

## **Configure hardware (SG5700)**

StorageGRID

NetApp June 13, 2025

This PDF was generated from https://docs.netapp.com/us-en/storagegrid-116/sg5700/accessingstoragegrid-appliance-installer-sg5700.html on June 13, 2025. Always check docs.netapp.com for the latest.

# **Table of Contents**

Configure hardware (SG5700)	1
Configure StorageGRID connections (SG5700)	1
Access StorageGRID Appliance Installer	1
Verify and upgrade StorageGRID Appliance Installer version	4
Configure network links (SG5700)	5
Set IP configuration	. 11
Verify network connections	. 18
Verify port-level network connections	. 20
Access and configure SANtricity System Manager (SG5700)	. 22
Set up and access SANtricity System Manager	. 22
Review hardware status in SANtricity System Manager	. 26
Set IP addresses for storage controllers using StorageGRID Appliance Installer	. 28
Optional: Enable node encryption	. 29
Optional: Change RAID mode (SG5760 only)	. 31
Optional: Remap network ports for appliance	. 32

# Configure hardware (SG5700)

After applying power to the appliance, you must configure SANtricity System Manager, which is the software you will use to monitor the hardware. You must also configure the network connections that will be used by StorageGRID.

## **Configure StorageGRID connections (SG5700)**

Before you can deploy a StorageGRID appliance as a Storage Node in a StorageGRID grid, you must configure the connections between the appliance and the networks you plan to use. You can configure networking by browsing to the StorageGRID Appliance Installer, which is included on the E5700SG controller (the compute controller in the appliance).

### Steps

- Access StorageGRID Appliance Installer
- Verify and upgrade StorageGRID Appliance Installer version
- Configure network links (SG5700)
- Set IP configuration
- Verify network connections
- Verify port-level network connections

## Access StorageGRID Appliance Installer

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

### What you'll need

- You are using a supported web browser.
- The appliance is connected to all of the StorageGRID networks you plan to use.
- You know the IP address, gateway, and subnet for the appliance on these networks.
- You have configured the network switches you plan to use.

#### About this task

When you first access the StorageGRID Appliance Installer, you can use the DHCP-assigned IP address for the Admin Network (assuming the appliance is connected to the Admin Network) or the DHCP-assigned IP address for the Grid Network. Using the IP address for the Admin Network is preferred. Otherwise, if you access the StorageGRID Appliance Installer using the DHCP address for the Grid Network, you might lose connection with the StorageGRID Appliance Installer when you change link settings and when you enter a static IP.

#### Steps

1. Obtain the DHCP address for the appliance on the Admin Network (if it is connected) or the Grid Network (if the Admin Network is not connected).

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.

- Provide the MAC address for management port 1 to your network administrator, so they can look up the DHCP address for this port on the Admin Network. The MAC address is printed on a label on the E5700SG controller, next to the port.
- 2. If you were able to obtain either of the DHCP addresses:
  - a. Open a web browser on the service laptop.
  - b. Enter this URL for the StorageGRID Appliance Installer: https://E5700SG\_Controller\_IP:8443

For *E5700SG\_Controller\_IP*, use the DHCP address for the controller (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 <sup>®</sup> StorageGRID <sup>®</sup> Appliance Installer					
Home	Configure Networking -	Configure Hardware 👻	Monitor Installation	Advanced 👻	

#### Home

1 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	
	Cancel Save	
Primary Admin Node connection		
Enable Admin Node discovery		
Primary Admin Node IP	172.16.1.178	
Connection state	Connection to 172.16.1.178 ready	
	Cancel 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.	
	Start Installation	

- 3. If the E5700SG controller could not acquire an IP address using DHCP:
  - a. Connect the service laptop to management port 2 on the E5700SG controller, using an Ethernet cable.



b. Open a web browser on the service laptop.

c. 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.



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

4. Review any messages displayed on the Home page and configure the link configuration and the IP configuration, as required.

#### **Related information**

Web browser requirements

### 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.

#### What you'll need

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 do not 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 file is a .zip archive that contains the current and previous firmware versions for all StorageGRID appliance models, in subdirectories for each controller type.

After downloading the Support file for StorageGRID Appliances file, 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 the StorageGRID Appliance Installer to perform these steps:
  - a. Upload the appropriate support file (firmware image) for your controller type and the checksum file.
  - b. Upgrade the inactive partition.
  - c. Reboot and swap partitions.
  - d. Upgrade the second (inactive) partition.

#### **Related information**

Access StorageGRID Appliance Installer

## Configure network links (SG5700)

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.

#### What you'll need

If you plan to use the 25-GbE link speed for the 10/25-GbE ports:

- You have installed SFP28 transceivers in the ports you plan to use.
- You have connected the ports to switches that can support these features.
- You understand how to configure the switches to use this higher speed.

If you plan to use Aggregate port bond mode, LACP network bond mode, or VLAN tagging for the 10/25-GbE ports:

- You have connected the 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.
- If you plan to use Active-Backup mode for the Admin Network, you have connected Ethernet cables to both management ports on the controller.

#### About this task

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.

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

• Fixed (default) port bond mode

Network bond mode	Client Network disabled (default)	Client Network enabled
Active-Backup (default)	<ul> <li>Ports 2 and 4 use an active- backup bond for the Grid Network.</li> <li>Ports 1 and 3 are not used.</li> <li>A VLAN tag is optional.</li> </ul>	<ul> <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.</li> </ul>
LACP (802.3ad)	<ul> <li>Ports 2 and 4 use an LACP bond for the Grid Network.</li> <li>Ports 1 and 3 are not used.</li> <li>A VLAN tag is optional.</li> </ul>	<ul> <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.</li> </ul>

#### Aggregate port bond mode

Network bond mode	Client Network disabled (default)	Client Network enabled
LACP (802.3ad) only	<ul> <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> <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>

See the information about 10/25-GbE port connections for the E5700SG controller for more information about port bond and network bond modes.

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.



#### 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.

Network Link Configuration



A You might lose your connection if you make changes to the network or link you are connected through. If you are not reconnected within 1 minute, re-enter the URL using one of the other IP addresses assigned to the appliance.

The Link Status table lists the link state (up/down) and speed (1/10/25/40/100 Gbps) of the numbered ports.

Link	State	Speed (Gbps)	
1	Up	25	
2	Up	25	
3	Up	25	
4	Up	25	
5	Up	1	
6	Up	1	

#### Link Status

The first time you access this page:

- Link Speed is set to 10GbE.
- Port bond mode is set to Fixed.
- Network bond mode for the Grid Network is set to Active-Backup.
- The Admin Network is enabled, and the network bond mode is set to Independent.

• The Client Network is disabled.

Link Settings	
Link speed	Auto
Port bond mode	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     O LACP (802.3ad)
Enable VLAN (802.1q) tagging	
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     O Active-Backup
	Connect the Admin Network to port 5. Leave port 6 unconnected. If necessary, you can make a temporary direct Ethernet connection to port 6 and use 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	Enabling the Client Network causes the default gateway for this node to move to the Client

2. If you plan to use the 25-GbE link speed for the 10/25 GbE ports, select **25GbE** from the Link speed dropdown list.

to the Grid Network Subnet List. Otherwise, the connection to the node might be lost.

The network switches you are using for the Grid Network and the Client Network must also support and be configured for this speed. SFP28 transceivers must be installed in the ports.

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

The Grid Network is required. You cannot disable this network.

a. If the appliance is not connected to the Admin Network, unselect the **Enable network** check box for the Admin Network.

Admin Network	

Enable network

b. If the appliance is connected to the Client Network, select the **Enable network** check box for the Client Network.

The Client Network settings for the 10/25-GbE ports are now shown.

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

The 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	Auto
Port bond mode	C 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	CActive-Backup (CLACP (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	328
Admin Network	
Enable network	
Network bond mode	Connect the Admin Network to ports 5 and 8. If necessary, you can make a temporary direct Ethernet connection by disconnecting ports 5 and 8, then connecting to port 8 and using link-local IP address 169.254.0.1 for access.
Client Network	
Enable network	
Network bond mode	CActive-Backup (ACP (802.3ad) If the port bond mode is Aggregate, all bonds must be in LACP (802.3ad) mode.
Enable VLAN (802.1q) tagging	
VLAN (802.1o) tao	332

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 are not 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

#### **Related information**

Port bond modes for E5700SG controller ports

## Set IP configuration

You use the StorageGRID Appliance Installer to configure the IP addresses and routing

information used for the appliance Storage Node on the StorageGRID Grid, Admin, and Client Networks.

#### 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.

If you want to change the link configuration, see the instructions for changing the link configuration of the E5700SG controller.

#### 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.

#### Grid Network

The Grid Network is used for all internal StorageGRID traffic. The Grid Network provides connectivity between all nodes in the grid, across all sites and subnets. All hosts on the Grid Network must be able to talk to all other hosts. The Grid Network can consist of multiple subnets. Networks containing critical grid services, such as NTP, can also be added as Grid subnets.

IP Assignment	● Static ○	DHCP	
IPv4 Address (CIDR)	172.16.3.72/21		
Gateway	172.16.0.1		]
All required Primary Admin	Grid Network subnets Node before starting	must also be defined in the Grid Netw installation.	ork Subnet List on the
Subnets (CIDR)	172.18.0.0/21		×
	172.18.0.0/21		×
	192.168.0.0/21		+×
MTU	1500	1	
	Cancel Save		

- 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 do not 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://services\_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 do not 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 must 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.

Pv4 Address (CIDR)	10.224.3.72/21	
Gateway	10.224.0.1	
Subnets (CIDR)	0.0.0/32	
MTU	1500	<b> </b>

- 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://services\_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 cannot 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 cannot 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 must 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     O DHCP	
IPv4 Address (CIDR)	47.47.7.183/21	
Gateway	47.47.0.1	
MTU	1500	<b>€</b>
	Cancel	
	Save	

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



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

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



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

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

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

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

b. Confirm that the gateway is correct.



If the Client Network is enabled, the default route is displayed. The default route uses the Client Network gateway and cannot 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.

#### **Related information**

Change link configuration of the E5700SG controller

### 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

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.

Network	Grid	~
Destination IPv4 Address or FQDN		
Test MTU		
	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.

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

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

#### 5. Click Test Connectivity.

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

#### 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

Destination IPv4 Address or FQDN Test MTU Test Connectivity	Network	Grid	~
Test MTU Test Connectivity	Destination IPv4 Address or FQDN	10.96.104.223	
	Test MTU	☑ Test Connectivity	
		Test Connectivity	

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 (SG5700)

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 port reference in the StorageGRID networking guidelines.



The Grid Network ports listed in the port connectivity table are valid only for StorageGRID version 11.6.0. To verify which ports are correct for each node type, you should always consult the networking guidelines for your version of StorageGRID.

#### Steps

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

The Port Connectivity Test page appears.

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

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

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

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

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

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

Port Connectivity Test						
Network	Grid 🔻					
IPv4 Address	10.224.6.160-161					
Ranges						
Port Ranges	22,2022					
Protocol	TCP UDP					
	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 -oNe 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.

```
O 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 Nay 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 cannot 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.

OPort connectivit Connection failed	ty test failed to one or more ports.
Nmap command out	put. Note: Unreachable hosts will not appear in the output.
# Nmap 7.70 scan Nmap scan report Host is up (0.00	n initiated Sat May 16 17:11:01 2020 as: /usr/bin/nmap -n -oNe br0 -p 22,79,80,443,1504,1505,1506,1508,7443,9999 172.16.4.71 t for 172.16.4.71 3029s latency).
PORT STATE	SERVICE
22/tcp open	ssh
79/tcp filter	ed 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 :	at May 16 17:11:02 2020 1 IP address (1 host up) scanned in 1.60 seconds

#### **Related information**

Networking guidelines

## Access and configure SANtricity System Manager (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.

#### What you'll need

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



You must have SANtricity firmware 8.70 (11.70) 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 do not 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 cannot 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 E-Series documentation center.

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. Use the StorageGRID Appliance Installer and select Advanced > SANtricity System Manager



If the StorageGRID Appliance Installer is not available or the login page does not appear, you must use the IP address of the storage controller. Access SANtricity System Manager by browsing to the storage controller IP: https://Storage\_Controller\_IP

The login page for SANtricity System Manager appears.

2. Set or enter the administrator password.



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

The Set Up wizard appears.



3. Select Cancel to close the wizard.



Do not complete the Set Up wizard for a StorageGRID appliance.

The SANtricity System Manager home page appears.

E States y Syst	lem Manager		Unnamed		Philosocat + ( Jold + ) Lig Dd
ft Harra		Welcome to SV	Your storage array Minch/ <sup>#</sup> System Manager. Ge volume group for your sto	is optimal. I started by creating a pool or rage array	Veer Operations, in Program >
0 Settings	STORAGE ARRAY LEV What does the IOPS graph 15 1 1	EL PERFORMANCE		7 74 584 Company IQ	View Proformance (Totalis 1 PT) with ••• CF 0000 -•• CPTS (Reade)
	4 (4)	NDPS #	102440 (1440.00 	notee Trail CPU	er siz aal
	CAPACITY O % Free 22551.39 GB Ter	Were Gapacity Data	STORAGE HER	ARCHY Brief - PDrivez: eVolume Grage -	Niteria - Uniteria -

- 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 administering StorageGRID and search for "proxy settings for E-Series AutoSupport."

#### Administer StorageGRID

- 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.

#### What you'll need

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



You must have SANtricity firmware 8.70 (11.70) 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 do not 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.

Set up and 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.

=	SADAncey <sup>®</sup> System Manager		Un	named		Philippicas + 1 Has	e i Light
*	Harrie		Welcome to SAVitricity Welcome to SAVitricity	Your storage array is o <sup>#</sup> System Manager. Get sta turne group for your storage	optimal. Hed by creating a pool or array.	View Operation	ons in Paymer >
-	(atleast		0	een a poil 1. Greate à volume	(horb		
~	Settinge Support	RAGE ARRAY LEVEL PER	RECREMANCE	64 <mark>68 69</mark> 69 6	Garryans Co	View Parform	OFTE (Assats)
		10.10.40 (4)	udian (43	w ców MB/s Ŏ	entras ent		DPS (Writed)
	CAR	ACITY O % Free 223531.39 GB Tinal	Www.Gague.30/ Datada # In integrate © program (Ma) In the © program (Ma) Integram (Ma) Int	STORAGE HERARCO	erY a Post • a Post • a Post • a Post • a Post • a Post • a Post •	Hind Cash	ns • BWuntoadx •

- 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.

	☐ Show status icon details 🕜
	Show front of shelf
<b>1</b> ,2	Fan Canister 2
<b>#</b>	*
<sup>1</sup> , <sup>1</sup>	

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 cannot access to the SANtricity System Manager from the StorageGRID Appliance Installer, you must set a static IP address for each storage controller to ensure that you do not lose your management connection to the hardware and the controller firmware in the controller shelf.

#### What you'll need

- 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 do not 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.



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.

Pv4 Address Assignment	Static	
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

## **Optional: Enable node encryption**

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

#### What you'll need

Review the information about KMS in the instructions for administering StorageGRID.

#### 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.



Data that exists prior to connecting to the KMS on an appliance that has node encryption enabled is encrypted with a temporary key that is not secure. The appliance is not protected from removal or theft until the key is set to a value provided by the KMS.

Without the KMS key needed to decrypt the disk, data on the appliance cannot be retrieved and is effectively lost. This is the case whenever the decryption key cannot be retrieved from the KMS. The key becomes inaccessible if you clear 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 cannot be decrypted without using the same KMS key.

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

NetApp <sup>®</sup> StorageGRID <sup>®</sup> Appliance Installer H						
Home	Configure Networking -	Configure Hardware 👻	Monitor Installation	Advanced -		
Nodo E	nonvotion					
Node en	cryption allows you to use an e	yternal key management sen	ver (KMS) to encrypt all S	toraneGRID data r	on this appliance. If node encryption is enabled for the	
applianc	e and a KMS is configured for t	he site, you cannot access a	ny data on the appliance u	inless the appliance	ce can communicate with the KMS.	
Encrypt	tion Status					
A You	u can only enable node encrypti	on for an appliance during inst	tallation. You cannot enabl	e or disable the no	de encryption setting after the appliance is installed.	
	Enable node encryption					
		Powe				
		oave				
Key Ma	nagement Server Details					

#### 3. Select Enable node encryption.

Prior to appliance installation you can unselect **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 are not able to 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 cannot 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.

#### **Related information**

Administer StorageGRID

Monitor node encryption in maintenance mode (SG5700)

## **Optional: Change RAID mode (SG5760 only)**

If you have an SG5760 with 60 drives, you can change to a different RAID mode to accommodate your storage and recovery requirements. You can only change the mode before deploying the StorageGRID appliance Storage Node.

#### What you'll need

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

#### About this task

Before deploying the SG5760 appliance as a Storage Node, you can choose one of the following volume configuration options:

• **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 RAID6, DDP delivers better system performance, reduced rebuild times after drive failures, and ease of management. DDP also provides drawer loss protection in 60-drive appliances.

- **DDP16**: This mode uses two parity drives for every 16 data drives, which results in higher storage efficiency compared to DDP. When compared to RAID6, 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. To use RAID 6 mode, your configuration must contain at least 20 drives. Although RAID6 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.

#### Steps

1. Using the service laptop, open a web browser and access the StorageGRID Appliance Installer: https://E5700SG\_Controller\_IP:8443

Where *E5700SG\_Controller\_IP* is any of the IP addresses for the E5700SG controller.

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

#### **Related information**

NetApp E-Series Systems Documentation Site

## **Optional: Remap network ports for appliance**

You might need to remap the internal ports on the appliance Storage Node to different external ports. For example, you might need to remap ports because of a firewall issue.

#### What you'll need

- You have previously accessed the StorageGRID Appliance Installer.
- You have not configured and do not plan to configure load balancer endpoints.



If you remap any ports, you cannot use the same ports to configure load balancer endpoints. If you want to configure load balancer endpoints and have already remapped ports, follow the steps in Remove port remaps.

#### Steps

1. From the menu bar of the StorageGRID Appliance Installer, click **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. Click Add Rule.

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

Remap Ports

If required, you can remap the internal ports on the appliance Storage Node to different external ports. For example, you might need to remap ports because of a firewall issue.

X Remove Select		ed Rule 🕂 Ad	dd Rule Network	Grid	Protocol TCP	•
	Remap Direction	Inbound	<ul> <li>Original Port</li> </ul>	1	÷	
Mapped-To Port 1						
	Network	Protocol	Remap Direction		Original Port	Mapped-To Port
$^{\circ}$	Grid	TCP	<b>Bi-directional</b>		1800	1801

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

#### **Copyright information**

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

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

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

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

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

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

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

#### **Trademark information**

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