

Amulet Hotkey CoreStation HX5

System Installation Guide

SG



Contents

1. Important Safety Information	2
2. Enclosure and services	3
3. Management and Network Modules	9
4. Hardware Installation and Setup	17
5. Management Serial Port	23
6. Security Features and Best Practice Deployment	25
7. Specifications and Compliance	27

1. Important Safety Information

Caution

To prevent damage to the CoreStation HX install and follow proper use guidelines in accordance with these instructions

- Only use accessories provided by Amulet Hotkey, including power supply mains leads. The mains leads include a protective earthing conductor which must be connected to a socket outlet with an earthing connection.
- Always turn off the compute nodes before disconnecting power
- Turn off and disconnect all power supplies before handling the enclosure
- This enclosure is designed to use one to four power supplies, to disconnect from its power source, all mains leads must be unplugged
- The network ports of this product are intended to be connected to the building internal network only and not to external ports outside of the building.
- Do not expose the enclosure to moisture
- Do not place objects filled with liquid on or near the enclosure
- Refer all servicing to qualified personnel

Laser Safety

- This enclosure may be fitted with SFP network modules that contain class 1 lasers. The SFP module emits invisible radiation which can cause harm if installed or serviced incorrectly.
- Complies with 1 CFR 1040.10 and 1040.11 except for deviations pursuant to Laser Notice No. 50, dated June 24, 2007.
- Warning: Class 1 laser product
- Warning: Invisible laser radiation can emit from the aperture of the SFP port when no fibre is connected. To avoid exposure to laser radiation, do not stare at apertures.
- Warning: Only trained and qualified personnel may install, replace, or service this equipment

2. Enclosure and services

2.1 System Front View

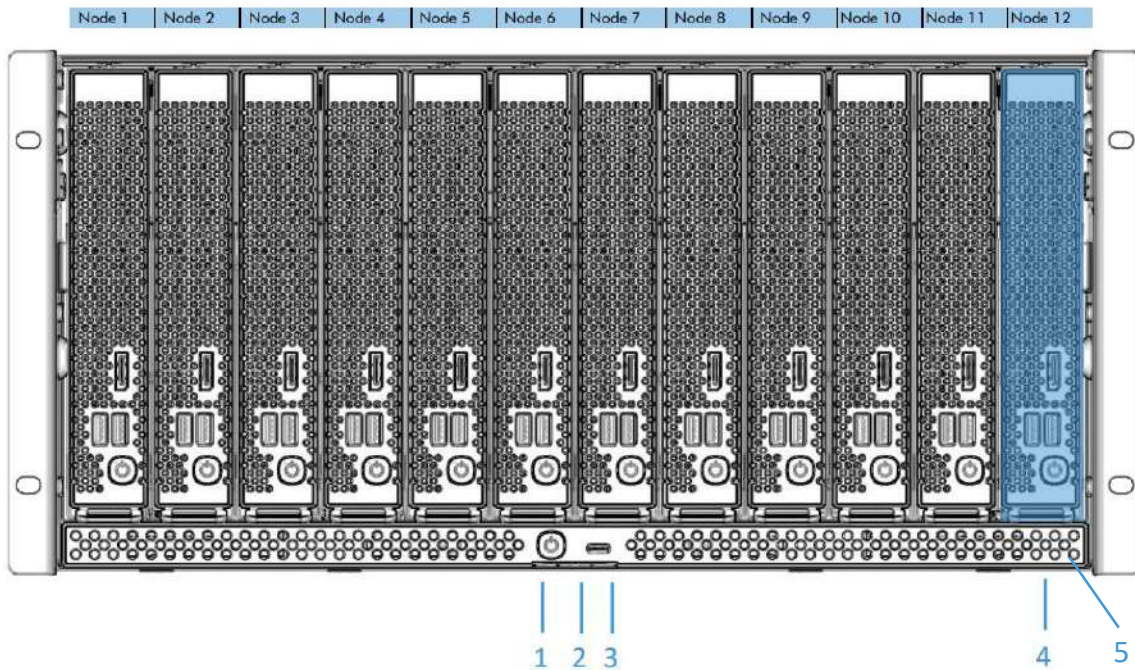


Figure 1 - CoreStation HX5 Enclosure front view

1	Enclosure power button and system status indicator	Power indicator shows a summary of the system state and any health warnings which affect the Enclosure.
2	Enclosure pull-out tab	Pull-out information label containing enclosure serial number and QR code link to Amulet Hotkey website
3	System front serial console (USB-C)	Serial interface for initial system configuration and setup. Not required in general use.
4	Workstation Node, slot 12 highlighted	Each workstation node can be independently inserted and removed as required using the blue handle at the front. Up to 12 single-width workstation nodes can be fitted.
5	Air inlet for cooling Power Supplies and IO Modules	Keep this area clear for correct system operation.

2.2 System Rear View

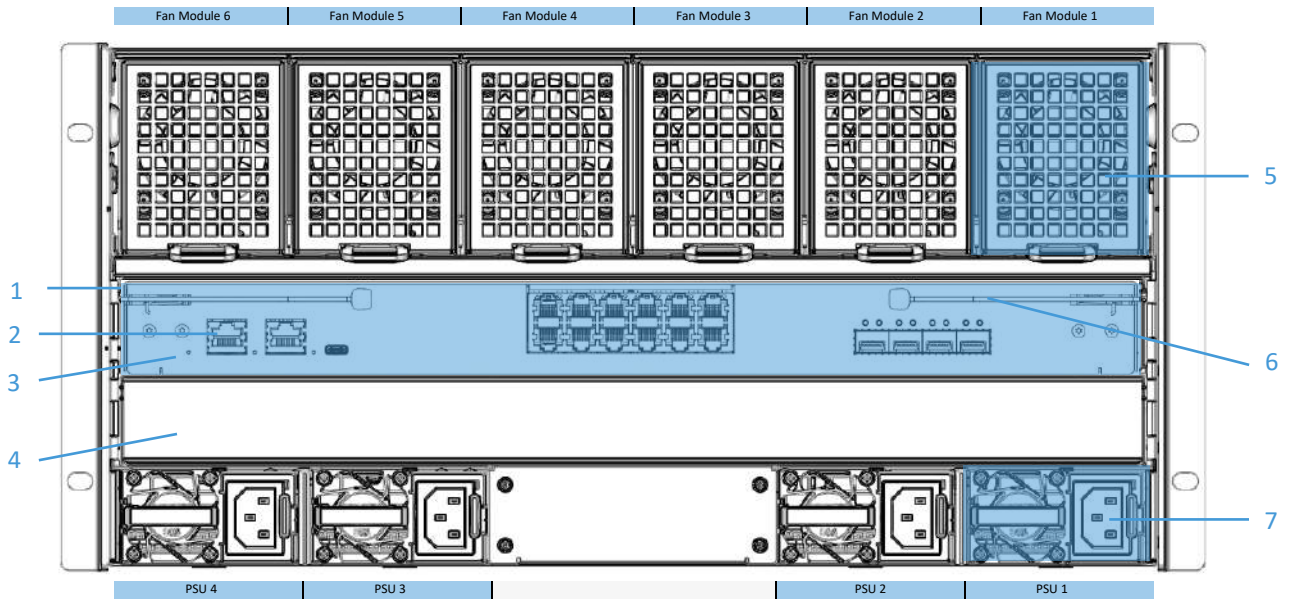


Figure 2 - CoreStation HX5 Enclosure rear view

1	Management controller module (IO Module 1)	Combined module for Network connectivity and System Management.
2	Management network port	Ethernet Connection used for communication with the system management console for all system management tasks.
3	Management Controller status indicator	This mirrors the enclosure front status indicator
4	Expansion module (IO Module 2)	For use with network expansion modules
5	Fan module	Six individual fan cooling modules, each contains two independent rotors such that a single rotor failure will not disrupt operations.
6	Data network ports	Network connections for the workstation nodes. The specific port configuration and capability depends on which Management module is fitted.
7	Power Supply Unit	Four power supply units with independent power connections

2.3 System Status Indicator

The enclosure front indicator and Management Controller rear system status indicators show the same state.

Colour and cadence	System State
Not illuminated	No power to the enclosure
Solid Amber	Management processor starting up
Solid Green	Powered on and healthy
Flashing Amber	Powered On, system error or enclosure health alert
Flashing Blue	Enclosure ID - The identification request has been enabled from the management console to signal to a technician that this Enclosure needs attention. This persists until the ID request has been cancelled.

2.4 Serial Console Port

The serial console port is intended for initial system configuration and is not required for normal operation. It is available whenever the system has power.

The following actions are available:

- Show system serial number, hostname and IP address
- Set to use DHCP or a static IP address
- Reset the Enclosure to factory settings, including default admin password

The serial console port is implemented as a USB type C connector supporting operation in both connector orientations with an internal USB-to-Serial converter which identifies as a standard USB CDC device and works with the drivers pre-installed in all common operating systems.

Connect to the UART port using a terminal emulator such as HyperTerminal or Putty with the following settings:

- 115,200 Baud Rate
- 8N1 - 8 Data bits, 1 stop bit, no parity.

2.5 Power Supplies

The system can be powered from One, Two, Three or Four power supplies and these can be populated in any order. Each power supply can be powered from a different voltage, phase or supply, but they should all have the same rating.



Figure 3 - CoreStation HX5 Power Supply Unit

Power supplies can be removed and inserted, and power feeds can be connected and removed whilst the system is running as long as sufficient power is always available. Depending on the power policy configured for the system, loss of a power supply may trigger actions such as powering-down some workstation nodes or reducing performance to maintain the configured level of redundancy.

The power supplies are used in rotation to share the loading and wear across all supplies and reduce the rate of failure whilst maintaining the highest operating efficiency, so at any moment the system power may be provided entirely from one supply or spread over all supplies.

Contact Amulet Hotkey support for detail of the power required for a specific configuration.

Available power supplies

Nominal Capacity	Maximum Heat Dissipation	Efficiency Standard	AC low-line range 100-127VAC 50/60Hz	AC high-line range 200-240VAC 50/60Hz	Input Connector
800W	3,003 BTU/hr	Titanium	800W output	800W output	IEC C14
1300W	4,875 BTU/hr	Titanium	1000W output	1300W output	IEC C14
2400W	8,184 BTU/hr	Titanium	1000W output	2400W output	IEC C20

2.6 PSU Indicator

Colour and cadence	Status
Off	No Inlet power to any PSU module
Solid Green	Normal operation
Blinking Green (Once per second)	This PSU is on standby and is not currently supplying power
Solid Amber	This PSU is unable to supply power either due to lack of inlet power or another failure.
Blinking amber (Once per second)	This PSU has a warning event, but is still operating
Flashing Green (twice per second)	PSU is performing firmware update

2.7 Cooling System

CoreStation HX5 uses front-to-back airflow provided by dual-rotor fans in the cooling module to keep the workstation nodes operating in a controlled temperature range. The enclosure is divided into six cooling channels, each of which correspond to a cooling module and the two node slots directly in front.

The cooling modules each contain two separate spinning fan rotors with independent power, control and monitoring circuitry for enhanced redundancy. Failure or degradation of one rotor will result in the remaining rotor increasing speed to compensate. In some cases, this will result in a reduction in overall performance within that cooling channel.

Each cooling module contains sprung flaps to prevent air re-circulation or bypass when only one of the two nodes is fitted to a cooling channel and the system can be operated indefinitely in this state, but it is recommended to fit node blanks to slots which are not in use.

All six cooling modules must be fitted to the enclosure as cooling channels which are not in use will run the fans slowly to provide cooling for the IO modules and internal circuitry.

The power supplies have their own cooling fans and draw cool air from the enclosure front panel under the nodes.

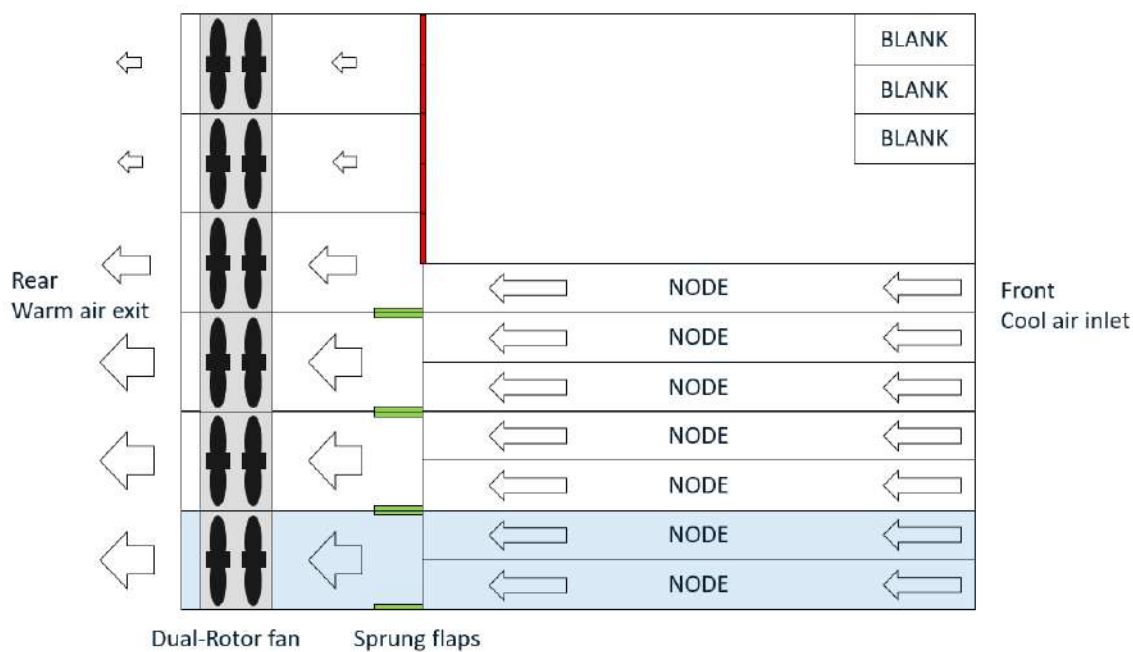


Figure 4 - CoreStation HX5 enclosure top-view cooling diagram

Cooling module indicator

This indicator is behind the fan exhaust grill on each fan module

Colour and cadence	Status
Off	No power is provided to the fan module
Solid Green	Normal Operation
Flashing Amber	This fan module is in a degraded health state or has lost communication with the management controller

3. Management and Network Modules

The combined Management and Network Controller module provides management and network connectivity for the whole system in a single module.

The Management Controller module must be present for the system to power up but can be removed and replaced without causing the system to power down. Whilst the Management Controller is not fitted, the fans will all run continuously at full speed to maintain component temperatures and no network connection will be available over network fabric 1A or fabric 1B. If there is a network path available over Fabric 2B using IO Module 2, then the Nodes will continue to operate normally. Once the Management Controller is re-fitted to IO Module 1, the network connectivity via Fabric 1A and 1B will be restored and the fans will reduce speed to match the thermal load.

3.1 Management module variants (IOM1)

IO Module 1 must be populated with a Management Controller for system operation.

Module	Management Storage	Management network	Data Network
N120	128GB	- Port 1 - 1Gb Ethernet - Port 2 - 1Gb Ethernet (Reserved for future use)	- Individual Ethernet connection direct to each node - Four 10G SFP uplinks with internal switch

3.2 Network module variants (IOM2)

IO Module 2 can be left blank or fitted with a network expansion module.

Module	Management processor	Management Storage	Management network	Data Network
Blank	None	None	None	None
N205	None	None	None	Individual Ethernet connection direct to each node

3.3 N120 I/O Module

The N120 provides the option to use either the individual network ports or the combined uplink ports for workstation data connections.

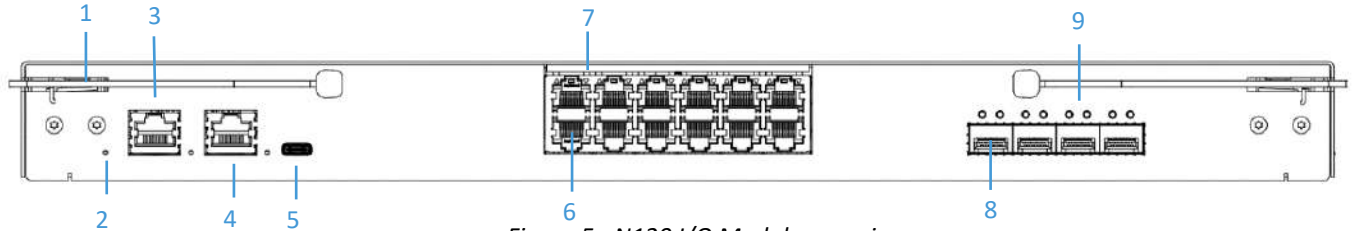


Figure 5 - N120 I/O Module rear view

1	Latch handle	Physical handle used to latch the module into the Enclosure.
2	Enclosure status indicator	Status indicator shows a summary of the system state and any serious health warnings which affect the Enclosure.
3	Management network port 1	Ethernet connection used for communication with the HX Management Console for all system management tasks.
4	Management network port 2	Reserved for future use
5	System rear serial console (USB-C)	Serial interface for initial system configuration and setup. Not required in general use.
6	Pass-Through network port	Individual network connections for the Workstation Nodes to provide all network traffic to and from the operating system.
7	Node identification indicator	Indicator to show the status of a workstation node
8	Switched network ports	Four network connections to provide combined, redundant network uplink for the workstation nodes.
9	Switched data network port indicators	Indicators to show link and activity

Node identification indicator

Used to indicate presence of a workstation node in this slot and to identify the network port associated to a specific node.

Colour and cadence	Status
Off	Slot empty
Solid Green	Workstation node present in this slot
Flashing Green (Once-per-second)	Node Identify - The identification request has been enabled from the management console to signal to a technician that this node needs attention.

Management network port indicator

The Management port uses a single indicator to indicate link and activity.

Colour and cadence	Status
Off	No link
Solid Green	1Gbit link, idle
Flashing Green	1Gbit link, activity
Solid Amber	100Mb link, idle
Flashing Amber	100Mb link, activity

Management network port specification

Network interface for all management traffic via browser and APIs.

Physical Interface	1000Base-T on 8P8C 'RJ45' connector
Supported link configs per port	Auto-negotiation 100Mbit/s or 1000Mit/s full-duplex only
Supported port configurations	Port 1 only, port 2 is reserved for future use
MAC Address	Amulet Hotkey MAC address range, starting 00:17:FD

3.4 N205 I/O Module

The N205 provides additional network connections to nodes which support redundant networking capability via fabric 2B. N205 must be installed in IO Module 2 and the enclosure must have an N120 Management Module fitted in IO Module 1. The N205 module does not provide Enclosure management capabilities, these are all provided using N120 in IO Module 1.

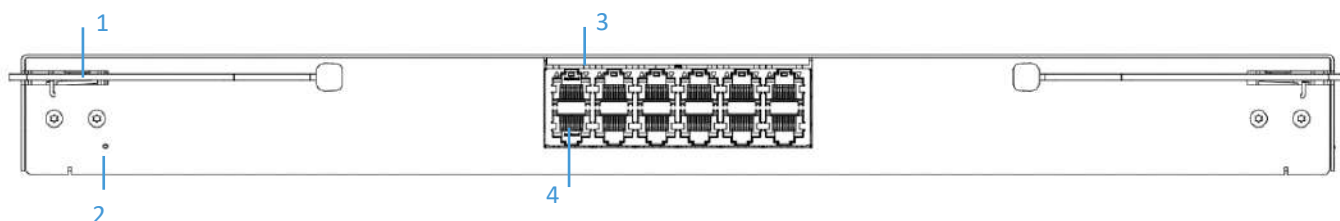


Figure 6 - N205 I/O Module rear view

1	Latch handle	Physical handle used to latch the module into the Enclosure.
2	Enclosure status indicator	Status indicator shows a summary of the system state and any serious health warnings which affect the Enclosure.
3	Pass-through data network port	Individual network connections for the Workstation Nodes to provide all network traffic to and from the operating system.
4	Node identification indicator	Indicator to show the status of a workstation node

Node identification indicator

Used to indicate presence of a workstation node in this slot and to identify the network port associated to a specific node.

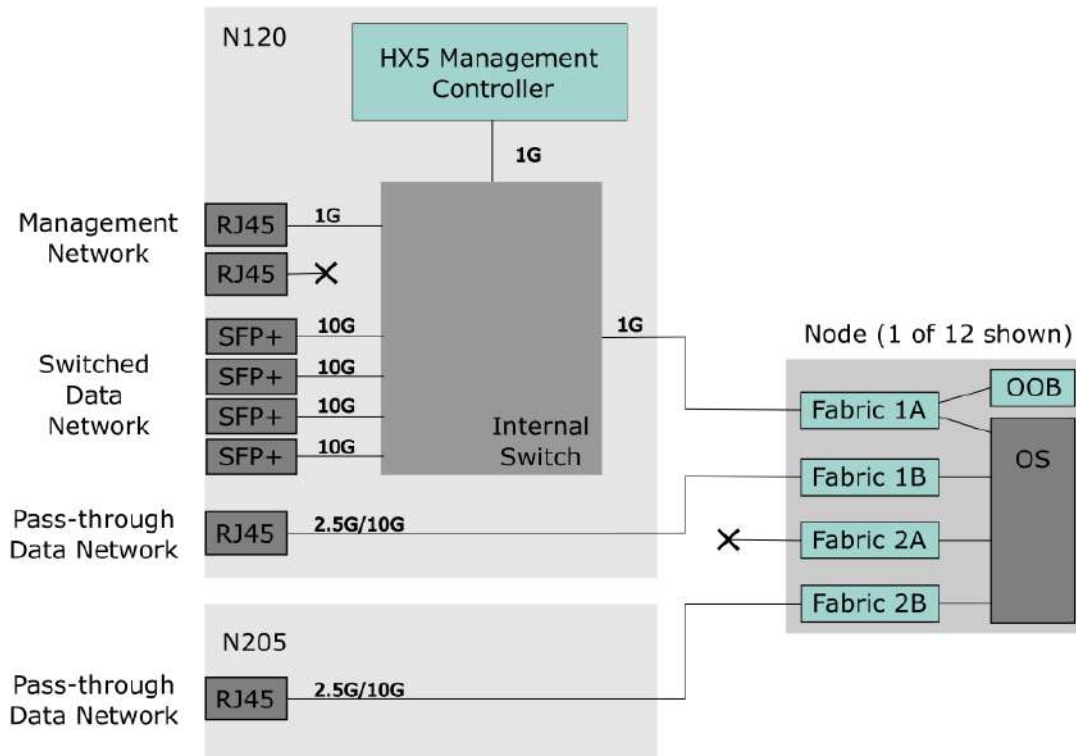
Colour and cadence	Status
Off	Slot empty
Solid Green	Workstation node present in this slot
Flashing Green (Once-per-second)	Node Identify - An identification request has been made from the management console to signal to a technician that this node needs attention.

3.5 System Network Topology

Each network fabric connects to a separate Network Interface Controllers (NIC) on the Node and these appear as separate Network interfaces to the Node Operating System. Multiple network Fabrics can be connected simultaneously to provide resilience, but these must be managed by the OS.

The Internal switch simply provides connectivity between the Node Operating System and the upstream network, it does not provide any additional network services such as DHCP, DNS or NAT.

Refer to HX Node user guide for details of the network controllers for each node type.



Interface	Internal connection	Capabilities	Functionality
Management ports (2)	Management controller via Internal switch	100/1000Base-T Ethernet	Enclosure Management
Data uplink ports (4)	Node Fabric 1A via Internal switch	10G SFP+ supporting DAC, Fiber and Copper modules	Combined uplink ports with link aggregation.
N120 Data passthrough ports (12)	Node Fabric 1B direct connection	100/1G/2.5G/10G Base-T Ethernet	Independent data connection for each workstation node. Port speed is based on the HX node capabilities: - HX2000 100M/1G/2.5G - HX3000 1G/2.5G/5G/10G
N205 Data passthrough ports (12)	Node Fabric 2B direct connection	100/1G/2.5G/10G Base-T Ethernet	Independent data connection for each workstation node. Port speed is based on the HX node capabilities: - HX2000 – No connection - HX3000 1G/2.5G/5G/10G

3.6 Switched Data network port specification

Network interface for all traffic to the workstation node.

Each of the four network ports connect to an internal switch which provides internal management services and configurable network routing to the workstation nodes.

Physical Interface	Four SFP+ modules supporting 10GbE network connections
Compatible SFP Modules	• 10G Direct-attach copper • 10G Copper Ethernet and Fiber modules • 1G Copper Ethernet and Fiber modules
Supported link speed	1Gbit/s or 10Gbit/s depending on SFP module fitted Full duplex only
Internal network interface to workstation nodes	1Gbit/s full duplex using Fabric 1A
MAC Address	Amulet Hotkey MAC address range, starting 00:17:FD.
Operating modes	• Disabled • Single Link Aggregation Group
Link Aggregation configuration (Fixed parameters)	• Active LAG using 802.3ad LACP over all four SFPs • LACP fast update rate • Valid with one, two, three or four active links • Hashing algorithm: Layer 2+3 source + destination
VLAN Configuration	Access port with without VLAN tagging. Flat network for all nodes.

3.7 Pass-Through Data network ports

Network interface for all traffic to the workstation node.

Each of the twelve network ports connect directly to a workstation node and carry all user traffic to that node. For further specifications, see the HX Node user manual

Physical Interface	N Base-T on 8P8C 'RJ45' connector • HX2000: up to 2.5GBase-T • HX3000: up to 10GBase-T
Supported link configs	Auto-negotiation 100Mbit/s, 1Gbit/s, 2.5Gbit/s, 5Gbit/s or 10Gbit/s full-duplex only
MAC Address	Amulet Hotkey MAC address range, starting 00:17:FD
HX Node Network Controller	See HX Node User Guide for further details

3.8 N120 Internal Network Topology

Internally, N120 uses multiple VLANs to separate management and data traffic. Fabric 1A carries both internal Management and external Data traffic between the internal switch and the Node and these are split before they leave the enclosure.

Network Setting	Description	Network Topology
Data Uplinks Disabled	- SFP Ports disabled - Fabric 1A - Internal Management only - Fabric 1B - Node OS data only - Fabric 1A can be disabled in the Node OS	
Data Uplinks Enabled	- SFP Ports enabled as single Link aggregation group with four members - Fabric 1A - Internal Management and Node OS data - Fabric 1B - Node OS data - Fabric 1A traffic separation using internal VLANs and traffic control rules - Internal Switch allows routing between nodes for OS data	

3.9 Management Controller network requirements

The Management Controller requires a set of network ports and services for correct operation.

Ports required

These ports must be open to bi-directional traffic to between the CoreStation Management port 1 and any user who needs to access the Management Controller.

Network Port	Protocol	Description	Requirement
80/tcp	http	Un-encrypted web traffic. Only used to initiate connections	Required for all Management functions
443/tcp	https	Encrypted web traffic. Used for all Management Controller browser sessions and API calls.	Required for all Management functions
8181/tcp	https	Encrypted traffic for Remote Console KVM sessions.	Required for Remote Console.

Network services required

These network services are required on the CoreStation Management port 1 for normal operation.

Service	Description	Required
DHCP	Provides IP address for Management Controller	Required unless using static IP on Management Controller
DNS	Provides network name resolution for network devices	Required unless using static IP on Management Controller
NTP	Provides accurate time updates for Management Controller. The NTP server can be specified on the config page. Inaccurate time/date can cause failures when validating website ssl/tls certificates. The default NTP server is pool.ntp.org.	Recommended

4. Hardware Installation and Setup

4.1 Rack mechanical requirements

CoreStation HX5 is designed to be mounted in a standard 19in data center Rack.

Service access to the system is from the front (Workstation nodes) and rear (Power Supplies, Fans and I/O module). There is no service access required from the top.

Enclosure airflow is front-to-back – cool air inlet at the front, warm air exhaust at the back.

All permanent cable connections are at the rear of the Enclosure.

Enclosure Dimensions

Rack height required (Ha)	5U (218mm / 8.58in)
Minimum width between rails (Wb)	447mm / 17.6in
Required depth across full width of rack (Db)	627mm / 24.7in
Depth including typical cable bend radius (Db+)	700mm / 27.6in
Required depth for removing rear modules without sliding Enclosure forward (De)	820mm / 32.3in
Front of rack protrusion (Df)	25mm / 1.0in

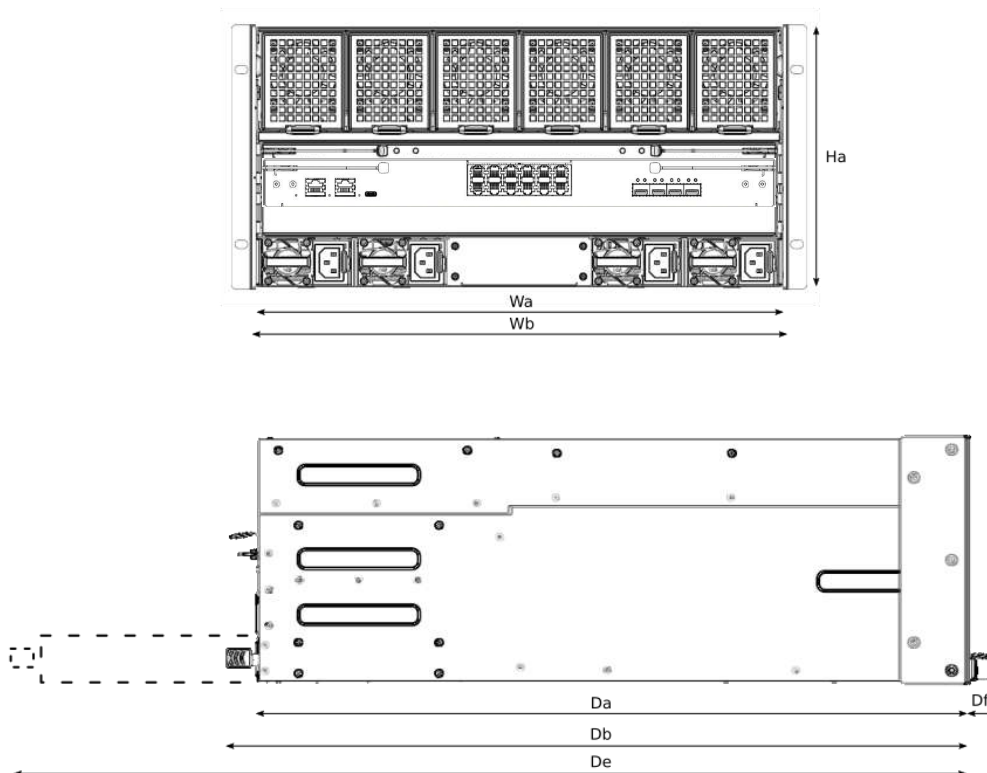


Figure 7 - CoreStation HX5 Enclosure Dimensions

4.2 Static adjustable rails for front-to-back mounting

These rails fit between the front and rear posts and provide a solid base to support the enclosure. These rails are required and are the only supported method for mounting the enclosure in a rack.

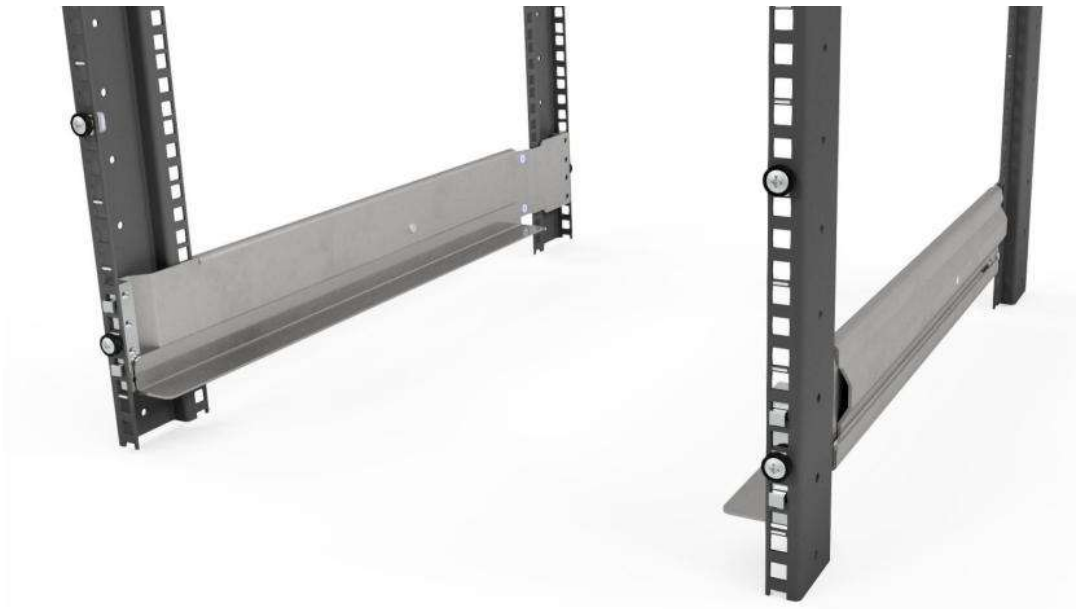
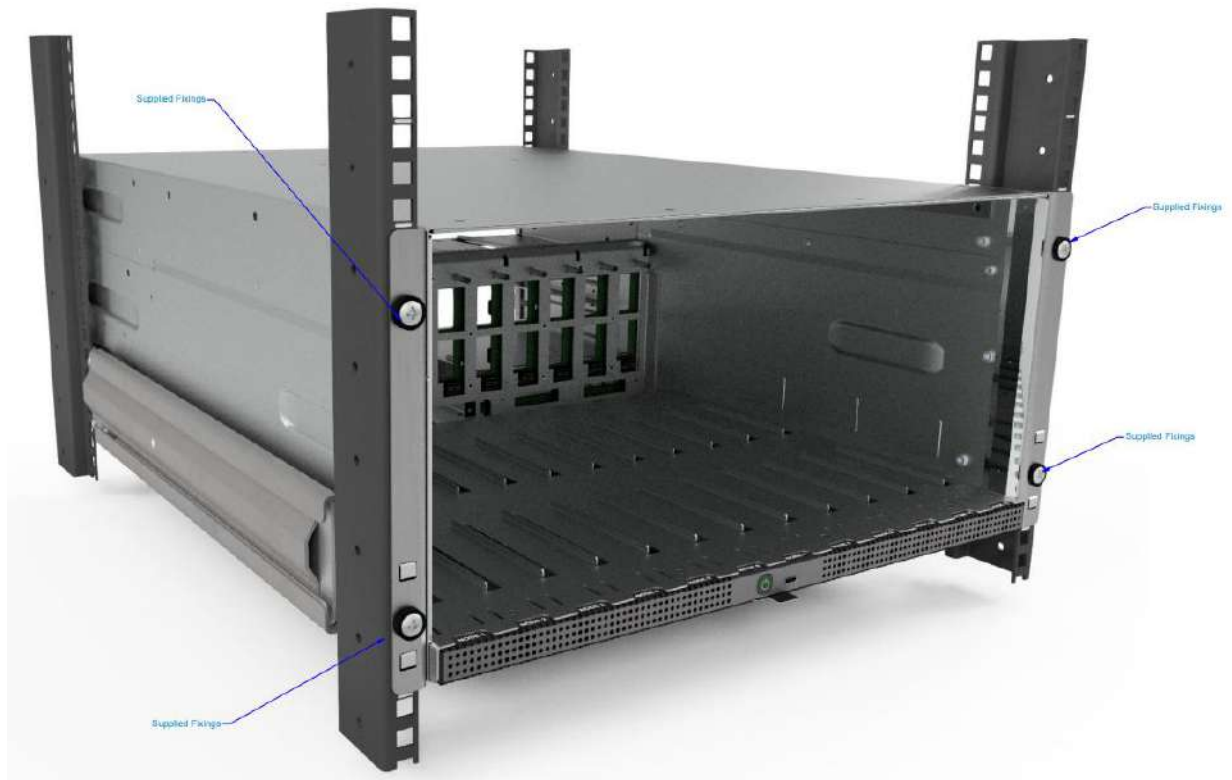


Figure 8 - HX5 Rackmount rail kit.

Rack type	Four-post racks with square holes only. Threaded racks are not supported. Two-post racks are not supported.
Mounting screw	M6x16 (supplied)
Minimum post spacing depth	600mm / 23.6in
Maximum post spacing depth	900mm / 35.4in

Rack mount installation process

1. Line up the rails so that the supports are at the bottom of the chosen 5U space
2. Extend the rails to match the inside faces of the rack posts
3. Locate the rail hooks in the rack holes to keep rails in position
4. Secure the rear of the rails using a pair of the supplied M6x16 screws with finishing washer
5. Slide the Enclosure into the rack and check it sits on the rails
6. Secure the Enclosure to the rails using four supplied M6 bolts with finishing washers



Precautions

- CoreStation HX5 system can weigh up to 80kg when fully loaded
- Either use appropriate data center lifting equipment or remove all the modules and workstation nodes prior to lifting the Enclosure into the rack.
- Two people are required to lift the empty enclosure if mechanical lifting equipment is not available.
- Module and Node retention mechanisms are designed for latching in the normal horizontal orientation and are not designed to allow the Enclosure to be significantly tilted during installation.

4.3 Ambient Operating Range

The system has an overall maximum ambient rating of 35°C and a safe continuous operating ambient based on the system configuration.

Recommended operating range	• ASHRAE Recommended • 18°C to 27°C • Up to 60% Relative Humidity • 5.5°C to 15°C dew point
Allowable operating range	• ASHRAE A2 • 10°C to 35°C • 20% to 80% Relative Humidity
Operating Altitude	• -50m to +3,000m (-160ft to +9,800ft)
Allowable range for storage and transport	• -20°C to 65°C (-4°F to 149°F) • 5% to 95% relative humidity, non-condensing • After storage or transport, ensure the system is allowed to reach the operating range and any moisture has evaporated before power-up

Ambient Thermal Tables

The maximum ambient temperature for continuous operation depends on the configuration of the system.

Each HX node has a valid range of operation, see the node user guide for details.

Contact Amulet Hotkey support for detailed analysis of ambient limits for a specific config.

4.4 Module Installation and Removal

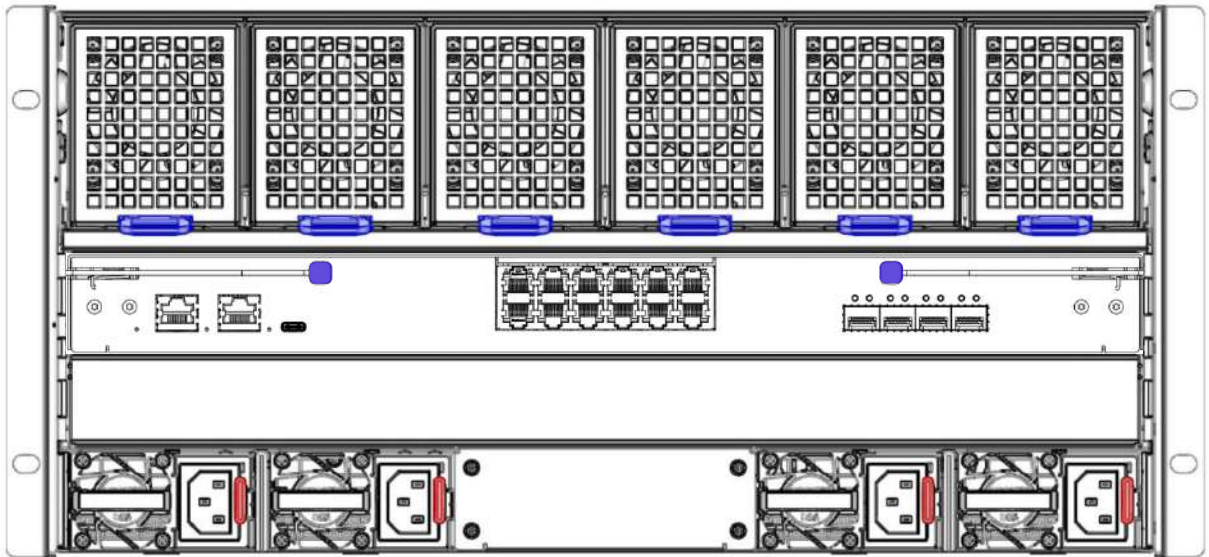


Figure 9 - CoreStation HX5 rear module latches

Module	To Insert	To Remove
Power Supply Unit	1. Line up with Enclosure opening 2. Push gently with little resistance, then firmly to mate the connector 3. Check the red handle has clicked into the Enclosure slots 4. Connect power inlet cable 5. The PSU should light the status indicator within two seconds	1. Disconnect power inlet cable 2. Wait five seconds to allow the fans to stop spinning 3. Press the red latch toward the fan 4. Pull the PSU out of from the Enclosure using the handle
I/O Module	1. Line up with Enclosure opening 2. Push gently until there is resistance 3. Push strongly until the rear face is flush with the Enclosure 4. Push the blue handles toward the Enclosure to engage the connectors and latch the module. The latch handles should touch the rear face of the I/O module when fully inserted 5. The I/O module should light the status indicator within two seconds	1. If possible, turn off the Enclosure and all services before removal 2. Pull the blue latch handles away from the Enclosure to unlatch and disengage the connectors 3. Pull the I/O module out of the Enclosure by approximately 50mm (2in) using the latch handles 4. Grasp the I/O module either at the sides or top/bottom with fingers and pull it completely out of the Enclosure.
Cooling Module	1. Line up with Enclosure opening with the blue latch handle at the bottom	1. If possible, turn off the nodes which are cooled by this fan module

	2. Push gently with little resistance, then firmly to mate the connector 3. Check the blue handle has clicked into the Enclosure slots 4. The fan module should spin up within two seconds.	2. Press the blue latch handle down and pull backwards to remove the module approximately 50mm (2in) from the Enclosure 3. Grasp the fan module at the sides or top/bottom with fingers and pull it completely out of the Enclosure. 4. If the nodes in this cooling channel are still operating, replace the fan module within 30 seconds to prevent thermal throttling
Workstation Node	1. Line up with Enclosure opening 2. Push gently with little resistance, then firmly to mate the connector 3. Check the blue handle has clicked into the Enclosure slot 4. The node should light the status indicator within two seconds	1. Turn off the node 2. Press the blue latch handle down and pull to remove the node approximately 50mm (2in) from the Enclosure 3. Grasp the node at the sides or top/bottom with fingers and pull it completely out of the Enclosure. 4. Take care with the rear of the node as the connectors are delicate and sensitive to electrostatic discharge (ESD)

4.5 Typical cable connections

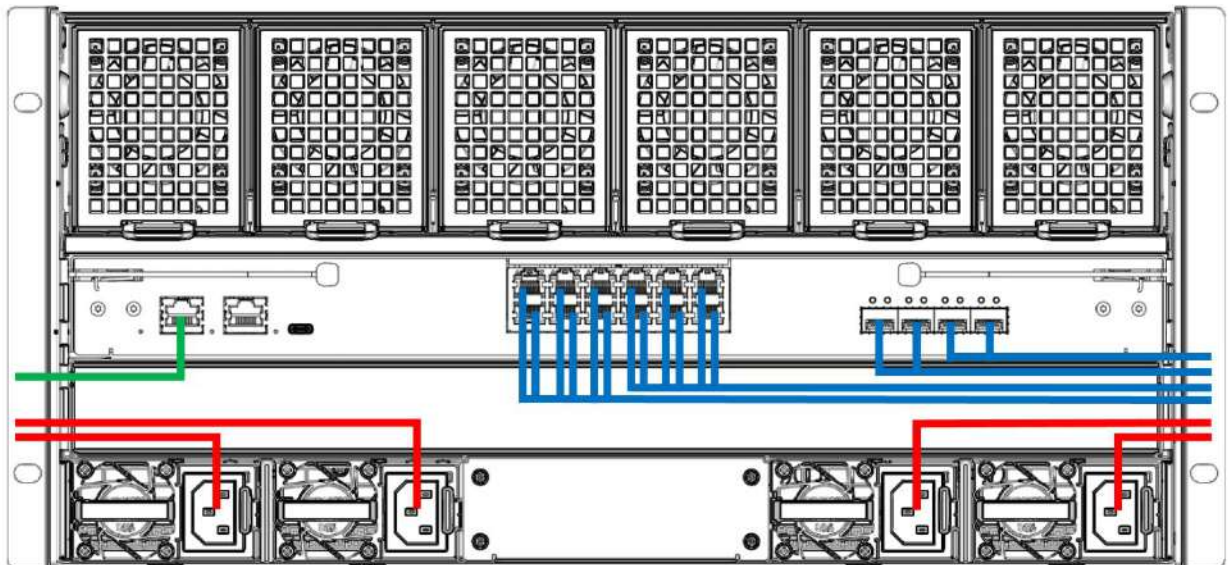


Figure 10 - Typical Cable connections

Red	Power
Green	Management Network
Blue	Data Network

5. Management Serial Port

The management serial port provides a simple method to read basic information about the enclosure, configure basic network settings and reset the enclosure. This is intended for initial setup and for recovery in the event of a lost password. The enclosure front serial port and N120 rear serial port are identical and either one can be used.

There is no authentication on the serial port and the functions are always available.

5.1 Serial Port Connection

Connect to the serial port using a standard USB cable (C to C or A to C) from a laptop or other PC and run a terminal emulator such as HyperTerminal or Putty with the following settings:

- 115,200 Baud Rate
- 8N1 - 8 Data bits, 1 stop bit, no parity.

Press <Enter> to confirm the port is active and a > prompt is visible

5.2 Serial Port commands and command syntax

Help – Show help messages and list of available commands

Info – Display status and network information about the enclosure

Net – Set the network to use DHCP or a static IP address

System reset – Reset the system to factory settings including default admin password

Command	Example syntax
help	<pre>> help Amulet Hotkey CoreStation N120 Management Controller Usage: help : show this screen info : display system and network details net : configure network fw : firmware update system : system reset For more details of each command type <command> help</pre>
info	<pre>> info Amulet Hotkey CoreStation N120 Management Controller Hostname: CSHX-Test-1 Serial number: 30032-0005 Firmware version: 2025.06.1 from A Date/Time: 2025-03-13 16:46:51Z CMC MAC Address: 00:17:FD:01:22:34 Network Address: 192.168.50.22 Netmask: 255.255.255.0 Gateway: 192.168.50.254 DNS: 192.168.200.10</pre>

	Network mode: DHCP
net	<pre>> net static 192.168.1.100 255.255.255.0 192.168.1.254 192.168.200.10 Set Corestation Management Controller network to the following static ip configuration? Network Address: 192.168.1.100 Netmask: 255.255.255.0 Gateway: 192.168.1.254 DNS: 192.168.200.10 (yes/no) >yes Done > net dhcp Set Corestation Management Controller network to DHCP? (yes/no) >yes Done</pre>
system reboot	<pre>> system reboot About to reboot Corestation Management Controller... Continue (yes/no) > yes</pre>
system reset	<pre>> system reset CAUTION: This operation will reset ALL configuration, passwords and certificate from the Corestation Management Controller. Node OS will not be affected ** THIS ACTION IS IRREVERSIBLE ** Are you sure you want to proceed? (yes/no)>yes Performing factory reset.....done</pre>
system format	For use in firmware recovery under guidance from Amulet Hotkey support
fw	

6. Security Features and Best Practice Deployment

Enterprise networks and deployments will vary, but CoreStation HX is designed around a set of assumptions and expectations for the environment in which it will be used. If the system will be used outside these best practice guidelines, please discuss with Amulet Hotkey support to understand if there are any additional limitations or risks which may be exposed.

6.1 Best Practice for System Deployment

Recommendation	Potential ways to implement	How this helps
Restrict access to management network and don't expose directly to the internet	- Firewalls - Network segregation using VLANs and subnets - Physically separate networks - Virtual Private Networks (VPN)	- Reduces the visibility of the management interface to attackers or compromised devices - Reduces exposure of management interface - Makes it simpler to isolate traffic
Only use encrypted methods to communicate with the management controller (HTTPS)	- Supported browser with HTTPS support - Corporate HTTPS certificate	- Prevents other devices on the network seeing the content of the session traffic - Avoids users bypassing warning messages
Prevent unknown devices connecting to open network ports	MAC address allow-list on the top-of-rack switch	- Prevents unknown devices accessing or seeing traffic on the management network. - Most interesting traffic is encrypted when using HTTPS, but basic network operations such as DHCP, DNS and ARP still expose a lot of information.
Restrict physical access to the data center room, rack and system	- Physical access control system (e.g. swipe card) - Lockable rack doors	- Reduces risk of physical-level attacks by malicious staff - Reduces risk of accidental operations on the wrong device
Secure the enclosure into the rack using the rack support bracket and fit all the rack nuts	- Use supplied mounting rails - Use rack-specific fixings	- Reduces risk of damage to other devices in the rack - Reduces risk of enclosure movement when inserting or removing modules
Stay up to date with the latest system firmware and receive notifications when new firmware is released	- Sign up to Amulet Hotkey CoreStation email alerts - Regularly review the Amulet Hotkey website	- Make sure the system is running the latest security patches and fixes - Avoid exposure to known vulnerabilities

6.2 Best Practice for Management configuration

Recommendation	How this helps
Use a corporate certificate generated by the company certificate authority.	- Removes the browser warning for self-signed certificates and the potential to normalise user behaviour to dismiss warnings. - Allows IT admins to use a higher level of security setting on their browser
Provide each user with their own login account with a strong password	- Enables use of strong, unique passwords - Avoids sharing passwords between multiple users and the temptation to use weak or common passwords - Associate activity of a user with a specific person when auditing system logs
Restrict each user to the level of access they require using role-based permissions	- Reduces the risk of accidental actions the user did not expect to perform - Restricts access to confidential user data and desktop sessions - Reduces the impact if a user account is compromised
Change the default password on the built-in admin account or disable the account	- The default password is unique to each unit, but can be seen by multiple people involved in the unboxing and install process - The admin account has full access to the system and all features, so could have a high impact if it is compromised
Regularly review the system logs to look for unusual login patterns	- Highlights login attempts from unexpected network locations (other countries, non-user devices) - Shows attempts to access the system without valid credentials
Disable Special Access Features	Avoids opening network ports for services which are not running

6.3 Best Practice for Workstation Node configuration

Recommendation	How this helps
Enable Secure Boot with a corporate PKI	Allows the nodes to boot only from validated boot media and installers
Enable full-disk encryption	- Reduces risk of sensitive data loss in the event of theft or accidental disposal - Reduces risk of data exposure when booting from another source
Stay up to date with the latest baseline driver pack	- Make sure the system is running the latest security patches and fixes - Avoid exposure to known vulnerabilities
Install the CoreStation agent on the node	- Provides rich information display on the Management Console - Provides further telemetry and monitoring
Disable Network and USB boot methods unless required	Prevents booting from unexpected sources due to misconfiguration or errors – e.g. plugging USB memory device into the wrong machine or configuring a PXE boot server on the network.

7. Specifications and Compliance

7.1 Dimensions

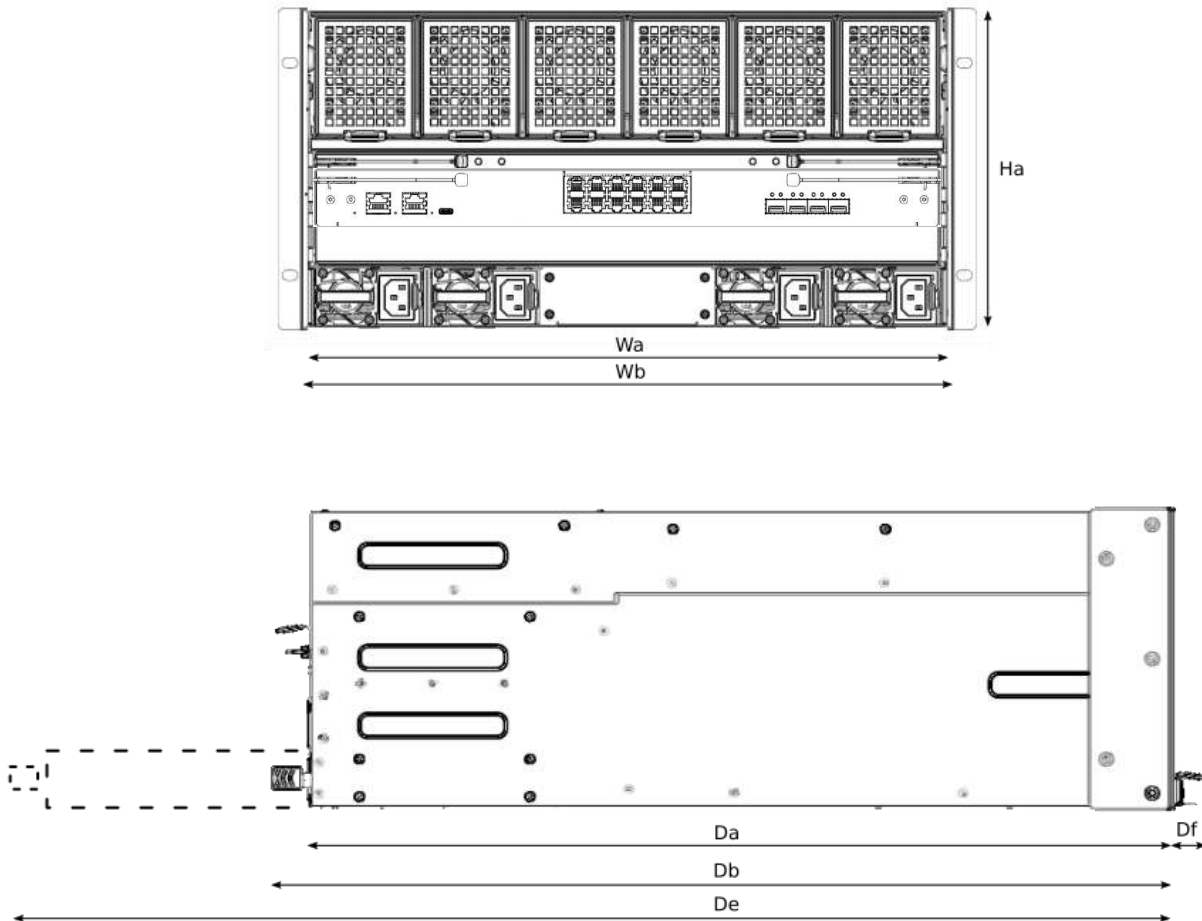


Figure 11 - CoreStation HX enclosure dimensions

Symbol	Description	Measurement
Da	Depth of system enclosure	602mm / 23.7in
Db	Depth to furthest point (PSU handles)	627mm / 24.7in
Db+	Depth including typical cable bend radius	700mm / 27.6in
De	Depth required to remove modules in situ	820mm / 32.3in
Df	Protrusion from front of rack	24.9mm / 0.98in
Ha	Height of system enclosure	218mm / 8.58in Fits within 5 rack units
Wa	Width of system enclosure	441mm / 17.4in
Wb	Width of enclosure to fit within rack posts	447mm / 17.6in

7.2 Electrical Specifications

System batteries

Used to maintain real-time clock when module or enclosure is not powered

Battery	Location and Purpose	Chemistry	Specification
Node RTC Battery	Battery holder on node carrier board. Maintains Node real-time clock when removed from Enclosure.	Lithium Manganese dioxide. Primary cell, not rechargeable.	CR2032 coin-cell battery. 20 mm diameter, 3.2 mm height Approx. 220 mAh capacity User-replaceable.
I/O Module RTC Battery	Battery holder on IO module board. Maintains Management Controller real-time clock when removed from Enclosure.		

7.3 Weights

Empty enclosure: 12.2 kg (26.9 lbs)

Enclosure with four PSUs, IO Module and cooling modules: 23.4 kg (51.6 lbs)

Fully populated system: 59.4 kg (131 lbs)

Fully populated shipping weight: 72.0kg (159 lbs)



Resources

<https://amulethotkey.com>

EMEA Support

+44(0)20 7960 2400

eurosupport@amulethotkey.com

North America Support

+1(212)269 9300

ussupport@amulethotkey.com

casupport@amulethotkey.com

Asia Pacific Support

apsupport@amulethotkey.com

Latin America Support

latamsupport@amulethotkey.com