Quick Start Guide

For models: G200, G400, G600, G800

Release Date: April 2019

SPHiNX is a fully integrated, disk-based data protection solution that allows host servers to backup to and restore data from a virtual tape drive or virtual tape library (VTL). For every host connection to SPHiNX, the host system “sees” a tape drive or virtual tape library. Data can be migrated to physical tape for archival storage or disaster recovery, if long-term backup copies are required.

This *Quick Start Guide* describes how to deploy the SPHiNX hardware and then configure SPHiNX on the network:

1. Review your model's hardware and configuration
2. Prepare for installation
3. Unpack the hardware
4. Cable the SPHiNX appliance
5. Power on the hardware
6. Install the appliance bezel
7. Configure network settings for the IPMI card
8. Configure storage space and path failover, if deploying external storage

Refer to the documentation provided with the external disk array(s) for mounting, cabling, and configuration instructions.

After completing the procedures in this guide, log in to the web interface as described in "Access the web interface" on page 23 and configure SPHiNX as described in the *Configuration Guide*."Get help" on page 25 describes how to access the product documentation and specifications and how to contact Support.

Review your model's hardware and configuration

Note Contact ETI-SPHiNX for available add-on or replacement components. Hardware components must be supplied by ETI- SPHiNX to ensure proper support, operation, and maintenance per your maintenance contract.

SPHiNX G200, G400, G600, and G800

All G-Series models come with an integrated engine that ensures outstanding backup efficiency and provides enhanced replication that simplifies data transfers. SPHiNX uses its own connected disk storage. Additionally, SPHiNX can be designated as an Alternate IPL device in order to migrate data to a new system or restore the entire system image of an old system or partition. This means that system downtime can be reduced as any full system save backups can be restored efficiently back to a system partition using a virtual tape drive on the SPHiNX as the designated Initial Program Load (IPL) device.

No internal storage disks are provided in the SPHiNX G800. Here is how the disks in the SPHiNX G Series servers are arranged when shipped from the factory.

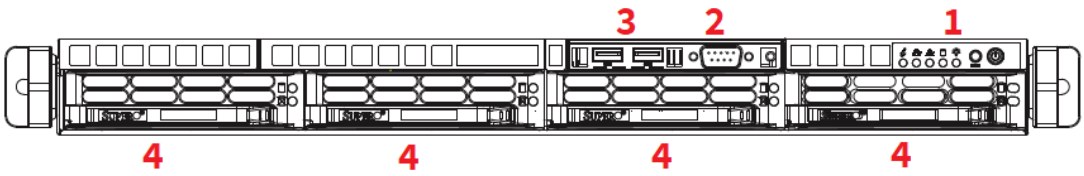
Model	Available Storage Bundle	CPU	OS	RAID Configuration
G200	6TB 18TB	1x6 cores	128GB DoM (mirrored)	One ZFS RAIDZ-1 set
G400	5TB 8TB	2x10 cores	250GB SSD (mirrored)	One RAID6 set
	no storage	2x6 cores	250GB SSD (mirrored)	
G600	16TB 24TB 32TB 40TB 48TB 64 TB 80TB 96TB	2x6 cores	256GB SSD (mirrored)	One ZFS RAIDZ-2 set
G800	16TB	2x10 cores	250GB SSD (mirrored)	One RAID6 set

SPHiNX G200 Business Standard

Here is an overview of the SPHiNX hardware that may have been purchased:

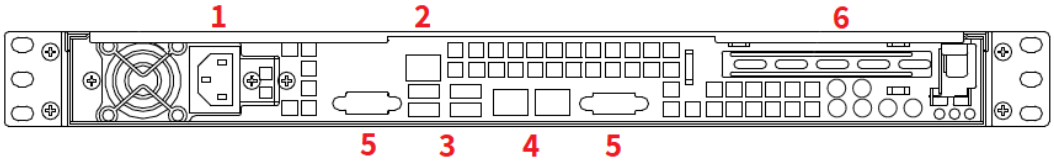
Model/ Storage Capacity	Max FC Ports/ Max Tape Devices	Replication	Deduplication/ Encryption	Internal Disks	External Disks
G200 6TB to 18TB	4x8Gbps 4 VTL & 32 VTD	Enhanced with Optimization Engine	-	SATA 6Gbps	FC, iSCSI, NFS

Front Panel



1. Control Panel
2. COM2 Port
3. USB Port(s)
4. SATA Drive(s)

Back Panel



Note : The G200 model features redundant power supplies (one, by default, the second one, optional).

1.Power Supply

2.IPMI Port

3.USB Port(s)

4.Ethernet Ports (left: eth0 - SPHiNX management port/ right: eth1 - optionally to be used for replication and remote export)

5.VGA Port(s)

6. PCI Expansion Slot FC/SAS

For slots 3-7, the following cards may be installed. The ports on each card are numbered (a and b on 2-port cards, a-d on 4-port cards).

- Dual-port 8Gb Fibre Channel card

- Quad-port 8Gb Fibre Channel card

- Dual-port SAS card

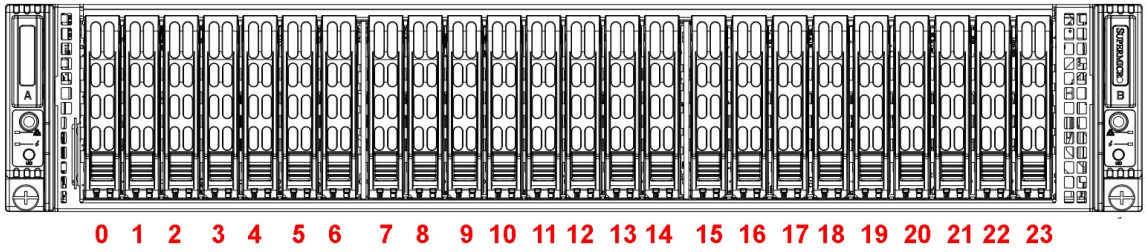
Slot 1 contains a SAS HBA for internal disk support (with no external ports), and slot 2 is reserved for future use.

SPHiNX G400 Business Dedup

Here is an overview of the SPHiNX hardware that may have been purchased:

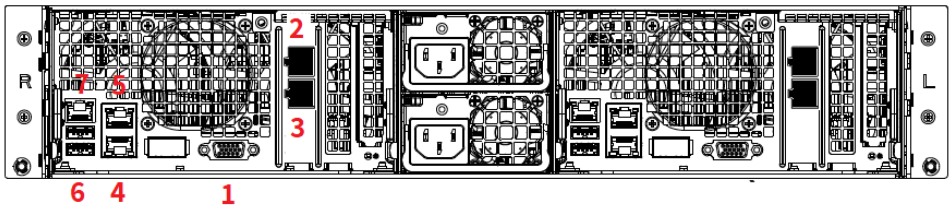
Model/ Storage Capacity	Max FC Ports/ Max Tape Devices	Replication	Deduplication/ Encryption	Internal Disks	External Disks
G400 5TB, 8TB	4x8Gbps up to 4 VTL & 32 VTD	Enhanced with Optimization Engine	in-line FIPS 140-2 / AES 256	SAS 12Gbps	FC, SAS, iSCSI, NFS

Front panel



Note The slots are distributed per server as follows: 0-13 Left / 14-23 Right.

Back Panel - SPHiNX (Right Side)



1.VGA Port

2. eth2

3.eth3

4.eth0

5.eth1

6.USB Port(s)

7.IPMI Port

Note eth0 and eth1 are Ethernet ports of 10Gbs each

Note eth2 and eth3 are Ethernet ports of 1Gbs each

For slots 5-7, the following cards may be installed. The ports on each card are numbered from top to bottom (a and b on 2-port cards, a-d on 4-port cards).

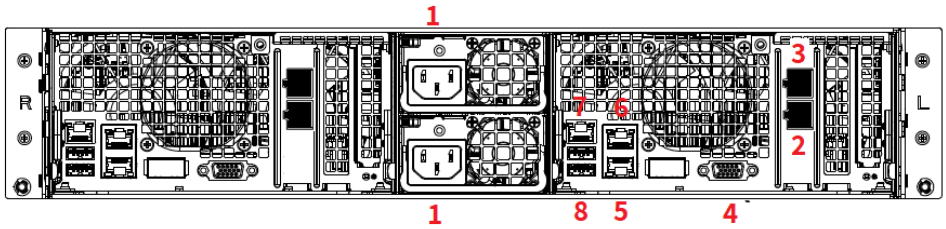
- Dual-port 8Gb Fibre Channel card

- Quad-port 8Gb Fibre Channel card

- Dual-port SAS card

Slots 1-4 are not supported and cannot be used.

Back Panel - G400 (Left Side)



1.Power Supply

2. ens2f1

3.ens2f0

4.VGA Port

5. ENO1

6.ENO2

7.IPMI Port

8. USB Port(s)

Note ENO1 and ENO2 are Ethernet ports of 10Gbs each.

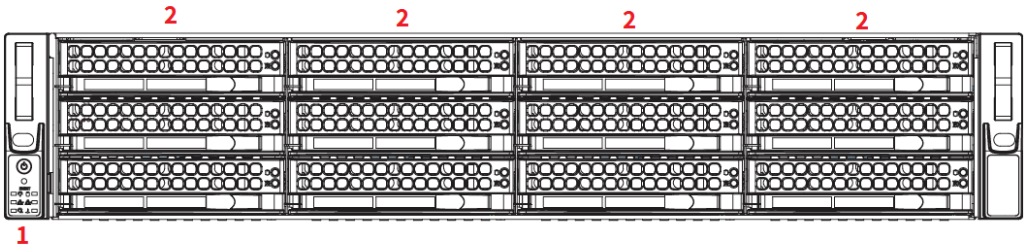
Note ENS2F0 and ENS2F1 are Ethernet ports of 1Gbs each.

SPHiNX G600-800 Enterprise Standard

Here is an overview of the SPHiNX G600 hardware:

Model/ Storage Capacity	Max FC Ports/ Max Tape Devices	Replication	Deduplication/ Encryption	Internal Disks	External Disks
G600 16TB to 96TB	16x8Gbps up to 16 VTL & 32 VTD	Enhanced with Optimization Engine	-	SAS 12Gbps	FC, SAS, iSCSI, NFS
G800(G600 bundle with G850 Deduplication shelf storage) 10TB to 120TB	16x8Gbps 16 VTL & 32 VTD	Enhanced with Optimization Engine	in-line FIPS 140-2 / AES 256	SAS 12Gbps	FC, SAS, iSCSI, NFS

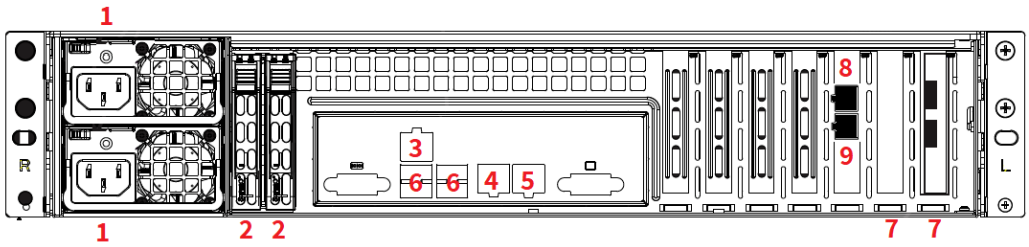
Front panel



1.Control Panel

2.SAS Drive(s) - 12 - no disks

Back panel - G600



1.Power Supply

2.OS Drive(s)

3.IPMI Port

4.eth0

5.eth1

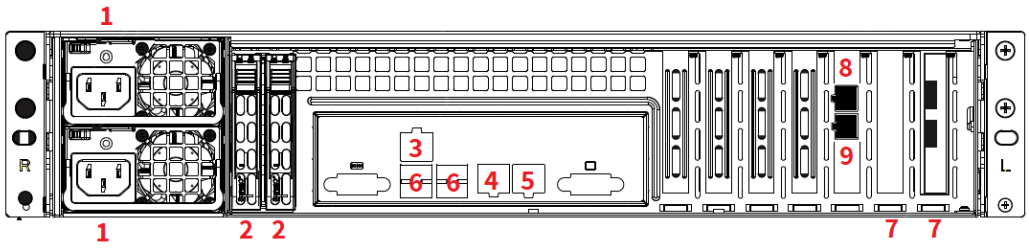
6.USB Port(s)

7. Reserved Slot(s)

8.eth2

9. eth3

Back panel - G850



1.Power Supply

2.OS Drive(s)

3.IPMI Port

4.ENO1

5.ENO2

6.USB Port(s)

7. Reserved Slot(s)

8.ENS3F0

9.ENS3F1

Prepare for installation

To ensure that you are ready for deployment, complete the following tasks:

Choose a location

When considering the location, note the following:

- ❑ Place the server and its components near 110 or 220/240 volt power outlets (unless you will mount the SPHiNX server in an IBM rack). SPHiNX uses redundant power supplies, so consider independent power sources for high-availability operation. Additional power outlets might be required for external tape drives or RAID storage devices.

  Note It is recommended that you connect SPHiNX through an uninterruptible power supply (UPS). Otherwise, data loss may occur in case of a power outage.

- ❑ Allow space for the SPHiNX server, depending on the model, and place the SPHiNX server near the host server.

- ❑ Determine the distance between the host server and the SPHiNX server and the distance between the SPHiNX server and external storage devices. These distances are important to your selection of HBA cables.

- ❑ If Data Encryption is licensed and you intend to encrypt data that is written to virtual tape, ensure the connection between the host and SPHiNX servers is secure. If you want to export encrypted virtual tapes, ensure the connection between the SPHiNX server and the physical drive or library is secure.

- ❑ Make sure the location is a clean, dust-free area that is well ventilated.

- ❑ Avoid areas where heat, electrical noise, and electromagnetic fields are generated.

Refer to the Get Help section for environmental considerations.

Zone SPHiNX for your environment

Configure zoning to include SPHiNX in the same zone as the resources needed by SPHiNX. This may include SANs, host servers, physical drives, physical libraries, backup management application servers, and so on. If you want to dedicate specific drives for use by SPHiNX, such as for exporting virtual tapes, it is recommended that you create a zone that includes the dedicated drives and also contains the backup management application, library changer, and drives to be used by the backup management application.

Gather network information

- eth0, eth1
- eth2, eth3
- EN01, EN02
- ens2f0, ens2f1

- Intelligent Platform Management Interface (IPMI) port

After you mount and cable the hardware, you must configure network settings. At a minimum, you must configure eth0 to specify a fully qualified domain name if using Dynamic Host Configuration Protocol (DHCP) and the IPMI port to be able to access the server console remotely.

Note You must use a static IP address if GFS is configured in your environment. DHCP is not supported with GFS.

For the eth0 port, gather this information if you do not want to use DHCP:

- IP address: _____
- Subnet mask: _____
- Default gateway: _____
- IP addresses of DNS servers: _____
- DNS search domains: _____

If a second subnet is available, you can use eth1 for replication (if the Data Replication feature will be used). It is recommended that you use eth1 in addition to eth0 to segregate replication traffic from network traffic to ensure adequate response times.

Note If a second subnet is not available, you cannot use eth1.

For the eth1 port, gather this information if you do not want to use DHCP:

- IP address: _____
- Subnet mask: _____
- Default gateway: _____

Always configure the IPMI port to ensure remote access to ETI-SPHiNX support team, in case you require such support. To monitor the hardware, you need to configure network settings for the IPMIcard, which are set to DHCP by default.

- IP address: _____
- Subnet mask: _____
- Default gateway: _____

Finally, in order to log in to configure network settings, you must obtain the serial number of the SPHiNX appliance. Note the serial number that is provided on a label on the back of the appliance.

Serial number: _____

Refer to the *Configuration Guide* for instructions to fully configure network settings.

Obtain tools and supplies for installation

You may need the following items to complete the installation instructions:

- #2 Phillips screwdriver
- Tape measure

- One of the following to access the command line interface and set up SPHiNX:
    - Terminal or a computer running a terminal emulation program
    - Keyboard and monitor, plus a VGA cable to connect the monitor to SPHiNX

Unpack the hardware

Before mounting and cabling SPHiNX, you must unpack the hardware and verify the box contents.

To unpack all hardware:

1. Unpack all hardware and retain packing materials.

   Note Always lift the SPHiNX appliance by the sides. Because the hardware is heavy, it is recommended that you use an assistant when lifting it.

2. Inspect the hardware and the contents of the box(es). If damage is apparent, contact the carrier and your vendor.

3. Place hardware on a flat, stable work surface.

Confirm that you received the following components, in addition to this guide and the appliance:

- ❑ Serial cable (RS-232, 3 meters / 10 feet)

- ❑ 2 rack rails

- ❑ Mounting hardware for G200, which includes

   x 4-8 (nut clips)

   x 4-8 (long, round-head screws)

- ❑ Rail kit, which includes

   x 2 (short, flat-head M4 screws)

   x 8 (long, flat-head M5 screws)

   x 2 (long, round-head M5 screws)

   x 8 (washers for the M5 screws)

Note Extra mounting hardware is provided that you may not use during installation.

Cable the SPHiNX appliance

You must cable the SPHiNX appliance to the host server, and then cable to any external storage devices.

Note If Data Encryption is licensed, it is recommended that you connect the SPHiNX server directly to the host server instead of connecting SPHiNX to a switch or router. If you want to export encrypted virtual tapes, ensure the connection between the host and SPHiNX servers is secure, and ensure the connection between the SPHiNX server and the physical drive or library is secure.

Refer to Review your model's hardware and configuration for rear panel illustrations, to identify ports and plugs on the back of the appliance.

To connect to host servers over Fiber Channel

You can connect the server to up to 16 host servers using Fiber Channel ports.

Note When connecting host servers over Fibre Channel to the SPHiNX server, use one port per host server, if possible. If connecting more than one host server through a switch, be aware that each Fibre Channel port on the SPHiNX server is configured to emulate one host type only. Host servers of differing types must be connected to separate ports.

1. Connect one end of a Fibre optic cable to a Fibre Channel port on the SPHiNX server.
2. Connect the other end of the cable to the host server.
3. Note the port number used on the SPHiNX server. Later, you will have to set this port to virtual mode using the SPHiNX web interface.
4. If you are cabling multiple host servers to SPHiNX, repeat these steps for each host server.

To connect to host servers over SAS

You can connect the server to up to 10 host servers - depending on the model - using SAS ports. Each port is dedicated to a host server or external device; you cannot connect to host servers and external devices using the same port (over different channels).

1. Connect one end of a SAS cable to a SAS port on the SPHiNX server.
2. Connect the other end of the cable to the host server.
3. Note the port number used on the SPHiNX server. Later, you will have to set this port to virtual mode using the SPHiNX web interface.
4. If you are cabling multiple host servers to SPHiNX, repeat these steps for each host server.

To connect to external tape devices (standalone drives or libraries)

1. For a Fibre Channel connection, connect one end of a Fibre optic cable to a Fibre Channel port on the SPHiNX server. For a SAS connection, connect one end of a SAS cable to a SAS port on the SPHiNX server.
2. Connect the other end of the cable to the external drive or library.
3. Note the port number used on the SPHiNX server. Later, you will have to set the port to physical mode using the SPHiNX web interface.
4. Repeat these steps for additional drives or libraries.

To connect to external disk array controllers

1. For a Fibre Channel connection, connect one end of a Fibre optic cable to a Fibre Channel port on the SPHiNX server. For a SAS connection, connect one end of a SAS cable to a SAS port on the SPHiNX server.
2. Connect the other end of the cable to the external disk array.
3. Note the port number used on the SPHiNX server. Later, you will have to set the port to physical mode using the SPHiNX web interface.
4. Repeat these steps for additional external disk arrays.

To connect to the network

Connect one end of an Ethernet cable to any Ethernet port. Connect the other end of the cable to the LAN or WAN switch.

For the IPMI card (to monitor the server), connect an Ethernet cable to the IPMI port. Connect the other end of the cable to the LAN or WAN switch. Refer to the *Configuration Guide* for more information about using this card.

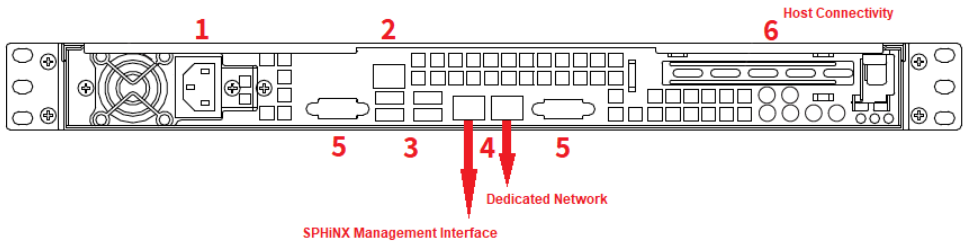
How to connect G200 to the network

To connect G200 to the network use the Ethernet ports 4 (left and right). The connection is indicated by a red arrow.

eth0 - port 4 left is connected to the SPHiNX management interface

eth1 - port 4 right is optionally connected to a dedicated network and it can be used for replication and remote export

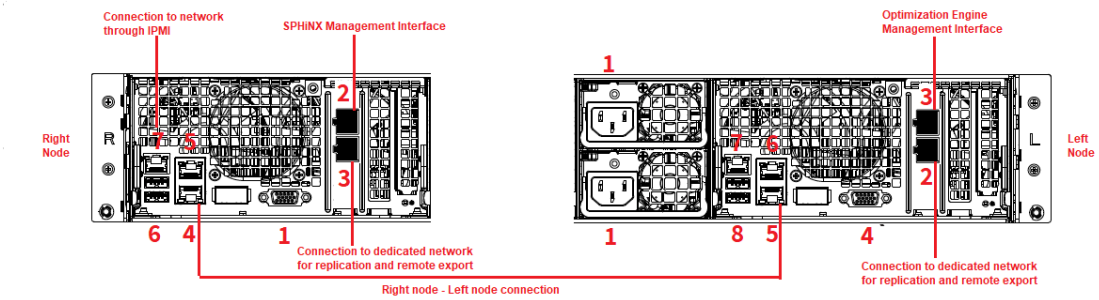
Ports 6 - PCI Expansion Slots FC/SAS - to be used for host connectivity



For a description of the other ports for each model, see Review your model's hardware and configuration.

How to connect G400 to the network

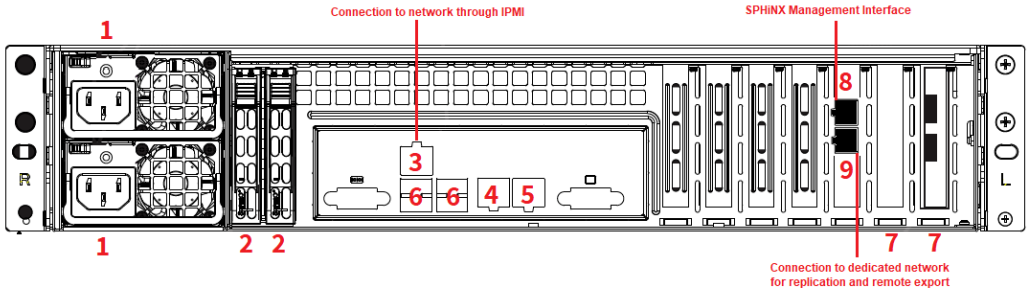
To connect G400 to the netowork follow the diagram below with the indicated connections:



For a description of the other ports for each model, see Review your model's hardware and configuration.

How to connect G600 to the network

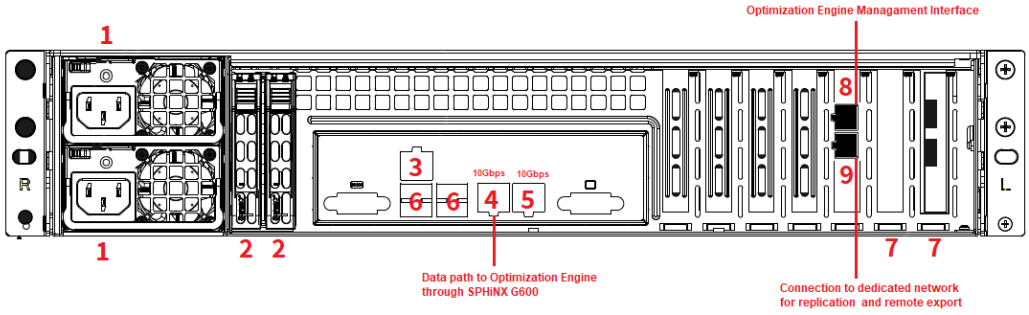
To connect G600 to the netowork follow the diagram below with the indicated connections:



For a description of the other ports for each model, see Review your model's hardware and configuration.

How to connect G850 to the network

To connect G600 to the netowork follow the diagram below with the indicated connections:



Power on the hardware

Press the power button on the front panel of the SPHiNX server, which changes from yellow to green, and the server self-boots. Allow the SPHiNX server to completely boot before proceeding. The console will display a login prompt when it is ready.

If problems arise, make sure there are no warning lights for any of the disk drives. Contact Support if you encounter hardware issues.

Install the appliance bezel

On all models except the WS, attach the bezel to the front of the SPHiNX appliance by inserting the bezel into the left side of the appliance and then into the right. Use the holes as guides and verify that both sides are seated firmly.

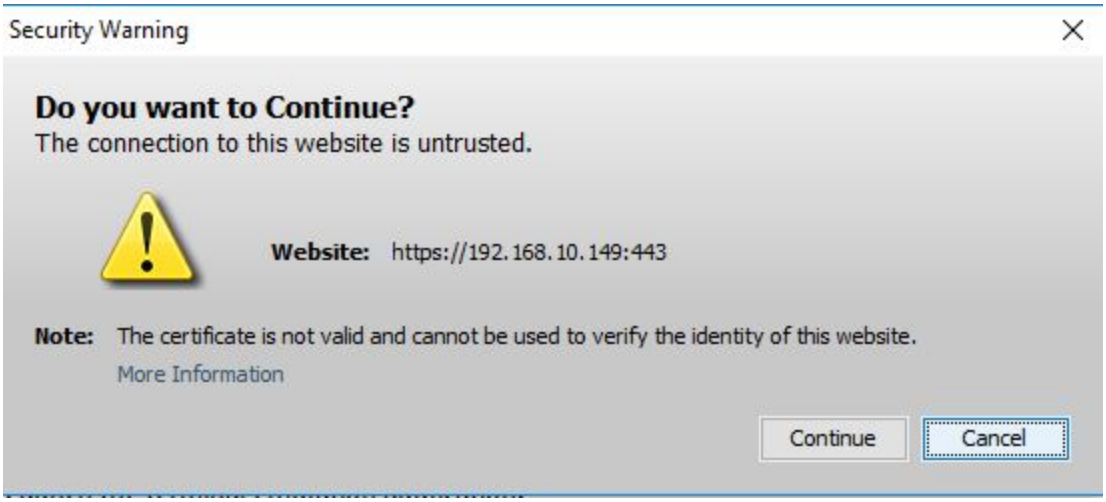
Network Configuration Settings

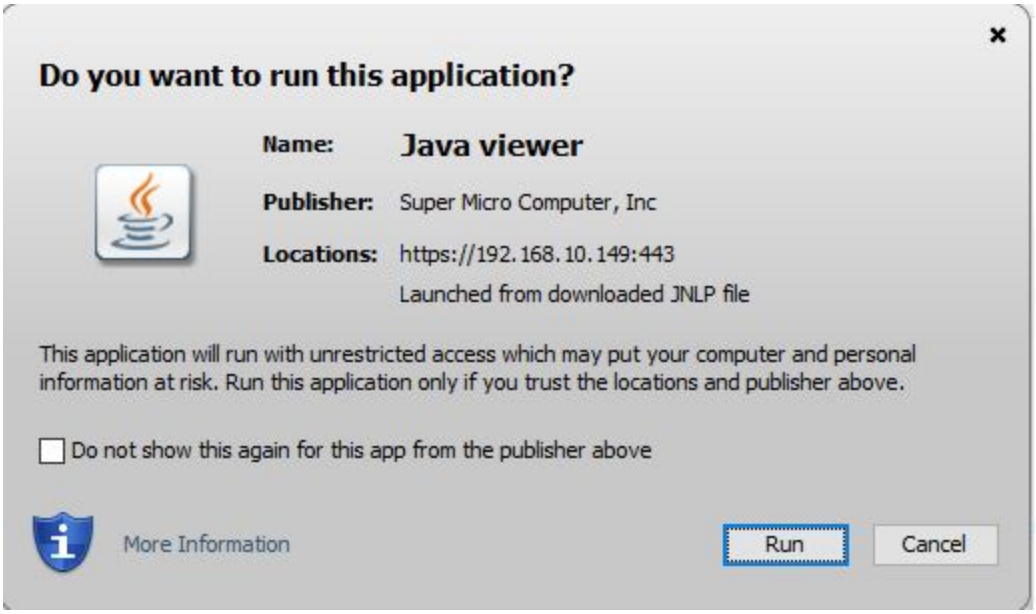
Proceed to configuring the network once the server is racked and the SPHiNX application is pre-installed. Use the IPMI configuration in the default DHTP mode (with the assigned IP address).

Note The IP address can be physically changed by the network admin!

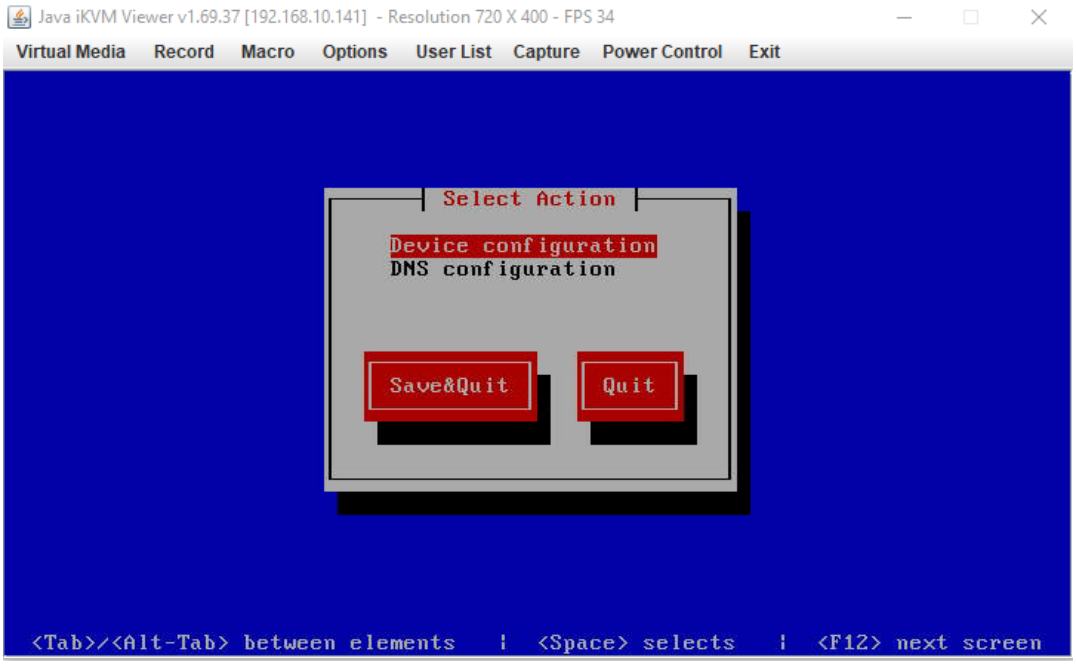
IPMI Configuration

1. Connect to IPMI via a supported web browser.
2. Use default credentials (**ADMIN/ADMIN**) to log into the IPMI Management Page.
    a. Use <**Remote Control**> menu and go to <**Console Redirection**>
    b. **Launch Console** and click **Keep** when promoted to acknowledge the security warning.
    c. Download the application, click **Continue**and then **Run**.

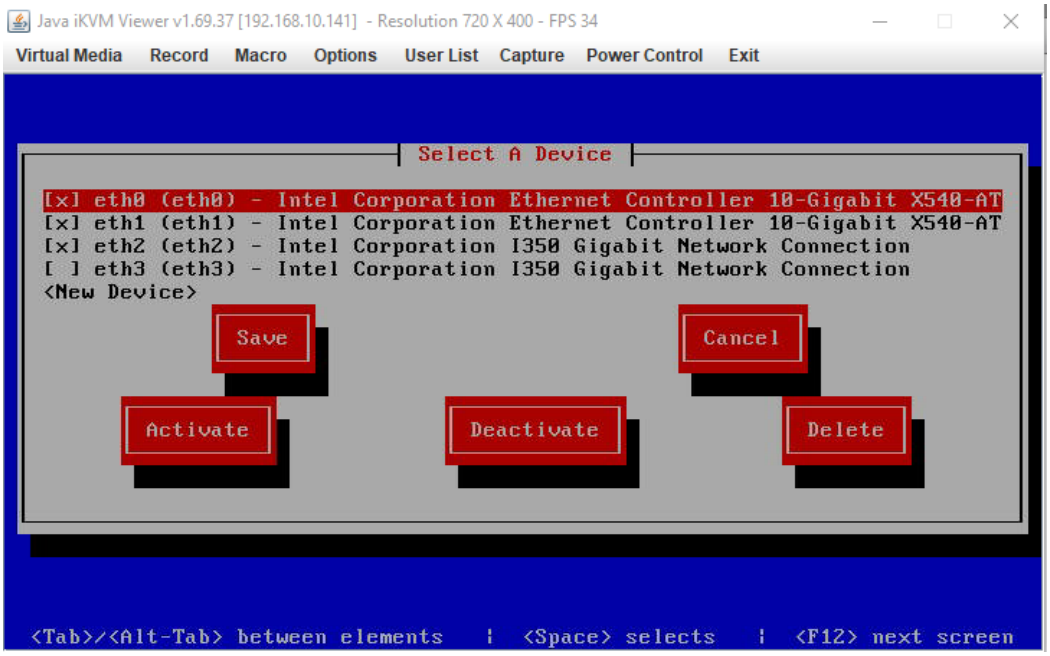




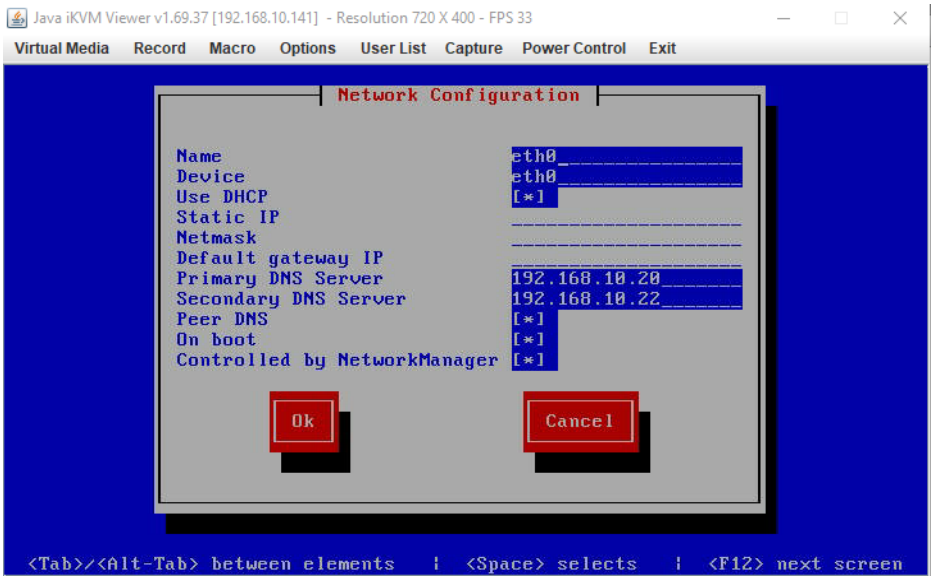
3. Connect as `root` and run `netconfig` to list all your connections.
4. Run `system-config-network` to configure the network through the interface.



5. Select **Device configuration** to configure the connection device. A list of connection devices allows to choose the device to be configure.



6. Configure the network through the chosen device by filling out the info for the network configuration parameters.



7. Click **OK** and select another device for configuration, if necessary.
8. When all the devices are configured, click **Save** and then **Save&Quit**.
9. Restart the service network.

NTP Server - To set the system clock

1. If you are not logged in, log in as **bill** and then change to the **root** user:

   ```
   su - root
   ```

2. Set the timezone as follows:
   a. Check the timezone setting by entering this command:

      ```
      date
      ```

   b. If the timezone is incorrect, edit the **/etc/sysconfig/clock** file to set the timezone. Here is an example of the timezone entry in the file:

      ```
      ZONE="America/New_York"
      ```

      where **America/New_York** is the timezone file in **/usr/share/zoneinfo/posix**. You can get a list of valid timezone files by entering this:

      ```
      tree –fi /usr/share/zoneinfo/posix | cut –d/ -f6-
      ```

   c. Enter this command to update **/etc/localtime**:

      ```
      /usr/sbin/tzdata-update
      ```

   d. Change the PHP timezone by editing the **/etc/php.ini** file and updating the following line with the correct timezone:

      ```
      date.timezone = America/Chicago
      ```

3. Set the time using this command:

   ```
   date MMDDhhmmyyyy.ss
   ```

   where

   - *MM* is the month
   - *DD* is the day
   - *hh* is the hour (in 24-hour format)
   - *mm* is the minute
   - *yyyy* is the year
   - *ss* is the seconds

4. To set the hardware clock, enter this command:

   ```
   hwclock --systohc
   ```

5. Configure the Network Time Protocol (NTP) by editing the **/etc/ntp.conf** file, as follows:
   a. Remove this line:

      ```
      restrict -6 default kod nomodify notrap nopeer noquery
      ```

   b. Add these lines, which specify servers with which to synchronize (there should be three lines only):

```
restrict 0.centos.pool.ntp.org mask 255.255.255.255 nomodify
notrap noquery
restrict 1.centos.pool.ntp.org mask 255.255.255.255 nomodify
notrap noquery
restrict 2.centos.pool.ntp.org mask 255.255.255.255 nomodify
notrap noquery
```

c. Save and close the file.

6. Enable the NTP service:

```
chkconfig ntpd on
```

7. Start the NTP service:

```
/etc/init.d/ntpd start
```

8. Disconnect the serial cable, Ethernet cable attached to port 2, or the keyboard and monitor from the server.

Configure storage space and path failover

If you are deploying an external array, you must define a storage space on the array for use with the Linux operating system. Then, present a logical unit number (LUN) that refers to this storage space. When defining LUNs on an array, start at LUN 0. Otherwise, SPHiNX might not recognize them. Each LUN should not represent more than 16TB of space. See the array documentation for details.

Multi-pathing is required when more than one physical or logical path exists between SPHiNX and external disk storage. If a path fails, path failover occurs and another path becomes active and handles I/O for the LUNs on the failed path. Only one path is active at a time for a LUN.

Note Path failover is supported for Fibre Channel disk array controllers only; failover is not supported for SAS controllers.

To support multipathing, SPHiNX uses the **dm-multipath**, **device-mapper**, and **device-mapper-multipath** RPMs, which are installed by default on the server.

To enable multipathing and start the multipathd daemon

1. At the command prompt, log in as **bill**.
2. Become **root**:

   ```
   su -
   ```

3. Configure multipathing with defaults and start the daemon:

   ```
   mpathconf --enable --with_multipathd y
   ```

   Note The **/etc/multipath.conf** file is created when you run this command.

4. Run following commands to review the list of known multipathed disks:

   ```
   ls /dev/mapper/
   multipath -v2 -ll
   ```

   The multipath devices can be accessed using the device names:

   ```
   /dev/mapper/mpathN
   ```

Multipath settings, such as device names, can be customized by editing the **/etc/multipath.conf** file and restarting the multipathd daemon using these commands:

```
vi /etc/multipath.conf
service multipathd restart
```

For additional information on configuring an external storage array and path failover, consult the array vendor's documentation (for Linux).

IPMI

The IPMI port ensures the connection to the system management software in order to manage multiple, disparate servers. IPMI operates independently of the operating system (OS) to allow the system to be managed remotely.

Note Make sure the SPHiNX appliance is connected to the LAN through the IPMI port.

Access the web interface

The SPHiNX web interface enables you to configure and manage SPHiNX.

To access the web interface

On a computer that is connected to the same network as SPHiNX, launch a web browser.

Enter the hostname or IP address of SPHiNX in the address field.

Your browser may display a warning page and certificate errors. SPHiNX ships with a self-signed certificate that is used to establish a secure communication channel between your browser and the SPHiNX web application server.

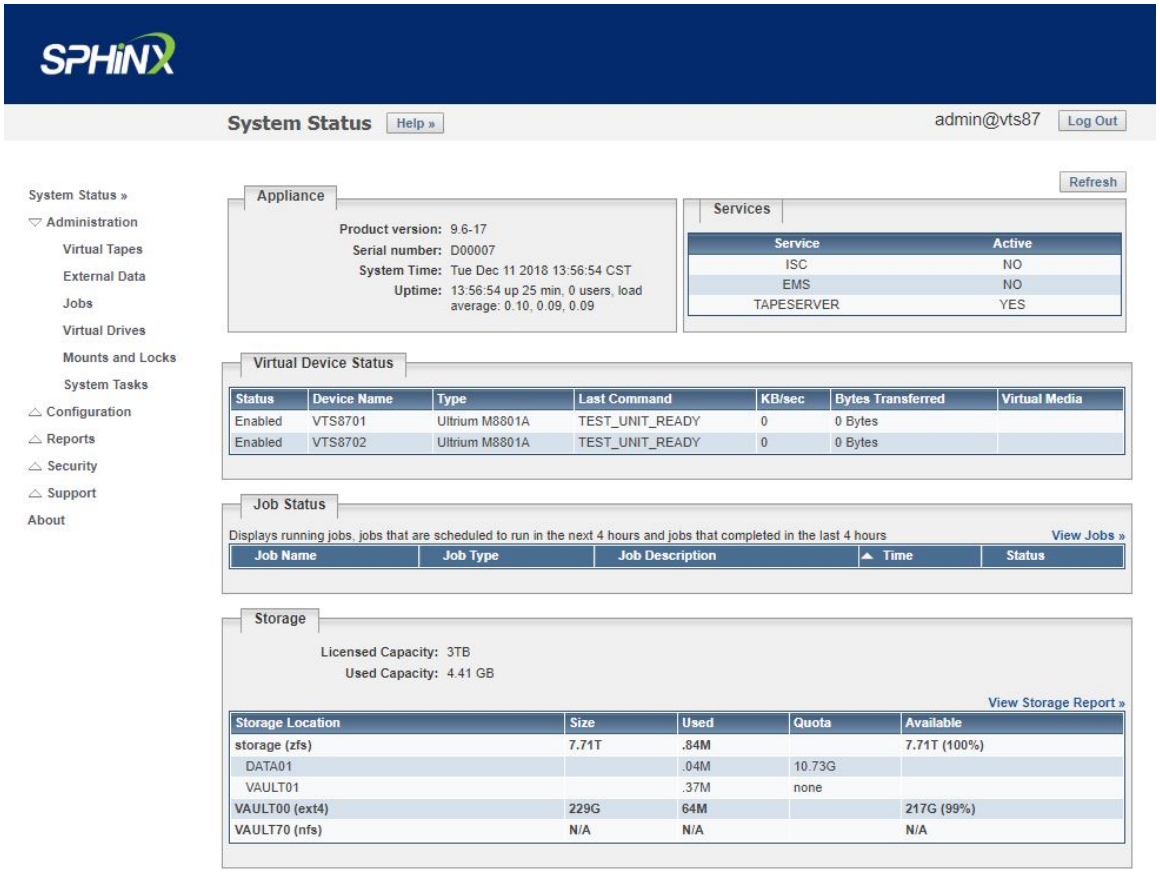
This self-signed certificate may cause your browser to display a certificate warning for these reasons:

- Many browsers warn you when a web application employs a self-signed certificate. These certificates are not considered as secure as a certificate signed by a Certificate Authority.
- When the SPHiNX default self-signed certificate is created, a temporary hostname is used for the appliance. During deployment, this hostname most likely changed. Many browsers warn you when the hostname on the certificate and the hostname on the appliance do not match.

When the browser displays this warning, accept the certificate or add an exception (depending on your browser) and continue to the web interface. Refer to the browser help for more information.

When prompted, log in by entering a username and password. (Authentication is required once for each browser session. If this is the first time you are logging in, enter **admin** as the username and **virtual** as the password. For a list of these accounts, refer to the Configuring User Accounts chapter in the *Configuration Guide*.

Then, this page is displayed.



To install the VPD (Vital Product Data) file

1. Once logged into the UI, go to **Configuration** page and under **System** Configuration click **Upload Vital Product Data (VPD) File**
2. Choose the provided VPD file and click **UPLOAD**. The VPD file has been provided with your product.
3. Once the file is uploaded, the serial number of your appliance has been changed in such a way that it can be now used on the certificate portal to generate license key(s) for different SPHiNX features.
4. Go to the **Certificate Portal** and copy the ceriticate code that has been provided via email with your appliance.
5. Generate License Key(s) and submit it/them on the **Manage System Licenses** page under **Configuration** tab> **System**.

To obtain the license key

Refer to the Certificate sent to you by email with your product.

Get help

This section lists documents and URLs that you can reference for more information about SPHiNX.

Documentation

- *Configuration Guide*, which describes how to configure SPHiNX and use the SPHiNX web interface to manage SPHiNX
- Help, which provides detailed instructions for working with the web interface

All documentation is available on the About page of the web interface.

Specifications

- SPHiNX G200: https://www.supermicro.com/products/system/1U/5018/SYS-5018R-M.cfm?parts=SHOW#jump
- SPHiNX G400: https://www.supermicro.com/products/system/2u/2028/SYS-2028TP-DC1TR.cfm?parts=SHOW#jump
- SPHiNX G600: https://www.supermicro.com/products/system/2U/6028/SSG-6028R-E1CR12L.cfm?parts=SHOW#jump
- SPHiNX G850: https://www.supermicro.com/products/system/2U/6028/SSG-6028R-E1CR12T.cfm?parts=SHOW#jump

Support

For Technical Support, refer to https://etinet.atlassian.net/servicedesk/customer/portals.

Safety guidelines

To reduce the risk of bodily injury, electrical shock, fire, and damage to the equipment, observe the following precautions. This equipment must be installed by trained service personnel in a restricted-access location, as defined by UL 60950 and IEC 60950, The Standard for Safety of Information Technology Equipment.

Electrical safety precautions

Basic electrical safety precautions should be followed to protect you from harm and the system from damage.

- Be aware of the locations of the on/off switch on the chassis as well as the room's emergency power-off switch, disconnection switch or electrical outlet(s). The on/off switch does not disconnect power to the chassis. If an electrical accident occurs, quickly remove power to the system by removing the plug(s) from the outlet(s). Some models may have multiple power cords which connect to more than one outlet.
- The power supply power cords must include a grounding pin and must be plugged into grounded electrical outlets. When a power cord is not packaged with the equipment, the local installer is to select approved detachable power cords, suitable for the current and voltage ratings of the equipment
- When working around high voltage electrical circuits, another person who is familiar with the power-off controls should be nearby to switch off (or remove) power to the chassis if necessary.
- Power should always be disconnected from the system when removing or installing main system components, such as the boards, memory modules, DVD-ROM, and floppy drives (not necessary for hot swappable drives). When disconnecting power, you should perform an orderly shut down using the SPHiNX command line or web interface and then unplug the power cords of all the power supply units in the system.
- Use only one hand when working with powered-on electrical equipment. This is to avoid making a complete circuit, which will cause electrical shock. Use extreme caution when using metal tools, which can easily damage electrical components or circuit boards they come into contact with.
- Do not use mats designed to decrease electrostatic discharge as protection from electrical shock. Instead, use rubber mats that have been specifically designed as electrical insulators.
- DVD-ROM Laser: CAUTION - this server may have come equipped with a DVD-ROM drive. To prevent direct exposure to the laser beam and hazardous radiation exposure, do not open the enclosure or use the unit in any unconventional way.
- Do not work alone when working with high voltage components.
- Mainboard replaceable soldered-in fuses: Self-resetting PTC (Positive Temperature Coefficient) fuses on the mainboard must be replaced by trained service technicians only. The new fuse must be the same or equivalent as the one replaced.

General safety precautions

Follow these rules to ensure general safety.

- Keep the area around the system clean and free of clutter.
- The system is heavy. When lifting the system, two people at either end should lift slowly with their feet spread out to distribute the weight. Always keep your back straight and lift with your legs.
- Place the chassis top cover and any system components that have been removed away from the system or on a table so that they will not accidentally be stepped on.
- While working on the system, do not wear loose clothing, such as neckties and unbuttoned shirt sleeves, that can come into contact with electrical circuits or be pulled into a cooling fan.
- Remove any jewelry or metal objects from your body, which are excellent metal conductors that can create short circuits and harm you if they come into contact with printed circuit boards or areas where power is present.
- After accessing the inside of the system, close the system back up and secure it to the rack unit with the retention screws after ensuring that all connections have been made.
- Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.
- Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
- Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).
- This equipment is only intended to be used in areas with restricted admittance and from trained personnel.
- This equipment is not be used as a workstation
- Slide- and rail-mounted equipment is not to be used as shelf or workspace.

ESD precautions

Electrostatic discharge (ESD) is generated by two objects with different electrical charges coming into contact with each other. An electrical discharge is created to neutralize this difference, which can damage electronic components and printed circuit boards. The following measures are generally sufficient to neutralize this difference before contact is made to protect your equipment from ESD.

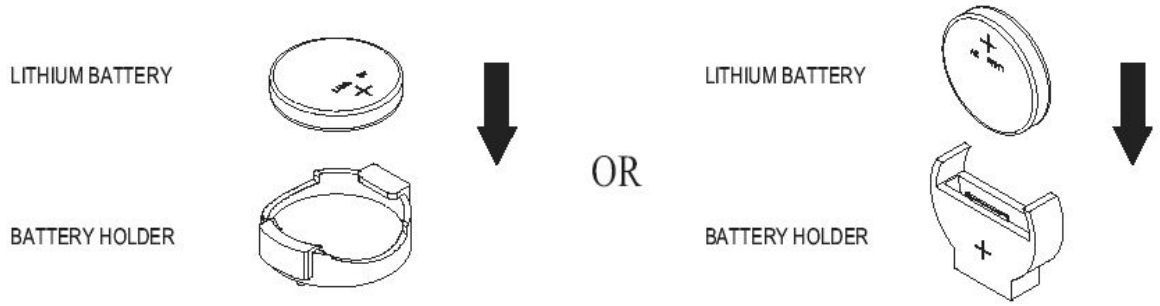
- Use a grounded wrist strap designed to prevent static discharge.
- Keep all components and printed circuit boards (PCBs) in their antistatic bags until ready for use.
- Touch a grounded metal object before removing the board from the antistatic bag.

- Do not let components or PCBs come into contact with your clothing, which may retain a charge even if you are wearing a wrist strap.
- Handle a board by its edges only; do not touch its components, peripheral chips, memory modules or contacts.
- When handling chips or modules, avoid touching their pins.
- Put the serverboard and peripherals back into their antistatic bags when not in use.
- For grounding purposes, make sure your computer chassis provides excellent conductivity between the power supply, the case, the mounting fasteners and the serverboard.

Operating precautions

Care must be taken to assure that the chassis cover is in place when SPHiNX is operating to assure proper cooling. Out of warranty damage to the system can occur if this practice is not strictly followed.

CAUTION: When installing the serverboard battery, there is a danger of explosion if the onboard battery is installed upside down, which will reverse its polarities (see figure). The battery must be replaced only with the same or an equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.



Provide input power to the system by plugging the power cord(s) from the power supply unit(s) into a high-quality power strip that offers protection from electrical noise and power surges. An uninterruptible power supply (UPS) is recommended.