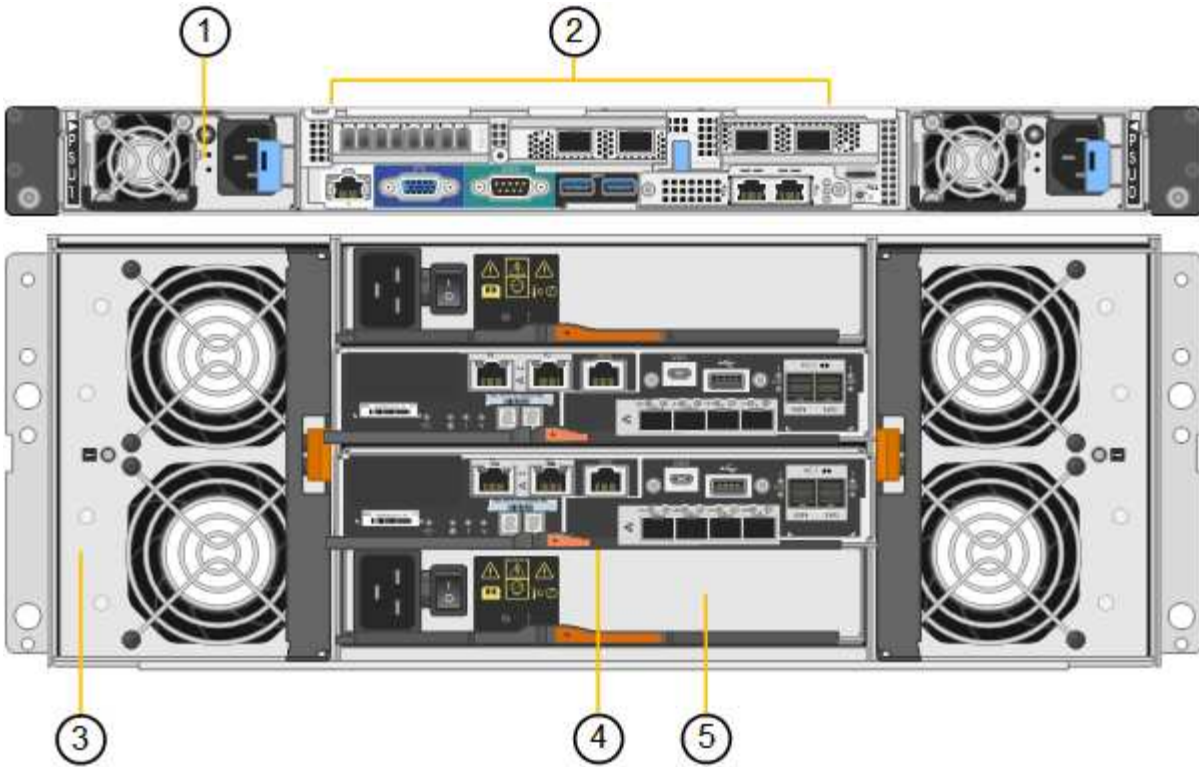
This figure shows the back of the SG6060, including the compute and storage controllers, fans, and power supplies.



Callout	Description
1	Power supply (1 of 2) for SG6000-CN compute controller
2	Connectors for SG6000-CN compute controller
3	Fan (1 of 2) for E2860 controller shelf
4	E-Series E2800A storage controller (1 of 2) and connectors
5	Power supply (1 of 2) for E2860 controller shelf

### SG6060X rear view

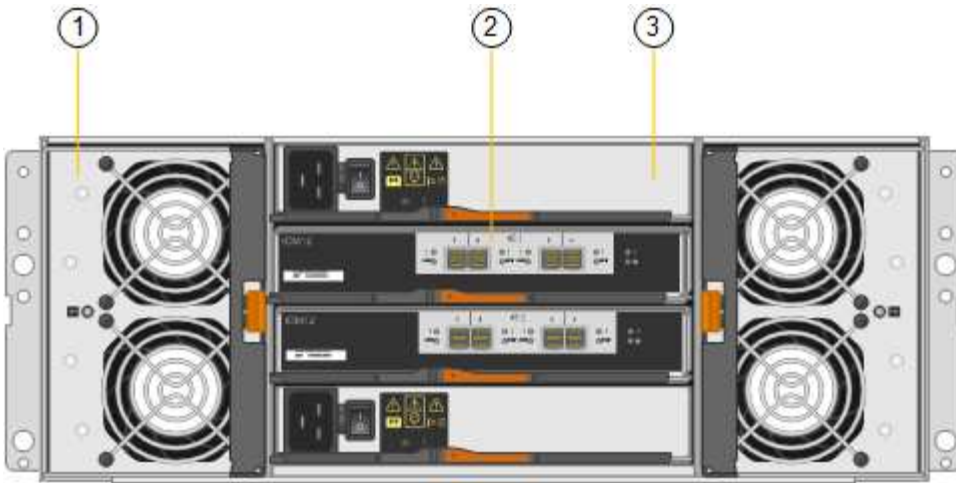
This figure shows the back of the SG6060X.



Callout	Description
1	Power supply (1 of 2) for SG6000-CN compute controller
2	Connectors for SG6000-CN compute controller
3	Fan (1 of 2) for E2860 controller shelf
4	E-Series E2800B storage controller (1 of 2) and connectors
5	Power supply (1 of 2) for E2860 controller shelf

### Expansion shelf

This figure shows the back of the optional expansion shelf for the SG6060 and SG6060X, including the input/output modules (IOMs), fans, and power supplies. Each SG6060 can be installed with one or two expansion shelves, which can be included in the initial installation or added later.



Callout	Description
1	Fan (1 of 2) for expansion shelf
2	IOM (1 of 2) for expansion shelf
3	Power supply (1 of 2) for expansion shelf

### SG6000 controllers

Each model of the StorageGRID SG6000 appliance includes an SG6000-CN compute controller in a 1U enclosure and duplex E-Series storage controllers in a 2U or 4U enclosure, depending on the model. Review the diagrams to learn more about each type of controller.

#### SG6000-CN compute controller

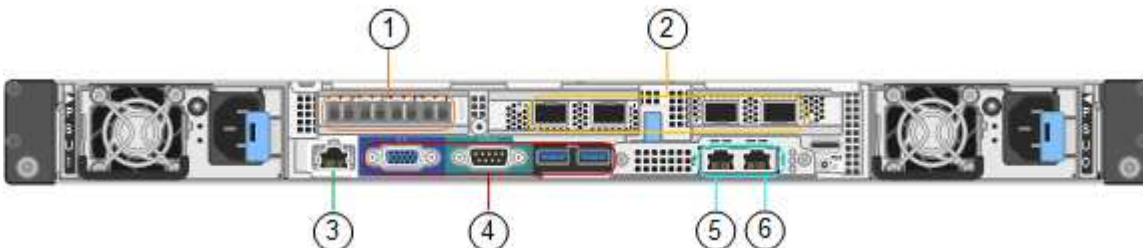
- Provides compute resources for the appliance.
- Includes the StorageGRID Appliance Installer.



StorageGRID software is not preinstalled on the appliance. This software is retrieved from the Admin Node when you deploy the appliance.

- Can connect to all three StorageGRID networks, including the Grid Network, the Admin Network, and the Client Network.
- Connects to the E-Series storage controllers and operates as the initiator.

#### SG6000-CN connectors



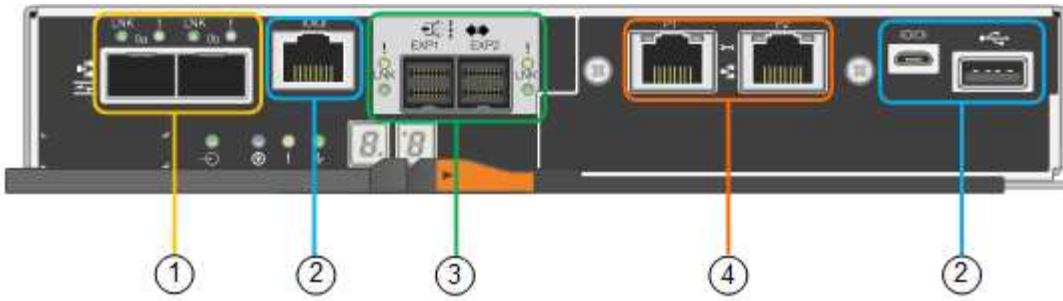
Callout	Port	Type	Use
1	Interconnect ports 1-4	16-Gb/s Fibre Channel (FC), with integrated optics	Connect the SG6000-CN controller to the E2800 controllers (two connections to each E2800).
2	Network ports 1-4	10-GbE or 25-GbE, based on cable or SFP transceiver type, switch speed, and configured link speed	Connect to the Grid Network and the Client Network for StorageGRID.
3	BMC management port	1-GbE (RJ-45)	Connect to the SG6000-CN baseboard management controller.
4	Diagnostic and support ports	<ul style="list-style-type: none"> <li>• VGA</li> <li>• Serial, 115200 8-N-1</li> <li>• USB</li> </ul>	Reserved for technical support use.
5	Admin Network port 1	1-GbE (RJ-45)	Connect the SG6000-CN to the Admin Network for StorageGRID.
6	Admin Network port 2	1-GbE (RJ-45)	Options: <ul style="list-style-type: none"> <li>• Bond with management port 1 for a redundant connection to the Admin Network for StorageGRID.</li> <li>• Leave unwired and available for temporary local access (IP 169.254.0.1).</li> <li>• During installation, use port 2 for IP configuration if DHCP-assigned IP addresses aren't available.</li> </ul>

#### SGF6024: EF570 storage controllers

- Two controllers for failover support.
- Manage the storage of data on the drives.
- Function as standard E-Series controllers in a duplex configuration.
- Include SANtricity OS Software (controller firmware).
- Include SANtricity System Manager for monitoring storage hardware and for managing alerts, the AutoSupport feature, and the Drive Security feature.
- Connect to the SG6000-CN controller and provide access to the flash storage.

#### EF570 connectors





Callout	Port	Type	Use
1	Interconnect ports 1 and 2	16-Gb/s FC optical SFP	<p>Connect each of the EF570 controllers to the SG6000-CN controller.</p> <p>There are four connections to the SG6000-CN controller (two from each EF570).</p>
2	Diagnostic and support ports	<ul style="list-style-type: none"> <li>• RJ-45 serial port</li> <li>• Micro USB serial port</li> <li>• USB port</li> </ul>	Reserved for technical support use.
3	Drive expansion ports	12Gb/s SAS	Not used. The SGF6024 appliance does not support expansion drive shelves.
4	Management ports 1 and 2	1-Gb (RJ-45) Ethernet	<ul style="list-style-type: none"> <li>• Port 1 connects to the network where you access SANtricity System Manager on a browser.</li> <li>• Port 2 is reserved for technical support use.</li> </ul>

#### SG6060 and SG6060X: E2800 storage controllers

- Two controllers for failover support.
- Manage the storage of data on the drives.
- Function as standard E-Series controllers in a duplex configuration.
- Include SANtricity OS Software (controller firmware).
- Include SANtricity System Manager for monitoring storage hardware and for managing alerts, the AutoSupport feature, and the Drive Security feature.
- Connect to the SG6000-CN controller and provide access to the storage.

The SG6060 and SG6060X use E2800 storage controllers.

Appliance	Controller	Controller HIC
SG6060	Two E2800A storage controllers	None

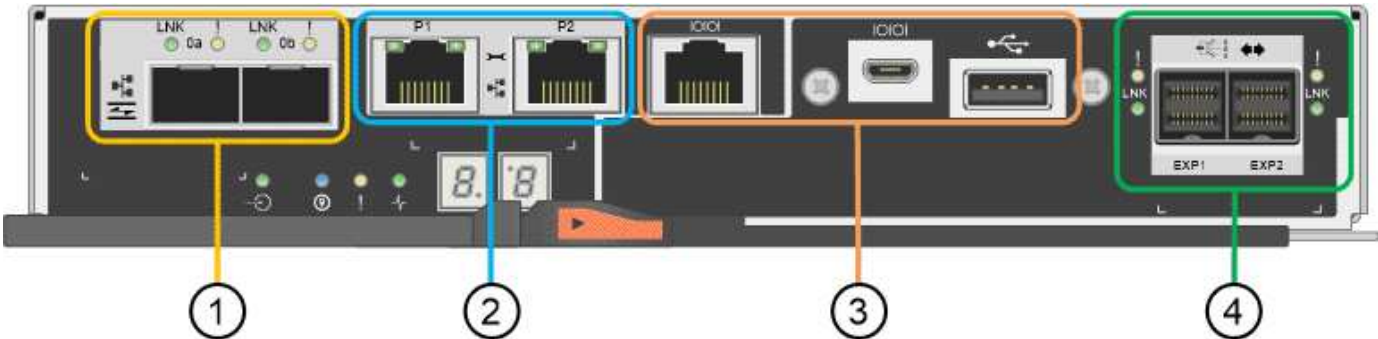
Appliance	Controller	Controller HIC
SG6060X	Two E2800B storage controllers	Four-port HIC

The E2800A and the E2800B storage controllers are identical in specifications and function except for the location of the interconnect ports.



Don't use an E2800A and an E2800B in the same appliance.

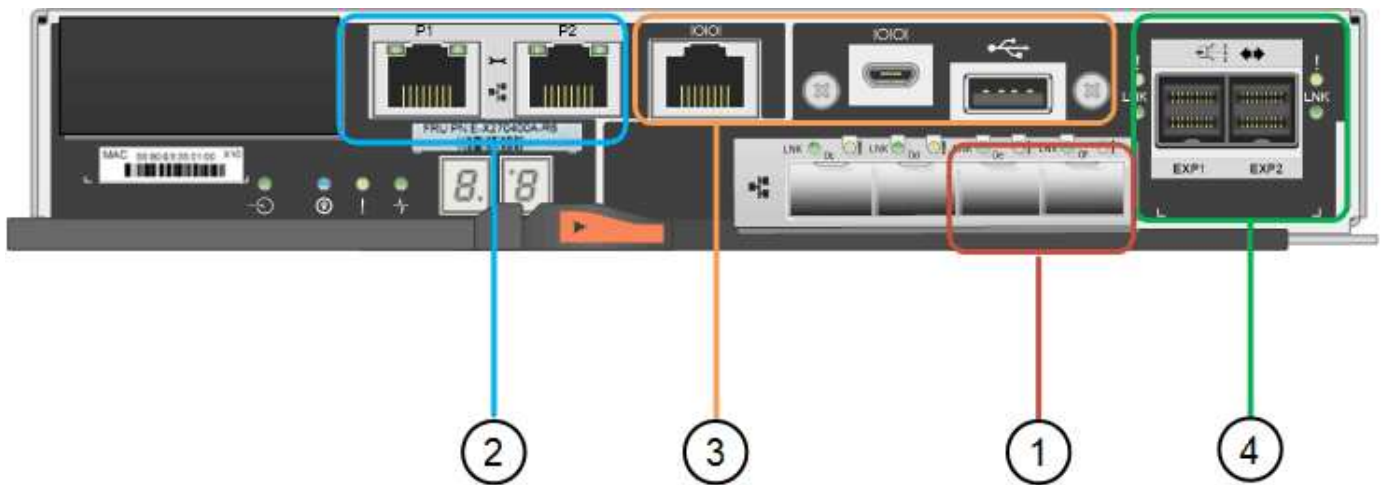
**E2800A connectors**



Callout	Port	Type	Use
1	Interconnect ports 1 and 2	16-Gb/s FC optical SFP	<p>Connect each of the E2800A controllers to the SG6000-CN controller.</p> <p>There are four connections to the SG6000-CN controller (two from each E2800A).</p>

Callout	Port	Type	Use
2	Management ports 1 and 2	1-Gb (RJ-45) Ethernet	<ul style="list-style-type: none"> <li>Port 1 Options: <ul style="list-style-type: none"> <li>Connect to a management network to enable direct TCP/IP access to SANtricity System Manager</li> <li>Leave unwired to save a switch port and IP address. Access SANtricity System Manager using the Grid Manager or Storage Grid Appliance Installer UIs.</li> </ul> </li> </ul> <p><b>Note:</b> some optional SANtricity functionality, such as NTP sync for accurate log timestamps, is not available when you choose to leave Port 1 unwired.</p> <p><b>Note:</b> StorageGRID 11.5 or greater, and SANtricity 11.70 or greater, are required when you leave Port 1 unwired.</p> <ul style="list-style-type: none"> <li>Port 2 is reserved for technical support use.</li> </ul>
3	Diagnostic and support ports	<ul style="list-style-type: none"> <li>RJ-45 serial port</li> <li>Micro USB serial port</li> <li>USB port</li> </ul>	Reserved for technical support use.
4	Drive expansion ports 1 and 2	12Gb/s SAS	Connect the ports to the drive expansion ports on the IOMs in the expansion shelf.

### E2800B connectors

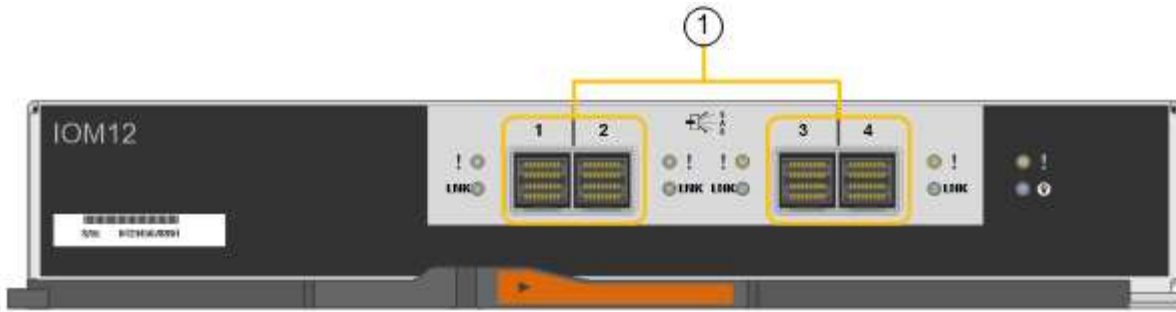


Callout	Port	Type	Use
1	Interconnect ports 1 and 2	16-Gb/s FC optical SFP	<p>Connect each of the E2800B controllers to the SG6000-CN controller.</p> <p>There are four connections to the SG6000-CN controller (two from each E2800B).</p>
2	Management ports 1 and 2	1-Gb (RJ-45) Ethernet	<ul style="list-style-type: none"> <li>• Port 1 Options: <ul style="list-style-type: none"> <li>◦ Connect to a management network to enable direct TCP/IP access to SANtricity System Manager</li> <li>◦ Leave unwired to save a switch port and IP address. Access SANtricity System Manager using the Grid Manager or Storage Grid Appliance Installer UIs.</li> </ul> </li> </ul> <p><b>Note:</b> some optional SANtricity functionality, such as NTP sync for accurate log timestamps, is not available when you choose to leave Port 1 unwired.</p> <p><b>Note:</b> StorageGRID 11.5 or greater, and SANtricity 11.70 or greater, are required when you leave Port 1 unwired.</p> <ul style="list-style-type: none"> <li>• Port 2 is reserved for technical support use.</li> </ul>
3	Diagnostic and support ports	<ul style="list-style-type: none"> <li>• RJ-45 serial port</li> <li>• Micro USB serial port</li> <li>• USB port</li> </ul>	Reserved for technical support use.
4	Drive expansion ports 1 and 2	12Gb/s SAS	Connect the ports to the drive expansion ports on the IOMs in the expansion shelf.

### SG6060 and SG6060X: IOMs for optional expansion shelves

The expansion shelf contains two input/output modules (IOMs) that connect to the storage controllers or to other expansion shelves.

### IOM connectors



Callout	Port	Type	Use
1	Drive expansion ports 1-4	12Gb/s SAS	Connect each port to the storage controllers or additional expansion shelf (if any).

## SG6100 appliances: Overview

The StorageGRID SGF6112 appliance operates as a Storage Node in a StorageGRID system. The appliance can be used in a hybrid grid environment that combines appliance Storage Nodes and virtual (software-based) Storage Nodes.

The SGF6112 appliance provides the following features:

- 12 NVMe (nonvolatile memory express) SSD drives with integrated compute and storage controllers.
- Integrates the storage and computing elements for a StorageGRID Storage Node.
- Includes the StorageGRID Appliance Installer to simplify Storage Node deployment and configuration.
- Includes a baseboard management controller (BMC) for monitoring and diagnosing the hardware in the compute controller.
- Supports up to four 10-GbE or 25-GbE connections to the StorageGRID Grid Network and Client Network.

### SGF6112 hardware description

The StorageGRID SGF6112 is an all-flash appliance that features a compact design with compute controller and storage controller integrated into a 1U chassis. The appliance supports 12 SSD NVMe drives with a storage capacity of up to 15.3 TB per drive.

### Resilient object storage

The SGF6112 is designed with SSDs in a RAID that provides the following data protection features:

- Ability to function after the failure of a single SSD with no impact on object availability.
- Ability to function after multiple SSD failures with a minimum necessary reduction in object availability (based on the design of the underlying RAID scheme).
- Fully recoverable, while in service, from SSD failures that don't result in extreme damage to the RAID housing the node's root volume (the StorageGRID operating system).

### SGF6112 hardware components

The SGF6112 appliance includes the following components:

## Compute and storage platform

A one-rack unit (1U) server that includes:

- Two 2.1/2.6 GHz 165 W processors providing 48 cores
- 256 GB RAM
- 2 × 1/10 GBase-T ports
- 4 × 10/25 GbE Ethernet ports
- 1 × 256 GB Internal Boot drive (includes StorageGRID software)
- Baseboard management controller (BMC) that simplifies hardware management
- Redundant power supplies and fans

## SGF6112 diagrams

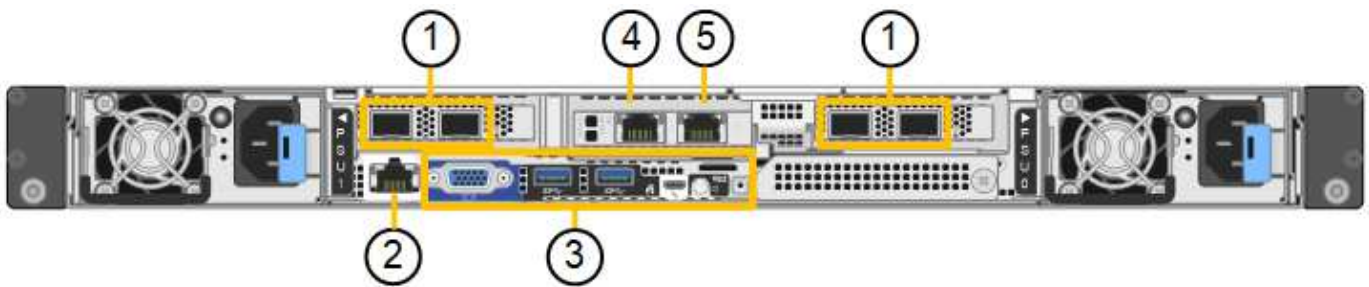
### SGF6112 front view

This figure shows the front of the SGF6112 without the bezel. The appliance includes a 1U compute and storage platform that contains 12 SSD drives.



### SGF6112 rear view

This figure shows the back of the SGF6112, including the ports, fans, and power supplies.



Callout	Port	Type	Use
1	Network ports 1-4	10/25-GbE, based on cable or SFP transceiver type (SFP28 and SFP+ modules are supported), switch speed, and configured link speed.	Connect to the Grid Network and the Client Network for StorageGRID.
2	BMC management port	1-GbE (RJ-45)	Connect to the appliance baseboard management controller.

Callout	Port	Type	Use
3	Diagnostic and support ports	<ul style="list-style-type: none"> <li>• VGA</li> <li>• USB</li> <li>• Micro-USB console port</li> <li>• Micro-SD slot module</li> </ul>	Reserved for technical support use.
4	Admin Network port 1	1/10-GbE (RJ-45)	Connect the appliance to the Admin Network for StorageGRID.
5	Admin Network port 2	1/10-GbE (RJ-45)	Options: <ul style="list-style-type: none"> <li>• Bond with Admin Network port 1 for a redundant connection to the Admin Network for StorageGRID.</li> <li>• Leave disconnected and available for temporary local access (IP 169.254.0.1).</li> <li>• During installation, use port 2 for IP configuration if DHCP-assigned IP addresses aren't available.</li> </ul>

# Install StorageGRID appliance hardware

## Quick start for appliance installation

Follow these high-level steps to install and set up a StorageGRID appliance and deploy it as a node in your StorageGRID system.

1

### Prepare for installation

1. Work with your NetApp Professional Services consultant to automate installation and configuration. See [Automate appliance installation and configuration](#).

This step is optional. However, streamlining and automating configuration steps can save time and provide consistency in the configuration of multiple appliances.

2. [Prepare site](#)
3. [Unpack boxes](#)
4. [Obtain additional equipment and tools](#)
5. [Review web browser requirements](#)
6. [Gather network information](#)

2

### Install hardware

1. [Register hardware](#)
2. Install into cabinet or rack
  - [SG100 and SG1000](#)
  - [SG5700](#)
  - [SG6000](#)
  - [SG6100](#)
3. [Cable appliance](#)
4. [Connect power cords and apply power](#)
5. [View status indicators and codes](#)

3

### Set up hardware

If you are configuring and deploying more than one appliance, use the NetApp ConfigBuilder tool to automate the following configuration and deployment steps. For guidance, contact your NetApp Professional Services consultant. See [Automate appliance installation and configuration](#).

1. Configure StorageGRID connections
  - [Access StorageGRID Appliance Installer](#) and verify you are running most recent version
  - [Configure network links](#)
  - [Configure StorageGRID IP addresses](#)



- [Verify network connections](#)
  - [Verify port-level network connections](#)
2. [Access and configure SANtricity System Manager](#) (SG6000 and SG5700)
  3. [Configure the BMC interface](#) (SG100, SG1000, SG6000, and SG6100)
  4. Perform optional setup steps
    - [Enable node or drive encryption](#)
    - [Change RAID mode](#) (SG6000 and SG5700)
    - [Remap network ports](#)

## 4

### Deploy appliance node

Deploy the appliance as a new node in your StorageGRID system.

- [Deploy appliance Storage Node](#)
- [Deploy services appliance node](#)

## Prepare for StorageGRID installation

### Prepare site

Before installing the appliance, you must make sure that the site and the cabinet or rack you plan to use meet the specifications for a StorageGRID appliance.

#### Steps

1. Confirm that the site meets the requirements for temperature, humidity, altitude range, airflow, heat dissipation, wiring, power, and grounding. See the [NetApp Hardware Universe](#) for more information.
2. Confirm that your location provides the correct voltage of AC power:

Model	Requirement
SG100 and SG1000	120 to 240 volts AC
SG5760	240-volt AC
SGF6024	120-volt AC
SG6060	240-volt AC
SGF6112	100 to 240 volts AC

3. Obtain a 19-inch (48.3-cm) cabinet or rack to fit shelves of the following size (without cables).

**SG100 and SG1000**

Height	Width	Depth	Maximum weight
1.70 in. (4.32 cm)	17.32 in. (44.0 cm)	32.0 in. (81.3 cm)	39 lb. (17.7 kg)

**SG5700**

Appliance model	Height	Width	Depth	Maximum weight
SG5712 (12 drives)	3.41 in. (8.68 cm)	17.6 in. (44.7 cm)	21.1 in. (53.6 cm)	63.9 lb (29.0 kg)
SG5760 (60 drives)	6.87 in. (17.46 cm)	17.66 in. (44.86 cm)	38.25 in. (97.16 cm)	250 lb. (113 kg)

**SG6000**

Type of shelf	Height	Width	Depth	Maximum weight
E2860 controller shelf (SG6060)	6.87 in. (17.46 cm)	17.66 in. (44.86 cm)	38.25 in. (97.16 cm)	250 lb. (113 kg)
Expansion shelf (SG6060) - Optional	6.87 in. (17.46 cm)	17.66 in. (44.86 cm)	38.25 in. (97.16 cm)	250 lb. (113 kg)
EF570 controller shelf (SGF6024)	3.35 in. (8.50 cm)	17.66 in. (44.86 cm)	19.00 in. (48.26 cm)	51.74 lb. (23.47 kg)
SG6000-CN compute controller	1.70 in. (4.32 cm)	17.32 in. (44.0 cm)	32.0 in. (81.3 cm)	39 lb. (17.7 kg)

**SG6100**

Height	Width	Depth	Maximum weight
1.70 in. (4.31 cm)	18.98 in. (48.2 cm)	33.11 in. (84.1 cm)	43.83 lb. (19.88 kg)

4. Decide where you are going to install the appliance.



When installing the E2860 controller shelf or optional expansion shelves, install hardware from the bottom to the top of the rack or cabinet to prevent the equipment from tipping over. To ensure that the heaviest equipment is at the bottom of the cabinet or rack, install the SG6000-CN controller above the E2860 controller shelf and expansion shelves.



Before committing to the installation, verify that the 0.5m optic cables shipped with an SG6000 appliance, or cables that you supply, are long enough for the planned layout.

5. Install any required network switches. See the [NetApp Interoperability Matrix Tool](#) for compatibility information.

## Unpack boxes

Before installing your StorageGRID appliance, unpack all boxes and compare the contents to the items on the packing slip.

## SG100 and SG1000

- Hardware

### SG100 or SG1000



### Rail kit with instructions



- Power cords



Your cabinet might have special power cords that you use instead of the power cords that ship with the appliance.

### Two power cords for your country



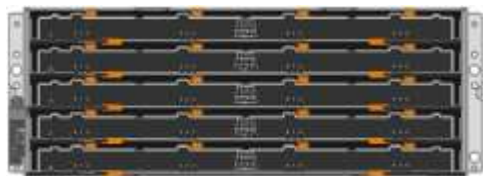
## SG5700

- Hardware

### SG5712 appliance with 12 drives installed



### SG5760 appliance with no drives installed



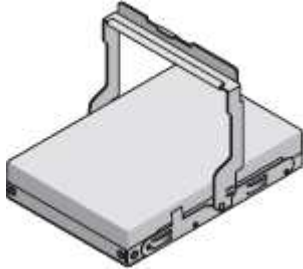
### Front bezel for the appliance



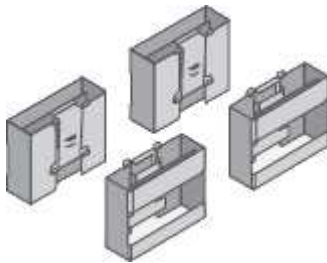
**Rail kit with instructions**



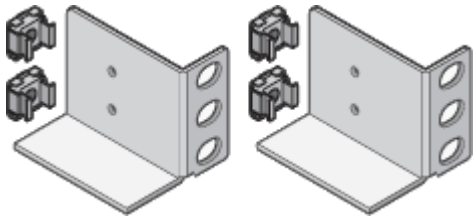
**SG5760: Sixty drives**



**SG5760: Handles**



**SG5760: Back brackets and cage nuts for square-hole rack installation**



• **Cables and connectors**



Your cabinet might have special power cords that you use instead of the power cords that ship with the appliance.

**Two power cords for your country**



**Optical cables and SFP transceivers**



- Two optical cables for the FC interconnect ports

- Eight SFP+ transceivers, compatible with both the four 16Gb/s FC interconnect ports and the four 10-GbE network ports

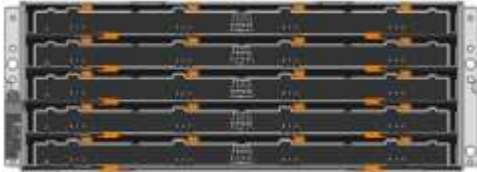
## SG6000

- SG6060 hardware

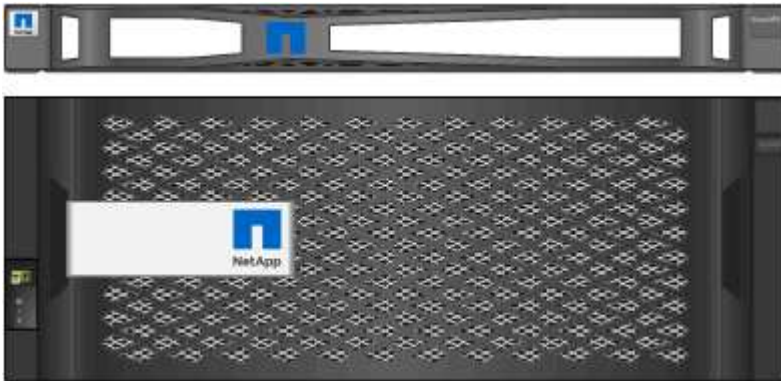
### SG6000-CN controller



### E2860 controller shelf with no drives installed



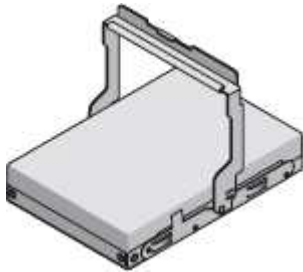
### Two front bezels



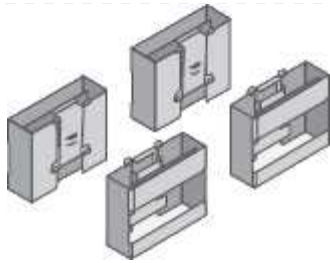
### Two rail kits with instructions



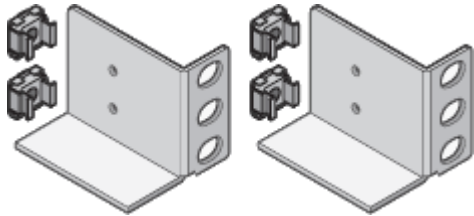
### 60 drives (2 SSD and 58 NL-SAS)



### Four handles



**Back brackets and cage nuts for square-hole rack installation**



- **SG6060 expansion shelf**

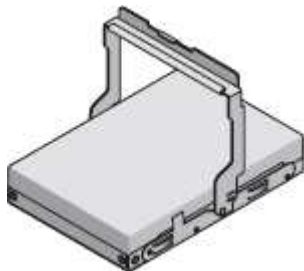
**Expansion shelf with no drives installed**



**Front bezel**



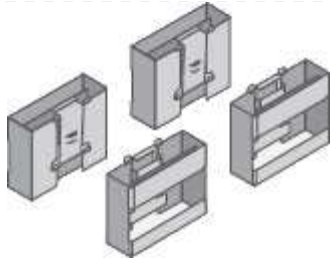
**60 NL-SAS drives**



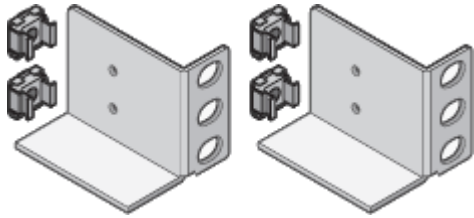
**One rail kit with instructions**



**Four handles**



**Back brackets and cage nuts for square-hole rack installation**



- **SGF6024 hardware**

**SG6000-CN controller**



**EF570 flash array with 24 solid state (flash) drives installed**



**Two front bezels**



**Two rail kits with instructions**



**Shelf endcaps**



- **Cables and connectors**





Your cabinet might have special power cords that you use instead of the power cords that ship with the appliance.

#### Four power cords for your country



#### Optical cables and SFP transceivers



- Four optical cables for the FC interconnect ports
- Four SFP+ transceivers, which support 16-Gb/s FC

#### Optional: Two SAS cables for connecting each SG6060 expansion shelf



### SG6100

- Hardware

#### SGF6112



#### Rail kit with instructions



#### Front bezel



- Power cords



Your cabinet might have special power cords that you use instead of the power cords that ship with the appliance.

#### Two power cords for your country



## Obtain additional equipment and tools

Before installing a StorageGRID appliance, confirm you have all of the additional equipment and tools that you need.

### All appliances

You need the following equipment to install and configure all appliances.

#### Screwdrivers

- Phillips No. 2 screwdriver
- Medium flat-blade screwdriver

#### ESD wrist strap

#### Service laptop

- [Supported web browser](#)
- SSH client, such as PuTTY
- 1-GbE (RJ-45) port



Some ports might not support 10/100 Ethernet speeds.

#### Optional tools

- Power drill with Phillips head bit
- Flashlight

### Appliance-specific equipment and tools

## **SG100 and SG1000**

You need the following additional equipment to install and configure the SG100 and SG1000 hardware.

### **Optical cables and transceivers**

- Cables, 1 to 4 of either:
  - TwinAx/Copper
  - Fibre/Optical
- Transceivers/adapters, 1 to 4 of each, based on link speed (mixed speeds aren't supported):
  - SG100:
    - 10-GbE SFP+
    - 25-GbE SFP28
  - SG1000:
    - 10-GbE QSFP-to-SFP adapter (QSA) and SFP+
    - 25-GbE QSFP-to-SFP adapter (QSA) and SFP28
    - 40-GbE QSFP+
    - 100-GbE QFSP28

### **Ethernet cables**

RJ-45 (Cat5/Cat5e/Cat6/Cat6a)

## **SG5700**

You need the following additional equipment to install and configure the SG5700 hardware.

### **Optical cables and SFP transceivers**

- Optical cables for the 10/25-GbE ports you plan to use
- Optional: SFP28 transceivers if you want to use 25-GbE link speed

### **Ethernet cables**

#### **Optional tools**

Mechanized lift for SG5760

## **SG6000**

You need the following additional equipment to install and configure the SG6000 hardware.

### **Optical cables and SFP transceivers**

- Cables, 1 to 4 of either:
  - TwinAx/Copper
  - Fibre/Optical
- Transceivers/adapters, 1 to 4 of each, based on link speed (mixed speeds aren't supported):
  - 10-GbE SFP+
  - 25-GbE SFP28

### **Ethernet cables**

RJ-45 (Cat5/Cat5e/Cat6)

### **Optional tools**

Mechanized lift for 60-drive shelves

### **SG6100**

You need the following additional equipment to install and configure the SGF6112 hardware.

### **Optical cables and transceivers**

- Cables, 1 to 4 of either:
  - TwinAx/Copper
  - Fibre/Optical
- Transceivers/adapters, 1 to 4 of each, based on link speed (mixed speeds aren't supported):
  - 10-GbE SFP+
  - 25-GbE SFP28

### **Ethernet cables**

RJ-45 (Cat5/Cat5e/Cat6/Cat6a)

## **Gather network information**

### **StorageGRID network types**

Before installing the StorageGRID appliance, you should understand which networks can be connected to the appliance and how the ports on each controller are used.

StorageGRID network requirements are fully explained in the [Networking guidelines](#).

Refer to the instructions for your appliance to determine what information you need:

- [SG100 and SG1000](#)
- [SG5700](#)
- [SG6000](#)
- [SG6100](#)

Alternatively, you can work with your NetApp Professional Services consultant to use the NetApp ConfigBuilder tool to streamline and automate the configuration steps. See [Automate appliance installation and configuration](#).

When you deploy a StorageGRID appliance as a node in a StorageGRID system, you can connect it to the following networks:

- **Grid Network for StorageGRID:** The Grid Network is used for all internal StorageGRID traffic. It provides connectivity between all nodes in the grid, across all sites and subnets. The Grid Network is required.
- **Admin Network for StorageGRID:** The Admin Network is a closed network used for system administration and maintenance. The Admin Network is typically a private network and does not need to be routable between sites. The Admin Network is optional.
- **Client Network for StorageGRID:** The Client Network is an open network used to provide access to client

applications, including S3 and Swift. The Client Network provides client protocol access to the grid, so the Grid Network can be isolated and secured. You can configure the Client Network so that the appliance can be accessed over this network using only the ports you choose to open. The Client Network is optional.

- **Management network for SANtricity** (optional for storage appliances, not needed for the SG6100): This network provides access to SANtricity System Manager, allowing you to monitor and manage the hardware components in the appliance and storage controller shelf. This management network can be the same as the Admin Network for StorageGRID, or it can be an independent management network.
- **BMC management network** (optional for SG100, SG1000, SG6000, and SG6100): This network provides access to the baseboard management controller in the SG100, SG1000, SG6000, and SG6100 appliances allowing you to monitor and manage the hardware components in the appliance. This management network can be the same as the Admin Network for StorageGRID, or it can be an independent management network.

If the optional BMC management network is not connected, some support and maintenance procedures will be more difficult to perform. You can leave the BMC management network unconnected except when needed for support purposes.



For detailed information about StorageGRID networks, see the [StorageGRID network types](#).

### Gather network information (SG100 and SG1000)

Using the tables, record the required information for each network you connect to the appliance. These values are required to install and configure the hardware.



Instead of using the tables, use the workbook provided with ConfigBuilder. Using the ConfigBuilder workbook allows you to upload your system information and generate a JSON file to automatically complete some configuration steps in the StorageGRID Appliance Installer. See [Automate appliance installation and configuration](#).

### Check StorageGRID version

Before installing an SG100 or SG1000 services appliance, confirm your StorageGRID system is using a required version of StorageGRID software.

Appliance	Required StorageGRID version
SG1000	11.3 or later (latest hotfix recommended)
SG100	11.4 or later (latest hotfix recommended)

### Administration and maintenance ports

The Admin Network for StorageGRID is an optional network, used for system administration and maintenance. The appliance connects to the Admin Network using the following 1-GbE management ports on the appliance.

SG100 RJ-45 ports:



SG1000 RJ-45 ports:



Information needed	Your value
Admin Network enabled	Choose one: <ul style="list-style-type: none"> <li>• No</li> <li>• Yes (default)</li> </ul>
Network bond mode	Choose one: <ul style="list-style-type: none"> <li>• Independent (default)</li> <li>• Active-Backup</li> </ul>
Switch port for the left port circled in the diagram (default active port for Independent network bond mode)	
Switch port for the right port circled in the diagram (Active-Backup network bond mode only)	
MAC address for the Admin Network port <p><b>Note:</b> The MAC address label on the front of the appliance lists the MAC address for the BMC management port. To determine the MAC address for the Admin Network port, add <b>2</b> to the hexadecimal number on the label. For example, if the MAC address on the label ends in <b>09</b>, the MAC address for the Admin Port would end in <b>0B</b>. If the MAC address on the label ends in <b>(y)FF</b>, the MAC address for the Admin Port would end in <b>(y+1)01</b>. You can easily make this calculation by opening Calculator in Windows, setting it to Programmer mode, selecting Hex, typing the MAC address, then typing <b>+ 2 =</b>.</p>	
DHCP-assigned IP address for the Admin Network port, if available after power on <p><b>Note:</b> You can determine the DHCP-assigned IP address by using the MAC address to look up the assigned IP.</p>	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>
Static IP address you plan to use for the appliance node on the Admin Network <p><b>Note:</b> If your network does not have a gateway, specify the same static IPv4 address for the gateway.</p>	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>
Admin Network subnets (CIDR)	

## Networking ports

The four networking ports on the appliance connect to the StorageGRID Grid Network and the optional Client Network.

Information needed	Your value
Link speed	<p>For the SG100, choose one of the following:</p> <ul style="list-style-type: none"><li>• Auto (default)</li><li>• 10 GbE</li><li>• 25 GbE</li></ul> <p>For the SG1000, choose one of the following:</p> <ul style="list-style-type: none"><li>• Auto (default)</li><li>• 10 GbE</li><li>• 25 GbE</li><li>• 40 GbE</li><li>• 100 GbE</li></ul> <p><b>Note:</b> For the SG1000, 10- and 25-GbE speeds require the use of QSA adapters.</p>
Port bond mode	<p>Choose one:</p> <ul style="list-style-type: none"><li>• Fixed (default)</li><li>• Aggregate</li></ul>
Switch port for port 1 (Client Network for Fixed mode)	
Switch port for port 2 (Grid Network for Fixed mode)	
Switch port for port 3 (Client Network for Fixed mode)	
Switch port for port 4 (Grid Network for Fixed mode)	

## Grid Network ports

The Grid Network for StorageGRID is a required network, used for all internal StorageGRID traffic. The appliance connects to the Grid Network using the four network ports.

Information needed	Your value
Network bond mode	Choose one: <ul style="list-style-type: none"> <li>• Active-Backup (default)</li> <li>• LACP (802.3ad)</li> </ul>
VLAN tagging enabled	Choose one: <ul style="list-style-type: none"> <li>• No (default)</li> <li>• Yes</li> </ul>
VLAN tag(if VLAN tagging is enabled)	Enter a value between 0 and 4095:
DHCP-assigned IP address for the Grid Network, if available after power on	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>
Static IP address you plan to use for the appliance node on the Grid Network  <b>Note:</b> If your network does not have a gateway, specify the same static IPv4 address for the gateway.	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>
Grid Network subnets (CIDRs)	
Maximum transmission unit (MTU) setting (optional)You can use the default value of 1500, or set the MTU to a value suitable for jumbo frames, such as 9000.	

#### Client Network ports

The Client Network for StorageGRID is an optional network, typically used to provide client protocol access to the grid. The appliance connects to the Client Network using the four network ports.

Information needed	Your value
Client Network enabled	Choose one: <ul style="list-style-type: none"> <li>• No (default)</li> <li>• Yes</li> </ul>
Network bond mode	Choose one: <ul style="list-style-type: none"> <li>• Active-Backup (default)</li> <li>• LACP (802.3ad)</li> </ul>



Information needed	Your value
VLAN tagging enabled	Choose one: <ul style="list-style-type: none"> <li>No (default)</li> <li>Yes</li> </ul>
VLAN tag (If VLAN tagging is enabled)	Enter a value between 0 and 4095:
DHCP-assigned IP address for the Client Network, if available after power on	<ul style="list-style-type: none"> <li>IPv4 address (CIDR):</li> <li>Gateway:</li> </ul>
Static IP address you plan to use for the appliance node on the Client Network	<ul style="list-style-type: none"> <li>IPv4 address (CIDR):</li> <li>Gateway:</li> </ul>
<p><b>Note:</b> If the Client Network is enabled, the default route on the appliance will use the gateway specified here.</p>	

### BMC management network ports

You can access the BMC interface on the services appliance using the 1-GbE management port circled in the diagram. This port supports remote management of the controller hardware over Ethernet using the Intelligent Platform Management Interface (IPMI) standard.



You can enable or disable remote IPMI access for all appliances containing a BMC. The remote IPMI interface allows low-level hardware access to your StorageGRID appliances by anyone with a BMC account and password. If you do not need remote IPMI access to the BMC, disable this option using one of the following methods:

In Grid Manager, go to **CONFIGURATION > Security > Security settings > Appliances** and clear the **Enable remote IPMI access** checkbox.

In the Grid management API, use the private endpoint: `PUT /private/bmc`.

SG100 BMC management port:



SG1000 BMC management port:



Information needed	Your value
Ethernet switch port you will connect to the BMC management port (circled in the diagram)	

Information needed	Your value
DHCP-assigned IP address for the BMC management network, if available after power on	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>
Static IP address you plan to use for the BMC management port	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>

### Port bond modes

When configuring network links for the SG100 and SG1000 appliances, you can use port bonding for the ports that connect to the Grid Network and optional Client Network, and the 1-GbE management ports that connect to the optional Admin Network. Port bonding helps protect your data by providing redundant paths between StorageGRID networks and the appliance.

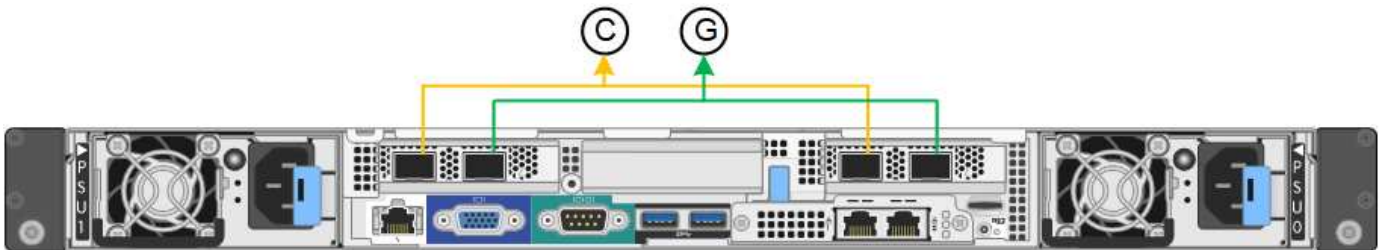
### Network bond modes

The networking ports on the services appliance support Fixed port bond mode or Aggregate port bond mode for the Grid Network and Client Network connections.

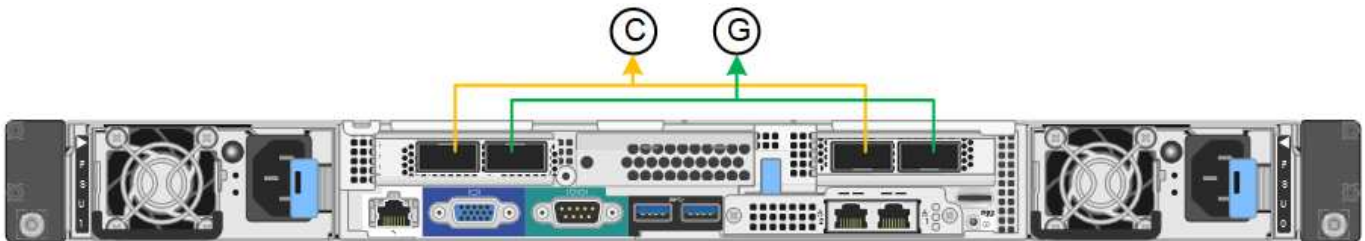
### Fixed port bond mode

Fixed port bond mode is the default configuration for the networking ports. The figures show how the network ports on the SG1000 or SG100 are bonded in fixed port bond mode.

SG100:



SG1000:



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.

When using Fixed port bond mode, the ports can be bonded using active-backup mode or Link Aggregation Control Protocol mode (LACP 802.3ad).

- In active-backup mode (default), only one port is active at a time. If the active port fails, its backup port automatically provides a failover connection. Port 4 provides a backup path for port 2 (Grid Network), and port 3 provides a backup path for port 1 (Client Network).
- In LACP mode, each pair of ports forms a logical channel between the services appliance and the network, allowing for higher throughput. If one port fails, the other port continues to provide the channel. Throughput is reduced, but connectivity is not impacted.

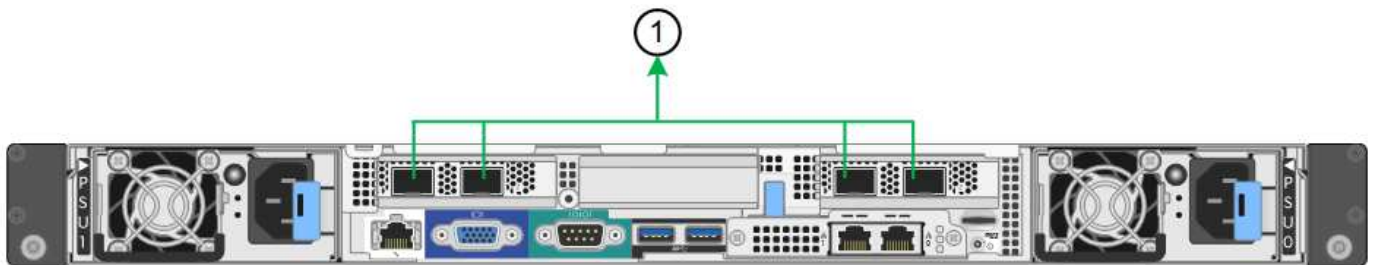


If you don't need redundant connections, you can use only one port for each network. However, be aware that the **Services appliance link down** alert might be triggered in the Grid Manager after StorageGRID is installed, indicating that a cable is unplugged. You can safely disable this alert rule.

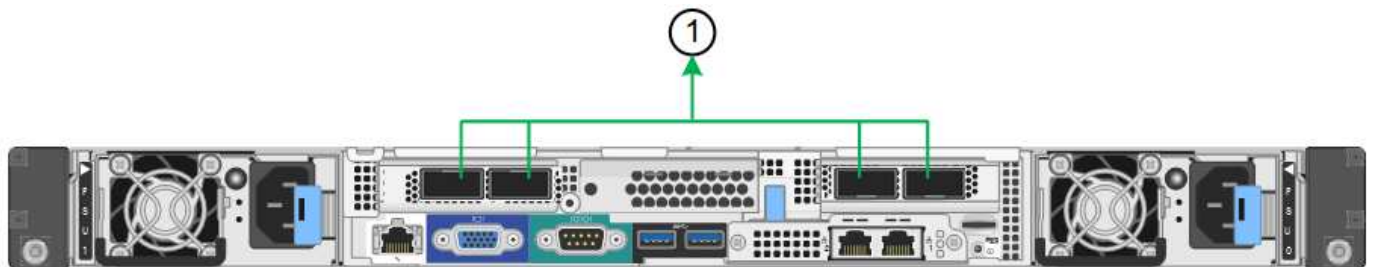
### Aggregate port bond mode

Aggregate port bond mode significantly increases the throughput for each StorageGRID network and provides additional failover paths. These figures show how the network ports are bonded in aggregate port bond mode.

SG100:



SG1000:



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

If you plan to use aggregate port bond mode:

- You must use LACP network bond mode.
- You must specify a unique VLAN tag for each network. This VLAN tag will be added to each network packet to ensure that network traffic is routed to the correct network.
- The ports must be connected to switches that can support VLAN and LACP. If multiple switches are

participating in the LACP bond, the switches must support multi-chassis link aggregation groups (MLAG), or equivalent.

- You understand how to configure the switches to use VLAN, LACP, and MLAG, or equivalent.

If you don't want to use all four ports, you can use one, two, or three ports. Using more than one port maximizes the chance that some network connectivity will remain available if one of the ports fails.



If you choose to use fewer than four network ports, be aware that a **Services appliance link down** alert might be triggered in the Grid Manager after the appliance node is installed, indicating that a cable is unplugged. You can safely disable this alert rule for the triggered alert.

### Network bond modes for management ports

For the two 1-GbE management ports on the services appliance, you can choose Independent network bond mode or Active-Backup network bond mode to connect to the optional Admin Network. These figures show how the management ports on the appliances are bonded in network bond mode for the Admin Network.

SG100:



SG1000:



Callout	Network bond mode
A	Active-Backup mode. Both management ports are bonded into one logical management port connected to the Admin Network.
I	Independent mode. The port on the left is connected to the Admin Network. The port on the right is available for temporary local connections (IP address 169.254.0.1).

In Independent mode, only the management port on the left is connected to the Admin Network. This mode does not provide a redundant path. The management port on the right is unconnected and available for temporary local connections (uses IP address 169.254.0.1)

In Active-Backup mode, both management ports are connected to the Admin Network. Only one port is active at a time. If the active port fails, its backup port automatically provides a failover connection. Bonding these two physical ports into one logical management port provides a redundant path to the Admin Network.



If you need to make a temporary local connection to the services appliance when the 1-GbE management ports are configured for Active-Backup mode, remove the cables from both management ports, plug your temporary cable into the management port on the right, and access the appliance using IP address 169.254.0.1.

#### Related information

- [Cable appliance](#)
- [Configure StorageGRID IP addresses](#)

#### Gather network information (SG5700)

Using the tables, record the required information for each network you connect to the appliance. These values are required to install and configure the hardware.



Instead of using the tables, use the workbook provided with ConfigBuilder. Using the ConfigBuilder workbook allows you to upload your system information and generate a JSON file to automatically complete some configuration steps in the StorageGRID Appliance Installer. See [Automate appliance installation and configuration](#).

#### Information needed to connect to SANtricity System Manager on E2800 controller

You connect the E2800 series controller to the management network you will use for SANtricity System Manager.

Information needed	Your value
Ethernet switch port you will connect to management port 1	
MAC address for management port 1 (printed on a label near port P1)	
DHCP-assigned IP address for management port 1, if available after power on  <b>Note:</b> If the network you will connect to the E2800 controller includes a DHCP server, the network administrator can use the MAC address to determine the IP address that was assigned by the DHCP server.	
Speed and duplex mode  <b>Note:</b> You must make sure the Ethernet switch for the SANtricity System Manager management network is set to autonegotiate.	Must be: <ul style="list-style-type: none"> <li>• Autonegotiate (default)</li> </ul>
IP address format	Choose one: <ul style="list-style-type: none"> <li>• IPv4</li> <li>• IPv6</li> </ul>

Information needed	Your value
Static IP address you plan to use for the appliance on the management network	For IPv4: <ul style="list-style-type: none"> <li>• IPv4 address:</li> <li>• Subnet mask:</li> <li>• Gateway:</li> </ul> For IPv6: <ul style="list-style-type: none"> <li>• IPv6 address:</li> <li>• Routable IP address:</li> <li>• E2800 controller router IP address:</li> </ul>

**Information needed to connect E5700SG controller to Admin Network**

The Admin Network for StorageGRID is an optional network, used for system administration and maintenance. The appliance connects to the Admin Network using the 1-GbE management ports on the E5700SG controller.

Information needed	Your value
Admin Network enabled	Choose one: <ul style="list-style-type: none"> <li>• No</li> <li>• Yes (default)</li> </ul>
Network bond mode	Choose one: <ul style="list-style-type: none"> <li>• Independent</li> <li>• Active-Backup</li> </ul>
Switch port for port 1	
Switch port for port 2 (Active-Backup network bond mode only)	
DHCP-assigned IP address for management port 1, if available after power on  <b>Note:</b> If the Admin Network includes a DHCP server, the E5700SG controller displays the DHCP-assigned IP address on its seven-segment display after it boots up. You can also determine the DHCP-assigned IP address by using the MAC address to look up the assigned IP.	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>

Information needed	Your value
Static IP address you plan to use for the appliance Storage Node on the Admin Network  <b>Note:</b> If your network does not have a gateway, specify the same static IPv4 address for the gateway.	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>
Admin Network subnets (CIDR)	

#### Information needed to connect and configure 10/25-GbE ports on E5700SG controller

The four 10/25-GbE ports on the E5700SG controller connect to the StorageGRID Grid Network and Client Network.



See [Port bond modes \(E5700SG controller\)](#).

Information needed	Your value
Link speed  <b>Note:</b> If you select 25 GbE, install SPF28 transceivers. Autonegotiation is not supported, so you must also configure the ports and the connected switches for 25GbE.	Choose one: <ul style="list-style-type: none"> <li>• 10 GbE (default)</li> <li>• 25 GbE</li> </ul>
Port bond mode	Choose one: <ul style="list-style-type: none"> <li>• Fixed (default)</li> <li>• Aggregate</li> </ul>
Switch port for port 1 (Client Network)	
Switch port for port 2 (Grid Network)	
Switch port for port 3 (Client Network)	
Switch port for port 4 (Grid Network)	

#### Information needed to connect E5700SG controller to Grid Network

The Grid Network for StorageGRID is a required network, used for all internal StorageGRID traffic. The appliance connects to the Grid Network using the 10/25-GbE ports on the E5700SG controller.



See [Port bond modes \(E5700SG controller\)](#).

Information needed	Your value
Network bond mode	Choose one: <ul style="list-style-type: none"> <li>• Active-Backup (default)</li> <li>• LACP (802.3ad)</li> </ul>
VLAN tagging enabled	Choose one: <ul style="list-style-type: none"> <li>• No (default)</li> <li>• Yes</li> </ul>
VLAN tag(if VLAN tagging is enabled)	Enter a value between 0 and 4095:
DHCP-assigned IP address for the Grid Network, if available after power on  <b>Note:</b> If the Grid Network includes a DHCP server, the E5700SG controller displays the DHCP-assigned IP address for the Grid Network on its seven-segment display after it boots up.	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>
Static IP address you plan to use for the appliance Storage Node on the Grid Network  <b>Note:</b> If your network does not have a gateway, specify the same static IPv4 address for the gateway.	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>
Grid Network subnets (CIDR)  <b>Note:</b> If the Client Network is not enabled, the default route on the controller will use the gateway specified here.	

#### Information needed to connect E5700SG controller to Client Network

The Client Network for StorageGRID is an optional network, typically used to provide client protocol access to the grid. The appliance connects to the Client Network using the 10/25-GbE ports on the E5700SG controller.



See [Port bond modes \(E5700SG controller\)](#).

Information needed	Your value
Client Network enabled	Choose one: <ul style="list-style-type: none"> <li>• No (default)</li> <li>• Yes</li> </ul>



Information needed	Your value
Network bond mode	Choose one: <ul style="list-style-type: none"> <li>• Active-Backup (default)</li> <li>• LACP (802.3ad)</li> </ul>
VLAN tagging enabled	Choose one: <ul style="list-style-type: none"> <li>• No (default)</li> <li>• Yes</li> </ul>
VLAN tag (if VLAN tagging is enabled)	Enter a value between 0 and 4095:
DHCP-assigned IP address for the Client Network, if available after power on	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>
Static IP address you plan to use for the appliance Storage Node on the Client Network  <b>Note:</b> If the Client Network is enabled, the default route on the controller will use the gateway specified here.	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>

### Port bond modes

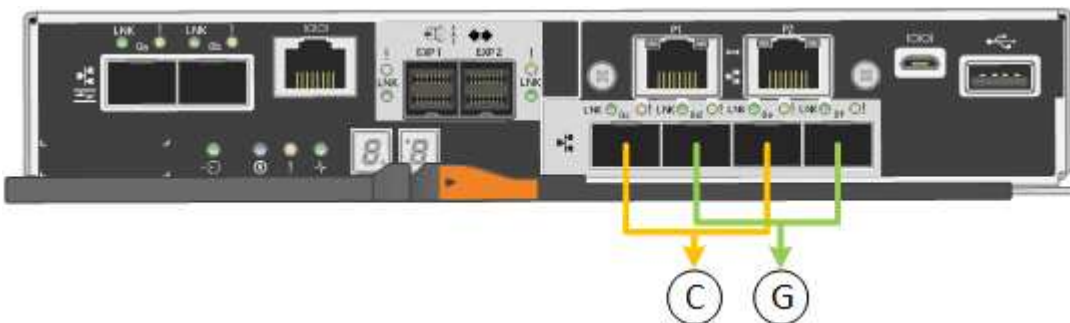
When [configuring network links](#) for the E5700SG controller, you can use port bonding for the 10/25-GbE ports that connect to the Grid Network and optional Client Network, and the 1-GbE management ports that connect to the optional Admin Network. Port bonding helps protect your data by providing redundant paths between StorageGRID networks and the appliance.

### Network bond modes for 10/25-GbE ports

The 10/25-GbE networking ports on the E5700SG controller support Fixed port bond mode or Aggregate port bond mode for the Grid Network and Client Network connections.

### Fixed port bond mode

Fixed mode is the default configuration for the 10/25-GbE networking ports.



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.

When using Fixed port bond mode, you can use one of two network bond modes: Active-Backup or Link Aggregation Control Protocol (LACP).

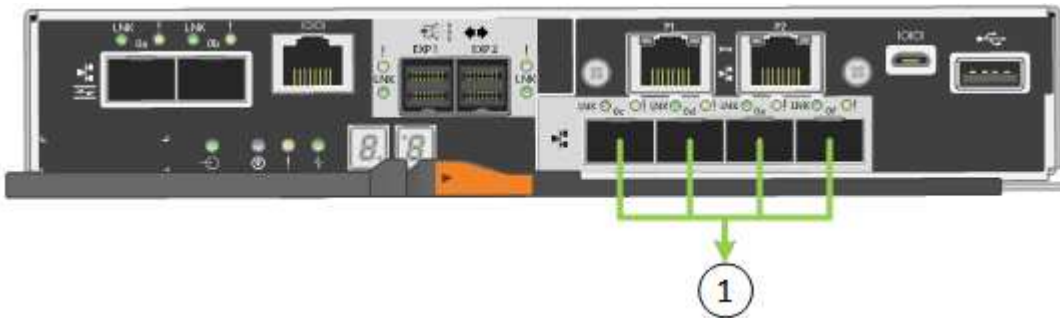
- In Active-Backup mode (default), only one port is active at a time. If the active port fails, its backup port automatically provides a failover connection. Port 4 provides a backup path for port 2 (Grid Network), and port 3 provides a backup path for port 1 (Client Network).
- In LACP mode, each pair of ports forms a logical channel between the controller and the network, allowing for higher throughput. If one port fails, the other port continues to provide the channel. Throughput is reduced, but connectivity is not impacted.



If you don't need redundant connections, you can use only one port for each network. However, be aware that an alarm will be raised in the Grid Manager after StorageGRID is installed, indicating that a cable is unplugged. You can safely acknowledge this alarm to clear it.

### Aggregate port bond mode

Aggregate port bond mode significantly increases the throughput for each StorageGRID network and provides additional failover paths.



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

If you plan to use Aggregate port bond mode:

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

If you don't want to use all four 10/25-GbE ports, you can use one, two, or three ports. Using more than one port maximizes the chance that some network connectivity will remain available if one of the 10/25-GbE ports fails.



If you choose to use fewer than four ports, be aware that one or more alarms will be raised in the Grid Manager after StorageGRID is installed, indicating that cables are unplugged. You can safely acknowledge the alarms to clear them.

### Network bond modes for 1-GbE management ports

For the two 1-GbE management ports on the E5700SG controller, you can choose Independent network bond mode or Active-Backup network bond mode to connect to the optional Admin Network.

In Independent mode, only management port 1 is connected to the Admin Network. This mode does not provide a redundant path. Management port 2 is left unwired and available for temporary local connections (use IP address 169.254.0.1)

In Active-Backup mode, both management ports 1 and 2 are connected to the Admin Network. Only one port is active at a time. If the active port fails, its backup port automatically provides a failover connection. Bonding these two physical ports into one logical management port provides a redundant path to the Admin Network.



If you need to make a temporary local connection to the E5700SG controller when the 1-GbE management ports are configured for Active-Backup mode, remove the cables from both management ports, plug your temporary cable into management port 2, and access the appliance using IP address 169.254.0.1.



### Related information

- [Cable appliance \(SG5700\)](#)
- [Port bond modes \(E5700SG controller\)](#)
- [Configure hardware \(SG5700\)](#)

### Gather network information (SG6000)

Using the tables, record the required information for each network you connect to the appliance. These values are required to install and configure the hardware.



Instead of using the tables, use the workbook provided with ConfigBuilder. Using the ConfigBuilder workbook allows you to upload your system information and generate a JSON file to automatically complete some configuration steps in the StorageGRID Appliance Installer. See [Automate appliance installation and configuration](#).

### Information needed to connect to SANtricity System Manager on storage controllers

You connect both of the storage controllers in the appliance (either the E2800 series controllers or the EF570 controllers) to the management network you will use for SANtricity System Manager. The controllers are

located in each appliance as follows:

- SG6060 and SG6060X: Controller A is on the top, and controller B is on the bottom.
- SGF6024: Controller A is on the left, and controller B is on the right.

Information needed	Your value for controller A	Your value for controller B
Ethernet switch port you will connect to management port 1 (labeled as P1 on the controller)		
MAC address for management port 1 (printed on a label near port P1)		
DHCP-assigned IP address for management port 1, if available after power on  <b>Note:</b> If the network you will connect to the storage controller includes a DHCP server, the network administrator can use the MAC address to determine the IP address that was assigned by the DHCP server.		
Static IP address you plan to use for the appliance on the management network	For IPv4: <ul style="list-style-type: none"> <li>• IPv4 address:</li> <li>• Subnet mask:</li> <li>• Gateway:</li> </ul> For IPv6: <ul style="list-style-type: none"> <li>• IPv6 address:</li> <li>• Routable IP address:</li> <li>• storage controller router IP address:</li> </ul>	For IPv4: <ul style="list-style-type: none"> <li>• IPv4 address:</li> <li>• Subnet mask:</li> <li>• Gateway:</li> </ul> For IPv6: <ul style="list-style-type: none"> <li>• IPv6 address:</li> <li>• Routable IP address:</li> <li>• storage controller router IP address:</li> </ul>
IP address format	Choose one: <ul style="list-style-type: none"> <li>• IPv4</li> <li>• IPv6</li> </ul>	Choose one: <ul style="list-style-type: none"> <li>• IPv4</li> <li>• IPv6</li> </ul>
Speed and duplex mode  <b>Note:</b> You must make sure the Ethernet switch for the SANtricity System Manager management network is set to autonegotiate.	Must be: <ul style="list-style-type: none"> <li>• Autonegotiate (default)</li> </ul>	Must be: <ul style="list-style-type: none"> <li>• Autonegotiate (default)</li> </ul>

### Information needed to connect SG6000-CN controller to Admin Network

The Admin Network for StorageGRID is an optional network, used for system administration and maintenance. The appliance connects to the Admin Network using the following 1-GbE management ports on the SG6000-CN controller.



Information needed	Your value
Admin Network enabled	Choose one: <ul style="list-style-type: none"> <li>• No</li> <li>• Yes (default)</li> </ul>
Network bond mode	Choose one: <ul style="list-style-type: none"> <li>• Independent (default)</li> <li>• Active-Backup</li> </ul>
Switch port for the left port in the red circle in the diagram (default active port for Independent network bond mode)	
Switch port for the right port in the red circle in the diagram (Active-Backup network bond mode only)	
MAC address for the Admin Network port <p><b>Note:</b> The MAC address label on the front of the SG6000-CN controller lists the MAC address for the BMC management port. To determine the MAC address for the Admin Network port, you must add <b>2</b> to the hexadecimal number on the label. For example, if the MAC address on the label ends in <b>09</b>, the MAC address for the Admin Port would end in <b>0B</b>. If the MAC address on the label ends in <b>(y)FF</b>, the MAC address for the Admin Port would end in <b>(y+1)01</b>. You can easily make this calculation by opening Calculator in Windows, setting it to Programmer mode, selecting Hex, typing the MAC address, then typing <b>+ 2 =</b>.</p>	
DHCP-assigned IP address for the Admin Network port, if available after power on <p><b>Note:</b> You can determine the DHCP-assigned IP address by using the MAC address to look up the assigned IP.</p>	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>
Static IP address you plan to use for the appliance Storage Node on the Admin Network <p><b>Note:</b> If your network does not have a gateway, specify the same static IPv4 address for the gateway.</p>	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>

Information needed	Your value
Admin Network subnets (CIDR)	

**Information needed to connect and configure 10/25-GbE ports on SG6000-CN controller**

The four 10/25-GbE ports on the SG6000-CN controller connect to the StorageGRID Grid Network and the optional Client Network.

Information needed	Your value
Link speed	Choose one: <ul style="list-style-type: none"> <li>• Auto (default)</li> <li>• 10 GbE</li> <li>• 25 GbE</li> </ul>
Port bond mode	Choose one: <ul style="list-style-type: none"> <li>• Fixed (default)</li> <li>• Aggregate</li> </ul>
Switch port for port 1 (Client Network for Fixed mode)	
Switch port for port 2 (Grid Network for Fixed mode)	
Switch port for port 3 (Client Network for Fixed mode)	
Switch port for port 4 (Grid Network for Fixed mode)	

**Information needed to connect SG6000-CN controller to Grid Network**

The Grid Network for StorageGRID is a required network, used for all internal StorageGRID traffic. The appliance connects to the Grid Network using the 10/25-GbE ports on the SG6000-CN controller.

Information needed	Your value
Network bond mode	Choose one: <ul style="list-style-type: none"> <li>• Active-Backup (default)</li> <li>• LACP (802.3ad)</li> </ul>
VLAN tagging enabled	Choose one: <ul style="list-style-type: none"> <li>• No (default)</li> <li>• Yes</li> </ul>

Information needed	Your value
VLAN tag(if VLAN tagging is enabled)	Enter a value between 0 and 4095:
DHCP-assigned IP address for the Grid Network, if available after power on	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>
Static IP address you plan to use for the appliance Storage Node on the Grid Network  <b>Note:</b> If your network does not have a gateway, specify the same static IPv4 address for the gateway.	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>
Grid Network subnets (CIDRs)	

#### Information needed to connect SG6000-CN controller to Client Network

The Client Network for StorageGRID is an optional network, typically used to provide client protocol access to the grid. The appliance connects to the Client Network using the 10/25-GbE ports on the SG6000-CN controller.

Information needed	Your value
Client Network enabled	Choose one: <ul style="list-style-type: none"> <li>• No (default)</li> <li>• Yes</li> </ul>
Network bond mode	Choose one: <ul style="list-style-type: none"> <li>• Active-Backup (default)</li> <li>• LACP (802.3ad)</li> </ul>
VLAN tagging enabled	Choose one: <ul style="list-style-type: none"> <li>• No (default)</li> <li>• Yes</li> </ul>
VLAN tag(if VLAN tagging is enabled)	Enter a value between 0 and 4095:
DHCP-assigned IP address for the Client Network, if available after power on	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>

Information needed	Your value
Static IP address you plan to use for the appliance Storage Node on the Client Network  <b>Note:</b> If the Client Network is enabled, the default route on the controller will use the gateway specified here.	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>

**Information needed to connect SG6000-CN controller to BMC management network**

You can access the BMC interface on the SG6000-CN controller using the following 1-GbE management port. This port supports remote management of the controller hardware over Ethernet using the Intelligent Platform Management Interface (IPMI) standard.



You can enable or disable remote IPMI access for all appliances containing a BMC. The remote IPMI interface allows low-level hardware access to your StorageGRID appliances by anyone with a BMC account and password. If you do not need remote IPMI access to the BMC, disable this option using one of the following methods:  
 In Grid Manager, go to **CONFIGURATION > Security > Security settings > Appliances** and clear the **Enable remote IPMI access** checkbox.  
 In the Grid management API, use the private endpoint: `PUT /private/bmc`.

Information needed	Your value
Ethernet switch port you will connect to the BMC management port (circled in the diagram)	
DHCP-assigned IP address for the BMC management network, if available after power on	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>
Static IP address you plan to use for the BMC management port	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>

**Port bond modes**

When [configuring network links](#) for the SG6000-CN controller, you can use port bonding for the 10/25-GbE ports that connect to the Grid Network and optional Client Network, and the 1-GbE management ports that connect to the optional Admin Network. Port bonding helps protect your data by providing redundant paths between StorageGRID networks and the appliance.

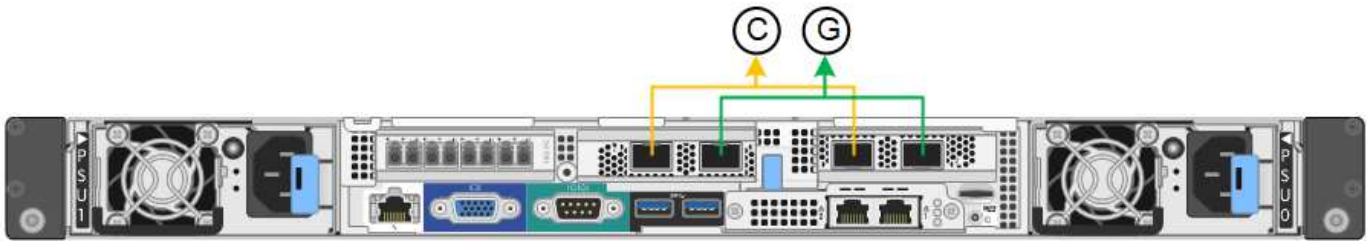
**Network bond modes for 10/25-GbE ports**

The 10/25-GbE networking ports on the SG6000-CN controller support Fixed port bond mode or Aggregate port bond mode for the Grid Network and Client Network connections.



## Fixed port bond mode

Fixed mode is the default configuration for the 10/25-GbE networking ports.



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.

When using Fixed port bond mode, the ports can be bonded using active-backup mode or Link Aggregation Control Protocol mode (LACP 802.3ad).

- In active-backup mode (default), only one port is active at a time. If the active port fails, its backup port automatically provides a failover connection. Port 4 provides a backup path for port 2 (Grid Network), and port 3 provides a backup path for port 1 (Client Network).
- In LACP mode, each pair of ports forms a logical channel between the controller and the network, allowing for higher throughput. If one port fails, the other port continues to provide the channel. Throughput is reduced, but connectivity is not impacted.

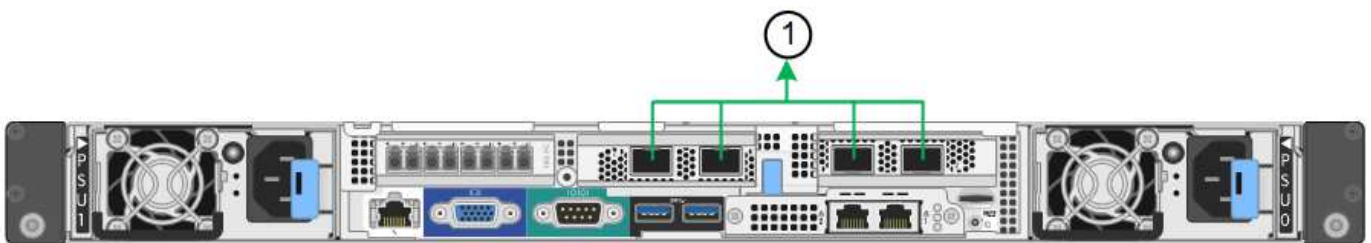


If you don't need redundant connections, you can use only one port for each network. However, be aware that an alert will be triggered in the Grid Manager after StorageGRID is installed, indicating that the link is down. Because this port is disconnected on purpose, you can safely disable this alert.

From the Grid Manager, select **Alert > Rules**, select the rule, and click **Edit rule**. Then, uncheck the **Enabled** checkbox.

## Aggregate port bond mode

Aggregate port bond mode significantly increases the throughput for each StorageGRID network and provides additional failover paths.



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

If you plan to use aggregate port bond mode:

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

If you don't want to use all four 10/25-GbE ports, you can use one, two, or three ports. Using more than one port maximizes the chance that some network connectivity will remain available if one of the 10/25-GbE ports fails.



If you choose to use fewer than four ports, be aware that one or more alarms will be raised in the Grid Manager after StorageGRID is installed, indicating that cables are unplugged. You can safely acknowledge the alarms to clear them.

### Network bond modes for 1-GbE management ports

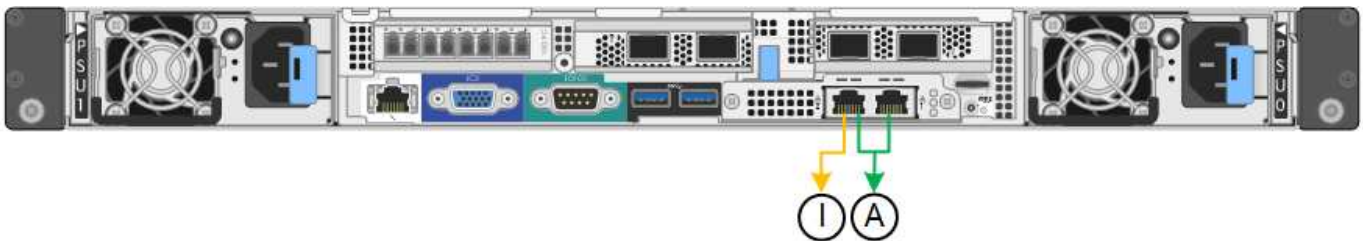
For the two 1-GbE management ports on the SG6000-CN controller, you can choose Independent network bond mode or Active-Backup network bond mode to connect to the optional Admin Network.

In Independent mode, only the management port on the left is connected to the Admin Network. This mode does not provide a redundant path. The management port on the right is unconnected and available for temporary local connections (uses IP address 169.254.0.1)

In Active-Backup mode, both management ports are connected to the Admin Network. Only one port is active at a time. If the active port fails, its backup port automatically provides a failover connection. Bonding these two physical ports into one logical management port provides a redundant path to the Admin Network.



If you need to make a temporary local connection to the SG6000-CN controller when the 1-GbE management ports are configured for Active-Backup mode, remove the cables from both management ports, plug your temporary cable into the management port on the right, and access the appliance using IP address 169.254.0.1.



Callout	Network bond mode
A	Both management ports are bonded into one logical management port connected to the Admin Network.
I	The port on the left is connected to the Admin Network. The port on the right is available for temporary local connections (IP address 169.254.0.1).

### Related information

- [SG6000 controllers](#)
- [Determine appliance network connections](#)
- [Port bond modes \(SG6000-CN controller\)](#)
- [Cable appliance](#)
- [Configure StorageGRID IP addresses](#)

### Gather network information (SG6100)

Using the following tables, record the required information for each network you connect to the appliance. These values are required to install and configure the hardware.



Instead of using the tables, use the workbook provided with ConfigBuilder. Using the ConfigBuilder workbook allows you to upload your system information and generate a JSON file to automatically complete some configuration steps in the StorageGRID Appliance Installer. See [Automate appliance installation and configuration](#).

### Check StorageGRID version

Before installing an SGF6112 appliance, confirm your StorageGRID system is using a required version of StorageGRID software.

Appliance	Required StorageGRID version
SGF6112	11.7 or later (latest hotfix recommended)

### Administration and maintenance ports

The Admin Network for StorageGRID is an optional network, used for system administration and maintenance. The appliance connects to the Admin Network using the following 1/10-GbE ports on the appliance.

The following figure shows the RJ-45 ports on the SGF6112 appliance.



Information needed	Your value
Admin Network enabled	Choose one: <ul style="list-style-type: none"> <li>• No</li> <li>• Yes (default)</li> </ul>
Network bond mode	Choose one: <ul style="list-style-type: none"> <li>• Independent (default)</li> <li>• Active-Backup</li> </ul>
Switch port for the left port circled in the diagram (default active port for Independent network bond mode)	
Switch port for the right port circled in the diagram (Active-Backup network bond mode only)	
DHCP-assigned IP address for the Admin Network port, if available after power on  <b>Note:</b> Contact your network administrator for the Admin Network port DHCP-assigned IP address.	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>
Static IP address you plan to use for the appliance node on the Admin Network  <b>Note:</b> If your network does not have a gateway, specify the same static IPv4 address for the gateway.	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>
Admin Network subnets (CIDR)	

### Networking ports

The four networking ports on the appliance connect to the StorageGRID Grid Network and the optional Client Network.

Information needed	Your value
Link speed	For the SGF6112, choose one of the following: <ul style="list-style-type: none"> <li>• Auto (default)</li> <li>• 10 GbE</li> <li>• 25 GbE</li> </ul>

Information needed	Your value
Port bond mode	Choose one: <ul style="list-style-type: none"> <li>• Fixed (default)</li> <li>• Aggregate</li> </ul>
Switch port for port 1 (Client Network for Fixed mode)	
Switch port for port 2 (Grid Network for Fixed mode)	
Switch port for port 3 (Client Network for Fixed mode)	
Switch port for port 4 (Grid Network for Fixed mode)	

### Grid Network ports

The Grid Network for StorageGRID is a required network, used for all internal StorageGRID traffic. The appliance connects to the Grid Network using the four network ports.

Information needed	Your value
Network bond mode	Choose one: <ul style="list-style-type: none"> <li>• Active-Backup (default)</li> <li>• LACP (802.3ad)</li> </ul>
VLAN tagging enabled	Choose one: <ul style="list-style-type: none"> <li>• No (default)</li> <li>• Yes</li> </ul>
VLAN tag (if VLAN tagging is enabled)	Enter a value between 0 and 4095:
DHCP-assigned IP address for the Grid Network, if available after power on	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>
Static IP address you plan to use for the appliance node on the Grid Network  <b>Note:</b> If your network does not have a gateway, specify the same static IPv4 address for the gateway.	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>
Grid Network subnets (CIDRs)	

Information needed	Your value
Maximum transmission unit (MTU) setting (optional). You can use the default value of 1500, or set the MTU to a value suitable for jumbo frames, such as 9000.	

### Client Network ports

The Client Network for StorageGRID is an optional network, typically used to provide client protocol access to the grid. The appliance connects to the Client Network using the four network ports.

Information needed	Your value
Client Network enabled	Choose one: <ul style="list-style-type: none"> <li>• No (default)</li> <li>• Yes</li> </ul>
Network bond mode	Choose one: <ul style="list-style-type: none"> <li>• Active-Backup (default)</li> <li>• LACP (802.3ad)</li> </ul>
VLAN tagging enabled	Choose one: <ul style="list-style-type: none"> <li>• No (default)</li> <li>• Yes</li> </ul>
VLAN tag(If VLAN tagging is enabled)	Enter a value between 0 and 4095:
DHCP-assigned IP address for the Client Network, if available after power on	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>
Static IP address you plan to use for the appliance node on the Client Network	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>
<b>Note:</b> If the Client Network is enabled, the default route on the appliance will use the gateway specified here.	

### BMC management network ports

You can access the BMC interface on the appliance using the 1-GbE management port circled in the diagram. This port supports remote management of the controller hardware over Ethernet using the Intelligent Platform Management Interface (IPMI) standard.



You can enable or disable remote IPMI access for all appliances containing a BMC. The remote IPMI interface allows low-level hardware access to your StorageGRID appliances by anyone with a BMC account and password. If you do not need remote IPMI access to the BMC, disable this option using one of the following methods:

In Grid Manager, go to **CONFIGURATION > Security > Security settings > Appliances** and clear the **Enable remote IPMI access** checkbox.

In the Grid management API, use the private endpoint: PUT /private/bmc.

The following figure shows the BMC management port on the SGF6112 appliance.



Information needed	Your value
Ethernet switch port you will connect to the BMC management port (circled in the diagram)	
DHCP-assigned IP address for the BMC management network, if available after power on	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>
Static IP address you plan to use for the BMC management port	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>

### Port bond modes

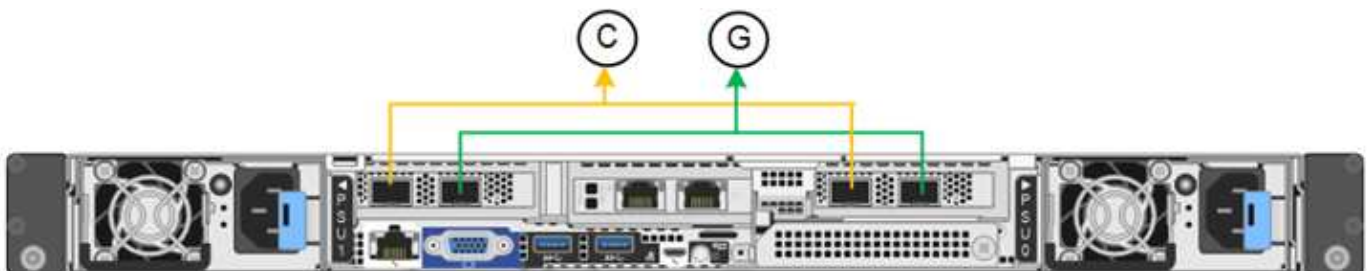
When [configuring network links](#) for the SGF6112 appliance, you can use port bonding for the ports that connect to the Grid Network and optional Client Network, and the 1/10-GbE management ports that connect to the optional Admin Network. Port bonding helps protect your data by providing redundant paths between StorageGRID networks and the appliance.

### Network bond modes

The networking ports on the appliance support Fixed port bond mode or Aggregate port bond mode for the Grid Network and Client Network connections.

### Fixed port bond mode

Fixed port bond mode is the default configuration for the networking ports.



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.

When using Fixed port bond mode, the ports can be bonded using active-backup mode or Link Aggregation Control Protocol mode (LACP 802.3ad).

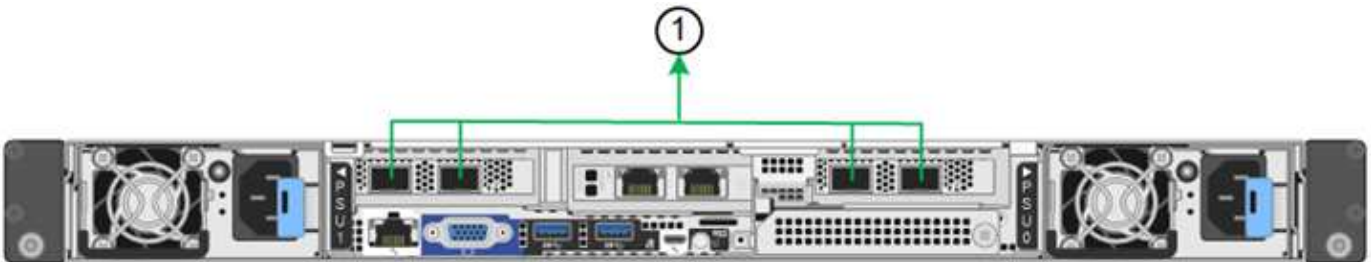
- In active-backup mode (default), only one port is active at a time. If the active port fails, its backup port automatically provides a failover connection. Port 4 provides a backup path for port 2 (Grid Network), and port 3 provides a backup path for port 1 (Client Network).
- In LACP mode, each pair of ports forms a logical channel between the appliance and the network, allowing for higher throughput. If one port fails, the other port continues to provide the channel. Throughput is reduced, but connectivity is not impacted.



If you don't need redundant connections, you can use only one port for each network. However, be aware that the **Storage appliance link down** alert might be triggered in the Grid Manager after StorageGRID is installed, indicating that a cable is unplugged. You can safely disable this alert rule.

### Aggregate port bond mode

Aggregate port bond mode significantly increases the throughput for each StorageGRID network and provides additional failover paths.



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

If you plan to use aggregate port bond mode:

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



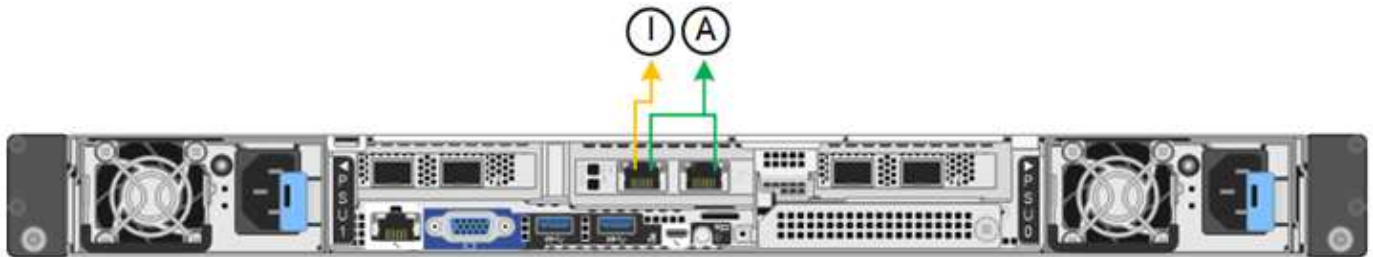
If you don't want to use all four ports, you can use one, two, or three ports. Using more than one port maximizes the chance that some network connectivity will remain available if one of the ports fails.



If you choose to use fewer than four network ports, be aware that a **Services appliance link down** alert might be triggered in the Grid Manager after the appliance node is installed, indicating that a cable is unplugged. You can safely disable this alert rule for the triggered alert.

### Network bond modes for management ports

For the two 1/10-GbE management ports, you can choose Independent network bond mode or Active-Backup network bond mode to connect to the optional Admin Network.



Callout	Network bond mode
A	Active-Backup mode. Both management ports are bonded into one logical management port connected to the Admin Network.
I	Independent mode. The port on the left is connected to the Admin Network. The port on the right is available for temporary local connections (IP address 169.254.0.1).

In Independent mode, only the management port on the left is connected to the Admin Network. This mode does not provide a redundant path. The management port on the right is unconnected and available for temporary local connections (uses IP address 169.254.0.1).

In Active-Backup mode, both management ports are connected to the Admin Network. Only one port is active at a time. If the active port fails, its backup port automatically provides a failover connection. Bonding these two physical ports into one logical management port provides a redundant path to the Admin Network.



If you need to make a temporary local connection to the appliance when the 1/10-GbE management ports are configured for Active-Backup mode, remove the cables from both management ports, plug your temporary cable into the management port on the right, and access the appliance using IP address 169.254.0.1.

### Related information

- [Cable appliance](#)
- [Configure StorageGRID IP addresses](#)

## Automate appliance installation and configuration

Automating installation and configuration can be useful for deploying multiple StorageGRID instances or one large, complex StorageGRID instance.

Using NetApp StorageGRID tools, you can automate the installation and configuration of your StorageGRID appliances. After you install and configure the appliances, you can [automate the configuration of the entire StorageGRID system](#).

You can automate the configuration of the following:

- Grid Network, Admin Network, and Client Network IP addresses
- BMC interface
- Network links
  - Port bond mode
  - Network bond mode
  - Link speed

## Automation options

To automate appliance installation and configuration, use one or more of the following options:

- Generate a JSON file that contains configuration details. Work with your NetApp Professional Services consultant to use the [NetApp ConfigBuilder tool](#) to complete these steps:
  1. Consult with NetApp Professional Services to get a sales order number.
  2. Get the workbook from ConfigBuilder.
  3. Consult with Professional Services to complete the workbook.
  4. Use ConfigBuilder to upload the workbook.
  5. Use ConfigBuilder to generate a JSON file.
  6. Consult with Professional Services to upload the JSON file to the appliance.

See [Automate using Appliance Installer](#).



You can use the same JSON file to configure more than one appliance.

Configuring your appliance using an uploaded JSON file is often more efficient than performing the configuration manually, especially if you have to configure many nodes. Performing the configuration manually requires using multiple pages in the StorageGRID Appliance Installer and applying the configuration file for each node one at a time.

- If you are an advanced user, you can use the following StorageGRID Python scripts to install and configure your system:
  - `configure-sga.py`: Automate the installation and configuration of your appliances. See [Automate appliance installation and configuration using configure-sga.py script](#).
  - `configure-storagegrid.py`: Configure other components of the entire StorageGRID system (the "grid"). See [Automate StorageGRID configuration](#).



You can use StorageGRID automation Python scripts directly, or you can use them as examples of how to use the StorageGRID Installation REST API in grid deployment and configuration tools you develop yourself. See the instructions for [downloading and extracting the StorageGRID installation files](#).

# Automate appliance configuration using StorageGRID Appliance Installer

After you have generated a JSON file, you can automate the configuration of one or more appliances by using the StorageGRID Appliance Installer to upload the JSON file.

## Before you begin

- The appliance has been installed in a rack, connected to your networks, and powered on.
- You have [generated the JSON file](#) with the guidance of your NetApp Professional Services consultant.
- Your appliance contains the latest firmware compatible with StorageGRID 11.5 or higher.
- You are connected to the StorageGRID Appliance Installer on the appliance you are configuring using a [supported web browser](#).

## Steps

1. In the StorageGRID Appliance Installer, select **Advanced > Update Appliance Configuration**. The Update Appliance Configuration page appears.
2. Browse for and select the JSON file with the configuration you want to upload.

The file is uploaded and validated. When the validation process is complete, the file name is shown next to a green check mark.



You might lose connection to the appliance if the configuration from the JSON file includes sections for `link_config`, `networks`, or both. If you aren't reconnected within 1 minute, re-enter the appliance URL using one of the other IP addresses assigned to the appliance.

### Upload JSON

JSON configuration	<input type="button" value="Browse"/>	<input type="text" value="✓ appliances.orig.json"/>
Node name	<input type="text" value="-- Select a node"/>	
<input type="button" value="Apply JSON configuration"/>		

The **Node name** drop down is populated with the top-level node names defined in the JSON file.



If the file is not valid, the file name is shown in red and an error message is displayed in a yellow banner. The invalid file is not applied to the appliance. ConfigBuilder verifies that you have a valid JSON file.

3. Select a node from the list in the **Node name** drop down.

The **Apply JSON configuration** button becomes enabled.

4. Select **Apply JSON configuration**.

The configuration is applied to the selected node.

## Automate appliance installation and configuration using `configure-sga.py` script

If you are an advanced user, you can use the `configure-sga.py` script to automate many of the installation and configuration tasks for StorageGRID appliance nodes, including installing and configuring a primary Admin Node. This script can be useful if you have a large number of appliances to configure.

You can also use the script to generate a JSON file that contains appliance configuration information. You can upload the JSON file to the StorageGRID Appliance Installer to configure all appliance nodes at the same time. You can also edit the JSON file, then upload it to apply a new configuration to one or more appliances.



This procedure is for advanced users with experience using command-line interfaces. Alternatively, you can [use the StorageGRID Appliance Installer to automate the configuration](#).

### Before you begin

- The appliance has been installed in a rack, connected to your networks, and powered on.
- You have [generated the JSON file](#) with the guidance of your NetApp Professional Services consultant.
- Your appliance contains the latest firmware compatible with StorageGRID 11.5 or higher.
- You have configured the IP address of the Admin Network for the appliance.
- You have downloaded the `configure-sga.py` file. The file is included in the installation archive, or you can access it by clicking **Help > Appliance Installation Script** in the StorageGRID Appliance Installer.

### Steps

1. Log in to the Linux machine you are using to run the Python script.
2. For general help with the script syntax and to see a list of the available parameters, enter the following:

```
./configure-sga.py --help
```

The `configure-sga.py` script uses five subcommands:

- `advanced` for advanced StorageGRID appliance interactions, including BMC configuration and creating a JSON file containing the current configuration of the appliance
- `configure` for configuring the RAID mode, node name, and networking parameters
- `install` for starting a StorageGRID installation
- `monitor` for monitoring a StorageGRID installation
- `reboot` for rebooting the appliance

If you enter a subcommand (`advanced`, `configure`, `install`, `monitor`, or `reboot`) argument followed by the `--help` option you will get a different help text providing more detail on the options available within that subcommand:

```
./configure-sga.py subcommand --help
```

If you will [back up the appliance configuration to a JSON file](#), ensure the node names follow these requirements:

- Each node name is unique if you want to automatically configure all appliance nodes using a JSON file.

- Must be a valid hostname containing at least 1 and no more than 32 characters.
  - Can use letters, numbers, and hyphens.
  - Can't start or end with a hyphen.
  - Can't contain only numbers.
3. To apply the configuration from the JSON file to the appliance, enter the following, where *SGA-INSTALL-IP* is the Admin Network IP address for the appliance, *json-file-name* is the name of the JSON file, and *node-name-inside-json-file* is the name of the node with the configuration being applied:
 

```
./configure-sga.py advanced --restore-file json-file-name --restore-node node-name-inside-json-file SGA-INSTALL-IP
```
  4. To confirm the current configuration of the appliance node, enter the following where *SGA-INSTALL-IP* is the Admin Network IP address for the appliance:
 

```
./configure-sga.py configure SGA-INSTALL-IP
```

The results show current IP information for the appliance, including the IP address of the primary Admin Node and information about the Admin, Grid, and Client Networks.

```
Connecting to +https://10.224.2.30:8443+ (Checking version and
connectivity.)
2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
200
```

```
StorageGRID Appliance
Name:          LAB-SGA-2-30
Node type:    storage
```

```
StorageGRID primary Admin Node
IP:           172.16.1.170
State:        unknown
Message:      Initializing...
Version:      Unknown
```

#### Network Link Configuration

```
Link Status
```

Link	State	Speed (Gbps)
1	Up	10
2	Up	10
3	Up	10

4	Up	10
5	Up	1
6	Down	N/A

#### Link Settings

Port bond mode: FIXED  
Link speed: 10GBE

Grid Network: ENABLED  
Bonding mode: active-backup  
VLAN: novlan  
MAC Addresses: 00:a0:98:59:8e:8a 00:a0:98:59:8e:82

Admin Network: ENABLED  
Bonding mode: no-bond  
MAC Addresses: 00:80:e5:29:70:f4

Client Network: ENABLED  
Bonding mode: active-backup  
VLAN: novlan  
MAC Addresses: 00:a0:98:59:8e:89 00:a0:98:59:8e:81

#### Grid Network

CIDR: 172.16.2.30/21 (Static)  
MAC: 00:A0:98:59:8E:8A  
Gateway: 172.16.0.1  
Subnets: 172.17.0.0/21  
172.18.0.0/21  
192.168.0.0/21  
MTU: 1500

#### Admin Network

CIDR: 10.224.2.30/21 (Static)  
MAC: 00:80:E5:29:70:F4  
Gateway: 10.224.0.1  
Subnets: 10.0.0.0/8  
172.19.0.0/16  
172.21.0.0/16  
MTU: 1500

#### Client Network

CIDR: 47.47.2.30/21 (Static)  
MAC: 00:A0:98:59:8E:89  
Gateway: 47.47.0.1  
MTU: 2000

```
#####
##### If you are satisfied with this configuration, #####
##### execute the script with the "install" sub-command. #####
#####
```

5. If you need to change any of the values in the current configuration, use the `configure` subcommand to update them. For example, if you want to change the IP address that the appliance uses for connection to the primary Admin Node to `172.16.2.99`, enter the following:

```
./configure-sga.py configure --admin-ip 172.16.2.99 SGA-INSTALL-IP
```

6. If you want to back up the appliance configuration to a JSON file, use the `advanced` and `backup-file` subcommands. For example, if you want to back up the configuration of an appliance with IP address `SGA-INSTALL-IP` to a file named `appliance-SG1000.json`, enter the following:

```
./configure-sga.py advanced --backup-file appliance-SG1000.json SGA-INSTALL-IP
```

The JSON file containing the configuration information is written to the path of the output file specified, in this case the relative path for the file `appliance-SG1000.json`.



Check that the top-level node name in the generated JSON file matches the appliance name. Don't make any changes to this file unless you are an experienced user and have a thorough understanding of StorageGRID APIs.

7. When you are satisfied with the appliance configuration, use the `install` and `monitor` subcommands to install the appliance:

```
./configure-sga.py install --monitor SGA-INSTALL-IP
```

```
./configure-sga.py monitor --monitor-storagegrid-install SGA-INSTALL-IP
```

8. If you want to reboot the appliance, enter the following:

```
./configure-sga.py reboot SGA-INSTALL-IP
```

## Automate StorageGRID configuration

After you have installed and configured the grid nodes, you can automate the configuration of the StorageGRID system.

### Before you begin

- You know the location of the following files from the installation archive.

Filename	Description
<code>configure-storagegrid.py</code>	Python script used to automate the configuration
<code>configure-storagegrid.sample.json</code>	Example configuration file for use with the script
<code>configure-storagegrid.blank.json</code>	Blank configuration file for use with the script

- You have created a `configure-storagegrid.json` configuration file. To create this file, you can modify the example configuration file (`configure-storagegrid.sample.json`) or the blank configuration file

(configure-storagegrid.blank.json).

### About this task

You can use the `configure-storagegrid.py` Python script and the `configure-storagegrid.json` configuration file to automate the configuration of your StorageGRID system.



You can also configure the system using the [Grid Manager](#) or the [Installation API](#).

### Steps

1. Log in to the Linux machine you are using to run the Python script.
2. Change to the directory where you extracted the installation archive.

For example:

```
cd StorageGRID-Webscale-version/platform
```

where *platform* is `debs`, `rpms`, or `vsphere`.

3. Run the Python script and use the configuration file you created.

For example:

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

### After you finish

A Recovery Package `.zip` file is generated during the configuration process, and it is downloaded to the directory where you are running the installation and configuration process. You must back up the Recovery Package file so that you can recover the StorageGRID system if one or more grid nodes fails. For example, copy it to a secure, backed up network location and to a secure cloud storage location.



The Recovery Package file must be secured because it contains encryption keys and passwords that can be used to obtain data from the StorageGRID system.

If you specified that random passwords should be generated, you need to extract the `Passwords.txt` file and look for the passwords required to access your StorageGRID system.

```
#####  
##### The StorageGRID "recovery package" has been downloaded as: #####  
#####      ./sgws-recovery-package-994078-rev1.zip      #####  
##### Safeguard this file as it will be needed in case of a #####  
##### StorageGRID node recovery. #####  
#####
```

Your StorageGRID system is installed and configured when a confirmation message is displayed.

```
StorageGRID has been configured and installed.
```



# Overview of installation REST APIs

StorageGRID provides two REST APIs for performing installation tasks: the StorageGRID Installation API and the StorageGRID Appliance Installer API.

Both APIs use the Swagger open source API platform to provide the API documentation. Swagger allows both developers and non-developers to interact with the API in a user interface that illustrates how the API responds to parameters and options. This documentation assumes that you are familiar with standard web technologies and the JSON data format.



Any API operations you perform using the API Docs webpage are live operations. Be careful not to create, update, or delete configuration data or other data by mistake.

Each REST API command includes the API's URL, an HTTP action, any required or optional URL parameters, and an expected API response.

## StorageGRID Installation API

The StorageGRID Installation API is only available when you are initially configuring your StorageGRID system, and if you need to perform a primary Admin Node recovery. The Installation API can be accessed over HTTPS from the Grid Manager.

To access the API documentation, go to the installation web page on the primary Admin Node and select **Help > API documentation** from the menu bar.

The StorageGRID Installation API includes the following sections:

- **config**: Operations related to the product release and versions of the API. You can list the product release version and the major versions of the API supported by that release.
- **grid**: Grid-level configuration operations. You can get and update grid settings, including grid details, Grid Network subnets, grid passwords, and NTP and DNS server IP addresses.
- **nodes**: Node-level configuration operations. You can retrieve a list of grid nodes, delete a grid node, configure a grid node, view a grid node, and reset a grid node's configuration.
- **provision**: Provisioning operations. You can start the provisioning operation and view the status of the provisioning operation.
- **recovery**: Primary Admin Node recovery operations. You can reset information, upload the Recover Package, start the recovery, and view the status of the recovery operation.
- **recovery-package**: Operations to download the Recovery Package.
- **sites**: Site-level configuration operations. You can create, view, delete, and modify a site.

## StorageGRID Appliance Installer API

The StorageGRID Appliance Installer API can be accessed over HTTPS from `Controller_IP:8443`.

To access the API documentation, go to the StorageGRID Appliance Installer on the appliance and select **Help > API Docs** from the menu bar.

The StorageGRID Appliance Installer API includes the following sections:

- **clone**: Operations to configure and control node cloning.

- **encryption:** Operations to manage encryption and view encryption status.
- **hardware config:** Operations to configure system settings on attached hardware.
- **installation:** Operations for starting the appliance installation and for monitoring installation status.
- **networking:** Operations related to the Grid, Admin, and Client Network configuration for a StorageGRID appliance and appliance port settings.
- **setup:** Operations to help with initial appliance installation setup including requests to get information about the system and update the primary Admin Node IP.
- **support:** Operations for rebooting the controller and getting logs.
- **update-config:** Operations to update StorageGRID appliance configuration.
- **upgrade:** Operations related to upgrading appliance firmware.
- **uploadsg:** Operations for uploading StorageGRID installation files.

## Install appliance hardware

### Register hardware

Registering the appliance hardware provides support benefits.

#### Steps

1. Locate the chassis serial number for the appliance. For SG6000 appliances the chassis serial number is on the storage controller shelf.

You can find the number on the packing slip, in your confirmation email, or on the appliance after you unpack it.



There are several serial numbers on the SG6000 storage appliance. The serial number on the storage controller shelf is the one that must be registered and used if you call for service or support on the SG6000 appliance.

2. Go to the NetApp Support Site at [mysupport.netapp.com](https://mysupport.netapp.com).
3. Determine whether you need to register the hardware:

If you are a...	Follow these steps...
Existing NetApp customer	<ol style="list-style-type: none"> <li>a. Sign in with your username and password.</li> <li>b. Select <b>Products &gt; My Products</b>.</li> <li>c. Confirm that the new serial number is listed.</li> <li>d. If it is not, follow the instructions for new NetApp customers.</li> </ol>

If you are a...	Follow these steps...
New NetApp customer	<p>a. Click <b>Register Now</b>, and create an account.</p> <p>b. Select <b>Products &gt; Register Products</b>.</p> <p>c. Enter the product serial number and requested details.</p> <p>After your registration is approved, you can download any required software. The approval process might take up to 24 hours.</p>

## Install into cabinet or rack

### Install into cabinet or rack (SG100 and SG1000)

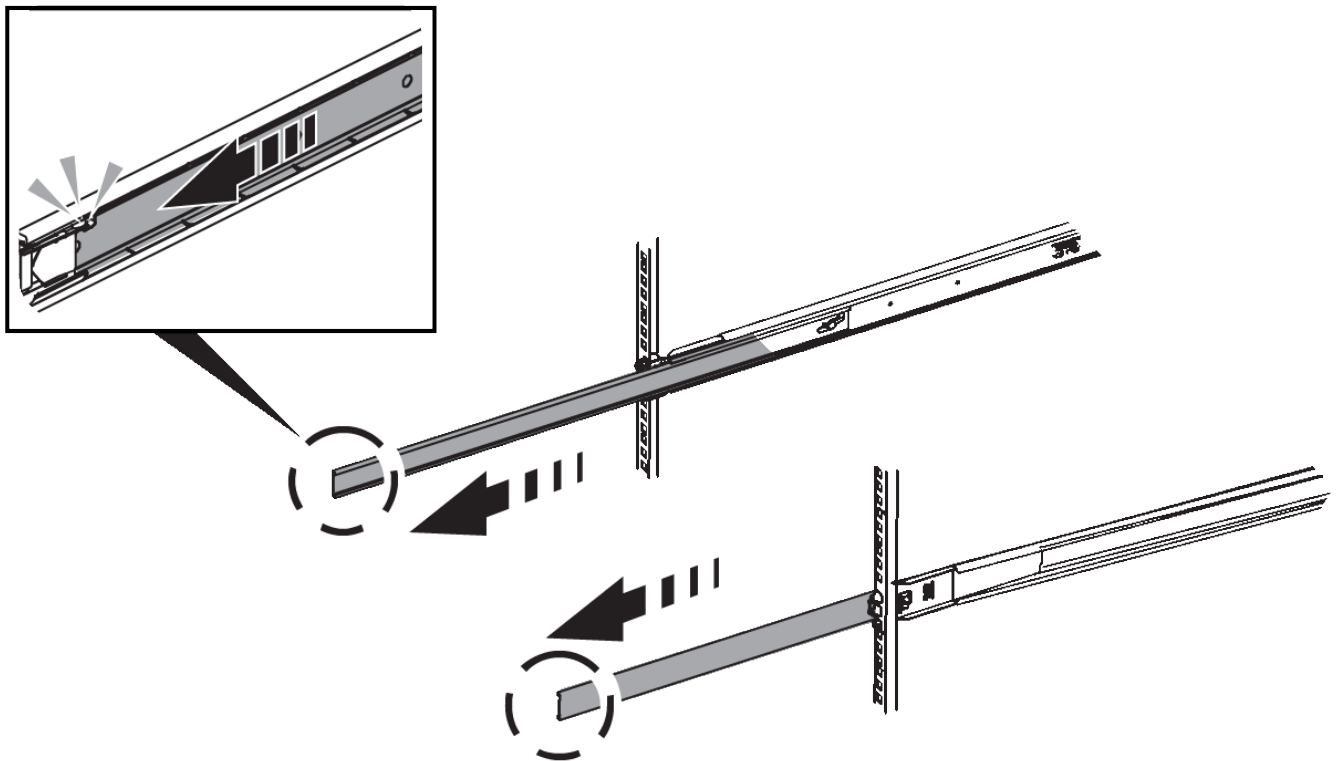
You install a set of rails for the appliance in your cabinet or rack, and then slide the appliance onto the rails.

#### Before you begin

- You have reviewed the Safety Notices document included in the box, and understand the precautions for moving and installing hardware.
- You have the instructions packaged with the rail kit.

#### Steps

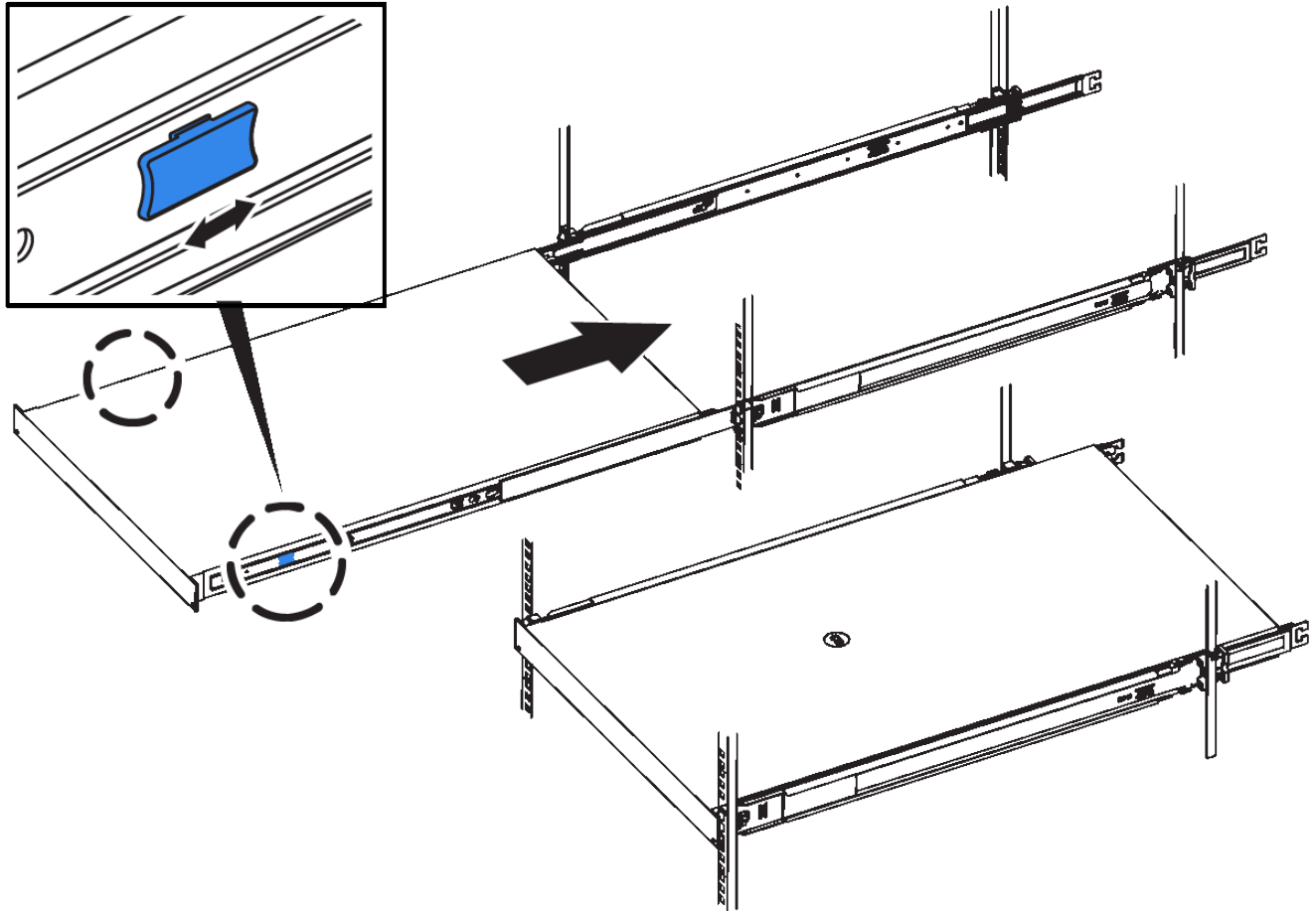
1. Carefully follow the instructions for the rail kit to install the rails in your cabinet or rack.
2. On the two rails installed in the cabinet or rack, extend the movable parts of the rails until you hear a click.



3. Insert the appliance into the rails.

4. Slide the appliance into the cabinet or rack.

When you can't move the appliance any further, pull the blue latches on both sides of the chassis to slide the appliance all the way in.



Don't attach the front bezel until after you power on the appliance.

**Install into cabinet or rack (SG5700)**

You install a set of rails in your cabinet or rack and then slide the appliance onto the rails. If you have an SG5760, install the drives after installing the appliance.

**Before you begin**

- You have reviewed the Safety Notices document included in the box, and understand the precautions for moving and installing hardware.
- You have the instructions packaged with the rail kit.

**Install SG5712**

Follow these steps to install an SG5712 appliance into a rack or cabinet.



The SG5712 weighs approximately 64 lb (29 kg) when fully loaded with drives. Two people or a mechanized lift are required to safely move the SG5712.



Install hardware from the bottom of the rack or cabinet or rack up to prevent the equipment from tipping over.

### Steps

1. Follow the instructions for the rail kit to install the rails.
2. Place the back of the appliance (the end with the connectors) on the rails.
3. Carefully slide the appliance all the way back into the cabinet or rack.
4. Secure the appliance to the cabinet or rack as directed in the rail kit instructions.
5. Attach the bezel to the front.

### Install SG5760

Follow these steps to install an SG5760 appliance and any expansion shelves into a rack or cabinet.



Install hardware from the bottom of the rack or cabinet or rack up to prevent the equipment from tipping over.



The SG5760 weighs approximately 132 lb (60 kg) with no drives installed. Four people or a mechanized lift are required to safely move an empty SG5760.



To avoid damaging the hardware, never move an SG5760 if drives are installed. You must remove all drives before moving the shelf.

### Steps

1. Follow the instructions for the rail kit to install the rails in your cabinet or rack.
2. Prepare to move the appliance:
  - a. Remove the outer packing box.
  - b. Fold down the flaps on the inner box.
  - c. If you are lifting the SG5760 by hand, attach the four handles to the sides of the chassis.

You remove these handles as you slide the appliance onto the rails.

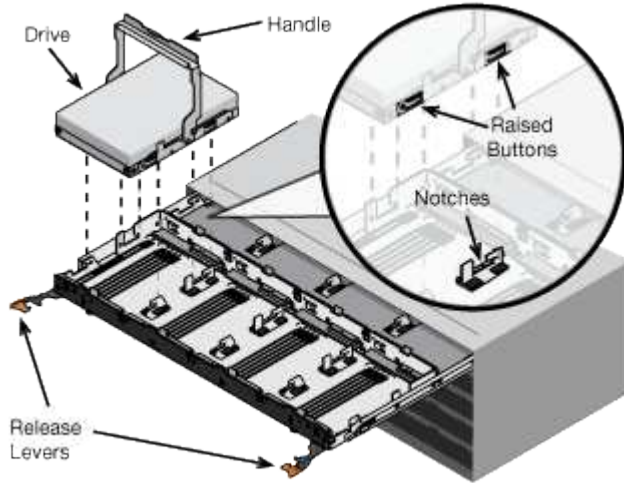
3. If your cabinet has square hole, install the cage nuts so that you can secure the front and rear of the shelf with screws.
4. Place the back of the appliance (the end with the connectors) on the rails.
5. Supporting the appliance from the bottom, slide it into the rack or cabinet.

Use the thumb latches to detach the handles as you slide the appliance in.

6. Secure the appliance to the front of the rack by inserting two screws in the first and third holes (counting down from the top) on each side.
7. Secure the appliance to the rear of the rack or cabinet with the brackets.
8. Install 12 drives in each of the five drive drawers.

You must install all 60 drives to ensure correct operation.

- a. Put on the ESD wristband, and remove the drives from their packaging.
- b. Release the levers on the top drive drawer, and slide the drawer out using the levers.
- c. Raise the drive handle to vertical, and align the buttons on the drive with the notches on the drawer.



- d. Pressing gently on the top of the drive, rotate the drive handle down until the drive snaps into place.
- e. After installing the first 12 drives, slide the drawer back in by pushing on the center and closing both levers gently.
- f. Repeat these steps for the other four drawers.

9. Attach the front bezel.

## SG6000

### Install into cabinet or rack (SG6000)

For the SG6060 and SGF6024, you install rails in your cabinet or rack and slide the controller shelf, any expansion shelves, and the compute controller onto the rails. For the SG6060, don't install the drives in each shelf until the shelves are installed.

Model	Install	For information
SG6060	60-drive controller shelf and any 60-drive expansion shelves	<a href="#">Install 60-drive shelves</a>
SG6060	60 drives into each shelf	<a href="#">Install drives</a>
SGF6024	24-drive controller shelf	<a href="#">Install 24-drive shelves</a>
SG6060 and SGF6024	SG6000-CN compute controller	<a href="#">Install SG6000-CN controller</a>

### Install 60-drive shelves (SG6060)

You install a set of rails for the E2860 controller shelf in your cabinet or rack, and then slide the controller shelf onto the rails. If you are installing 60-drive expansion shelves,

the same procedure applies.

### Before you begin

- You have reviewed the Safety Notices document included in the box, and understand the precautions for moving and installing hardware.
- You have the instructions packaged with the rail kit.



Each 60-drive shelf weighs approximately 132 lb (60 kg) without drives installed. Four people or a mechanized lift are required to safely move the shelf.



To avoid damaging the hardware, never move the shelf if drives are installed. You must remove all drives before moving the shelf.



When installing the E2860 controller shelf or optional expansion shelves, install hardware from the bottom to the top of the rack or cabinet to prevent the equipment from tipping over. To ensure that the heaviest equipment is at the bottom of the cabinet or rack, install the SG6000-CN controller above the E2860 controller shelf and expansion shelves.



Before committing to the installation, verify that the 0.5m optic cables shipped with the appliance, or cables that you supply, are long enough for the planned layout.

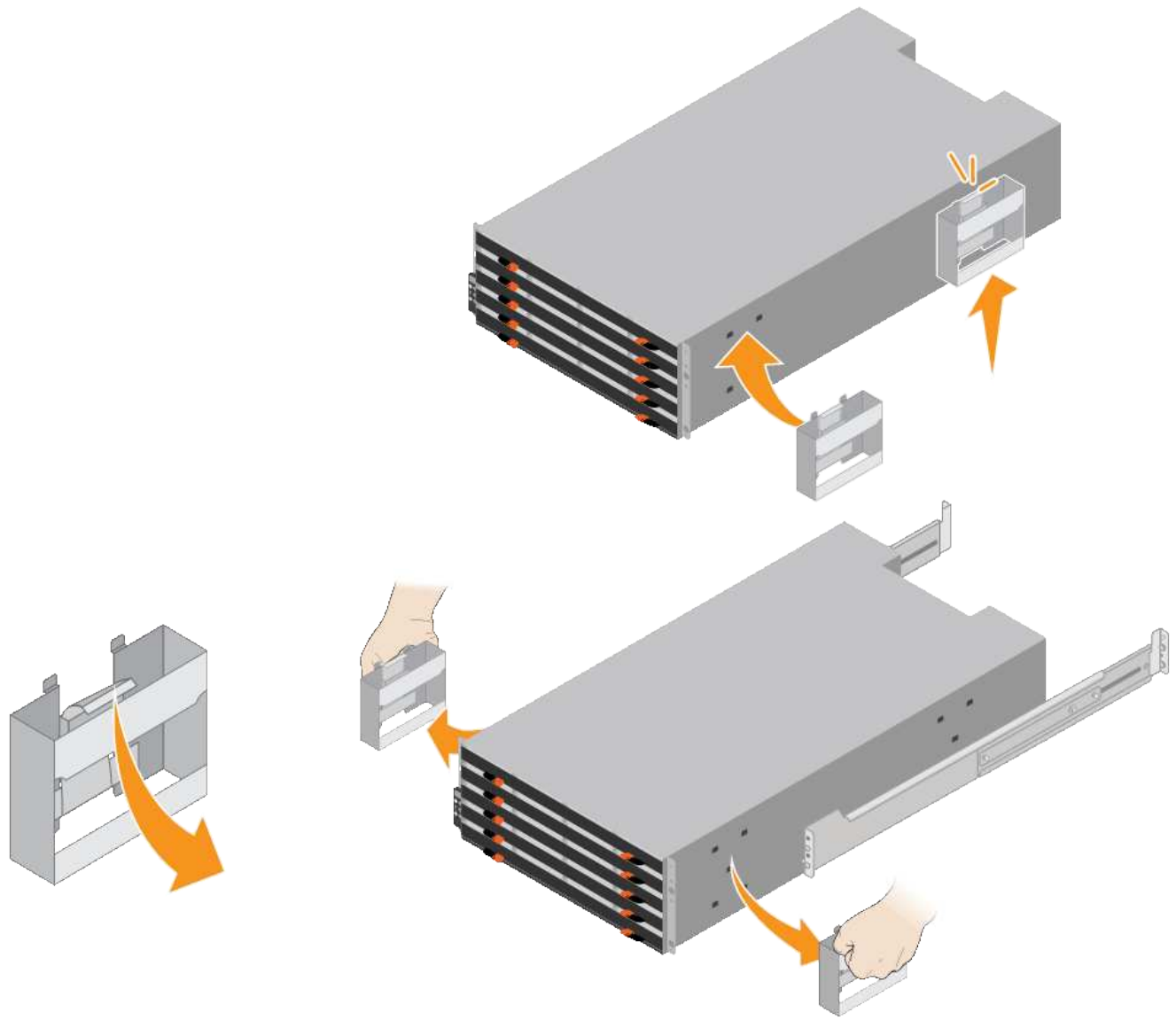
### Steps

1. Carefully follow the instructions for the rail kit to install the rails in your cabinet or rack.

For square hole cabinets, first install the provided cage nuts to secure the front and rear of the shelf with screws.

2. Remove the outer packing box for the appliance. Then, fold down the flaps on the inner box.
3. If you are lifting the appliance by hand, attach the four handles to the sides of the chassis.

Push up on each handle until it clicks into place.



4. Place the back of the shelf (the end with the connectors) on the rails.
5. Supporting the shelf from the bottom, slide it into the cabinet. If you are using the handles, use the thumb latches to detach one handle at a time as you slide the shelf in.

To remove the handles, pull back on the release latch, push down, then pull away from the shelf.

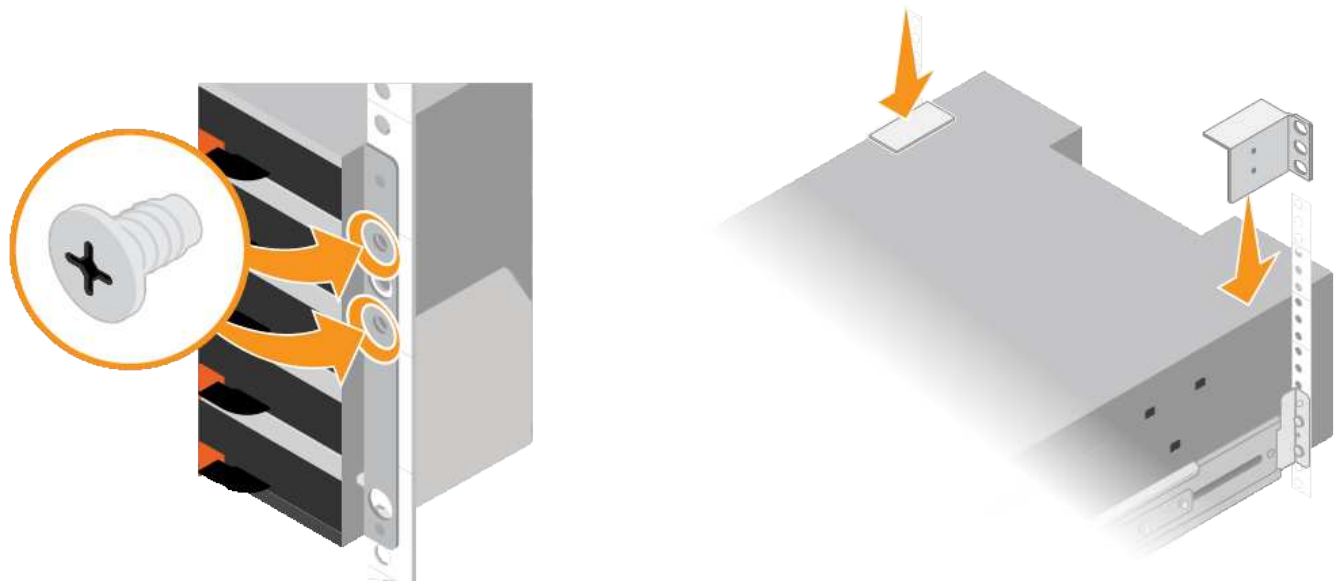
6. Secure the shelf to the front of the cabinet.

Insert screws into the first and third holes from the top of the shelf on both sides.

7. Secure the shelf to the rear of the cabinet.

Place two back brackets on each side of the upper rear section of the shelf. Insert screws into the first and third holes of each bracket.





8. Repeat these steps for any expansion shelves.

#### Install drives (SG6060)

After installing the 60-drive shelf into a cabinet or rack, install all 60 drives into the shelf. The shipment for the E2860 controller shelf includes two SSD drives, which you should install in the top drawer of the controller shelf. Each optional expansion shelf includes 60 HDD drives and no SSD drives.

#### Before you begin

You have installed the E2860 controller shelf or optional expansion shelves (one or two) in the cabinet or rack.



To avoid damaging the hardware, never move the shelf if drives are installed. You must remove all drives before moving the shelf.

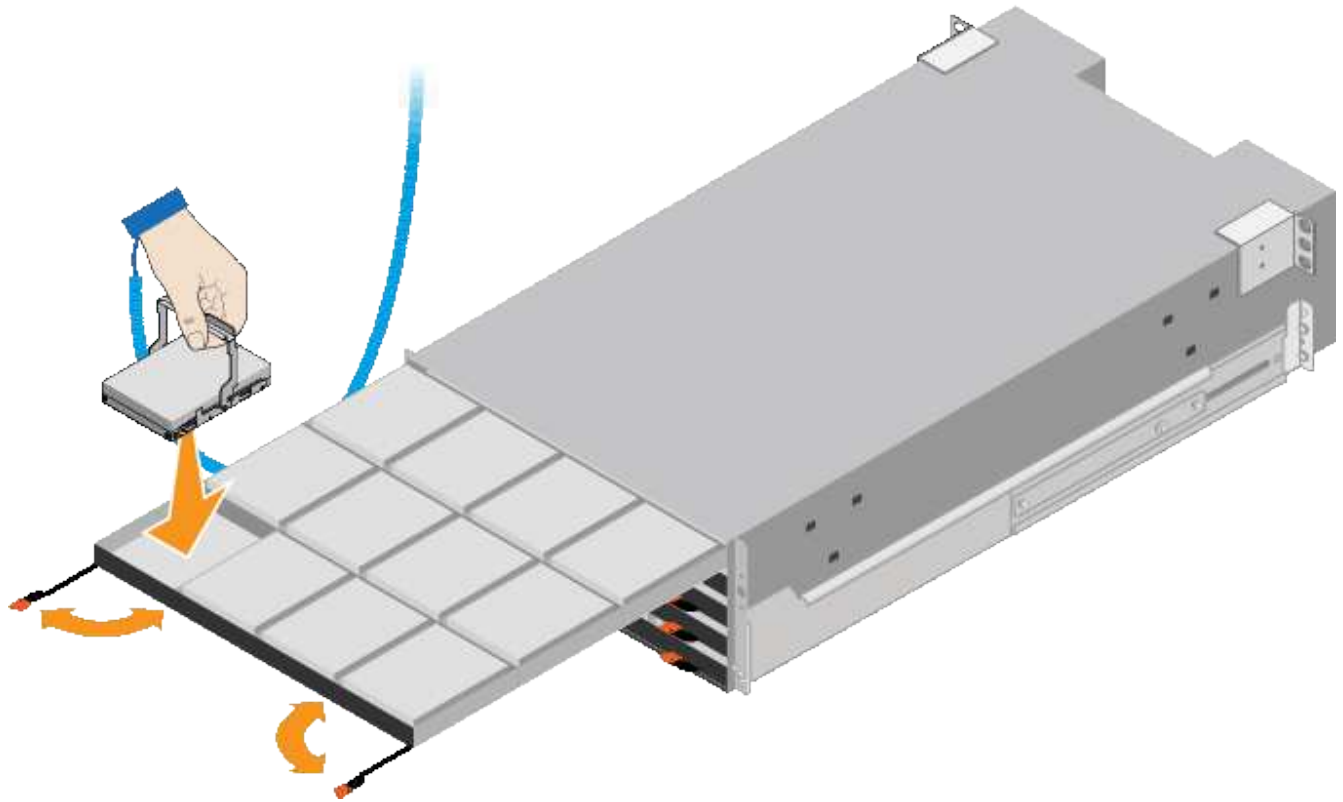
#### Steps

1. Wrap the strap end of the ESD wristband around your wrist, and secure the clip end to a metal ground to prevent static discharge.
2. Remove the drives from their packaging.
3. Release the levers on the top drive drawer, and slide the drawer out using the levers.
4. Locate the two SSD drives.



Expansion shelves don't use SSD drives.

5. Raise each drive handle to a vertical position.
6. Install the two SSD drives in slots 0 and 1 (the first two slots along the lefthand side of the drawer).
7. Gently position each drive into its slot, and lower the raised drive handle until it clicks into place.



8. Install 10 HDD drives into the top drawer.
9. Slide the drawer back in by pushing on the center and closing both levers gently.



Stop pushing the drawer if you feel binding. Use the release levers at the front of the drawer to slide the drawer back out. Then, carefully reinsert the drawer into the slot.

10. Repeat these steps to install HDD drives into the other four drawers.



You must install all 60 drives to ensure correct operation.

11. Attach the front bezel to the shelf.
12. If you have expansion shelves, repeat these steps to install 12 HDD drives into each drawer of each expansion shelf.
13. Proceed to the instructions for installing the SG6000-CN into a cabinet or rack.

#### Install 24-drive shelves (SGF6024)

You install a set of rails for the EF570 controller shelf in your cabinet or rack, and then slide the array onto the rails.

#### Before you begin

- You have reviewed the Safety Notices document included in the box, and understand the precautions for moving and installing hardware.
- You have the instructions packaged with the rail kit.

#### Steps

1. Carefully follow the instructions for the rail kit to install the rails in your cabinet or rack.

For square hole cabinets, first install the provided cage nuts to secure the front and rear of the shelf with screws.

2. Remove the outer packing box for the appliance. Then, fold down the flaps on the inner box.
3. Place the back of the shelf (the end with the connectors) on the rails.



A fully loaded shelf weighs approximately 52 lb (24 kg). Two people are required to safely move the enclosure.

4. Carefully slide the enclosure all the way onto the rails.



You might need to adjust the rails to ensure that the enclosure slides all the way onto the rails.

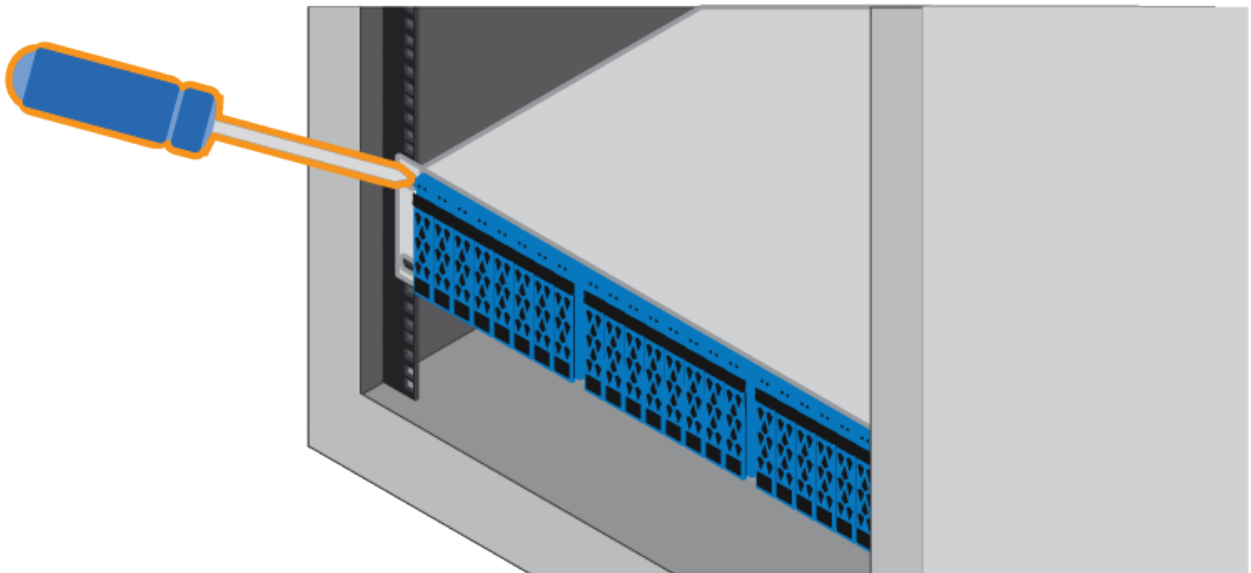


Don't place additional equipment on the rails after you finish installing the enclosure. The rails aren't designed to bear additional weight.

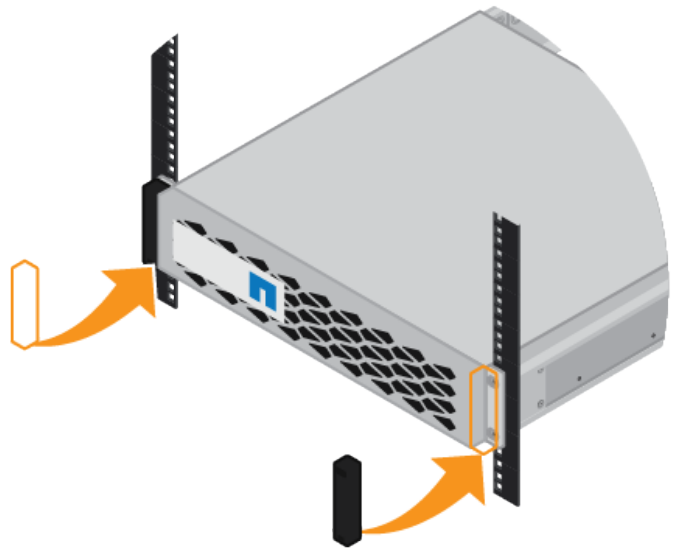


If applicable, you might need to remove the shelf end caps or the system bezel to secure the enclosure to the rack post; if so, you need to replace the end caps or bezel when you are done.

5. Secure the enclosure to the front of the cabinet or rack and rails by inserting two M5 screws through the mounting brackets (preinstalled on either side of the front of the enclosure), the holes on the rack or system cabinet, and the holes on the front of rails.



6. Secure the enclosure to the back of the rails by inserting two M5 screws through the brackets at the enclosure and the rail kit bracket.
7. If applicable, replace the shelf end caps or the system bezel.



#### Install SG6000-CN controller (SG6060 and SG6024)

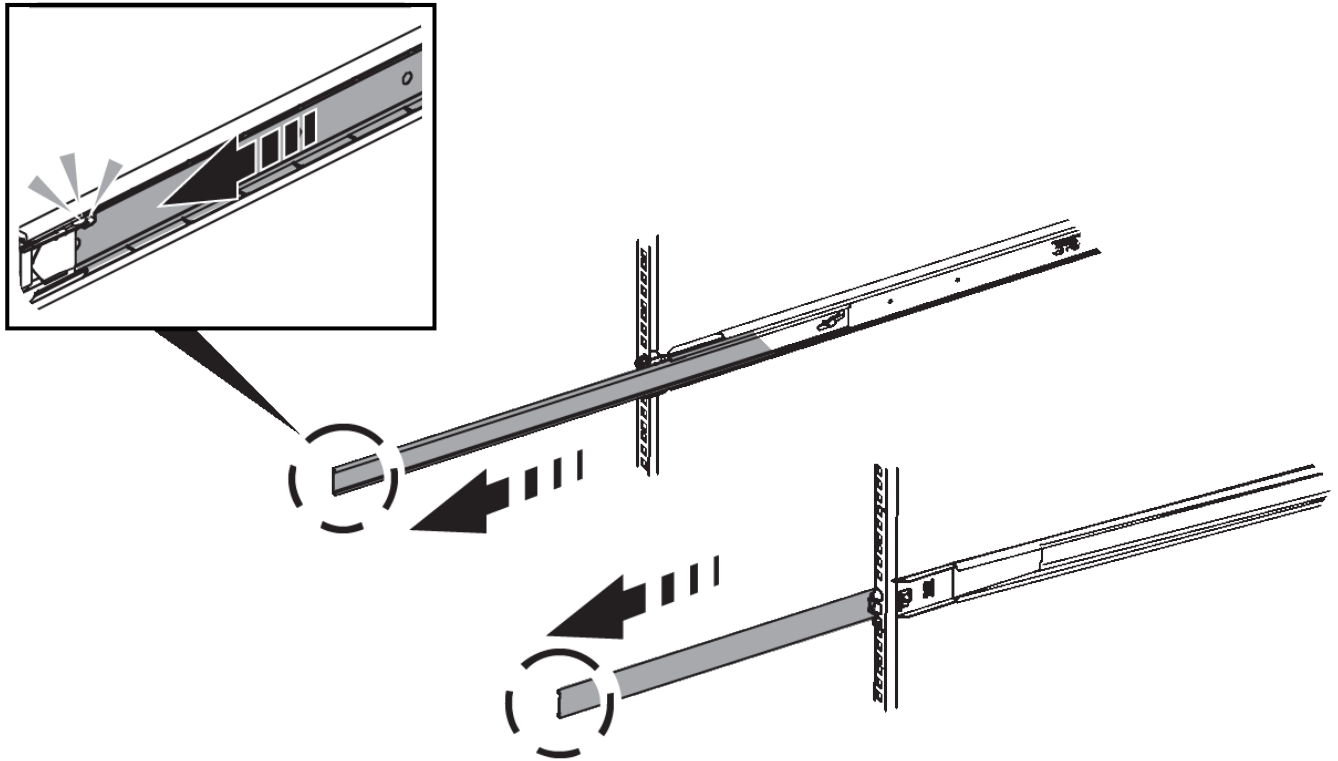
You install a set of rails for the SG6000-CN controller in your cabinet or rack, and then slide the controller onto the rails.

#### Before you begin

- You have reviewed the Safety Notices document included in the box, and understand the precautions for moving and installing hardware.
- You have the instructions packaged with the rail kit.
- You have installed the E2860 controller shelf and drives or the EF570 controller shelf.

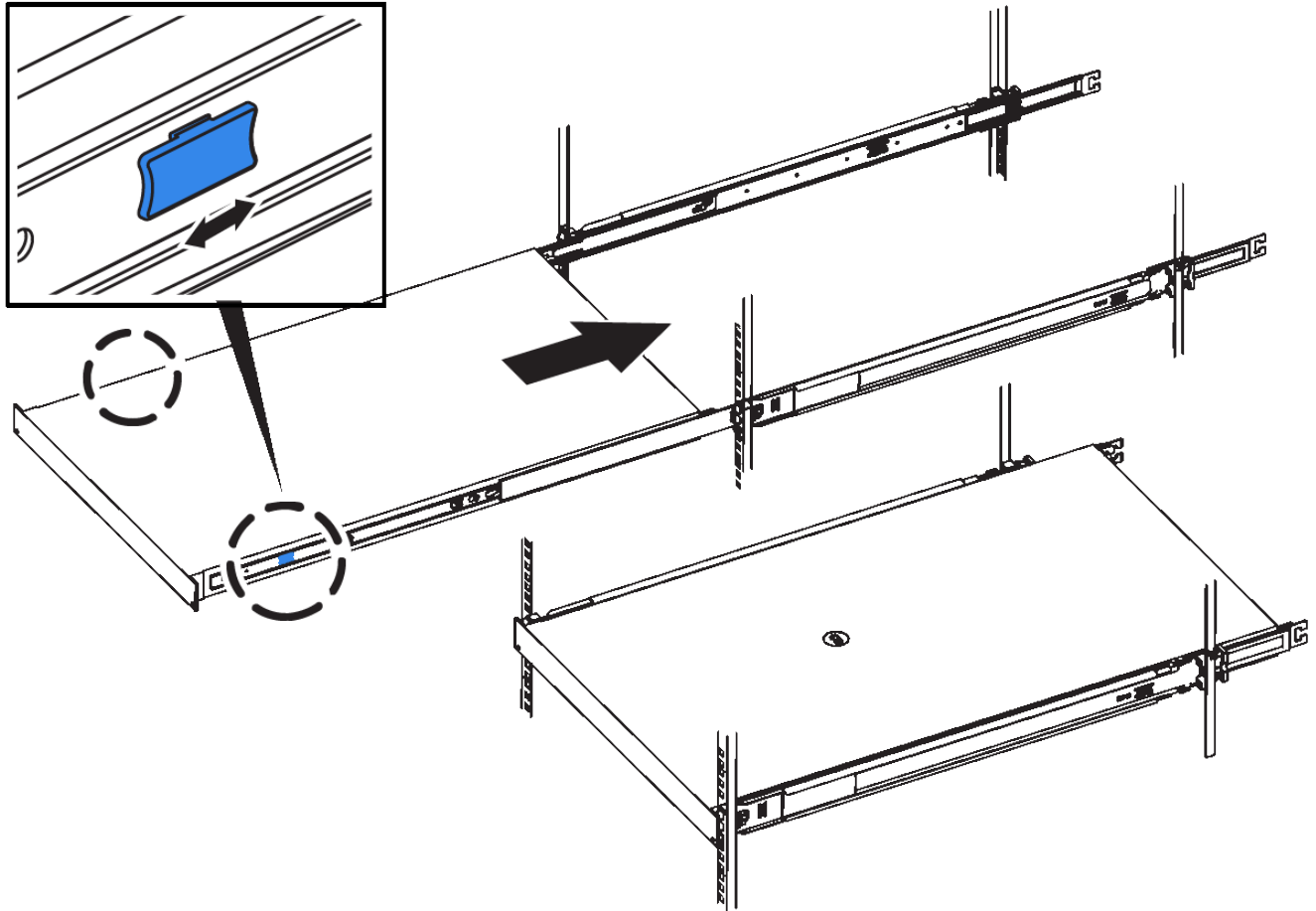
#### Steps

1. Carefully follow the instructions for the rail kit to install the rails in your cabinet or rack.
2. On the two rails installed in the cabinet or rack, extend the movable parts of the rails until you hear a click.



3. Insert the SG6000-CN controller into the rails.
4. Slide the controller into the cabinet or rack.

When you can't move the controller any further, pull the blue latches on both sides of the chassis to slide the controller all the way in.



Don't attach the front bezel until after you power on the controller.

5. Tighten the captive screws on the controller front panel to secure the controller in the rack.



### Install into cabinet or rack (SGF6112)

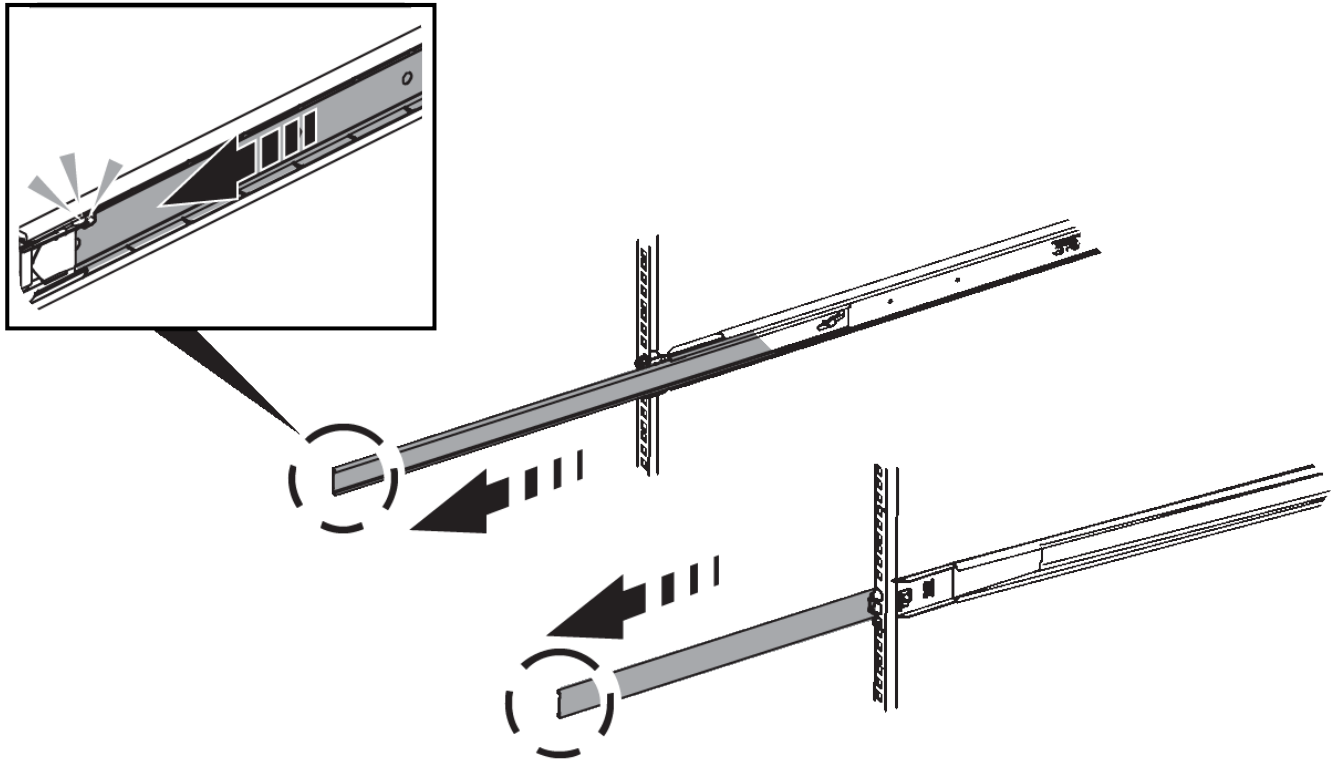
You install a set of rails for the appliance in your cabinet or rack, and then slide the appliance onto the rails.

#### Before you begin

- You have reviewed the Safety Notices document included in the box and understand the precautions for moving and installing hardware.
- You have the instructions packaged with the rail kit.

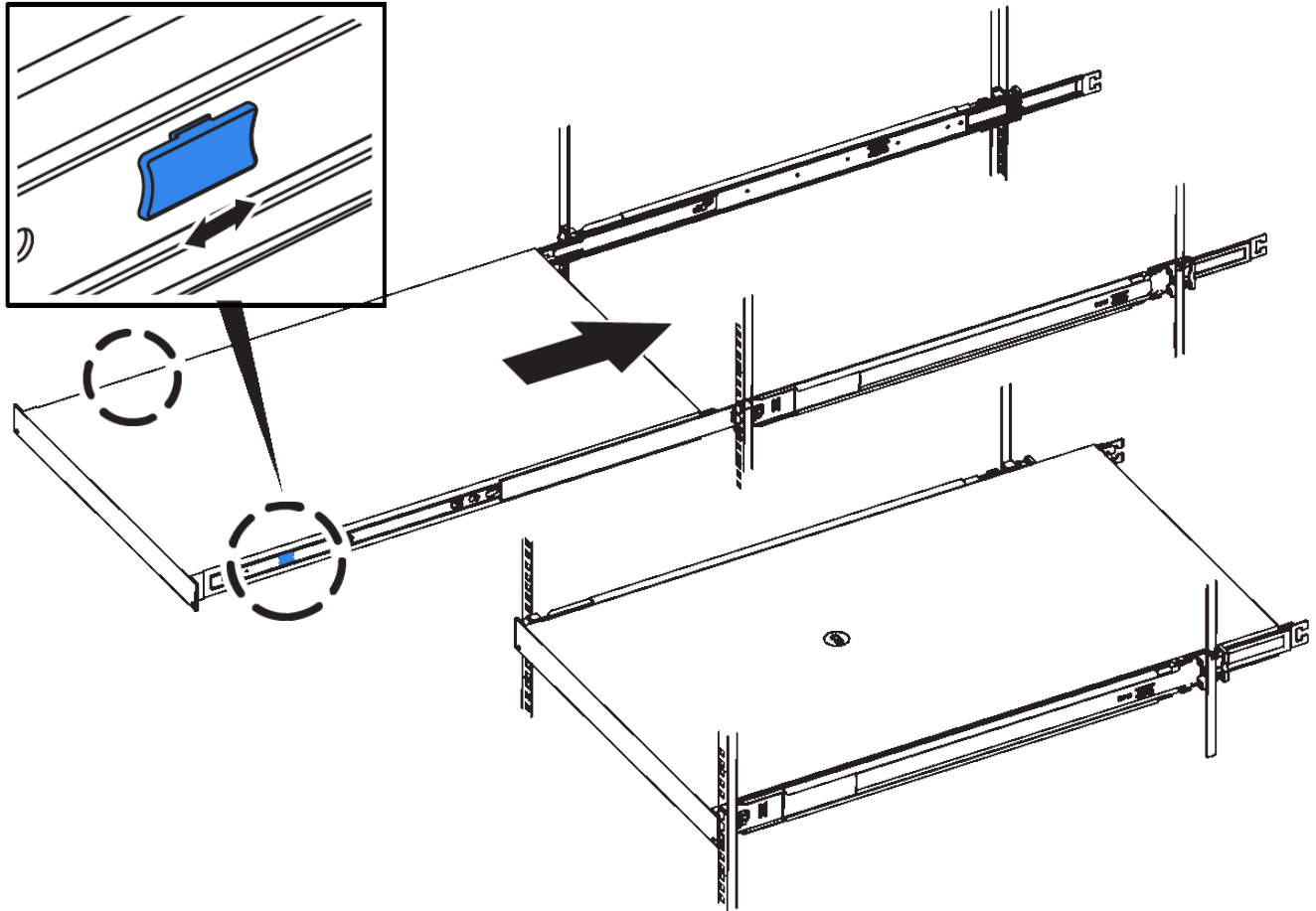
#### Steps

1. Carefully follow the instructions for the rail kit to install the rails in your cabinet or rack.
2. On the two rails installed in the cabinet or rack, extend the movable parts of the rails until you hear a click.



3. Insert the appliance into the rails.
4. Slide the appliance into the cabinet or rack.

When you can't move the appliance any further, pull the blue latches on both sides of the chassis to slide the appliance all the way in.



5. Tighten the captive screws on the appliance front panel to secure the appliance in the rack.



Don't attach the front bezel until after you power on the appliance.

## Cable appliance

Connect the network ports on the appliance or controller to the Grid Network and optional Client Network for StorageGRID. For some appliances, you also connect the management port on the appliance to the service laptop or make connections between the controller management ports.



## SG100 and SG1000

You must connect the management port on the appliance to the service laptop and connect the network ports on the appliance to the Grid Network and optional Client Network for StorageGRID.

### Before you begin

- You have an RJ-45 Ethernet cable for connecting the management port.
- You have one of the following options for the network ports. These items aren't provided with the appliance.
  - One to four TwinAx cables for connecting the four network ports.
  - For the SG100, one to four SFP+ or SFP28 transceivers if you plan to use optical cables for the ports.
  - For the SG1000, one to four QSFP+ or QSFP28 transceivers if you plan to use optical cables for the ports.

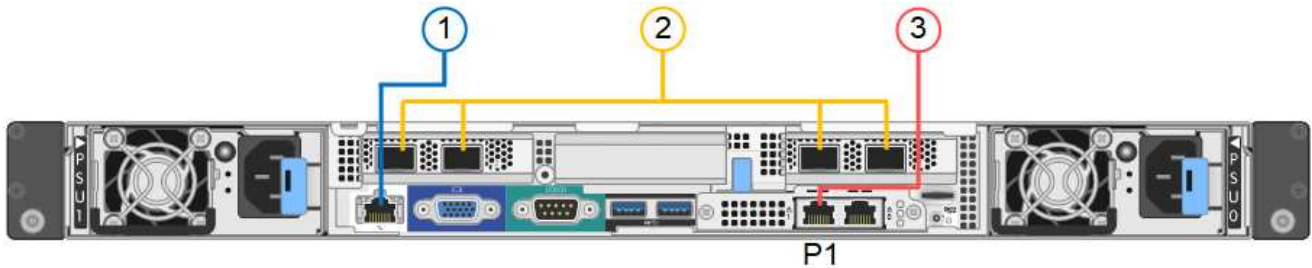


**Risk of exposure to laser radiation** — Don't disassemble or remove any part of an SFP or QSFP transceiver. You might be exposed to laser radiation.

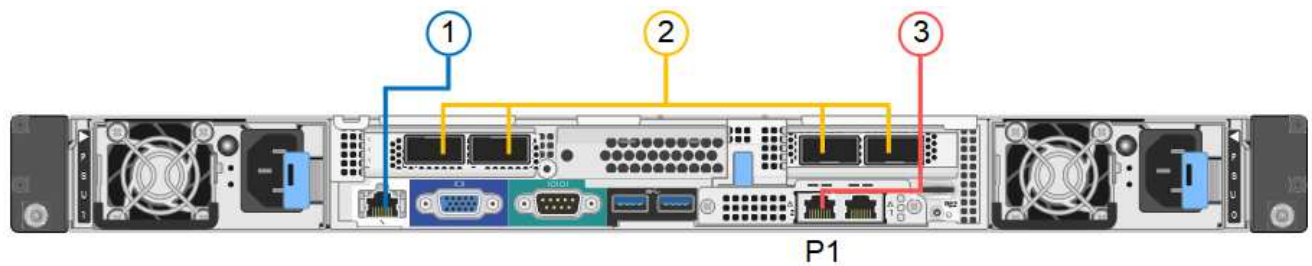
### About this task

The following figures show the ports on the back of the appliance.

SG100 port connections:



SG1000 port connections:



Callout	Port	Type of port	Use
1	BMC management port on the appliance	1-GbE (RJ-45)	Connects to the network where you access the BMC interface.

Callout	Port	Type of port	Use
2	Four network ports on the appliance	<ul style="list-style-type: none"> <li>For the SG100: 10/25-GbE</li> <li>For the SG1000: 10/25/40/100-GbE</li> </ul>	Connect to the Grid Network and the Client Network for StorageGRID. See <a href="#">Port bond modes (Port bond modes (SG100 and SG1000))</a> .
3	Admin Network port on the appliance (labeled P1 in the figures)	1-GbE (RJ-45)  <b>Important:</b> This port operates only at 1000 baseT/full and does not support 10- or 100-megabit speeds.	Connects the appliance to the Admin Network for StorageGRID.
	Rightmost RJ-45 port on the appliance	1-GbE (RJ-45)  <b>Important:</b> This port operates only at 1000 baseT/full and does not support 10- or 100-megabit speeds.	<ul style="list-style-type: none"> <li>Can be bonded with management port 1 if you want a redundant connection to the Admin Network.</li> <li>Can be left disconnected and available for temporary local access (IP 169.254.0.1).</li> <li>During installation, can be used to connect the appliance to a service laptop if DHCP-assigned IP addresses aren't available.</li> </ul>

### Steps

1. Connect the BMC management port on the appliance to the management network, using an Ethernet cable.

Although this connection is optional, it is recommended to facilitate support.

2. Connect the network ports on the appliance to the appropriate network switches, using TwinAx cables or optical cables and transceivers.

See the following table for the equipment required for your hardware and link speed.

SG100 link speed (GbE)	Required equipment
10	SFP+ transceiver
25	SFP28 transceiver
SG1000 link speed (GbE)	Required equipment
10	QSA and SFP+ transceiver
25	QSA and SFP28 transceiver

SG100 link speed (GbE)	Required equipment
40	QSFP+ transceiver
100	QFSP28 transceiver

- On models that support Autonegotiate as a port speed option, if Fixed port bonding mode is selected you can run the ports dedicated to the StorageGRID Grid network at a different speed than the ports dedicated to the Client network.
- On models that do not support Autonegotiate as a port speed option, all four network ports must use the same link speed.
- If you plan to use Fixed port bond mode (default), connect the ports to the StorageGRID Grid and Client Networks, as shown in the table.

Port	Connects to...
Port 1	Client Network (optional)
Port 2	Grid Network
Port 3	Client Network (optional)
Port 4	Grid Network

- If you plan to use the Aggregate port bond mode, connect one or more of the network ports to one or more switches. You should connect at least two of the four ports to avoid having a single point of failure. If you use more than one switch for a single LACP bond, the switches must support MLAG or equivalent.
3. If you plan to use the Admin Network for StorageGRID, connect the Admin Network port on the appliance to the Admin Network, using an Ethernet cable.

## SG5700

You connect the two controllers to each other, connect the management ports on each controller, and connect the 10/25-GbE ports on the E5700SG controller to the Grid Network and optional Client Network for StorageGRID.

### Before you begin

- You have unpacked the following items, which are included with the appliance:
  - Two power cords.
  - Two optical cables for the FC interconnect ports on the controllers.
  - Eight SFP+ transceivers, which support either 10-GbE or 16-Gbps FC. The transceivers can be used with the two interconnect ports on both controllers and with the four 10/25-GbE network ports on the E5700SG controller, assuming you want the network ports to use a 10-GbE link speed.
- You have obtained the following items, which aren't included with the appliance:
  - One to four optical cables for the 10/25-GbE ports you plan to use.

- One to four SFP28 transceivers, if you plan to use 25-GbE link speed.
- Ethernet cables for connecting the management ports.

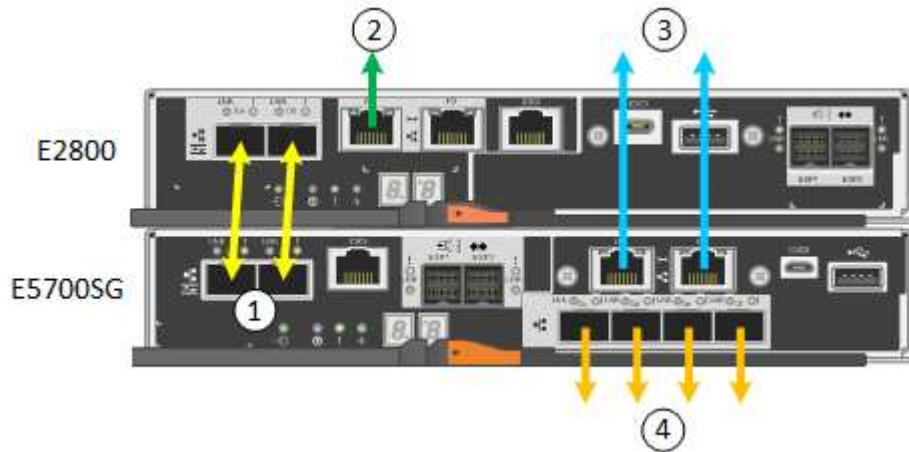


**Risk of exposure to laser radiation** — Don't disassemble or remove any part of an SFP transceiver. You might be exposed to laser radiation.

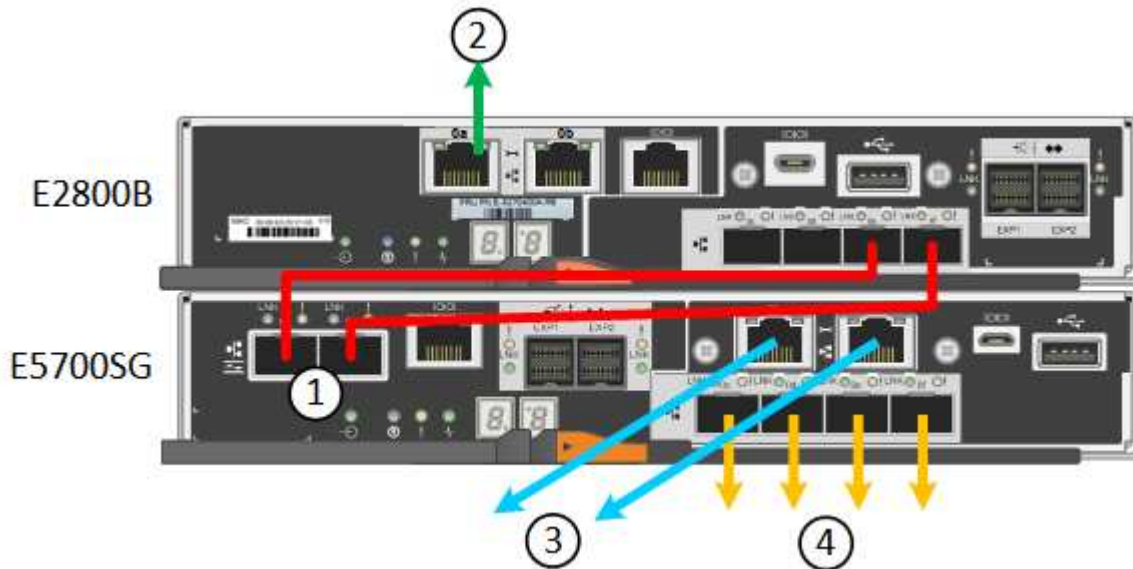
### About this task

The figures show the two controllers in the SG5760 and SG5760X, with the E2800 series storage controller on the top and the E5700SG controller on the bottom. In the SG5712 and SG5712X, the E2800 series storage controller is to the left of the E5700SG controller when viewed from the back.

SG5760 connections:



SG5760X connections:



Callout	Port	Type of port	Use
1	Two interconnect ports on each controller	16Gb/s FC optical SFP+	Connect the two controllers to each other.

Callout	Port	Type of port	Use
2	Management port 1 on the E2800 series controller	1-GbE (RJ-45)	Connects to the network where you access SANtricity System Manager. You can use the Admin Network for StorageGRID or an independent management network.
2	Management port 2 on the E2800 series controller	1-GbE (RJ-45)	Reserved for technical support.
3	Management port 1 on the E5700SG controller	1-GbE (RJ-45)	Connects the E5700SG controller to the Admin Network for StorageGRID.
3	Management port 2 on the E5700SG controller	1-GbE (RJ-45)	<ul style="list-style-type: none"> <li>• Can be bonded with management port 1 if you want a redundant connection to the Admin Network.</li> <li>• Can be left unwired and available for temporary local access (IP 169.254.0.1).</li> <li>• During installation, can be used to connect the E5700SG controller to a service laptop if DHCP-assigned IP addresses aren't available.</li> </ul>
4	10/25-GbE ports 1-4 on the E5700SG controller	10-GbE or 25-GbE <b>Note:</b> The SFP+ transceivers included with the appliance support 10-GbE link speeds. If you want to use 25-GbE link speeds for the four network ports, you must provide SFP28 transceivers.	Connect to the Grid Network and the Client Network for StorageGRID. See <a href="#">Port bond modes (E5700SG controller)</a> .

### Steps

1. Connect the E2800 controller to the E5700SG controller, using two optical cables and four of the eight SFP+ transceivers.

Connect this port...	To this port...
Interconnect port 1 on the E2800 controller	Interconnect port 1 on the E5700SG controller
Interconnect port 2 on the E2800 controller	Interconnect port 2 on the E5700SG controller

- If you plan to use SANtricity System Manager, connect management port 1 (P1) on the E2800 controller (the RJ-45 port on the left) to the management network for SANtricity System Manager, using an Ethernet cable.

Don't use management port 2 (P2) on the E2800 controller (the RJ-45 port on the right). This port is reserved for technical support.

- If you plan to use the Admin Network for StorageGRID, connect management port 1 on the E5700SG controller (the RJ-45 port on the left) to the Admin Network, using an Ethernet cable.

If you plan to use active-backup network bond mode for the Admin Network, connect management port 2 on the E5700SG controller (the RJ-45 port on the right) to the Admin Network, using an Ethernet cable.

- Connect the 10/25-GbE ports on the E5700SG controller to the appropriate network switches, using optical cables and SFP+ or SFP28 transceivers.



Install SFP+ transceivers if you plan to use 10-GbE link speeds. Install SFP28 transceivers if you plan to use 25-GbE link speeds.

- On models that support Autonegotiate as a port speed option, if Fixed port bonding mode is selected you can run the ports dedicated to the StorageGRID Grid network at a different speed than the ports dedicated to the Client network.
- On models that do not support Autonegotiate as a port speed option, all four network ports must use the same link speed.
- If you plan to use Fixed port bond mode (default), connect the ports to the StorageGRID Grid and Client Networks, as shown in the table.

Port	Connects to...
Port 1	Client Network (optional)
Port 2	Grid Network
Port 3	Client Network (optional)
Port 4	Grid Network

- If you plan to use the Aggregate port bond mode, connect one or more of the network ports to one or more switches. You should connect at least two of the four ports to avoid having a single point of failure. If you use more than one switch for a single LACP bond, the switches must support MLAG or equivalent.

## SG6000

You connect the storage controllers to the SG6000-CN controller, connect the management ports on all three controllers, and connect the network ports on the SG6000-CN controller to the Grid Network and optional Client Network for StorageGRID.

### Before you begin

- You have the four optical cables provided with the appliance for connecting the two storage controllers to the SG6000-CN controller.
- You have RJ-45 Ethernet cables (four minimum) for connecting the management ports.
- You have one of the following options for the network ports. These items aren't provided with the appliance.
  - One to four TwinAx cables for connecting the four network ports.
  - One to four SFP+ or SFP28 transceivers if you plan to use optical cables for the ports.



**Risk of exposure to laser radiation** — Don't disassemble or remove any part of an SFP transceiver. You might be exposed to laser radiation.

### About this task

The following figures show the three controllers in the SG6060 and SG6060X appliances, with the SG6000-CN compute controller on the top and the two E2800 storage controllers on the bottom. The SG6060 uses E2800A controllers, and the SG6060X uses E2800B controllers.

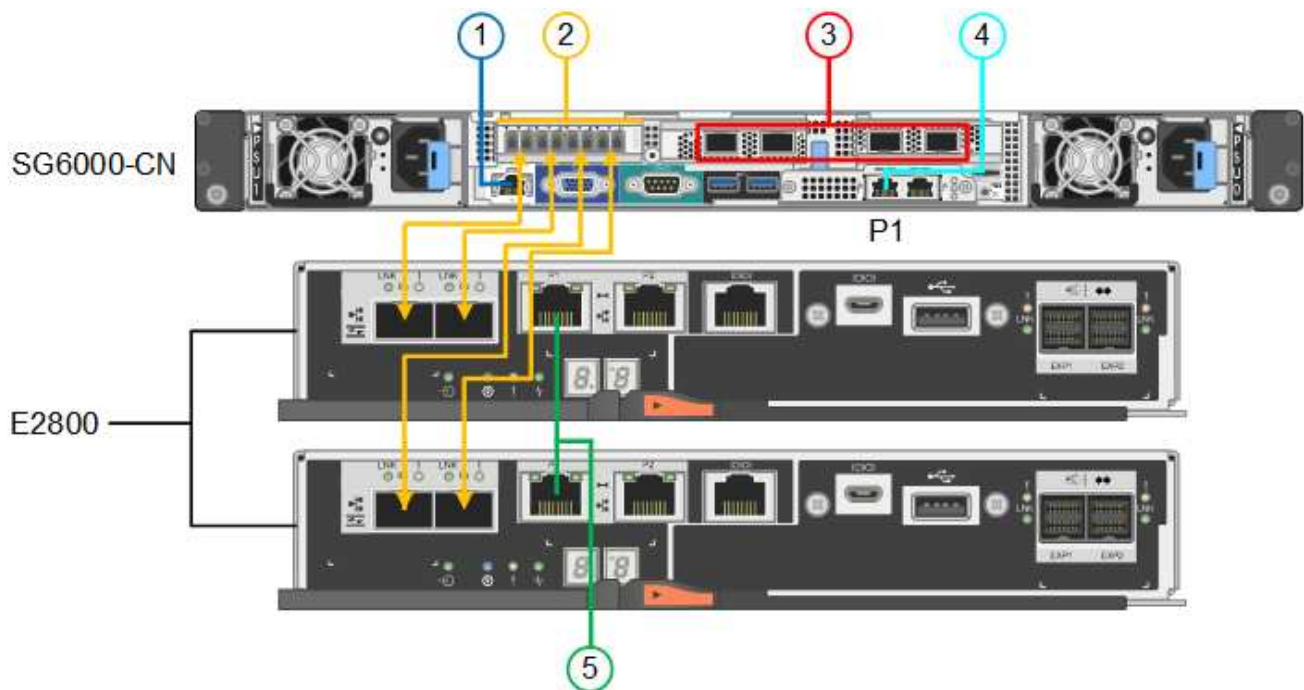


Both versions of the E2800 controller have identical specifications and function except for the location of the interconnect ports.

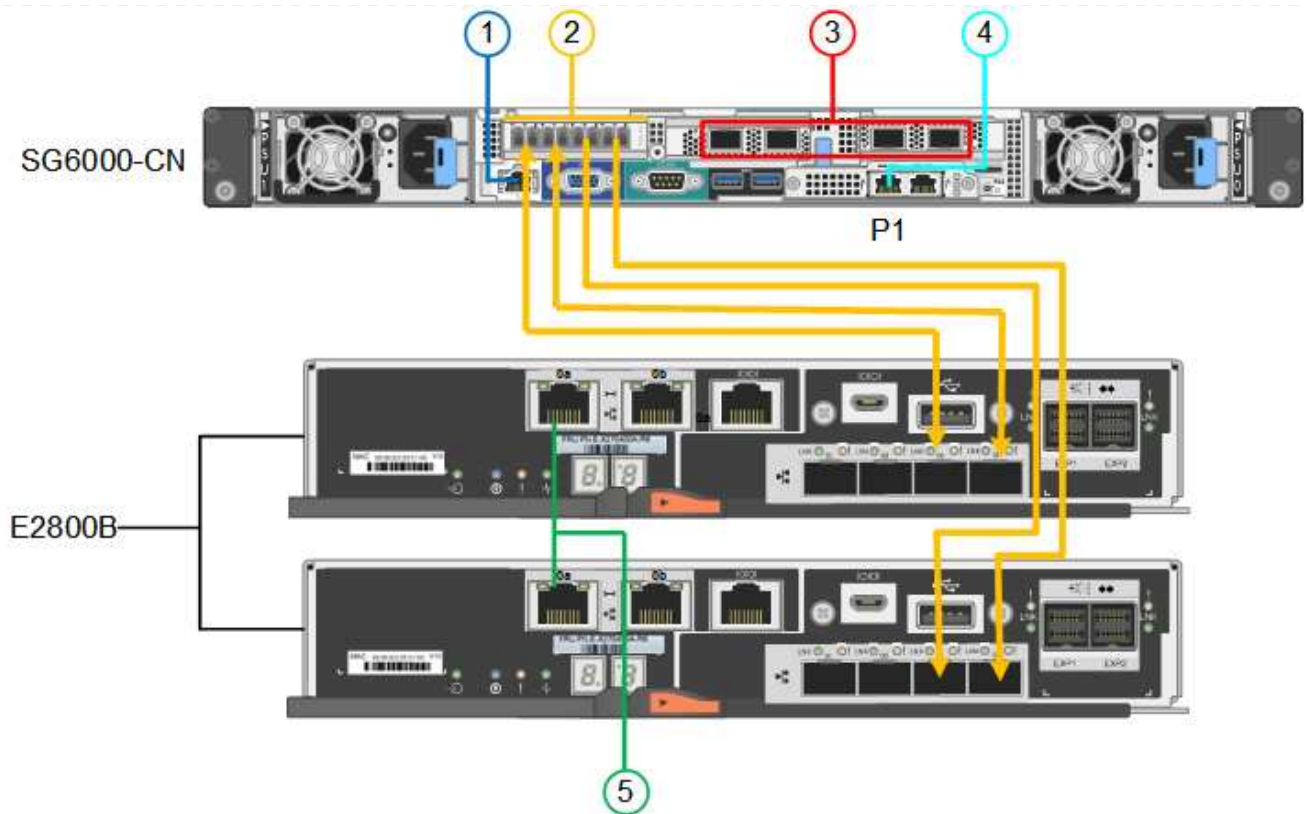


Don't use an E2800A and E2800B controller in the same appliance.

SG6060 connections:

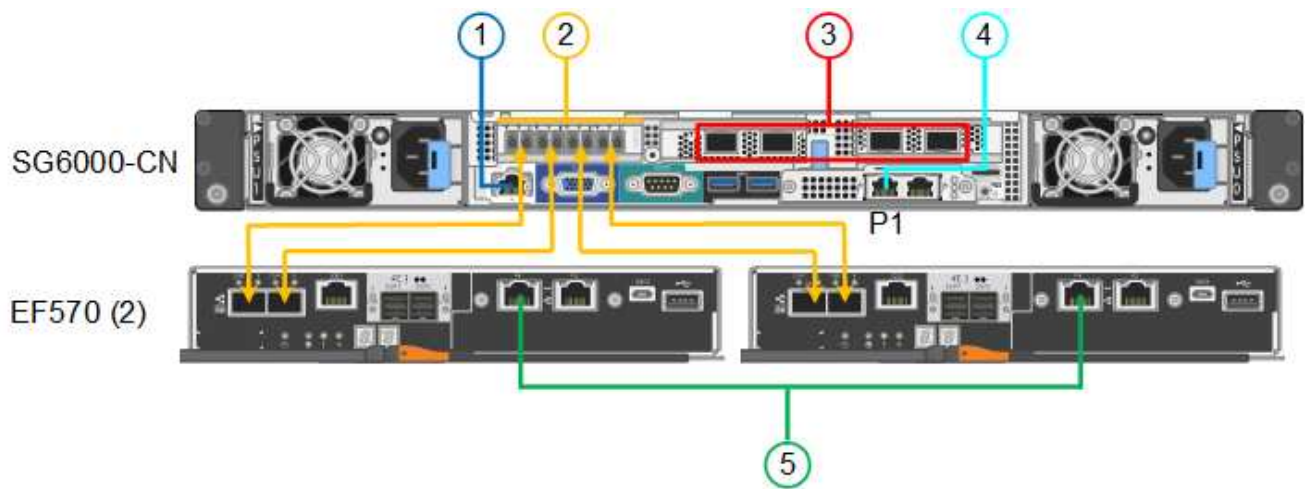


SG6060X connections:



The following figure shows the three controllers in the SGF6024 appliance, with the SG6000-CN compute controller on the top and the two EF570 storage controllers side by side below the compute controller.

SGF6024 connections:



Callout	Port	Type of port	Use
1	BMC management port on the SG6000-CN controller	1-GbE (RJ-45)	Connects to the network where you access the BMC interface.



Callout	Port	Type of port	Use
2	FC connection ports: <ul style="list-style-type: none"> <li>• 4 on the SG6000-CN controller</li> <li>• 2 on each storage controller</li> </ul>	16-Gb/s FC optical SFP+	Connect each storage controller to the SG6000-CN controller.
3	Four network ports on the SG6000-CN controller	10/25-GbE	Connect to the Grid Network and the Client Network for StorageGRID. See <a href="#">Port bond modes (SG6000-CN controller)</a> .
4	Admin Network port on the SG6000-CN controller (labeled P1 in the figure)	1-GbE (RJ-45) <b>Important:</b> This port operates only at 1000 baseT/full and does not support 10- or 100-megabit speeds.	Connects the SG6000-CN controller to the Admin Network for StorageGRID.
	Rightmost RJ-45 port on the SG6000-CN controller	1-GbE (RJ-45) <b>Important:</b> This port operates only at 1000 baseT/full and does not support 10- or 100-megabit speeds.	<ul style="list-style-type: none"> <li>• Can be bonded with management port 1 if you want a redundant connection to the Admin Network.</li> <li>• Can be left unwired and available for temporary local access (IP 169.254.0.1).</li> <li>• During installation, can be used to connect the SG6000-CN controller to a service laptop if DHCP-assigned IP addresses aren't available.</li> </ul>
5	Management port 1 on each storage controller	1-GbE (RJ-45)	Connects to the network where you access SANtricity System Manager.
	Management port 2 on each storage controller	1-GbE (RJ-45)	Reserved for technical support.

### Steps

1. Connect the BMC management port on the SG6000-CN controller to the management network, using an Ethernet cable.

Although this connection is optional, it is recommended to facilitate support.

2. Connect the two FC ports on each storage controller to the FC ports on the SG6000-CN controller, using four optical cables and four SFP+ transceivers for the storage controllers.
3. Connect the network ports on the SG6000-CN controller to the appropriate network switches, using TwinAx cables or optical cables and SFP+ or SFP28 transceivers.



Install SFP+ transceivers if you plan to use 10-GbE link speeds. Install SFP28 transceivers if you plan to use 25-GbE link speeds.

- On models that support Autonegotiate as a port speed option, if Fixed port bonding mode is selected you can run the ports dedicated to the StorageGRID Grid network at a different speed than the ports dedicated to the Client network.
- On models that do not support Autonegotiate as a port speed option, all four network ports must use the same link speed.
- If you plan to use Fixed port bond mode (default), connect the ports to the StorageGRID Grid and Client Networks, as shown in the table.

Port	Connects to...
Port 1	Client Network (optional)
Port 2	Grid Network
Port 3	Client Network (optional)
Port 4	Grid Network

- If you plan to use the Aggregate port bond mode, connect one or more of the network ports to one or more switches. You should connect at least two of the four ports to avoid having a single point of failure. If you use more than one switch for a single LACP bond, the switches must support MLAG or equivalent.
4. If you plan to use the Admin Network for StorageGRID, connect the Admin Network port on the SG6000-CN controller to the Admin Network, using an Ethernet cable.
  5. If you plan to use the management network for SANtricity System Manager, connect management port 1 (P1) on each storage controller (the RJ-45 port on the left) to the management network for SANtricity System Manager, using an Ethernet cable.

Don't use management port 2 (P2) on the storage controllers (the RJ-45 port on the right). This port is reserved for technical support.

### SG6100

You connect the management port on the appliance to the service laptop and connect the network ports on the appliance to the Grid Network and optional Client Network for StorageGRID.

#### Before you begin

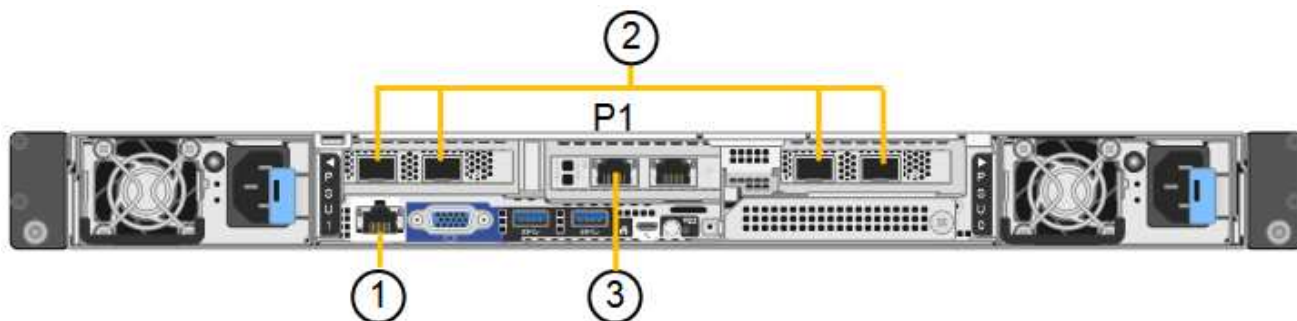
- You have an RJ-45 Ethernet cable for connecting the management port.
- You have one of the following options for the network ports. These items aren't provided with the appliance.
  - One to four TwinAx cables for connecting the four network ports.
  - One to four SFP+ or SFP28 transceivers if you plan to use optical cables for the ports.



**Risk of exposure to laser radiation** — Don't disassemble or remove any part of an SFP transceiver. You might be exposed to laser radiation.

## About this task

The following figures show the ports on the back of the SGF6112.



Callout	Port	Type of port	Use
1	BMC management port on the appliance	1-GbE (RJ-45)	Connects to the network where you access the BMC interface.
2	Four 10/25-GbE network ports on the appliance		Connect to the Grid Network and the Client Network for StorageGRID. See <a href="#">Port bond modes (SGF6112)</a>
3	Admin Network port on the appliance (labeled P1 in the figure)	1-GbE (RJ-45) <b>Important:</b> This port operates only at 1/10-GbE (RJ-45) and does not support 100-megabit speeds.	Connects the appliance to the Admin Network for StorageGRID.
	Rightmost RJ-45 port on the appliance	1-GbE (RJ-45) <b>Important:</b> This port operates only at 1/10-GbE (RJ-45) and does not support 100-megabit speeds.	<ul style="list-style-type: none"><li>• Can be bonded with management port 1 if you want a redundant connection to the Admin Network.</li><li>• Can be left disconnected and available for temporary local access (IP 169.254.0.1).</li><li>• During installation, can be used to connect the appliance to a service laptop if DHCP-assigned IP addresses aren't available.</li></ul>

## Steps

1. Connect the BMC management port on the appliance to the management network, using an Ethernet cable.

Although this connection is optional, it is recommended to facilitate support.

2. Connect the network ports on the appliance to the appropriate network switches, using TwinAx cables or optical cables and transceivers.

SGF6112 link speed (GbE)	Required equipment
10	SFP+ transceiver
25	SFP28 transceiver

- On models that support Autonegotiate as a port speed option, if Fixed port bonding mode is selected you can run the ports dedicated to the StorageGRID Grid network at a different speed than the ports dedicated to the Client network.
- On models that do not support Autonegotiate as a port speed option, all four network ports must use the same link speed.
- If you plan to use Fixed port bond mode (default), connect the ports to the StorageGRID Grid and Client Networks, as shown in the table.

Port	Connects to...
Port 1	Client Network (optional)
Port 2	Grid Network
Port 3	Client Network (optional)
Port 4	Grid Network

- If you plan to use the Aggregate port bond mode, connect one or more of the network ports to one or more switches. You should connect at least two of the four ports to avoid having a single point of failure. If you use more than one switch for a single LACP bond, the switches must support MLAG or equivalent.
3. If you plan to use the Admin Network for StorageGRID, connect the Admin Network port on the appliance to the Admin Network, using an Ethernet cable.

## Connect power cords and apply power

After connecting the network cables, you are ready to apply power to an appliance, controller, or expansion shelf.

## SG100 and SG1000

### Steps

1. Connect a power cord to each of the two power supply units in the appliance.
2. Connect these two power cords to two different power distribution units (PDUs) in the cabinet or rack.
3. If the power button on the front of the appliance is not currently illuminated blue, press the button to turn on power to the appliance.

Don't press the power button again during the power-on process.

4. If errors occur, correct any issues.
5. Attach the front bezel to the appliance if removed.

## SG5700

### Before you begin

Both appliance power switches must be off before connecting power.



**Risk of electrical shock** — Before connecting the power cords, make sure that the two power switches on the appliance are off.

### Steps

1. Confirm that the two power switches on the appliance are off.
2. Connect the two power cords to the appliance.
3. Connect the two power cords to different power distribution units (PDUs) in the cabinet or rack.
4. Turn on the two power switches on the appliance.
  - Don't turn off the power switches during the power-on process.
  - The fans are very loud when they first start up. The loud noise during start-up is normal.
5. After the controllers have booted up, check their seven-segment displays.

## SG6000

### Steps

1. Confirm that both controllers in the storage controller shelf are off.



**Risk of electrical shock** — Before connecting the power cords, make sure that the power switches for each of the two storage controllers are off.

2. If you have expansion shelves, confirm that both of the IOM power switches are off.



**Risk of electrical shock** — Before connecting the power cords, make sure that the two power switches for each of the expansion shelves are off.

3. Connect a power cord to each of the two power supply units in the SG6000-CN controller.
4. Connect these two power cords to two different power distribution units (PDUs) in the cabinet or rack.
5. Connect a power cord to each of the two power supply units in the storage controller shelf.
6. If you have expansion shelves, connect a power cord to each of the two power supply units in each expansion shelf.

7. Connect the two power cords in each storage shelf (including the optional expansion shelves) to two different PDUs in the cabinet or rack.
8. If the power button on the front of the SG6000-CN controller is not currently illuminated blue, press the button to turn on power to the controller.

Don't press the power button again during the power-on process.

9. Turn on the two power switches on the back of the storage controller shelf. If you have expansion shelves, turn on the two power switches for each shelf.
  - Don't turn off the power switches during the power-on process.
  - The fans in the storage controller shelf and optional expansion shelves might be very loud when they first start up. The loud noise during start-up is normal.
10. After the components have booted up, check their status.
  - Check the seven-segment display on the back of each storage controller. Refer to the article about viewing boot-up status codes for more information.
  - Verify that the power button on the front of the SG6000-CN controller is lit.
11. If errors occur, correct any issues.
12. Attach the front bezel to the SG6000-CN controller if removed.

## **SG6100**

### **Steps**

1. Connect a power cord to each of the two power supply units in the appliance.
2. Connect these two power cords to two different power distribution units (PDUs) in the cabinet or rack.
3. If the power button on the front of the SG6100-CN appliance is not currently illuminated blue, press the button to turn on power to the appliance.

Don't press the power button again during the power-on process.

The LED on the power supply should be illuminated green without blinking.

4. If errors occur, correct any issues.
5. Attach the front bezel to the appliance if removed.

### **Related information**

[View status indicators](#)

## **View status indicators and codes**

The appliances and controllers include indicators that help you determine the status of the appliance components.

## SG100 and SG1000

The appliance includes indicators that help you determine the status of the appliance controller and the two SSDs:

- [Appliance indicators and buttons](#)
- [General boot-up codes](#)
- [SSD indicators](#)

Use this information to help [troubleshoot SG100 and SG1000 hardware installation](#).

### Appliance indicators and buttons

The following figure shows status indicators and buttons on the SG100 and SG1000.



Callout	Display	State
1	Power button	<ul style="list-style-type: none"><li>• Blue: the appliance is powered on.</li><li>• Off: the appliance is powered off.</li></ul>
2	Reset button	Use this button to perform a hard reset of the controller.
3	Identify button	This button can be set to Blink, On (Solid), or Off. <ul style="list-style-type: none"><li>• Blue, blinking: Identifies the appliance in the cabinet or rack.</li><li>• Blue, solid: Identifies the appliance in the cabinet or rack.</li><li>• Off: The appliance is not visually identifiable in the cabinet or rack.</li></ul>
4	Alarm LED	<ul style="list-style-type: none"><li>• Amber, solid: An error has occurred.</li></ul> <p><b>Note:</b> To view the boot-up and error codes, <a href="#">access the BMC interface</a>.</p> <ul style="list-style-type: none"><li>• Off: No errors are present.</li></ul>

### General boot-up codes

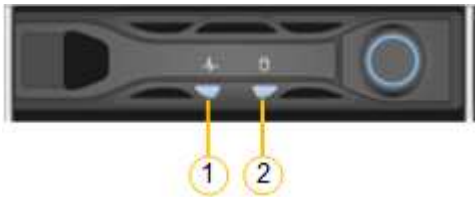
During boot-up or after a hard reset of the appliance, the following occurs:

1. The baseboard management controller (BMC) logs codes for the boot-up sequence, including any errors that occur.
2. The power button lights up.
3. If any errors occur during boot-up, the alarm LED lights up.

To view the boot-up and error codes, [access the BMC interface](#).

### SSD indicators

The following figure shows SSD indicators on the SG100 and SG1000.



LED	Display	State
1	Drive status/fault	<ul style="list-style-type: none"> <li>• Blue (solid): drive is online</li> <li>• Amber (solid): drive failure</li> <li>• Amber (blinking): drive locator light on</li> <li>• Off: slot is empty</li> </ul>
2	Drive active	Blue (blinking): drive is being accessed

### SG5700

The appliance controllers include indicators that help you determine the status of the appliance controller:

- [SG5700 boot-up status codes](#)
- [Status indicators on E5700SG controller](#)
- [General boot-up codes](#)
- [E5700SG controller boot-up codes](#)
- [E5700SG controller error codes](#)

Use this information to help [troubleshoot SG5700 hardware installation](#).

### SG5700 boot-up status codes

The seven-segment displays on each controller show status and error codes as the appliance powers up.

The E2800 controller and the E5700SG controller display different statuses and error codes.

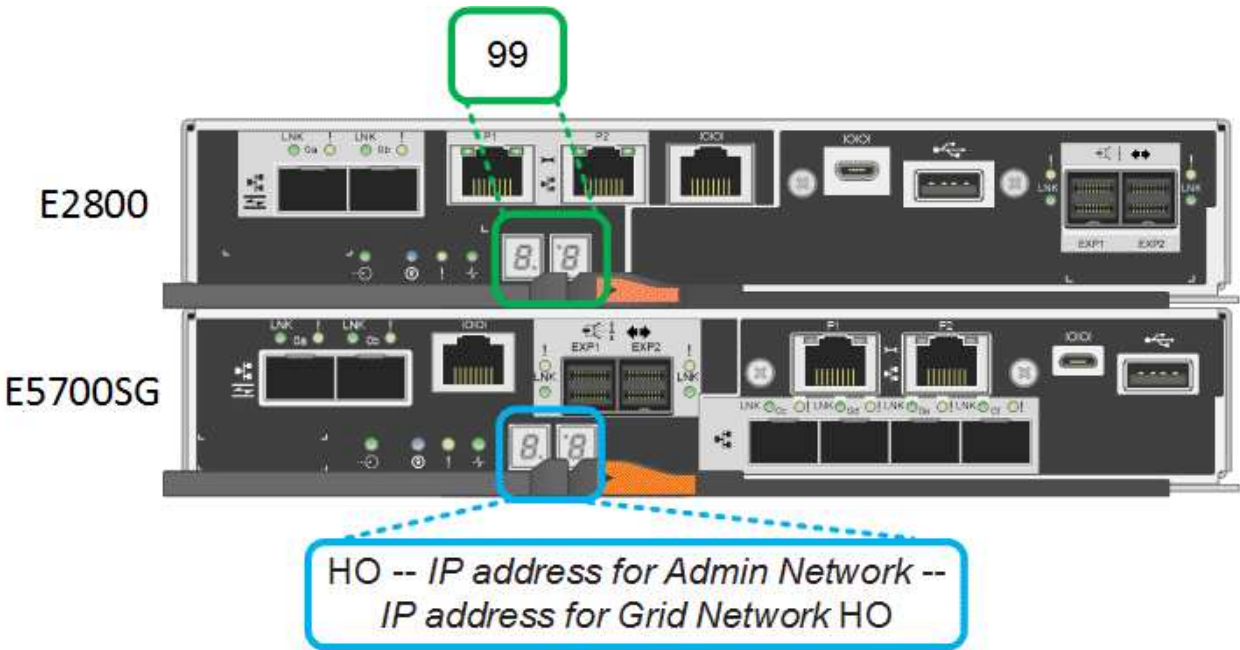
To understand what these codes mean, see the following resources:



Controller	Reference
E2800 controller	<i>E5700 and E2800 System Monitoring Guide</i>  <b>Note:</b> The codes listed for the E-Series E5700 controller don't apply to the E5700SG controller in the appliance.
E5700SG controller	"Status indicators on the E5700SG controller"

**Steps**

- During boot-up, monitor progress by viewing the codes shown on the seven-segment displays.
  - The seven-segment display on the E2800 controller shows the repeating sequence **OS**, **Sd**, **blank** to indicate that it is performing start-of-day processing.
  - The seven-segment display on the E5700SG controller shows a sequence of codes, ending with **AA** and **FF**.
- After the controllers have booted up, confirm the seven-segment displays show the following:



Controller	Seven-segment display
E2800 controller	Shows 99, which is the default ID for an E-Series controller shelf.

Controller	Seven-segment display
E5700SG controller	<p>Shows <b>HO</b>, followed by a repeating sequence of two numbers.</p> <div style="border: 1px solid gray; padding: 10px; margin: 10px 0;"> <pre>HO -- IP address for Admin Network -- IP address for Grid Network HO</pre> </div> <p>In the sequence, the first set of numbers is the DHCP-assigned IP address for the controller's management port 1. This address is used to connect the controller to the Admin Network for StorageGRID. The second set of numbers is the DHCP-assigned IP address used to connect the appliance to the Grid Network for StorageGRID.</p> <p><b>Note:</b> If an IP address could not be assigned using DHCP, 0.0.0.0 is displayed.</p>

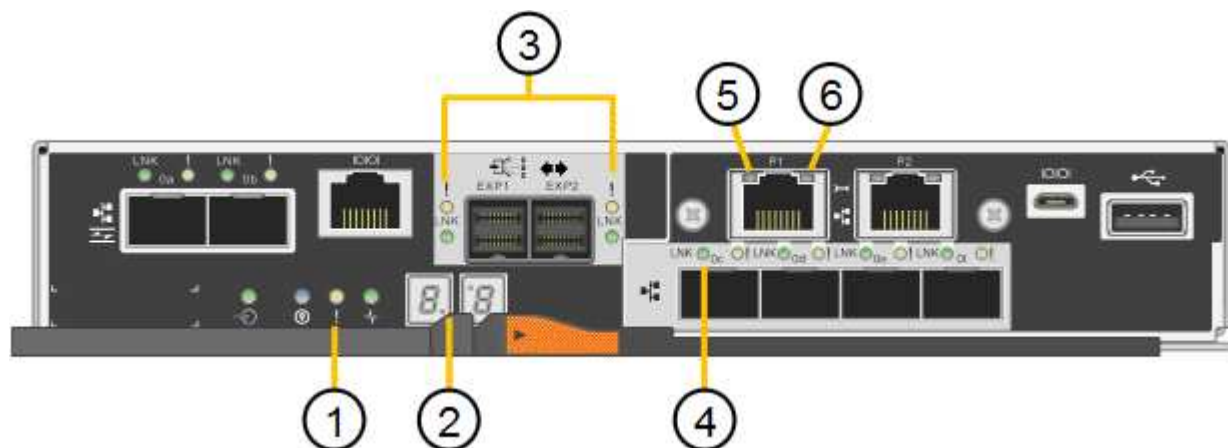
- If the seven-segment displays show other values, see [Troubleshoot hardware installation \(SG6000 or SG5700\)](#) and confirm you completed the installation steps correctly. If you are unable to resolve the problem, contact technical support.

### Status indicators on E5700SG controller

The seven-segment display and the LEDs on the E5700SG controller show status and error codes while the appliance powers up and while the hardware is initializing. You can use these displays to determine status and troubleshoot errors.

After the StorageGRID Appliance Installer has started, you should periodically review the status indicators on the E5700SG controller.

The following figure shows status indicators on the E5700SG controller.



Callout	Display	Description
1	Attention LED	Amber: The controller is faulty and requires operator attention, or the installation script was not found.  Off: The controller is operating normally.
2	Seven-segment display	Shows a diagnostic code  Seven-segment display sequences enable you to understand errors and the operational state of the appliance.
3	Expansion Port Attention LEDs	Amber: These LEDs are always amber (no link established) because the appliance does not use the expansion ports.
4	Host Port Link Status LEDs	Green: The link is up.  Off: The link is down.
5	Ethernet Link State LEDs	Green: A link is established.  Off: No link is established.
6	Ethernet Activity LEDs	Green: The link between the management port and the device to which it is connected (such as an Ethernet switch) is up.  Off: There is no link between the controller and the connected device.  Blinking Green: There is Ethernet activity.

### General boot-up codes

During boot-up or after a hard reset of the appliance, the following occurs:

1. The seven-segment display on the E5700SG controller shows a general sequence of codes that is not specific to the controller. The general sequence ends with the codes AA and FF.
2. Boot-up codes that are specific to the E5700SG controller appear.

### E5700SG controller boot-up codes

During a normal boot-up of the appliance, the seven-segment display on the E5700SG controller shows the following codes in the order listed:

Code	Indicates
HI	The master boot script has started.
PP	The system is checking to see if the FPGA needs to be updated.
HP	The system is checking to see if the 10/25-GbE controller firmware needs to be updated.
RB	The system is rebooting after applying firmware updates.
FP	The hardware subsystem firmware update checks have been completed. Inter-controller communication services are starting.
HE	The system is awaiting connectivity with the E2800 controller and synchronizing with the SANtricity operating system.  <b>Note:</b> If this boot procedure does not progress past this stage, check the connections between the two controllers.
HC	The system is checking for existing StorageGRID installation data.
HO	The StorageGRID Appliance Installer is running.
HA	StorageGRID is running.

### E5700SG controller error codes

These codes represent error conditions that might be shown on the E5700SG controller as the appliance boots up. Additional two-digit hexadecimal codes are displayed if specific low-level hardware errors occur. If any of these codes persists for more than a second or two, or if you are unable to resolve the error by following one of the prescribed troubleshooting procedures, contact technical support.

Code	Indicates
22	No master boot record found on any boot device.
23	The internal flash disk is not connected.
2A, 2B	Stuck bus, unable to read DIMM SPD data.
40	Invalid DIMMs.
41	Invalid DIMMs.
42	Memory test failed.

Code	Indicates
51	SPD reading failure.
92 to 96	PCI bus initialization.
A0 to A3	SATA drive initialization.
AB	Alternate boot code.
AE	Booting OS.
EA	DDR4 training failed.
E8	No memory installed.
EU	The installation script was not found.
EP	Installation or communication with the E2800 controller has failed.

#### Related information

- [NetApp Support](#)
- [E5700 and E2800 System Monitoring Guide](#)

#### SG6000

The SG6000 appliance controllers include indicators that help you determine the status of the appliance controller:

- [Status indicators and buttons on SG6000-CN controller](#)
- [General boot-up codes](#)
- [Boot-up status codes for SG6000 storage controllers](#)

Use this information to help [troubleshoot SG6000 installation](#).

#### Status indicators and buttons on SG6000-CN controller

The SG6000-CN controller includes indicators that help you determine the status of the controller, including the following indicators and buttons.

The following figure shows status indicators and buttons on the SG6000-CN controller.



Callout	Display	Description
1	Power button	<ul style="list-style-type: none"> <li>• Blue: The controller is powered on.</li> <li>• Off: The controller is powered off.</li> </ul>
2	Reset button	<p><i>No indicator</i></p> <p>Use this button to perform a hard reset of the controller.</p>
3	Identify button	<ul style="list-style-type: none"> <li>• Blinking or solid blue: Identifies the controller in the cabinet or rack.</li> <li>• Off: The controller is not visually identifiable in the cabinet or rack.</li> </ul> <p>This button can be set to Blink, On (Solid), or Off.</p>
4	Alarm LED	<ul style="list-style-type: none"> <li>• Amber: An error has occurred.</li> </ul> <p><b>Note:</b> To view the boot-up and error codes, <a href="#">access the BMC interface</a>.</p> <ul style="list-style-type: none"> <li>• Off: No errors are present.</li> </ul>

### General boot-up codes

During boot-up or after a hard reset of the SG6000-CN controller, the following occurs:

1. The baseboard management controller (BMC) logs codes for the boot-up sequence, including any errors that occur.
2. The power button lights up.
3. If any errors occur during boot-up, the alarm LED lights up.

To view the boot-up and error codes, [access the BMC interface](#).

### Boot-up status codes for SG6000 storage controllers

Each storage controller has a seven-segment display that provides status codes as the controller powers up. The status codes are the same for both the E2800 controller and the EF570 controller.

For descriptions of these codes, see the E-Series system monitoring information for your storage controller type.

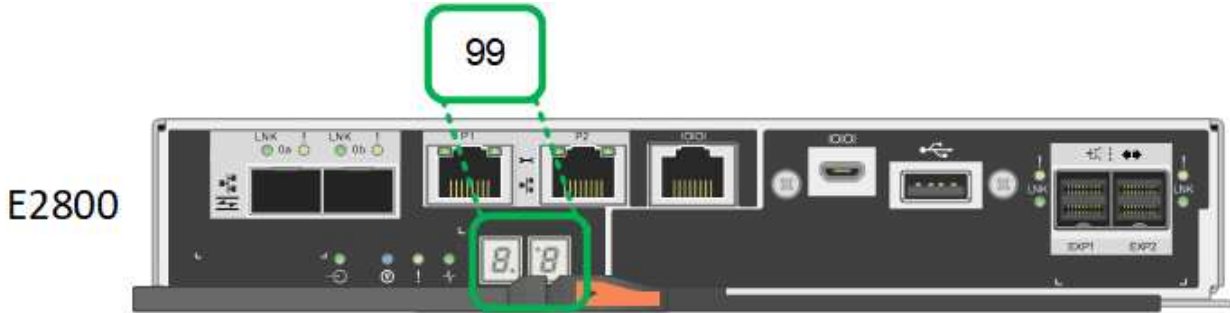
### Steps

1. During boot-up, monitor progress by viewing the codes shown on the seven-segment display for each storage controller.

The seven-segment display on each storage controller shows the repeating sequence **OS**, **Sd**, **blank** to indicate that the controller is performing start-of-day processing.

2. After the controllers have booted up, confirm that each storage controller shows 99, which is the default ID for an E-Series controller shelf.

Make sure this value is displayed on both storage controllers, as shown in this example E2800 controller.



3. If one or both controllers show other values, see [Troubleshoot hardware installation \(SG6000 or SG5700\)](#) and confirm you completed the installation steps correctly. If you are unable to resolve the problem, contact technical support.

#### Related information

- [NetApp Support](#)
- [Power on SG6000-CN controller and verify operation](#)

#### SG6100

The appliance includes indicators that help you determine the status of the appliance controller and the SSDs:

- [Appliance indicators and buttons](#)
- [General boot-up codes](#)
- [SSD indicators](#)

Use this information to help [troubleshoot SG6100 hardware installation](#).

#### Appliance indicators and buttons

The following figure shows indicators and buttons on the SGF6112 appliance.



Callout	Display	State
1	Power button	<ul style="list-style-type: none"> <li>• Blue: the appliance is powered on.</li> <li>• Off: the appliance is powered off.</li> </ul>
2	Reset button	Use this button to perform a hard reset of the controller.

Callout	Display	State
3	Identify button	<p>Using the BMC, this button can be set to blink, On (Solid), or Off.</p> <ul style="list-style-type: none"> <li>• Blue, blinking: Identifies the appliance in the cabinet or rack.</li> <li>• Blue, solid: Identifies the appliance in the cabinet or rack.</li> <li>• Off: The appliance is not visually identifiable in the cabinet or rack.</li> </ul>
4	Status LED	<ul style="list-style-type: none"> <li>• Amber, solid: An error has occurred.</li> </ul> <p><b>Note:</b> To view the boot-up and error codes, <a href="#">access the BMC interface</a>.</p> <ul style="list-style-type: none"> <li>• Off: No errors are present.</li> </ul>
5	PFR	This light is not used by the SGF6112 appliance and remains off.

### General boot-up codes

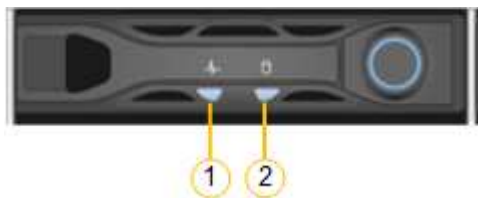
During boot-up or after a hard reset of the appliance, the following occurs:

1. The baseboard management controller (BMC) logs codes for the boot-up sequence, including any errors that occur.
2. The power button lights up.
3. If any errors occur during boot-up, the alarm LED lights up.

To view the boot-up and error codes, [access the BMC interface](#).

### SSD indicators

The following figure shows SSD indicators on the SGF6112 appliance.





LED	Display	State
1	Drive status/fault	<ul style="list-style-type: none"> <li>• Blue (solid): drive is online</li> <li>• Amber (solid): drive failure</li> <li>• Off: slot is empty</li> </ul> <p><b>Note:</b> If a new working SSD is inserted into a working SGF6112 StorageGRID node, the LEDs on the SSD should blink initially, but stop blinking as soon as the system determines that the drive has enough capacity and is functional.</p>
2	Drive active	Blue (blinking): drive is being accessed

## 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:

- SG100
- SG1000
- SG6000

- SG6100

## Optional configuration

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

## 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.)

### SG100



### SG1000



### 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.

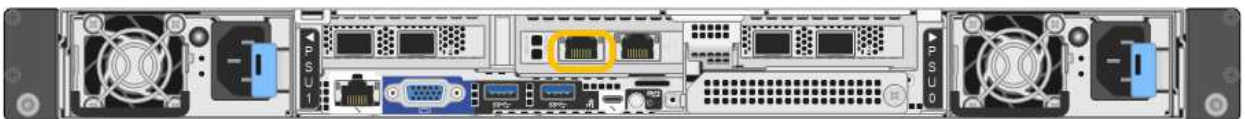


If an IP address could not be assigned using DHCP, 0.0.0.0 is displayed.

### SG6000-CN



### SGF6112



- Obtain the DHCP address for the appliance on the Admin Network from your network administrator.
- 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).

- c. 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.

## NetApp® StorageGRID® Appliance Installer

Home	Configure Networking ▾	Configure Hardware ▾	Monitor Installation	Advanced ▾
------	------------------------	----------------------	----------------------	------------

### Home

**i** The installation is ready to be started. Review the settings below, and then click Start Installation.

### This Node

Node type	Storage ▾
Node name	MM-2-108-SGA-lab25
	<input type="button" value="Cancel"/> <input type="button" value="Save"/>

### Primary Admin Node connection

Enable Admin Node discovery	<input type="checkbox"/>
Primary Admin Node IP	172.16.1.178
Connection state	Connection to 172.16.1.178 ready
	<input type="button" value="Cancel"/> <input type="button" value="Save"/>

### Installation

Current state	Ready to start installation of MM-2-108-SGA-lab25 into grid with Admin Node 172.16.1.178 running StorageGRID 11.2.0, using StorageGRID software downloaded from the Admin Node.
	<input type="button" value="Start Installation"/>

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

### 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.



### E5700SG

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



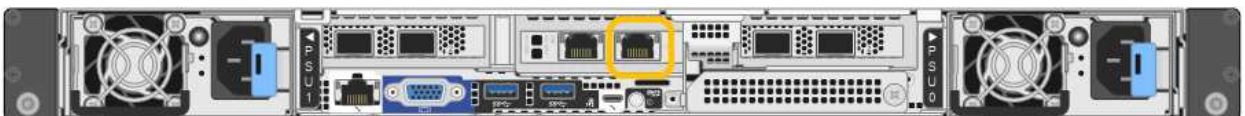
### SG6000-CN

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



### SGF6112

Connect a service laptop directly to the rightmost RJ-45 port on the 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.

**NetApp® StorageGRID® Appliance Installer**

Home | Configure Networking | Configure Hardware | Monitor Installation | Advanced

### Home

**This Node**

Node type: Gateway

Node name: xlr-10

Cancel Save

**Primary Admin Node connection**

Enable Admin Node discovery:

Primary Admin Node IP: 192.168.7.44

Connection state: Connection to 192.168.7.44 ready

Cancel Save

**Installation**

Current state: Ready to start installation of xlr-10 into grid with Admin Node 192.168.7.44 running StorageGRID 11.6.0, using StorageGRID software downloaded from the Admin Node.

Start installation

## 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 \(SG1000 and SG100\)](#)
- [Port bond modes \(E5700SG\)](#)
- [Port bond modes \(SG6000-CN\)](#)
- [Port bond modes \(SGF6112\)](#)

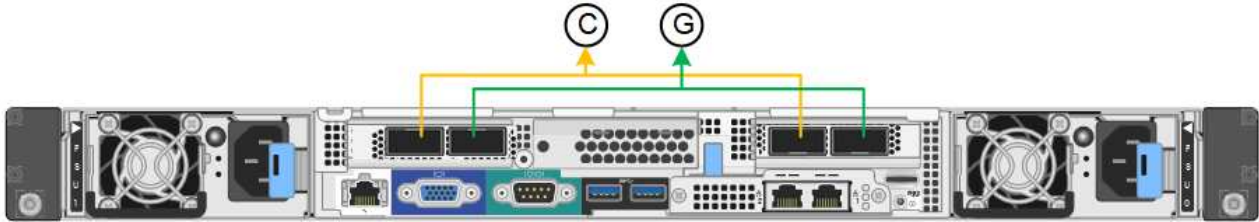


## SG100 and SG1000

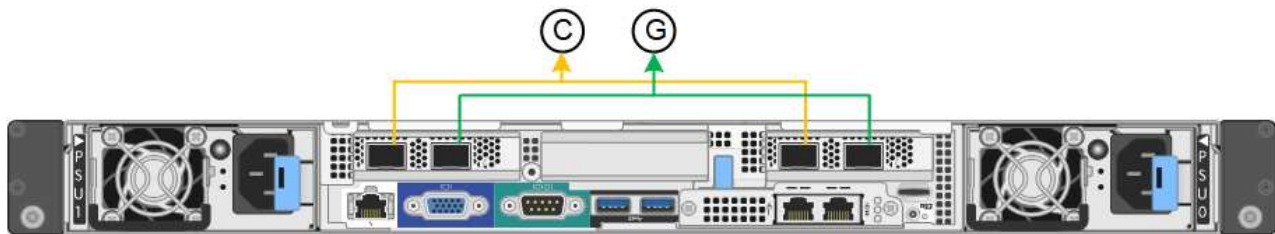
### Fixed port bond mode (default)

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.

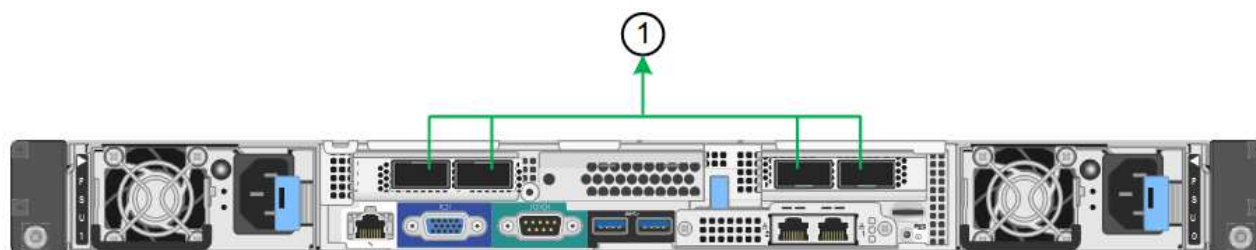
Network bond mode	Client Network disabled (default)	Client Network enabled
Active-Backup (default)	<ul style="list-style-type: none"> <li>Ports 2 and 4 use an active-backup bond for the Grid Network.</li> <li>Ports 1 and 3 aren't used.</li> <li>A VLAN tag is optional.</li> </ul>	<ul style="list-style-type: none"> <li>Ports 2 and 4 use an active-backup bond for the Grid Network.</li> <li>Ports 1 and 3 use an active-backup bond for the Client Network.</li> <li>VLAN tags can be specified for both networks for the convenience of the network administrator.</li> </ul>

Network bond mode	Client Network disabled (default)	Client Network enabled
LACP (802.3ad)	<ul style="list-style-type: none"> <li>Ports 2 and 4 use an LACP bond for the Grid Network.</li> <li>Ports 1 and 3 aren't used.</li> <li>A VLAN tag is optional.</li> </ul>	<ul style="list-style-type: none"> <li>Ports 2 and 4 use an LACP bond for the Grid Network.</li> <li>Ports 1 and 3 use an LACP bond for the Client Network.</li> <li>VLAN tags can be specified for both networks for the convenience of the network administrator.</li> </ul>

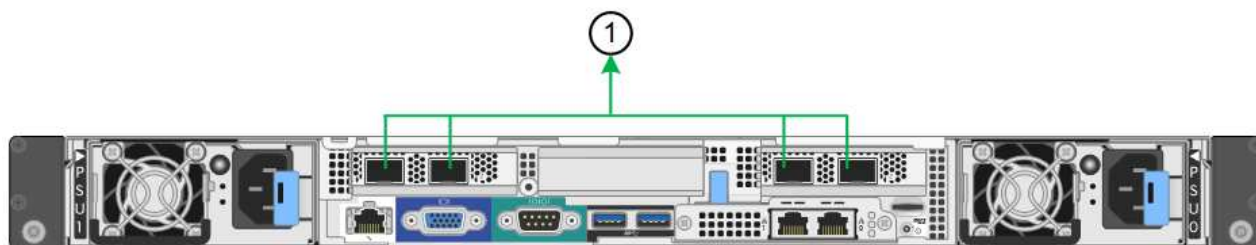
### Aggregate port bond mode

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.

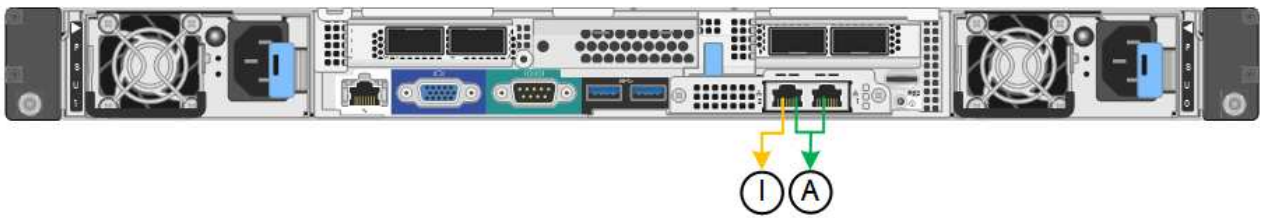
The table summarizes the options for configuring the four network ports. You only need to configure the settings on the Link Configuration page if you want to use a non-default setting.

Network bond mode	Client Network disabled (default)	Client Network enabled
LACP (802.3ad) only	<ul style="list-style-type: none"> <li>Ports 1-4 use a single LACP bond for the Grid Network.</li> <li>A single VLAN tag identifies Grid Network packets.</li> </ul>	<ul style="list-style-type: none"> <li>Ports 1-4 use a single LACP bond for the Grid Network and the Client Network.</li> <li>Two VLAN tags allow Grid Network packets to be segregated from Client Network packets.</li> </ul>

**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:



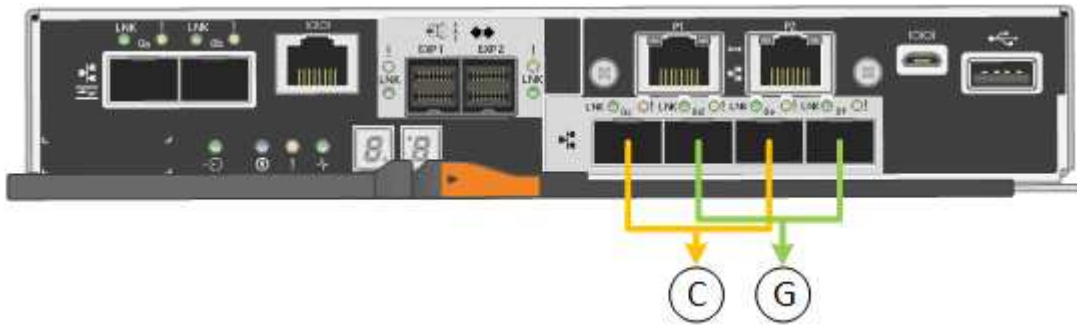
SG100:



**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).



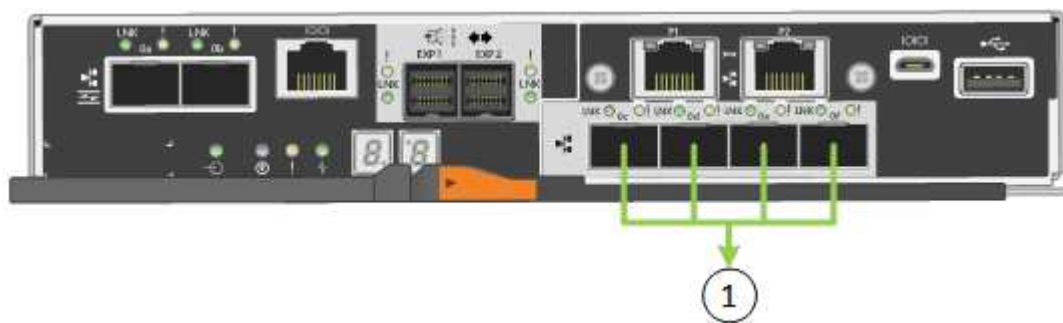
Callout	Which ports are bonded
C	Ports 1 and 3 are bonded together for the Client Network, if this network is used.
G	Ports 2 and 4 are bonded together for the Grid Network.

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)	<ul style="list-style-type: none"> <li>Ports 2 and 4 use an active-backup bond for the Grid Network.</li> <li>Ports 1 and 3 aren't used.</li> <li>A VLAN tag is optional.</li> </ul>	<ul style="list-style-type: none"> <li>Ports 2 and 4 use an active-backup bond for the Grid Network.</li> <li>Ports 1 and 3 use an active-backup bond for the Client Network.</li> <li>VLAN tags can be specified for both networks for the convenience of the network administrator.</li> </ul>
LACP (802.3ad)	<ul style="list-style-type: none"> <li>Ports 2 and 4 use an LACP bond for the Grid Network.</li> <li>Ports 1 and 3 aren't used.</li> <li>A VLAN tag is optional.</li> </ul>	<ul style="list-style-type: none"> <li>Ports 2 and 4 use an LACP bond for the Grid Network.</li> <li>Ports 1 and 3 use an LACP bond for the Client Network.</li> <li>VLAN tags can be specified for both networks for the convenience of the network administrator.</li> </ul>

### 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	<ul style="list-style-type: none"> <li>Ports 1-4 use a single LACP bond for the Grid Network.</li> <li>A single VLAN tag identifies Grid Network packets.</li> </ul>	<ul style="list-style-type: none"> <li>Ports 1-4 use a single LACP bond for the Grid Network and the Client Network.</li> <li>Two VLAN tags allow Grid Network packets to be segregated from Client Network packets.</li> </ul>

### Active-Backup network bond mode for management ports

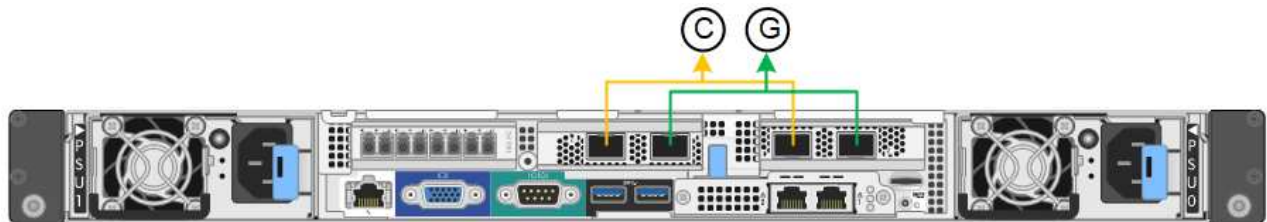
This figure shows how the two 1-GbE management ports on the E5700SG controller are bonded in Active-Backup network bond mode for the Admin Network.



### SG6000

#### Fixed port bond mode (default)

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



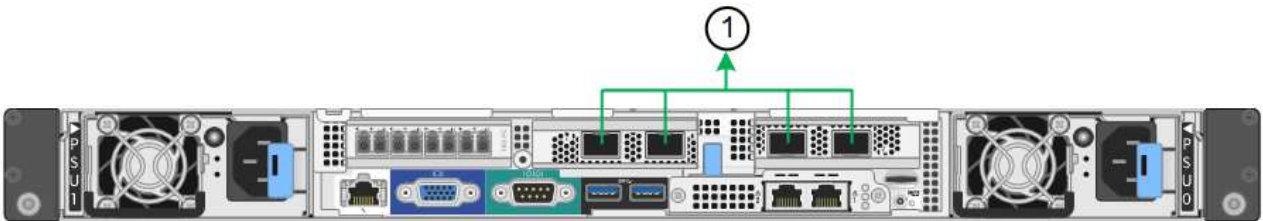
Callout	Which ports are bonded
C	Ports 1 and 3 are bonded together for the Client Network, if this network is used.
G	Ports 2 and 4 are bonded together for the Grid Network.

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)	<ul style="list-style-type: none"> <li>Ports 2 and 4 use an active-backup bond for the Grid Network.</li> <li>Ports 1 and 3 aren't used.</li> <li>A VLAN tag is optional.</li> </ul>	<ul style="list-style-type: none"> <li>Ports 2 and 4 use an active-backup bond for the Grid Network.</li> <li>Ports 1 and 3 use an active-backup bond for the Client Network.</li> <li>VLAN tags can be specified for both networks for the convenience of the network administrator.</li> </ul>
LACP (802.3ad)	<ul style="list-style-type: none"> <li>Ports 2 and 4 use an LACP bond for the Grid Network.</li> <li>Ports 1 and 3 aren't used.</li> <li>A VLAN tag is optional.</li> </ul>	<ul style="list-style-type: none"> <li>Ports 2 and 4 use an LACP bond for the Grid Network.</li> <li>Ports 1 and 3 use an LACP bond for the Client Network.</li> <li>VLAN tags can be specified for both networks for the convenience of the network administrator.</li> </ul>

### Aggregate port bond mode

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



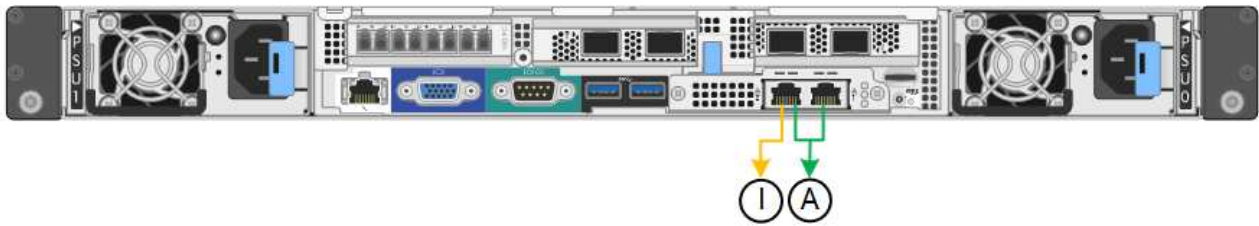
Callout	Which ports are bonded
1	All four ports are grouped in a single LACP bond, allowing all ports to be used for Grid Network and Client Network traffic.

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	<ul style="list-style-type: none"> <li>Ports 1-4 use a single LACP bond for the Grid Network.</li> <li>A single VLAN tag identifies Grid Network packets.</li> </ul>	<ul style="list-style-type: none"> <li>Ports 1-4 use a single LACP bond for the Grid Network and the Client Network.</li> <li>Two VLAN tags allow Grid Network packets to be segregated from Client Network packets.</li> </ul>

### Active-Backup network bond mode for management ports

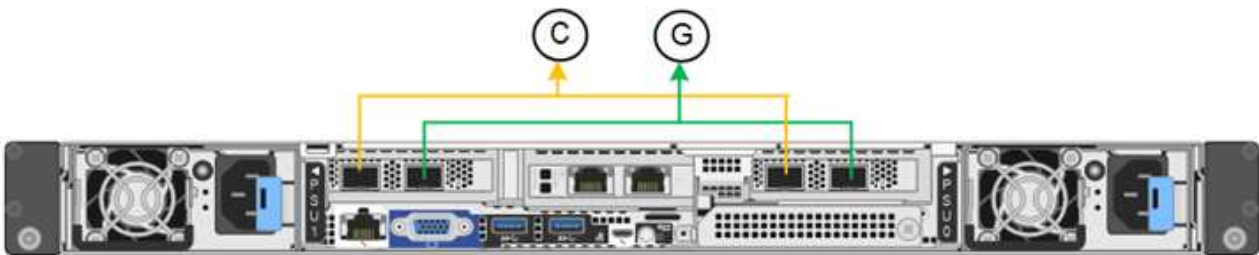
This figure shows how the two 1-GbE management ports on the SG6000-CN controller are bonded in Active-Backup network bond mode for the Admin Network.



### 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.

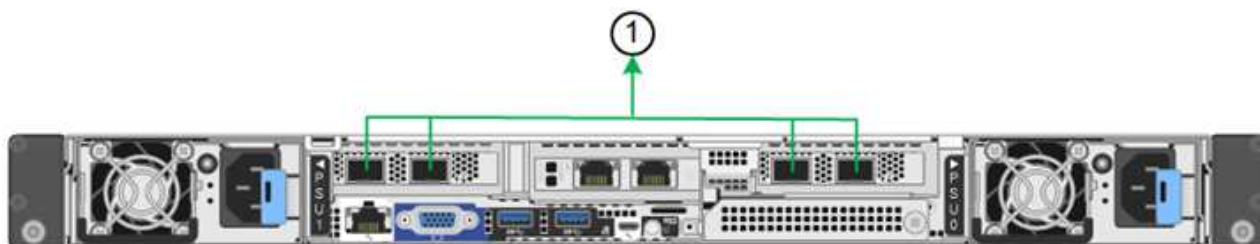
The table summarizes the options for configuring the network ports. You only need to configure the settings on the Link Configuration page if you want to use a non-default setting.

Network bond mode	Client Network disabled (default)	Client Network enabled
Active-Backup (default)	<ul style="list-style-type: none"> <li>Ports 2 and 4 use an active-backup bond for the Grid Network.</li> <li>Ports 1 and 3 aren't used.</li> <li>A VLAN tag is optional.</li> </ul>	<ul style="list-style-type: none"> <li>Ports 2 and 4 use an active-backup bond for the Grid Network.</li> <li>Ports 1 and 3 use an active-backup bond for the Client Network.</li> <li>VLAN tags can be specified for both networks for the convenience of the network administrator.</li> </ul>

Network bond mode	Client Network disabled (default)	Client Network enabled
LACP (802.3ad)	<ul style="list-style-type: none"> <li>Ports 2 and 4 use an LACP bond for the Grid Network.</li> <li>Ports 1 and 3 aren't used.</li> <li>A VLAN tag is optional.</li> </ul>	<ul style="list-style-type: none"> <li>Ports 2 and 4 use an LACP bond for the Grid Network.</li> <li>Ports 1 and 3 use an LACP bond for the Client Network.</li> <li>VLAN tags can be specified for both networks for the convenience of the network administrator.</li> </ul>

### 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.

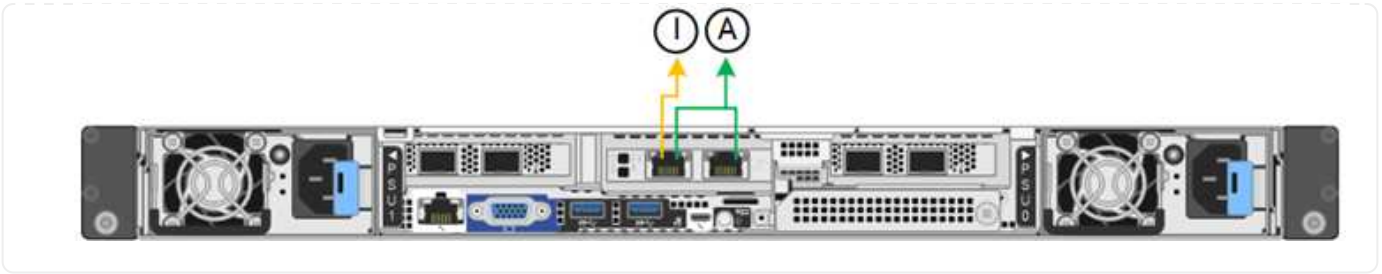
The table summarizes the options for configuring the network ports. You only need to configure the settings on the Link Configuration page if you want to use a non-default setting.

Network bond mode	Client Network disabled (default)	Client Network enabled
LACP (802.3ad) only	<ul style="list-style-type: none"> <li>Ports 1-4 use a single LACP bond for the Grid Network.</li> <li>A single VLAN tag identifies Grid Network packets.</li> </ul>	<ul style="list-style-type: none"> <li>Ports 1-4 use a single LACP bond for the Grid Network and the Client Network.</li> <li>Two VLAN tags allow Grid Network packets to be segregated from Client Network packets.</li> </ul>

### 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.





## 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 SG5700, select **25GbE** from the **Link speed** drop-down list.
  - For the SG6000, select **Auto** 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.

#### Link Settings

Link speed

Port bond mode  Fixed  **Aggregate**

Choose Fixed port bond mode if you want to use ports 2 and 4 for the Grid Network and ports 1 and 3 for the Client Network (if enabled). Choose Aggregate port bond mode if you want all connected ports to share a single LACP bond for both the Grid and Client Networks.

#### Grid Network

Enable network

Network bond mode  Active-Backup  **LACP (802.3ad)**

If the port bond mode is Aggregate, all bonds must be in LACP (802.3ad) mode.

Enable VLAN (802.1q) tagging

VLAN (802.1q) tag

MAC Addresses 50:6b:4b:42:d7:00 50:6b:4b:42:d7:01 50:6b:4b:42:d7:24 50:6b:4b:42:d7:25

If you are using DHCP, it is recommended that you configure a permanent DHCP reservation. Use all of these MAC addresses in the reservation to assign one IP address to this network interface.

#### Admin Network

Enable network

Network bond mode  Independent  **Active-Backup**

Connect the Admin Network to ports 5 and 6. If necessary, you can make a temporary direct Ethernet connection by disconnecting ports 5 and 6, then connecting to port 6 and using link-local IP address 169.254.0.1 for access.

MAC Addresses d8:c4:97:2a:e4:95

If you are using DHCP, it is recommended that you configure a permanent DHCP reservation. Use all of these MAC addresses in the reservation to assign one IP address to this network interface.

#### Client Network

Enable network

Network bond mode  Active-Backup  **LACP (802.3ad)**

If the port bond mode is Aggregate, all bonds must be in LACP (802.3ad) mode.

Enable VLAN (802.1q) tagging

VLAN (802.1q) tag

MAC Addresses 50:6b:4b:42:d7:00 50:6b:4b:42:d7:01 50:6b:4b:42:d7:24 50:6b:4b:42:d7:25

If you are using DHCP, it is recommended that you configure a permanent DHCP reservation. Use all of these MAC addresses in the reservation to assign one IP address to this network interface.

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 SG100 or SG1000 services appliance](#)
- [Change link configuration of the E5700SG controller](#)
- [Change link configuration of the SG6000-CN controller](#)
- [Change link configuration of the SG6100 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 **x**.

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 **x**.

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.

## Admin Network

The Admin Network is a closed network used for system administration and maintenance. The Admin Network is typically a private network and does not need to be routable between sites.

IP Assignment  Static  DHCP

IPv4 Address (CIDR)

Gateway

Subnets (CIDR)  **+**

MTU

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 **x**.

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 **x**.

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.

## Client Network

The Client Network is an open network used to provide access to client applications, including S3 and Swift. The Client Network enables grid nodes to communicate with any subnet reachable through the Client Network gateway. The Client Network does not become operational until you complete the StorageGRID configuration steps.

IP Assignment  Static  DHCP

IPv4 Address (CIDR)

Gateway

MTU

9. If you selected **Static**, follow these steps to configure the Client Network:

- Enter the static IPv4 address, using CIDR notation.
- Click **Save**.
- 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.

- 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.

- Click **Save**.

10. If you selected **DHCP**, follow these steps to configure the Client Network:

- 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.

### Ping and MTU Test

Use a ping request to check the appliance's connectivity to a remote host. Select the network you want to check connectivity through, and enter the IP address of the host you want to reach. To verify the MTU setting for the entire path through the network to the destination, select Test MTU.

#### Ping and MTU Test

Network	<input type="text" value="Grid"/>
Destination IPv4 Address or FQDN	<input type="text"/>
Test MTU	<input type="checkbox"/>
<input type="button" value="Test Connectivity"/>	

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.



- 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.

- Click **Test Connectivity**.

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

### Ping and MTU Test

Use a ping request to check the appliance's connectivity to a remote host. Select the network you want to check connectivity through, and enter the IP address of the host you want to reach. To verify the MTU setting for the entire path through the network to the destination, select Test MTU.

#### Ping and MTU Test

Network	Grid
Destination IPv4 Address or FQDN	10.96.104.223
Test MTU	<input checked="" type="checkbox"/>
<b>Test Connectivity</b>	

Ping test passed

#### Ping command output

```
PING 10.96.104.223 (10.96.104.223) 1472(1500) bytes of data.  
1480 bytes from 10.96.104.223: icmp_seq=1 ttl=64 time=0.318 ms  
  
--- 10.96.104.223 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.318/0.318/0.318/0.000 ms  
  
Found MTU 1500 for 10.96.104.223 via br0
```

#### 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 or later. 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.

**Port Connectivity Test**

---

Network	<input type="text" value="Grid"/>
IPv4 Address Ranges	<input type="text" value="10.224.6.160-161"/>
Port Ranges	<input type="text" value="22,2022"/>
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
<input type="button" value="Test Connectivity"/>	

---

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.

Port connectivity test passed

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Fri Nov 13 18:32:03 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,2022 10.224.6.160-161
Nmap scan report for 10.224.6.160
Host is up (0.00072s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
2022/tcp  open  down

Nmap scan report for 10.224.6.161
Host is up (0.00060s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
2022/tcp  open  down

# Nmap done at Fri Nov 13 18:32:04 2020 -- 2 IP addresses (2 hosts up) scanned in 0.55 seconds
```

- 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.

 Port connectivity test failed  
Connection not established. Services might not be listening on target ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:07:02 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,80,443,1504,1505,1506,1508,7443,9999
Nmap scan report for 172.16.4.71
Host is up (0.00020s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   open  https
1504/tcp  closed evb-elm
1505/tcp  open  funkproxy
1506/tcp  open  utcd
1508/tcp  open  diagmond
7443/tcp  open  oracleas-https
9999/tcp  open  abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:07:03 2020 -- 1 IP address (1 host up) scanned in 0.59 seconds
```

- 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.

❗ Port connectivity test failed  
Connection failed to one or more ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:11:01 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,79,80,443,1504,1505,1506,1508,7443,9999 172.16.4.71
Nmap scan report for 172.16.4.71
Host is up (0.00029s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
79/tcp    filtered finger
80/tcp    open  http
443/tcp   open  https
1504/tcp   closed evb-elm
1505/tcp   open  funkproxy
1506/tcp   open  utcd
1508/tcp   open  diagmond
7443/tcp   open  oracleas-https
9999/tcp   open  abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:11:02 2020 -- 1 IP address (1 host up) scanned in 1.60 seconds
```

## 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:

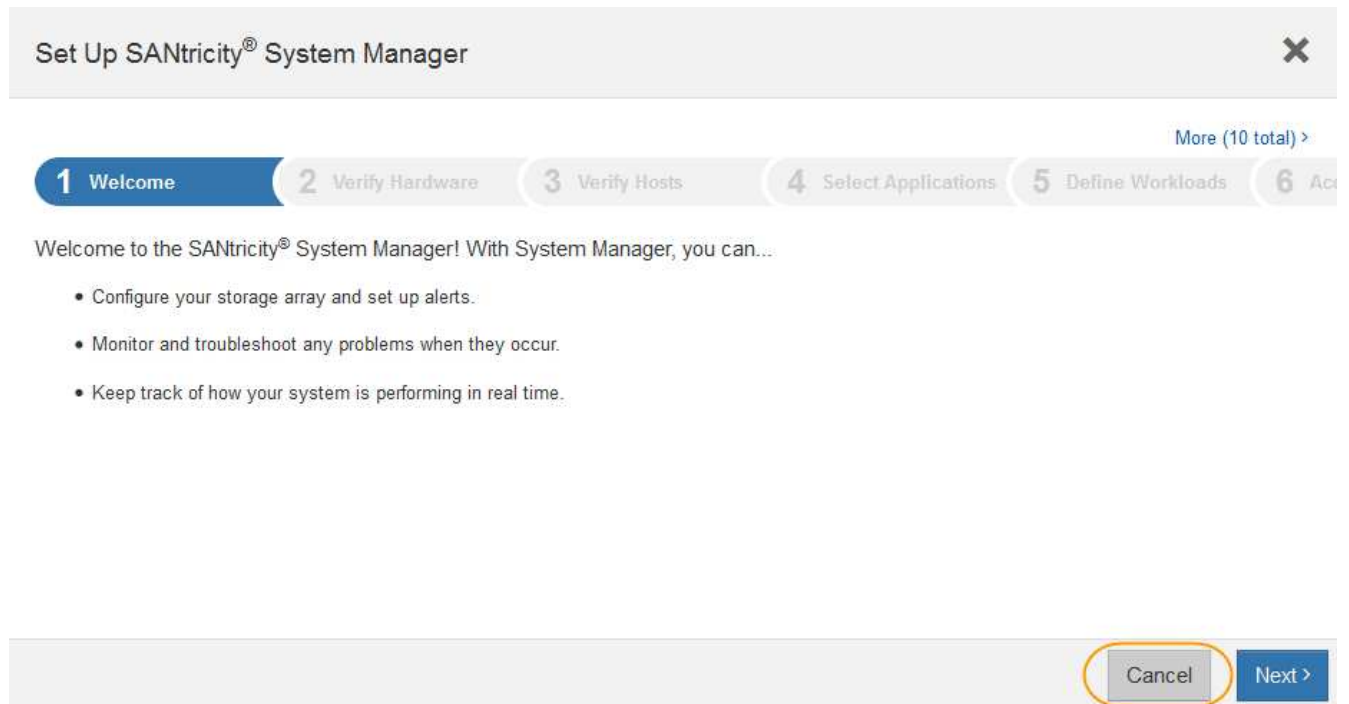
- Use the StorageGRID Appliance Installer and select **Advanced > SANtricity System Manager**
- Use the Grid Manager and select **NODES > *appliance Storage Node* > SANtricity System Manager**



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.

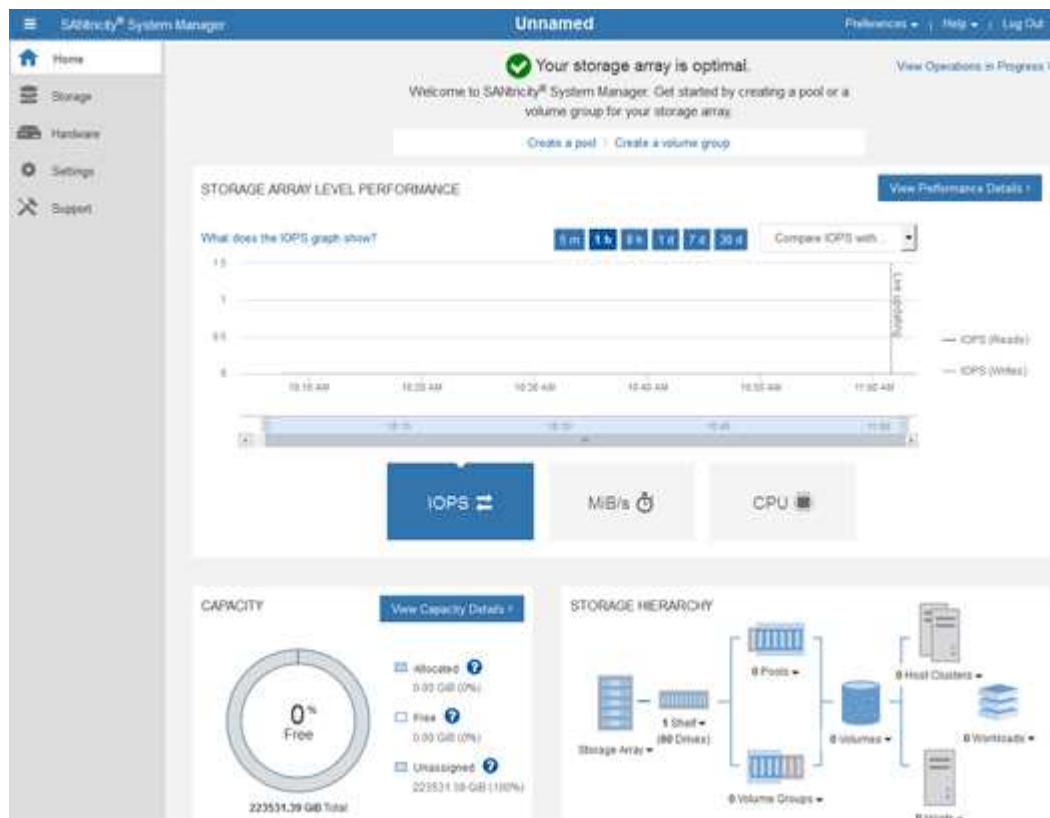
SANtricity System Manager uses a single administrator password that is shared among all users.



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.

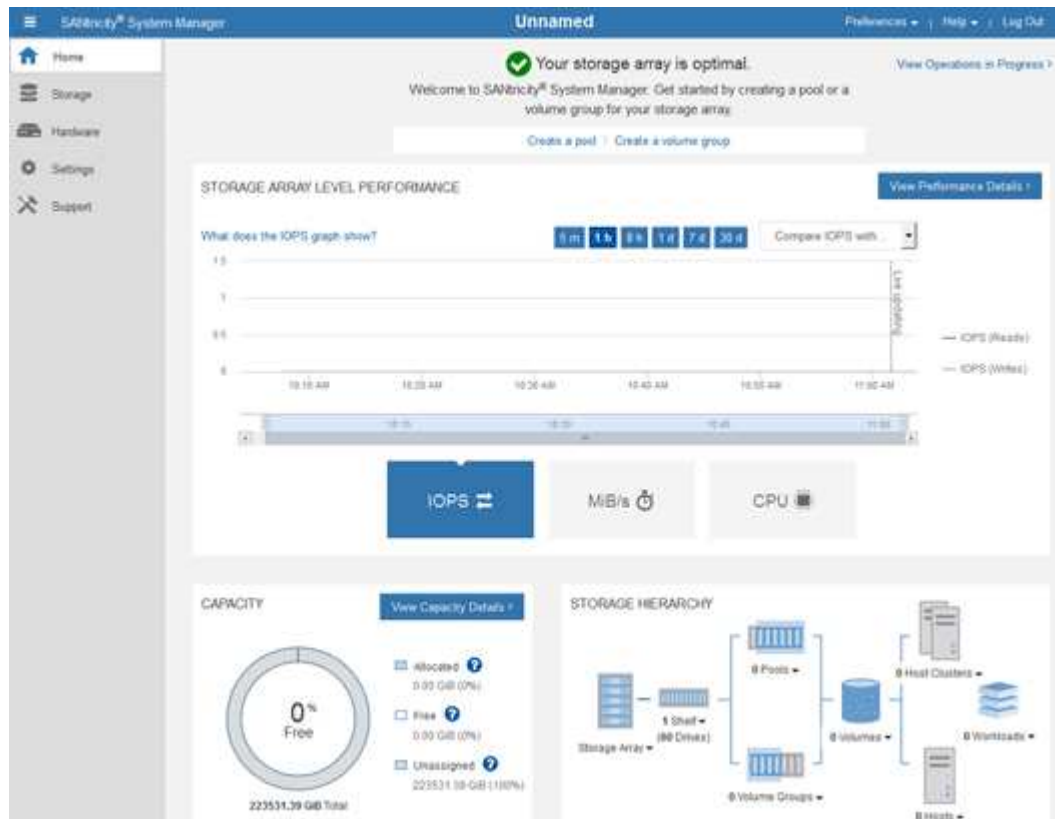


Accessing SANtricity System Manager from the Grid Manager or from the Appliance Installer is generally meant only for monitoring your hardware and configuring E-Series AutoSupport. Many features and operations within SANtricity System Manager such as upgrading firmware don't apply to monitoring your 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.

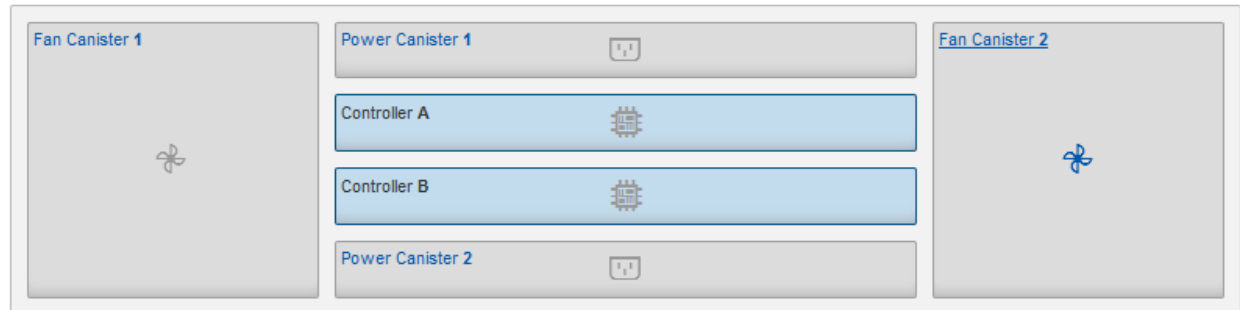
The SANtricity System Manager home page appears. In SANtricity System Manager, the controller shelf is referred to as a storage array.



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**.



## HARDWARE

[Learn More >](#)Legend ▼ Show status icon details ?Controller Shelf 99 ▼[Show front 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.

IPv4 Address Assignment     Static     DHCP

IPv4 Address (CIDR)	10.224.5.166/21
Default Gateway	10.224.0.1

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.

IPv4 Address Assignment     Static     DHCP

IPv4 Address (CIDR)	10.224.2.200/21
Default Gateway	10.224.0.1

- 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 (SG100, SG1000, SG6000, and SG6100)

### BMC interface: Overview (SG100, SG1000, SG6000, and SG6100)

The user interface for the baseboard management controller (BMC) on the SG6100, 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

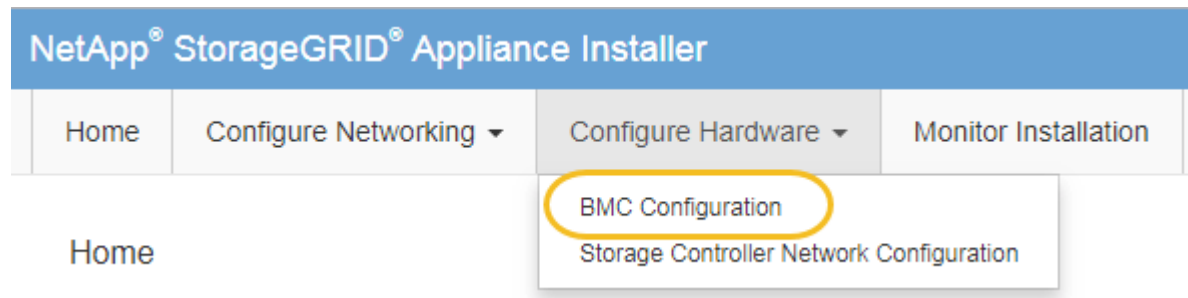
1. From the client, enter the URL for the StorageGRID Appliance Installer:

**`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. Select **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.

### SG100



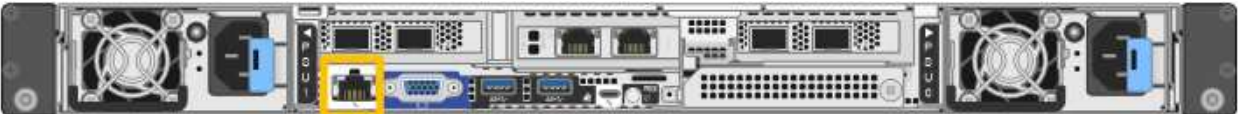
### SG1000



### SG6000



### SG6100



### 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.

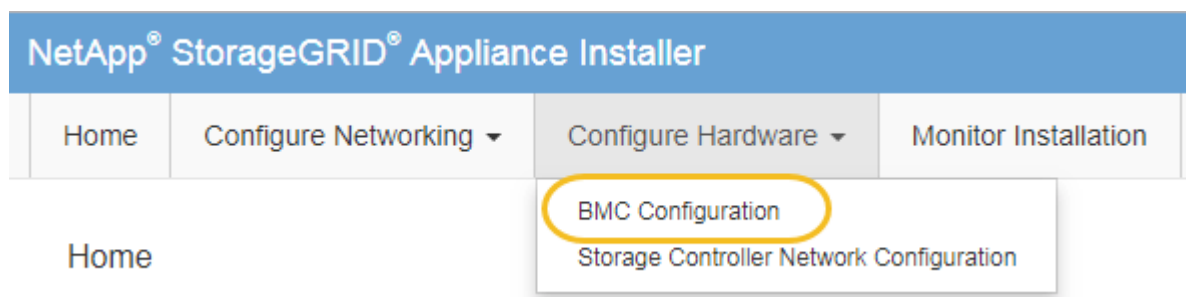
### Steps

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.

#### Baseboard Management Controller Configuration

##### LAN IP Settings

IP Assignment	<input type="radio"/> Static <input checked="" type="radio"/> DHCP
MAC Address	<input type="text" value="d8:c4:97:28:50:62"/>
IPv4 Address (CIDR)	<input type="text" value="10.224.3.225/21"/>
Default gateway	<input type="text" value="10.224.0.1"/>

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.

- Select **Static**.
- Enter the IPv4 address, using CIDR notation.
- Enter the default gateway.

#### Baseboard Management Controller Configuration

##### LAN IP Settings

IP Assignment	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
MAC Address	<input type="text" value="d8:c4:97:28:50:62"/>
IPv4 Address (CIDR)	<input type="text" value="10.224.3.225/21"/>
Default gateway	<input type="text" value="10.224.0.1"/>

d. Click **Save**.

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

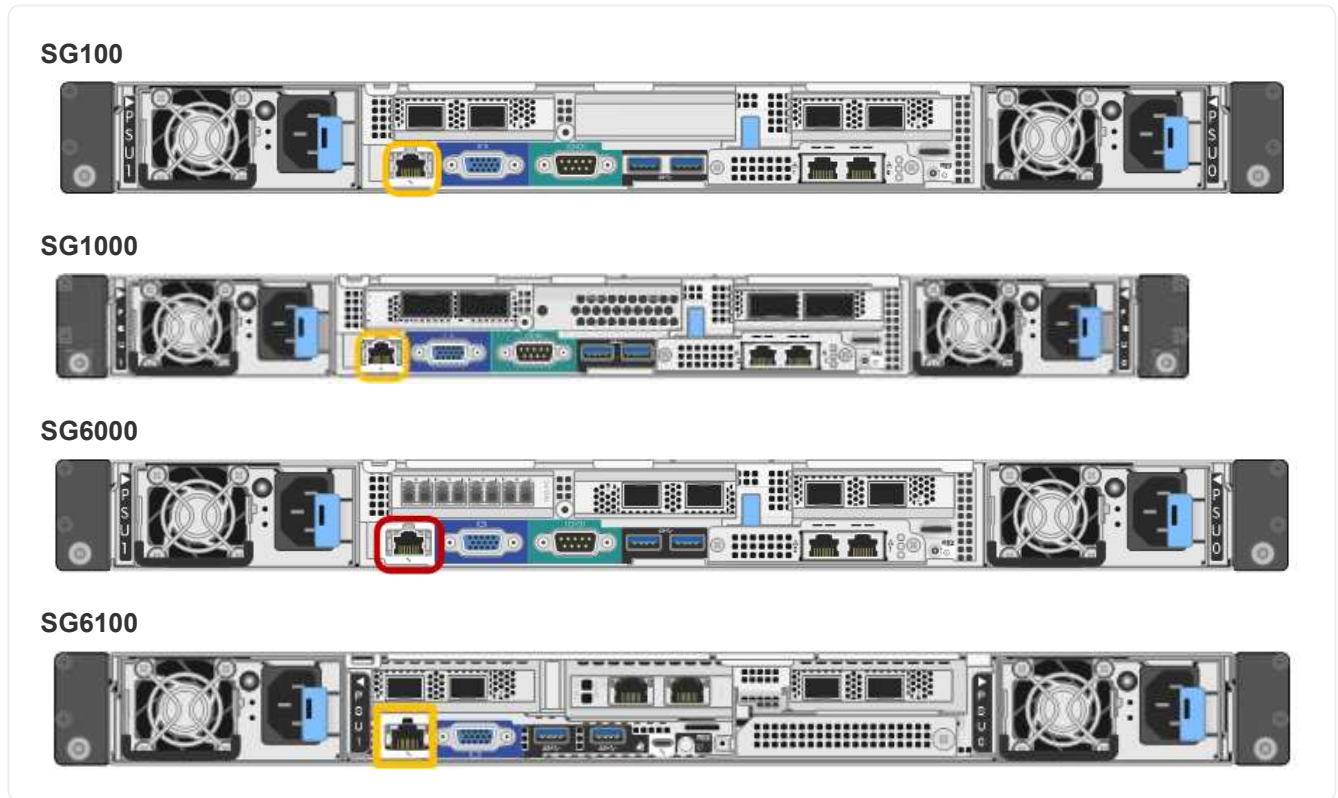
## Access BMC interface

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

- SG100
- SG1000
- SG6000
- SG6100

### 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.



### 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.



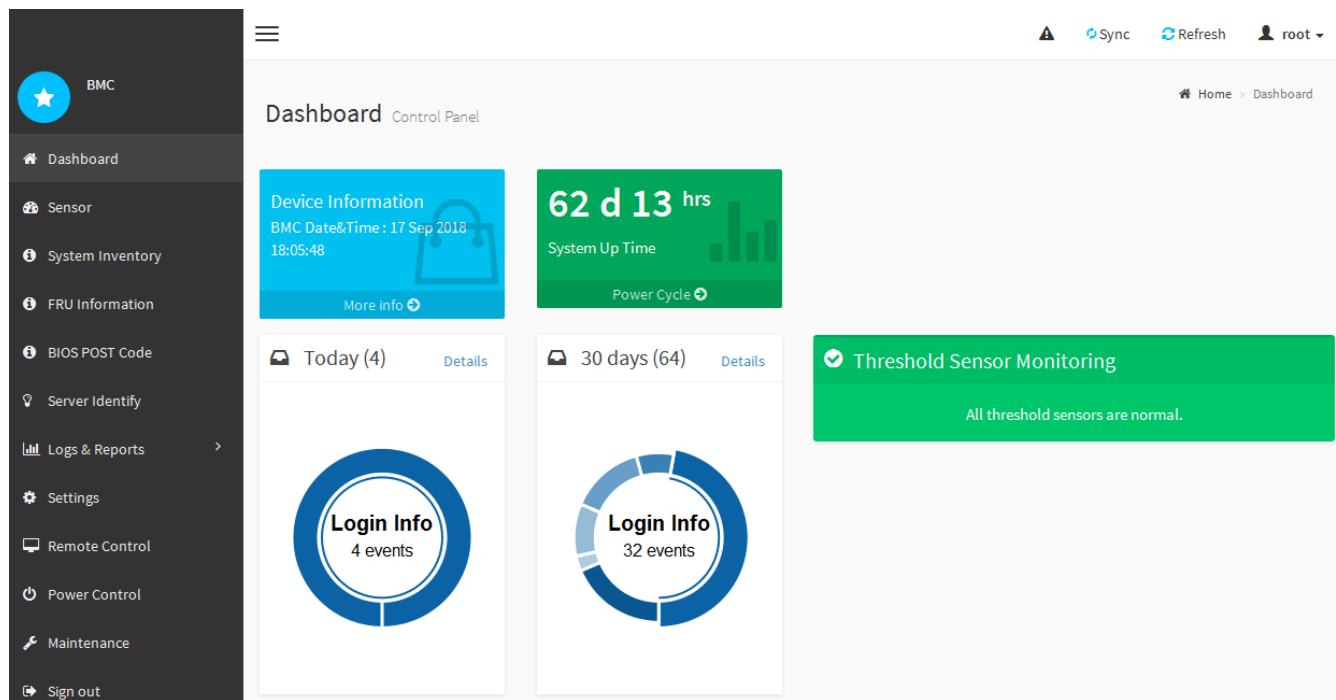
If you haven't yet configured `BMC_Port_IP`, follow the instructions in [Configure BMC interface](#). If you are unable to follow that procedure due to a hardware problem, and have not yet configured a BMC IP address, you might still be able to access the BMC. By default, the BMC obtains an IP address 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 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 SG6100, 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. DNS 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.



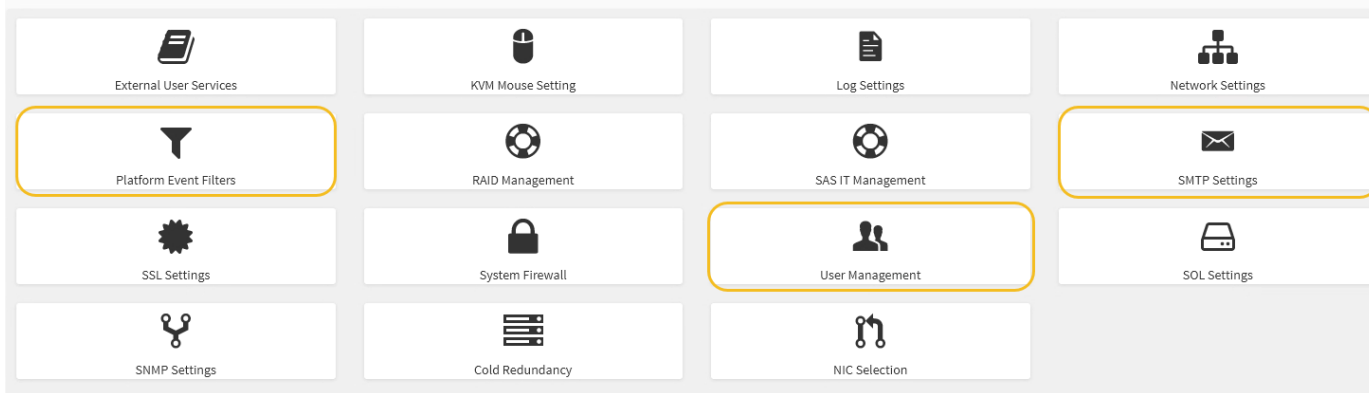
BMC settings made by this procedure might not be preserved if the SG6000-CN controller or services appliance fails and has to be replaced. Make sure you have a record of all settings you have applied, so they can be easily reapplied after a hardware replacement if necessary.

### 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 or drive encryption

You can enable encryption at the node and disk levels to protect the disks in your appliance against physical loss or removal from the site.

- [Node encryption](#) uses software encryption to protect all disks in the appliance. It does not require special drive hardware. Node encryption is performed by appliance software using keys managed by an external key management server (KMS).
- [Drive encryption](#) uses hardware encryption to protect self-encrypting drives (SEDs), also known as full-disk encryption (FED) drives, including those drives that meet the Federal Information Processing Standards (FIPS). Drive encryption is performed within each drive using encryption keys managed by a StorageGRID key manager.

You can perform both encryption levels on supported drives for additional security.

See [StorageGRID encryption methods](#) for information about all encryption methods available for StorageGRID appliances.

### 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**.

NetApp® StorageGRID® Appliance Installer Help ▾

Home | Configure Networking ▾ | Configure Hardware ▾ | Monitor Installation | Advanced ▾

### Node Encryption

Node encryption allows you to use an external key management server (KMS) to encrypt all StorageGRID data on this appliance. If node encryption is enabled for the appliance and a KMS is configured for the site, you cannot access any data on the appliance unless the appliance can communicate with the KMS.

#### Encryption Status

**⚠** You can only enable node encryption for an appliance during installation. You cannot enable or disable the node encryption setting after the appliance is installed.

Enable node encryption

**Save**

#### Key Management Server Details

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.

### Drive encryption

Drive encryption is managed on self-encrypting drive (SED) hardware during the write and read processes. Access to data on these drives is controlled by a user-defined passphrase. Drive encryption is used for direct-attached solid-state drives (SSDs) that are used for caching in StorageGRID appliances.

Encrypted SEDs automatically lock when the appliance is powered down or when the drive is removed from the appliance. An encrypted SED remains locked after power is restored to it until the correct passphrase is entered. To allow drives to be accessed without manually reentering the passphrase, the passphrase is stored on the StorageGRID appliance to unlock encrypted drives that remain in the appliance when the appliance restarts. Drives encrypted with an SED passphrase can be accessed by anyone who knows the passphrase.

Drive encryption doesn't apply to SANtricity-managed drives. If you have a StorageGRID appliance with SEDs and SANtricity controllers, you can enable drive security in [SANtricity System Manager](#).

You can enable drive encryption during initial appliance installation before loading Grid Manager. You can also enable node encryption or change your passphrase by placing the appliance in maintenance mode.

### Before you begin

Review the information about [StorageGRID encryption methods](#).

### About this task

A passphrase is set when drive encryption is initially enabled. If a compute node is replaced or if an encrypted SED is moved to a new compute node, you must manually reenter the passphrase.



Make sure that you store the drive-encryption passphrase in a secure location. Encrypted SEDs can't be accessed without manually entering the same passphrase if the SED is installed in another StorageGRID appliance.

### Enable drive encryption

1. Access the StorageGRID Appliance Installer.
  - During initial appliance installation, 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.

- For an existing StorageGRID appliance, [place the appliance into maintenance mode](#).

2. From the StorageGRID Appliance Installer Home page, select **Configure Hardware > Drive Encryption**.
3. Select **Enable drive encryption**.



After enabling drive encryption and setting the passphrase the SED drives are hardware encrypted. The content of the drive can't be accessed without using the same passphrase.

4. Select **Save**.

After the drive is encrypted, drive passphrase information displays.



When a drive is initially encrypted, the passphrase is set to a default blank value and the current passphrase text indicates "default (not secure)." While the data on this drive is encrypted, it can be accessed without entering a passphrase until a unique passphrase is set.

5. Enter a unique passphrase for encrypted drive access and then enter the passphrase again to confirm it. The passphrase must be at least 8 and no more than 32 characters in length.
6. Enter passphrase display text that will help you recall the passphrase.

Save the passphrase and passphrase display text in a secure location, such as a password management application.

7. Select **Save**.

#### View drive-encryption status

1. [Place the appliance into maintenance mode](#).
2. From the StorageGRID Appliance Installer, select **Configure Hardware > Drive Encryption**.

#### Access an encrypted drive

You must enter the passphrase to access an encrypted drive after compute node replacement or after a drive is moved to a new compute node.

1. Access the StorageGRID Appliance Installer.
  - 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.

- [Place the appliance into maintenance mode](#).
2. From the StorageGRID Appliance Installer, select the **Drive Encryption** link in the warning banner.
  3. Enter the drive encryption passphrase you set previously in **New passphrase** and **Retype new passphrase**.



If you enter values for the passphrase and passphrase display text that do not match the values previously entered, drive authentication will fail. You will need to restart the appliance and enter the correct passphrase and passphrase display text.

4. Enter the passphrase display text you set previously in **New passphrase display text**.
5. Select **Save**.

The warning banners will no longer display when the drives are unlocked.

6. Return to the StorageGRID Appliance Installer Home page and select **Reboot** in the Installation section banner to restart the compute node and access the encrypted drives.

### Change the drive-encryption passphrase

1. Access the StorageGRID Appliance Installer.
  - 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.

- [Place the appliance into maintenance mode](#).
2. From the StorageGRID Appliance Installer, select **Configure Hardware > Drive Encryption**.
  3. Enter a new unique passphrase for drive access and then enter the passphrase again to confirm it. The passphrase must be at least 8 and no more than 32 characters in length.



You must have already authenticated with access to the drive before you can change the drive-encryption passphrase.

4. Enter passphrase display text that will help you recall the passphrase.
5. Select **Save**.



After setting a new passphrase the encrypted drives can't be decrypted without using the new passphrase and passphrase display text.

6. Save the new passphrase and passphrase display text in a secure location, such as a password management application.

### Disable drive encryption

1. Access the StorageGRID Appliance Installer.
  - 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.

- [Place the appliance into maintenance mode](#).

2. From the StorageGRID Appliance Installer, select **Configure Hardware > Drive Encryption**.
3. Clear **Enable drive encryption**.
4. To erase all drive data when drive encryption is disabled, select **Erase all data on drives**.



The data erasure option is only available from the StorageGRID Appliance Installer before the appliance is added to the grid. You cannot access this option when accessing the StorageGRID Appliance Installer from maintenance mode.

5. Select **Save**.

The drive contents are unencrypted or cryptographically erased, the encryption passphrase is erased, and the SEDs are now accessible without a passphrase.

## Optional: Change RAID mode (SG5760 and SG6000)

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.



## 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**.

## 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**.

## 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**.

# Deploy an appliance node

## Deploy appliance Storage Node

After installing and configuring the storage appliance, you can deploy it as a Storage Node in a StorageGRID system. When you deploy an appliance as a Storage Node, you use the StorageGRID Appliance Installer included on the appliance.

### Before you begin

- If you are cloning an appliance node, continue following the [appliance node cloning](#) process.
- The appliance has been installed in a rack or cabinet, connected to your networks, and powered on.
- Network links, IP addresses, and port remapping (if necessary) have been configured for the appliance using the StorageGRID Appliance Installer.
- You know one of the IP addresses assigned to the appliance's compute controller. You can use the IP address for any attached StorageGRID network.
- The primary Admin Node for the StorageGRID system has been deployed.
- All Grid Network subnets listed on the IP Configuration page of the StorageGRID Appliance Installer have been defined in the Grid Network Subnet List on the primary Admin Node.
- You have a service laptop with a supported web browser.

### About this task

Each storage appliance functions as a single Storage Node. Any appliance can connect to the Grid Network, the Admin Network, and the Client Network

To deploy an appliance Storage Node in a StorageGRID system, you access the StorageGRID Appliance Installer and perform the following steps:

- You specify or confirm the IP address of the primary Admin Node and the name of the Storage Node.

- You start the deployment and wait as volumes are configured and the software is installed.
- When the installation pauses partway through the appliance installation tasks, you resume the installation by signing into the Grid Manager, approving all grid nodes, and completing the StorageGRID installation and deployment processes.



If you need to deploy multiple appliance nodes at one time, you can automate the installation process by using the `configure-sga.py` [Appliance Installation script](#).

- If you are performing an expansion or recovery operation, follow the appropriate instructions:
  - To add an appliance Storage Node to an existing StorageGRID system, see the instructions for [adding grid nodes](#).
  - To deploy an appliance Storage Node as part of a recovery operation, see instructions [recovering an appliance Storage Node](#).

### Steps

1. Open a browser, and enter one of the IP addresses for the appliance's compute controller.  
**`https://Controller_IP:8443`**

The StorageGRID Appliance Installer Home page appears.

## Home

 The installation is ready to be started. Review the settings below, and then click Start Installation.

### Primary Admin Node connection

Enable Admin Node discovery

Primary Admin Node IP

Connection state

Connection to 172.16.4.210 ready



### Node name

Node name




### Installation

Current state

Ready to start installation of NetApp-SGA into grid with Admin Node 172.16.4.210.

2. In the **Primary Admin Node connection** section, determine whether you need to specify the IP address for the primary Admin Node.

If you have previously installed other nodes in this data center, the StorageGRID Appliance Installer can discover this IP address automatically, assuming the primary Admin Node, or at least one other grid node with ADMIN\_IP configured, is present on the same subnet.

3. If this IP address is not shown or you need to change it, specify the address:

Option	Description
Manual IP entry	<ol style="list-style-type: none"> <li>Clear the <b>Enable Admin Node discovery</b> checkbox.</li> <li>Enter the IP address manually.</li> <li>Click <b>Save</b>.</li> <li>Wait for the connection state for the new IP address to become ready.</li> </ol>
Automatic discovery of all connected primary Admin Nodes	<ol style="list-style-type: none"> <li>Select the <b>Enable Admin Node discovery</b> checkbox.</li> <li>Wait for the list of discovered IP addresses to be displayed.</li> <li>Select the primary Admin Node for the grid where this appliance Storage Node will be deployed.</li> <li>Click <b>Save</b>.</li> <li>Wait for the connection state for the new IP address to become ready.</li> </ol>

- In the **Node name** field, provide the system name you want to use for this appliance node, and click **Save**.

The name that appears here will be the appliance node's system name. System names are required for internal StorageGRID operations and can't be changed.

- In the **Installation** section, confirm that the current state is "Ready to start installation of *node name* into grid with primary Admin Node *admin\_ip*" and that the **Start Installation** button is enabled.

If the **Start Installation** button is not enabled, you might need to change the network configuration or port settings. For instructions, see the maintenance instructions for your appliance.



If you are deploying the Storage Node appliance as a node cloning target, stop the deployment process here and continue the [node cloning procedure](#).

- From the StorageGRID Appliance Installer home page, click **Start Installation**.

The Current state changes to "Installation is in progress," and the [Monitor Installation page](#) is displayed.



If you need to access the Monitor Installation page manually, click **Monitor Installation**.

- If your grid includes multiple appliance Storage Nodes, repeat these steps for each appliance.



If you need to deploy multiple appliance Storage Nodes at one time, you can automate the installation process by using the `configure-sga.py` [Appliance Installation script](#).

## Deploy services appliance node

You can deploy a services appliance as a primary Admin Node, a non-primary Admin Node, or a Gateway Node. All services appliances can operate as Gateway Nodes and Admin Nodes (primary or non-primary) at the same time.

## Deploy services appliance as primary Admin Node

When you deploy a services appliance as a primary Admin Node, you use the StorageGRID Appliance Installer included on the appliance to install the StorageGRID software, or you upload the software version you want to install. You must install and configure the primary Admin Node before you install any other appliance node types. A primary Admin Node can connect to the Grid Network, and to the optional Admin Network and Client Network, if one or both are configured.

### Before you begin

- The appliance has been installed in a rack or cabinet, connected to your networks, and powered on.
- Network links, IP addresses, and port remapping (if necessary) have been configured for the appliance using the StorageGRID Appliance Installer.
- You have a service laptop with a [supported web browser](#).
- You know one of the IP addresses assigned to the appliance. You can use the IP address for any attached StorageGRID network.

### About this task

To install StorageGRID on an appliance primary Admin Node:

- You use the StorageGRID Appliance Installer to install the StorageGRID software. If you want to install a different version of the software, you first upload it using the StorageGRID Appliance Installer.
- You wait as the software is installed.
- When the software has been installed, the appliance is rebooted automatically.

### Steps

1. Open a browser, and enter the IP address for the appliance.  
**`https://services_appliance_IP:8443`**

The StorageGRID Appliance Installer Home page appears.

2. In the **This Node** section, select **Primary Admin**.
3. In the **Node name** field, enter the name you want to use for this appliance node, and click **Save**.

The node name is assigned to this appliance node in the StorageGRID system. It is shown on the Grid Nodes page in the Grid Manager.

4. Optionally, to install a different version of the StorageGRID software, follow these steps:
  - a. Download the installation archive:  
  
[NetApp Downloads: StorageGRID](#)
  - b. Extract the archive.
  - c. From the StorageGRID Appliance Installer, select **Advanced > Upload StorageGRID Software**.
  - d. Click **Remove** to remove the current software package.

### Upload StorageGRID Software

If this node is the primary Admin Node of a new deployment, you must use this page to upload the StorageGRID software installation package, unless the version of the software you want to install has already been uploaded. If you are adding this node to an existing deployment, you can avoid network traffic by uploading the installation package that matches the software version running on the existing grid. If you do not upload the correct package, the node obtains the software from the grid's primary Admin Node during installation.

### Current StorageGRID Installation Software

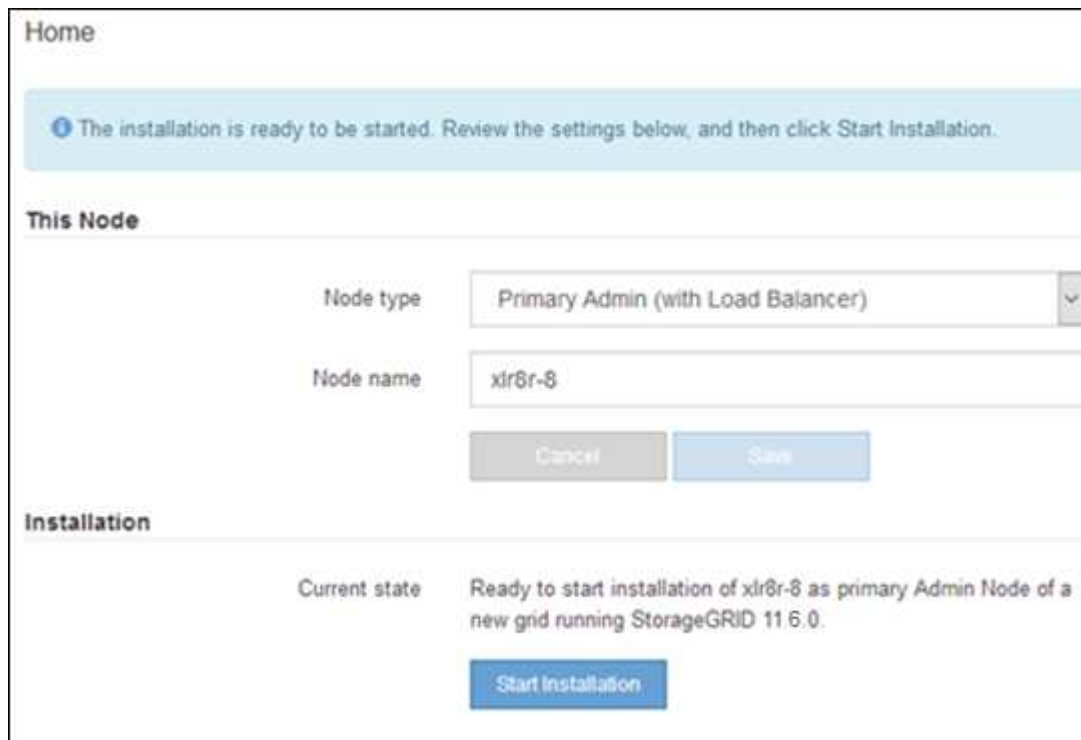
Version	11.3.0
Package Name	storagegrid-webscale-images-11-3-0_11.3.0-20190806.1731.4064510_amd64.deb
<input type="button" value="Remove"/>	

- e. Click **Browse** for the software package you downloaded and extracted. Select the `storagegrid-webscale-images-version.deb` package.
  - f. Select **Home** to return to the Home page.
5. Confirm that the current state is “Ready to start installation of primary Admin Node name with software version x.y” and that the **Start Installation** button is enabled.



If you are deploying the Admin Node appliance as a node cloning target, stop the deployment process here and continue the [node cloning procedure](#).

6. From the StorageGRID Appliance Installer home page, click **Start Installation**.



The Current state changes to “Installation is in progress,” and the Monitor Installation page is displayed.



If you need to access the Monitor Installation page manually, click **Monitor Installation** from the menu bar.

## Deploy services appliance as Gateway or non-primary Admin Node

When you deploy a services appliance as a Gateway Node or non-primary Admin Node, you use the StorageGRID Appliance Installer included on the appliance.

### Before you begin

- The appliance has been installed in a rack or cabinet, connected to your networks, and powered on.
- Network links, IP addresses, and port remapping (if necessary) have been configured for the appliance using the StorageGRID Appliance Installer.
- The primary Admin Node for the StorageGRID system has been deployed.
- All Grid Network subnets listed on the IP Configuration page of the StorageGRID Appliance Installer have been defined in the Grid Network Subnet List on the primary Admin Node.
- You have a service laptop with a [supported web browser](#).
- You know the IP address assigned to the appliance. You can use the IP address for any attached StorageGRID network.

### About this task

To install StorageGRID on a services appliance node:

- You specify or confirm the IP address of the primary Admin Node and the name of the appliance node.
- You start the installation and wait as the software is installed.

Partway through the appliance Gateway Node installation tasks, the installation pauses. To resume the installation, you sign into the Grid Manager, approve all grid nodes, and complete the StorageGRID installation process.



Don't deploy SG100 and SG1000 service appliances in the same site. Unpredictable performance might result.



If you need to deploy multiple appliance nodes at one time, you can automate the installation process. See [Automate appliance installation and configuration](#).

### Steps

1. Open a browser, and enter the IP address for the appliance.

```
https://Controller_IP:8443
```

The StorageGRID Appliance Installer Home page appears.

2. In the Primary Admin Node connection section, determine whether you need to specify the IP address for the primary Admin Node.

If you have previously installed other nodes in this data center, the StorageGRID Appliance Installer can discover this IP address automatically, assuming the primary Admin Node, or at least one other grid node with ADMIN\_IP configured, is present on the same subnet.



3. If this IP address is not shown or you need to change it, specify the address:

Option	Description
Manual IP entry	<ol style="list-style-type: none"> <li>Clear the <b>Enable Admin Node discovery</b> checkbox.</li> <li>Enter the IP address manually.</li> <li>Click <b>Save</b>.</li> <li>Wait for the connection state for the new IP address to become ready.</li> </ol>
Automatic discovery of all connected primary Admin Nodes	<ol style="list-style-type: none"> <li>Select the <b>Enable Admin Node discovery</b> checkbox.</li> <li>Wait for the list of discovered IP addresses to be displayed.</li> <li>Select the primary Admin Node for the grid where this appliance Storage Node will be deployed.</li> <li>Click <b>Save</b>.</li> <li>Wait for the connection state for the new IP address to become ready.</li> </ol>

4. In the **Node name** field, provide the system name you want to use for this appliance node, and click **Save**.

The name that appears here will be the appliance node's system name. System names are required for internal StorageGRID operations and can't be changed.

5. Optionally, to install a different version of the StorageGRID software, follow these steps:

a. Download the installation archive:

[NetApp Downloads: StorageGRID](#)

b. Extract the archive.

c. From the StorageGRID Appliance Installer, select **Advanced > Upload StorageGRID Software**.

d. Click **Remove** to remove the current software package.

The screenshot shows the NetApp StorageGRID Appliance Installer interface. At the top, there is a blue header with the text "NetApp® StorageGRID® Appliance Installer". Below the header is a navigation bar with several tabs: "Home", "Configure Networking", "Configure Hardware", "Monitor Installation", and "Advanced". The "Advanced" tab is currently selected. Below the navigation bar, the main content area is titled "Upload StorageGRID Software". Under this title, there is a paragraph of text explaining that if the node is the primary Admin Node of a new deployment, the user must use this page to upload the StorageGRID software installation package. Below this text, there is a section titled "Current StorageGRID Installation Software" which displays the following information:

Version	11.3.0
Package Name	storagegrid-webscale-images-11-3-0_11.3.0-20190806.1731.4064510_amd64.deb

Below the table, there is a button labeled "Remove".

- e. Click **Browse** for the software package you downloaded and extracted. Select the `storagegrid-webscale-images-version.deb` package.
  - f. Select **Home** to return to the Home page.
6. In the Installation section, confirm that the current state is "Ready to start installation of `node name` into grid with primary Admin Node `admin_ip`" and that the **Start Installation** button is enabled.

If the **Start Installation** button is not enabled, you might need to change the network configuration or port settings. For instructions, see the maintenance instructions for your appliance.

7. From the StorageGRID Appliance Installer home page, click **Start Installation**.

The Current state changes to "Installation is in progress," and the [Monitor Installation page](#) is displayed.



If you need to access the Monitor Installation page manually, click **Monitor Installation** from the menu bar.

8. If your grid includes multiple appliance nodes, repeat the previous steps for each appliance.

## Monitor appliance installation

The StorageGRID Appliance Installer provides status until installation is complete. When the software installation is complete, the appliance is rebooted.

## Example 1. Steps

### Storage appliance

1. To monitor the installation progress, click **Monitor Installation**.

The Monitor Installation page shows the installation progress.

Monitor Installation

1. Configure storage		Running
Step	Progress	Status
Connect to storage controller	<div style="width: 100%; height: 10px; background-color: green;"></div>	Complete
Clear existing configuration	<div style="width: 100%; height: 10px; background-color: green;"></div>	Complete
Configure volumes	<div style="width: 25%; height: 10px; background-color: blue;"></div>	Creating volume StorageGRID-obj-00
Configure host settings	<div style="width: 0%; height: 10px; background-color: gray;"></div>	Pending

2. Install OS	Pending
3. Install StorageGRID	Pending
4. Finalize installation	Pending

The blue status bar indicates which task is currently in progress. Green status bars indicate tasks that have completed successfully.



The installer ensures that tasks completed in a previous install aren't re-run. If you are re-running an installation, any tasks that don't need to be re-run are shown with a green status bar and a status of "Skipped."

2. Review the progress of the first two installation stages.

#### 1. Configure storage

During this stage, the installer connects to the storage controller, clears any existing configuration, creates RAIDs according to the configured RAID Mode, allocates volumes for StorageGRID software and object data storage, and configures host settings.

#### 2. Install OS

During this stage, the installer copies the base operating system image for StorageGRID to the appliance.

3. Continue monitoring the installation progress until the **Install StorageGRID** stage pauses and a message appears on the embedded console, prompting you to approve this node on the Admin Node using the Grid Manager. Go to the next step.

Home

Configure Networking ▾

Configure Hardware ▾

Monitor Installation

Advanced ▾

## Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```

/platform.type=: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```

- Go to the Grid Manager of the Primary Admin node, approve the pending storage node, and complete the StorageGRID installation process.

When you click **Install** from the Grid Manager, Stage 3 completes and stage 4, **Finalize Installation**, begins. When stage 4 completes, the controller is rebooted.




Close the window after all installation stages are complete.

### Services appliance

- To monitor the installation progress, click **Monitor Installation** from the menu bar.

The Monitor Installation page shows the installation progress.

## Monitor Installation

1. Configure storage		Complete
2. Install OS		Running
<b>Step</b>	<b>Progress</b>	<b>Status</b>
Obtain installer binaries		Complete
Configure installer		Complete
Install OS		Installer VM running
3. Install StorageGRID		Pending
4. Finalize installation		Pending

The blue status bar indicates which task is currently in progress. Green status bars indicate tasks that have completed successfully.



The installer ensures that tasks completed in a previous install aren't re-run. If you are re-running an installation, any tasks that don't need to be re-run are shown with a green status bar and a status of "Skipped."

### 2. Review the progress of first two installation stages.

#### ◦ 1. Configure storage

During this stage, the installer clears any existing configuration from the drives in the appliance, and configures host settings.

#### ◦ 2. Install OS

During this stage, the installer copies the base operating system image for StorageGRID to the appliance.

### 3. Continue monitoring the installation progress until one of the following processes occurs:

- For all appliance nodes except the primary Admin Node, the Install StorageGRID stage pauses and a message appears on the embedded console, prompting you to approve this node on the Admin Node using the [Grid Manager](#). Go to the next step.
- For appliance primary Admin Node installation, you don't need to approve the node. The appliance is rebooted. You can skip the next step.



During installation of an appliance primary Admin Node, a fifth phase appears to load the StorageGRID Installer (the example screen shot shows only the first four phases). If loading the StorageGRID Installer (fifth phase) is in progress for more than 10 minutes, refresh the web page manually.

Home

Configure Networking ▾

Configure Hardware ▾

Monitor Installation

Advanced ▾

## Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```

/platform.type#: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```

4. [Go to the Grid Manager](#) of the Primary Admin node, approve the pending grid node, and complete the StorageGRID installation process.

When you click **Install** from the Grid Manager, Stage 3 completes and stage 4, **Finalize Installation**, begins. When stage 4 completes, the appliance is rebooted.

Close the window after all installation stages are complete.

## Reboot appliance while StorageGRID Appliance Installer is running

You might need to reboot the appliance while the StorageGRID Appliance Installer is running. For example, you might need to reboot the appliance if the installation fails.

### About this task

This procedure only applies when the appliance is running the StorageGRID Appliance Installer. Once the

installation is completed, this step no longer works because the StorageGRID Appliance Installer is no longer available.

## Steps

1. From the StorageGRID Appliance Installer, click **Advanced** > **Reboot Controller**, and then select one of these options:
  - Select **Reboot into StorageGRID** to reboot the controller with the node rejoining the grid. Select this option if you are done working in maintenance mode and are ready to return the node to normal operation.
  - Select **Reboot into Maintenance Mode** to reboot the controller with the node remaining in maintenance mode. (This option is available only when the controller is in maintenance mode.) Select this option if there are additional maintenance operations you need to perform on the node before rejoining the grid.



The appliance is rebooted.

## Troubleshoot hardware installation (SG100 and SG1000)

If you encounter issues during the installation, you might find it helpful to review troubleshooting information related to hardware setup and connectivity issues.

### View boot-up codes

When you apply power to the appliance, the BMC logs a series of boot-up codes. You can view these codes on a graphical console that is connected to the BMC management port.

### Before you begin

- You know how to [access the BMC dashboard](#).
- If you want to use serial-over-LAN (SOL), you have experience using IPMI SOL console applications.

## Steps

1. Select one of the following methods for viewing the boot-up codes for the appliance controller, and gather the required equipment.

Method	Required equipment
VGA console	<ul style="list-style-type: none"> <li>• VGA-capable monitor</li> <li>• VGA cable</li> </ul>
KVM	<ul style="list-style-type: none"> <li>• RJ-45 cable</li> </ul>
Serial port	<ul style="list-style-type: none"> <li>• DB-9 serial cable</li> <li>• Virtual serial terminal</li> </ul>
SOL	<ul style="list-style-type: none"> <li>• Virtual serial terminal</li> </ul>

2. If you are using a VGA console, perform these steps:
  - a. Connect a VGA-capable monitor to the VGA port on the back of the appliance.
  - b. View the codes displayed on the monitor.
3. If you are using BMC KVM, perform these steps:
  - a. Connect to the BMC management port and log in to the BMC web interface.
  - b. Select **Remote Control**.
  - c. Launch the KVM.
  - d. View the codes on the virtual monitor.
4. If you are using a serial port and terminal, perform these steps:
  - a. Connect to the DB-9 serial port on the back of the appliance.
  - b. Use settings `115200 8-N-1`.
  - c. View the codes printed over the serial terminal.
5. If you are using SOL, perform these steps:
  - a. Connect to the IPMI SOL using the BMC IP address and login credentials.

```
ipmitool -I lanplus -H BMC_Port_IP -U admin -P Password sol activate
```



In some cases the default username might be `root` instead of `admin`.

- b. View the codes on the virtual serial terminal.
6. Use the table to look up the codes for your appliance.

Code	Indicates
HI	The master boot script has started.
HP	The system is checking to see if the network interface card (NIC) firmware needs to be updated.
RB	The system is rebooting after applying firmware updates.



Code	Indicates
FP	The hardware subsystem firmware update checks have been completed. Inter-controller communication services are starting.
HC	The system is checking for existing StorageGRID installation data.
HO	The StorageGRID appliance is running.
HA	StorageGRID is running.

### View error codes

If a hardware error occurs when the appliance is booting up, the BMC logs an error code. As required, you can view these error codes using the BMC interface, and then work with technical support to resolve the issue.

### Before you begin

- You know how to [access the BMC dashboard](#).

### Steps

- From the BMC dashboard, select **BIOS POST Code**.
- Review the information displayed for Current Code and the Previous Code.

If any of the following error codes are shown, work with technical support to resolve the issue.

Code	Indicates
0x0E	Microcode not found
0x0F	Microcode not loaded
0x50	Memory initialization error. Invalid memory type or incompatible memory speed.
0x51	Memory initialization error. SPD reading has failed.
0x52	Memory initialization error. Invalid memory size or memory modules don't match.
0x53	Memory initialization error. No usable memory detected.
0x54	Unspecified memory initialization error
0x55	Memory not installed
0x56	Invalid CPU type or speed

<b>Code</b>	<b>Indicates</b>
0x57	CPU mismatch
0x58	CPU self-test failed, or possible CPU cache error
0x59	CPU micro-code is not found, or micro-code update failed
0x5A	Internal CPU error
0x5B	Reset PPI is not available
0x5C	PEI phase BMC self-test failure
0xD0	CPU initialization error
0xD1	North bridge initialization error
0xD2	South bridge initialization error
0xD3	Some architectural protocols aren't available
0xD4	PCI resource allocation error. Out of resources.
0xD5	No space for legacy option ROM
0xD6	No console output devices are found
0xD7	No console input devices are found
0xD8	Invalid password
0xD9	Error loading boot option (LoadImage returned error)
0xDA	Boot option failed (StartImage returned error)
0xDB	Flash update failed
0xDC	Reset protocol is not available
0xDD	DXE phase BMC self-test failure
0xE8	MRC: ERR_NO_MEMORY
0xE9	MRC: ERR_LT_LOCK

<b>Code</b>	<b>Indicates</b>
0xEA	MRC: ERR_DDR_INIT
0xEB	MRC: ERR_MEM_TEST
0xEC	MRC: ERR_VENDOR_SPECIFIC
0xED	MRC: ERR_DIMM_COMPAT
0xEE	MRC: ERR_MRC_COMPATIBILITY
0xEF	MRC: ERR_MRC_STRUCT
0xF0	MRC: ERR_SET_VDD
0xF1	MRC: ERR_IOT_MEM_BUFFER
0xF2	MRC: ERR_RC_INTERNAL
0xF3	MRC: ERR_INVALID_REG_ACCESS
0xF4	MRC: ERR_SET_MC_FREQ
0xF5	MRC: ERR_READ_MC_FREQ
0x70	MRC: ERR_DIMM_CHANNEL
0x74	MRC: ERR_BIST_CHECK
0xF6	MRC: ERR_SMBUS
0xF7	MRC: ERR_PCU
0xF8	MRC: ERR_NGN
0xF9	MRC: ERR_INTERLEAVE_FAILURE

### **Hardware setup appears to hang**

The StorageGRID Appliance Installer might not be available if hardware faults or cabling errors prevent the appliance from completing its boot-up processing.

#### **Steps**

1. Review the LEDs on the appliance and the boot-up and error codes displayed in the BMC.

2. If you need help resolving an issue, contact technical support.

## Connection issues

If you can't connect to the services appliance, there might be a network issue, or the hardware installation might not have been completed successfully.

### Steps

1. Try to ping the appliance using the IP address for the appliance :  
**ping services\_appliance\_IP**

2. If you receive no response from the ping, confirm you are using the correct IP address.

You can use the IP address of the appliance on the Grid Network, the Admin Network, or the Client Network.

3. If the IP address is correct, check appliance cabling, QSFP or SFP transceivers, and the network setup.
4. If physical access to the appliance is available, you can use a direct connection to the permanent link-local IP 169.254.0.1 to check controller networking configuration and update if necessary. For detailed instructions, see step 2 in [Access StorageGRID Appliance Installer](#).

If that does not resolve the issue, contact technical support.

5. If the ping was successful, open a web browser.
6. Enter the URL for the StorageGRID Appliance Installer:  
**https://appliances\_controller\_IP:8443**

The Home page appears.

## Troubleshoot hardware installation (SG5700 or SG6000)

If you encounter issues during the installation, you might find it helpful to review troubleshooting information related to hardware setup and connectivity issues.

### View boot-up codes (SG6000-CN controller)

When you apply power to the appliance, the BMC logs a series of boot-up codes for the SG6000-CN controller. You can view these codes in several ways.

#### Before you begin

- You know how to [access the BMC dashboard](#).
- If you want to use serial-over-LAN (SOL), you have experience using IPMI SOL console applications.

### Steps

1. Select one of the following methods for viewing the boot-up codes for the appliance controller, and gather the required equipment.

Method	Required equipment
VGA console	<ul style="list-style-type: none"> <li>• VGA-capable monitor</li> <li>• VGA cable</li> </ul>
KVM	<ul style="list-style-type: none"> <li>• RJ-45 cable</li> </ul>
Serial port	<ul style="list-style-type: none"> <li>• DB-9 serial cable</li> <li>• Virtual serial terminal</li> </ul>
SOL	<ul style="list-style-type: none"> <li>• Virtual serial terminal</li> </ul>

2. If you are using a VGA console, perform these steps:
  - a. Connect a VGA-capable monitor to the VGA port on the back of the appliance.
  - b. View the codes displayed on the monitor.
3. If you are using BMC KVM, perform these steps:
  - a. Connect to the BMC management port and log in to the BMC web interface.
  - b. Select **Remote Control**.
  - c. Launch the KVM.
  - d. View the codes on the virtual monitor.
4. If you are using a serial port and terminal, perform these steps:
  - a. Connect to the DB-9 serial port on the back of the appliance.
  - b. Use settings `115200 8-N-1`.
  - c. View the codes printed over the serial terminal.
5. If you are using SOL, perform these steps:
  - a. Connect to the IPMI SOL using the BMC IP address and login credentials.

```
ipmitool -I lanplus -H BMC_Port_IP -U admin -P Password sol activate
```



In some cases the default username for an SG6000 appliance might be `root` instead of `admin`.

- b. View the codes on the virtual serial terminal.
6. Use the table to look up the codes for your appliance.

Code	Indicates
HI	The master boot script has started.
HP	The system is checking to see if the network interface card (NIC) firmware needs to be updated.

Code	Indicates
RB	The system is rebooting after applying firmware updates.
FP	The hardware subsystem firmware update checks have been completed. Inter-controller communication services are starting.
HE	<p>For an appliance Storage Node only:</p> <p>The system is awaiting connectivity with the storage controllers and synchronizing with the SANtricity operating system.</p> <p><b>Note:</b> If the boot-up procedure does not progress past this stage, perform these steps:</p> <ol style="list-style-type: none"> <li>Confirm that the four interconnect cables between the SG6000-CN controller and the two storage controllers are securely connected.</li> <li>As required, replace one or more of the cables, and try again.</li> <li>If this does not resolve the issue, contact technical support.</li> </ol>
HC	The system is checking for existing StorageGRID installation data.
HO	The StorageGRID Appliance Installer is running.
HA	StorageGRID is running.

### View error codes (SG6000-CN controller)

If a hardware error occurs when the SG6000-CN controller is booting up, the BMC logs an error code. As required, you can view these error codes using the BMC interface, and then work with technical support to resolve the issue.

#### Before you begin

- You know how to [access the BMC dashboard](#).

#### Steps

- From the BMC dashboard, select **BIOS POST Code**.
- Review the information displayed for Current Code and the Previous Code.

If any of the following error codes are shown, work with technical support to resolve the issue.

Code	Indicates
0x0E	Microcode not found
0x0F	Microcode not loaded

<b>Code</b>	<b>Indicates</b>
0x50	Memory initialization error. Invalid memory type or incompatible memory speed.
0x51	Memory initialization error. SPD reading has failed.
0x52	Memory initialization error. Invalid memory size or memory modules don't match.
0x53	Memory initialization error. No usable memory detected.
0x54	Unspecified memory initialization error
0x55	Memory not installed
0x56	Invalid CPU type or speed
0x57	CPU mismatch
0x58	CPU self-test failed, or possible CPU cache error
0x59	CPU micro-code is not found, or micro-code update failed
0x5A	Internal CPU error
0x5B	Reset PPI is not available
0x5C	PEI phase BMC self-test failure
0xD0	CPU initialization error
0xD1	North bridge initialization error
0xD2	South bridge initialization error
0xD3	Some architectural protocols aren't available
0xD4	PCI resource allocation error. Out of resources.
0xD5	No space for legacy option ROM
0xD6	No console output devices are found
0xD7	No console input devices are found

<b>Code</b>	<b>Indicates</b>
0xD8	Invalid password
0xD9	Error loading boot option (LoadImage returned error)
0xDA	Boot option failed (StartImage returned error)
0xDB	Flash update failed
0xDC	Reset protocol is not available
0xDD	DXE phase BMC self-test failure
0xE8	MRC: ERR_NO_MEMORY
0xE9	MRC: ERR_LT_LOCK
0xEA	MRC: ERR_DDR_INIT
0xEB	MRC: ERR_MEM_TEST
0xEC	MRC: ERR_VENDOR_SPECIFIC
0xED	MRC: ERR_DIMM_COMPAT
0xEE	MRC: ERR_MRC_COMPATIBILITY
0xEF	MRC: ERR_MRC_STRUCT
0xF0	MRC: ERR_SET_VDD
0xF1	MRC: ERR_IOT_MEM_BUFFER
0xF2	MRC: ERR_RC_INTERNAL
0xF3	MRC: ERR_INVALID_REG_ACCESS
0xF4	MRC: ERR_SET_MC_FREQ
0xF5	MRC: ERR_READ_MC_FREQ
0x70	MRC: ERR_DIMM_CHANNEL
0x74	MRC: ERR_BIST_CHECK



<b>Code</b>	<b>Indicates</b>
0xF6	MRC: ERR_SMBUS
0xF7	MRC: ERR_PCU
0xF8	MRC: ERR_NGN
0xF9	MRC: ERR_INTERLEAVE_FAILURE

### **Hardware setup appears to hang (SG6000 or SG5700)**

The StorageGRID Appliance Installer might not be available if hardware faults or cabling errors prevent the storage controllers or the appliance controller from completing their boot-up processing.

## Example 2. Steps

### SG5700

1. [Watch the codes on the SG5700 seven-segment displays.](#)

While the hardware is initializing during power up, the two seven-segment displays show a sequence of codes. When the hardware boots successfully, the seven-segment displays show different codes for each controller.

2. Review the codes on the seven-segment display for the E5700SG controller.



The installation and provisioning take time. Some installation phases don't report updates to the StorageGRID Appliance Installer for several minutes.

If an error occurs, the seven-segment display flashes a sequence, such as HE.

3. To understand what these codes mean, see the following resources:

Controller	Reference
E5700SG controller	<ul style="list-style-type: none"><li>• “Status indicators on the E5700SG controller”</li><li>• “HE error: Error synchronizing with SANtricity OS Software”</li></ul>
E2800 controller	<p><a href="#">E5700 and E2800 System Monitoring Guide</a></p> <p><b>Note:</b> The codes described for the E-Series E5700 controller don't apply to the E5700SG controller in the appliance.</p>

4. If this does not resolve the issue, contact technical support.

### SG6000

1. For the storage controllers, watch the codes on the seven-segment displays.

While the hardware is initializing during power up, the two seven-segment displays show a sequence of codes. When the hardware boots successfully, both seven-segment displays show 99.

2. Review the LEDs on the SG6000-CN controller and the boot-up and error codes displayed in the BMC.
3. If you need help resolving an issue, contact technical support.

## Connection issues (SG5700 or SG6000)

If you encounter connection issues during the StorageGRID appliance installation, you should perform the corrective action steps listed.

### Unable to connect to SG6000 appliance

If you can't connect to the appliance, there might be a network issue, or the hardware installation might not have been completed successfully.

## Steps

1. If you are unable to connect to SANtricity System Manager:
  - a. Try to ping the appliance using the IP address for either storage controller on the management network for SANtricity System Manager:  
**ping Storage\_Controller\_IP**
  - b. If you receive no response from the ping, confirm you are using the correct IP address.  
  
Use the IP address for management port 1 on either storage controller.
  - c. If the IP address is correct, check appliance cabling and the network setup.  
  
If that does not resolve the issue, contact technical support.
  - d. If the ping was successful, open a web browser.
  - e. Enter the URL for SANtricity System Manager:  
**https://Storage\_Controller\_IP**  
  
The log in page for SANtricity System Manager appears.
2. If you are unable to connect to the SG6000-CN controller:
  - a. Try to ping the appliance using the IP address for the SG6000-CN controller:  
**ping SG6000-CN\_Controller\_IP**
  - b. If you receive no response from the ping, confirm you are using the correct IP address.  
  
You can use the IP address of the appliance on the Grid Network, the Admin Network, or the Client Network.
  - c. If the IP address is correct, check appliance cabling, SFP transceivers, and the network setup.
  - d. If physical access to the SG6000-CN is available, you can use a direct connection to the permanent link-local IP 169.254.0.1 to check controller networking configuration and update if necessary. For detailed instructions, see step 2 in [Accessing StorageGRID Appliance Installer](#).  
  
If that does not resolve the issue, contact technical support.
  - e. If the ping was successful, open a web browser.
  - f. Enter the URL for the StorageGRID Appliance Installer:  
**https://SG6000-CN\_Controller\_IP:8443**  
  
The Home page appears.

### **SG6060 expansion shelves don't appear in Appliance Installer**

If you have installed expansion shelves for the SG6060 and they don't appear in the StorageGRID Appliance Installer, you should verify that the shelves have been completely installed and powered on.

#### **About this task**

You can verify that the expansion shelves are connected to the appliance by viewing the following information in the StorageGRID Appliance Installer:

- The **Home** page contains a message about expansion shelves.

**i** The storage system contains 2 expansion shelves.

- The **Advanced > RAID Mode** page indicates by number of drives whether or not the appliance includes expansion shelves. For example, in the following screen shot, two SSDs and 178 HDDs are shown. An SG6060 with two expansion shelves contains 180 total drives.

## Configure RAID Mode

This appliance contains the following drives.

Type	Size	Number of drives
SSD	800 GB	2
HDD	11.8 TB	178

If the StorageGRID Appliance Installer pages don't indicate that expansion shelves are present, follow this procedure.

### Steps

1. Verify that all required cables have been firmly connected. See [Cable appliance](#).
2. Verify that you have powered on the expansion shelves. See [Connect power cords and apply power \(SG6000\)](#).
3. If you need help resolving an issue, contact technical support.

### Unable to connect to SG5700 appliance

If you can't connect to the appliance, there might be a network issue, or the hardware installation might not have been completed successfully.

### Steps

1. If you are unable to connect to SANtricity System Manager:
  - a. Try to ping the appliance using the IP address for the E2800 controller on the management network for SANtricity System Manager:  
**ping E2800\_Controller\_IP**
  - b. If you receive no response from the ping, confirm you are using the correct IP address.  
  
Use the IP address for management port 1 on the E2800 controller.
  - c. If the IP address is correct, check appliance cabling and the network setup.  
  
If that does not resolve the issue, contact technical support.
  - d. If the ping was successful, open a web browser.
  - e. Enter the URL for SANtricity System Manager:  
**https://E2800\_Controller\_IP**  
  
The log in page for SANtricity System Manager appears.
2. If you are unable to connect to the E5700SG controller:

- a. Try to ping the appliance using the IP address for the E5700SG controller:  
`ping E5700SG_Controller_IP`
- b. If you receive no response from the ping, confirm you are using the correct IP address.  
  
You can use the IP address of the appliance on the Grid Network, the Admin Network, or the Client Network.
- c. If the IP address is correct, check appliance cabling, SFP transceivers, and the network setup.  
  
If that does not resolve the issue, contact technical support.
- d. If the ping was successful, open a web browser.
- e. Enter the URL for the StorageGRID Appliance Installer:  
`https://E5700SG_Controller_IP:8443`  
  
The Home page appears.

### **HE error: Error synchronizing with SANtricity OS Software (SG5700)**

The seven-segment display on the compute controller shows an HE error code if the StorageGRID Appliance Installer can't synchronize with SANtricity OS Software.

#### **About this task**

If an HE error code is displayed, perform this corrective action.

#### **Steps**

1. Check the integrity of the two SAS interconnect cables, and confirm they are securely connected.
2. As required, replace one or both of the cables, and try again.
3. If this does not resolve the issue, contact technical support.

### **Troubleshoot hardware installation (SG6100)**

If you encounter issues during the installation, you might find it helpful to review troubleshooting information related to hardware setup and connectivity issues.

#### **View boot-up codes**

When you apply power to the appliance, the BMC logs a series of boot-up codes. You can view these codes on a graphical console that is connected to the BMC management port.

#### **Before you begin**

- You know how to [access the BMC dashboard](#).
- If you want to use serial-over-LAN (SOL), you have experience using IPMI SOL console applications.

#### **Steps**

1. Select one of the following methods for viewing the boot-up codes for the appliance controller, and gather the required equipment.

Method	Required equipment
VGA console	<ul style="list-style-type: none"> <li>• VGA-capable monitor</li> <li>• VGA cable</li> </ul>
KVM	<ul style="list-style-type: none"> <li>• RJ-45 cable</li> </ul>
Serial port	<ul style="list-style-type: none"> <li>• DB-9 serial cable</li> <li>• Virtual serial terminal</li> </ul>
SOL	<ul style="list-style-type: none"> <li>• Virtual serial terminal</li> </ul>

2. If you are using a VGA console, perform these steps:
  - a. Connect a VGA-capable monitor to the VGA port on the back of the appliance.
  - b. View the codes displayed on the monitor.
3. If you are using BMC KVM, perform these steps:
  - a. Connect to the BMC management port and log in to the BMC web interface.
  - b. Select **Remote Control**.
  - c. Launch the KVM.
  - d. View the codes on the virtual monitor.
4. If you are using a serial port and terminal, perform these steps:
  - a. Connect to the serial USB port on the back of the appliance.
  - b. Use settings 115200 8-N-1.
  - c. View the codes printed over the serial terminal.
5. If you are using SOL, perform these steps:
  - a. Connect to the IPMI SOL using the BMC IP address and login credentials.

```
ipmitool -I lanplus -H BMC_Port_IP -U admin -P Password sol activate
```

- b. View the codes on the virtual serial terminal.
6. Use the table to look up the codes for your appliance.

Code	Indicates
HI	The master boot script has started.
HP	The system is checking to see if the network interface card (NIC) firmware needs to be updated.
RB	The system is rebooting after applying firmware updates.
FP	The hardware subsystem firmware update checks have been completed. Inter-controller communication services are starting.

Code	Indicates
HC	The system is checking for existing StorageGRID installation data.
HO	The StorageGRID appliance is running.
HA	StorageGRID is running.

### View error codes

If a hardware error occurs when the appliance is booting up, the BMC logs an error code. As required, you can view these error codes using the BMC interface, and then work with technical support to resolve the issue.

### Before you begin

- You know how to [access the BMC dashboard](#).

### Steps

- From the BMC dashboard, select **BIOS POST Code**.
- Review the information displayed for Current Code and the Previous Code.

If any of the following error codes are shown, work with technical support to resolve the issue.

Code	Indicates
0x0E	Microcode not found
0x0F	Microcode not loaded
0x50	Memory initialization error. Invalid memory type or incompatible memory speed.
0x51	Memory initialization error. SPD reading has failed.
0x52	Memory initialization error. Invalid memory size or memory modules don't match.
0x53	Memory initialization error. No usable memory detected.
0x54	Unspecified memory initialization error
0x55	Memory not installed
0x56	Invalid CPU type or speed
0x57	CPU mismatch

<b>Code</b>	<b>Indicates</b>
0x58	CPU self-test failed, or possible CPU cache error
0x59	CPU micro-code is not found, or micro-code update failed
0x5A	Internal CPU error
0x5B	Reset PPI is not available
0x5C	PEI phase BMC self-test failure
0xD0	CPU initialization error
0xD1	North bridge initialization error
0xD2	South bridge initialization error
0xD3	Some architectural protocols aren't available
0xD4	PCI resource allocation error. Out of resources.
0xD5	No space for legacy option ROM
0xD6	No console output devices are found
0xD7	No console input devices are found
0xD8	Invalid password
0xD9	Error loading boot option (LoadImage returned error)
0xDA	Boot option failed (StartImage returned error)
0xDB	Flash update failed
0xDC	Reset protocol is not available
0xDD	DXE phase BMC self-test failure
0xE8	MRC: ERR_NO_MEMORY
0xE9	MRC: ERR_LT_LOCK
0xEA	MRC: ERR_DDR_INIT



<b>Code</b>	<b>Indicates</b>
0xEB	MRC: ERR_MEM_TEST
0xEC	MRC: ERR_VENDOR_SPECIFIC
0xED	MRC: ERR_DIMM_COMPAT
0xEE	MRC: ERR_MRC_COMPATIBILITY
0xEF	MRC: ERR_MRC_STRUCT
0xF0	MRC: ERR_SET_VDD
0xF1	MRC: ERR_IOT_MEM_BUFFER
0xF2	MRC: ERR_RC_INTERNAL
0xF3	MRC: ERR_INVALID_REG_ACCESS
0xF4	MRC: ERR_SET_MC_FREQ
0xF5	MRC: ERR_READ_MC_FREQ
0x70	MRC: ERR_DIMM_CHANNEL
0x74	MRC: ERR_BIST_CHECK
0xF6	MRC: ERR_SMBUS
0xF7	MRC: ERR_PCU
0xF8	MRC: ERR_NGN
0xF9	MRC: ERR_INTERLEAVE_FAILURE

### **Hardware setup appears to hang**

The StorageGRID Appliance Installer might not be available if hardware faults or cabling errors prevent the appliance from completing its boot-up processing.

#### **Steps**

1. Review the LEDs on the appliance and the boot-up and error codes displayed in the BMC.
2. If you need help resolving an issue, contact technical support.

## Connection issues

If you can't connect to the services appliance, there might be a network issue, or the hardware installation might not have been completed successfully.

### Steps

1. Try to ping the appliance using the IP address for the appliance :

**ping appliance\_IP**

2. If you receive no response from the ping, confirm you are using the correct IP address.

You can use the IP address of the appliance on the Grid Network, the Admin Network, or the Client Network.

3. If the IP address is correct, check appliance cabling, QSFP or SFP transceivers, and the network setup.
4. If physical access to the appliance is available, you can use a direct connection to the permanent link-local IP 169.254.0.1 to check controller networking configuration and update if necessary. For detailed instructions, see step 2 in [Access StorageGRID Appliance Installer](#).

If that does not resolve the issue, contact technical support.

5. If the ping was successful, open a web browser.
6. Enter the URL for the StorageGRID Appliance Installer:

**https://appliances\_controller\_IP:8443**

The Home page appears.

# Maintain appliance hardware

## Maintain appliance configuration

### Common procedures for node maintenance: Overview

Use these instructions to maintain your StorageGRID system.

#### About these instructions

These instructions describe procedures common to all nodes such as how to apply a software hotfix, recover grid nodes, recover a failed site, decommission grid nodes or an entire site, perform network maintenance, perform host-level and middleware maintenance procedures, and perform grid node procedures.



In these instructions, “Linux” refers to a Red Hat® Enterprise Linux®, Ubuntu®, or Debian® deployment. Use the [NetApp Interoperability Matrix Tool \(IMT\)](#) to get a list of supported versions.

#### Before you begin

- You have a broad understanding of the StorageGRID system.
- You have reviewed your StorageGRID system’s topology and you understand the grid configuration.
- You understand that you must follow all instructions exactly and heed all warnings.
- You understand that maintenance procedures not described aren’t supported or require a services engagement.

#### Maintenance procedures for appliances

Specific maintenance procedures for each type of StorageGRID appliance are in the appliance maintenance sections:

- [Maintain SG6100 appliance](#)
- [Maintain SG6000 appliance](#)
- [Maintain SG5700 appliance](#)
- [Maintain SG100 and SG1000 appliances](#)

#### Place appliance into maintenance mode

You must place the appliance into maintenance mode before performing specific maintenance procedures.

#### Before you begin

- You are signed in to the Grid Manager using a [supported web browser](#).
- You have the Maintenance or Root access permission. For details, see the instructions for administering StorageGRID.

#### About this task

In rare instances, placing a StorageGRID appliance into maintenance mode might make the appliance unavailable for remote access.




The admin account password and SSH host keys for a StorageGRID appliance in maintenance mode remain the same as they were when the appliance was in service.

## Steps

1. From the Grid Manager, select **NODES**.
2. From the tree view of the Nodes page, select the appliance Storage Node.
3. Select **Tasks**.
4. Select **Maintenance mode**. A confirmation dialog box appears.
5. Enter the provisioning passphrase, and select **OK**.

A progress bar and a series of messages, including "Request Sent," "Stopping StorageGRID," and "Rebooting," indicate that the appliance is completing the steps for entering maintenance mode.

When the appliance is in maintenance mode, a confirmation message lists the URLs you can use to access the StorageGRID Appliance Installer.

 This node is currently in maintenance mode. Navigate to one of the URLs listed below and perform any necessary maintenance procedures.

- <https://172.16.2.24:8443>
- <https://10.224.2.24:8443>

When you are done with any required maintenance procedures, you must exit maintenance mode by selecting Reboot Controller from the StorageGRID Appliance Installer.

6. To access the StorageGRID Appliance Installer, browse to any of the URLs displayed.

If possible, use the URL containing the IP address of the appliance's Admin Network port.




If you have a direct connection to the appliance's management port, use <https://169.254.0.1:8443> to access the StorageGRID Appliance Installer page.

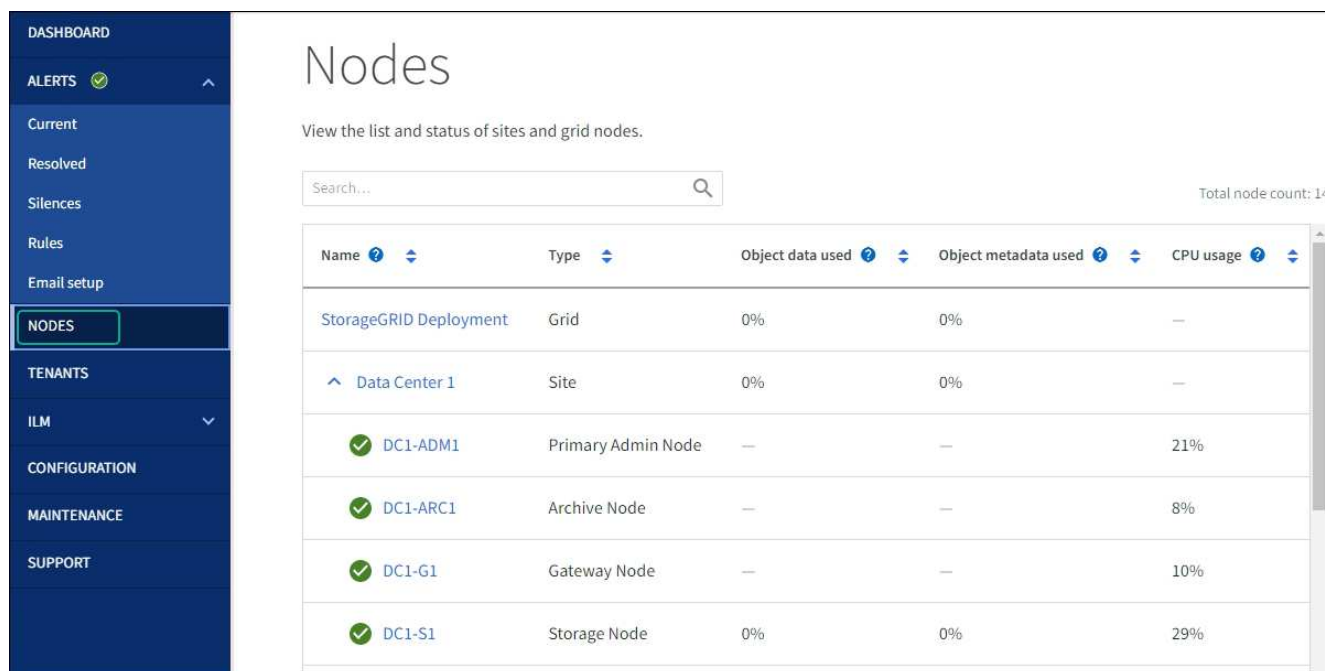
7. From the StorageGRID Appliance Installer, confirm that the appliance is in maintenance mode.

 This node is in maintenance mode. Perform any required maintenance procedures. If you want to exit maintenance mode manually to resume normal operation, go to **Advanced > Reboot Controller** to **reboot** the controller.

8. Perform any required maintenance tasks.
9. After completing maintenance tasks, exit maintenance mode and resume normal node operation. From the StorageGRID Appliance Installer, select **Advanced > Reboot Controller**, and then select **Reboot into StorageGRID**.



It can take up to 20 minutes for the appliance to reboot and rejoin the grid. To confirm that the reboot is complete and that the node has rejoined the grid, go back to the Grid Manager. The **NODES** page should display a normal status (green check mark icon  to the left of the node name) for the appliance node, indicating that no alerts are active and the node is connected to the grid.



## Change MTU setting

You can change the MTU setting that you assigned when you configured IP addresses for the appliance node.



### About this task

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.

To change the MTU setting without rebooting the appliance node, [use the Change IP tool](#).

If the Client or Admin Network was not configured in the StorageGRID Appliance Installer during the initial installation, [change the MTU setting using maintenance mode](#).

## Change the MTU setting using the Change IP tool

### Before you begin

You have the `Passwords.txt` file to use the Change IP tool.

### Steps

Access the Change IP tool and update the MTU settings as described in [Change node network configuration](#).

## Change the MTU setting using maintenance mode

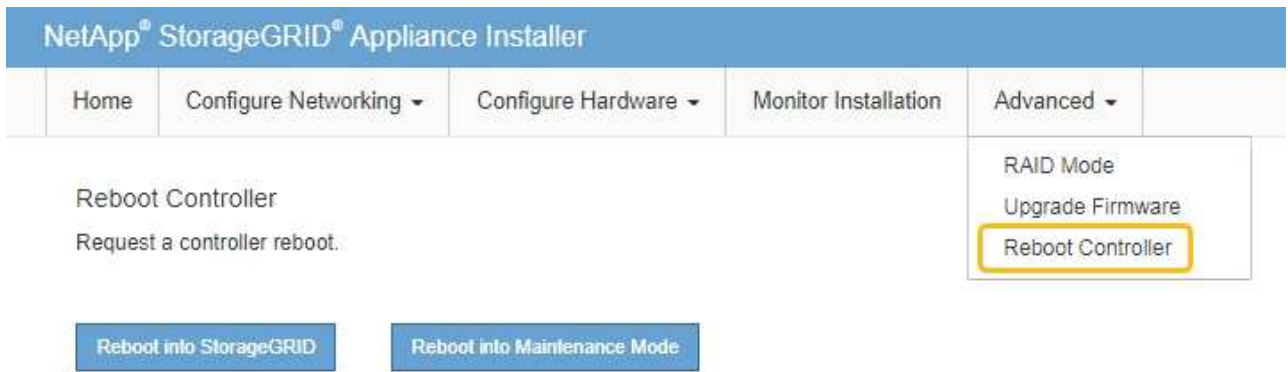
Change the MTU setting using maintenance mode if you are unable to access these settings using the Change IP tool.


### Before you begin

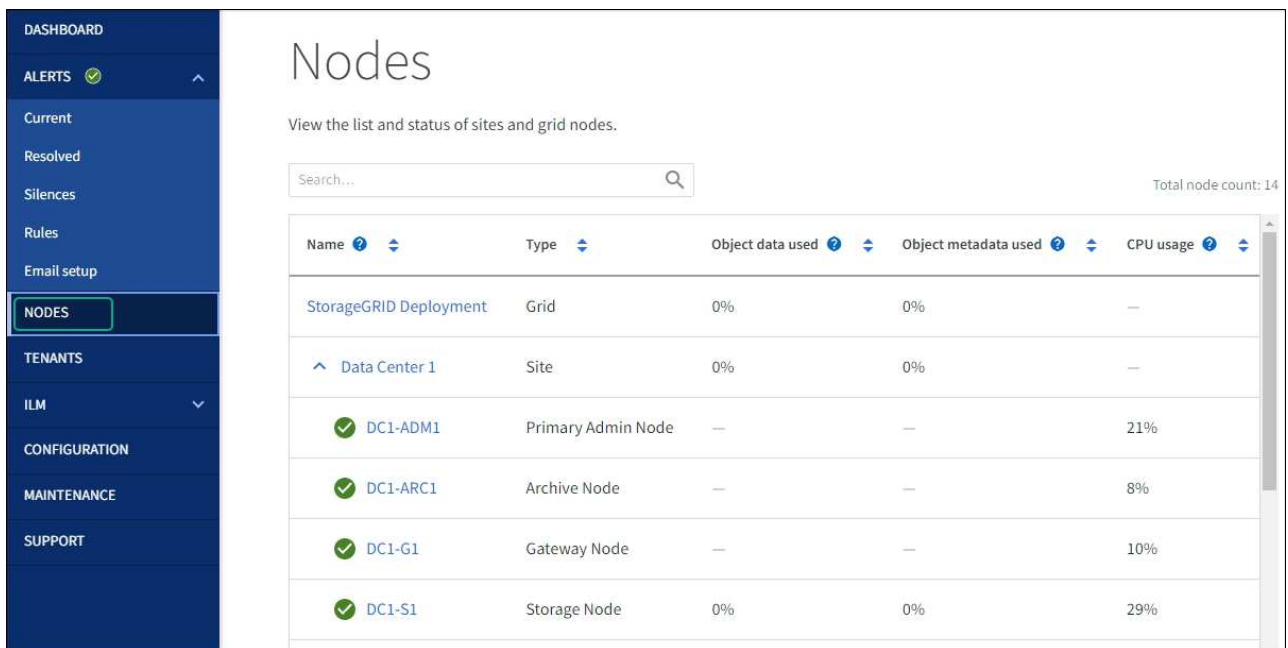
The appliance has been [placed maintenance mode](#).

### Steps

1. From the StorageGRID Appliance Installer, select **Configure Networking > IP Configuration**.
2. Make the desired changes to the MTU settings for the Grid Network, Admin Network, and Client Network.
3. When you are satisfied with the settings, select **Save**.
4. If this procedure completed successfully and you have additional procedures to perform while the node is in maintenance mode, perform them now. When you are done, or if you experienced any failures and want to start over, select **Advanced > Reboot Controller**, and then select one of these options:
  - Select **Reboot into StorageGRID**
  - Select **Reboot into Maintenance Mode** to reboot the controller with the node remaining in maintenance mode. Select this option if you experienced any failures during the procedure and want to start over. After the node finishes rebooting into maintenance mode, restart from the appropriate step in the procedure that failed.



It can take up to 20 minutes for the appliance to reboot and rejoin the grid. To confirm that the reboot is complete and that the node has rejoined the grid, go back to the Grid Manager. The **NODES** page should display a normal status (green check mark icon  to the left of the node name) for the appliance node, indicating that no alerts are active and the node is connected to the grid.



## Check DNS server configuration

You can check and temporarily change the DNS servers that are currently in use by this appliance node.

### Before you begin

The appliance has been [placed in maintenance mode](#).

### About this task

You might need to change the DNS server settings if an encrypted appliance can't connect to the key management server (KMS) or KMS cluster because the hostname for the KMS was specified as a domain name instead of an IP address. Any changes that you make to the DNS settings for the appliance are

temporary and are lost when you exit maintenance mode. To make these changes permanent, specify the DNS servers in Grid Manager (**MAINTENANCE > Network > DNS servers**).

- Temporary changes to the DNS configuration are necessary only for node-encrypted appliances where the KMS server is defined using a fully qualified domain name, instead of an IP address, for the hostname.
- When a node-encrypted appliance connects to a KMS using a domain name, it must connect to one of the DNS servers defined for the grid. One of these DNS servers then translates the domain name into an IP address.
- If the node can't reach a DNS server for the grid, or if you changed the grid-wide DNS settings when a node-encrypted appliance node was offline, the node is unable to connect to the KMS. Encrypted data on the appliance can't be decrypted until the DNS issue is resolved.


To resolve a DNS issue preventing KMS connection, specify the IP address of one or more DNS servers in the StorageGRID Appliance Installer. These temporary DNS settings allow the appliance to connect to the KMS and decrypt data on the node.

For example, if the DNS server for the grid changes while an encrypted node was offline, the node will not be able to reach the KMS when it comes back online, because it is still using the previous DNS values. Entering the new DNS server IP address in the StorageGRID Appliance Installer allows a temporary KMS connection to decrypt the node data.



### Steps

1. From the StorageGRID Appliance Installer, select **Configure Networking > DNS Configuration**.
2. Verify that the DNS servers specified are correct.

#### DNS Servers

 Configuration changes made on this page will not be passed to the StorageGRID software after appliance installation.

#### Servers

Server 1	<input type="text" value="10.224.223.135"/>	
Server 2	<input type="text" value="10.224.223.136"/>	
<input type="button" value="Cancel"/>		<input type="button" value="Save"/>

3. If required, change the DNS servers.



Changes made to the DNS settings are temporary and are lost when you exit maintenance mode.

4. When you are satisfied with the temporary DNS settings, select **Save**.

The node uses the DNS server settings specified on this page to reconnect to the KMS, allowing data on the node to be decrypted.

5. After node data is decrypted, reboot the node. From the StorageGRID Appliance Installer, select **Advanced > Reboot Controller**, and then select one of these options:



- Select **Reboot into StorageGRID** to reboot the controller with the node rejoining the grid. Select this option if you are done working in maintenance mode and are ready to return the node to normal operation.
- Select **Reboot into Maintenance Mode** to reboot the controller with the node remaining in maintenance mode. (This option is available only when the controller is in maintenance mode.) Select this option if there are additional maintenance operations you need to perform on the node before rejoining the grid.

NetApp® StorageGRID® Appliance Installer

Home   Configure Networking ▾   Configure Hardware ▾   Monitor Installation   Advanced ▾


Reboot Controller  
Request a controller reboot.

- RAID Mode
- Upgrade Firmware
- Reboot Controller**

Reboot into StorageGRID   Reboot into Maintenance Mode







When the node reboots and rejoins the grid, it uses the system-wide DNS servers listed in the Grid Manager. After rejoining the grid, the appliance will no longer use the temporary DNS servers specified in the StorageGRID Appliance Installer while the appliance was in maintenance mode.

It can take up to 20 minutes for the appliance to reboot and rejoin the grid. To confirm that the reboot is complete and that the node has rejoined the grid, go back to the Grid Manager. The **NODES** page should display a normal status (green check mark icon  to the left of the node name) for the appliance node, indicating that no alerts are active and the node is connected to the grid.

Nodes

View the list and status of sites and grid nodes.

Search... Total node count: 14

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
Data Center 1	Site	0%	0%	—
 DC1-ADM1	Primary Admin Node	—	—	21%
 DC1-ARC1	Archive Node	—	—	8%
 DC1-G1	Gateway Node	—	—	10%
 DC1-S1	Storage Node	0%	0%	29%

## Update MAC address references

In some cases you might need to update MAC address references after the replacement of an appliance.

### About this task

If any of the network interfaces on an appliance you are replacing are configured for DHCP, you might need to update the permanent DHCP lease assignments on the DHCP servers to reference the MAC addresses of the replacement appliance. The update ensures the replacement appliance is assigned the expected IP addresses.

### Steps

1. Locate the label on the front of the appliance. The label lists the MAC address for the BMC management port of the appliance.
2. To determine the MAC address for the Admin Network port, you must 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 =**.

3. Ask your network administrator to associate the DNS/network and IP address for the appliance you removed with the MAC address for the replacement appliance.



You must ensure that all IP addresses for the original appliance have been updated before you apply power to the replacement appliance. Otherwise, the appliance will obtain new DHCP IP addresses when it boots up and might not be able to reconnect to StorageGRID. This step applies to all StorageGRID networks that are attached to the appliance.



If the original appliance used static IP address, the new appliance will automatically adopt the IP addresses of the appliance you removed.

## Monitor node encryption in maintenance mode

If you enabled node encryption for the appliance during installation, you can monitor the node-encryption status of each appliance node, including the node-encryption state and key management server (KMS) details.

See [Configure key management servers](#) for information about implementing KMS for StorageGRID appliances.

### Before you begin

- You enabled node encryption for the appliance during installation. You can't enable node encryption after the appliance is installed.
- You have [placed the appliance into maintenance mode](#).


### Steps

1. From the StorageGRID Appliance Installer, select **Configure Hardware > Node Encryption**.

## Node Encryption

Node encryption allows you to use an external key management server (KMS) to encrypt all StorageGRID data on this appliance. If node encryption is enabled for the appliance and a KMS is configured for the site, you cannot access any data on the appliance unless the appliance can communicate with the KMS.

### Encryption Status

 You can only enable node encryption for an appliance during installation. You cannot enable or disable the node encryption setting after the appliance is installed.

Enable node encryption

Save

### Key Management Server Details


View the status and configuration details for the KMS that manages the encryption key for this appliance. You must use the Grid Manager to make configuration changes.

KMS display name	thales
External key UID	41b0306abcce451facfe01b1b4870ae1c1ec6bd5e3849d790223766baf35c57
Hostnames	10.96.99.164 10.96.99.165
Port	5696

Server certificate >

Client certificate >

### Clear KMS Key

 Do not clear the KMS key if you need to access or preserve any data on this appliance.

If you want to reinstall this appliance node (for example, in another grid), you must clear the KMS key. When the KMS key is cleared, all data on this appliance is deleted.

Clear KMS Key and Delete Data

The Node Encryption page includes three sections:

- Encryption Status shows whether node encryption is enabled or disabled for the appliance.
- Key Management Server Details shows information about the KMS being used to encrypt the appliance. You can expand the server and client certificate sections to view certificate details and status.
  - To address issues with the certificates themselves, such as renewing expired certificates, see the [instructions for configuring KMS](#).
  - If there are unexpected problems connecting to KMS hosts, verify that the [DNS servers are correct](#) and that [appliance networking is correctly configured](#).
  - If you are unable to resolve your certificate issues, contact technical support.
- Clear KMS Key disables node encryption for the appliance, removes the association between the appliance and the key management server that was configured for the StorageGRID site, and deletes all data from the appliance. You must [clear the KMS key](#) before you can install the appliance into another StorageGRID system.



Clearing the KMS configuration deletes data from the appliance, rendering it permanently inaccessible. This data is not recoverable.

- When you are done checking node-encryption status, reboot the node. From the StorageGRID Appliance Installer, select **Advanced > Reboot Controller**, and then select one of these options:
  - Select **Reboot into StorageGRID** to reboot the controller with the node rejoining the grid. Select this option if you are done working in maintenance mode and are ready to return the node to normal operation.
  - Select **Reboot into Maintenance Mode** to reboot the controller with the node remaining in maintenance mode. (This option is available only when the controller is in maintenance mode.) Select this option if there are additional maintenance operations you need to perform on the node before rejoining the grid.


NetApp® StorageGRID® Appliance Installer

Home   Configure Networking ▾   Configure Hardware ▾   Monitor Installation   Advanced ▾


Reboot Controller  
Request a controller reboot.

RAID Mode  
Upgrade Firmware  
**Reboot Controller**

Reboot into StorageGRID   Reboot into Maintenance Mode

It can take up to 20 minutes for the appliance to reboot and rejoin the grid. To confirm that the reboot is complete and that the node has rejoined the grid, go back to the Grid Manager. The **NODES** page should display a normal status (green check mark icon  to the left of the node name) for the appliance node, indicating that no alerts are active and the node is connected to the grid.

DASHBOARD

ALERTS  ^

Current

Resolved

Silences

Rules

Email setup

**NODES**

TENANTS

ILM ▾


CONFIGURATION

MAINTENANCE










SUPPORT

## Nodes

View the list and status of sites and grid nodes.

Search... 

Total node count: 14

Name  ▾	Type  ▾	Object data used  ▾	Object metadata used  ▾	CPU usage  ▾
StorageGRID Deployment	Grid	0%	0%	—
^ Data Center 1	Site	0%	0%	—
 DC1-ADM1	Primary Admin Node	—	—	21%
 DC1-ARC1	Archive Node	—	—	8%
 DC1-G1	Gateway Node	—	—	10%
 DC1-S1	Storage Node	0%	0%	29%

## Clear key management server configuration

Clearing the key management server (KMS) configuration disables node encryption on your appliance. After clearing the KMS configuration, the data on your appliance is permanently deleted and is no longer accessible. This data is not recoverable.

### Before you begin

If you need to preserve data on the appliance, you must either perform a node decommission procedure or clone the node before you clear the KMS configuration.



When KMS is cleared, data on the appliance will be permanently deleted and no longer accessible. This data is not recoverable.

[Decommission the node](#) to move any data it contains to other nodes in StorageGRID.

### About this task

Clearing the appliance KMS configuration disables node encryption, removing the association between the appliance node and the KMS configuration for the StorageGRID site. Data on the appliance is then deleted and the appliance is left in a pre-install state. This process can't be reversed.

You must clear the KMS configuration:

- Before you can install the appliance into another StorageGRID system, that does not use a KMS or that uses a different KMS.



Don't clear the KMS configuration if you plan to reinstall an appliance node in a StorageGRID system that uses the same KMS key.

- Before you can recover and reinstall a node where the KMS configuration was lost and the KMS key is not recoverable.
- Before returning any appliance that was previously in use at your site.
- After decommissioning a appliance that had node encryption enabled.



Decommission the appliance before clearing KMS to move its data to other nodes in your StorageGRID system. Clearing KMS before decommissioning the appliance will result in data loss and might render the appliance inoperable.

### 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 **Configure Hardware > Node Encryption**.



If the KMS configuration is cleared, data on the appliance will be permanently deleted. This data is not recoverable.

3. At the bottom of the window, select **Clear KMS Key and Delete Data**.
4. If you are sure that you want to clear the KMS configuration, type **clear** in the warning dialog box and select **Clear KMS Key and Delete Data**.

The KMS encryption key and all data are deleted from the node, and the appliance reboots. This can take up to 20 minutes.

5. 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.

6. Select **Configure Hardware > Node Encryption**.
7. Verify that node encryption is disabled and that the key and certificate information in **Key Management Server Details** and the **Clear KMS Key and Delete Data** control are removed from the window.

Node encryption can't be reenabled on the appliance until it is reinstalled in a grid.

### After you finish

After the appliance reboots and you have verified that KMS has been cleared and that the appliance is in a pre-install state, you can physically remove the appliance from your StorageGRID system. See the [instructions for preparing the appliance for reinstallation](#).

## Appliance node cloning

### Appliance node cloning: Overview

You can clone an appliance node in StorageGRID to use an appliance of newer design or increased capabilities. Cloning transfers all information about the existing node to the new appliance, provides a hardware-upgrade process that is easy to perform, and provides an alternative to decommissioning and expansion for replacing appliances.

Appliance node cloning lets you easily replace an existing appliance node (source) in your grid with a compatible appliance (target) that is part of the same logical StorageGRID site. The process transfers all data to the new appliance, placing it in service to replace the old appliance node and leaving the old appliance in a pre-install state.

### Why clone an appliance node?

You can clone an appliance node if you need to:

- Replace appliances that are reaching end-of-life.
- Upgrade existing nodes to take advantage of improved appliance technology.
- Increase grid storage capacity without changing the number of Storage Nodes in your StorageGRID system.
- Improve storage efficiency, such as by changing the RAID mode from DDP-8 to DDP-16, or to RAID-6.

- Efficiently implement node encryption to allow the use of external key management servers (KMS).

### **Which StorageGRID network is used?**

Cloning transfers data from the source node directly to the target appliance over any of the three StorageGRID networks. The Grid Network is typically used, but you can also use the Admin Network or the Client Network if the source appliance is connected to these networks. Choose the network to use for cloning traffic that provides the best data-transfer performance without degrading StorageGRID network performance or data availability.

When you install the replacement appliance, you must specify temporary IP addresses for StorageGRID connection and data transfer. Because the replacement appliance will be part of the same networks as the appliance node it replaces, you must specify temporary IP addresses for each of these networks on the replacement appliance.

### **Target appliance compatibility**

Replacement appliances must be the same type as the source node they are replacing and both must be part of the same logical StorageGRID site.

- A replacement services appliance can be different than the Admin Node or Gateway Node it is replacing.
  - You can clone an SG100 source node appliance to an SG1000 services target appliance to give the Admin Node or Gateway Node greater capability.
  - You can clone an SG1000 source node appliance to an SG100 services target appliance to redeploy the SG1000 for a more demanding application.

For example, if an SG1000 source node appliance is being used as an Admin Node and you want to use it as a dedicated load-balancing node.

- Replacing an SG1000 source node appliance with an SG100 services target appliance reduces the maximum speed of the network ports from 100-GbE to 25-GbE.
  - The services appliances have different network connectors. Changing the appliance type might require replacing the cables or SFP modules.
- A replacement storage appliance must have greater capacity than the Storage Node it is replacing.
    - If the target storage appliance has the same number of drives as the source node, the drives in the target appliance must have greater capacity (in TB).
    - If you plan to use the same RAID mode on the target node as was used on the source node, or a less storage efficient RAID mode (for example, switching from RAID 6 to DDP), the drives in the target appliance must be larger (in TB) than the drives in the source appliance.
    - If the number of standard drives installed in a target storage appliance is less than the number of drives in the source node, due to installation of solid-state drives (SSDs), the overall storage capacity of the standard drives in the target appliance (in TB) must exceed the total functional drive capacity of all drives in the source Storage Node.

For example, when cloning an SG5760 source Storage Node appliance with 60 drives to an SG6060 target appliance with 58 standard drives, larger drives should be installed in the SG6060 target appliance before cloning to maintain storage capacity. (The two drive slots containing SSDs in the target appliance aren't included in the total appliance-storage capacity.)

However, if a 60-drive SG5760 source node appliance is configured with SANtricity Dynamic Disk Pools DDP-8, configuring a 58-drive same-size-drive SG6060 target appliance with DDP-16 might

make the SG6060 appliance a valid clone target due to its improved storage efficiency.

You can view information about the current RAID mode of the source appliance node on the **NODES** page in Grid Manager. Select the **Storage** tab for the appliance.

- The number of volumes in a target storage appliance must be greater than or equal to the number of volumes in the source node. You cannot clone a source node with 16 object store volumes (rangedb) to a target storage appliance with 12 object store volumes even if the target appliance has larger capacity than the source node. Most storage appliances have 16 object store volumes, except the SGF6112 storage appliance that has only 12 object store volumes.

### What information is not cloned?

The following appliance configurations don't transfer to the replacement appliance during cloning. You must configure them during initial set up of the replacement appliance.

- BMC interface
- Network links
- Node encryption status
- SANtricity System Manager (for Storage Nodes)
- RAID mode (for Storage Nodes)

### What issues prevent cloning?

If any of the following issues are encountered while cloning, the cloning process halts and an error message is generated:

- Wrong network configuration
- Lack of connectivity between the source and target appliances
- Source and target appliance incompatibility
- For Storage Nodes, a replacement appliance of insufficient capacity

You must resolve each issue for cloning to continue.

## Considerations and requirements for appliance node cloning

Before cloning an appliance node, you must understand the considerations and requirements.

### Hardware requirements for the replacement appliance

Ensure that the replacement appliance meets the following criteria:

- The source node (appliance being replaced) and the target (new) appliance must be the same type of appliance:
  - You can only clone an Admin Node appliance or a Gateway Node appliance to a new services appliance.
  - You can only clone a Storage Node appliance to a new storage appliance.
- For Admin Node or Gateway Node appliances, the source node appliance and the target appliance don't need to be the same appliance model; however, changing the appliance model might require replacing the



cables or SFP modules.

For example, you can replace a SG1000 node appliance with a SG100 or replace a SG100 appliance with a SG1000 appliance.

- For Storage Node appliances, the source node appliance and the target appliance don't need to be the same type of appliance; however:

- The target appliance must have greater storage capacity than the source appliance.

For example, you can replace a SG5700 node appliance with a SG6000 appliance.

- The target appliance must have an equal or greater number of object storage volumes than the source appliance.

For example, you cannot replace a SG6000 node appliance (16 object store volumes) with a SGF6112 appliance (12 object store volumes).

Contact your StorageGRID sales representative for help choosing compatible replacement appliances to clone specific appliance nodes in your StorageGRID installation.

### Prepare to clone an appliance node

You must have the following information before you clone an appliance node:

- Obtain a temporary IP address for the Grid Network from your network administrator for use with the target appliance during initial installation. If the source node belongs to an Admin Network or Client Network, obtain temporary IP addresses for these networks.

Temporary IP addresses are normally on the same subnet as the source node appliance being cloned and aren't needed after cloning completes. The source and target appliances must both connect to the primary Admin Node of your StorageGRID to establish a cloning connection.

- Determine which network to use for cloning data-transfer traffic that provides the best data-transfer performance without degrading StorageGRID network performance or data availability.



Using the 1-GbE Admin Network for clone data transfer results in slower cloning.

- Determine if node encryption using a key management server (KMS) will be used on the target appliance, so that you can enable node encryption during initial target appliance installation before cloning. You can check if node encryption is enabled on the source appliance node as described in the [enabling node encryption](#).

The source node and target appliance can have different node-encryption settings. Data decryption and encryption is performed automatically during data transfer and when the target node restarts and joins the grid.

- Determine if the RAID mode on the target appliance should be changed from its default setting, so you can specify this information during initial target appliance installation before cloning. You can view information about the current RAID mode of the source appliance node on the **NODES** page in Grid Manager. Select the **Hardware** tab for the appliance.

The source node and target appliance can have different RAID settings.

- Plan for sufficient time to complete the node cloning process. Several days might be required to transfer

data from an operational Storage Node to a target appliance. Schedule cloning at a time that minimizes the impact to your business.

- You should only clone one appliance node at a time. Cloning can prevent you from performing other StorageGRID maintenance functions at the same time.
- After you have cloned an appliance node, you can use the source appliance that was returned to a pre-install state as the target to clone another compatible node appliance.

## Clone appliance node

The cloning process might take several days to transfer data between the source node (appliance being replaced) and the target (new) appliance.

### Before you begin

- You have installed the compatible target appliance into a cabinet or rack, connected all cables, and applied power.
- You have verified that the StorageGRID Appliance Installer version on the replacement appliance matches the software version of your StorageGRID system, upgrading and downgrading the StorageGRID Appliance Installer firmware, if necessary.
- You have configured the target appliance, including configuring StorageGRID connections, SANtricity System Manager (storage appliances only), and the BMC interface.
  - When configuring StorageGRID connections, use the temporary IP addresses.
  - When configuring network links, use the final link configuration.



Leave the StorageGRID Appliance Installer open after you complete initial target appliance configuration. You will return to the target appliance's installer page after you start the node cloning process.

- You have optionally enabled node encryption for the target appliance.
- You have optionally set the RAID mode for the target appliance (storage appliances only).
- You have reviewed the [considerations and requirements for appliance node cloning](#).

You should clone only one appliance node at a time to maintain StorageGRID network performance and data availability.

### Steps

1. [Place the source node you are cloning into maintenance mode](#).
2. From the StorageGRID Appliance Installer on the source node, in the Installation section of the Home page, select **Enable Cloning**.

The Primary Admin Node connection section is replaced with the Clone target node connection section.

NetApp® StorageGRID® Appliance Installer Help

Home   Configure Networking ▾   Configure Hardware ▾   Monitor Installation   Advanced ▾

Home

**⚠** This node is in maintenance mode. Perform any required maintenance procedures. If you want to exit maintenance mode manually to resume normal operation, go to Advanced > Reboot Controller to **reboot** the controller.

**This Node**

Node type: Storage ▾

Node name: hrmny2-1-254-sn

Cancel   Save

**Clone target node connection**

Clone target node IP: 0.0.0.0

Connection state: No connection information available.

Cancel   Save

**Installation**

Current state: Waiting for configuration and validation of clone target.

Start Cloning   Disable Cloning

- For **Clone target node IP**, enter the temporary IP address assigned to the target node for the network to use for clone data-transfer traffic, and then select **Save**.

Typically, you enter the IP address for the Grid Network, but if you need to use a different network for clone data-transfer traffic, enter the IP address of the target node on that network.



Using the 1-GbE Admin Network for clone data transfer results in slower cloning.

After the target appliance is configured and validated, in the Installation section, **Start Cloning** is enabled on the source node.

If issues exist that prevent cloning, **Start Cloning** is not enabled and issues that you must resolve are listed as the **Connection state**. These issues are listed on the StorageGRID Appliance Installer Home page of both the source node and the target appliance. Only one issue displays at a time and the state automatically updates as conditions change. Resolve all cloning issues to enable **Start Cloning**.

When **Start Cloning** is enabled, the **Current state** indicates the StorageGRID network that was selected for cloning traffic, along with information about using that network connection. See [Considerations and requirements for appliance node cloning](#).

- Select **Start Cloning** on the source node.
- Monitor the cloning progress using the StorageGRID Appliance Installer on either the source or target

node.

The StorageGRID Appliance Installer on both the source and target nodes indicate similar status.

NetApp® StorageGRID® Appliance Installer Help

Home | Configure Networking ▾ | Configure Hardware ▾ | Monitor Installation | Advanced ▾

### Monitor Cloning

1. Establish clone peering relationship	Complete
2. Clone another node from this node	Running
3. Activate cloned node and leave this one offline	Pending

Step	Progress	Status
Send data to clone target node	<div style="width: 0%;"></div>	Sending data, 0% complete, 8.99 GB transferred

The Monitor Cloning page provides detailed progress for each stage of the cloning process:

- **Establish clone peering relationship** shows the progress of cloning set up and configuration.
  - **Clone another node from this node** shows the progress of data transfer. (This part of the cloning process can take several days to complete.)
  - **Activate cloned node and leave this one offline** shows the progress of transferring control to the target node and placing the source node in a pre-install state, after data transfer is complete.
6. If you need to terminate the cloning process and return the source node to service before cloning is complete, on the source node go to the StorageGRID Appliance Installer Home page and select **Advanced > Reboot Controller**, and then select **Reboot into StorageGRID**.

If the cloning process is terminated:

- The source node exits maintenance mode and rejoins StorageGRID.
- The target node remains in the pre-install state.  
To restart cloning the source node, start the cloning process again from step 1.

When cloning successfully completes:

- The source and target nodes swap IP addresses:
  - The target node now uses the IP addresses originally assigned to the source node for the Grid, Admin, and Client Networks.
  - The source node now uses the temporary IP address initially assigned to the target node.
- The target node exits maintenance mode and joins StorageGRID, replacing the source node.
- The source appliance is in a pre-installed state, as if you had [prepared it for reinstallation](#).



If the target appliance does not join the grid, go to the StorageGRID Appliance Installer Home page for the source node, select **Advanced > Reboot Controller**, and then select **Reboot into Maintenance Mode**. After the source node reboots in maintenance mode, repeat the node cloning procedure.

- User data remains on the source appliance as a recovery option if an unexpected issue occurs with the target node. After the target node has successfully joined StorageGRID, user data on the source appliance is outdated and is no longer needed.

Outdated user data is overwritten when you install or expand the source appliance as a new node in another grid.

You can also reset the controller configuration on the source appliance to make this data inaccessible:

1. Open the [StorageGRID Appliance Installer](#) for the source appliance using the temporary IP address initially assigned to the target node.
2. Select **Help > Support and Debug Tools**.
3. Select **Reset Storage Controller Configuration**.



If needed, contact technical support for assistance resetting the storage controller configuration.



Overwriting the data or resetting the controller configuration makes the outdated data difficult or impossible to retrieve; however, neither method securely removes the data from the source appliance. If a secure erase is required, use a data-wiping tool or service to permanently and securely remove data from the source appliance.

You can:

- Use the source appliance as a target for additional cloning operations: no additional configuration is required. This appliance already has the temporary IP address assigned that were originally specified for the first clone target.
- Install and set up the source appliance as a new appliance node.
- Discard the source appliance if it is no longer of use with StorageGRID.

## Maintain SG1000 and SG100 services appliance hardware

### Maintain SG100 and SG1000 appliances

You might need to perform maintenance procedures on the appliance. The procedures in this section assume that the appliance has already been deployed as a Gateway Node or an Admin Node in a StorageGRID system.

Procedures specific to maintaining your SG100 or SG1000 appliance are in this section.

See [Common procedures](#) for maintenance procedures that are used by all appliances.

See [Set up hardware](#) for maintenance procedures that are also performed during initial appliance installation and configuration.

### Maintenance configuration procedures

## Turn SG100 or SG1000 identify LED on and off

The blue identify LED on the front and back of the controller can be turned on to help locate the appliance in a data center.

### Before you begin

You have the BMC IP address of the controller you want to identify.

### Steps

1. Access the appliance BMC interface.
2. Select **Server Identify**.

The current status of the identify LED is selected.

3. Select **ON** or **OFF**, and then select **Perform Action**.

When you select **ON**, the blue identify LEDs light on the front (shown) and rear of the appliance.



If a bezel is installed on the controller, it might be difficult to see the front identify LED.

4. Turn the LED on and off as needed.

### Related information

[Locate controller in data center](#)

[Access BMC interface](#)

## Locate SG100 or SG1000 in data center

Locate the controller so that you can perform hardware maintenance or upgrades.

### Before you begin

- You have determined which controller requires maintenance.
- (Optional) To help locate the controller in your data center, [turn on the blue identify LED](#).

### Steps

1. Find the controller requiring maintenance in the data center.
  - Look for a lit blue identify LED on the front or rear of the controller.

The front identify LED is behind the controller front bezel and might be difficult to see if the bezel is installed.



- Check the tags attached to the front of each controller for a matching part number.
- 2. Remove the controller front bezel, if one is installed, to access the front panel controls and indicators.
- 3. Optional: [Turn off the blue identify LED](#) if you used it to locate the controller.
  - Press the identify LED switch on the controller front panel.
  - Use the controller BMC interface.

## Shut down the SG100 or SG1000

Shut down the services appliance to perform hardware maintenance.

### Before you begin

- You have physically [located the services appliance](#) requiring maintenance in the data center.

### About this task

To prevent service interruptions, shut down the services appliance during a scheduled maintenance window when periods of service disruption are acceptable.

### Steps

1. Shut down the appliance:



You must perform a controlled shut down of the appliance by entering the commands specified below. It is a best practice to perform a controlled shutdown when possible to avoid unnecessary alerts, ensure full logs are available, and avoid service disruptions.

- a. If you have not already logged into the grid node, log in using PuTTY or another ssh client:
  - i. Enter the following command: `ssh admin@grid_node_IP`
  - ii. Enter the password listed in the `Passwords.txt` file.
  - iii. Enter the following command to switch to root: `su -`
  - iv. Enter the password listed in the `Passwords.txt` file.

When you are logged in as root, the prompt changes from `$` to `#`.

b. Shut down the services appliance:

```
shutdown -h now
```

This command might take up to 10 minutes to complete.

2. Use one of the following methods to verify that the appliance is powered off:

- Look at the power LED on the front of the appliance and confirm that it is off.
- Check the Power Control page of the BMC interface to confirm the appliance is off.

### Change link configuration of SG100 or SG1000

You can change the Ethernet link configuration of the services appliance. You can change the port bond mode, the network bond mode, and the link speed.

#### Before you begin

- You have [placed the appliance into maintenance mode](#).



In rare instances, placing a StorageGRID appliance into maintenance mode might make the appliance unavailable for remote access.

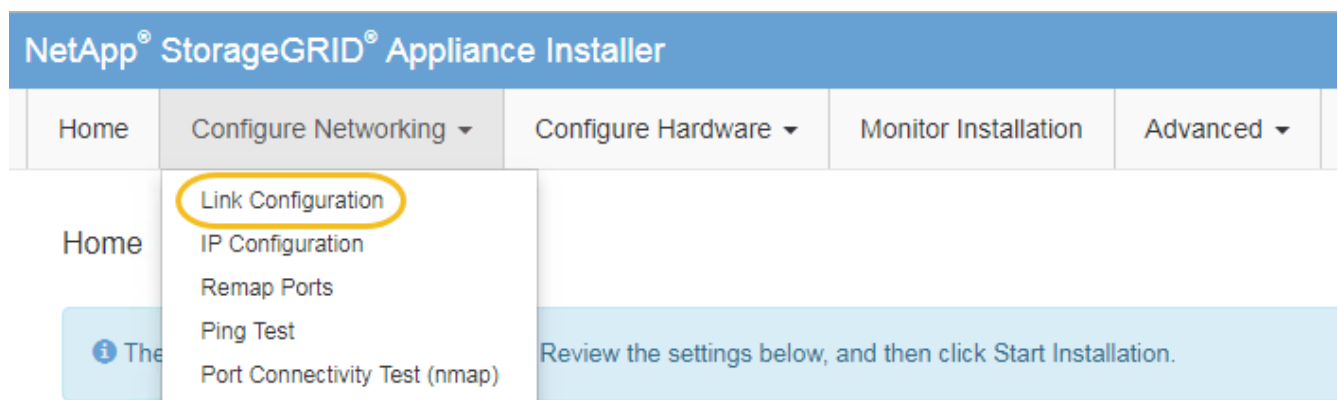
#### About this task

Options for changing the Ethernet link configuration of the services appliance include:

- Changing **Port bond mode** from Fixed to Aggregate, or from Aggregate to Fixed
- Changing **Network bond mode** from Active-Backup to LACP, or from LACP to Active-Backup
- Enabling or disabling VLAN tagging, or changing the value of a VLAN tag
- Changing the link speed

#### Steps

1. From the StorageGRID Appliance Installer, select **Configure Networking > Link Configuration**.



2. Make the desired changes to the link configuration.

For more information about the options, see [Configure network links](#).

3. 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://services_appliance_IP:8443`**

4. Make any necessary changes to the IP addresses for the appliance.

If you made changes to the VLAN settings, the subnet for the appliance might have changed. If you need to change the IP addresses for the appliance, see [Configure StorageGRID IP addresses](#).

5. Select **Configure Networking > Ping Test** from the menu.


6. Use the Ping Test tool to check connectivity to IP addresses on any networks that might have been affected by the link configuration changes you made when configuring the appliance.

In addition to any other tests you choose to perform, confirm that you can ping the Grid Network IP address of the primary Admin Node, and the Grid Network IP address of at least one other node. If necessary, return to the instructions for configuring network links, and correct any issues.

7. Once you are satisfied that your link configuration changes are working, reboot the node. From the StorageGRID Appliance Installer, select **Advanced > Reboot Controller**, and then select one of these options:

- Select **Reboot into StorageGRID** to reboot the controller with the node rejoining the grid. Select this option if you are done working in maintenance mode and are ready to return the node to normal operation.
- Select **Reboot into Maintenance Mode** to reboot the controller with the node remaining in maintenance mode. (This option is available only when the controller is in maintenance mode.) Select this option if there are additional maintenance operations you need to perform on the node before rejoining the grid.



It can take up to 20 minutes for the appliance to reboot and rejoin the grid. To confirm that the reboot is complete and that the node has rejoined the grid, go back to the Grid Manager. The **NODES** page should display a normal status (green check mark icon  to the left of the node name) for the appliance node, indicating that no alerts are active and the node is connected to the grid.

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
Data Center 1	Site	0%	0%	—
DC1-ADM1	Primary Admin Node	—	—	21%
DC1-ARC1	Archive Node	—	—	8%
DC1-G1	Gateway Node	—	—	10%
DC1-S1	Storage Node	0%	0%	29%

## Hardware procedures

### Replace one or both power supplies in the SG100 or SG1000

The services appliance has two power supplies for redundancy. If one of the power supplies fails, you must replace it as soon as possible to ensure that the compute controller has redundant power. Both power supplies operating in the controller must be the same model and wattage.

#### Before you begin

- You have [physically located the controller](#) with the power supply to be replaced.
- If you are replacing only one power supply:
  - You have unpacked the replacement power supply unit and ensured that it is the same model and wattage as the power supply unit you are replacing.
  - You have confirmed that the other power supply is installed and running.
- If you are replacing both power supplies at the same time:
  - You have unpacked the replacement power supply units and ensured they are the same model and wattage.

#### About this task

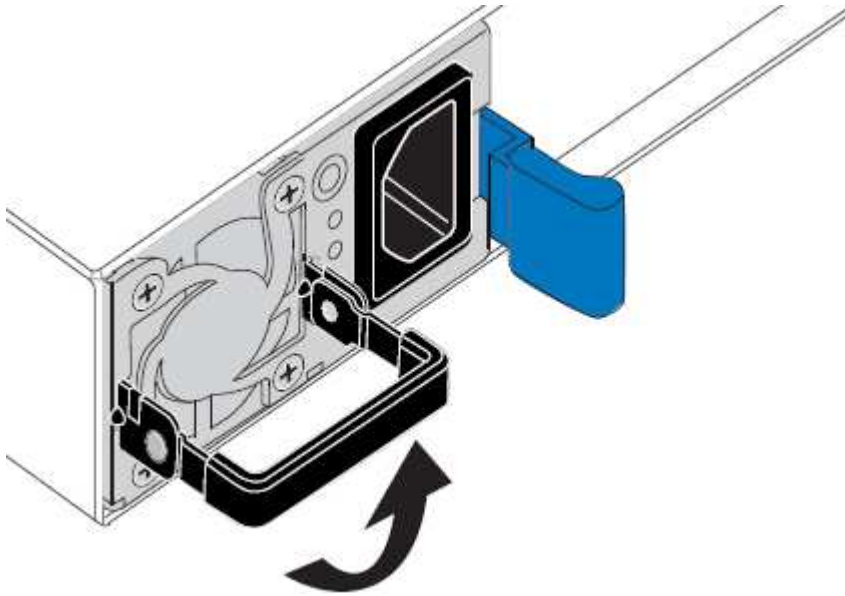
The figure shows the two power supply units for the SG100, which are accessible from the back of the appliance.



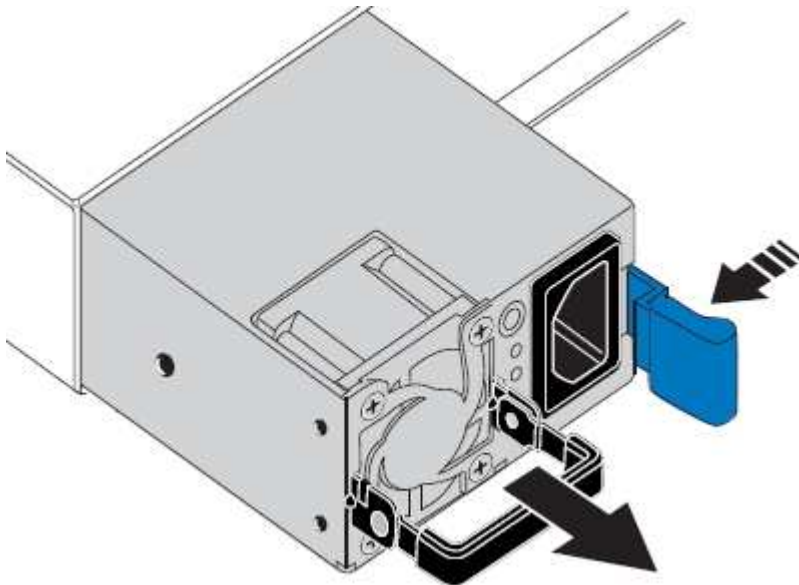
The power supplies for the SG1000 are identical.

## Steps

1. If you are replacing only one power supply, you don't need to shut down the appliance. Go to the [Unplug the power cord](#) step. If you are replacing both power supplies at the same time, do the following before unplugging the power cords:
  - a. [Shut down the appliance](#).
2. Unplug the power cord from each power supply to be replaced.
3. Lift the cam handle on the first supply to be replaced.



4. Press the blue latch and pull the power supply out.

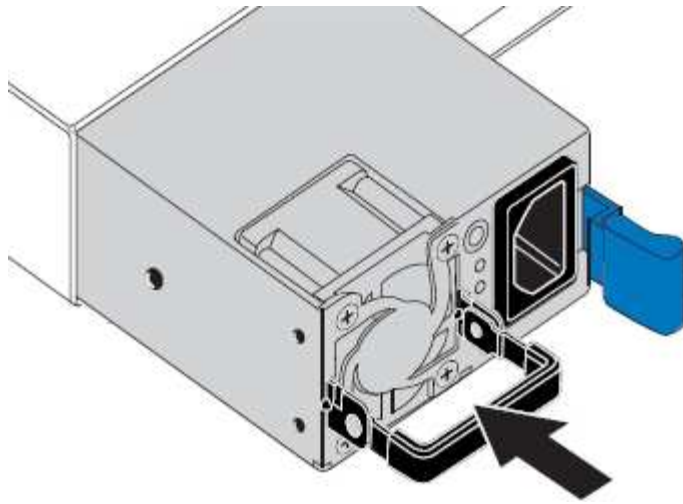


5. With the blue latch on the right, slide the replacement power supply into the chassis.



Both power supplies must be the same model and wattage.

Ensure that the blue latch is on the right side when you slide the replacement unit in.



6. Push the cam handle down to secure the replacement power supply.
7. If you are replacing both power supplies, repeat steps 2 through 6 to replace the second power supply.
8. [Connect the power cords to the replaced units and apply power.](#)

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return & Replacements](#) page for further information.

### Replace fan in SG100 or SG1000

The services appliance has eight cooling fans. If one of the fans fails, you must replace it as soon as possible to ensure that the appliance has proper cooling.

#### Before you begin

- You have unpacked the replacement fan.
- You have [physically located the appliance.](#)
- You have confirmed that the other fans are installed and running.

#### About this task

The appliance node will not be accessible while you replace the fan.

The photograph shows a fan for the services appliance. The cooling fans are accessible after you take the top cover off the appliance.



Each of the two power supply units also contain a fan. Those fans aren't included in this procedure.

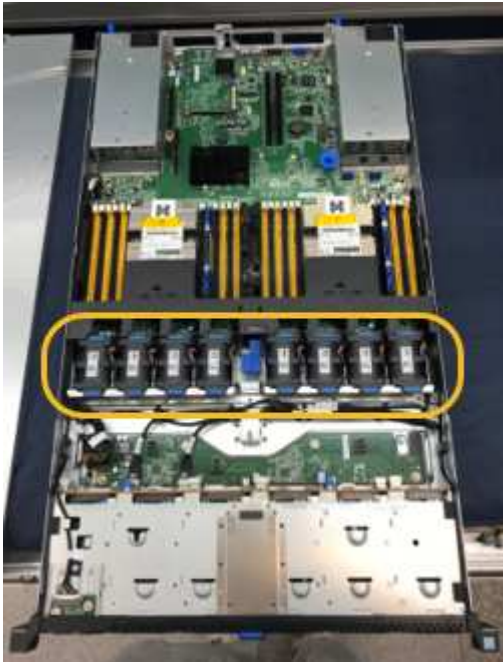


## Steps

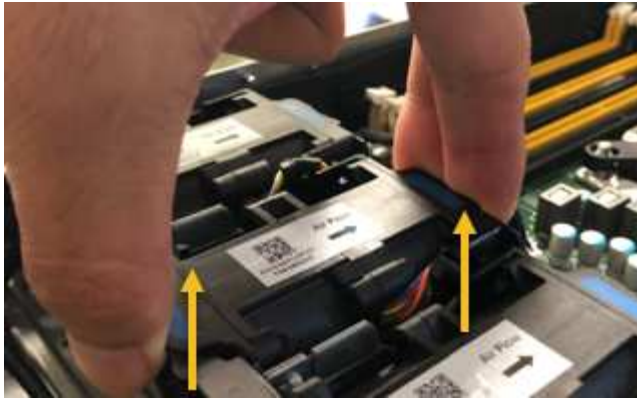
1. Shut down the appliance.
  - a. Log in to the grid node:
    - i. Enter the following command: `ssh admin@grid_node_IP`
    - ii. Enter the password listed in the `Passwords.txt` file.
    - iii. Enter the following command to switch to root: `su -`
    - iv. Enter the password listed in the `Passwords.txt` file.

When you are logged in as root, the prompt changes from `$` to `#`.

- b. Shut down the services appliance:  
**`shutdown -h now`**
2. Use one of two methods to verify that the power for the services appliance is off:
  - The power indicator LED on the front of the appliance is off.
  - The Power Control page of the BMC interface indicates that the appliance is off.
3. Pull the appliance out of the rack.
4. Lift the latch on the top cover and remove the cover from the appliance.
5. Locate the fan that failed.

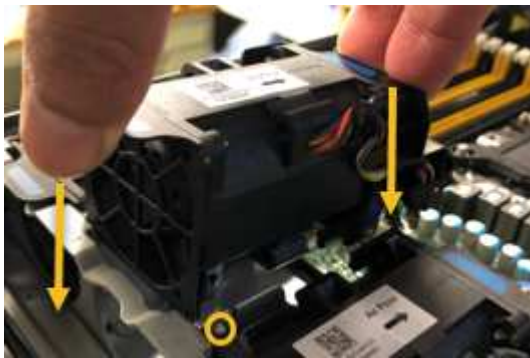


6. Lift the failed fan out of the chassis.



7. Slide the replacement fan into the open slot in the chassis.

Line up the edge of the fan with the guide pin. The pin is circled in the photograph.



8. Press the fan's connector firmly into the circuit board.



9. Put the top cover back on the appliance, and press the latch down to secure the cover in place.
10. Power on the appliance and monitor the controller LEDs and boot-up codes.

Use the BMC interface to monitor boot-up status.

11. Confirm that the appliance node appears in the Grid Manager and that no alerts appear.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return & Replacements](#) page for further information.

### Replace drive in SG100 or SG1000

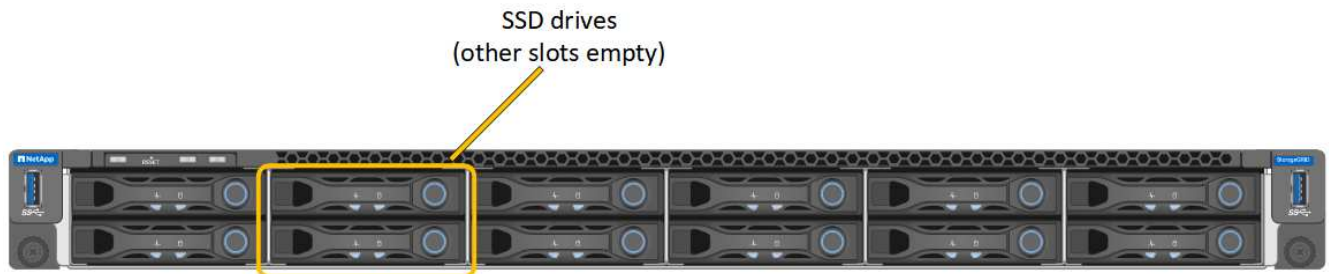
The SSDs in the services appliance contain the StorageGRID operating system. Additionally, when the appliance is configured as an Admin Node, the SSDs also contain

audit logs, metrics, and database tables. The drives are mirrored using RAID1 for redundancy. If one of the drives fails, you must replace it as soon as possible to ensure redundancy.

### Before you begin

- You have [physically located the appliance](#).
- You have verified which drive has failed by noting that its left LED is blinking amber.

The two SSDs are placed in the slots as shown in the following diagram:



If you remove the working drive, you will bring down the appliance node. See the information about viewing status indicators to verify the failure.

- You have obtained the replacement drive.
- You have obtained proper ESD protection.

### Steps

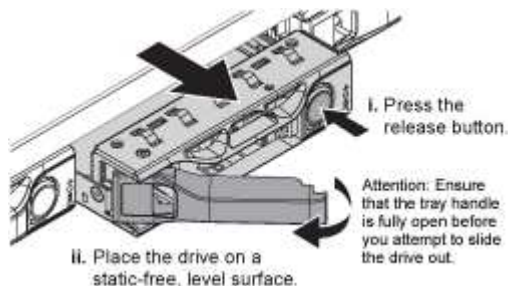
1. Verify that the drive to be replaced has the left LED blinking amber. If a drive issue was reported in the Grid Manager or BMC UIs, HDD02 or HDD2 refer to the drive in the upper slot, and HDD03 or HDD3 refer to the drive in the lower slot.

You can also use the Grid Manager to monitor the status of the SSDs. Select **NODES**. Then select **Appliance Node > Hardware**. If a drive has failed, the Storage RAID Mode field contains a message about which drive has failed.

2. Wrap the strap end of the ESD wristband around your wrist, and secure the clip end to a metal ground to prevent static discharge.
3. Unpack the replacement drive, and set it on a static-free, level surface near the appliance.

Save all packing materials.

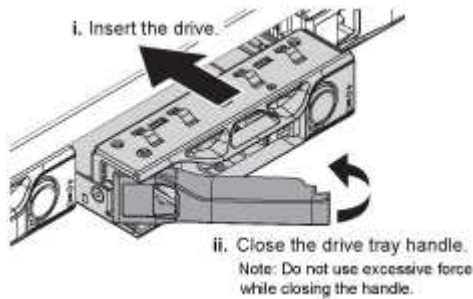
4. Press the release button on the failed drive.



The handle on the drive springs open partially, and the drive releases from the slot.

5. Open the handle, slide the drive out, and place it on a static-free, level surface.
6. Press the release button on the replacement drive before you insert it into the drive slot.

The latch springs open.



7. Insert the replacement drive in the slot, and then close the drive handle.



Don't use excessive force while closing the handle.

When the drive is fully inserted, you hear a click.

The drive is automatically rebuilt with mirrored data from the working drive. You can check the status of the rebuild by using the Grid Manager. Select **NODES**. Then select **Appliance Node > Hardware**. The Storage RAID Mode field contains a “rebuilding” message until the drive is completely rebuilt.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return & Replacements](#) page for further information.

## Replace an SG100 or SG1000

You might need to replace the appliance if it is not functioning optimally or if it has failed.

### Before you begin

- You have a replacement appliance with the same part number as the appliance you are replacing.
- You have labels to identify each cable that is connected to the appliance.
- You have [physically located the appliance](#).

### About this task

The StorageGRID node will not be accessible while you replace the appliance. If the appliance is functioning sufficiently, you can perform a controlled shutdown at the start of this procedure.



If you are replacing the appliance before installing StorageGRID software, you might not be able to access the StorageGRID Appliance Installer immediately after completing this procedure. While you can access the StorageGRID Appliance Installer from other hosts on the same subnet as the appliance, you can't access it from hosts on other subnets. This condition should resolve itself within 15 minutes (when any ARP cache entries for the original appliance time out), or you can clear the condition immediately by purging any old ARP cache entries manually from the local router or gateway.

### Steps

1. Display the current configurations of the appliance and record them.



- a. Log in to the appliance to be replaced:
  - i. Enter the following command: `ssh admin@grid_node_IP`
  - ii. Enter the password listed in the `Passwords.txt` file.
  - iii. Enter the following command to switch to root: `su -`
  - iv. Enter the password listed in the `Passwords.txt` file.

When you are logged in as root, the prompt changes from `$` to `#`.

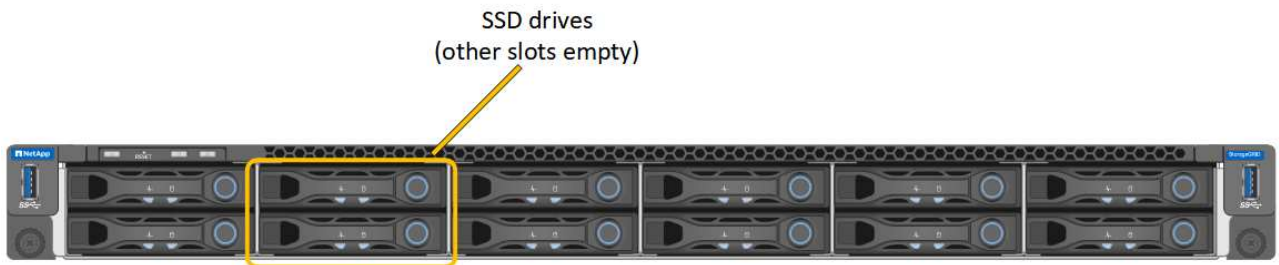
- b. Enter: **`run-host-command ipmitool lan print`** to display the current BMC configurations for the appliance.
2. Shut down the appliance: `shutdown -h now`
  3. If any of the network interfaces on this StorageGRID appliance are configured for DHCP, you might need to update the permanent DHCP lease assignments on the DHCP servers to reference the MAC addresses of the replacement appliance. The update ensures the appliance is assigned the expected IP addresses. See [Update MAC address references](#).
  4. Remove and replace the appliance:
    - a. Label the cables and then disconnect the cables and any network transceivers.



To prevent degraded performance, don't twist, fold, pinch, or step on the cables.

- b. Remove the failed appliance from the cabinet or rack.
- c. Transfer the two power supplies, eight cooling fans, and two SSDs from the failed appliance to the replacement appliance.

The two SSDs are placed in the slots as shown in the following diagram:



HDD02 or HDD2 refer to the drive in the upper slot, and HDD03 or HDD3 refer to the drive in the lower slot.

Follow the instructions provided for replacing these components.

- d. Install the replacement appliance into the cabinet or rack.
  - e. Replace the cables and any optical transceivers.
  - f. Power on the appliance and wait for it to rejoin the grid.
  - g. Confirm that the appliance node appears in the Grid Manager and that no alerts appear.
5. Log in to the replaced appliance:
    - a. Enter the following command: `ssh admin@grid_node_IP`

- b. Enter the password listed in the `Passwords.txt` file.
  - c. Enter the following command to switch to root: `su -`
  - d. Enter the password listed in the `Passwords.txt` file.
6. Restore BMC network connectivity for the replaced appliance. There are two options:
- Use static IP, netmask, and gateway
  - Use DHCP to obtain an IP, netmask, and gateway
- a. To restore the BMC configuration to use a static IP, netmask, and gateway, enter the following commands:

```
run-host-command ipmitool lan set 1 ipsrc static
```

```
run-host-command ipmitool lan set 1 ipaddr Appliance_IP
```

```
run-host-command ipmitool lan set 1 netmask Netmask_IP
```

```
run-host-command ipmitool lan set 1 defgw ipaddr Default_gateway
```

- b. To restore the BMC configuration to use DHCP to obtain an IP, netmask, and gateway, enter the following command:

```
run-host-command ipmitool lan set 1 ipsrc dhcp
```

7. After restoring BMC network connectivity, connect to the BMC interface to audit and restore any additional custom BMC configuration you might have applied. For example, you should confirm the settings for SNMP trap destinations and email notifications. See [Configure BMC interface](#).
8. Confirm that the appliance node appears in the Grid Manager and that no alerts appear.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return & Replacements](#) page for further information.

#### Related information

[View status indicators](#)

[View boot-up codes for appliance](#)

## Maintain SG5600 hardware

### Maintain SG5600 appliance

The SG5600 appliance has reached End Of Support. Contact your NetApp Sales Representative for hardware refresh options.

If you need to perform maintenance procedures on SG5600 hardware, use the [StorageGRID 11.6 instructions](#).

## Maintain SG5700 storage appliance hardware

## Maintain SG5700 appliance

You might need to upgrade the SANtricity OS Software on the E2800 controller, change the Ethernet link configuration of the E5700SG controller, replace the E2800 controller or the E5700SG controller, or replace specific components. The procedures in this section assume that the appliance has already been deployed as a Storage Node in a StorageGRID system.

Procedures specific to maintaining your SG5700 appliance are in this section.

See [Common procedures](#) for maintenance procedures that are used by all appliances.

See [Set up hardware](#) for maintenance procedures that are also performed during initial appliance installation and configuration.

## Maintenance configuration procedures

### Upgrade SANtricity OS on SG5700 storage controller

To ensure optimal functioning of the storage controller, you must upgrade to the latest maintenance release of the SANtricity OS that is qualified for your StorageGRID appliance.

Consult the [NetApp Interoperability Matrix Tool \(IMT\)](#) to determine which version you should be using.

Download the new SANtricity OS Software file from [NetApp Downloads: StorageGRID Appliance](#).

Use one of the following procedures based on the version of SANtricity OS currently installed:

- If the storage controller is using SANtricity OS 08.42.20.00 (11.42) or newer, use the Grid Manager to perform the upgrade.

[Upgrade SANtricity OS on storage controllers using Grid Manager](#)

- If the storage controller is using a SANtricity OS version older than 08.42.20.00 (11.42), use maintenance mode to perform the upgrade.

[Upgrade SANtricity OS on E2800 controller using maintenance mode](#)

### Upgrade SANtricity OS on SG5700 storage controllers using Grid Manager

For storage controllers currently using SANtricity OS 08.42.20.00 (11.42) or newer, you must use the Grid Manager to apply an upgrade.

#### Before you begin

- You have consulted the [NetApp Interoperability Matrix Tool \(IMT\)](#) to confirm that the SANtricity OS version you are using for the upgrade is compatible with your appliance.
- You have the [Maintenance or Root access permission](#).
- You are signed in to the Grid Manager using a [supported web browser](#).
- You have the provisioning passphrase.

- You have access to [NetApp Downloads: StorageGRID Appliance](#).

### About this task

You can't perform other software updates (StorageGRID software upgrade or a hotfix) until you have completed the SANtricity OS upgrade process. If you attempt to start a hotfix or a StorageGRID software upgrade before the SANtricity OS upgrade process has finished, you are redirected to the SANtricity OS upgrade page.

The procedure will not be complete until the SANtricity OS upgrade has been successfully applied to all applicable nodes that have been selected for the upgrade. It might take more than 30 minutes to load the SANtricity OS on each node (sequentially) and up to 90 minutes to reboot each StorageGRID storage appliance. Any nodes in your grid that don't use SANtricity OS will not be affected by this procedure.



The following steps are only applicable when you are using the Grid Manager to perform the upgrade. The storage controllers in the appliance can't be upgraded using the Grid Manager when the controllers are using SANtricity OS older than 08.42.20.00 (11.42).



This procedure will automatically upgrade the NVSRAM to the most recent version associated with the SANtricity OS upgrade. You don't need to apply a separate NVSRAM upgrade file.



Be sure to apply the latest StorageGRID hotfix before you begin this procedure. See [StorageGRID hotfix procedure](#) for details.

### Steps

1. Download the new SANtricity OS Software file from [NetApp Downloads: StorageGRID Appliance](#).

Be sure to choose the SANtricity OS version for your storage controllers.

2. Select **MAINTENANCE > System > Software update**.

**Software update**

You can upgrade StorageGRID software, apply a hotfix, or upgrade the SANtricity OS software on StorageGRID storage appliances. NetApp recommends you apply the latest hotfix before and after each software upgrade. Some hotfixes are required to prevent data loss.

StorageGRID upgrade	StorageGRID hotfix	SANtricity OS update
Upgrade to the next StorageGRID version and apply the latest hotfix for that version.	Apply a hotfix to your current StorageGRID software version.	Update the SANtricity OS software on your StorageGRID storage appliances.
<a href="#">Upgrade →</a>	<a href="#">Apply hotfix →</a>	<a href="#">Update →</a>

3. In the SANtricity OS update section, select **Update**.

The SANtricity OS upgrade page appears and lists the details for each appliance node including:

- Node name
- Site
- Appliance model
- SANtricity OS version
- Status
- Last upgrade status

4. Review the information in the table for all of your upgradable appliances. Confirm that all storage controllers have **Nominal** status. If the status for any controller is **Unknown**, go to **Nodes > appliance node > Hardware** to investigate and resolve the issue.
5. Select the SANtricity OS upgrade file you downloaded from the NetApp Support Site.
  - a. Select **Browse**.
  - b. Locate and select the file.
  - c. Select **Open**.

The file is uploaded and validated. When the validation process is done, the file name is shown with a green check mark next to the **Browse** button. Don't change the file name because it is part of the verification process.

6. Enter the provisioning passphrase and select **Continue**.

A warning box appears stating that your browser's connection might be lost temporarily as services on nodes that are upgraded are restarted.

7. Select **Yes** to stage the SANtricity OS upgrade file to the primary Admin Node.

When the SANtricity OS upgrade starts:

- a. The health check is run. This process checks that no nodes have the status of Needs Attention.



If any errors are reported, resolve them and select **Start** again.

- b. The SANtricity OS Upgrade Progress table appears. This table shows all Storage Nodes in your grid and the current stage of the upgrade for each node.



The table shows all appliance Storage Nodes. Software-based Storage Nodes aren't displayed. Select **Approve** for all nodes that require the upgrade.

## SANtricity OS

Upload files —  **2** Upgrade

Approved nodes are added to a queue and upgraded sequentially. Each node can take up to 30 minutes, which includes updating NVSRAM. When the upgrade is complete, the node is rebooted.

Select **Approve all** or approve nodes one at a time. To remove nodes from the queue, select **Remove all** or remove nodes one at a time. If the uploaded file doesn't apply to an approved node, the upgrade process skips that node and moves to the next node in the queue.

Optionally, select **Skip nodes and finish** to end the upgrade and skip any unapproved nodes.

SANtricity OS upgrade file: RCB\_11.70.3\_280x\_6283a64d.dlp

0 out of 3 completed

Node name	Current version	Progress	Stage	Details	Status	Actions
10-224-2-24-S1	08.40.60.01	<div style="width: 100%; height: 10px; background-color: #4f81bd;"></div>	Waiting for you to approve		Nominal	<a href="#">Approve</a>
lab-37-sgws- quanta-10	08.73.00.00	<div style="width: 100%; height: 10px; background-color: #4f81bd;"></div>	Waiting for you to approve		Nominal	<a href="#">Approve</a>
storage-7	98.72.09.00	<div style="width: 100%; height: 10px; background-color: #4f81bd;"></div>	Waiting for you to approve		Nominal	<a href="#">Approve</a>

8. Optionally, sort the list of nodes in ascending or descending order by:

- Node name
- Current version
- Progress
- Stage
- Status

You can also enter a term in the Search box to search for specific nodes.

9. Approve the grid nodes you are ready to add to the upgrade queue. Approved nodes are upgraded one at a time.



Don't approve the SANtricity OS upgrade for an appliance Storage Node unless you are sure the node is ready to be stopped and rebooted. When the SANtricity OS upgrade is approved on a node, the services on that node are stopped and the upgrade process begins. Later, when the node is finished upgrading, the appliance node is rebooted. These operations might cause service interruptions for clients that are communicating with the node.

- Select the **Approve All** button to add all Storage Nodes to the SANtricity OS upgrade queue.



If the order in which nodes are upgraded is important, approve nodes or groups of nodes one at a time and wait until the upgrade is complete on each node before approving the next node.

- Select one or more **Approve** buttons to add one or more nodes to the SANtricity OS upgrade queue. The **Approve** button is disabled if the Status is not Nominal.

After you select **Approve**, the upgrade process determines if the node can be upgraded. If a node can be upgraded, it is added to the upgrade queue.

For some nodes, the selected upgrade file is intentionally not applied and you can complete the upgrade process without upgrading these specific nodes. Nodes intentionally not upgraded show a stage of Complete (upgrade attempted) and list the reason the node was not upgraded in the Details column.

10. If you need to remove a node or all nodes from the SANtricity OS upgrade queue, select **Remove** or **Remove All**.

When the stage progresses beyond Queued, the **Remove** button is hidden and you can no longer remove the node from the SANtricity OS upgrade process.

11. Wait while the SANtricity OS upgrade is applied to each approved grid node.

- If any node shows a stage of Error while the SANtricity OS upgrade is applied, the upgrade has failed for the node. With the assistance of technical support, you might need to place the appliance in maintenance mode to recover it.
- If the firmware on the node is too old to be upgraded with the Grid Manager, the node shows a stage of Error with the details that you must use maintenance mode to upgrade SANtricity OS on the node. To resolve the error, do the following:
  - a. Use maintenance mode to upgrade SANtricity OS on the node that shows a stage of Error.
  - b. Use the Grid Manager to restart and complete the SANtricity OS upgrade.

When the SANtricity OS upgrade is complete on all approved nodes, the SANtricity OS Upgrade Progress table closes and a green banner shows the number of nodes upgraded, and the date and time the upgrade completed.

12. If a node can't be upgraded, note the reason shown in the Details column and take the appropriate action.



The SANtricity OS upgrade process will not be complete until you approve the SANtricity OS upgrade on all the listed Storage Nodes.

Reason	Recommended action
Storage Node was already upgraded.	No further action required.
SANtricity OS upgrade is not applicable to this node.	The node does not have a storage controller that can be managed by the StorageGRID system. Complete the upgrade process without upgrading the node displaying this message.

Reason	Recommended action
SANtricity OS file is not compatible with this node.	The node requires a SANtricity OS file different than the one you selected. After completing the current upgrade, download the correct SANtricity OS file for the node and repeat the upgrade process.

13. If you want to end approving nodes and return to the SANtricity OS page to allow for an upload of a new SANtricity OS file, do the following:

a. Select **Skip Nodes and Finish**.

A warning appears asking if you are sure you want to finish the upgrade process without upgrading all applicable nodes.

b. Select **OK** to return to the **SANtricity OS** page.

c. When you are ready to continue approving nodes, [download the SANtricity OS](#) to restart the upgrade process.



Nodes already approved and upgraded without errors remain upgraded.

14. Repeat this upgrade procedure for any nodes with a stage of Complete that require a different SANtricity OS upgrade file.



For any nodes with a status of Needs Attention, use maintenance mode to perform the upgrade.

### Related information

[NetApp Interoperability Matrix Tool](#)

[Upgrade SANtricity OS on E2800 controller using maintenance mode](#)

#### Upgrade SANtricity OS on E2800 controller using maintenance mode

For storage controllers currently using SANtricity OS older than 08.42.20.00 (11.42), you must use the maintenance mode procedure to apply an upgrade.

#### Before you begin

- You have consulted the [NetApp Interoperability Matrix Tool \(IMT\)](#) to confirm that the SANtricity OS version you are using for the upgrade is compatible with your appliance.
- You must place the E5700SG controller into [maintenance mode](#), which interrupts the connection to the E2800 controller.



In rare instances, placing a StorageGRID appliance into maintenance mode might make the appliance unavailable for remote access.

#### About this task

Don't upgrade the SANtricity OS or NVSRAM in the E-Series controller on more than one StorageGRID appliance at a time.





Upgrading more than one StorageGRID appliance at a time might cause data unavailability, depending on your deployment model and ILM policies.

### Steps

1. Confirm the appliance is in [maintenance mode](#).
2. From a service laptop, access SANtricity System Manager and sign in.
3. Download the new SANtricity OS Software file and NVSRAM file to the management client.



The NVSRAM is specific to the StorageGRID appliance. Don't use the standard NVSRAM download.


4. Follow the instructions in the *E2800 and E5700 SANtricity Software and Firmware Upgrade Guide* or the SANtricity System Manager online help to upgrade the E2800 controller's firmware and NVSRAM.



Activate the upgrade files immediately. Don't defer activation.

5. If this procedure completed successfully and you have additional procedures to perform while the node is in maintenance mode, perform them now. When you are done, or if you experienced any failures and want to start over, select **Advanced > Reboot Controller**, and then select one of these options:
  - Select **Reboot into StorageGRID**
  - Select **Reboot into Maintenance Mode** to reboot the controller with the node remaining in maintenance mode. Select this option if you experienced any failures during the procedure and want to start over. After the node finishes rebooting into maintenance mode, restart from the appropriate step in the procedure that failed.



It can take up to 20 minutes for the appliance to reboot and rejoin the grid. To confirm that the reboot is complete and that the node has rejoined the grid, go back to the Grid Manager. The Nodes page should display a normal status (green check mark icon  to the left of the node name) for the appliance node, indicating that no alerts are active and the node is connected to the grid.

View the list and status of sites and grid nodes.

Search...

Total node count: 14

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
^ Data Center 1	Site	0%	0%	—
✓ DC1-ADM1	Primary Admin Node	—	—	21%
✓ DC1-ARC1	Archive Node	—	—	8%
✓ DC1-G1	Gateway Node	—	—	10%
✓ DC1-S1	Storage Node	0%	0%	29%

## Related information

[Upgrade SANtricity OS on storage controllers using Grid Manager](#)

## Upgrade drive firmware using SANtricity System Manager

### Upgrade SG5700 drive firmware using SANtricity System Manager online method

Use the SANtricity System Manager online method to upgrade the firmware on the drives in your appliance to make sure you have all the latest features and bug fixes.

### Before you begin

- The storage appliance has an Optimal status.
- All drives have an Optimal status.



Don't upgrade the drive firmware on more than one StorageGRID appliance at a time. Doing so might cause data unavailability, depending on your deployment model and ILM policy.

### About this task

The drives are upgraded one at a time while the appliance is performing I/O. This method does not require you to place the appliance in maintenance mode. However, system performance might be impacted and the upgrade might take several hours longer than the offline method.



Drives belonging to volumes that don't have redundancy must be updated using the [offline method](#). The offline method should be used for any drive associated with flash read cache, or any pool or volume group that is currently degraded.

You must use the [offline method](#) when upgrading SSD drives.

### Steps

1. Access SANtricity System Manager using one of these methods:
  - Use the StorageGRID Appliance Installer and select **Advanced** > **SANtricity System Manager**

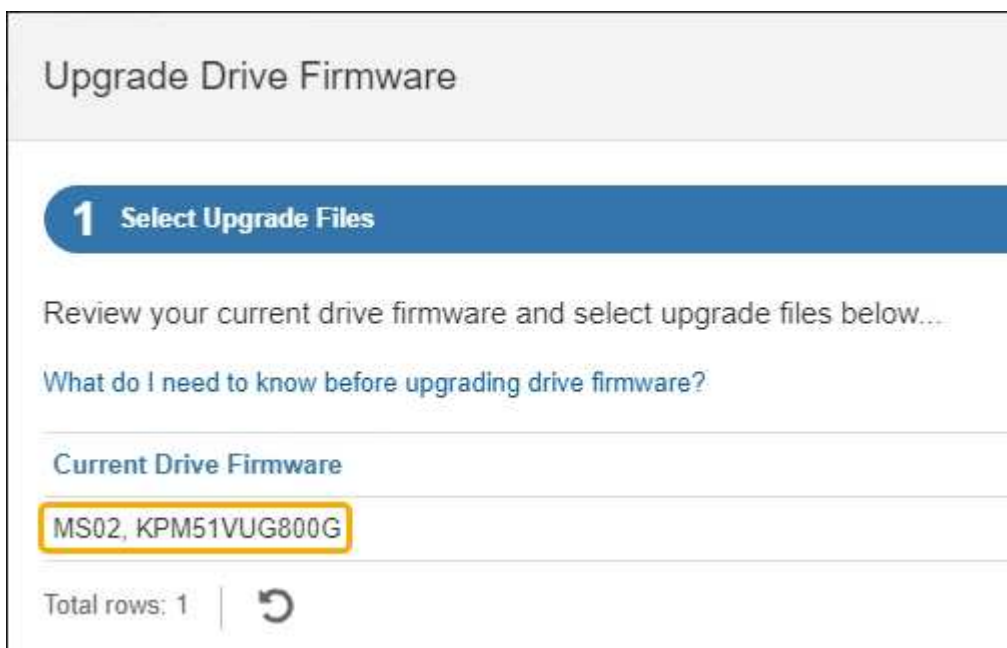
- Use the Grid Manager and select **NODES > Storage Node > SANtricity System Manager**
- Use SANtricity System Manager by browsing to the storage controller IP:

**https://Storage\_Controller\_IP**

2. Enter the SANtricity System Manager administrator username and password, if required.
3. Verify the drive firmware version currently installed in the storage appliance:
  - a. From SANtricity System Manager, select **SUPPORT > Upgrade Center**.
  - b. Under Drive Firmware upgrade, select **Begin Upgrade**.

The Upgrade Drive Firmware page displays the drive firmware files currently installed.

- c. Note the current drive firmware revisions and drive identifiers in the Current Drive Firmware column.



In this example:

- The drive firmware revision is **MS02**.
- The drive identifier is **KPM51VUG800G**.

- d. Select **View drives** in the Associated Drives column to display where these drives are installed in your storage appliance.
  - e. Close the Upgrade Drive Firmware window.
4. Download and prepare the available drive firmware upgrade:
    - a. Under Drive Firmware upgrade, select **NetApp Support**.
    - b. On the NetApp Support Site, select the **Downloads** tab, and then select **E-Series Disk Drive Firmware**.

The E-Series Disk Firmware page displays.

- c. Search for each **Drive Identifier** installed in your storage appliance and verify that each drive identifier has the latest firmware revision.

- If the firmware revision is not a link, this drive identifier has the latest firmware revision.
- If one or more drive part numbers are listed for a drive identifier, a firmware upgrade is available for these drives. You can select any link to download the firmware file.

PRODUCTS ▾ SYSTEMS ▾ DOCS & KNOWLEDGEBASE ▾ COMMUNITY ▾ DOWNLOADS ▾ TOOLS ▾ CASES ▾ PARTS ▾

Downloads > Firmware > E-Series Disk Firmware

## E-Series Disk Firmware

[Download all current E-Series Disk Firmware](#)

Drive Part Number ▾	Descriptions ▾	Drive Identifier ▾	Firmware Rev. (Download)	Notes and Config Info	Release Date ▾
<input type="text" value="Drive Part Number"/>	<input type="text" value="Descriptions"/>	<input type="text" value="KPM51VUG800G"/>	<input type="text" value="Firmware Rev. (Download)"/>		
E-X4041C	SSD, 800GB, SAS, PI	KPM51VUG800G	<a href="#">MS03</a>	MS02 Fixes <a href="#">Bug 1194908</a> MS03 Fixes <a href="#">Bug 1334862</a>	04-Sep-2020

- If a later firmware revision is listed, select the link in the Firmware Rev. (Download) column to download a .zip archive containing the firmware file.
  - Extract (unzip) the drive firmware archive files you downloaded from the Support site.
- Install the drive firmware upgrade:
    - From SANtricity System Manager, under Drive Firmware upgrade, select **Begin Upgrade**.
    - Select **Browse**, and select the new drive firmware files that you downloaded from the Support site.

Drive firmware files have a filename similar to  
 D\_HUC101212CSS600\_30602291\_MS01\_2800\_0002.dlp.

You can select up to four drive firmware files, one at a time. If more than one drive firmware file is compatible with the same drive, you get a file conflict error. Decide which drive firmware file you want to use for the upgrade and remove the other one.

- Select **Next**.

**Select Drives** lists the drives that you can upgrade with the selected firmware files.

Only drives that are compatible appear.

The selected firmware for the drive appears in the **Proposed Firmware** column. If you must change this firmware, select **Back**.

- Select **Upgrade all drives online** — Upgrades the drives that can support a firmware download while the storage array is processing I/O. You don't have to stop I/O to the associated volumes using these drives when you select this upgrade method.



An online upgrade can take several hours longer than an offline upgrade.

- In the first column of the table, select the drive or drives you want to upgrade.

The best practice is to upgrade all drives of the same model to the same firmware revision.

- Select **Start** and confirm that you want to perform the upgrade.

If you need to stop the upgrade, select **Stop**. Any firmware downloads currently in progress complete. Any firmware downloads that have not started are canceled.



Stopping the drive firmware upgrade might result in data loss or unavailable drives.

g. (Optional) To see a list of what was upgraded, select **Save Log**.

The log file is saved in the downloads folder for your browser with the name `latest-upgrade-log-timestamp.txt`.

If required, [troubleshoot driver firmware upgrade errors](#).

## Upgrade SG5700 drive firmware using SANtricity System Manager using offline method

Use the SANtricity System Manager online method to upgrade the firmware on the drives in your appliance to make sure you have all the latest features and bug fixes.

### Before you begin

- The storage appliance has an Optimal status.
- All drives have an Optimal status.
- You have [placed the StorageGRID appliance into maintenance mode](#).



While the appliance is in maintenance mode, I/O (input/output) activity to the storage controller is stopped to make disruptive storage operations safe.



Don't upgrade the drive firmware on more than one StorageGRID appliance at a time. Doing so might cause data unavailability, depending on your deployment model and ILM policy.

### About this task

The drives are upgraded in parallel while the appliance is in maintenance mode. If the pool or volume group does not support redundancy or is degraded, you must use the offline method to upgrade the drive firmware. You should also use the offline method for any drive associated with flash read cache, or any pool or volume group that is currently degraded. The offline method upgrades firmware only while all I/O activity is stopped on the drives to be upgraded. To stop I/O activity, place the node into maintenance mode.

The offline method is faster than the online method and will be significantly faster when many drives in a single appliance need upgrades. However, it requires that nodes be taken out of service, which might require scheduling a maintenance window and monitoring progress. Choose the method that is the best fit for your operational procedures and the number of drives that need to be upgraded.

### Steps

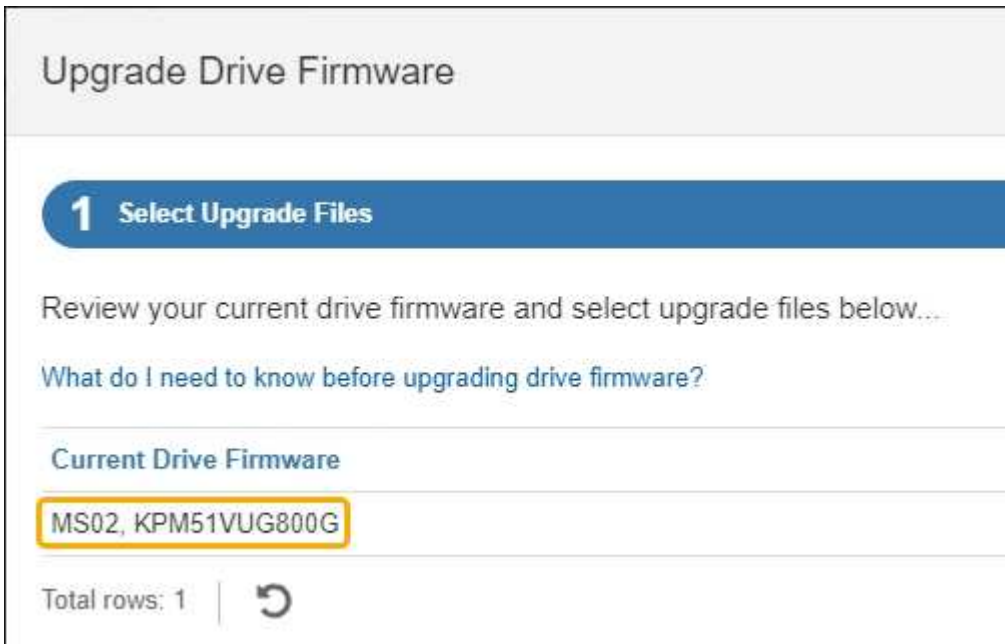
1. Confirm that the appliance is in [maintenance mode](#).
2. Access SANtricity System Manager using one of these methods:
  - Use the StorageGRID Appliance Installer and select **Advanced** > **SANtricity System Manager**
  - Use the Grid Manager and select **NODES** > **Storage Node** > **SANtricity System Manager**
  - Use SANtricity System Manager by browsing to the storage controller IP:

**`https://Storage_Controller_IP`**

3. Enter the SANtricity System Manager administrator username and password, if required.
4. Verify the drive firmware version currently installed in the storage appliance:
  - a. From SANtricity System Manager, select **SUPPORT > Upgrade Center**.
  - b. Under Drive Firmware upgrade, select **Begin Upgrade**.

The Upgrade Drive Firmware page displays the drive firmware files currently installed.

- c. Note the current drive firmware revisions and drive identifiers in the Current Drive Firmware column.



In this example:

- The drive firmware revision is **MS02**.
  - The drive identifier is **KPM51VUG800G**.
- d. Select **View drives** in the Associated Drives column to display where these drives are installed in your storage appliance.
  - e. Close the Upgrade Drive Firmware window.
5. Download and prepare the available drive firmware upgrade:
    - a. Under Drive Firmware upgrade, select **NetApp Support**.
    - b. On the NetApp Support Site, select the **Downloads** tab, and then select **E-Series Disk Drive Firmware**.

The E-Series Disk Firmware page displays.

- c. Search for each **Drive Identifier** installed in your storage appliance and verify that each drive identifier has the latest firmware revision.
  - If the firmware revision is not a link, this drive identifier has the latest firmware revision.
  - If one or more drive part numbers are listed for a drive identifier, a firmware upgrade is available for these drives. You can select any link to download the firmware file.

PRODUCTS ▾ SYSTEMS ▾ DOCS & KNOWLEDGEBASE ▾ COMMUNITY ▾ DOWNLOADS ▾ TOOLS ▾ CASES ▾ PARTS ▾

Downloads > Firmware > E-Series Disk Firmware

## E-Series Disk Firmware

Download all current E-Series Disk Firmware

Drive Part Number ▾	Descriptions ▾	Drive Identifier ▾	Firmware Rev. (Download)	Notes and Config Info	Release Date ▾
Drive Part Number	Descriptions	KPM51VUG800G	Firmware Rev. (Download)		
E-X4041C	SSD, 800GB, SAS, PI	KPM51VUG800G	MS03	MS02 Fixes <a href="#">Bug 1194908</a> MS03 Fixes <a href="#">Bug 1334862</a>	04-Sep-2020

- d. If a later firmware revision is listed, select the link in the Firmware Rev. (Download) column to download a .zip archive containing the firmware file.
  - e. Extract (unzip) the drive firmware archive files you downloaded from the Support site.
6. Install the drive firmware upgrade:
- a. From SANtricity System Manager, under Drive Firmware upgrade, select **Begin Upgrade**.
  - b. Select **Browse**, and select the new drive firmware files that you downloaded from the Support site.

Drive firmware files have a filename similar to  
D\_HUC101212CSS600\_30602291\_MS01\_2800\_0002.dlp.

You can select up to four drive firmware files, one at a time. If more than one drive firmware file is compatible with the same drive, you get a file conflict error. Decide which drive firmware file you want to use for the upgrade and remove the other one.

- c. Select **Next**.

**Select Drives** lists the drives that you can upgrade with the selected firmware files.

Only drives that are compatible appear.

The selected firmware for the drive appears in the **Proposed Firmware** column. If you must change this firmware, select **Back**.

- d. Select **Upgrade all drives offline (parallel)** — Upgrades the drives that can support a firmware download only while all I/O activity is stopped on any volumes that use the drives.



You must place the appliance into maintenance mode before using this method. You should use the **Offline** method to upgrade the drive firmware.



If you want to use the Offline (parallel) upgrade, don't proceed unless you are certain that the appliance is in maintenance mode. Failure to place the appliance into maintenance mode before initiating an offline drive firmware update might cause data loss.

- e. In the first column of the table, select the drive or drives you want to upgrade.

The best practice is to upgrade all drives of the same model to the same firmware revision.

- f. Select **Start** and confirm that you want to perform the upgrade.

If you need to stop the upgrade, select **Stop**. Any firmware downloads currently in progress complete. Any firmware downloads that have not started are canceled.



Stopping the drive firmware upgrade might result in data loss or unavailable drives.

g. (Optional) To see a list of what was upgraded, select **Save Log**.


The log file is saved in the downloads folder for your browser with the name `latest-upgrade-log-timestamp.txt`.

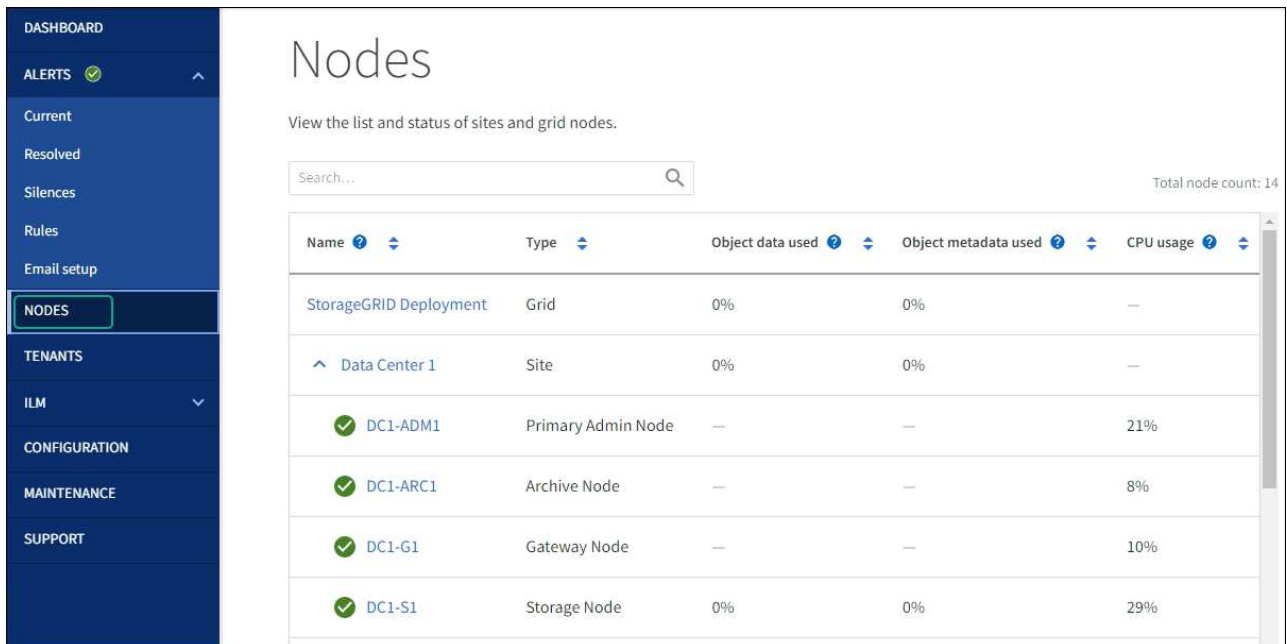
If required, [troubleshoot driver firmware upgrade errors](#).

7. After the procedure completes successfully, perform any additional maintenance procedures while the node is in maintenance mode. When you are done, or if you experienced any failures and want to start over, go to the StorageGRID Appliance Installer and select **Advanced > Reboot Controller**. Then select one of these options:

- **Reboot into StorageGRID.**
- **Reboot into Maintenance Mode.** Reboot the controller and keep the node in maintenance mode. Select this option if there were any failures during the procedure and you want to start over. After the node finishes rebooting into maintenance mode, restart from the appropriate step in the procedure that failed.

It can take up to 20 minutes for the appliance to reboot and rejoin the grid. To confirm that the reboot is complete and that the node has rejoined the grid, go back to the Grid Manager. The Nodes page

should display a normal status (green check mark icon  to the left of the node name) for the appliance node, indicating that no alerts are active and the node is connected to the grid.



Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
Data Center 1	Site	0%	0%	—
DC1-ADM1	Primary Admin Node	—	—	21%
DC1-ARC1	Archive Node	—	—	8%
DC1-G1	Gateway Node	—	—	10%
DC1-S1	Storage Node	0%	0%	29%

### Troubleshoot drive firmware upgrade errors

Troubleshoot errors that can occur when using SANtricity System Manager to upgrade the firmware on the drives in your appliance.



- **Failed assigned drives**

- One reason for the failure might be that the drive does not have the appropriate signature. Make sure that the affected drive is an authorized drive. Contact technical support for more information.
- When replacing a drive, make sure that the replacement drive has a capacity equal to or greater than the failed drive you are replacing.
- You can replace the failed drive while the storage array is receiving I/O.

- **Check storage array**

- Make sure that an IP address has been assigned to each controller.
- Make sure that all cables connected to the controller aren't damaged.
- Make sure that all cables are tightly connected.

- **Integrated hot spare drives**

This error condition must be corrected before you can upgrade the firmware.

- **Incomplete volume groups**

If one or more volume groups or disk pools are incomplete, you must correct this error condition before you can upgrade the firmware.

- **Exclusive operations (other than background media/parity scan) currently running on any volume groups**

If one or more exclusive operations are in progress, the operations must complete before the firmware can be upgraded. Use System Manager to monitor the progress of the operations.

- **Missing volumes**

You must correct the missing volume condition before the firmware can be upgraded.

- **Either controller in a state other than Optimal**

One of the storage array controllers needs attention. This condition must be corrected before the firmware can be upgraded.

- **Mismatched Storage Partition information between Controller Object Graphs**

An error occurred while validating the data on the controllers. Contact technical support to resolve this issue.

- **SPM Verify Database Controller check fails**

A storage partitions mapping database error occurred on a controller. Contact technical support to resolve this issue.

- **Configuration Database Validation (If supported by the storage array's controller version)**

A configuration database error occurred on a controller. Contact technical support to resolve this issue.

- **MEL Related Checks**

Contact technical support to resolve this issue.

- **More than 10 DDE Informational or Critical MEL events were reported in the last 7 days**

Contact technical support to resolve this issue.

- **More than 2 Page 2C Critical MEL Events were reported in the last 7 days**

Contact technical support to resolve this issue.

- **More than 2 Degraded Drive Channel Critical MEL events were reported in the last 7 days**

Contact technical support to resolve this issue.

- **More than 4 critical MEL entries in the last 7 days**

Contact technical support to resolve this issue.

### Change link configuration of E5700SG controller

You can change the Ethernet link configuration of the E5700SG controller. You can change the port bond mode, the network bond mode, and the link speed.

#### Before you begin

Place [E5700SG controller into maintenance mode](#).



In rare instances, placing a StorageGRID appliance into maintenance mode might make the appliance unavailable for remote access.

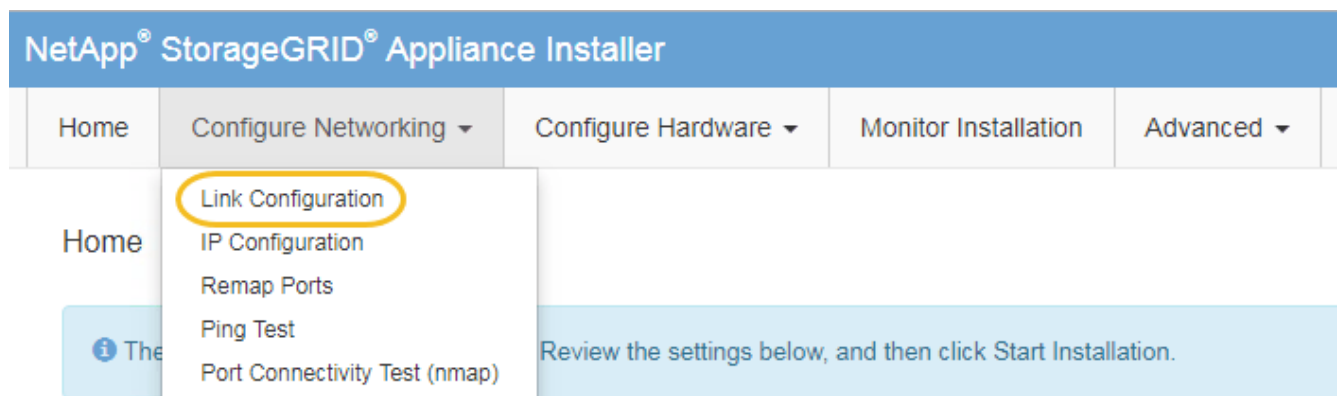
#### About this task

Options for changing the Ethernet link configuration of the E5700SG controller include:

- Changing **Port bond mode** from Fixed to Aggregate, or from Aggregate to Fixed
- Changing **Network bond mode** from Active-Backup to LACP, or from LACP to Active-Backup
- Enabling or disabling VLAN tagging, or changing the value of a VLAN tag
- Changing the link speed from 10-GbE to 25-GbE, or from 25-GbE to 10-GbE

#### Steps

1. Select **Configure Networking > Link Configuration** from the menu.



2. Make the desired changes to the link configuration.

For more information about the options, see [Configure network links](#).

3. 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://E5700SG_Controller_IP:8443`**


If you made changes to the VLAN settings, the subnet for the appliance might have changed. If you need to change the IP addresses for the appliance, follow the [configure StorageGRID IP addresses](#) instructions.

4. From the StorageGRID Appliance Installer, select **Configure Networking > Ping Test**.
5. Use the Ping Test tool to check connectivity to IP addresses on any networks that might have been affected by the link configuration changes you made in the [Change link configuration](#) step.

In addition to any other tests you choose to perform, confirm that you can ping the grid IP address of the primary Admin Node, and the grid IP address of at least one other Storage Node. If necessary, correct any link configuration issues.

6. Once you are satisfied that your link configuration changes are working, reboot the node. From the StorageGRID Appliance Installer, select **Advanced > Reboot Controller**, and then select one of these options:
  - Select **Reboot into StorageGRID** to reboot the controller with the node rejoining the grid. Select this option if you are done working in maintenance mode and are ready to return the node to normal operation.
  - Select **Reboot into Maintenance Mode** to reboot the controller with the node remaining in maintenance mode. (This option is available only when the controller is in maintenance mode.) Select this option if there are additional maintenance operations you need to perform on the node before rejoining the grid.



It can take up to 20 minutes for the appliance to reboot and rejoin the grid. To confirm that the reboot is complete and that the node has rejoined the grid, go back to the Grid Manager. The **NODES** page should display a normal status (green check mark icon  to the left of the node name) for the

appliance node, indicating that no alerts are active and the node is connected to the grid.

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
Data Center 1	Site	0%	0%	—
DC1-ADM1	Primary Admin Node	—	—	21%
DC1-ARC1	Archive Node	—	—	8%
DC1-G1	Gateway Node	—	—	10%
DC1-S1	Storage Node	0%	0%	29%

## Hardware procedures

### Replace E2800 series storage controller in the SG5700

You might need to replace the E2800 series controller if it is not functioning optimally or if it has failed.

#### Before you begin

- You have a replacement controller with the same part number as the controller you are replacing.



Don't rely on the E-Series instructions to replace a controller in the StorageGRID appliance, because the procedures aren't the same.

- You have labels to identify each cable that is connected to the controller.
- If all drives are secured, you have reviewed the steps in the [simplex E2800 series controller replacement procedure](#), which include downloading and installing E-Series SANtricity System Manager from the NetApp Support Site and then using the Enterprise Management Window (EMW) to unlock the secured drives after you have replaced the controller.



You will not be able to use the appliance until you unlock the drives with the saved key.

- You must have specific access permissions.
- You must be signed in to the Grid Manager using a [supported web browser](#).

#### About this task

You can determine if you have a failed controller canister in two ways:

- The Recovery Guru in SANtricity System Manager directs you to replace the controller.
- The amber Attention LED on the controller is on, indicating that the controller has a fault.

The appliance Storage Node will not be accessible when you replace the controller. If the E2800 series controller is functioning sufficiently, you can [place the E5700SG controller into maintenance mode](#).

When you replace a controller, you must remove the battery from the original controller and install it in the replacement controller. In some cases, you might also need to remove the host interface card from the original controller and install it in the replacement controller.

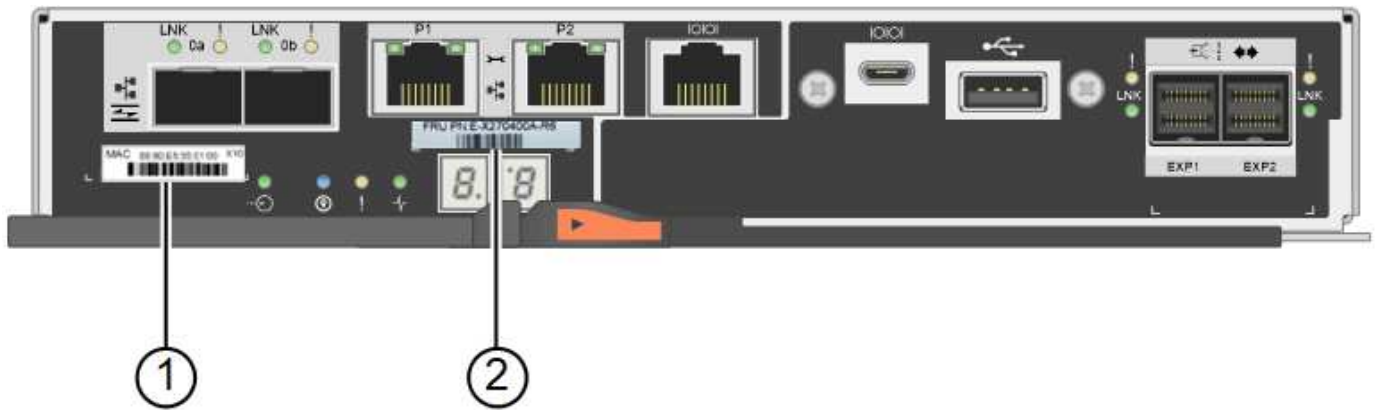


The storage controllers in most appliance models don't include host interface cards (HIC).

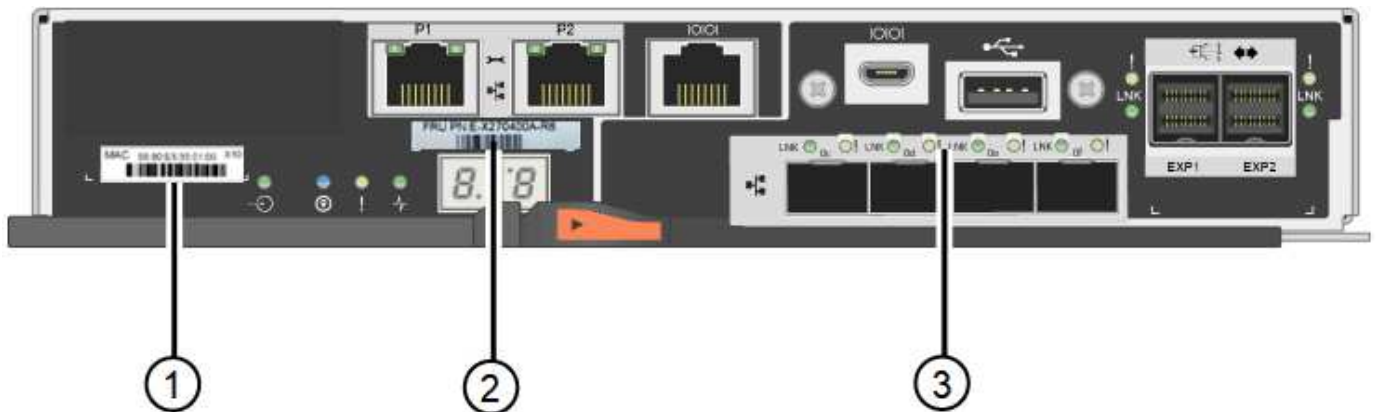
**Step 1: Prepare to remove the controller**

These figures show the E2800A controller and the E2800B controller. The procedure for replacing the E2800 series controllers and the EF570 controller is identical.

E2800A storage controller:



E2800B storage controller:



Label	component	Description
1	MAC address	The MAC address for management port 1 (“P1 on the E2800A and 0a on the E2800B”). If you used DHCP to obtain the original controller’s IP address, you will need this address to connect to the new controller.

Label	component	Description
2	FRU part number	The FRU part number. This number must match the replacement part number for the currently installed controller.
3	4-port HIC	The 4-port host interface card (HIC). This card must be moved to the new controller when you perform the replacement.  <b>Note:</b> the E2800A controller does not have a HIC.

Follow the instructions in the E2800 controller replacement procedure to prepare to remove the controller.

You use SANtricity System Manager to perform the following steps.

### Steps

1. Make a note of which version of SANtricity OS software is currently installed on the controller.
2. Make a note of which version of NVSRAM is currently installed.
3. If the Drive Security feature is enabled, be sure a saved key exists and that you know the pass phrase required to install it.



**Possible loss of data access** — If all drives in the appliance are security enabled, the new controller will not be able to access the appliance until you unlock the secured drives using the Enterprise Management Window in SANtricity System Manager.

4. Back up the configuration database.

If a problem occurs when you remove a controller, you can use the saved file to restore your configuration.

5. Collect support data for the appliance.



Collecting support data before and after replacing a component ensures you can send a full set of logs to technical support if the replacement does not resolve the problem.

### Step 2: Take the controller offline

Take the controller offline and confirm that all operations are complete.

### Steps

1. If the StorageGRID appliance is running in a StorageGRID system, [place the E5700SG controller into maintenance mode](#).
2. If the E2800 controller is functioning sufficiently to allow for a controlled shutdown, confirm that all operations have completed.
  - a. From the home page of SANtricity System Manager, select **View Operations in Progress**.
  - b. Confirm that all operations have completed.
3. Power off the controller shelf.

### Step 3: Remove the controller

Remove the failed controller from the appliance.

#### Steps

1. Put on an ESD wristband or take other antistatic precautions.
2. Label the cables and then disconnect the cables and SFPs.



To prevent degraded performance, don't twist, fold, pinch, or step on the cables.

3. Release the controller from the appliance by squeezing the latch on the cam handle until it releases, and then open the cam handle to the right.
4. Using two hands and the cam handle, slide the controller out of the appliance.



Always use two hands to support the weight of the controller.

5. Place the controller on a flat, static-free surface with the removable cover facing up.
6. Remove the cover by pressing down on the button and sliding the cover off.

### Step 4: Move battery to the new controller

Remove the battery from the failed controller, and install it into the replacement controller.

#### Steps

1. Confirm that the green LED inside the controller (between the battery and the DIMMs) is off.

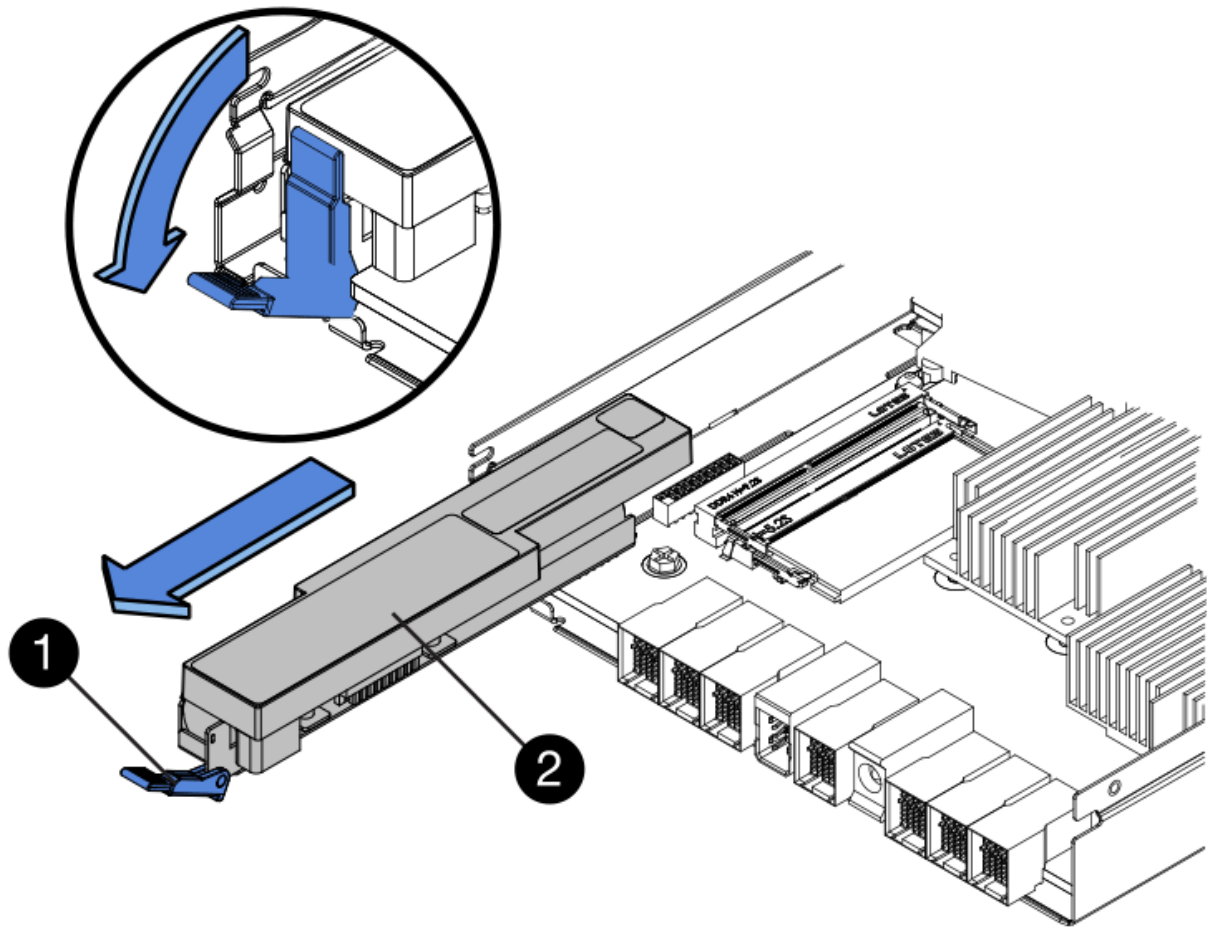
If this green LED is on, the controller is still using battery power. You must wait for this LED to go off before removing any components.



Item	Description
1	Internal Cache Active LED
2	Battery

2. Locate the blue release latch for the battery.
3. Unlatch the battery by pushing the release latch down and away from the controller.





Item	Description
1	Battery release latch
2	Battery

4. Lift up on the battery, and slide it out of the controller.
5. Remove the cover from the replacement controller.
6. Orient the replacement controller so that the slot for the battery faces toward you.
7. Insert the battery into the controller at a slight downward angle.

You must insert the metal flange at the front of the battery into the slot on the bottom of the controller, and slide the top of the battery beneath the small alignment pin on the left side of the controller.

8. Move the battery latch up to secure the battery.

When the latch clicks into place, the bottom of the latch hooks into a metal slot on the chassis.

9. Turn the controller over to confirm that the battery is installed correctly.



**Possible hardware damage** — The metal flange at the front of the battery must be completely inserted into the slot on the controller (as shown in the first figure). If the battery is not installed correctly (as shown in the second figure), the metal flange might contact the controller board, causing damage.

- **Correct** — The battery's metal flange is completely inserted into the slot on the controller:



- **Incorrect** — The battery's metal flange is not inserted into the slot on the controller:



10. Replace the controller cover.

**Step 5: Move HIC to new controller, if needed**

If the failed controller includes a host interface card (HIC), move the HIC from the failed controller to the replacement controller.

A separate HIC is used for the E2800B controller only. The HIC is mounted to the main controller board and includes two SPF connectors.



The illustrations in this procedure show a 2-port HIC. The HIC in your controller might have a different number of ports.

## E2800A

An E2800A controller does not have a HIC.

Replace the E2800A controller cover, and go to [Step 6: Replace controller](#)

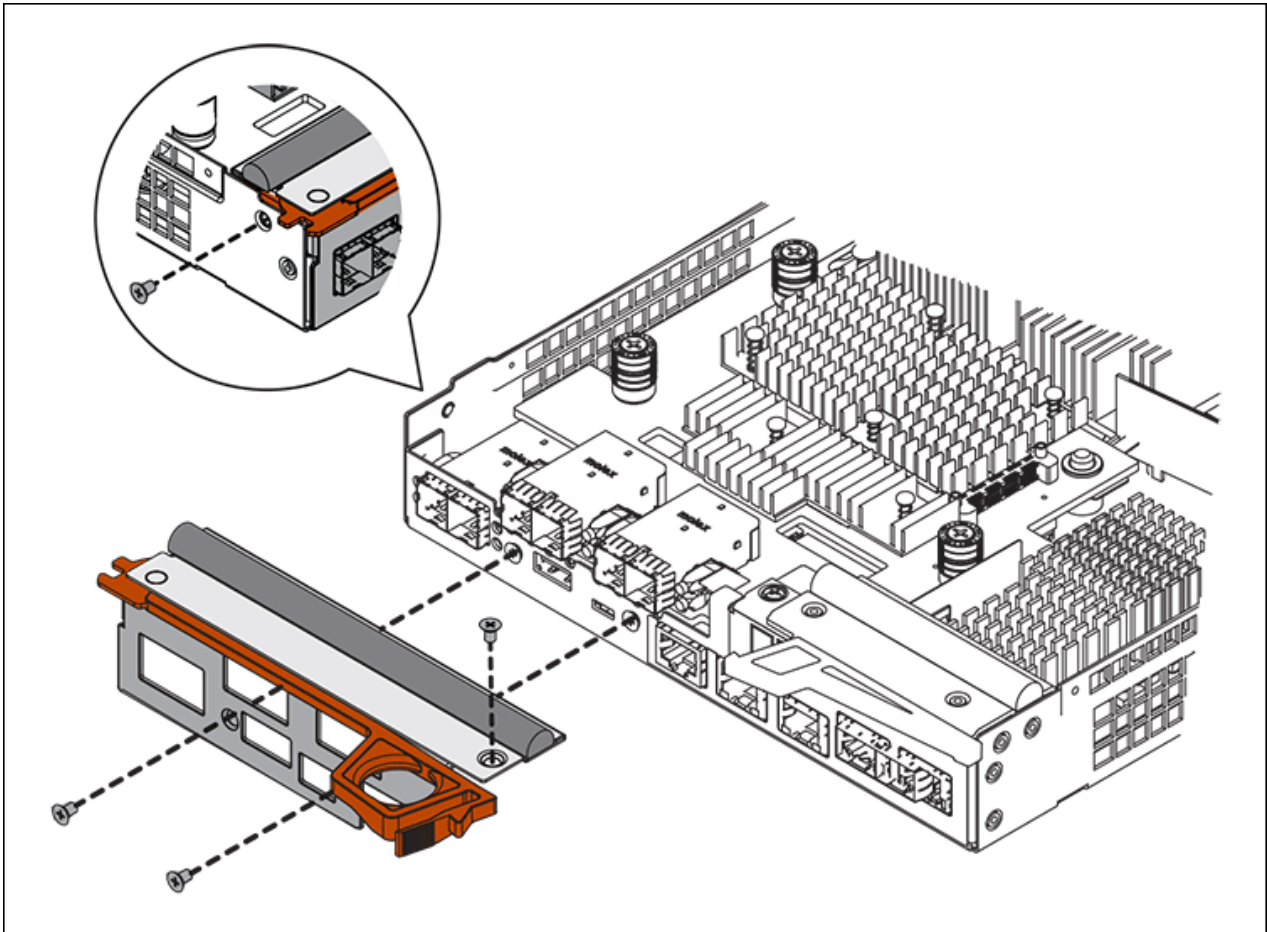
## E2800B

Move the HIC from the failed E2800B controller to the replacement controller.

### Steps

1. Remove any SFPs from the HIC.
2. Using a #1 Phillips screwdriver, remove the screws that attach the HIC faceplate to the controller.

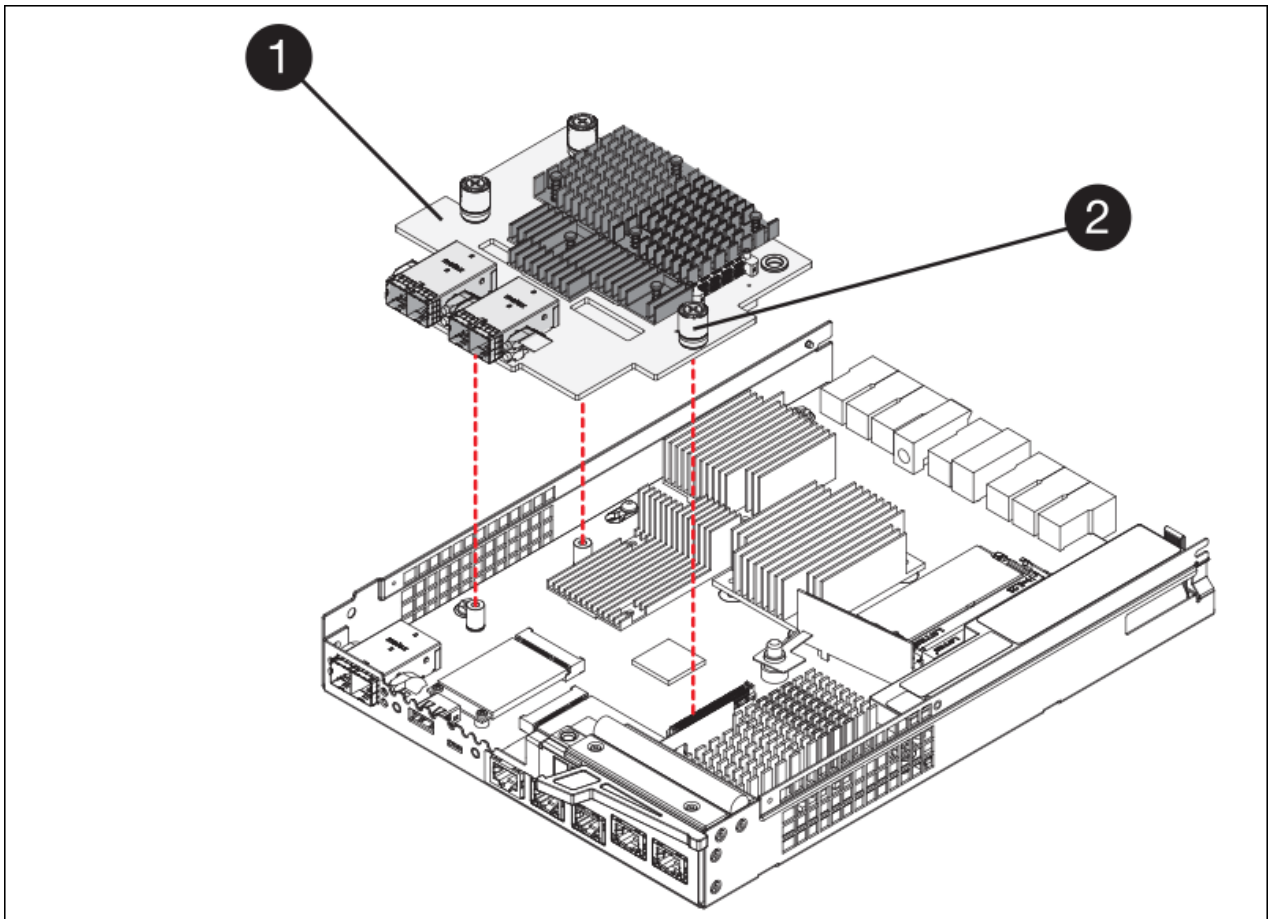
There are four screws: one on the top, one on the side, and two on the front.



3. Remove the HIC faceplate.
4. Using your fingers or a Phillips screwdriver, loosen the three thumbscrews that secure the HIC to the controller card.
5. Carefully detach the HIC from the controller card by lifting the card up and sliding it back.



Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.



Label	Description
1	Host interface card
2	Thumbscrews

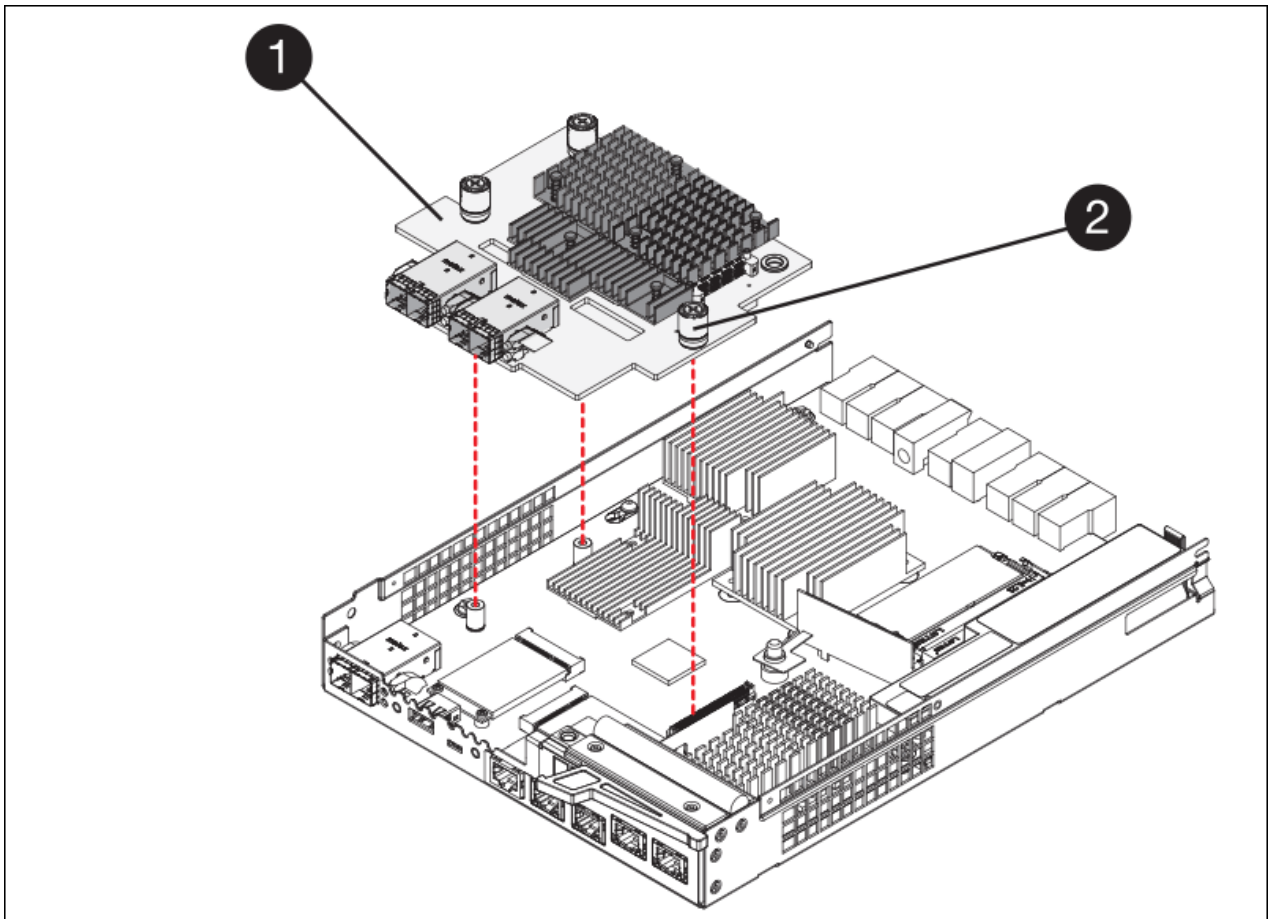
6. Place the HIC on a static-free surface.
7. Using a #1 Phillips screwdriver, remove the four screws that attach the blank faceplate to the replacement controller, and remove the faceplate.
8. Align the three thumbscrews on the HIC with the corresponding holes on the replacement controller, and align the connector on the bottom of the HIC with the HIC interface connector on the controller card.

Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.

9. Carefully lower the HIC into place, and seat the HIC connector by pressing gently on the HIC.



**Possible equipment damage** — Be careful not to pinch the gold ribbon connector for the controller LEDs between the HIC and the thumbscrews.

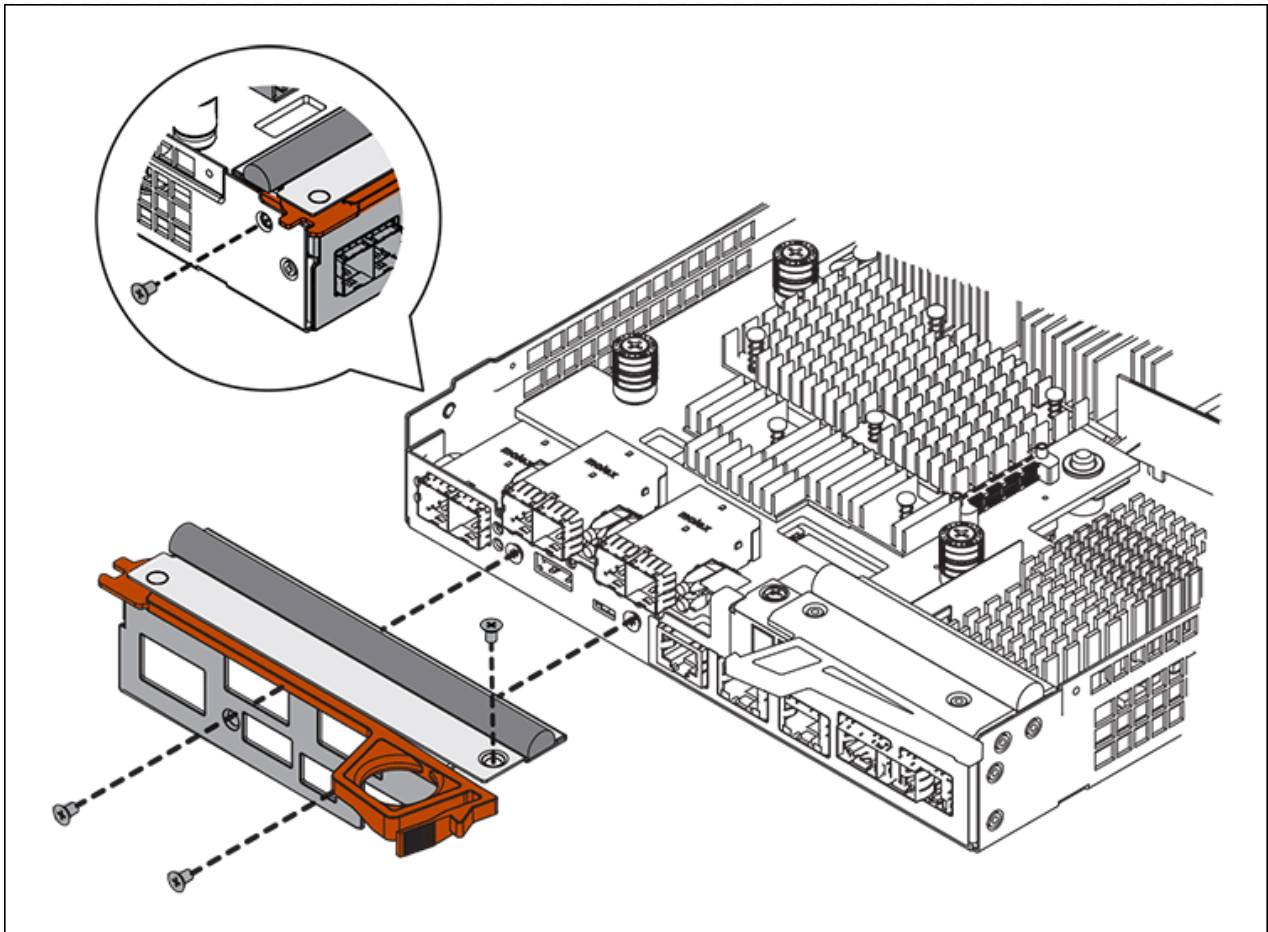


Label	Description
1	Host interface card
2	Thumbscrews

10. Hand-tighten the HIC thumbscrews.

Don't use a screwdriver, or you might over tighten the screws.

11. Using a #1 Phillips screwdriver, attach the HIC faceplate you removed from the original controller to the new controller with four screws.



12. Reinstall any removed SFPs into the HIC.

### Step 6: Replace controller

Install the replacement controller and verify that it has rejoined the grid.

#### Steps

1. Install the replacement controller into the appliance.
  - a. Turn the controller over, so that the removable cover faces down.
  - b. With the cam handle in the open position, slide the controller all the way into the appliance.
  - c. Move the cam handle to the left to lock the controller in place.
  - d. Replace the cables and SFPs.
  - e. Power on the controller shelf.
  - f. Wait for the E2800 controller to reboot. Verify that the seven-segment display shows a state of 99.
  - g. Determine how you will assign an IP address to the replacement controller.



The steps for assigning an IP address to the replacement controller depend on whether you connected management port 1 to a network with a DHCP server and on whether all drives are secured.

If management port 1 is connected to a network with a DHCP server, the new controller will obtain its


IP address from the DHCP server. This value might be different than the original controller's IP address.

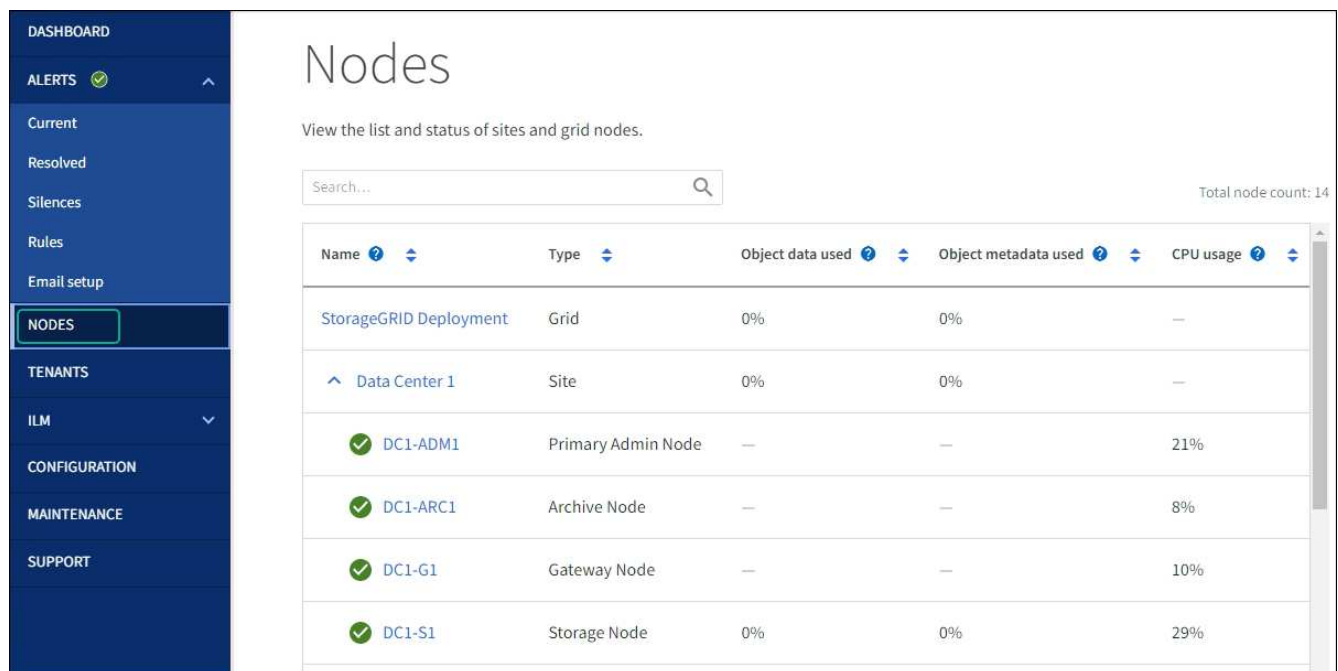
2. If the appliance uses secured drives, follow the instructions in the E2800 controller replacement procedure to import the drive security key.
3. Return the appliance to normal operating mode. From the StorageGRID Appliance Installer, select **Advanced > Reboot Controller**, and then select **Reboot into StorageGRID**.



4. During the reboot, monitor the node's status to determine when it has rejoined the grid.

The appliance reboots and rejoins the grid. This process can take up to 20 minutes.

5. Confirm that the reboot is complete and that the node has rejoined the grid. In the Grid Manager, verify that the Nodes page displays a normal status (green check mark icon  to the left of the node name) for the appliance node, indicating that no alerts are active and the node is connected to the grid.



6. From SANtricity System Manager, confirm that the new controller is Optimal, and collect support data.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return & Replacements](#) page for further information.

## Replace E5700SG compute controller

You might need to replace the E5700SG controller if it is not functioning optimally or if it has failed.

### Before you begin

- You have a replacement controller with the same part number as the controller you are replacing.
- You have downloaded the E-Series instructions for replacing a failed E5700 controller.



Use the E-Series instructions for reference only if you need more details to perform a specific step. Don't rely on the E-Series instructions to replace a controller in the StorageGRID appliance, because the procedures aren't the same. For example, the E-Series instructions for the E5700 controller describe how to remove the battery and the host interface card (HIC) from a failed controller and install them in a replacement controller. These steps don't apply to the E5700SG controller.

- You have labels to identify each cable that is connected to the controller.

### About this task

The appliance Storage Node will not be accessible when you replace the controller. If the E5700SG controller is functioning sufficiently, you can perform a controlled shutdown at the start of this procedure.



If you are replacing the controller before installing StorageGRID software, you might not be able to access the StorageGRID Appliance Installer immediately after completing this procedure. While you can access the StorageGRID Appliance Installer from other hosts on the same subnet as the appliance, you can't access it from hosts on other subnets. This condition should resolve itself within 15 minutes (when any ARP cache entries for the original controller time out), or you can clear the condition immediately by purging any old ARP cache entries manually from the local router or gateway.

### Steps

1. Shut down the E5700SG controller.
  - a. Log in to the grid node:
    - i. Enter the following command: `ssh admin@grid_node_IP`
    - ii. Enter the password listed in the `Passwords.txt` file.
    - iii. Enter the following command to switch to root: `su -`
    - iv. Enter the password listed in the `Passwords.txt` file.

When you are logged in as root, the prompt changes from `$` to `#`.

- b. Shut down the E5700SG controller:  
**shutdown -h now**
- c. Wait for any data in cache memory to be written to the drives.

The green Cache Active LED on the back of the E2800 controller is on when cached data needs to be



written to the drives. You must wait for this LED to turn off.

2. Turn off the power.
  - a. From the home page of SANtricity System Manager, select **View Operations in Progress**.
  - b. Confirm that all operations have completed.
  - c. Turn off both power switches on the appliance.
  - d. Wait for all LEDs to turn off.
3. If the StorageGRID networks attached to the controller use DHCP servers:
  - a. Note the MAC addresses for the ports on the replacement controller (located on labels on the controller).
  - b. Ask your network administrator to update the IP address settings for the original controller to reflect the MAC addresses for the replacement controller.



You must ensure that the IP addresses for the original controller have been updated before you apply power to the replacement controller. Otherwise, the controller will obtain new DHCP IP addresses when it boots up and might not be able to reconnect to StorageGRID. This step applies to all StorageGRID networks that are attached to the controller.

4. Remove the controller from the appliance:
  - a. Put on an ESD wristband or take other antistatic precautions.
  - b. Label the cables and then disconnect the cables and SFPs.



To prevent degraded performance, don't twist, fold, pinch, or step on the cables.

- c. Release the controller from the appliance by squeezing the latch on the cam handle until it releases, and then open the cam handle to the right.
  - d. Using two hands and the cam handle, slide the controller out of the appliance.



Always use two hands to support the weight of the controller.

5. Install the replacement controller into the appliance.
  - a. Turn the controller over, so that the removable cover faces down.
  - b. With the cam handle in the open position, slide the controller all the way into the appliance.
  - c. Move the cam handle to the left to lock the controller in place.
  - d. Replace the cables and SFPs.
6. Power on the appliance, and monitor the controller LEDs and seven-segment displays.

After the controllers have successfully booted up, the seven-segment displays should show the following:

- E2800 series controller:  
The final state is 99.
- E5700SG controller:

The final state is HA.

7. Confirm that the appliance Storage Node appears in the Grid Manager and that no alarms appear.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return & Replacements](#) page for further information.

#### Related information

[NetApp E-Series Systems Documentation Site](#)

### Replace other hardware components in the SG5700

You might need to replace a controller battery, drive, fan, or power supply, in the StorageGRID appliance.

#### Before you begin

- You have the E-Series hardware replacement procedure.
- The appliance has been [placed into maintenance mode](#) if the component replacement procedure requires that you shut down the appliance.

#### About this task

To replace the battery in the E2800 controller, see the instructions in these instructions for [replacing the E2800 controller](#). Those instructions describe how to remove the controller from the appliance, remove the battery from the controller, install the battery, and replace the controller.

To replace a drive, power-fan canister, fan canister, power canister, or drive drawer in the appliance, access the [E-Series procedures for maintaining E2800 hardware](#).

#### SG5712 component replacement instructions

FRU	See E-Series instructions for
Drive	Replacing a drive in E2800 12-drive or 24-drive shelves
Power-fan canister	Replacing a power-fan canister in E2800 shelves

#### SG5760 component replacement instructions

FRU	See E-Series instructions for
Drive	Replacing a drive in E2860 shelves
Power canister	Replacing a power canister in E2860 shelves
Fan canister	Replacing a fan canister in E2860 shelves
Drive drawer	Replacing a drive drawer in E2860 shelves

# Maintain SG6000 storage appliance hardware

## Maintain SG6000 appliance

You might need to perform maintenance procedures on the SG6000 appliance.

Procedures specific to maintaining your SG6000 appliance are in this section and assume that the appliance has already been deployed as a Storage Node in a StorageGRID system.

See [Common procedures](#) for maintenance procedures that are used by all appliances.

See [Set up hardware](#) for maintenance procedures that are also performed during initial appliance installation and configuration.

To prevent service interruptions, confirm that all other Storage Nodes are connected to the grid before shutting down the appliance or shut down the appliance during a scheduled maintenance window when periods of service disruption are acceptable. See the information about [monitoring node connection states](#).



If you have ever used an ILM rule that creates only one copy of an object, you must shut down the appliance during a scheduled maintenance window. Otherwise, you might temporarily lose access to those objects during any maintenance procedure that takes a storage node out of service. See the information about [managing objects with information lifecycle management](#).

## Maintenance configuration procedures

### Upgrade SANtricity OS on SG6000 storage controllers

To ensure optimal functioning of the storage controller, you must upgrade to the latest maintenance release of the SANtricity OS that is qualified for your StorageGRID appliance.

Consult the [NetApp Interoperability Matrix Tool \(IMT\)](#) to determine which version you should be using.

Download the new SANtricity OS Software file from [NetApp Downloads: StorageGRID Appliance](#).

Use one of the following procedures based on the version of SANtricity OS currently installed:

- If the storage controller is using SANtricity OS 08.42.20.00 (11.42) or newer, use the Grid Manager to perform the upgrade.

[Upgrade SANtricity OS on storage controllers using Grid Manager](#)

- If the storage controller is using a SANtricity OS version older than 08.42.20.00 (11.42), use maintenance mode to perform the upgrade.

[Upgrade SANtricity OS on storage controllers using maintenance mode](#)



When upgrading the SANtricity OS for your storage appliance, you must follow the instructions in the StorageGRID documentation. If you use any other instructions, your appliance could become inoperable.

## Upgrade SANtricity OS on SG6000 storage controllers using Grid Manager

For storage controllers currently using SANtricity OS 08.42.20.00 (11.42) or newer, you must use the Grid Manager to apply an upgrade.

### Before you begin

- You have consulted the [NetApp Interoperability Matrix Tool \(IMT\)](#) to confirm that the SANtricity OS version you are using for the upgrade is compatible with your appliance.
- You have the [Maintenance or Root access permission](#).
- You are signed in to the Grid Manager using a [supported web browser](#).
- You have the provisioning passphrase.
- You have access to [NetApp Downloads: StorageGRID Appliance](#).

### About this task

You can't perform other software updates (StorageGRID software upgrade or a hotfix) until you have completed the SANtricity OS upgrade process. If you attempt to start a hotfix or a StorageGRID software upgrade before the SANtricity OS upgrade process has finished, you are redirected to the SANtricity OS upgrade page.

The procedure will not be complete until the SANtricity OS upgrade has been successfully applied to all applicable nodes that have been selected for the upgrade. It might take more than 30 minutes to load the SANtricity OS on each node (sequentially) and up to 90 minutes to reboot each StorageGRID storage appliance. Any nodes in your grid that don't use SANtricity OS will not be affected by this procedure.



The following steps are only applicable when you are using the Grid Manager to perform the upgrade. The storage controllers in the appliance can't be upgraded using the Grid Manager when the controllers are using SANtricity OS older than 08.42.20.00 (11.42).



This procedure will automatically upgrade the NVSRAM to the most recent version associated with the SANtricity OS upgrade. You don't need to apply a separate NVSRAM upgrade file.



Be sure to apply the latest StorageGRID hotfix before you begin this procedure. See [StorageGRID hotfix procedure](#) for details.

### Steps

1. Download the new SANtricity OS Software file from [NetApp Downloads: StorageGRID Appliance](#).

Be sure to choose the SANtricity OS version for your storage controllers.

2. Select **MAINTENANCE** > **System** > **Software update**.

## Software update

You can upgrade StorageGRID software, apply a hotfix, or upgrade the SANtricity OS software on StorageGRID storage appliances. NetApp recommends you apply the latest hotfix before and after each software upgrade. Some hotfixes are required to prevent data loss.

The screenshot shows three distinct update options, each with a blue header and a white body containing text and a right-pointing arrow button.

- StorageGRID upgrade:** Upgrade to the next StorageGRID version and apply the latest hotfix for that version. Button: Upgrade →
- StorageGRID hotfix:** Apply a hotfix to your current StorageGRID software version. Button: Apply hotfix →
- SANtricity OS update:** Update the SANtricity OS software on your StorageGRID storage appliances. Button: Update →

3. In the SANtricity OS update section, select **Update**.

The SANtricity OS upgrade page appears and lists the details for each appliance node including:

- Node name
- Site
- Appliance model
- SANtricity OS version
- Status
- Last upgrade status

4. Review the information in the table for all of your upgradable appliances. Confirm that all storage controllers have **Nominal** status. If the status for any controller is **Unknown**, go to **Nodes > appliance node > Hardware** to investigate and resolve the issue.
5. Select the SANtricity OS upgrade file you downloaded from the NetApp Support Site.
  - a. Select **Browse**.
  - b. Locate and select the file.
  - c. Select **Open**.

The file is uploaded and validated. When the validation process is done, the file name is shown with a green check mark next to the **Browse** button. Don't change the file name because it is part of the verification process.

6. Enter the provisioning passphrase and select **Continue**.

A warning box appears stating that your browser's connection might be lost temporarily as services on nodes that are upgraded are restarted.

7. Select **Yes** to stage the SANtricity OS upgrade file to the primary Admin Node.

When the SANtricity OS upgrade starts:

a. The health check is run. This process checks that no nodes have the status of Needs Attention.



If any errors are reported, resolve them and select **Start** again.

b. The SANtricity OS Upgrade Progress table appears. This table shows all Storage Nodes in your grid and the current stage of the upgrade for each node.



The table shows all appliance Storage Nodes. Software-based Storage Nodes aren't displayed. Select **Approve** for all nodes that require the upgrade.

### SANtricity OS

1 Upload files — 2 Upgrade

Approved nodes are added to a queue and upgraded sequentially. Each node can take up to 30 minutes, which includes updating NVSRAM. When the upgrade is complete, the node is rebooted.

Select **Approve all** or approve nodes one at a time. To remove nodes from the queue, select **Remove all** or remove nodes one at a time. If the uploaded file doesn't apply to an approved node, the upgrade process skips that node and moves to the next node in the queue.

Optionally, select **Skip nodes and finish** to end the upgrade and skip any unapproved nodes.

SANtricity OS upgrade file: RCB\_11.70.3\_280x\_6283a64d.dlp

0 out of 3 completed

Node name	Current version	Progress	Stage	Details	Status	Actions
10-224-2-24-S1	08.40.60.01	<div style="width: 100%;"></div>	Waiting for you to approve		Nominal	<a href="#">Approve</a>
lab-37-sgws-quanta-10	08.73.00.00	<div style="width: 100%;"></div>	Waiting for you to approve		Nominal	<a href="#">Approve</a>
storage-7	98.72.09.00	<div style="width: 100%;"></div>	Waiting for you to approve		Nominal	<a href="#">Approve</a>

8. Optionally, sort the list of nodes in ascending or descending order by:

- Node name
- Current version
- Progress
- Stage
- Status

You can also enter a term in the Search box to search for specific nodes.

9. Approve the grid nodes you are ready to add to the upgrade queue. Approved nodes are upgraded one at a time.



Don't approve the SANtricity OS upgrade for an appliance Storage Node unless you are sure the node is ready to be stopped and rebooted. When the SANtricity OS upgrade is approved on a node, the services on that node are stopped and the upgrade process begins. Later, when the node is finished upgrading, the appliance node is rebooted. These operations might cause service interruptions for clients that are communicating with the node.

- Select the **Approve All** button to add all Storage Nodes to the SANtricity OS upgrade queue.



If the order in which nodes are upgraded is important, approve nodes or groups of nodes one at a time and wait until the upgrade is complete on each node before approving the next node.

- Select one or more **Approve** buttons to add one or more nodes to the SANtricity OS upgrade queue. The **Approve** button is disabled if the Status is not Nominal.

After you select **Approve**, the upgrade process determines if the node can be upgraded. If a node can be upgraded, it is added to the upgrade queue.

For some nodes, the selected upgrade file is intentionally not applied and you can complete the upgrade process without upgrading these specific nodes. Nodes intentionally not upgraded show a stage of Complete (upgrade attempted) and list the reason the node was not upgraded in the Details column.

10. If you need to remove a node or all nodes from the SANtricity OS upgrade queue, select **Remove** or **Remove All**.

When the stage progresses beyond Queued, the **Remove** button is hidden and you can no longer remove the node from the SANtricity OS upgrade process.

11. Wait while the SANtricity OS upgrade is applied to each approved grid node.
  - If any node shows a stage of Error while the SANtricity OS upgrade is applied, the upgrade has failed for the node. With the assistance of technical support, you might need to place the appliance in maintenance mode to recover it.
  - If the firmware on the node is too old to be upgraded with the Grid Manager, the node shows a stage of Error with the details that you must use maintenance mode to upgrade SANtricity OS on the node. To resolve the error, do the following:
    - a. Use maintenance mode to upgrade SANtricity OS on the node that shows a stage of Error.
    - b. Use the Grid Manager to restart and complete the SANtricity OS upgrade.

When the SANtricity OS upgrade is complete on all approved nodes, the SANtricity OS Upgrade Progress table closes and a green banner shows the number of nodes upgraded, and the date and time the upgrade completed.

12. If a node can't be upgraded, note the reason shown in the Details column and take the appropriate action.



The SANtricity OS upgrade process will not be complete until you approve the SANtricity OS upgrade on all the listed Storage Nodes.

Reason	Recommended action
Storage Node was already upgraded.	No further action required.
SANtricity OS upgrade is not applicable to this node.	The node does not have a storage controller that can be managed by the StorageGRID system. Complete the upgrade process without upgrading the node displaying this message.
SANtricity OS file is not compatible with this node.	The node requires a SANtricity OS file different than the one you selected. After completing the current upgrade, download the correct SANtricity OS file for the node and repeat the upgrade process.

13. If you want to end approving nodes and return to the SANtricity OS page to allow for an upload of a new SANtricity OS file, do the following:

a. Select **Skip Nodes and Finish**.

A warning appears asking if you are sure you want to finish the upgrade process without upgrading all applicable nodes.

b. Select **OK** to return to the **SANtricity OS** page.

c. When you are ready to continue approving nodes, [download the SANtricity OS](#) to restart the upgrade process.



Nodes already approved and upgraded without errors remain upgraded.

14. Repeat this upgrade procedure for any nodes with a stage of Complete that require a different SANtricity OS upgrade file.



For any nodes with a status of Needs Attention, use maintenance mode to perform the upgrade.

## Related information

[NetApp Interoperability Matrix Tool](#)

[Upgrade SANtricity OS on storage controllers using maintenance mode](#)

**Upgrade SANtricity OS on SG6000 storage controllers using maintenance mode**

For storage controllers currently using SANtricity OS older than 08.42.20.00 (11.42), you must use the maintenance mode procedure to apply an upgrade.

## Before you begin

- You have consulted the [NetApp Interoperability Matrix Tool \(IMT\)](#) to confirm that the SANtricity OS version you are using for the upgrade is compatible with your appliance.
- If the StorageGRID appliance is running in a StorageGRID system, you have placed the SG6000-CN controller into [maintenance mode](#).





Maintenance mode interrupts the connection to the storage controller.

### About this task

Don't upgrade the SANtricity OS or NVSRAM in the E-Series controller on more than one StorageGRID appliance at a time.



Upgrading more than one StorageGRID appliance at a time might cause data unavailability, depending on your deployment model and ILM policies.

### Steps

1. Confirm that the appliance is in [maintenance mode](#).
2. From a service laptop, access SANtricity System Manager and sign in.
3. Download the new SANtricity OS Software file and NVSRAM file to the management client.



The NVSRAM is specific to the StorageGRID appliance. Don't use the standard NVSRAM download.

4. Follow the instructions in the *Upgrading SANtricity OS* guide or the SANtricity System Manager online help to upgrade the firmware and NVSRAM.



Activate the upgrade files immediately. Don't defer activation.

5. If this procedure completed successfully and you have additional procedures to perform while the node is in maintenance mode, perform them now. When you are done, or if you experienced any failures and want to start over, select **Advanced > Reboot Controller**, and then select one of these options:
  - Select **Reboot into StorageGRID**
  - Select **Reboot into Maintenance Mode** to reboot the controller with the node remaining in maintenance mode. Select this option if you experienced any failures during the procedure and want to start over. After the node finishes rebooting into maintenance mode, restart from the appropriate step in the procedure that failed.



It can take up to 20 minutes for the appliance to reboot and rejoin the grid. To confirm that the reboot is complete and that the node has rejoined the grid, go back to the Grid Manager. The Nodes page should display a normal status (green check mark icon to the left of the node name) for the

appliance node, indicating that no alerts are active and the node is connected to the grid.

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
Data Center 1	Site	0%	0%	—
DC1-ADM1	Primary Admin Node	—	—	21%
DC1-ARC1	Archive Node	—	—	8%
DC1-G1	Gateway Node	—	—	10%
DC1-S1	Storage Node	0%	0%	29%

## Related information

[NetApp Interoperability Matrix Tool](#)

[Upgrade SANtricity OS on storage controllers using Grid Manager](#)

## Upgrade drive firmware using SANtricity System Manager

[Upgrade SG6000 drive firmware using SANtricity System Manager using the online method](#)

Use the SANtricity System Manager online method to upgrade the firmware on the drives in your appliance to make sure you have all the latest features and bug fixes.

## Before you begin

- The storage appliance has an Optimal status.
- All drives have an Optimal status.



Don't upgrade the drive firmware on more than one StorageGRID appliance at a time. Doing so might cause data unavailability, depending on your deployment model and ILM policy.

## About this task

The drives are upgraded one at a time while the appliance is performing I/O. This method does not require you to place the appliance in maintenance mode. However, system performance might be impacted and the upgrade might take several hours longer than the offline method.



Drives belonging to volumes that don't have redundancy must be updated using the [offline method](#). The offline method should be used for any drive associated with flash read cache (for example, SSD drives in the SG6060), or any pool or volume group that is currently degraded.

There are two types of drives: SSD and HDD. You must use the [offline method](#) to upgrade the firmware on the SSDs (for example, SSD drives in the SG6060). You can use either the online or offline method to upgrade the firmware on HDDs.

## Steps

1. Access SANtricity System Manager using one of these methods:
  - Use the StorageGRID Appliance Installer and select **Advanced > SANtricity System Manager**
  - Use the Grid Manager and select **NODES > Storage Node > SANtricity System Manager**
  - Use SANtricity System Manager by browsing to the storage controller IP:

**`https://Storage_Controller_IP`**

2. Enter the SANtricity System Manager administrator username and password, if required.
3. Verify the drive firmware version currently installed in the storage appliance:
  - a. From SANtricity System Manager, select **SUPPORT > Upgrade Center**.
  - b. Under Drive Firmware upgrade, select **Begin Upgrade**.

The Upgrade Drive Firmware page displays the drive firmware files currently installed.

- c. Note the current drive firmware revisions and drive identifiers in the Current Drive Firmware column.

Upgrade Drive Firmware

**1 Select Upgrade Files**

Review your current drive firmware and select upgrade files below...

[What do I need to know before upgrading drive firmware?](#)

Current Drive Firmware
MS02, KPM51VUG800G

Total rows: 1 |

In this example:

- The drive firmware revision is **MS02**.
  - The drive identifier is **KPM51VUG800G**.
- d. Select **View drives** in the Associated Drives column to display where these drives are installed in your storage appliance.

- e. Close the Upgrade Drive Firmware window.
4. Download and prepare the available drive firmware upgrade:
  - a. Under Drive Firmware upgrade, select **NetApp Support**.
  - b. On the NetApp Support Site, select the **Downloads** tab, and then select **E-Series Disk Drive Firmware**.

The E-Series Disk Firmware page displays.

- c. Search for each **Drive Identifier** installed in your storage appliance and verify that each drive identifier has the latest firmware revision.
  - If the firmware revision is not a link, this drive identifier has the latest firmware revision.
  - If one or more drive part numbers are listed for a drive identifier, a firmware upgrade is available for these drives. You can select any link to download the firmware file.

Drive Part Number	Descriptions	Drive Identifier	Firmware Rev. (Download)	Notes and Config Info	Release Date
<input type="text" value="Drive Part Number"/>	<input type="text" value="Descriptions"/>	<input type="text" value="KPM51VUG800G"/>	<input type="text" value="Firmware Rev. (Download)"/>		
<a href="#">E-X4041C</a>	SSD, 800GB, SAS, PI	KPM51VUG800G	<a href="#">MS03</a>	MS02 Fixes <a href="#">Bug 1194908</a> MS03 Fixes <a href="#">Bug 1334862</a>	04-Sep-2020

- d. If a later firmware revision is listed, select the link in the Firmware Rev. (Download) column to download a .zip archive containing the firmware file.
- e. Extract (unzip) the drive firmware archive files you downloaded from the Support site.
5. Install the drive firmware upgrade:
  - a. From SANtricity System Manager, under Drive Firmware upgrade, select **Begin Upgrade**.
  - b. Select **Browse**, and select the new drive firmware files that you downloaded from the Support site.

Drive firmware files have a filename similar to  
 D\_HUC101212CSS600\_30602291\_MS01\_2800\_0002.dlp.

You can select up to four drive firmware files, one at a time. If more than one drive firmware file is compatible with the same drive, you get a file conflict error. Decide which drive firmware file you want to use for the upgrade and remove the other one.

- c. Select **Next**.

**Select Drives** lists the drives that you can upgrade with the selected firmware files.

Only drives that are compatible appear.

The selected firmware for the drive appears in the **Proposed Firmware** column. If you must change this firmware, select **Back**.

- d. Select **Upgrade all drives online** — Upgrades the drives that can support a firmware download while the storage array is processing I/O. You don't have to stop I/O to the associated volumes using these drives when you select this upgrade method.



An online upgrade can take several hours longer than an offline upgrade.

You must use the [offline method](#) to upgrade the firmware on SSDs.

- e. In the first column of the table, select the drive or drives you want to upgrade.

The best practice is to upgrade all drives of the same model to the same firmware revision.

- f. Select **Start** and confirm that you want to perform the upgrade.

If you need to stop the upgrade, select **Stop**. Any firmware downloads currently in progress complete. Any firmware downloads that have not started are canceled.



Stopping the drive firmware upgrade might result in data loss or unavailable drives.

- g. (Optional) To see a list of what was upgraded, select **Save Log**.

The log file is saved in the downloads folder for your browser with the name `latest-upgrade-log-timestamp.txt`.

[If required, troubleshoot driver firmware upgrade errors.](#)

#### Upgrade SG6000 drive firmware using SANtricity System Manager using the offline method

Use the SANtricity System Manager offline method to upgrade the firmware on the drives in your appliance to make sure you have all the latest features and bug fixes.

#### Before you begin

- The storage appliance has an Optimal status.
- All drives have an Optimal status.
- You have [placed the StorageGRID appliance into maintenance mode](#).



While the appliance is in maintenance mode, I/O (input/output) activity to the storage controller is stopped to make disruptive storage operations safe.



Don't upgrade the drive firmware on more than one StorageGRID appliance at a time. Doing so might cause data unavailability, depending on your deployment model and ILM policy.

#### About this task

The drives are upgraded in parallel while the appliance is in maintenance mode. If the pool or volume group does not support redundancy or is degraded, you must use the offline method to upgrade the drive firmware. You should also use the offline method for any drive associated with flash read cache, or any pool or volume group that is currently degraded. The offline method upgrades firmware only while all I/O activity is stopped on the drives to be upgraded. To stop I/O activity, place the node into maintenance mode.

The offline method is faster than the online method and will be significantly faster when many drives in a single

appliance need upgrades. However, it requires that nodes be taken out of service, which might require scheduling a maintenance window and monitoring progress. Choose the method that is the best fit for your operational procedures and the number of drives that need to be upgraded.



There are two types of drives: SSD and HDD. You must use the offline method to upgrade the firmware on the SSDs (for example, SSD drives in the SG6060). You can use either the online or offline method to upgrade the firmware on HDDs.

## Steps

1. Confirm that the appliance is in [maintenance mode](#).



If you are upgrading the firmware in SSD drives that are part of a cache group, you must ensure that no I/O is sent to any cached volumes while the upgrade is in progress. When the appliance is in maintenance mode, no I/O is sent to any volumes while the upgrade is in progress.

2. Access SANtricity System Manager using one of these methods:
  - Use the StorageGRID Appliance Installer and select **Advanced** > **SANtricity System Manager**
  - Use the Grid Manager and select **NODES** > **Storage Node** > **SANtricity System Manager**
  - Use SANtricity System Manager by browsing to the storage controller IP:

**`https://Storage_Controller_IP`**

3. Enter the SANtricity System Manager administrator username and password, if required.
4. Verify the drive firmware version currently installed in the storage appliance:
  - a. From SANtricity System Manager, select **SUPPORT** > **Upgrade Center**.
  - b. Under Drive Firmware upgrade, select **Begin Upgrade**.

The Upgrade Drive Firmware page displays the drive firmware files currently installed.

- c. Note the current drive firmware revisions and drive identifiers in the Current Drive Firmware column.

Upgrade Drive Firmware

**1 Select Upgrade Files**

Review your current drive firmware and select upgrade files below...

[What do I need to know before upgrading drive firmware?](#)

**Current Drive Firmware**

MS02, KPM51VUG800G
--------------------

Total rows: 1 |

In this example:

- The drive firmware revision is **MS02**.
  - The drive identifier is **KPM51VUG800G**.
- d. Select **View drives** in the Associated Drives column to display where these drives are installed in your storage appliance.
  - e. Close the Upgrade Drive Firmware window.
5. Download and prepare the available drive firmware upgrade:
- a. Under Drive Firmware upgrade, select **NetApp Support**.
  - b. On the NetApp Support Site, select the **Downloads** tab, and then select **E-Series Disk Drive Firmware**.

The E-Series Disk Firmware page displays.

- c. Search for each **Drive Identifier** installed in your storage appliance and verify that each drive identifier has the latest firmware revision.
  - If the firmware revision is not a link, this drive identifier has the latest firmware revision.
  - If one or more drive part numbers are listed for a drive identifier, a firmware upgrade is available for these drives. You can select any link to download the firmware file.

Drive Part Number	Descriptions	Drive Identifier	Firmware Rev. (Download)	Notes and Config Info	Release Date
<input type="text" value="Drive Part Number"/>	<input type="text" value="Descriptions"/>	<input type="text" value="KPM51VUG800G"/>	<input type="text" value="Firmware Rev. (Download)"/>		
E-X4041C	SSD, 800GB, SAS, PI	KPM51VUG800G	<a href="#">MS03</a>	MS02 Fixes Bug 1194908 MS03 Fixes Bug 1334862	04-Sep-2020

- d. If a later firmware revision is listed, select the link in the Firmware Rev. (Download) column to download a .zip archive containing the firmware file.
  - e. Extract (unzip) the drive firmware archive files you downloaded from the Support site.
6. Install the drive firmware upgrade:
- a. From SANtricity System Manager, under Drive Firmware upgrade, select **Begin Upgrade**.
  - b. Select **Browse**, and select the new drive firmware files that you downloaded from the Support site.

Drive firmware files have a filename similar to

D\_HUC101212CSS600\_30602291\_MS01\_2800\_0002.dlp.

You can select up to four drive firmware files, one at a time. If more than one drive firmware file is compatible with the same drive, you get a file conflict error. Decide which drive firmware file you want to use for the upgrade and remove the other one.

- c. Select **Next**.

**Select Drives** lists the drives that you can upgrade with the selected firmware files.

Only drives that are compatible appear.

The selected firmware for the drive appears in the **Proposed Firmware** column. If you must change this firmware, select **Back**.

- d. Select **Upgrade all drives offline (parallel)** — Upgrades the drives that can support a firmware download only while all I/O activity is stopped on any volumes that use the drives.



You must place the appliance into maintenance mode before using this method. You should use the **Offline** method to upgrade the drive firmware.



If you want to use the Offline (parallel) upgrade, don't proceed unless you are certain that the appliance is in maintenance mode. Failure to place the appliance into maintenance mode before initiating an offline drive firmware update might cause data loss.

- e. In the first column of the table, select the drive or drives you want to upgrade.

The best practice is to upgrade all drives of the same model to the same firmware revision.

- f. Select **Start** and confirm that you want to perform the upgrade.

If you need to stop the upgrade, select **Stop**. Any firmware downloads currently in progress complete. Any firmware downloads that have not started are canceled.



Stopping the drive firmware upgrade might result in data loss or unavailable drives.


- g. (Optional) To see a list of what was upgraded, select **Save Log**.

The log file is saved in the downloads folder for your browser with the name `latest-upgrade-log-timestamp.txt`.

[If required, troubleshoot driver firmware upgrade errors.](#)

7. After the procedure completes successfully, perform any additional maintenance procedures while the node is in maintenance mode. When you are done, or if you experienced any failures and want to start over, go to the StorageGRID Appliance Installer and select **Advanced > Reboot Controller**. Then select one of these options:
- **Reboot into StorageGRID.**
  - **Reboot into Maintenance Mode.** Reboot the controller and keep the node in maintenance mode. Select this option if there were any failures during the procedure and you want to start over. After the node finishes rebooting into maintenance mode, restart from the appropriate step in the procedure that failed.

It can take up to 20 minutes for the appliance to reboot and rejoin the grid. To confirm that the reboot is complete and that the node has rejoined the grid, go back to the Grid Manager. The Nodes page

should display a normal status (green check mark icon  to the left of the node name) for the appliance node, indicating that no alerts are active and the node is connected to the grid.



View the list and status of sites and grid nodes.

Search...

Total node count: 14

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
^ Data Center 1	Site	0%	0%	—
✓ DC1-ADM1	Primary Admin Node	—	—	21%
✓ DC1-ARC1	Archive Node	—	—	8%
✓ DC1-G1	Gateway Node	—	—	10%
✓ DC1-S1	Storage Node	0%	0%	29%

### Troubleshoot drive firmware upgrade errors

Troubleshoot errors that can occur when using SANtricity System Manager to upgrade the firmware on the drives in your appliance.

- **Failed assigned drives**

- One reason for the failure might be that the drive does not have the appropriate signature. Make sure that the affected drive is an authorized drive. Contact technical support for more information.
- When replacing a drive, make sure that the replacement drive has a capacity equal to or greater than the failed drive you are replacing.
- You can replace the failed drive while the storage array is receiving I/O.

- **Check storage array**

- Make sure that an IP address has been assigned to each controller.
- Make sure that all cables connected to the controller aren't damaged.
- Make sure that all cables are tightly connected.

- **Integrated hot spare drives**

This error condition must be corrected before you can upgrade the firmware.

- **Incomplete volume groups**

If one or more volume groups or disk pools are incomplete, you must correct this error condition before you can upgrade the firmware.

- **Exclusive operations (other than background media/parity scan) currently running on any volume groups**

If one or more exclusive operations are in progress, the operations must complete before the firmware can be upgraded. Use System Manager to monitor the progress of the operations.

- **Missing volumes**

You must correct the missing volume condition before the firmware can be upgraded.

- **Either controller in a state other than Optimal**

One of the storage array controllers needs attention. This condition must be corrected before the firmware can be upgraded.

- **Mismatched Storage Partition information between Controller Object Graphs**

An error occurred while validating the data on the controllers. Contact technical support to resolve this issue.

- **SPM Verify Database Controller check fails**

A storage partitions mapping database error occurred on a controller. Contact technical support to resolve this issue.

- **Configuration Database Validation (If supported by the storage array's controller version)**

A configuration database error occurred on a controller. Contact technical support to resolve this issue.

- **MEL Related Checks**

Contact technical support to resolve this issue.

- **More than 10 DDE Informational or Critical MEL events were reported in the last 7 days**

Contact technical support to resolve this issue.

- **More than 2 Page 2C Critical MEL Events were reported in the last 7 days**

Contact technical support to resolve this issue.

- **More than 2 Degraded Drive Channel Critical MEL events were reported in the last 7 days**

Contact technical support to resolve this issue.

- **More than 4 critical MEL entries in the last 7 days**

Contact technical support to resolve this issue.

## **Turn SG6000-CN controller identify LED on and off**

The blue identify LED on the front and back of the controller can be turned on to help locate the appliance in a data center.

### **Before you begin**

You have the BMC IP address of the controller you want to identify.

### **Steps**

1. Access the controller BMC interface.
2. Select **Server Identify**.

The current status of the identify LED is selected.

3. Select **ON** or **OFF**, and then select **Perform Action**.

When you select **ON**, the blue identify LEDs light on the front (shown) and rear of the appliance.



If a bezel is installed on the controller, it might be difficult to see the front identify LED.

4. Turn the LED on and off as needed.

#### Related information

[Verify Fibre Channel HBA to replace](#)

[Locate controller in data center](#)

[Access BMC interface](#)

#### Locate SG6000-CN controller in data center

Locate the controller so that you can perform hardware maintenance or upgrades.

#### Before you begin

- You have determined which controller requires maintenance.

(Optional) To help locate the controller in your data center, [turn on the blue identify LED](#).

#### Steps

1. Find the controller requiring maintenance in the data center.
  - Look for a lit blue identify LED on the front or rear of the controller.

The front identify LED is behind the controller front bezel and might be difficult to see if the bezel is installed.



- Check the tags attached to the front of each controller for a matching part number.
- 2. Remove the controller front bezel, if one is installed, to access the front panel controls and indicators.
- 3. Optional: [Turn off the blue identify LED](#) if you used it to locate the controller.
  - Press the identify LED switch on the controller front panel.
  - Use the controller BMC interface.

#### Related information

[Remove Fibre Channel HBA](#)

[Remove SG6000-CN controller from cabinet or rack](#)

[Shut down SG6000-CN controller](#)

#### Power SG6000-CN controller off and on

You can shut down the SG6000-CN controller and power it back on to perform maintenance.

#### Shut down SG6000-CN controller

Shut down the SG6000-CN controller to perform hardware maintenance.

#### Before you begin

- You have physically located the SG6000-CN controller requiring maintenance in the data center. See [Locate controller in data center](#).

#### About this task

To prevent service interruptions, confirm that all other Storage Nodes are connected to the grid before shutting down the controller or shut down the controller during a scheduled maintenance window when periods of service disruption are acceptable. See the information about [monitoring node connection states](#).



If you have ever used an ILM rule that creates only one copy of an object, you must shut down the controller during a scheduled maintenance window. Otherwise, you might temporarily lose access to those objects during this procedure. See information about managing objects with information lifecycle management.

#### Steps

1. Shut down the SG6000-CN controller.



You must perform a controlled shut down of the appliance by entering the commands specified below. It is a best practice to perform a controlled shutdown when possible to avoid unnecessary alerts, ensure full logs are available, and avoid service disruptions.

a. If you have not already logged into the grid node, log in using PuTTY or another ssh client:

- i. Enter the following command: `ssh admin@grid_node_IP`
- ii. Enter the password listed in the `Passwords.txt` file.
- iii. Enter the following command to switch to root: `su -`
- iv. Enter the password listed in the `Passwords.txt` file.

When you are logged in as root, the prompt changes from `$` to `#`.

b. Shut down the SG6000-CN controller:

**`shutdown -h now`**

This command might take up to 10 minutes to complete.

2. Use one of the following methods to verify that the SG6000-CN controller is powered off:

- Look at the blue power LED on the front of the controller and confirm that it is off.



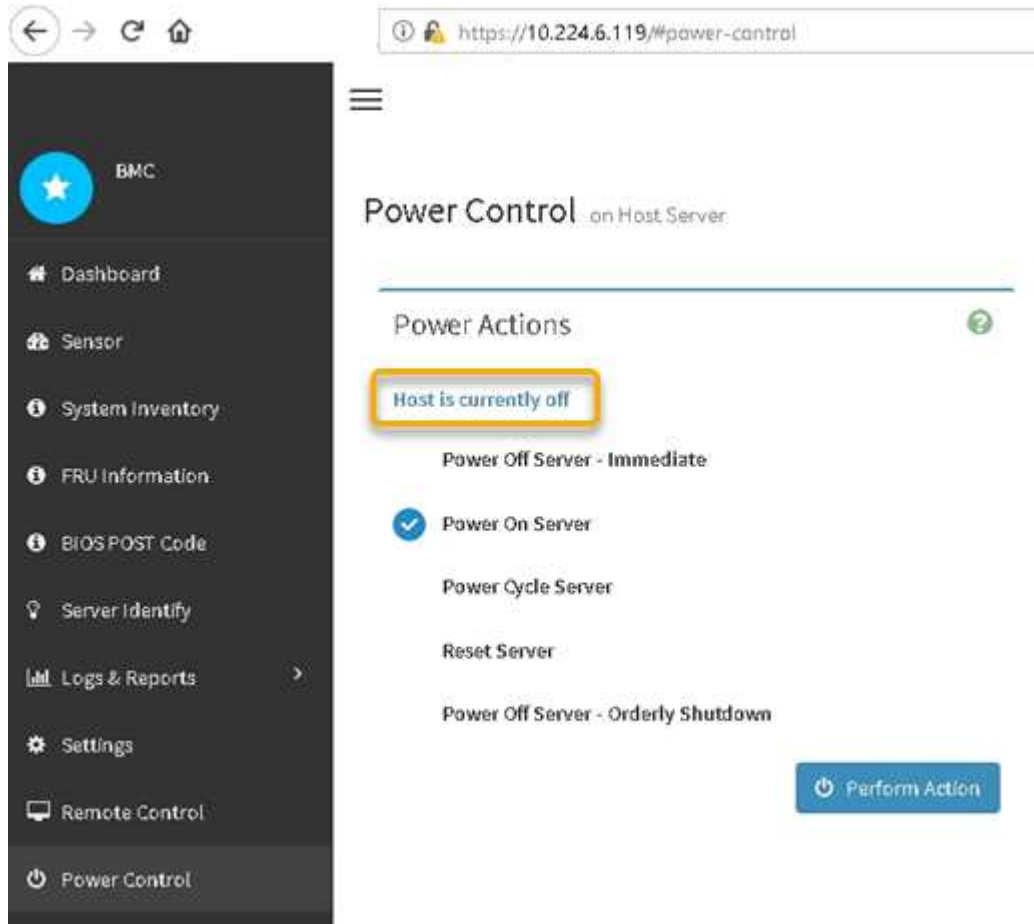
- Look at the green LEDs on both power supplies in the rear of the controller and confirm that they blink at a regular rate (approximately one blink per second).



- Use the controller BMC interface:
  - i. Access the controller BMC interface.

[Access BMC interface](#)

- ii. Select **Power Control**.
- iii. Verify that the Power Actions indicates that the host is currently off.



### Power on SG6000-CN controller and verify operation

Power on the controller after completing maintenance.

#### Before you begin

- You have installed the controller in a cabinet or rack and connected the data and power cables.

[Reinstall SG6000-CN controller into cabinet or rack](#)

- You have physically located the controller in the data center.

[Locate controller in data center](#)

#### Steps

1. Power on the SG6000-CN controller and monitor the controller LEDs and boot-up codes using one of the following methods:

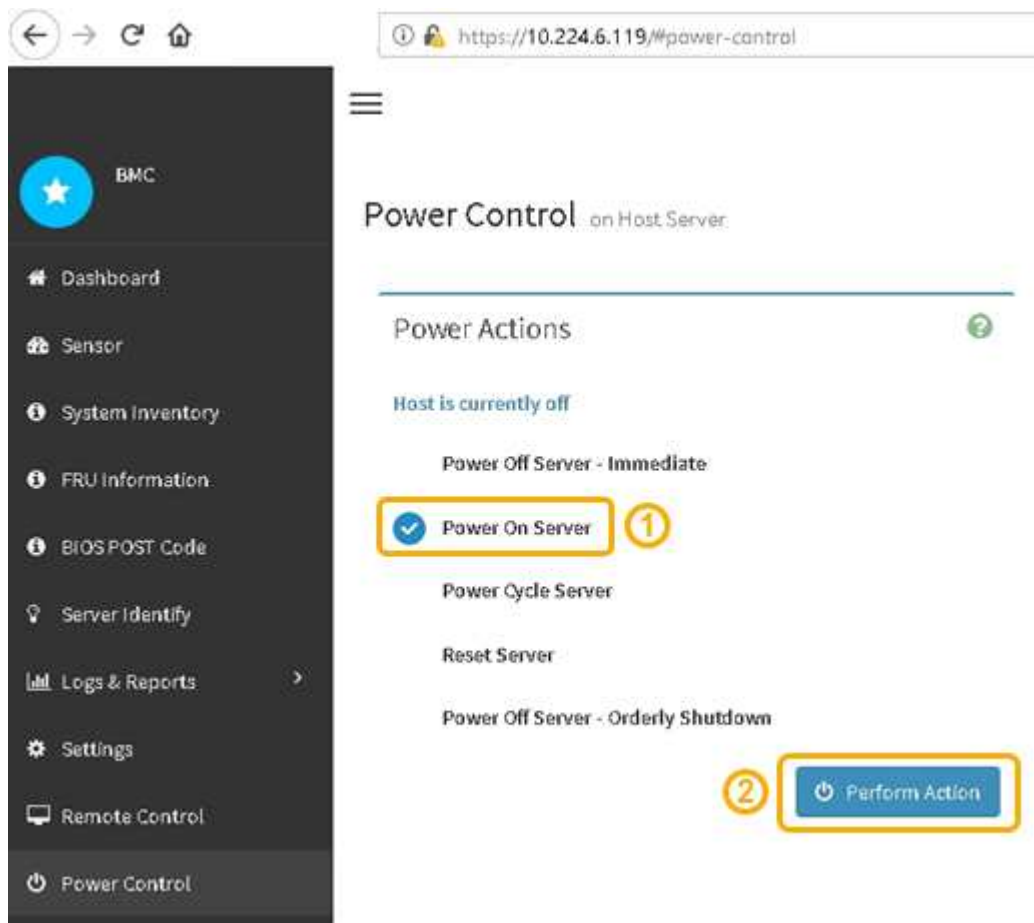
- Press the power switch on the front of the controller.



- Use the controller BMC interface:
  - i. Access the controller BMC interface.

[Access BMC interface](#)

- ii. Select **Power Control**.
- iii. Select **Power On Server** and then select **Perform Action**.



Use the BMC interface to monitor start-up status.

- 2. Confirm that the appliance controller displays in the Grid Manager and with no alerts.

It might take up to 20 minutes for the controller to display in the Grid Manager.

3. Confirm that the new SG6000-CN controller is fully operational:

a. Log in to the grid node using PuTTY or another ssh client:

- i. Enter the following command: `ssh admin@grid_node_IP`
- ii. Enter the password listed in the `Passwords.txt` file.
- iii. Enter the following command to switch to root: `su -`
- iv. Enter the password listed in the `Passwords.txt` file.

When you are logged in as root, the prompt changes from `$` to `#`.

b. Enter the following command and verify that it returns the expected output:

```
cat /sys/class/fc_host/*/port_state
```

Expected output:

```
Online
Online
Online
Online
```

If the expected output is not returned, contact technical support.

c. Enter the following command and verify that it returns the expected output:

```
cat /sys/class/fc_host/*/speed
```

Expected output:

```
16 Gbit
16 Gbit
16 Gbit
16 Gbit
```

If the expected output is not returned, contact technical support.

d. From the Nodes page in Grid Manager, make sure that the appliance node is connected to the grid and does not have any alerts.



Don't take another appliance node offline unless this appliance has a green icon.

4. Optional: Install the front bezel, if one was removed.

**Related information**

- [Remove SG6000-CN controller from cabinet or rack](#)
- [View status indicators](#)



## Change link configuration of SG6000-CN controller

You can change the Ethernet link configuration of the SG6000-CN controller. You can change the port bond mode, the network bond mode, and the link speed.

### Before you begin

The appliance has been [placed in maintenance mode](#).

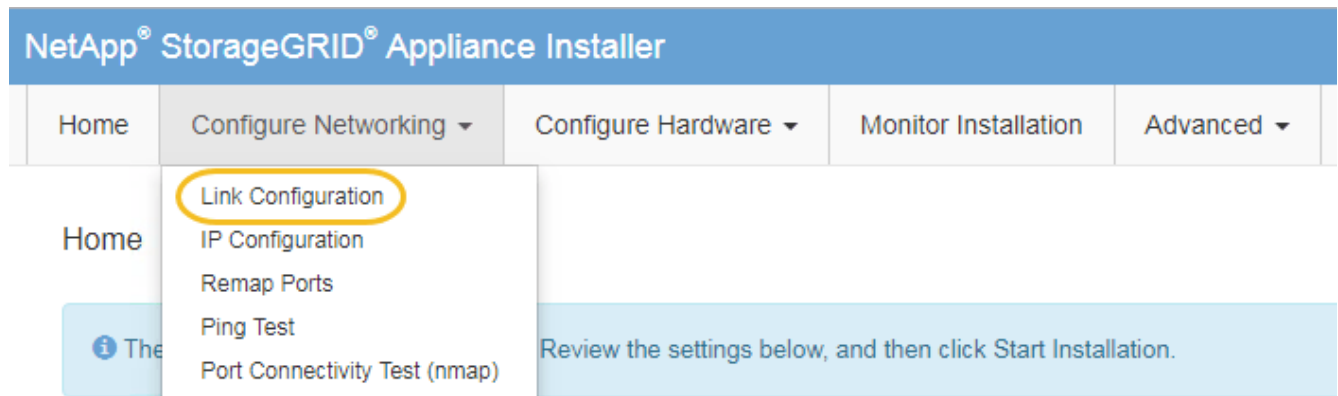
### About this task

Options for changing the Ethernet link configuration of the SG6000-CN controller include:

- Changing **Port bond mode** from Fixed to Aggregate, or from Aggregate to Fixed
- Changing **Network bond mode** from Active-Backup to LACP, or from LACP to Active-Backup
- Enabling or disabling VLAN tagging, or changing the value of a VLAN tag
- Changing the link speed.

### Steps

1. From the StorageGRID Appliance Installer, select **Configure Networking > Link Configuration**.



2. Make the desired changes to the link configuration.

For more information about the options, see [Configure network links](#).

3. 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_Controller_IP:8443`**

If you made changes to the VLAN settings, the subnet for the appliance might have changed. If you need to change the IP addresses for the appliance, follow the [Configure IP addresses](#) instructions.

### [Configure StorageGRID IP addresses](#)


4. Select **Configure Networking > Ping Test** from the menu.
5. Use the Ping Test tool to check connectivity to IP addresses on any networks that might have been

affected by the link configuration changes you made in the [link configuration changes](#) step.

In addition to any other tests you choose to perform, confirm that you can ping the Grid Network IP address of the primary Admin Node, and the Grid Network IP address of at least one other Storage Node. If necessary, return to the [link configuration changes](#) step and correct any link configuration issues.

6. When you are satisfied that your link configuration changes are working and you have additional procedures to perform while the node is in maintenance mode, perform them now. When you are done, or if you experienced any failures and want to start over, select **Advanced > Reboot Controller**, and then select one of these options:
  - Select **Reboot into StorageGRID**
  - Select **Reboot into Maintenance Mode** to reboot the controller with the node remaining in maintenance mode. Select this option if you experienced any failures during the procedure and want to start over. After the node finishes rebooting into maintenance mode, restart from the appropriate step in the procedure that failed.



It can take up to 20 minutes for the appliance to reboot and rejoin the grid. To confirm that the reboot is complete and that the node has rejoined the grid, go back to the Grid Manager. The **NODES** page should display a normal status (green check mark icon  to the left of the node name) for the appliance node, indicating that no alerts are active and the node is connected to the grid.

Nodes

View the list and status of sites and grid nodes.

Search...

Total node count: 14

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID Deployment	Grid	0%	0%	—
^ Data Center 1	Site	0%	0%	—
✓ DC1-ADM1	Primary Admin Node	—	—	21%
✓ DC1-ARC1	Archive Node	—	—	8%
✓ DC1-G1	Gateway Node	—	—	10%
✓ DC1-S1	Storage Node	0%	0%	29%

## Hardware procedures

### Add expansion shelf to deployed SG6060

To increase storage capacity, you can add one or two expansion shelves to an SG6060 that is already deployed in a StorageGRID system.

#### Before you begin

- You must have the provisioning passphrase.
- You must be running StorageGRID 11.4 or later.
- You have the expansion shelf and two SAS cables for each expansion shelf.
- You have physically located the storage appliance where you are adding the expansion shelf in the data center.

[Locate controller in data center](#)

#### About this task

To add an expansion shelf, you perform these high-level steps:

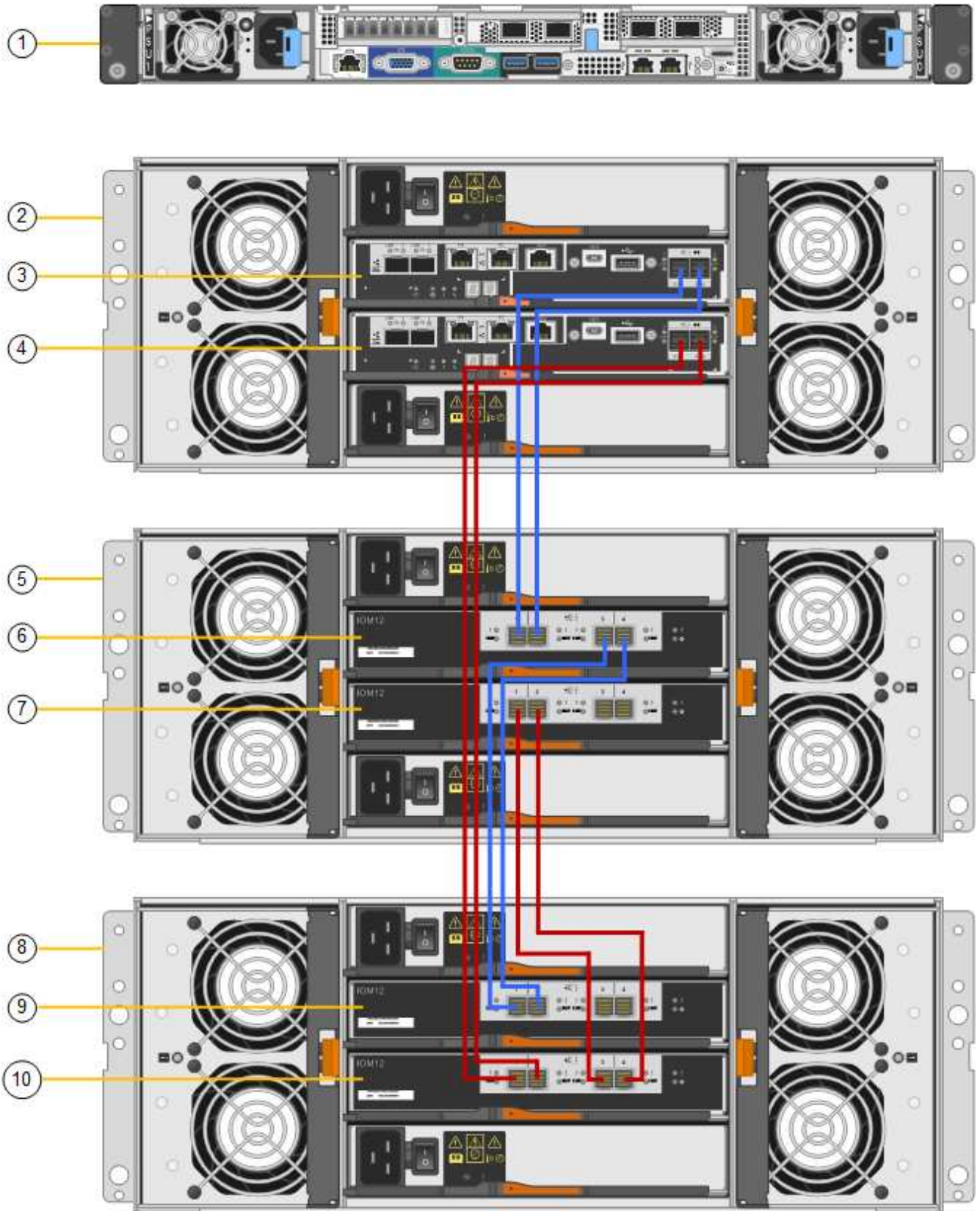
- Install the hardware in the cabinet or rack.
- Place the SG6060 into maintenance mode.
- Connect the expansion shelf to the E2860 controller shelf or to another expansion shelf.
- Start the expansion using the StorageGRID Appliance Installer
- Wait until the new volumes are configured.

Completing the procedure for one or two expansion shelves should take one hour or less per appliance node. To minimize downtime, the following steps instruct you to install the new expansion shelves and drives before placing the SG6060 into maintenance mode. The remaining steps should take approximately 20 to 30 minutes per appliance node.

## Steps

1. Follow the instructions for [installing 60-drive shelves into a cabinet or rack](#).
2. Follow the instructions for [installing the drives](#).
3. From the Grid Manager, [place the SG6000-CN controller into maintenance mode](#).
4. Connect each expansion shelf to the E2860 controller shelf as shown in the diagram.

This drawing shows two expansion shelves. If you have only one, connect IOM A to controller A and connect IOM B to controller B.



Callout	Description
1	SG6000-CN

Callout	Description
2	E2860 controller shelf
3	Controller A
4	Controller B
5	Expansion shelf 1
6	IOM A for expansion shelf 1
7	IOM B for expansion shelf 1
8	Expansion shelf 2
9	IOM A for expansion shelf 2
10	IOM B for expansion shelf 2

5. Connect the power cords and apply power to the expansion shelves.
  - a. Connect a power cord to each of the two power supply units in each expansion shelf.
  - b. Connect the two power cords in each expansion shelf to two different PDUs in the cabinet or rack.
  - c. Turn on the two power switches for each expansion shelf.
    - Don't turn off the power switches during the power-on process.
    - The fans in the expansion shelves might be very loud when they first start up. The loud noise during start-up is normal.
6. Monitor the Home page of the StorageGRID Appliance Installer.

In approximately five minutes, the expansion shelves finish powering up and are detected by the system. The Home page shows the number of new expansion shelves detected, and the Start Expansion button is enabled.

The screenshot shows examples of the messages that could appear on the Home page, depending on the number of existing or new expansion shelves, as follows:

- The banner circled at the top of the page indicates the total number of expansion shelves detected.
  - The banner indicates the total number of expansion shelves, whether the shelves are configured and deployed or new and unconfigured.
  - If no expansion shelves are detected, the banner will not appear.
- The message circled at the bottom of the page indicates an expansion is ready to be started.
  - The message indicates the number of new expansion shelves StorageGRID detects. "Attached" indicates that the shelf is detected. "Unconfigured" indicates that the shelf is new and not yet configured using the StorageGRID Appliance Installer.



Expansion shelves that are already deployed aren't included in this message. They are included in the count in the banner at the top of the page.

- The message will not appear if new expansion shelves aren't detected.

The screenshot displays a configuration page with several sections:

- Messages:** Two blue informational messages at the top. The first says, "The expansion is ready to be started. Make sure this page accurately indicates the number of new storage shelves you are trying to add, then click Start Expansion." The second says, "The storage system contains 2 expansion shelves."
- This Node:** A section with a "Node type" dropdown menu set to "Storage" and a "Node name" text field containing "NetApp-SGA". Below these are "Cancel" and "Save" buttons.
- Primary Admin Node connection:** A section with an "Enable Admin Node discovery" checkbox (unchecked), a "Primary Admin Node IP" text field containing "172.16.4.71", and a "Connection state" label showing "Connection to 172.16.4.71 ready". Below are "Cancel" and "Save" buttons.
- Installation:** A section with a "Current state" label showing "Ready to start configuration of 1 attached but unconfigured expansion shelf." and a prominent blue "Start Expansion" button.

7. As necessary, resolve any issues described in the messages on the Home page.

For example, use SANtricity System Manager to resolve any storage hardware issues.

8. Verify that the number of expansion shelves displayed on the Home page matches the number of expansion shelves you are adding.



If the new expansion shelves have not been detected, verify that they are properly cabled and powered up.

9. Click **Start Expansion** to configure the expansion shelves and make them available for object storage.

10. Monitor the progress of the expansion shelf configuration.

Progress bars appear on the web page, just as they do during initial installation.

1. Configure storage		Running
Step	Progress	Status
Connect to storage controller	<div style="width: 100%; height: 10px; background-color: green;"></div>	Complete
Clear existing configuration	<div style="width: 100%; height: 10px; background-color: green;"></div>	Skipped
Configure volumes	<div style="width: 30%; height: 10px; background-color: blue;"></div>	Creating volume StorageGRID-obj-22
Configure caching	<div style="width: 0%; height: 10px; background-color: gray;"></div>	Pending
Configure host settings	<div style="width: 0%; height: 10px; background-color: gray;"></div>	Pending

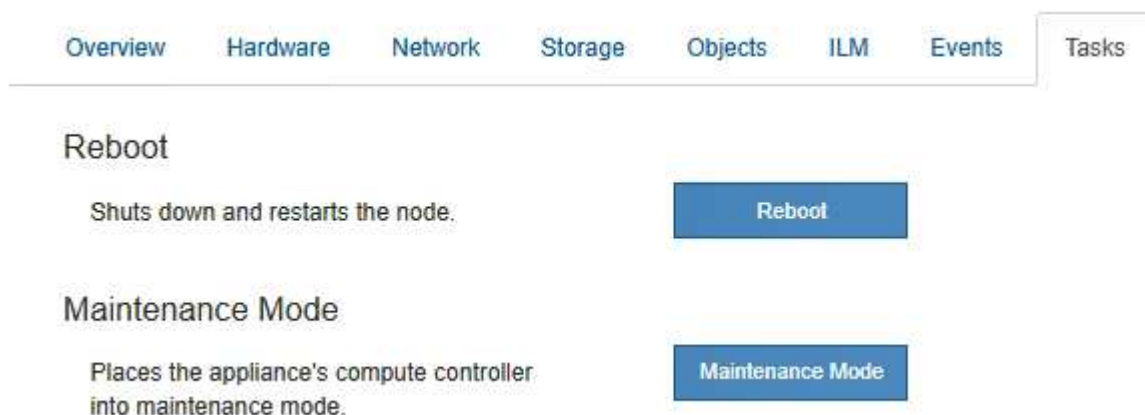
2. Complete storage expansion		Pending

When configuration is complete, the appliance automatically reboots to exit maintenance mode and rejoin the grid. This process can take up to 20 minutes.



To retry the expansion shelf configuration if it fails, go to the StorageGRID Appliance Installer, select **Advanced > Reboot Controller**, and then select **Reboot into Maintenance Mode**. After the node reboots, retry the [expansion shelf configuration](#).

When the reboot is complete, the **Tasks** tab looks like the following screenshot:



11. Verify the status of the appliance Storage Node and the new expansion shelves.

- a. In the Grid Manager, select **NODES** and verify that the appliance Storage Node has a green check mark icon.

The green check mark icon means that no alerts are active and the node is connected to the grid. For a description of node icons, see [Monitor node connection states](#).

- b. Select the **Storage** tab and confirm that 16 new object stores are shown in the Object Storage table for each expansion shelf you added.
- c. Verify that each new expansion shelf has a shelf status of Nominal and a configuration status of Configured.

### Replace storage controller in the SG6000

You might need to replace an E2800 series controller or an EF570 controller if it is not functioning optimally or if it has failed.



## Before you begin

- You have a replacement controller with the same part number as the controller you are replacing.
- You have labels to identify each cable that is connected to the controller.
- You have an ESD wristband, or you have taken other antistatic precautions.
- You have a #1 Phillips screwdriver.
- You have physically located the storage appliance where you are replacing the controller in the data center.

### [Locate controller in data center](#)



Don't rely on the E-Series instructions to replace a controller in the StorageGRID appliance, because the procedures aren't the same.

## About this task

You can determine if you have a failed controller in two ways:

- The Recovery Guru in SANtricity System Manager directs you to replace the controller.
- The amber Attention LED on the controller is on, indicating that the controller has a fault.



If both controllers in the shelf have their Attention LEDs on, contact technical support for assistance.

If your appliance contains two storage controllers, you can replace one of the controllers while your appliance is powered on and performing read/write operations, as long as the following conditions are true:

- The second controller in the shelf has Optimal status.
- The **OK to remove** field in the Details area of the Recovery Guru in SANtricity System Manager displays **Yes**, indicating that it is safe to remove this component.



When possible, place the appliance into maintenance mode for this replacement procedure to minimize the potential impact of unforeseen errors or failures.



If the second controller in the shelf does not have Optimal status or if the Recovery Guru indicates that it is not OK to remove the controller, contact technical support.

When you replace a controller, you must remove the battery from the original controller and install it in the replacement controller. In some cases, you might also need to remove the host interface card from the original controller and install it in the replacement controller.



The storage controllers in most appliance models don't include host interface cards (HIC).

## Step 1: Prepare the replacement controller

Prepare the replacement E2800A or E2800B controller.

### Steps

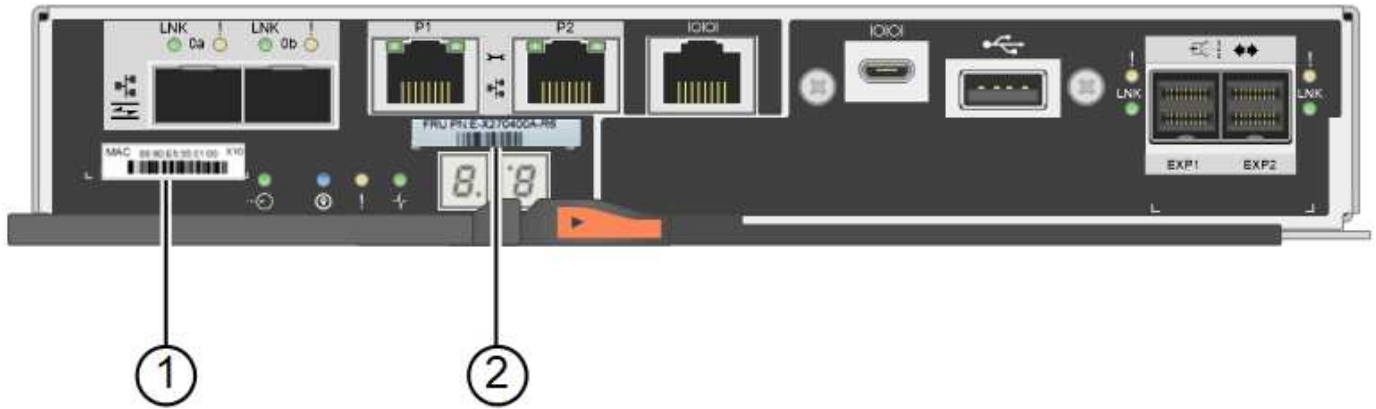
1. Unpack the new controller, and set it on a flat, static-free surface.

Save the packing materials to use when shipping the failed controller.

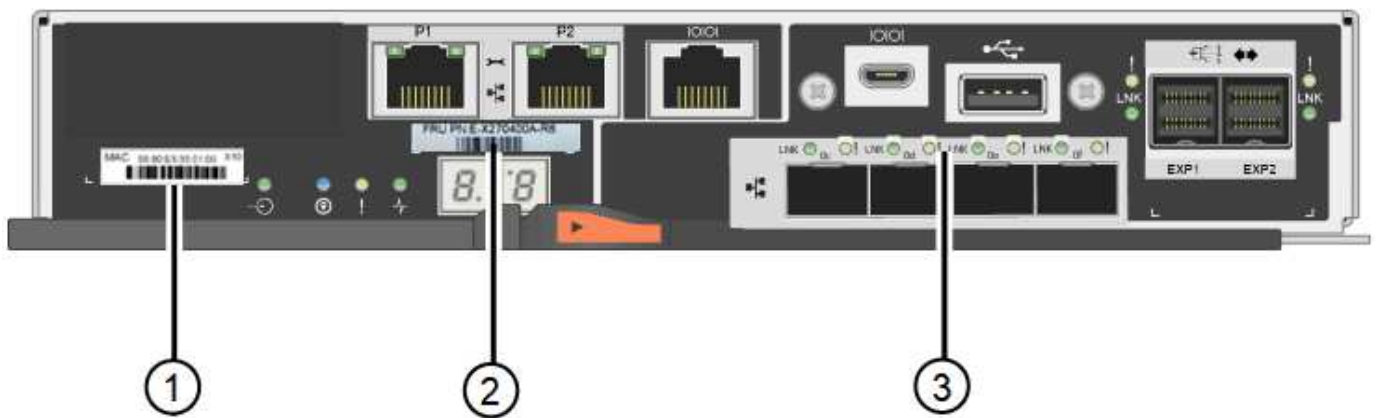
2. Locate the MAC address and FRU part number labels on the back of the replacement controller.

These figures show the E2800A controller and the E2800B controller. The procedure for replacing the E2800 series controllers and the EF570 controller is identical.

E2800A storage controller:



E2800B storage controller:



Label	component	Description
1	MAC address	The MAC address for management port 1 ("P1 on the E2800A and 0a on the E2800B"). If you used DHCP to obtain the original controller's IP address, you will need this address to connect to the new controller.
2	FRU part number	The FRU part number. This number must match the replacement part number for the currently installed controller.
3	4-port HIC	The 4-port host interface card (HIC). This card must be moved to the new controller when you perform the replacement.  <b>Note:</b> the E2800A controller does not have a HIC.

## Step 2: Take the controller offline

Prepare to remove the failed controller and and take it offline.

### Steps

1. Prepare to remove the controller. You use SANtricity System Manager to perform these steps.
  - a. Confirm that the replacement part number for the failed controller is the same as the FRU part number for the replacement controller.

When a controller has a fault and needs to be replaced, the replacement part number is displayed in the Details area of the Recovery Guru. If you need to find this number manually, you can look on the **Base** tab for the controller.



**Possible loss of data access** — If the two part numbers aren't the same, don't attempt this procedure.

- b. Back up the configuration database.

If a problem occurs when you remove a controller, you can use the saved file to restore your configuration.

- c. Collect support data for the appliance.



Collecting support data before and after replacing a component ensures you can send a full set of logs to technical support if the replacement does not resolve the problem.

- d. Take the controller you plan to replace offline.

2. Power off the controller shelf.

## Step 3: Remove the controller

Remove the failed controller from the appliance.

### Steps

1. Put on an ESD wristband or take other antistatic precautions.
2. Label the cables and then disconnect the cables and SFPs.



To prevent degraded performance, don't twist, fold, pinch, or step on the cables.

3. Release the controller from the appliance by squeezing the latch on the cam handle until it releases, and then open the cam handle to the right.
4. Using two hands and the cam handle, slide the controller out of the appliance.



Always use two hands to support the weight of the controller.

5. Place the controller on a flat, static-free surface with the removable cover facing up.
6. Remove the cover by pressing down on the button and sliding the cover off.

#### Step 4: Move battery to the new controller

Remove the battery from the failed controller, and install it into the replacement controller.

#### Steps

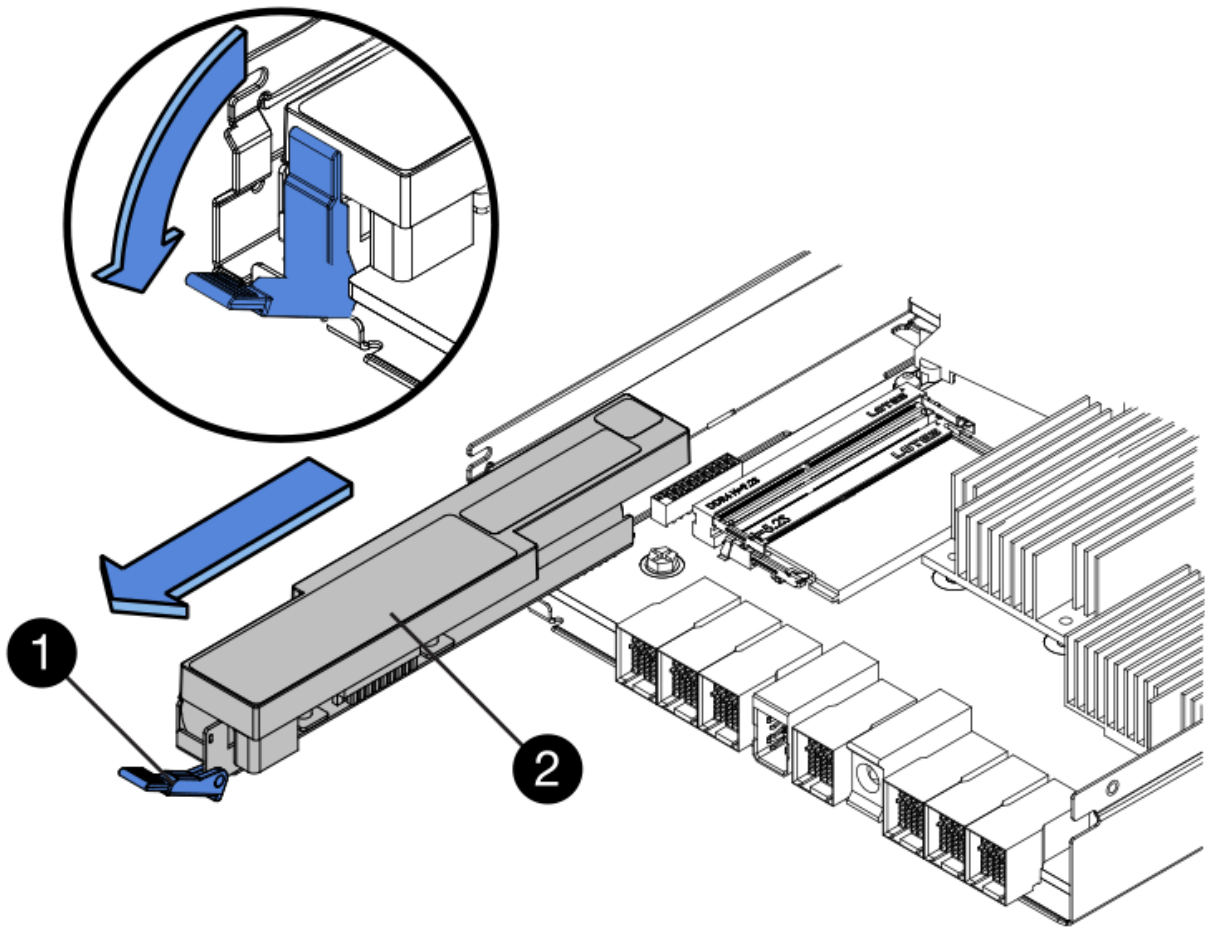
1. Confirm that the green LED inside the controller (between the battery and the DIMMs) is off.

If this green LED is on, the controller is still using battery power. You must wait for this LED to go off before removing any components.



Item	Description
1	Internal Cache Active LED
2	Battery

2. Locate the blue release latch for the battery.
3. Unlatch the battery by pushing the release latch down and away from the controller.



Item	Description
1	Battery release latch
2	Battery

4. Lift up on the battery, and slide it out of the controller.
5. Remove the cover from the replacement controller.
6. Orient the replacement controller so that the slot for the battery faces toward you.
7. Insert the battery into the controller at a slight downward angle.

You must insert the metal flange at the front of the battery into the slot on the bottom of the controller, and slide the top of the battery beneath the small alignment pin on the left side of the controller.

8. Move the battery latch up to secure the battery.

When the latch clicks into place, the bottom of the latch hooks into a metal slot on the chassis.

9. Turn the controller over to confirm that the battery is installed correctly.



**Possible hardware damage** — The metal flange at the front of the battery must be completely inserted into the slot on the controller (as shown in the first figure). If the battery is not installed correctly (as shown in the second figure), the metal flange might contact the controller board, causing damage.

- **Correct** — The battery's metal flange is completely inserted into the slot on the controller:



- **Incorrect** — The battery's metal flange is not inserted into the slot on the controller:



10. Replace the controller cover.

**Step 5: Move HIC to new controller, if needed**

If the failed controller includes a host interface card (HIC), move the HIC from the failed controller to the replacement controller.

A separate HIC is used for the E2800B controller only. The HIC is mounted to the main controller board and includes two SPF connectors.



The illustrations in this procedure show a 2-port HIC. The HIC in your controller might have a different number of ports.

## E2800A

An E2800A controller does not have a HIC.

Replace the E2800A controller cover, and go to [Step 6: Replace controller](#)

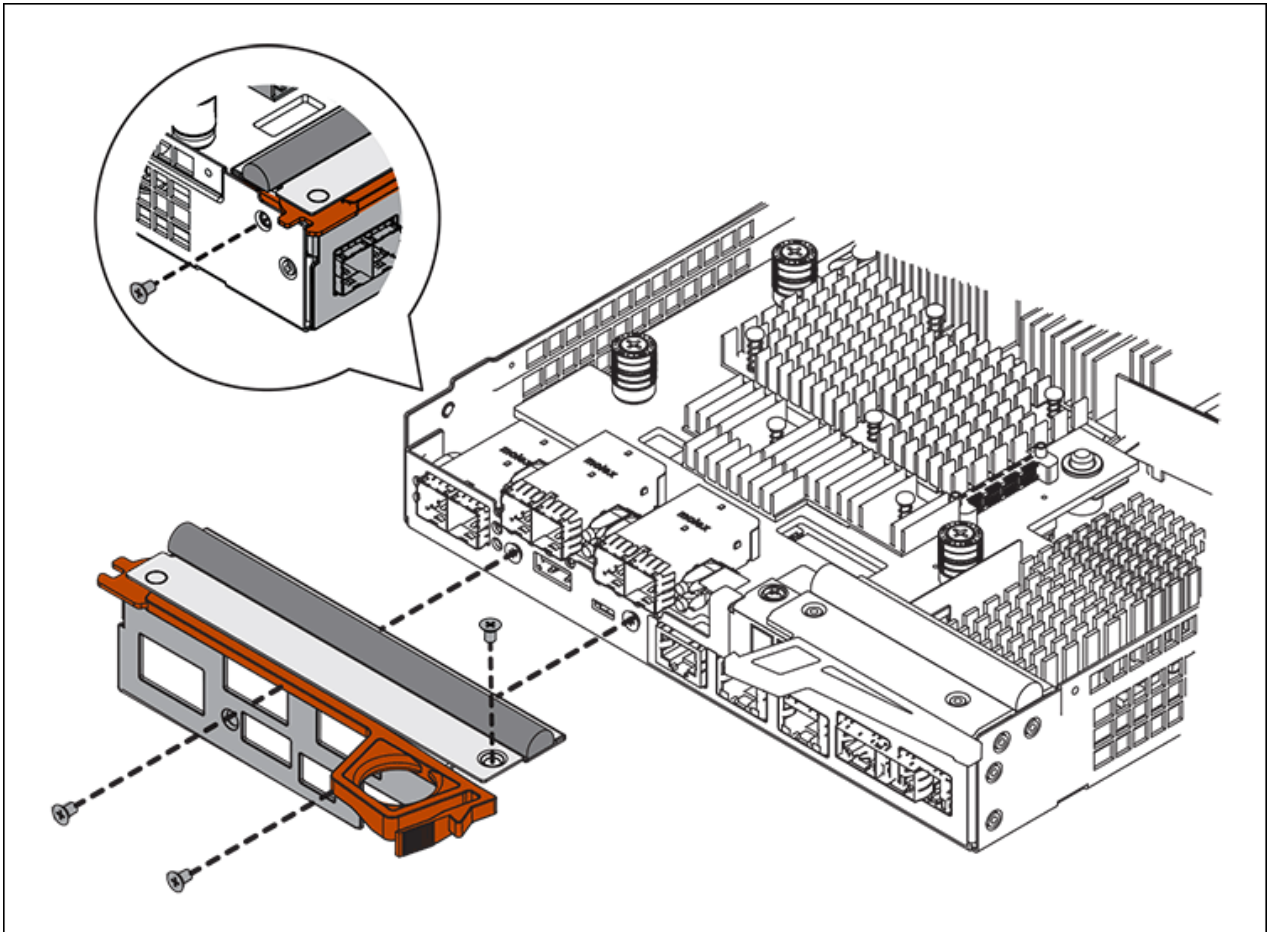
## E2800B

Move the HIC from the failed E2800B controller to the replacement controller.

### Steps

1. Remove any SFPs from the HIC.
2. Using a #1 Phillips screwdriver, remove the screws that attach the HIC faceplate to the controller.

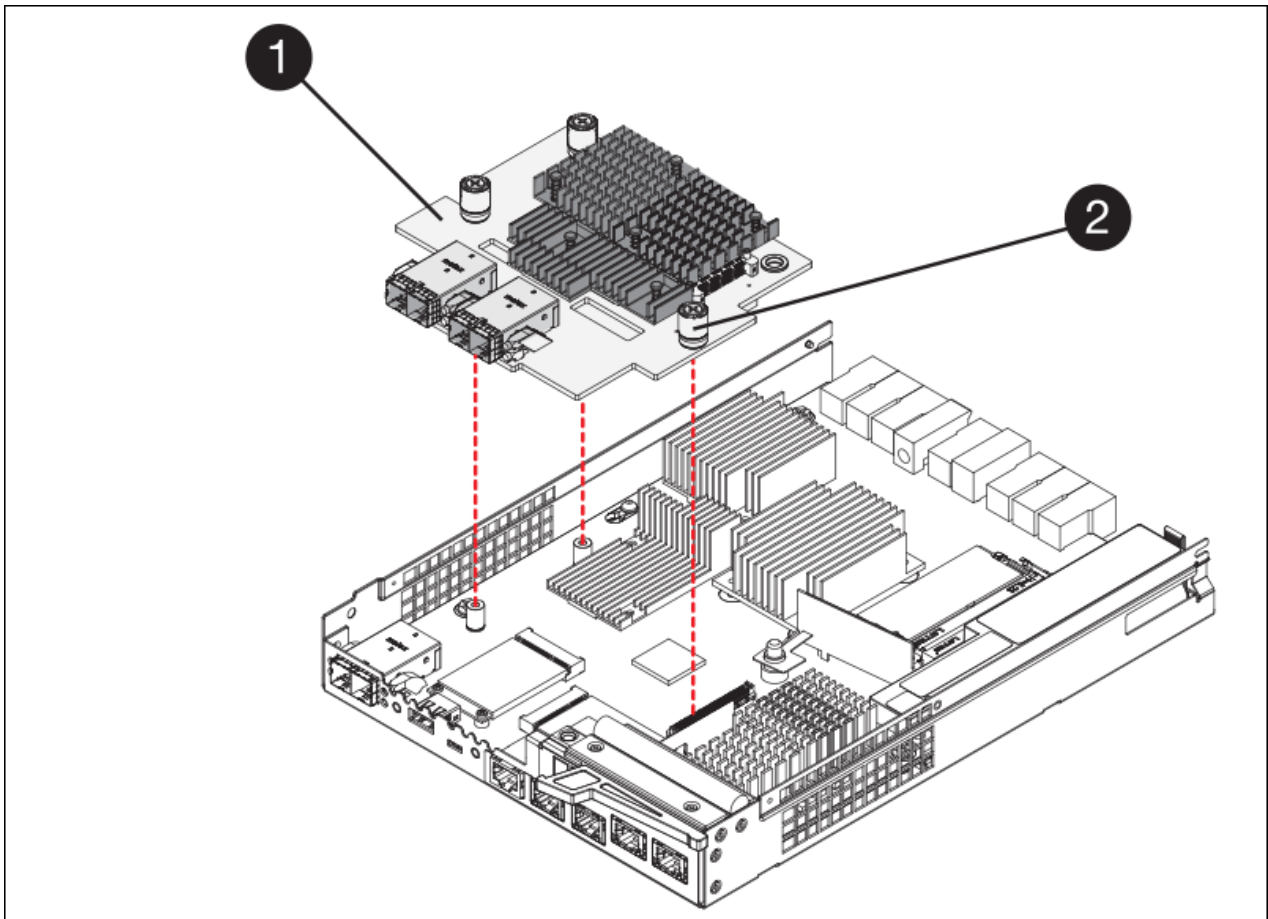
There are four screws: one on the top, one on the side, and two on the front.



3. Remove the HIC faceplate.
4. Using your fingers or a Phillips screwdriver, loosen the three thumbscrews that secure the HIC to the controller card.
5. Carefully detach the HIC from the controller card by lifting the card up and sliding it back.



Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.



Label	Description
1	Host interface card
2	Thumbscrews

6. Place the HIC on a static-free surface.
7. Using a #1 Phillips screwdriver, remove the four screws that attach the blank faceplate to the replacement controller, and remove the faceplate.
8. Align the three thumbscrews on the HIC with the corresponding holes on the replacement controller, and align the connector on the bottom of the HIC with the HIC interface connector on the controller card.

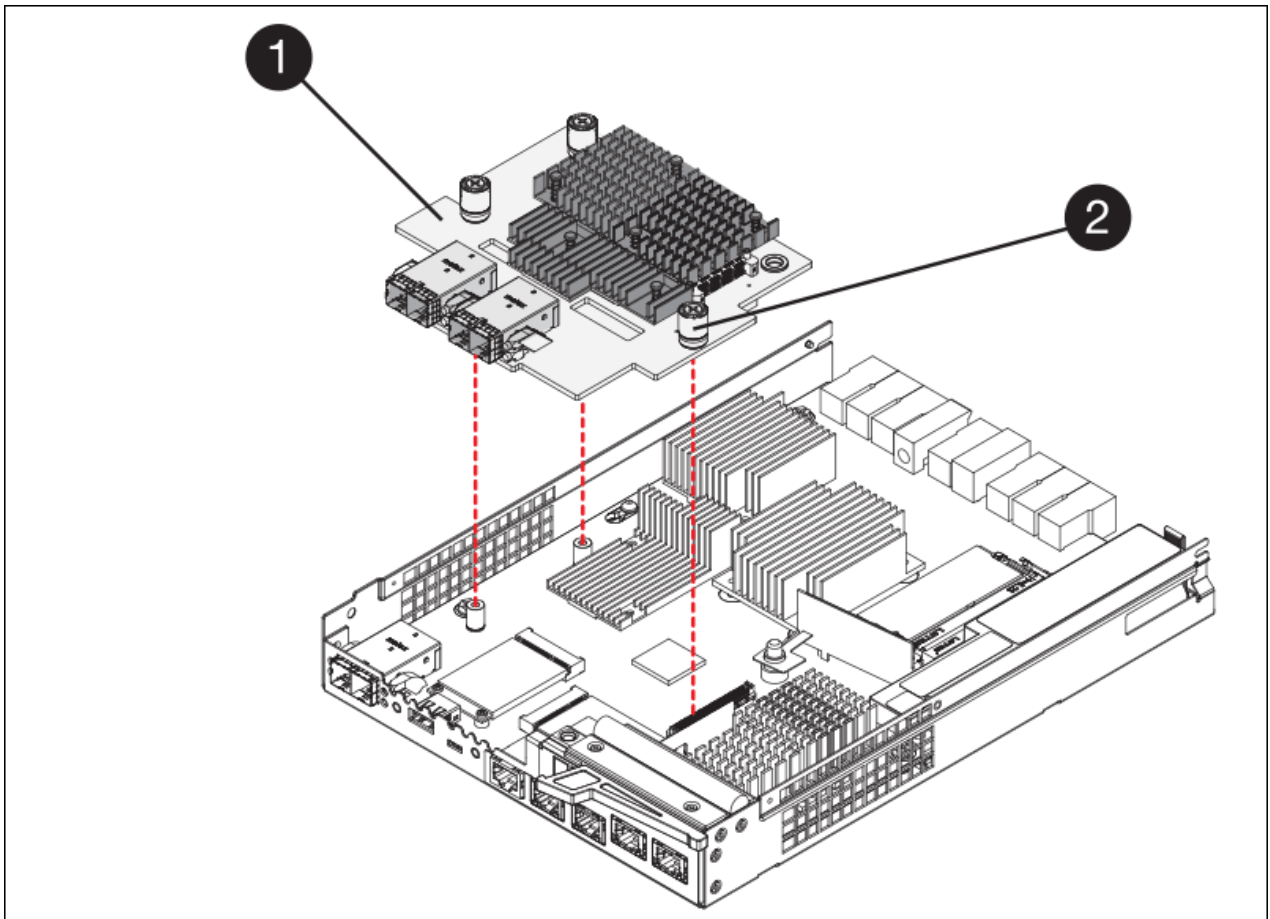
Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.

9. Carefully lower the HIC into place, and seat the HIC connector by pressing gently on the HIC.



**Possible equipment damage** — Be careful not to pinch the gold ribbon connector for the controller LEDs between the HIC and the thumbscrews.



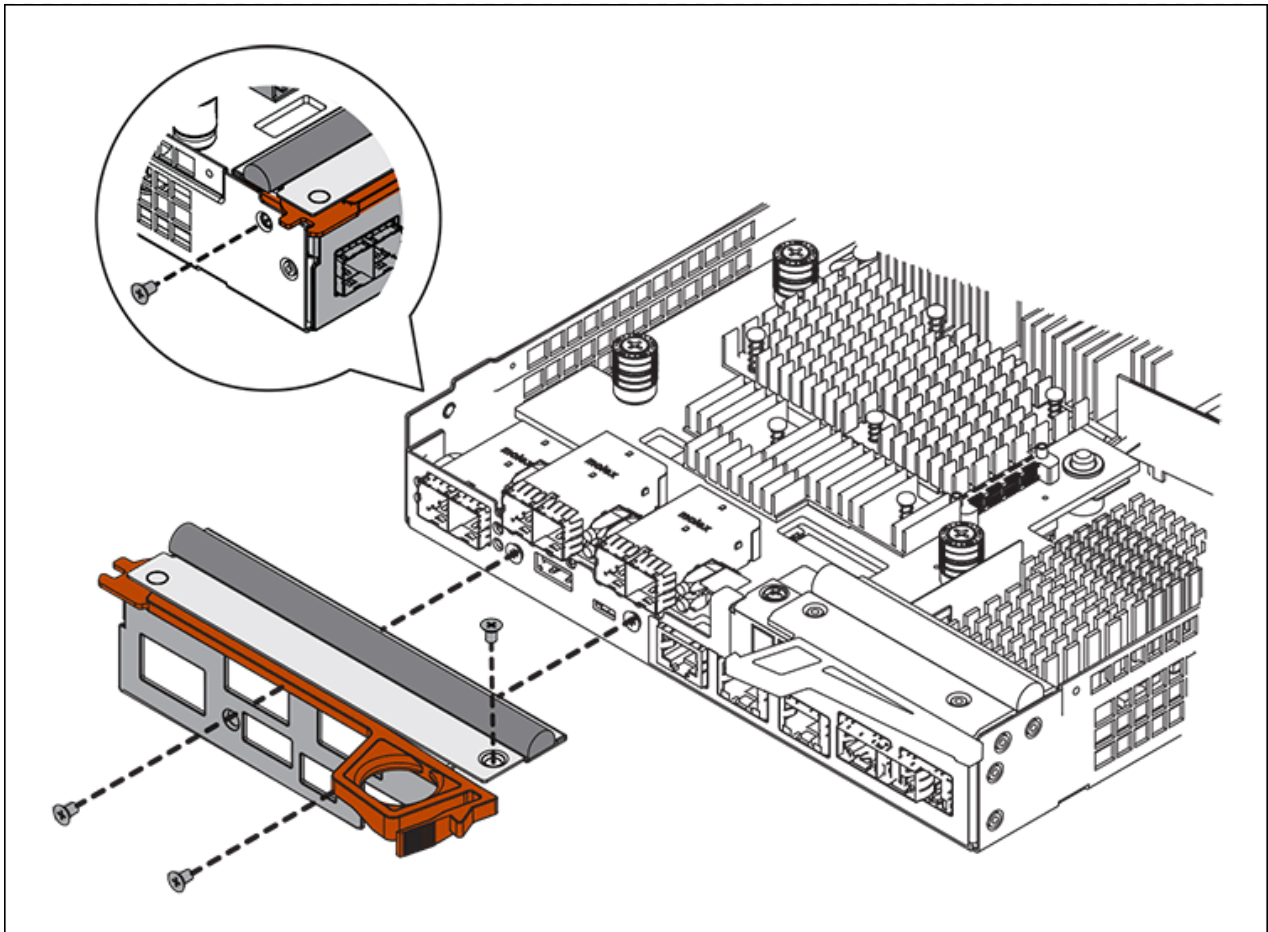


Label	Description
1	Host interface card
2	Thumbscrews

10. Hand-tighten the HIC thumbscrews.

Don't use a screwdriver, or you might over tighten the screws.

11. Using a #1 Phillips screwdriver, attach the HIC faceplate you removed from the original controller to the new controller with four screws.



12. Reinstall any removed SFPs into the HIC.

### Step 6: Replace controller

Install the replacement controller and verify that it has rejoined the grid.

#### Steps

1. Install the replacement controller into the appliance.
  - a. Turn the controller over, so that the removable cover faces down.
  - b. With the cam handle in the open position, slide the controller all the way into the appliance.
  - c. Move the cam handle to the left to lock the controller in place.
  - d. Replace the cables and SFPs.
  - e. Power on the controller shelf.
  - f. If the original controller used DHCP for the IP address, locate the MAC address on the label on the back of the replacement controller. Ask your network administrator to associate the DNS/network and IP address for the controller you removed with the MAC address for the replacement controller.



If the original controller did not use DHCP for the IP address, the new controller will adopt the IP address of the controller you removed.

2. Bring the controller online using SANtricity System Manager:

- a. Select **Hardware**.
  - b. If the graphic shows the drives, select **Show back of shelf**.
  - c. Select the controller you want to place online.
  - d. Select **Place Online** from the context menu, and confirm that you want to perform the operation.
  - e. Verify that the seven-segment display shows a state of 99.
3. Confirm that the new controller is Optimal, and collect support data.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return & Replacements](#) page for further information.

## Replace hardware components in SG6000 storage controller shelf

If a hardware problem occurs, you might need to replace a component in the storage controller shelf.

### Before you begin

- You have the E-Series hardware replacement procedure.
- You have physically located the storage appliance where you are replacing storage shelf hardware components in the data center.

[Locate controller in data center](#)

### About this task

To replace the battery in the storage controller, see the steps in the instructions for [replacing a storage controller](#). Those instructions describe how to remove a controller from the appliance, remove the battery from the controller, install the battery, and replace the controller.

For instructions for the other field replaceable units (FRUs) in the controller shelves, access the [E-Series procedures for system maintenance](#).

FRU	See instructions
Battery	StorageGRID (these instructions): <a href="#">Replacing a storage controller</a>
Drive	E-Series: <ul style="list-style-type: none"> <li>• Replace drive (60-drive)</li> <li>• Replace drive (12-drive or 24-drive)</li> </ul>
Power canister	E-Series <ul style="list-style-type: none"> <li>• Replace power canister (60-drive)</li> <li>• Replace power supply (12-drive or 24-drive)</li> </ul>
Fan canister (60-drive shelves only)	E-Series: <a href="#">Replace fan canister (60-drive)</a>

FRU	See instructions
Drive drawer (60-drive shelves only)	E-Series: Replace drive drawer (60-drive)

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return & Replacements](#) page for further information.

### Replace hardware components in optional SG6000 60-drive expansion shelf

You might need to replace an input/output module, a power supply, or a fan in the expansion shelf.

#### Before you begin

- You have the E-Series hardware replacement procedure.
- You have physically located the storage appliance where you are replacing expansion shelf hardware components in the data center.

[Locate controller in data center](#)

#### About this task

To replace an input/output module (IOM) in a 60-drive expansion shelf, see the steps in the instructions for [replacing a storage controller](#).

To replace a power supply or a fan in a 60-drive expansion shelf, access the E-Series procedures for maintaining 60-drive hardware.

FRU	See E-Series instructions for
Input/output module (IOM)	Replacing an IOM
Power canister	Replace power canister (60-drive)
Fan canister	Replace fan canister (60-drive)

### Replace SG6000-CN controller

You might need to replace the SG6000-CN controller if it is not functioning optimally or if it has failed.

#### Before you begin

- You have a replacement controller with the same part number as the controller you are replacing.
- You have labels to identify each cable that is connected to the controller.
- You have physically located the controller to replace in the data center.

[Locate controller in data center](#)

#### About this task

The appliance Storage Node will not be accessible when you replace the SG6000-CN controller. If the SG6000-CN controller is functioning sufficiently, you can perform a controlled shutdown at the start of this procedure.



If you are replacing the controller before installing StorageGRID software, you might not be able to access the StorageGRID Appliance Installer immediately after completing this procedure. While you can access the StorageGRID Appliance Installer from other hosts on the same subnet as the appliance, you can't access it from hosts on other subnets. This condition should resolve itself within 15 minutes (when any ARP cache entries for the original controller time out), or you can clear the condition immediately by purging any old ARP cache entries manually from the local router or gateway.

## Steps

1. Display the current configurations of the appliance and record them.
  - a. Log in to the appliance to be replaced:
    - i. Enter the following command: `ssh admin@grid_node_IP`
    - ii. Enter the password listed in the `Passwords.txt` file.
    - iii. Enter the following command to switch to root: `su -`
    - iv. Enter the password listed in the `Passwords.txt` file.

When you are logged in as root, the prompt changes from `$` to `#`.
  - b. Enter: **`run-host-command ipmitool lan print`** to display the current BMC configurations for the appliance.
2. If the SG6000-CN controller is functioning sufficiently to allow for a controlled shutdown, [shut down the SG6000-CN controller](#).
3. If any of the network interfaces on this StorageGRID appliance are configured for DHCP, you might need to update the permanent DHCP lease assignments on the DHCP servers to reference the MAC addresses of the replacement appliance. The update ensures the appliance is assigned the expected IP addresses. See [Update MAC address references](#).
4. Remove and replace the SG6000-CN controller:
  - a. Label the cables and then disconnect the cables and any SFP+ or SFP28 transceivers.



To prevent degraded performance, don't twist, fold, pinch, or step on the cables.

- b. Remove the failed controller from the cabinet or rack.
- c. Install the replacement controller into the cabinet or rack.
- d. Replace the cables and any SFP+ or SFP28 transceivers.
- e. Power on the controller and [monitor the controller LEDs](#) and [boot-up codes](#).

When the controller starts, it automatically installs pending updates for the controller and appliance components. Installation of these updates can take an hour or more to complete, and the controller might reboot multiple times.



Do not manually reboot the appliance unless you are certain that it is *not* in the middle of a firmware update.

You can connect a [monitor](#) or [service laptop](#) to the SG6000-CN controller to monitor update installation progress.



A service-laptop connection might not be available at some stages of the installation process.

5. If the appliance where you replaced the controller used a key management server (KMS) to encrypt data, additional configuration might be required before the node can join the grid. If the node does not automatically join the grid, make sure that these configuration settings have transferred to the new controller and manually configure any settings that don't have the expected configuration:
  - [Configure network links](#)
  - [Configure StorageGRID IP addresses](#)
  - [Configure node encryption for the appliance](#)
6. Log in to the appliance with the replaced controller:
  - a. Enter the following command: `ssh admin@grid_node_IP`
  - b. Enter the password listed in the `Passwords.txt` file.
  - c. Enter the following command to switch to root: `su -`
  - d. Enter the password listed in the `Passwords.txt` file.
7. Restore BMC network connectivity for the appliance. There are two options:
  - Use static IP, netmask, and gateway
  - Use DHCP to obtain an IP, netmask, and gateway
    - a. To restore the BMC configuration to use a static IP, netmask, and gateway, enter the following commands:

```
run-host-command ipmitool lan set 1 ipsrc static

run-host-command ipmitool lan set 1 ipaddr Appliance_IP

run-host-command ipmitool lan set 1 netmask Netmask_IP

run-host-command ipmitool lan set 1 defgw ipaddr Default_gateway
```
    - b. To restore the BMC configuration to use DHCP to obtain an IP, netmask, and gateway, enter the following command:

```
run-host-command ipmitool lan set 1 ipsrc dhcp
```
8. After restoring BMC network connectivity, connect to the BMC interface to audit and restore any additional custom BMC configuration you might have applied. For example, you should confirm the settings for SNMP trap destinations and email notifications. See [Configure BMC interface](#).
9. Confirm that the appliance node appears in the Grid Manager and that no alerts appear.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return & Replacements](#) page for further information.

## Related information

[Install SG6000-CN into cabinet or rack](#)

[View status indicators](#)

[View boot-up codes for SG6000-CN controller](#)

## Replace one or both power supplies in the SG6000-CN controller

The SG6000-CN controller has two power supplies for redundancy. If one of the power supplies fails, you must replace it as soon as possible to ensure that the compute controller has redundant power. Both power supplies operating in the controller must be the same model and wattage.

### Before you begin

- You have determined the physical location in the data center of the controller with the power supply to be replaced.

#### [Locating the controller in a data center](#)

- If you are replacing only one power supply:
  - You have unpacked the replacement power supply unit and ensured that it is the same model and wattage as the power supply unit you are replacing.
  - You have confirmed that the other power supply is installed and running.
- If you are replacing both power supplies at the same time:
  - You have unpacked the replacement power supply units and ensured they are the same model and wattage.

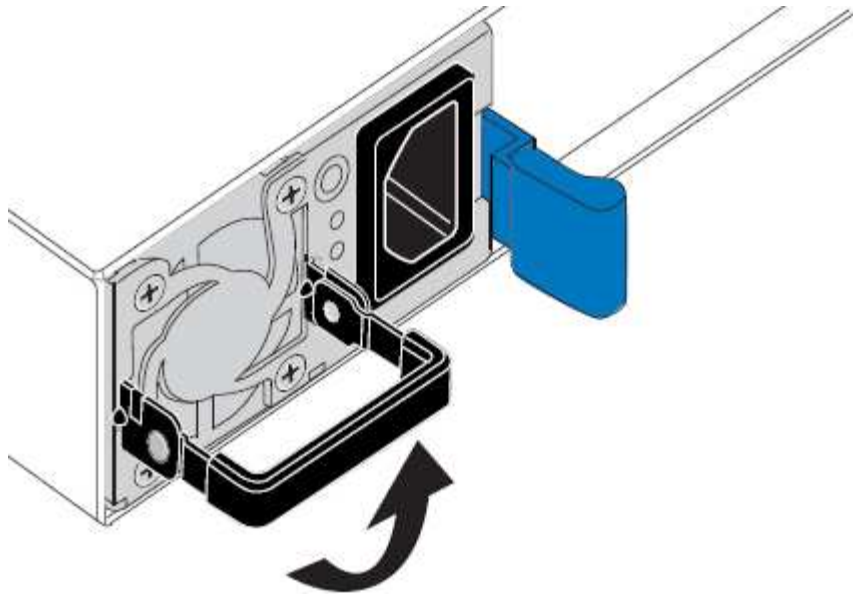
### About this task

The figure shows the two power supply units for the SG6000-CN controller, which are accessible from the back of the controller. Use this procedure to replace one or both of the power supplies. If you are replacing both power supplies, you must first perform a controlled shut down of the appliance.

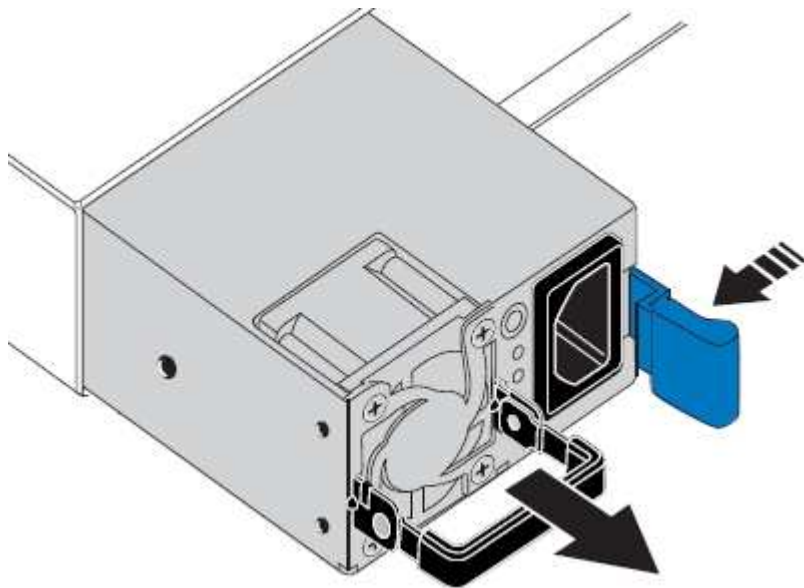


### Steps

1. If you are replacing only one power supply, you don't need to shut down the appliance. Go to the [Unplug the power cord](#) step. If you are replacing both power supplies at the same time, do the following before unplugging the power cords:
  - a. [Shut down the appliance](#).
2. Unplug the power cord from each power supply to be replaced.
3. Lift the cam handle on the first supply to be replaced.



4. Press the blue latch and pull the power supply out.



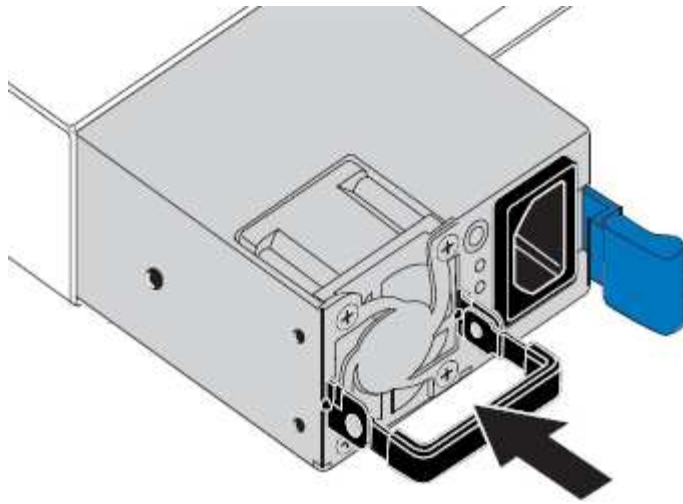
5. With the blue latch on the right, slide the replacement power supply into the chassis.



Both power supplies must be the same model and wattage.

Ensure that the blue latch is on the right side when you slide the replacement unit in.





6. Push the cam handle down to secure the replacement power supply.
7. If you are replacing both power supplies, repeat steps 2 through 6 to replace the second power supply.
8. [Connect the power cords to the replaced units and apply power.](#)

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return & Replacements](#) page for further information.

### Relocate SG6000-CN controller in cabinet or rack

Remove the SG6000-CN controller from a cabinet or rack to access the top cover or to move the appliance to a different location, then reinstall the controller into a cabinet or rack when hardware maintenance is complete.

### Remove SG6000-CN controller from cabinet or rack

Remove the SG6000-CN controller from a cabinet or rack to access the top cover or to move the controller to a different location.

### Before you begin

- You have labels to identify each cable that is connected to the SG6000-CN controller.
- You have physically located the SG6000-CN controller where you are performing maintenance in the data center.

#### [Locate controller in data center](#)

- You have [shut down the SG6000-CN controller](#).



Don't shut down the controller using the power switch.

### Steps

1. Label and then disconnect the controller power cables.
2. Wrap the strap end of the ESD wristband around your wrist, and secure the clip end to a metal ground to prevent static discharge.
3. Label and then disconnect the controller data cables and any SFP+ or SFP28 transceivers.



To prevent degraded performance, don't twist, fold, pinch, or step on the cables.

4. Loosen the two captive screws on the controller front panel.



5. Slide the SG6000-CN controller forward out of the rack until the mounting rails are fully extended and you hear the latches on both sides click.

The controller top cover is accessible.

6. Optional: If you are fully removing the controller from the cabinet or rack, follow the instructions for the rail kit to remove the controller from the rails.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return & Replacements](#) page for further information.

#### **Reinstall SG6000-CN controller into cabinet or rack**

Reinstall the controller into a cabinet or rack when hardware maintenance is complete.

#### **Before you begin**

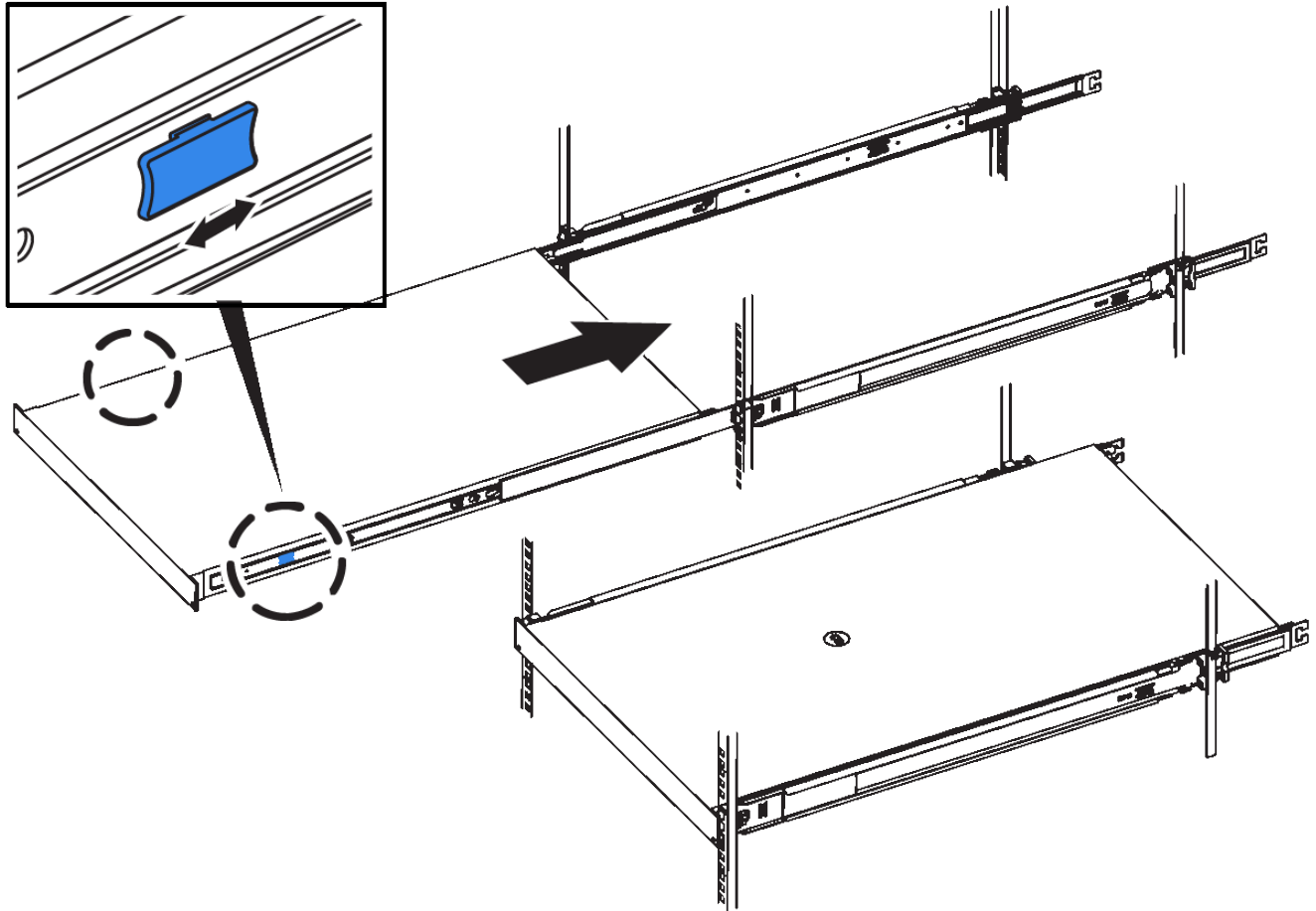
You have reinstalled the controller cover.

#### [Reinstall SG6000-CN controller cover](#)

#### **Steps**

1. Press the blue rail releases both rack rails at the same time and slide the SG6000-CN controller into the rack until it is fully seated.

When you can't move the controller any further, pull the blue latches on both sides of the chassis to slide the controller all the way in.



Don't attach the front bezel until after you power on the controller.

2. Tighten the captive screws on the controller front panel to secure the controller in the rack.



3. Wrap the strap end of the ESD wristband around your wrist, and secure the clip end to a metal ground to prevent static discharge.
4. Reconnect the controller data cables and any SFP+ or SFP28 transceivers.



To prevent degraded performance, don't twist, fold, pinch, or step on the cables.

#### Cable appliance

5. Reconnect the controller power cables.

#### Connect power cords and apply power (SG6000)

#### After you finish

The controller can be restarted [restarted](#).

## Replace SG6000 controller cover

Remove the appliance cover to access internal components for maintenance, and replace the cover when you are finished.

### Remove SG6000-CN controller cover

Remove the controller cover to access internal components for maintenance.

#### Before you begin

Remove the controller from the cabinet or rack to access the top cover.

### Remove SG6000-CN controller from cabinet or rack

#### Steps

1. Make sure that the SG6000-CN controller cover latch is not locked. If necessary, turn the blue plastic latch lock one-quarter turn in the unlock direction, as shown on the latch lock.
2. Rotate the latch up and back toward the rear of the SG6000-CN controller chassis until it stops; then, carefully lift the cover from the chassis and set it aside.



Wrap the strap end of an ESD wristband around your wrist and secure the clip end to a metal ground to prevent static discharge when working inside the SG6000-CN controller.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return & Replacements](#) page for further information.

### Reinstall SG6000-CN controller cover

Reinstall the controller cover when internal hardware maintenance is complete.

#### Before you begin

You have completed all maintenance procedures inside the controller.

## Steps

1. With the cover latch open, hold the cover above the chassis and align the hole in the top cover latch with the pin in the chassis. When the cover is aligned, lower it onto the chassis.



2. Rotate the cover latch forward and down until it stops and the cover fully seats into the chassis. Verify that there are no gaps along the front edge of the cover.

If the cover is not fully seated, you might not be able to slide the SG6000-CN controller into the rack.

3. Optional: Turn the blue plastic latch lock one-quarter turn in the lock direction, as shown on the latch lock, to lock it.

## After you finish

[Reinstall the controller in the cabinet or rack.](#)

## Replace Fibre Channel HBA in SG6000

You might need to replace a Fibre Channel HBA if it is not functioning optimally or if it has failed.

### Verify Fibre Channel HBA to replace

If you are unsure which Fibre Channel host bus adapter (HBA) to replace, complete this procedure to identify it.

### Before you begin

- You have the serial number of the storage appliance or SG6000-CN controller where the Fibre Channel HBA needs to be replaced.



If the serial number of the storage appliance containing the Fibre Channel HBA you are replacing starts with the letter Q, it will not be listed in the Grid Manager. You must check the tags attached to the front of each SG6000-CN controller in the data center until you find a match.

- You are signed in to the Grid Manager using a [supported web browser](#).

## Steps

1. From the Grid Manager, select **NODES**.
2. From the table on the Nodes page, select an appliance Storage Node.

3. Select the **Hardware** tab.

Check the **Storage appliance chassis serial number** and the **Compute controller serial number** in the StorageGRID Appliance section. See if one of these serial numbers matches the serial number of the storage appliance where you are replacing the Fibre Channel HBA. If either serial number matches, you have found the correct appliance.

### StorageGRID Appliance

Appliance model: ?	SG5660	
Storage controller name: ?	StorageGRID-SGA-Lab11	
Storage controller A management IP: ?	10.224.2.192	
Storage controller WWID: ?	600a098000a4a707000000005e8ed5fd	
Storage appliance chassis serial number: ?	1142FG000135	
Storage controller firmware version: ?	08.40.60.01	
Storage hardware: ?	Nominal	
Storage controller failed drive count: ?	0	
Storage controller A: ?	Nominal	
Storage controller power supply A: ?	Nominal	
Storage controller power supply B: ?	Nominal	
Storage data drive type: ?	NL-SAS HDD	
Storage data drive size: ?	2.00 TB	
Storage RAID mode: ?	RAID6	
Storage connectivity: ?	Nominal	
Overall power supply: ?	Nominal	
Compute controller serial number: ?	SV54365519	
Compute controller CPU temperature: ?	Nominal	
Compute controller chassis temperature: ?	Nominal	

### Storage shelves

Shelf chassis serial number ?	Shelf ID ?	Shelf status ?	IOM status ?
SN SV13304553	0	Nominal	N/A

- If the StorageGRID Appliance section does not display, the node selected is not a StorageGRID appliance. Select a different node from the tree view.
- If the Appliance Model is not SG6060 or SG6060X, select a different node from the tree view.
- If the serial numbers don't match, select a different node from the tree view.

4. After you locate the node where the Fibre Channel HBA needs to be replaced, write down the Compute controller BMC IP address listed the StorageGRID Appliance section.

You can use this IP address to [turn on the compute controller identify LED](#), to help you locate the appliance in the data center.

## Remove Fibre Channel HBA

You might need to replace the Fibre Channel host bus adapter (HBA) in the SG6000-CN controller if it is not functioning optimally or if it has failed.

### Before you begin

- You have the correct replacement Fibre Channel HBA.
- You have [determined which SG6000-CN controller contains the Fibre Channel HBA to replace](#).
- You have [physically located the SG6000-CN controller](#) in the data center.
- You have [shut down the SG6000-CN controller](#).



A controlled shutdown is required before you remove the controller from the rack.

- You have [removed the controller from the cabinet or rack](#).
- You have [removed the controller cover](#).

### About this task

To prevent service interruptions, confirm that all other Storage Nodes are connected to the grid before starting the Fibre Channel HBA replacement or replace the adapter during a scheduled maintenance window when periods of service disruption are acceptable. See the information about [monitoring node connection states](#).

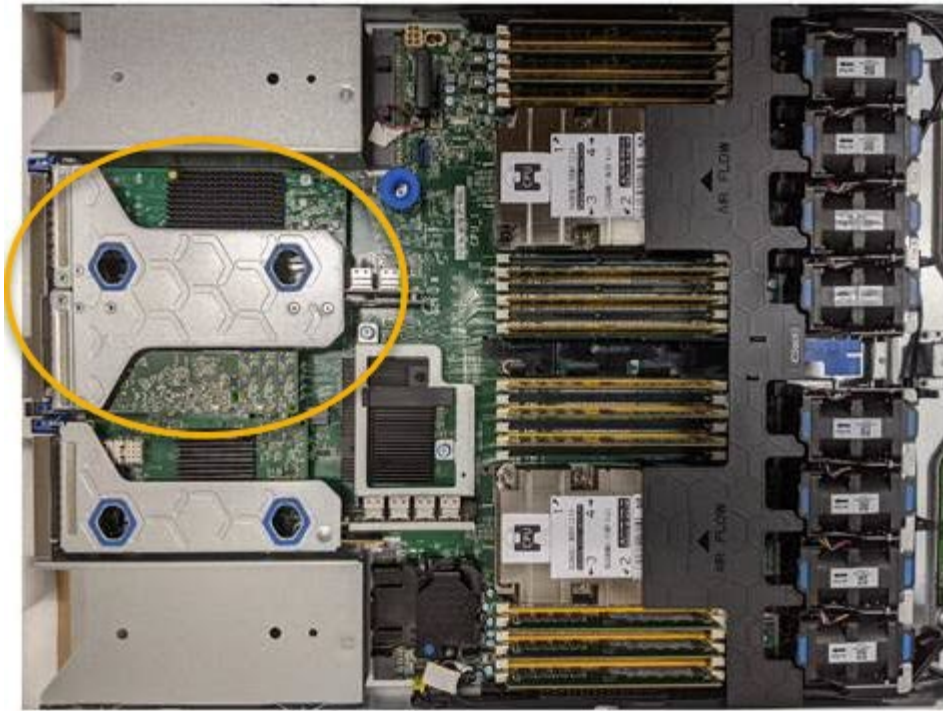


If you have ever used an ILM rule that creates only one copy of an object, you must replace the Fibre Channel HBA during a scheduled maintenance window. Otherwise, you might temporarily lose access to those objects during this procedure.

See information about [why you should not use single-copy replication](#).

### Steps

1. Wrap the strap end of the ESD wristband around your wrist, and secure the clip end to a metal ground to prevent static discharge.
2. Locate the riser assembly at the rear of the controller that contains the Fibre Channel HBA.



3. Grasp the riser assembly through the blue-marked holes and carefully lift it upwards. Move the riser assembly toward the front of the chassis as you lift it to allow the external connectors in its installed adapters to clear the chassis.
4. Place the riser card on a flat anti-static surface with the metal frame side down to access the adapters.



There are two adapters in the riser assembly: a Fibre Channel HBA and an Ethernet network adapter. The Fibre Channel HBA is indicated in the illustration.

5. Open the blue adapter latch (circled) and carefully remove the Fibre Channel HBA from the riser assembly. Rock the adapter slightly to help remove the adapter from its connector. Don't use excessive force.
6. Place the adapter on a flat anti-static surface.

#### After you finish

[Install the replacement Fibre Channel HBA.](#)

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return & Replacements](#) page for further information.



## Reinstall Fibre Channel HBA

The replacement Fibre Channel HBA is installed into the same location as the one that was removed.

### Before you begin

- You have the correct replacement Fibre Channel HBA.
- You have removed the existing Fibre Channel HBA.

### Remove Fibre Channel HBA

### Steps

1. Wrap the strap end of the ESD wristband around your wrist, and secure the clip end to a metal ground to prevent static discharge.
2. Remove the replacement Fibre Channel HBA from its packaging.
3. With the blue adapter latch in the open position, align the Fibre Channel HBA with its connector on the riser assembly; then, carefully press the adapter into the connector until it is fully seated.



There are two adapters in the riser assembly: a Fibre Channel HBA and an Ethernet network adapter. The Fibre Channel HBA is indicated in the illustration.

4. Locate the alignment hole on the riser assembly (circled) that aligns with a guide pin on the system board to ensure correct riser assembly positioning.



5. Position the riser assembly in the chassis, making sure that it aligns with the connector and guide pin on the system board; then, insert the riser assembly.

- Carefully press the riser assembly in place along its center line, next to the blue-marked holes, until it is fully seated.
- Remove the protective caps from the Fibre Channel HBA ports where you will be reinstalling cables.

### After you finish

If you have no other maintenance procedures to perform in the controller, [reinstall the controller cover](#).

## Maintain SG6100 storage appliance hardware

### Maintain SG6100 appliance

You might need to perform maintenance procedures on your appliance. Procedures specific to maintaining your SG6100 appliance are in this section.

The procedures in this section assume that the appliance has already been deployed as a Storage Node in a StorageGRID system.

**Configuration maintenance procedures** are performed using the Appliance Installer, Grid Manager, or BMC interface. These procedures include:

- [Turn appliance identify LED on and off](#)
- [Locate appliance in data center](#)
- [Shut down the appliance](#)
- [Change link configuration of the appliance](#)

**Hardware maintenance procedures** require the physical manipulation of specific SGF6112 components.

### Drive firmware upgrade

The firmware on the drives in the SGF6112 is automatically checked every time the appliance is rebooted. When necessary, the firmware is automatically upgraded to the version expected by the current StorageGRID release. Usually, firmware upgrades occur during StorageGRID software upgrades. Any necessary drive firmware upgrades for existing StorageGRID versions will be included in hotfixes. Follow the instructions provided with each hotfix to ensure that the upgrade is applied to all drives that could benefit from it.



SANtricity System Manager is not needed to maintain the SGF6112 appliance.

### General Maintenance procedures

See [Common maintenance procedures](#) for procedures that are the same for all appliances, such as applying a hotfix, recovering a node or site, and performing network maintenance.

See [Set up appliance hardware](#) for appliance maintenance procedures that are also performed during initial appliance installation and configuration.

## Configuration maintenance procedures

### Use the Manage drives tab

You can use the Manage drives tab in the Grid Manager to perform troubleshooting and

maintenance tasks on the drives in the SGF6112 appliance.

### Before you begin

- You are signed in to the Grid Manager using a [supported web browser](#).

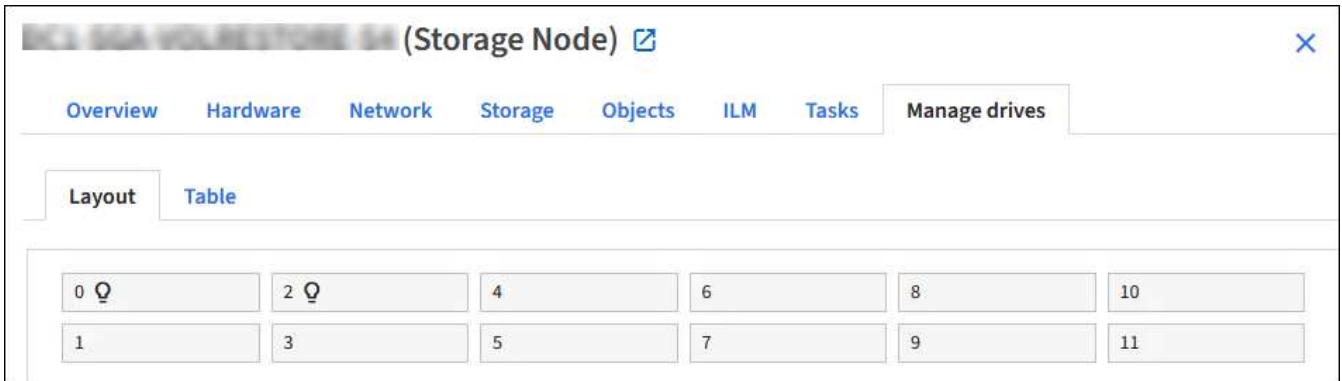
### About this task

If you have an SGF6112 appliance and either the [Storage appliance administrator](#) or [Root access permission](#), a Manage drives tab appears on the appliance details page.

The Manage drives tab contains the following views:

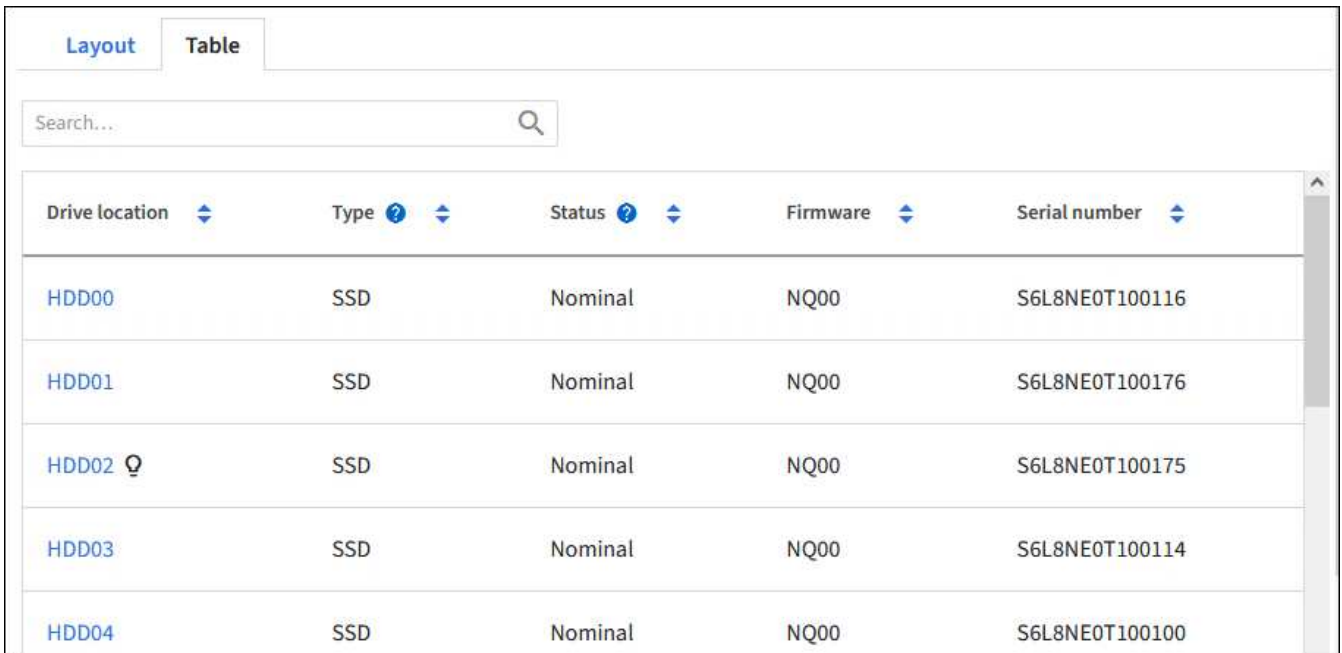
### Layout

Layout of data storage drives in the appliance. Select a drive to view drive details.



### Table

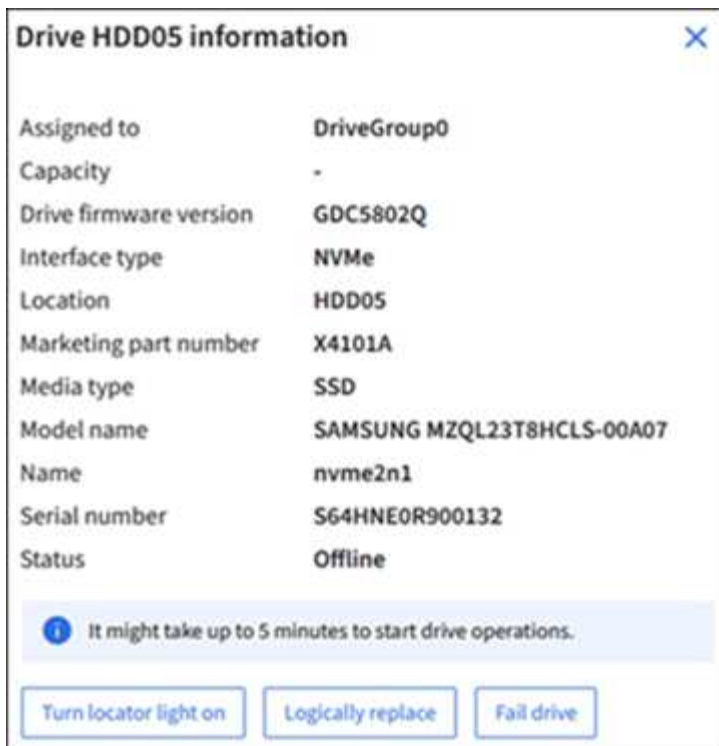
Lists information for each drive. Select a drive to view drive details.



Drive location	Type	Status	Firmware	Serial number
HDD00	SSD	Nominal	NQ00	S6L8NE0T100116
HDD01	SSD	Nominal	NQ00	S6L8NE0T100176
HDD02	SSD	Nominal	NQ00	S6L8NE0T100175
HDD03	SSD	Nominal	NQ00	S6L8NE0T100114
HDD04	SSD	Nominal	NQ00	S6L8NE0T100100

### Drive details

Summary for each drive. Select the appropriate task button, as described in the steps below.




### Turn locator light on or off

To physically locate a drive in the appliance:

1. From the Grid Manager, select **NODES > data center**.
2. Select **appliance storage node > Manage drives > Layout > drive**.

The drive details panel appears.

3. Select **Turn locator light on**.
  - A light bulb icon  appears for the drive.
  - An amber LED blinks on the physical drive.
4. When you want to turn off the locator light, select **Turn locator light off**.

### Logically replace drive

If a drive in the storage appliance needs to be rebuilt or reinitialized:

1. From the Grid Manager, select **NODES > data center**.
2. Select **appliance storage node > Manage drives > Layout > drive**.

The drive details panel appears.

3. Select **Logically replace**.

On the drive details panel, the drive's status indicates *Rebuilding*. Rebuilding a drive could take up to 5 minutes.

## Fail drive

For troubleshooting, you can manually "fail" a drive that you suspect is faulty. The system will then run without that drive.

1. From the Grid Manager, select **NODES > data center**.
2. Select **appliance storage node > Manage drives > Layout > drive**.

The drive details panel appears.

3. Select **Fail drive**.

After you fail a drive, you must either physically replace the drive or [logically replace the drive](#).

## Turn SGF6112 appliance identify LED on and off

The blue identify LED on the front and back of the appliance can be turned on to help locate the appliance in a data center.

### Before you begin

You have the BMC IP address of the appliance you want to identify.

### Steps

1. [Access the appliance BMC interface](#).
2. Select **Server Identify**.

The current status of the identify LED is selected.

3. Select **ON** or **OFF**, and then select **Perform Action**.

When you select **ON**, the blue identify LEDs light on the front (typical shown) and rear of the appliance.



If a bezel is installed on the controller, it might be difficult to see the front identify LED.

The rear identify LED is at the center of the appliance below the Micro-SD slot.

4. Turn the identify LEDs on and off as needed.

### Related information

[Locate appliance in data center](#)

## Locate SGF6112 appliance in data center

Locate the appliance so that you can perform hardware maintenance or upgrades.

### Before you begin

- You have determined which appliance requires maintenance.
- To help locate the appliance in your data center, [turn on the blue identify LED](#).

### Steps

1. Find the appliance in the data center.
  - Look for a lit blue identify LED on the front or rear of the appliance.

The front identify LED is behind the front bezel and might be difficult to see if the bezel is installed.



The rear identify LED is at the center of the appliance below the Micro-SD slot.

- Check the tags attached to the front of the appliance for a matching part number to confirm you have found the correct appliance.
2. Remove the front bezel, if one is installed, to access the front panel controls and indicators.

### After you finish

[Turn off the blue identify LED](#) if you used it to locate the appliance.

**Press the identify LED switch on the appliance front panel.**

Use the appliance BMC interface.

## Power SGF6112 appliance off and on

You can shut down the SGF6112 appliance and power it back on to perform maintenance.

### Shut down the SGF6112 appliance

Shut down the appliance to perform hardware maintenance.

### Before you begin

- You have [physically located the appliance](#).

### About this task

To prevent service interruptions, shut down the appliance during a scheduled maintenance window when periods of service disruption are acceptable.

## Steps

1. Shut down the appliance:



You must perform a controlled shut down of the appliance by entering the commands specified below. It is a best practice to perform a controlled shutdown when possible to avoid unnecessary alerts, ensure full logs are available, and avoid service disruptions.

- a. If you have not already logged into the grid node, log in using PuTTY or another ssh client:
  - i. Enter the following command: `ssh admin@grid_node_IP`
  - ii. Enter the password listed in the `Passwords.txt` file.
  - iii. Enter the following command to switch to root: `su -`
  - iv. Enter the password listed in the `Passwords.txt` file.

When you are logged in as root, the prompt changes from `$` to `#`.

- b. Shut down the appliance:

**`shutdown -h now`**

This command might take up to 10 minutes to complete.

2. Use one of the following methods to verify that the appliance is powered off:
  - Look at the power LED on the front of the appliance and confirm that it is off.
  - Check the Power Control page of the BMC interface to confirm the appliance is off.

## Power on SGF6112 and verify operation

Power on the controller after completing maintenance.

### Before you begin

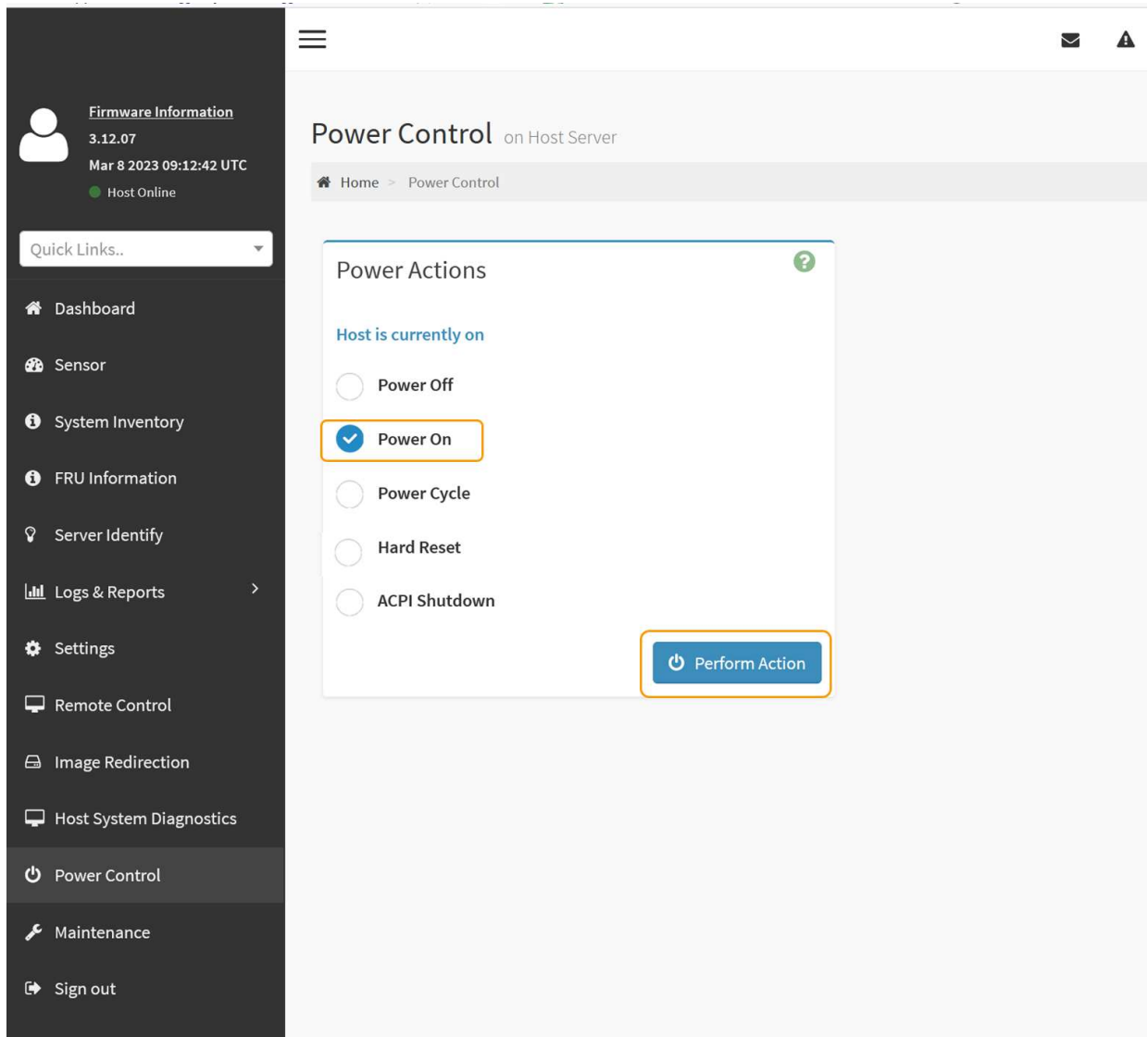
- You have [installed the controller in a cabinet or rack](#) and connected the data and power cables.
- You have [physically located the controller in the data center](#).

## Steps

1. Power on the appliance.

You might have to remove the bezel to access the power switch; if so, remember to reinstall it afterwards.

2. Monitor the controller LEDs and boot-up codes using one of the following methods:
  - Press the power switch on the front of the controller.
  - Use the controller BMC interface:
    - i. [Access the controller BMC interface](#).
    - ii. Select **Power Control**.
    - iii. Select **Power On** and then select **Perform Action**.



Use the BMC interface to monitor start-up status.

3. Confirm that the appliance controller displays in the Grid Manager and with no alerts.

It might take up to 20 minutes for the controller to display in the Grid Manager.



Don't take another appliance node offline unless this appliance has a green icon.

4. Confirm that the new appliance is fully operational by logging in to the grid node using PuTTY or another ssh client:
  - a. Enter the following command: `ssh Appliance_IP`
  - b. Enter the password listed in the `Passwords.txt` file.
  - c. Enter the following command to switch to root: `su -`
  - d. Enter the password listed in the `Passwords.txt` file.

When you are logged in as root, the prompt changes from `$` to `#`.

## Related information



## Change link configuration of SGF6112 appliance

You can change the Ethernet link configuration of the appliance including the port bond mode, the network bond mode, and the link speed.

### Before you begin

- You have [placed the appliance into maintenance mode](#).



In rare instances, placing a StorageGRID appliance into maintenance mode might make the appliance unavailable for remote access.

### Steps

1. From the StorageGRID Appliance Installer, select **Configure Networking > Link Configuration**.
2. Make the desired changes to the link configuration.

For more information about the options, see [Configure network links](#).



IP configuration changes made while the appliance is in maintenance mode are not applied to the installed StorageGRID environment. Run the `change-ip` [command](#) after rebooting the appliance into StorageGRID.

3. 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`**

4. Make any necessary changes to the IP addresses for the appliance.

If you made changes to the VLAN settings, the subnet for the appliance might have changed. If you need to change the IP addresses for the appliance, see [Configure StorageGRID IP addresses](#).


5. Select **Configure Networking > Ping Test** from the menu.
6. Use the Ping Test tool to check connectivity to IP addresses on any networks that might have been affected by the link configuration changes you made when configuring the appliance.

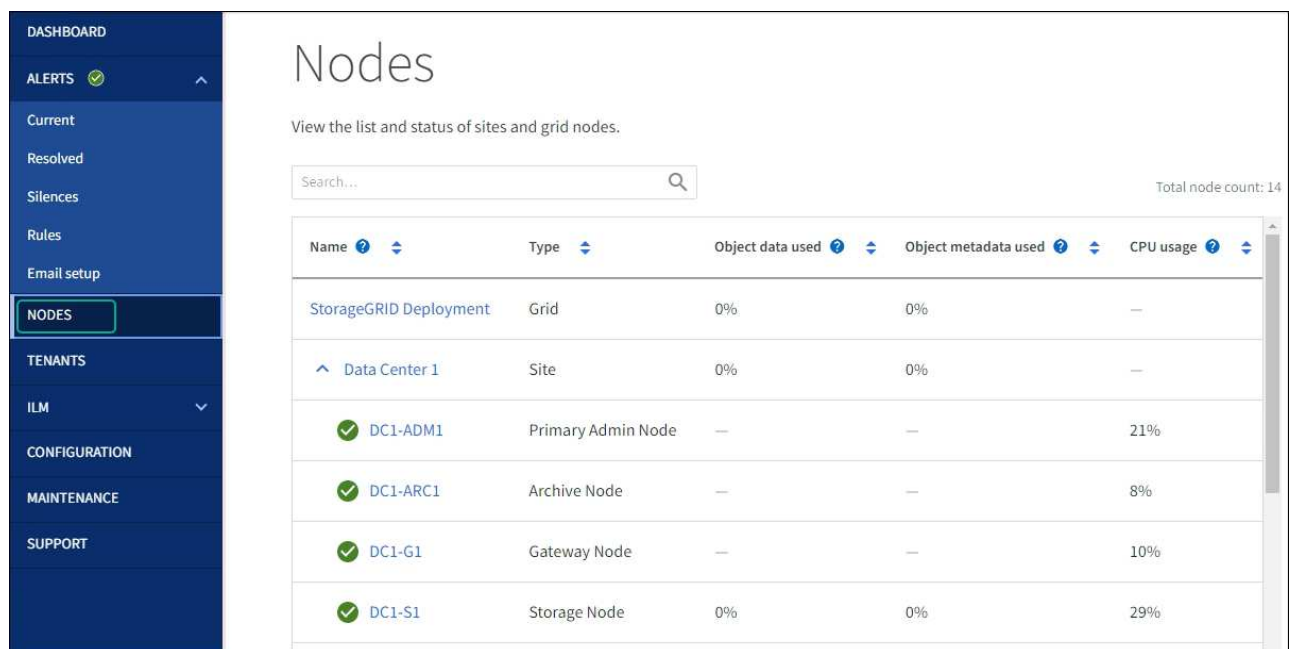
In addition to any other tests you choose to perform, confirm that you can ping the Grid Network IP address of the primary Admin Node, and the Grid Network IP address of at least one other node. If necessary, return to the instructions for configuring network links and correct any issues.

7. After you are satisfied that your link configuration changes are working, reboot the node. From the StorageGRID Appliance Installer, select **Advanced > Reboot Controller**, and then select one of these options:
  - Select **Reboot into StorageGRID** to reboot the compute controller with the node rejoining the grid. Select this option if you are done working in maintenance mode and are ready to return the node to normal operation.
  - Select **Reboot into Maintenance Mode** to reboot the compute controller with the node remaining in

maintenance mode. (This option is available only when the controller is in maintenance mode.) Select this option if there are additional maintenance operations you need to perform on the node before it rejoins the grid.



It can take up to 20 minutes for the appliance to reboot and rejoin the grid. To confirm that the reboot is complete and that the node has rejoined the grid, go back to the Grid Manager. The Nodes page should display a normal status (green check mark icon  to the left of the node name) for the appliance node, indicating that no alerts are active and the node is connected to the grid.



## Hardware maintenance procedures

### Verify component to replace in the SGF6112

If you are unsure which hardware component to replace in your appliance, complete this procedure to identify the component and the location of the appliance in the data center.

#### Before you begin

- You have the serial number of the storage appliance where the component needs to be replaced.

- You are signed in to the Grid Manager using a [supported web browser](#).

### About this task

Use this procedure to identify the appliance with failed hardware and which of the replaceable hardware components is not operating properly. Components that might be identified for replacement include:

- Power supplies
- Fans
- Solid state drives (SSDs)
- Network Interface Cards (NICs)
- CMOS battery

### Steps

1. Identify the failed component and the name of the appliance that it is installed in.
  - a. In Grid Manager, Select **ALERTS > Current**.

The Alerts page appears.

- b. Select the alert to see the alert details.



Select the alert, not the heading for a group of alerts.

- c. Record the node name and unique identifying label of the component that has failed.

## Appliance NIC fault detected


A problem with a network interface card (NIC) in the appliance was detected.

**Recommended actions**


1. Reseat the NIC. Refer to the instructions for your appliance.
2. If necessary, replace the NIC. See the maintenance instructions for your appliance.

**Time triggered**

2023-02-17 13:36:31 EST (2023-02-17 18:36:31 UTC)

Status  
Active (silence this alert )

Site / Node  
Data Center 1 **SGF6112-032-X6606A**

Severity  
 Critical

Description  
ConnectX-6 Lx EN adapter card,  
25GbE, Dual-port SFP28, PCIe 4.0 x8,  
No Crypto

Firmware Version  
26.33.1048 (MT\_0000000531)

**Device**  
hic3

Part number  
X1153A

2. Identify the chassis with the component that needs to be replaced.
  - a. From the Grid Manager, select **NODES**.

- b. From the table on the Nodes page, select the appliance Storage Node name with the failed component.
- c. Select the **Hardware** tab.

Check the **Compute controller serial number** in the StorageGRID Appliance section. Check if the serial number matches the serial number of the storage appliance where you are replacing the component. If the serial number matches, you have found the correct appliance.

- If the StorageGRID Appliance section in Grid Manager does not display, the node selected is not a StorageGRID appliance. Select a different node from the tree view.
  - If the serial numbers don't match, select a different node from the tree view.
3. After you locate the node where the component needs to be replaced, write down the appliance BMC IP address listed the StorageGRID Appliance section.

To help you locate the appliance in the data center, you can use the BMC IP address to turn on the appliance identify LED.

### Related information

[Turn on the appliance identify LED](#)

### Replace one or both power supplies in the SGF6112

The SGF6112 appliance has two power supplies for redundancy. If one of the power supplies fails, you must replace it as soon as possible to ensure that the appliance has redundant power. Both power supplies operating in the appliance must be of the same model and wattage.

### Before you begin

- You have [physically located the appliance](#) with the power supply to be replaced.
- You have [determined the location of the power supply to replace](#).
- If you are replacing only one power supply:
  - You have unpacked the replacement power supply unit and ensured that it is the same model and wattage as the power supply unit you are replacing.
  - You have confirmed that the other power supply is installed and running.
- If you are replacing both power supplies at the same time:
  - You have unpacked the replacement power supply units and ensured they are the same model and wattage.

### About this task

The figure shows the two power supply units for the SGF6112. The power supplies are accessible from the back of the appliance.



### Steps

1. If you are replacing only one power supply, you don't need to shut down the appliance. Go to the [Unplug](#)

the power cord step. If you are replacing both power supplies at the same time, do the following before unplugging the power cords:

- a. Shut down the appliance.

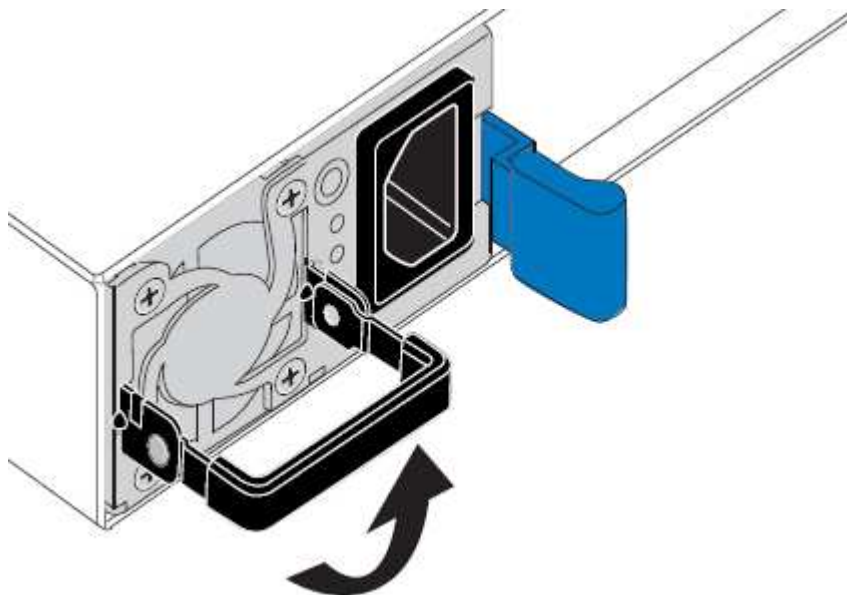


If you have ever used an ILM rule that creates only one copy of an object and you are replacing both power supplies at the same time, you must replace the power supplies during a scheduled maintenance window. Otherwise, you might temporarily lose access to those objects during this procedure. See information about [why you should not use single-copy replication](#).

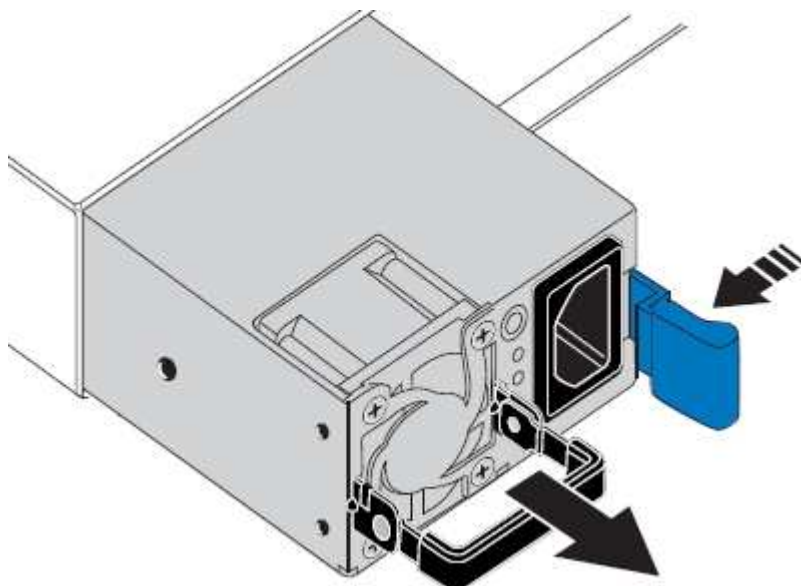
2. Unplug the power cord from each power supply to be replaced.

When viewed from the rear of the appliance, power supply A (PSU0) is on the right and power supply B (PSU1) is on the left.

3. Lift the handle on the first supply to be replaced.



4. Press the blue latch and pull the power supply out.



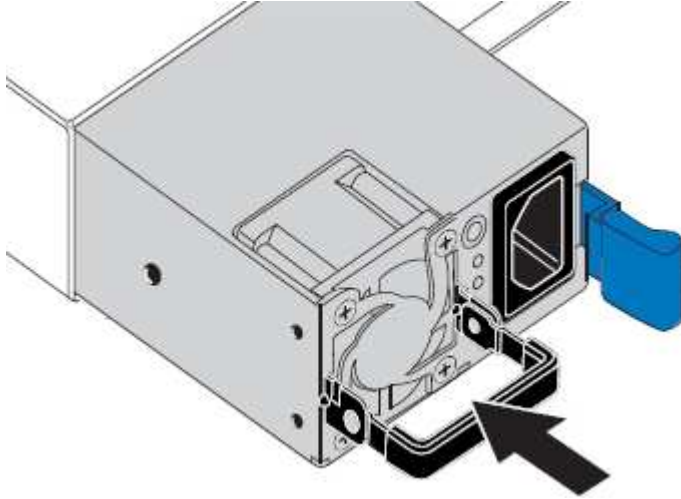
5. With the blue latch on the right, slide the replacement power supply into the chassis.



Both installed power supplies must be the same model and wattage.

Ensure that the blue latch is on the right side when you slide the replacement unit in.

You will feel a click when the power supply is locked into place.



6. Push the handle back down against the body of the PSU.

7. If you are replacing both power supplies, repeat steps 2 through 6 to replace the second power supply.

8. [Connect the power cords to the replaced units and apply power.](#)

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return & Replacements](#) page for further information.

## Replace fan in an SGF6112

The SGF6112 appliance has eight cooling fans. If one of the fans fails, you must replace it as soon as possible to ensure that the appliance has proper cooling.

### Before you begin

- You have the correct replacement fan.
- You have [determined the location of the fan to replace.](#)
- You have [physically located the SGF6112 appliance](#) where you are replacing the fan in the data center.



A [controlled shutdown of the appliance](#) is required before removing the appliance from the rack.

- You have disconnected all cables and [removed the appliance cover.](#)
- You have confirmed that the other fans are installed and running.

### About this task

To prevent service interruptions, confirm that all other Storage Nodes are connected to the grid before starting the fan replacement or replace the fan during a scheduled maintenance window when periods of service disruption are acceptable. See the information about [monitoring node connection states.](#)



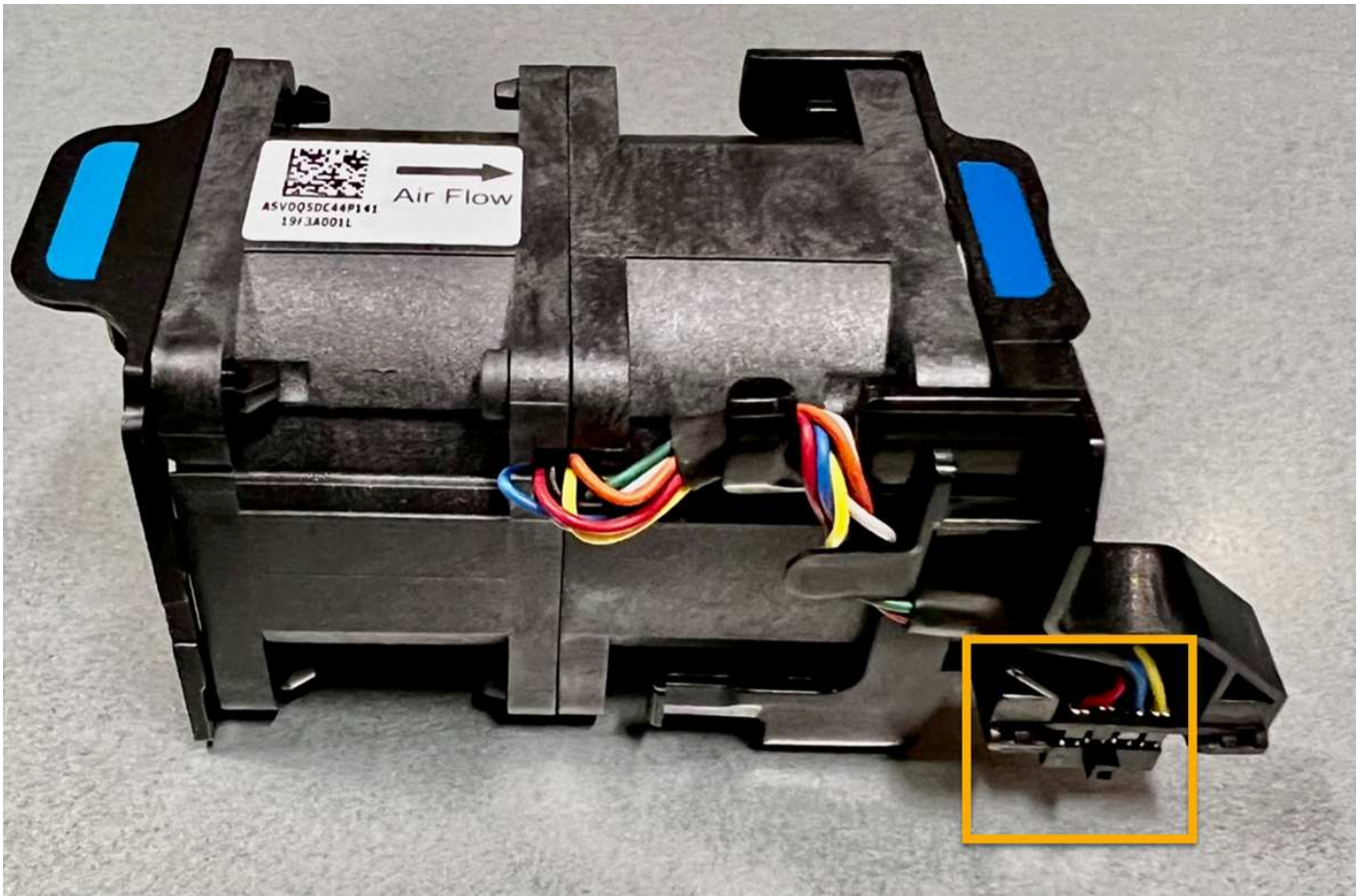
If you have ever used an ILM rule that creates only one copy of an object, you must replace the fan during a scheduled maintenance window. Otherwise, you might temporarily lose access to those objects during this procedure. See information about [why you should not use single-copy replication](#).

The appliance node will not be accessible while you replace the fan.

The photograph shows a fan for the appliance. The electrical connector is highlighted. The cooling fans are accessible after you take the top cover off of the appliance.



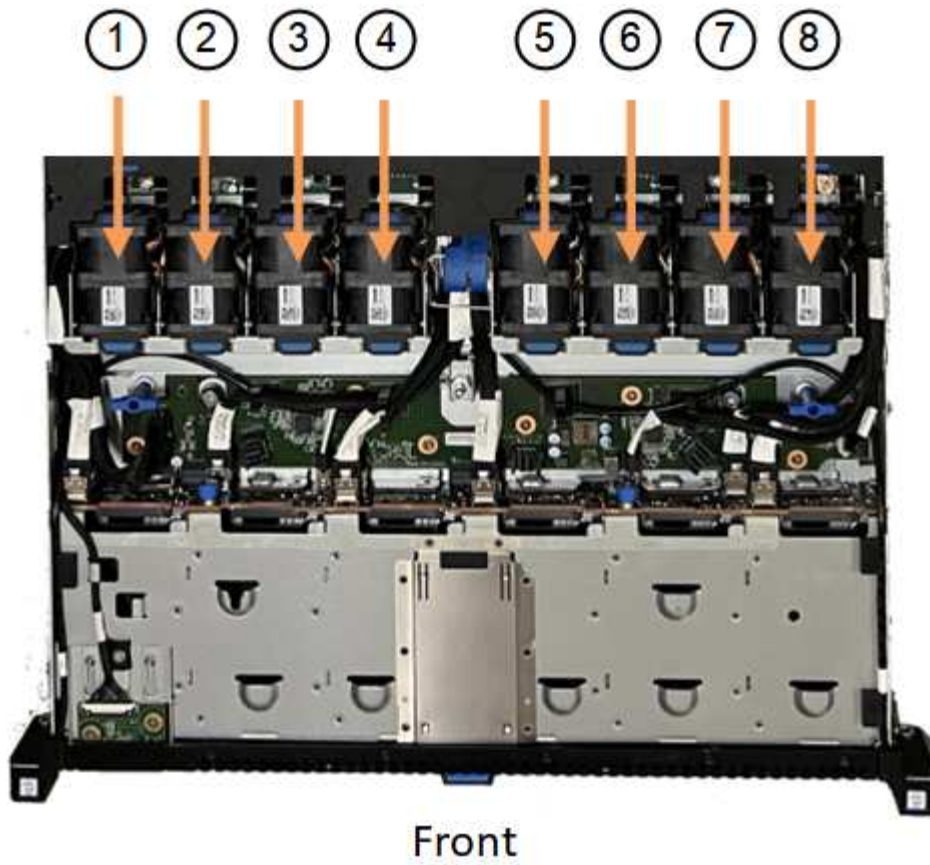
Each of the two power supply units also contain a fan. The power supply fans aren't included in this procedure.



### Steps

1. Wrap the strap end of the ESD wristband around your wrist, and secure the clip end to a metal ground to prevent static discharge.
2. Locate the fan that you need to replace.

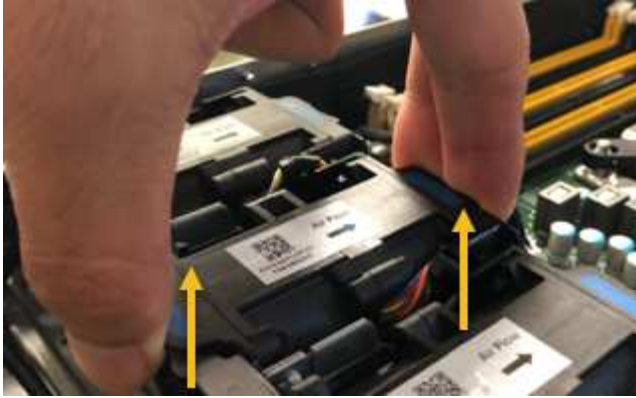
The eight fans are in the following positions in the chassis (front half of SGF6112 with top cover removed shown):



	Fan unit
1	Fan_SYS0
2	Fan_SYS1
3	Fan_SYS2
4	Fan_SYS3
5	Fan_SYS4
6	Fan_SYS5
7	Fan_SYS6
8	Fan_SYS7

3. Using the blue tabs on the fan, lift the failed fan out of the chassis.

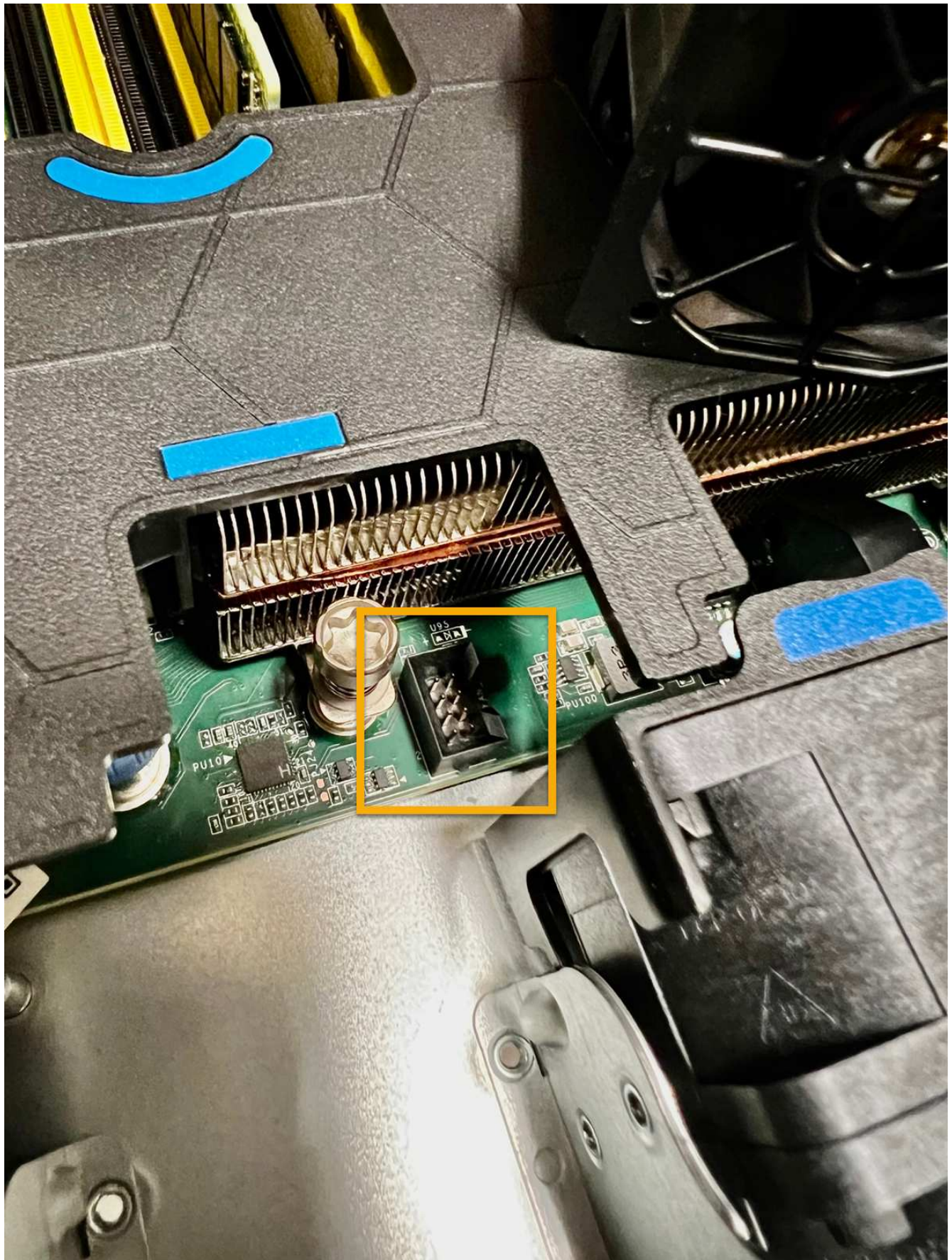




4. Slide the replacement fan into the open slot in the chassis.

Be sure to align the connector on the fan with the socket in the circuit board.

5. Press the fan's connector firmly into the circuit board (socket highlighted).



After you finish

1. [Put the top cover back on the appliance](#), and press the latch down to secure the cover in place.
2. [Power on the appliance](#) and monitor the appliance LEDs and boot-up codes.

Use the BMC interface to monitor boot-up status.

3. Confirm that the appliance node appears in the Grid Manager and that no alerts appear.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return & Replacements](#) page for further information.

## Replace drives in the SGF6112

The SGF6112 storage appliance contains 12 SSD drives. Data on the drives is protected by a RAID scheme that enables the appliance to recover from any single drive failure without having to copy data from another node.

The failure of a second drive before an initial drive failure has been corrected might require data be copied from other nodes to restore redundancy. This restoration of redundancy can take longer, and might be impossible, if single-copy ILM rules are in use or were used in the past, or if data redundancy has been impacted by failures on other nodes. Therefore, if one of the SGF6112 drives fails, you must replace it as soon as possible to ensure redundancy.

### Before you begin

- You have [physically located the appliance](#).
- You have verified which drive has failed by noting that the drive's left LED is solid amber or using the Grid Manager to [view the alert caused by the failed drive](#).



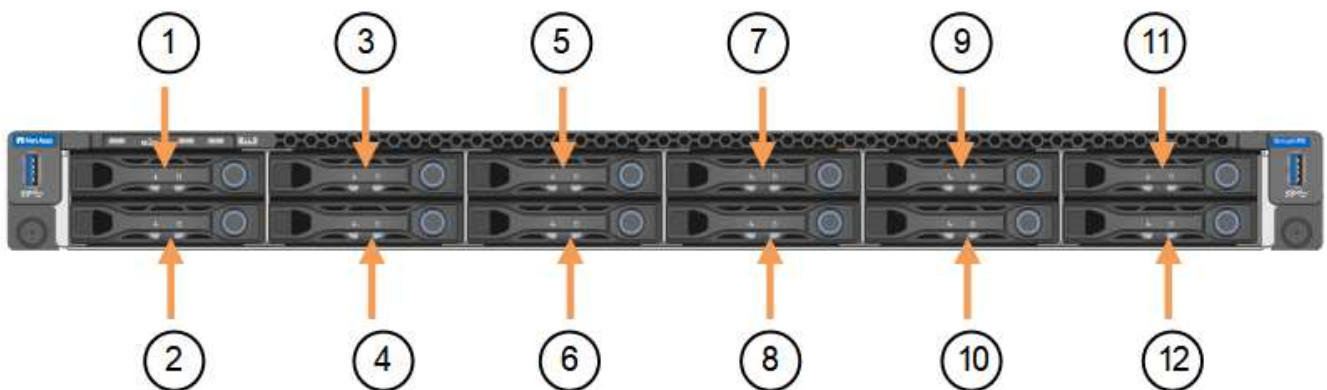
See the information about viewing status indicators to verify the failure.

- You have obtained the replacement drive.
- You have obtained proper ESD protection.

### Steps

1. Verify that the drive's left fault LED is amber or use the drive slot ID from the alert to locate the drive.

The twelve drives are in the following positions in the chassis (front of chassis with bezel removed shown):



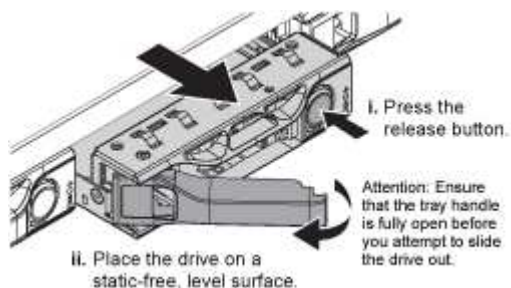
Position	Drive
1	HDD00
2	HDD01
3	HDD02
4	HDD03
5	HDD04
6	HDD05
7	HDD06
8	HDD07
9	HDD08
10	HDD09
11	HDD10
12	HDD11

You can also use the Grid Manager to monitor the status of the SSD drives. Select **NODES**. Then select **Storage Node > Hardware**. If a drive has failed, the Storage RAID Mode field contains a message about which drive has failed.

2. Wrap the strap end of the ESD wristband around your wrist, and secure the clip end to a metal ground to prevent static discharge.
3. Unpack the replacement drive, and set it on a static-free, level surface near the appliance.

Save all packing materials.

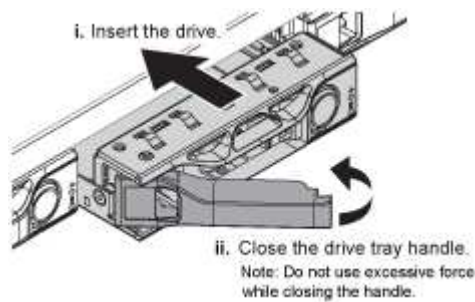
4. Press the release button on the failed drive.



The handle on the drive springs open partially, and the drive releases from the slot.

5. Open the handle, slide the drive out, and place it on a static-free, level surface.
6. Press the release button on the replacement drive before you insert it into the drive slot.

The latch springs open.



7. Insert the replacement drive in the slot, and then close the drive handle.



Don't use excessive force while closing the handle.

When the drive is fully inserted, you hear a click.

The replaced drive is automatically rebuilt with mirrored data from the working drives. The drive LED should blink initially, but then stop blinking as soon as the system determines that the drive has enough capacity and is functional.

You can check the status of the rebuild by using the Grid Manager.

8. If more than one drive failed and has been replaced, you might have alerts indicating that some volumes need to have data restored to them. If you receive an alert, before attempting volume recovery, select **NODES > appliance Storage Node > Hardware**. In the StorageGRID Appliance section of the page, verify that the Storage RAID mode is healthy or rebuilding. If the status lists one or more failed drives, correct this condition before attempting volume restoration.
9. In the Grid Manager, go to **NODES > appliance Storage Node > Hardware**. In the StorageGRID Appliance section of the page, verify that the Storage RAID mode is healthy.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return & Replacements](#) page for further information.

## Replace NIC in the SGF6112

You might need to replace a Network Interface Card (NIC) in the SGF6112 if it is not functioning optimally or if it has failed.

Use these procedures to:

- Remove the NIC
- Reinstall the NIC

### Remove the NIC

#### Before you begin

- You have the correct replacement NIC.

- You have determined the [location of the NIC to replace](#).
- You have [physically located the SGF6112 appliance](#) where you are replacing the NIC in the data center.



A [controlled shutdown of the appliance](#) is required before removing the appliance from the rack.

- You have disconnected all cables and [removed the appliance cover](#).

### About this task

To prevent service interruptions, confirm that all other Storage Nodes are connected to the grid before starting the Network Interface Card (NIC) replacement or replace the NIC during a scheduled maintenance window when periods of service disruption are acceptable. See the information about [monitoring node connection states](#).

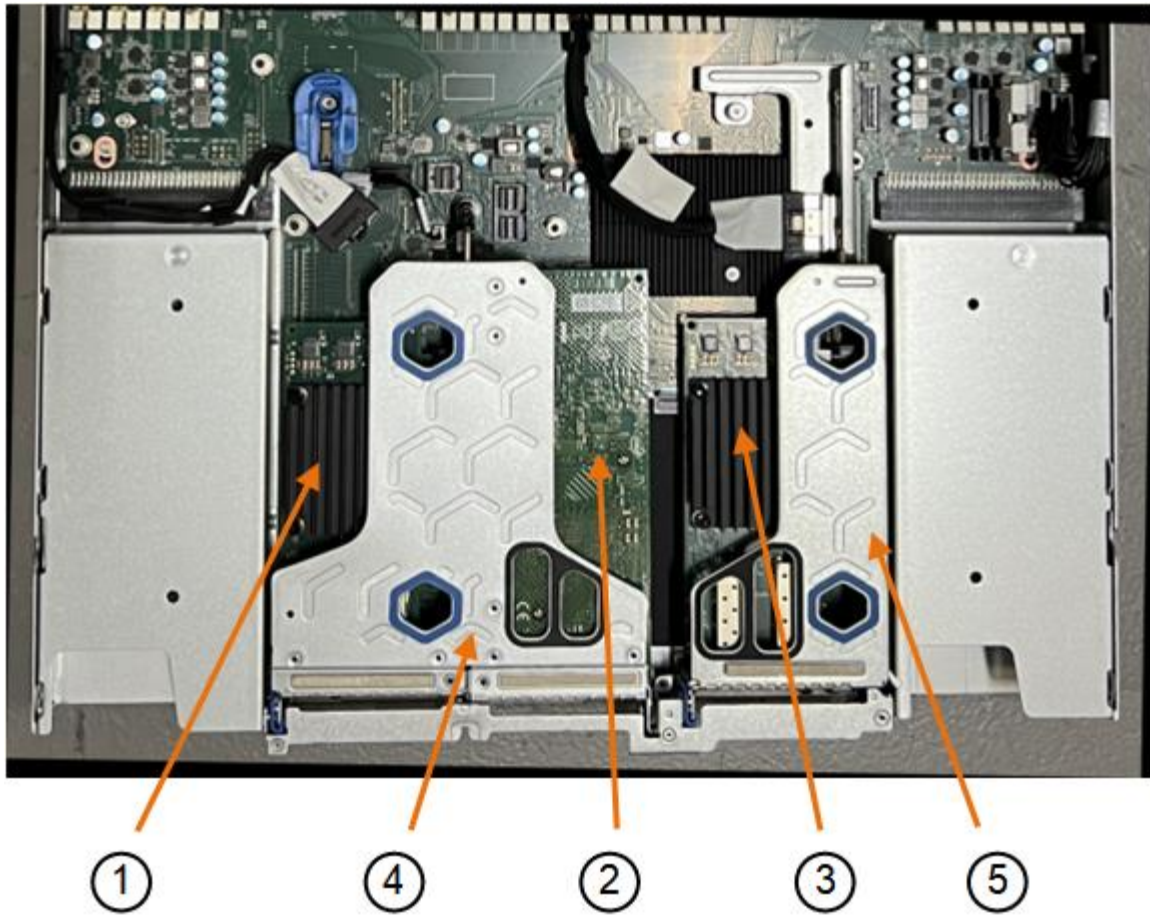


If you have ever used an ILM rule that creates only one copy of an object, you must replace the NIC during a scheduled maintenance window. Otherwise, you might temporarily lose access to those objects during this procedure. See information about [why you should not use single-copy replication](#).

### Steps

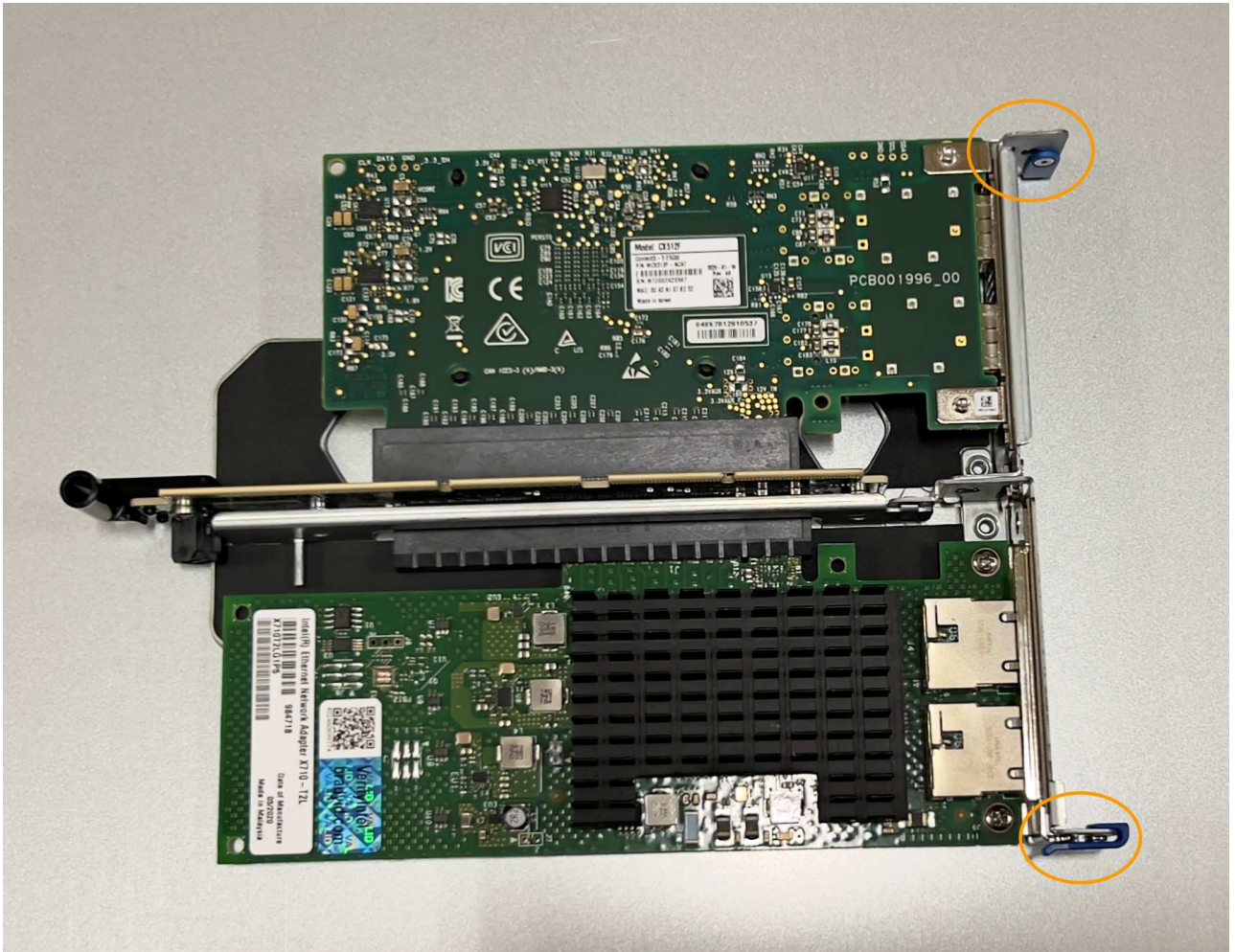
1. Wrap the strap end of the ESD wristband around your wrist, and secure the clip end to a metal ground to prevent static discharge.
2. Locate the riser assembly that contains the NIC at the rear of the appliance.

The three NICs in the appliance are in two riser assemblies in the positions in the chassis shown in the photograph (Rear of appliance with top cover removed shown):

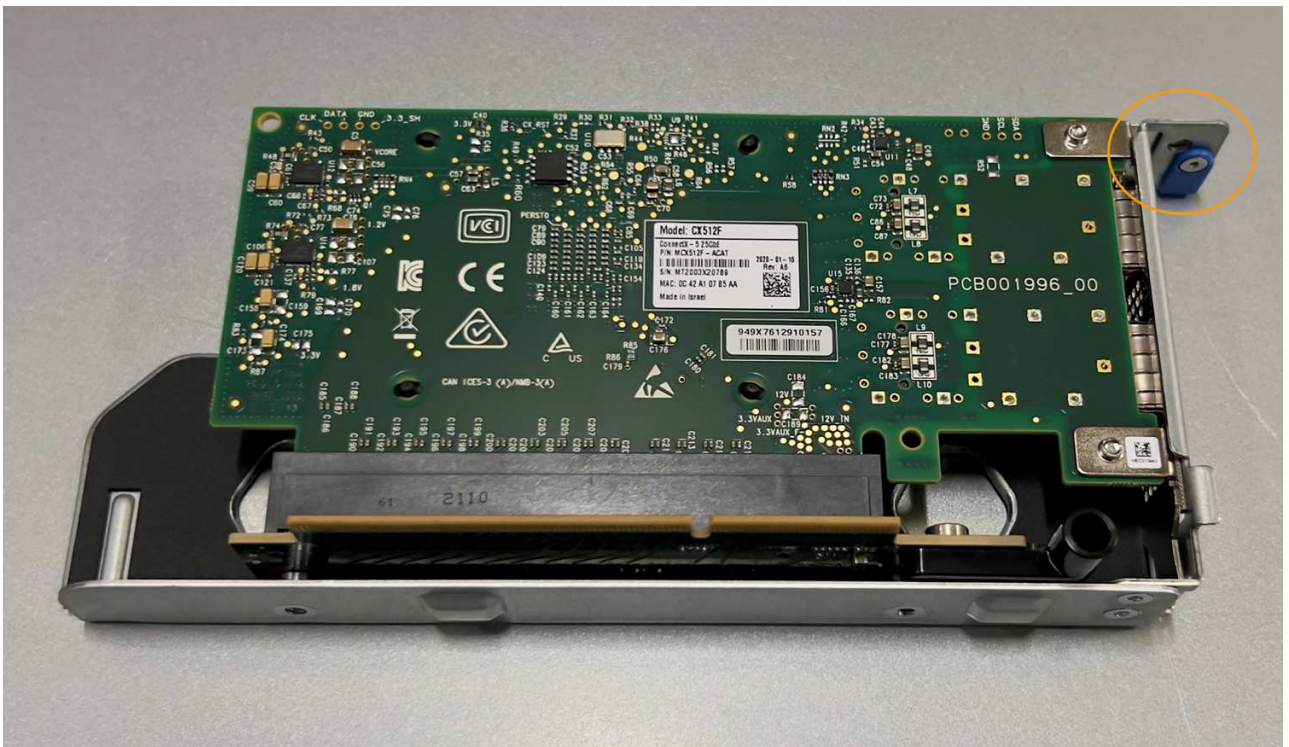


	Device or Part name	Description
1	hic1/hic2	10/25-GbE Ethernet network ports in the two-port riser assembly
2	mtc1/mtc2	1/10GBase-T management ports in the two-port riser assembly
3	hic3/hic4	10/25-GbE Ethernet network ports in the one-port riser assembly
4	Two-slot riser assembly	Support for one of the 10/25-GbE NICs and the 1/10GBase-T NIC
5	One-slot riser assembly	Support for one of the 10/25-GbE NICs

3. Grasp the riser assembly with the failed NIC through the blue-marked holes and carefully lift it upwards. Move the riser assembly toward the front of the chassis as you lift it to allow the external connectors in its installed NICs to clear the chassis.
4. Place the riser on a flat anti-static surface with the metal frame side down to access the NICs.
  - **Two-slot riser assembly with two NICs**



◦ One-slot riser assembly with one NIC





5. Open the blue latch (circled) on the NIC to be replaced and carefully remove the NIC from the riser assembly. Rock the NIC slightly to help remove the NIC from its connector. Don't use excessive force.
6. Place the NIC on a flat anti-static surface.

### Reinstall the NIC

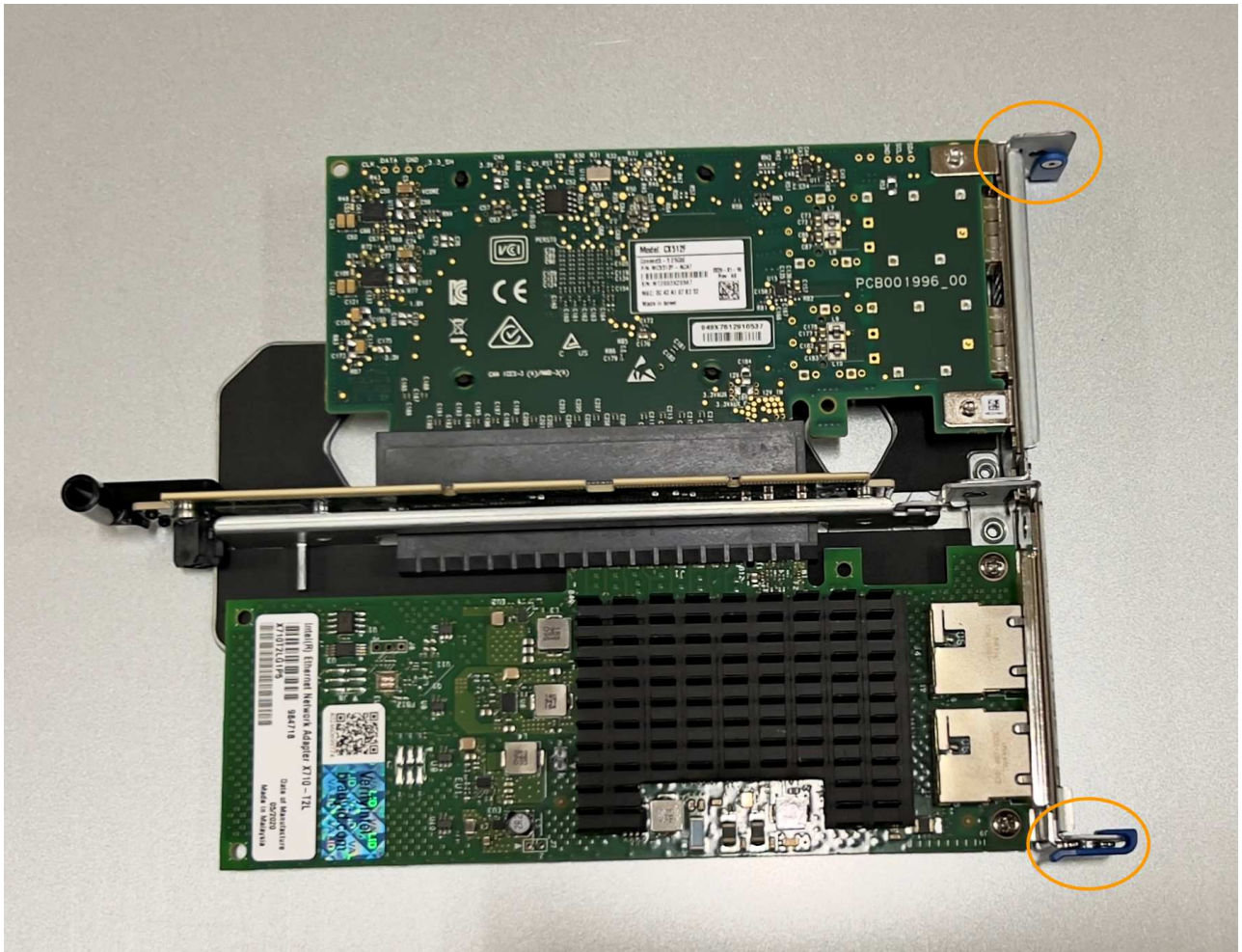
Install the replacement NIC into the same location as the one that was removed.

### Before you begin

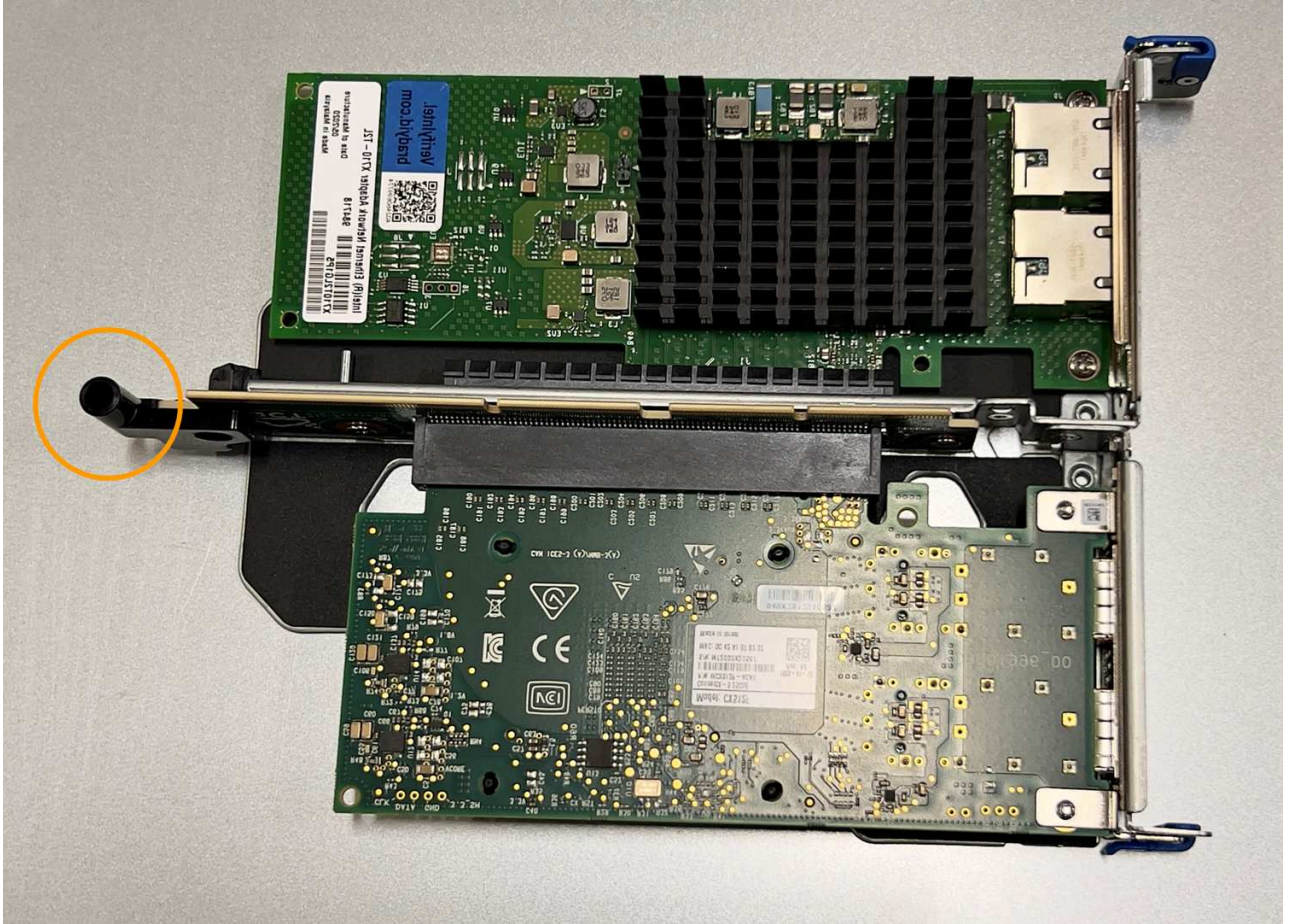
- You have the correct replacement NIC.
- You have removed the existing failed NIC.

### Steps

1. Wrap the strap end of the ESD wristband around your wrist, and secure the clip end to a metal ground to prevent static discharge.
2. Remove the replacement NIC from its packaging.
3. If you are replacing one of the NICs in the two-slot riser assembly, do the following:
  - a. Ensure the blue latch is in the open position.
  - b. Align the NIC with its connector on the riser assembly. Carefully press the NIC into the connector until it is fully seated, as shown in the photograph, and then close the blue latch.



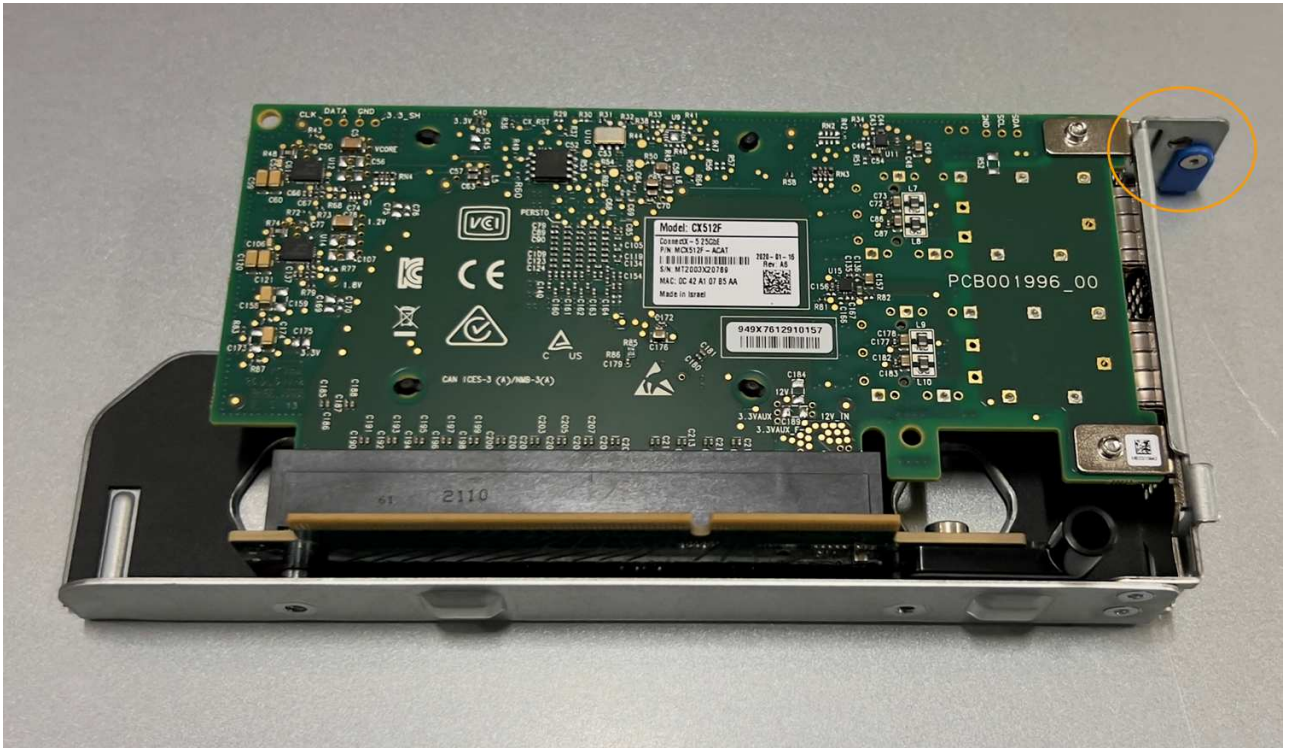
- c. Locate the alignment hole on the two-slot riser assembly (circled) that aligns with a guide pin on the system board to ensure correct riser assembly positioning.



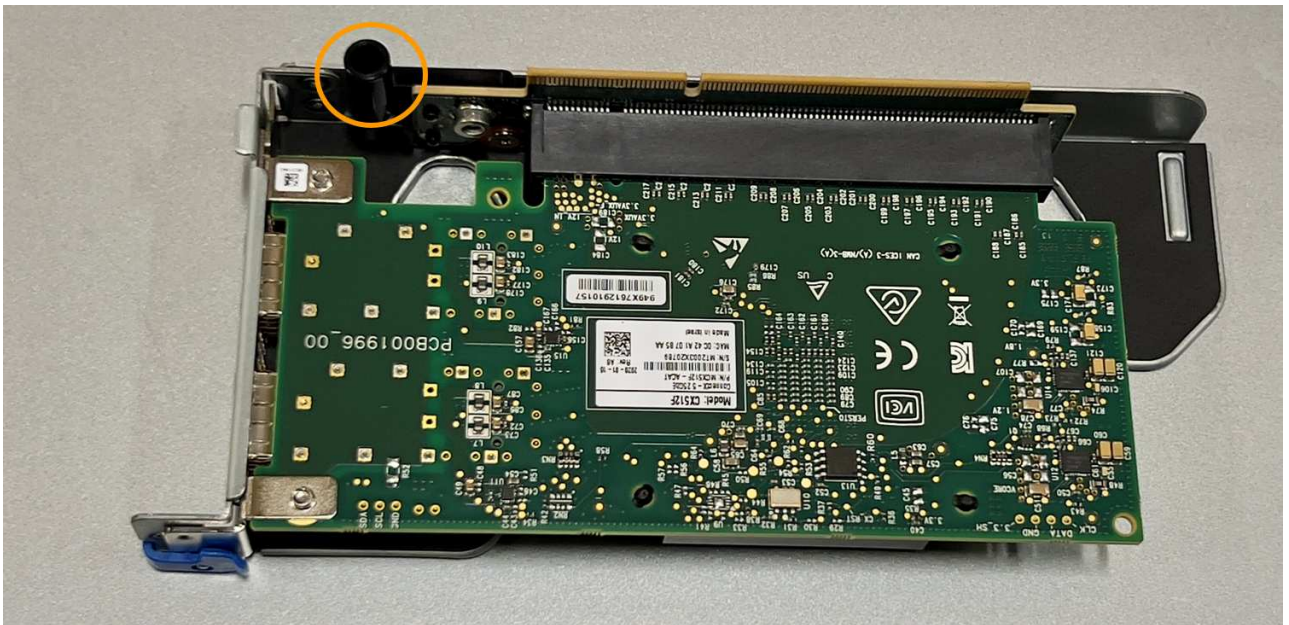
- d. Locate the guide pin on the system board



- e. Position the riser assembly in the chassis, making sure that it aligns with the connector on the system board and guide pin.
  - f. Carefully press the two-slot riser assembly in place along its center line, next to the blue-marked holes, until it is fully seated.
4. If you are replacing the NIC in the one-slot riser assembly, do the following:
- a. Ensure the blue latch is in the open position.
  - b. Align the NIC with its connector on the riser assembly. Carefully press the NIC into the connector until it is fully seated as shown in the photograph and close the blue latch.



- c. Locate the alignment hole on the one-slot riser assembly (circled) that aligns with a guide pin on the system board to ensure correct riser assembly positioning.



- d. Locate the guide pin on the system board



- e. Position the one-slot riser assembly in the chassis, making sure that it aligns with the connector on the system board and guide pin.
  - f. Carefully press the one-slot riser assembly in place along its center line, next to the blue-marked holes, until it is fully seated.
5. Remove the protective caps from the NIC ports where you will be reinstalling cables.

#### After you finish

If you have no other maintenance procedures to perform in the appliance, reinstall the appliance cover, return the appliance to the rack, attach cables, and apply power.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return & Replacements](#) page for further information.

#### Replace SGF6112 CMOS battery

Use this procedure to replace the CMOS coin cell battery on the system board.

Use these procedures to:

- Remove the CMOS battery
- Reinstall the CMOS battery

#### Remove the CMOS battery

##### Before you begin

- You have [verified the appliance where the CMOS battery needs to be replaced](#).
- You have [physically located the SGF6112 appliance](#) where you are replacing the CMOS battery in the data center.



A [controlled shutdown of the appliance](#) is required before removing the appliance from the rack.

- You have disconnected all cables and [removed the appliance cover](#).

### About this task

To prevent service interruptions, confirm that all other Storage Nodes are connected to the grid before starting the CMOS battery replacement or replace the battery during a scheduled maintenance window when periods of service disruption are acceptable. See the information about [monitoring node connection states](#).



If you have ever used an ILM rule that creates only one copy of an object, you must replace the battery during a scheduled maintenance window. Otherwise, you might temporarily lose access to those objects during this procedure. See information about [why you should not use single-copy replication](#).

### Steps

1. Wrap the strap end of the ESD wristband around your wrist, and secure the clip end to a metal ground to prevent static discharge.
2. Locate the two-slot riser assembly at the rear of the appliance.



3. Grasp the riser assembly through the blue-marked holes and carefully lift it upwards. Move the riser assembly toward the front of the chassis as you lift it to allow the external connectors in its installed NICs to clear the chassis.
4. Place the riser on a flat anti-static surface with the metal frame side down.
5. Locate the CMOS battery on the system board in the position beneath the removed riser assembly.



6. Use your finger or a plastic pry tool to press the retaining clip (highlighted) away from the battery to spring it from the socket.



7. Remove the battery and dispose of it properly.

#### Reinstall the CMOS battery

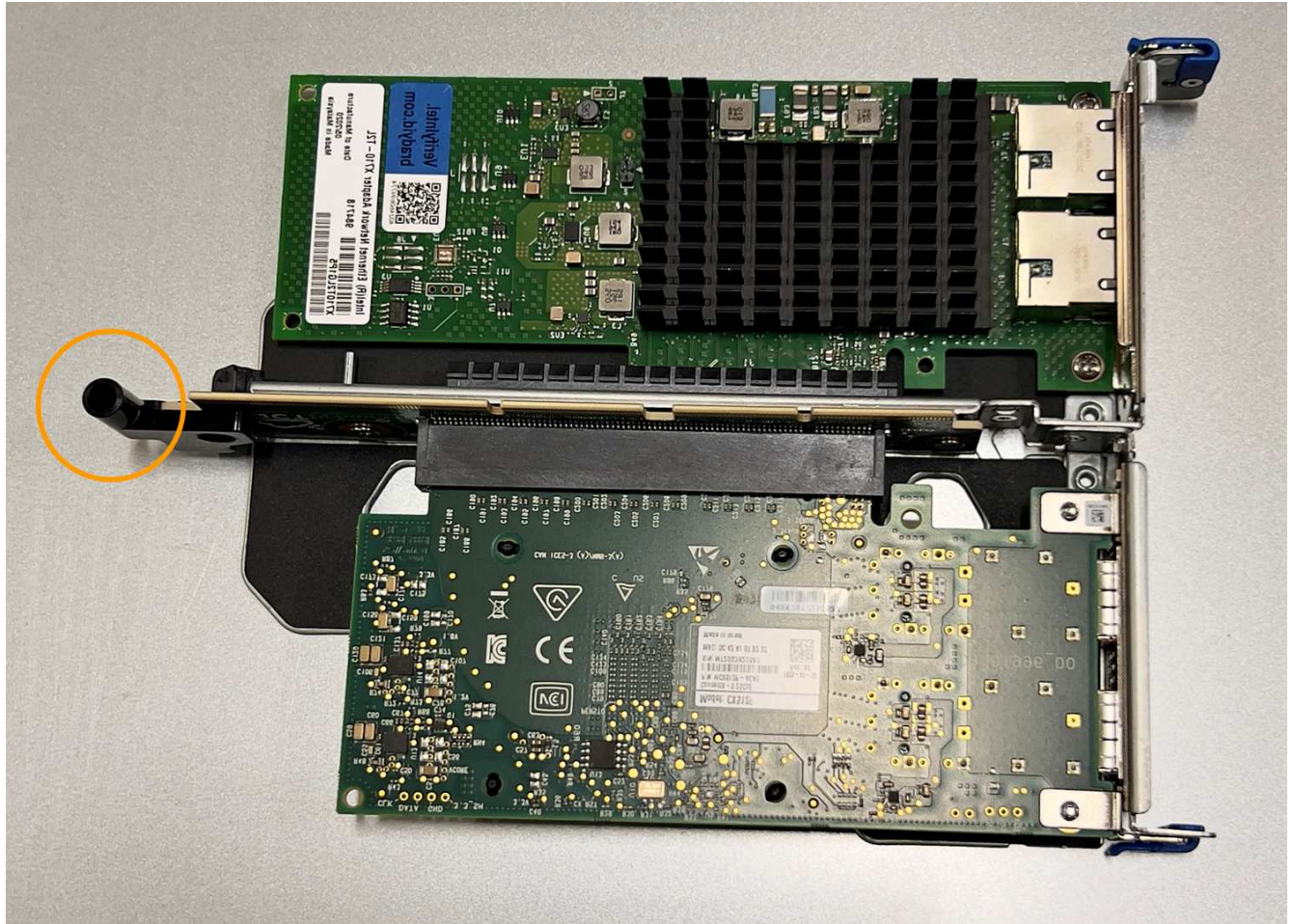
Install the replacement CMOS battery into the socket on the system board.

#### Before you begin

- You have the correct replacement CMOS battery (CR2032).
- You have removed the failed CMOS battery.

#### Steps

1. Wrap the strap end of the ESD wristband around your wrist, and secure the clip end to a metal ground to prevent static discharge.
2. Remove the CMOS battery from its packaging.
3. Press the replacement battery into the empty socket on the system board with the positive (+) side up until the battery snaps in place.
4. Locate the alignment hole on the two-slot riser assembly (circled) that aligns with the guide pin on the system board to ensure correct riser assembly positioning.



5. Locate the guide pin on the system board.





6. Position the riser assembly in the chassis, making sure that it aligns with the connector on the system board and guide pin.
7. Carefully press the two-slot riser assembly in place along its center line, next to the blue-marked holes, until it is fully seated.
8. If you have no other maintenance procedures to perform in the appliance, reinstall the appliance cover, return the appliance to the rack, attach cables, and apply power.
9. If the appliance you replaced had drive encryption enabled for the SED drives, you must [enter the drive encryption passphrase](#) to access the encrypted drives when the replacement appliance starts for the first time.
10. If the appliance you replaced used a key management server (KMS) to manage encryption keys for node encryption, additional configuration might be required before the node can join the grid. If the node does not automatically join the grid, make sure that these configuration settings have transferred to the new appliance and manually configure any settings that don't have the expected configuration:
  - [Configure StorageGRID connections](#)
  - [Configure node encryption for the appliance](#)
11. Log in to the appliance:
  - a. Enter the following command: `ssh admin@grid_node_IP`
  - b. Enter the password listed in the `Passwords.txt` file.
  - c. Enter the following command to switch to root: `su -`
  - d. Enter the password listed in the `Passwords.txt` file.
12. Restore BMC network connectivity for the appliance using one of these options:
  - Use static IP, netmask, and gateway
  - Use DHCP to obtain an IP, netmask, and gateway

- a. To restore the BMC configuration to use a static IP, netmask, and gateway, enter the following commands:

```
run-host-command ipmitool lan set 1 ipsrc static
```

```
run-host-command ipmitool lan set 1 ipaddr Appliance_IP
```

```
run-host-command ipmitool lan set 1 netmask Netmask_IP
```

```
run-host-command ipmitool lan set 1 defgw ipaddr Default_gateway
```

- b. To restore the BMC configuration to use DHCP to obtain an IP, netmask, and gateway, enter the following command:

```
run-host-command ipmitool lan set 1 ipsrc dhcp
```

13. After restoring BMC network connectivity, connect to the BMC interface to audit and restore any additional custom BMC configuration you might have applied. For example, you should confirm the settings for SNMP trap destinations and email notifications. See [Configure BMC interface](#).
14. Confirm that the appliance node appears in the Grid Manager and that no alerts appear.

## Replace SGF6112 cover

Remove the appliance cover to access internal components for maintenance, and replace the cover when you are finished.

### Remove cover

#### Before you begin

[Remove the appliance from the cabinet or rack](#) to access the top cover.

#### Steps

1. Make sure that the appliance cover latch is not locked. If necessary, turn the blue plastic latch lock one-quarter turn in the unlock direction, as shown on the latch lock.
2. Rotate the latch up and back toward the rear of the appliance chassis until it stops; then, carefully lift the cover from the chassis and set it aside.



Wrap the strap end of an ESD wristband around your wrist and secure the clip end to a metal ground to prevent static discharge when working inside the appliance.

### Reinstall cover

#### Before you begin

You have completed all maintenance procedures inside the appliance.

#### Steps

1. With the cover latch open, hold the cover above the chassis and align the hole in the top cover latch with the pin in the chassis. When the cover is aligned, lower it onto the chassis.



2. Rotate the cover latch forward and down until it stops and the cover fully seats into the chassis. Verify that there are no gaps along the front edge of the cover.

If the cover is not fully seated, you might not be able to slide the appliance into the rack.

3. Optional: Turn the blue plastic latch lock one-quarter turn in the lock direction, as shown on the latch lock, to lock it.

#### After you finish

Reinstall the appliance in the cabinet or rack.

## Replace SGF6112 appliance

You might need to replace the appliance if it is not functioning optimally or if it has failed.

### Before you begin

- You have a replacement appliance with the same part number as the appliance you are replacing.
- You have labels to identify each cable that is connected to the appliance.
- You have [physically located the appliance](#).

### About this task

The StorageGRID node will not be accessible while you replace the appliance. If the appliance is functioning sufficiently, you can perform a controlled shutdown at the start of this procedure.



If you are replacing the appliance before installing StorageGRID software, you might not be able to access the StorageGRID Appliance Installer immediately after completing this procedure. While you can access the StorageGRID Appliance Installer from other hosts on the same subnet as the appliance, you can't access it from hosts on other subnets. This condition should resolve itself within 15 minutes (when any ARP cache entries for the original appliance time out), or you can clear the condition immediately by purging any old ARP cache entries manually from the local router or gateway.

### Steps

1. Display the current configurations of the appliance and record them.
  - a. Log in to the appliance to be replaced:
    - i. Enter the following command: `ssh admin@grid_node_IP`
    - ii. Enter the password listed in the `Passwords.txt` file.
    - iii. Enter the following command to switch to root: `su -`
    - iv. Enter the password listed in the `Passwords.txt` file.

When you are logged in as root, the prompt changes from `$` to `#`.
  - b. Enter: `run-host-command ipmitool lan print` to display the current BMC configurations for the appliance.
2. [Shut down the appliance](#).
3. If any of the network interfaces on this StorageGRID appliance are configured for DHCP, you need to update the permanent DHCP lease assignments on the DHCP servers to reference the MAC addresses of the replacement appliance. This ensures that the appliance is assigned the expected IP addresses.

Contact your network or DHCP-server administrator to update the permanent DHCP lease assignments. The administrator can determine the MAC addresses of the replacement appliance from the DHCP server logs or by inspecting the MAC address tables in the switches to which the appliance Ethernet ports are connected.

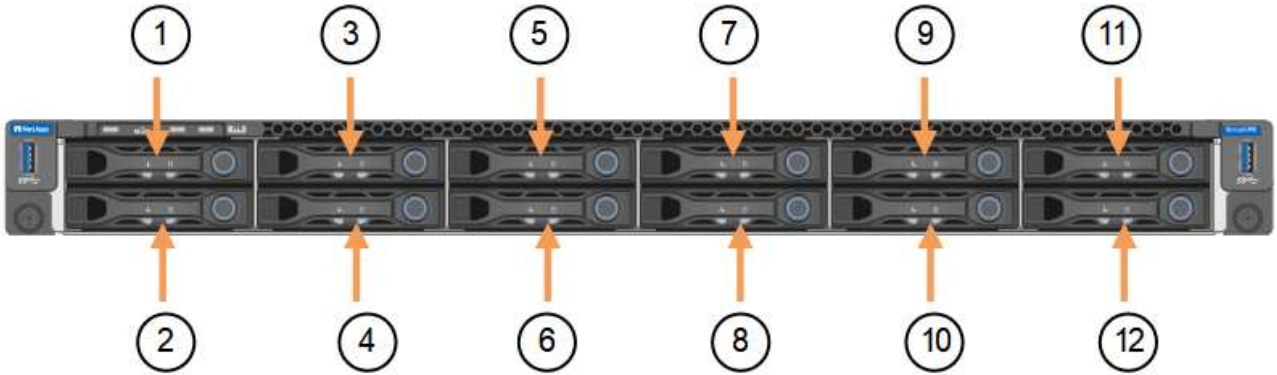
4. Remove and replace the appliance:
  - a. Label the cables and then disconnect the cables and any network transceivers.



To prevent degraded performance, don't twist, fold, pinch, or step on the cables.

- b. Remove the failed appliance from the cabinet or rack.
- c. Note the position of the replaceable components (two power supplies, three NICs, and twelve SSDs) in the failed appliance.

The twelve drives are in the following positions in the chassis (front of chassis with bezel removed shown):



	Drive
1	HDD00
2	HDD01
3	HDD02
4	HDD03
5	HDD04
6	HDD05
7	HDD06
8	HDD07
9	HDD08
10	HDD09
11	HDD10
12	HDD11

- d. Transfer the replaceable components to the replacement appliance.

Follow the maintenance instructions provided for reinstalling the replaceable components.



If you wish to retain the data on the drives, be sure to insert the SSD drives into the same drive slots they occupied in the failed appliance. If you don't, the Appliance Installer will display a warning message and you will have to put the drives into the correct slots and reboot the appliance before the appliance can rejoin the grid.

e. [Install the replacement appliance into the cabinet or rack.](#)

f. Replace the cables and any optical transceivers.

5. Power on the appliance.

6. If the appliance you replaced had hardware drive encryption enabled for the SED drives, you must [enter the drive encryption passphrase](#) to access the encrypted drives when the replacement appliance starts for the first time.

7. Wait for the appliance to rejoin the grid. If the appliance does not rejoin the grid, follow the guidance on the StorageGRID Appliance Installer home page to address any issues.



To prevent data loss if the Appliance Installer indicates that physical hardware changes are required, such as moving disk drives to different slots, power down the appliance before making hardware changes.

8. If the appliance you replaced used a key management server (KMS) to manage encryption keys for node encryption, additional configuration might be required before the node can join the grid. If the node does not automatically join the grid, make sure that these configuration settings have transferred to the new appliance and manually configure any settings that don't have the expected configuration:

- [Configure StorageGRID connections](#)
- [Configure node encryption for the appliance](#)

9. Log in to the replaced appliance:

a. Enter the following command: `ssh admin@grid_node_IP`

b. Enter the password listed in the `Passwords.txt` file.

c. Enter the following command to switch to root: `su -`

d. Enter the password listed in the `Passwords.txt` file.

10. Restore BMC network connectivity for the replaced appliance. There are two options:

- Use static IP, netmask, and gateway
- Use DHCP to obtain an IP, netmask, and gateway
  - a. To restore the BMC configuration to use a static IP, netmask, and gateway, enter the following commands:

```
run-host-command ipmitool lan set 1 ipsrc static
```

```
run-host-command ipmitool lan set 1 ipaddr Appliance_IP
```

```
run-host-command ipmitool lan set 1 netmask Netmask_IP
```

```
run-host-command ipmitool lan set 1 defgw ipaddr Default_gateway
```

- b. To restore the BMC configuration to use DHCP to obtain an IP, netmask, and gateway, enter the following command:

```
run-host-command ipmitool lan set 1 ipsrc dhcp
```

11. After restoring BMC network connectivity, connect to the BMC interface to audit and restore any additional custom BMC configuration you might have applied. For example, you should confirm the settings for SNMP trap destinations and email notifications. See [Configure BMC interface](#).
12. Confirm that the appliance node appears in the Grid Manager and that no alerts appear.

### After you finish

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return & Replacements](#) page for further information.

### Related information

[View status indicators](#)

[View boot-up codes for appliance](#)

### Relocate SGF6112 in cabinet or rack

Remove the SGF6112 from a cabinet or rack to access the top cover or to move the appliance to a different location, then reinstall the appliance into a cabinet or rack when hardware maintenance is complete.

### Remove SGF6112 from cabinet or rack

#### Before you begin

- You have labels to identify each cable that is connected to the SGF6112.
- You have [physically located the SGF6112](#) where you are performing maintenance in the data center.
- You have [shut down the SGF6112](#).



Don't shut down the appliance using the power switch.

#### Steps

1. Label and then disconnect the appliance power cables.
2. Wrap the strap end of the ESD wristband around your wrist, and secure the clip end to a metal ground to prevent static discharge.
3. Label and then disconnect the appliance data cables and any SFP+ or SFP28 transceivers.



To prevent degraded performance, don't twist, fold, pinch, or step on the cables.

4. Loosen the two captive screws on the appliance front panel.



5. Slide the SGF6112 forward out of the rack until the mounting rails are fully extended and you hear the latches on both sides click.

The appliance top cover is accessible.

6. Optional: If you are fully removing the appliance from the cabinet or rack, follow the instructions for the rail kit to remove the appliance from the rails.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the [Part Return & Replacements](#) page for further information.

### Reinstall SGF6112 into cabinet or rack

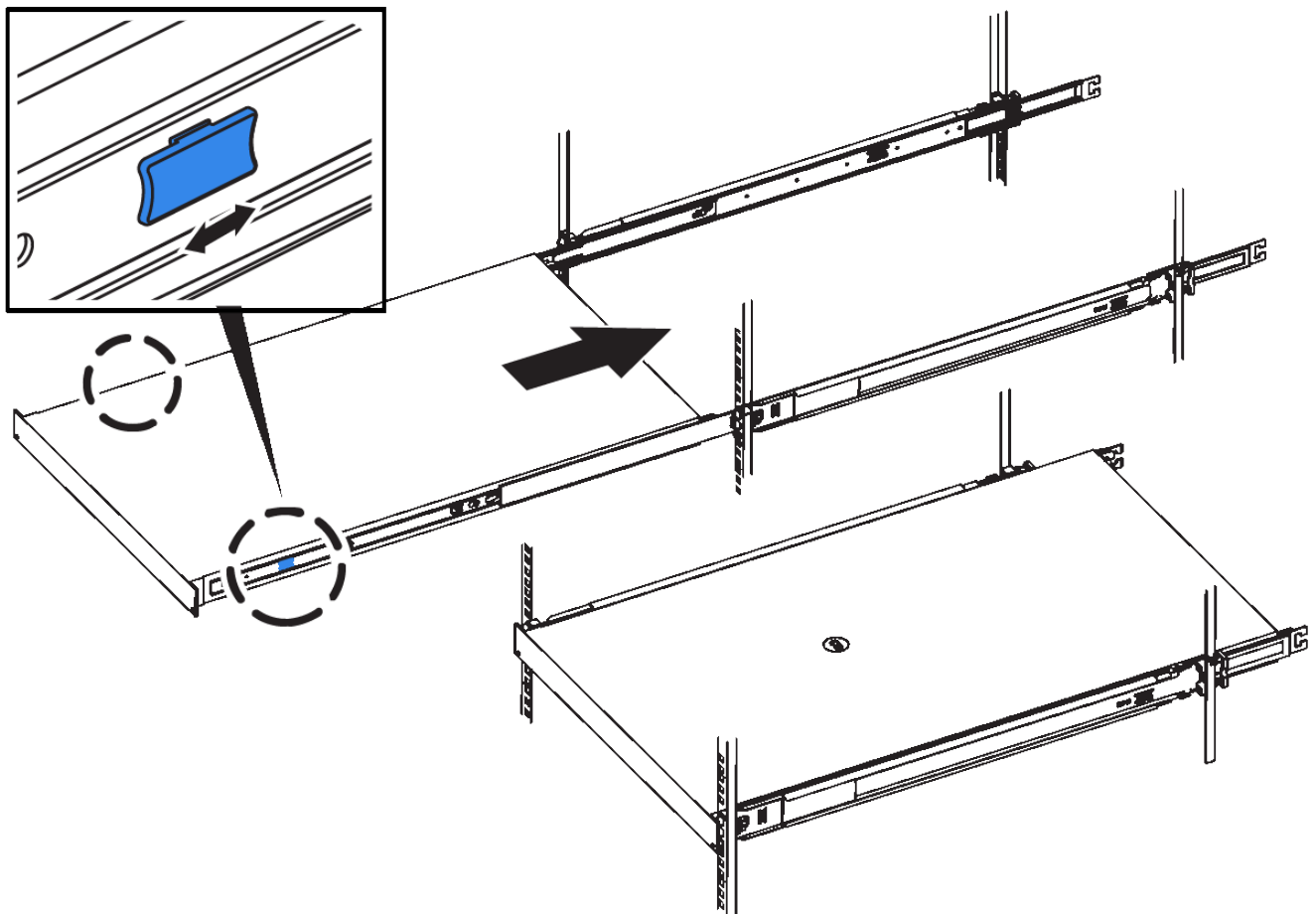
#### Before you begin

You have [reinstalled the appliance cover](#).

#### Steps

1. Press the blue rail releases both rack rails at the same time and slide the SGF6112 into the rack until it is fully seated.

When you can't move the controller any further, pull the blue latches on both sides of the chassis to slide the controller all the way in.



Don't attach the front bezel until after you power on the controller.



2. Tighten the captive screws on the controller front panel to secure the controller in the rack.



3. Wrap the strap end of the ESD wristband around your wrist, and secure the clip end to a metal ground to prevent static discharge.
4. [Reconnect the controller data cables and any SFP+ or SFP28 transceivers.](#)



To prevent degraded performance, don't twist, fold, pinch, or step on the cables.

5. [Reconnect the controller power cables.](#)

### **After you finish**

[Restart the appliance.](#)

# How to enable StorageGRID in your environment

Go to [How to enable StorageGRID in your environment](#) to learn how to test and enable applications in your StorageGRID environment.

The **storagegrid-enable** documentation site provides examples and cookbooks that expand upon the product documentation in this site, and it describes some next steps in evaluating and integrating with StorageGRID.

Some of the information included:

- Lists of validated third-party solutions for past and current StorageGRID releases.
- Product feature guides. For example, these guides provide all the information you need to create Cloud Storage Pools.
- Tool and application guides.
- API examples for using StorageGRID features such as S3 encryption and S3 Object Lock.

# Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

## Copyright

<https://www.netapp.com/company/legal/copyright/>

## Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

<https://www.netapp.com/company/legal/trademarks/>

## Patents

A current list of NetApp owned patents can be found at:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

## Privacy policy

<https://www.netapp.com/company/legal/privacy-policy/>

## Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

[https://library.netapp.com/ecm/ecm\\_download\\_file/ECMLP2886898](https://library.netapp.com/ecm/ecm_download_file/ECMLP2886898)

## Copyright information

Copyright © 2024 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.