AMULET HOTKEY

UM

Amulet Hotkey CoreStation HX5

User Manual

Contents

Version 1.4 - November 2025

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 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

Enclosure and services

System Front View

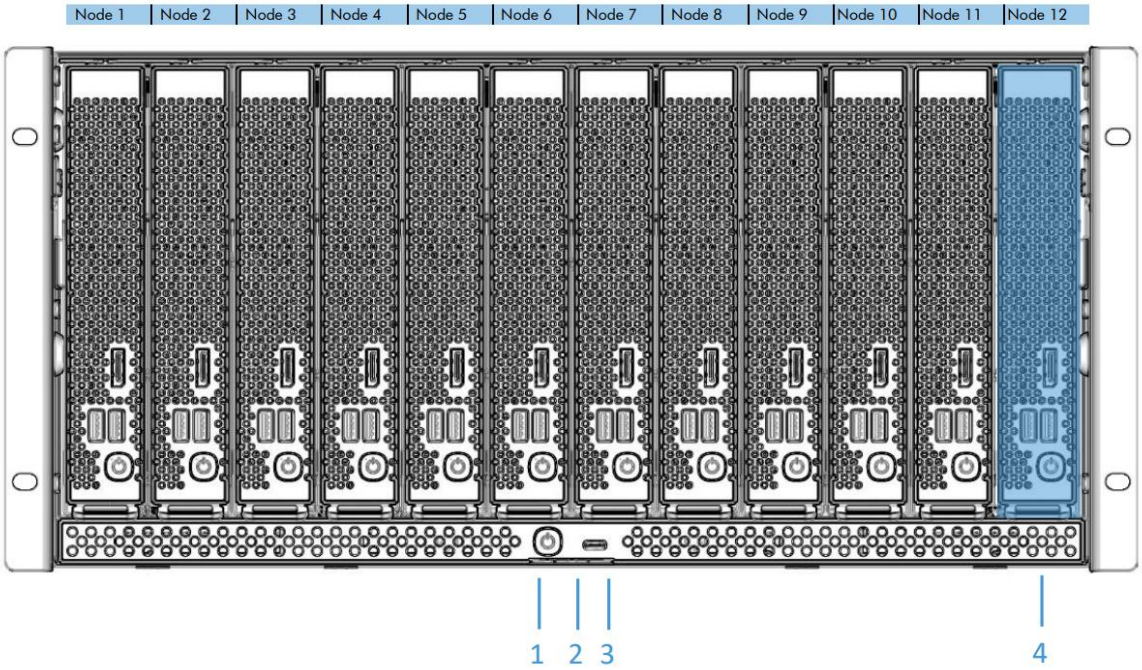


Figure 1 - CoreStation HX5 Enclosure front view

1	Enclosure power button and 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.

System Rear View

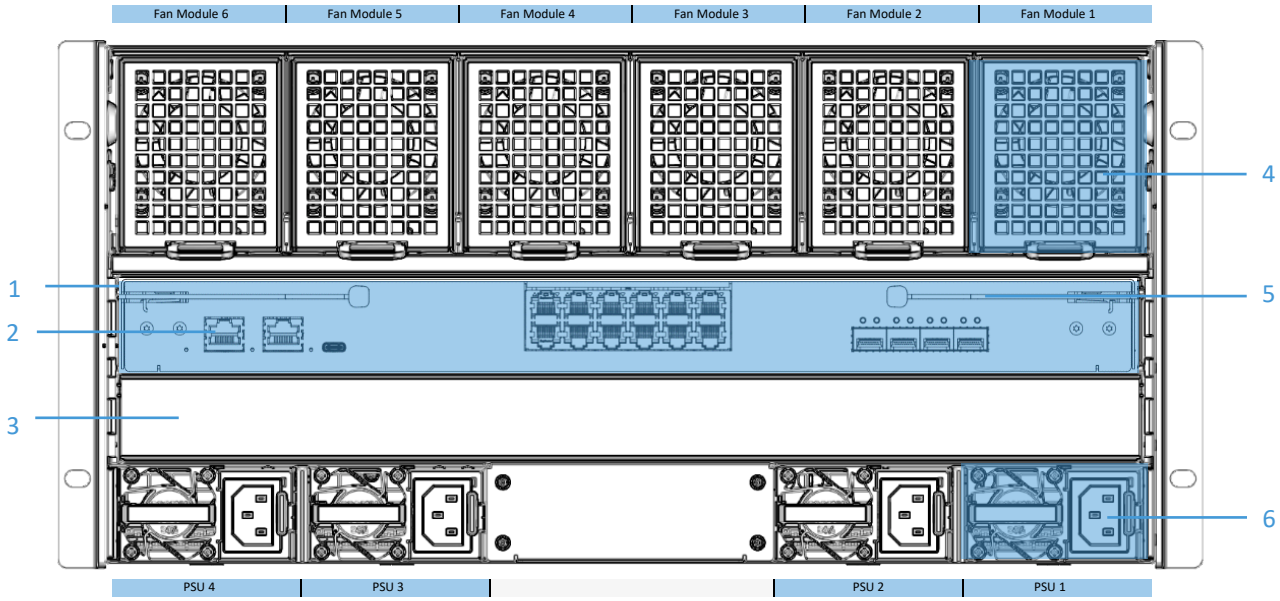


Figure 2 - CoreStation HX5 Enclosure rear view

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 Expansion module (IO Module 2)	Reserved for future use.
4 Fan module	Six individual fan cooling modules which are dedicated to the two slots in in their cooling channel. Each fan module contains two independent rotors such that a single rotor failure will not disrupt operations.
5 Data network ports	Network connections for the workstation nodes. The specific port configuration and capability depends on which Management module is fitted.
6 Power Supply Unit	Four power supply units which work together to power the system. The power supplies can be removed and inserted whilst the system is operating if sufficient power is still available for the current configuration.

System Status Indicator

Both front and 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 heath 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.

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.

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.

Refer to the CoreStation HX Power Estimation tool 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
2000W	6,824 BTU/hr	Titanium	1000W output	2000W output	IEC C14

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

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. Consult the CoreStation HX5 power and cooling guide for details.

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.

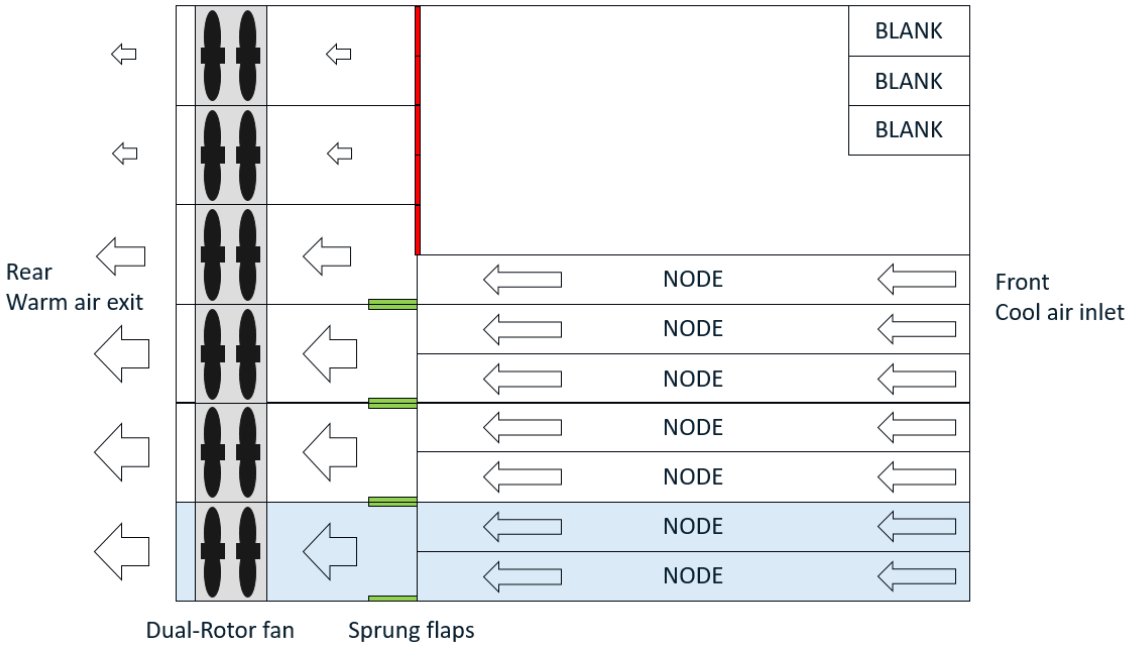


Figure 4 - CoreStation HX5 Cooling diagram

Cooling module indicator

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

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 module is not fitted, the fans will all run continuously at full speed and the workstation nodes have no network connection.

Once the module is re-fitted, the network connectivity should re-establish and the Operating System on the workstation nodes will not be affected.

Management module variants

Controller	Management processor	Management Storage	Management network	Data Network
N120	ARM Cortex A53 Quad Core	128GB	Dual 1G Ethernet	• Individual Ethernet connection direct to each node • Four 10G SFP uplinks with internal switch

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.

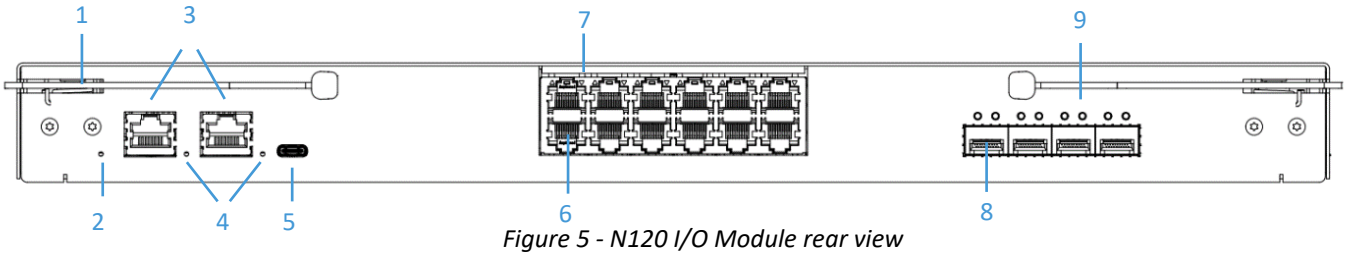


Figure 5 - N120 I/O Module rear view

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 ports	Two Ethernet connections used for communication with the system management console for all system management tasks.
4	Management network port indicators	Combined indicators to show link and activity
5	System rear serial console (USB-C)	Serial interface for initial system configuration and setup. Not required in general use.
6	Individual data 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	Combined data network ports	Four network connections to provide combined, redundant network uplink for the workstation nodes.
9	Combined 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 identity 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 ID - The identification request has been enabled from the management console to signal to a technician that this node needs attention. This persists until the ID request has been cancelled.

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

Two network interfaces 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
Network Phy	Microchip LAN8814

Combined 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 (from 2025.12 firmware release).

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
MAC Address	Amulet Hotkey MAC address range, starting 00:17:FD
Internal Switch	Microchip LAN9698
Operating modes	• Disabled • Link Aggregation Group with all four links (Planned for 2025.12 firmware release)

Individual 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.

Physical Interface	2.5GBase-T on 8P8C ‘RJ45’ connector
Supported link configs	Auto-negotiation 100Mbit/s, 1Gbit/s or 2.5Gbit/s full-duplex only
MAC Address	Amulet Hotkey MAC address range, starting 00:17:FD
Network Controller	Intel i226-LM

Hardware Installation and Setup

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.

All permanent cable connections are to/from 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
Required depth for removing rear modules without sliding Enclosure forward (De)	820mm / 32.3in
Front of rack protrusion (Df)	25mm / 1.0in

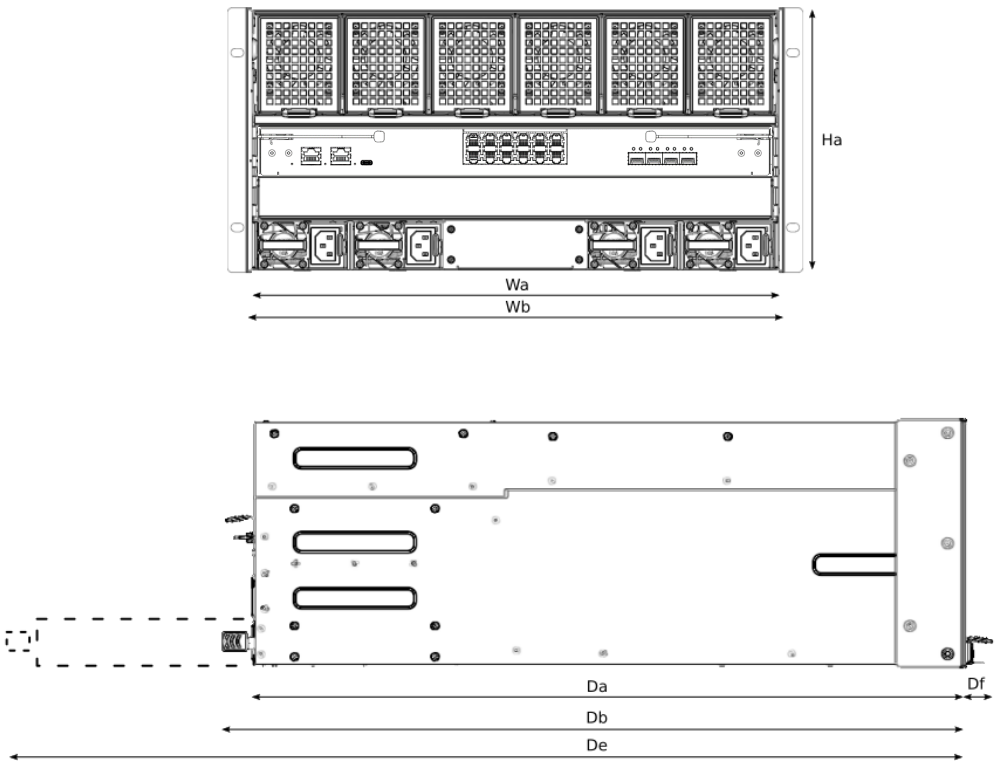


Figure 6 - CoreStation HX5 Enclosure Dimensions

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.

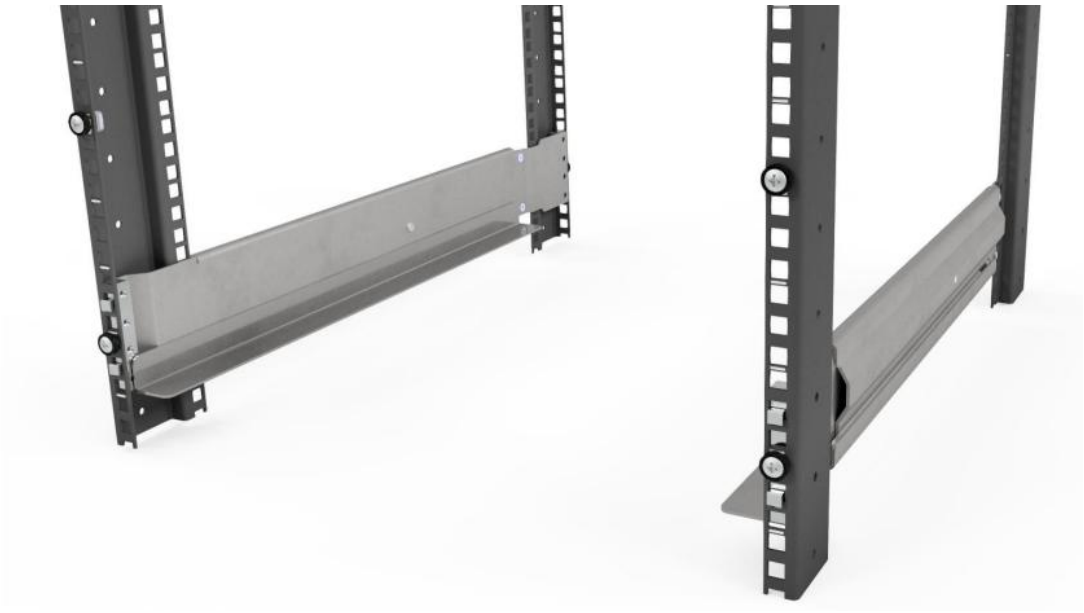
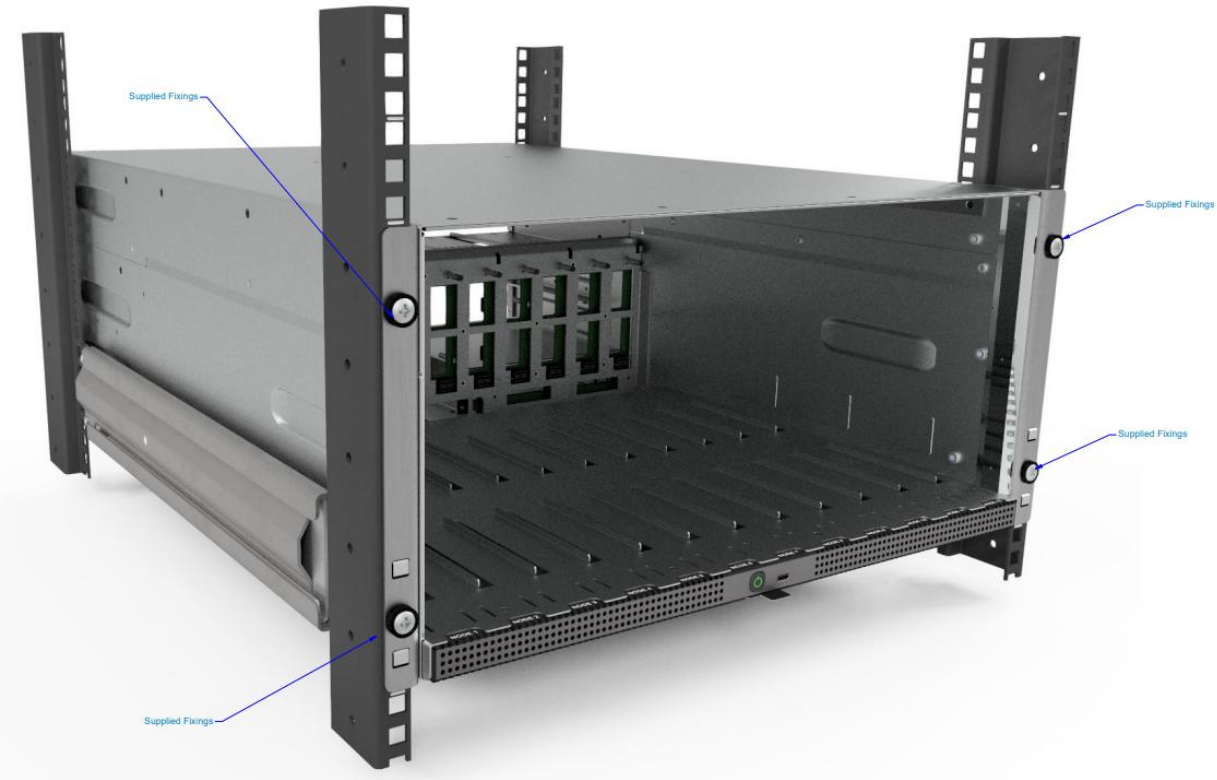


Figure 7 - HX5 Rackmount rail kit.

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.

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. The table below is based on a cooling channel using two identical workstation nodes.

Short-term operation above these limits will cause temporary performance throttling and higher fan speeds, but the system will continue to operate. Long-term use above these limits may result in premature failures in nodes and fans.

See the CoreStation HX Power Estimation tool for detailed analysis of ambient limits for a specific config.

Node CPU TDP	Up to 28W	Up to 45W	Up to 65W
Up to 27°C Ambient	Standard Heatsink	Standard Heatsink	Standard Heatsink
Up to 30°C Ambient	Standard Heatsink	Standard Heatsink	Not Supported
Up to 35°C Ambient	Standard Heatsink	Standard Heatsink	Not Supported

Module Installation and Removal

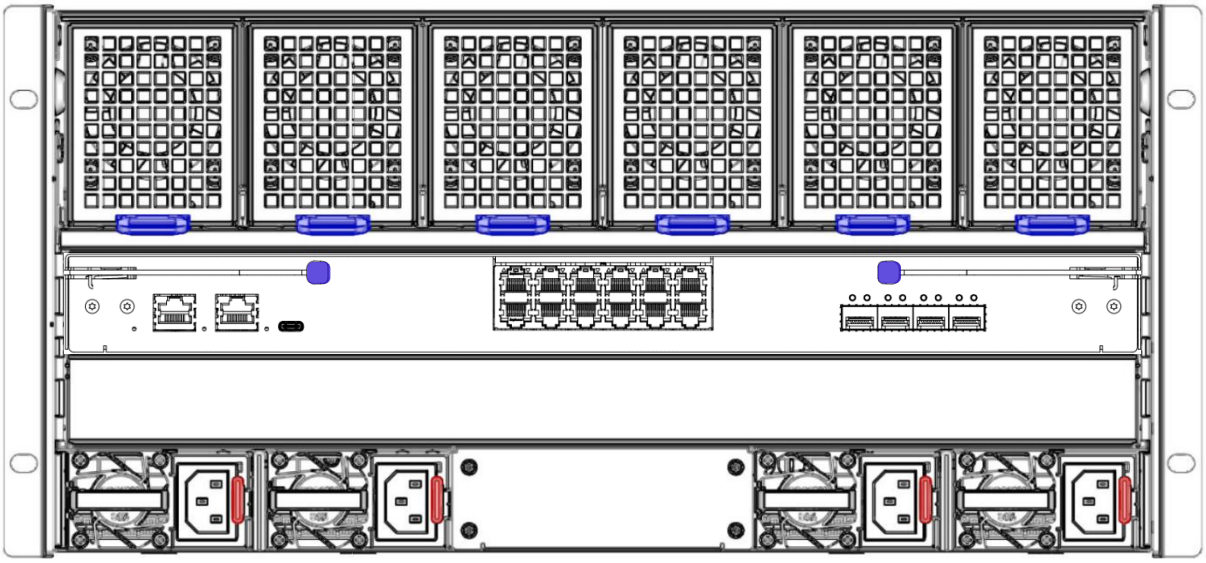


Figure 8 - CoreStation HX5 rear module latches

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	**The I/O Modules should be inserted before the nodes when possible.** 1. Line up with Enclosure opening 2. Push gently until there is resistance 3. Push strongly to 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 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.	1. If possible, turn off the nodes which are cooled by this fan module 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)

Typical cable connections

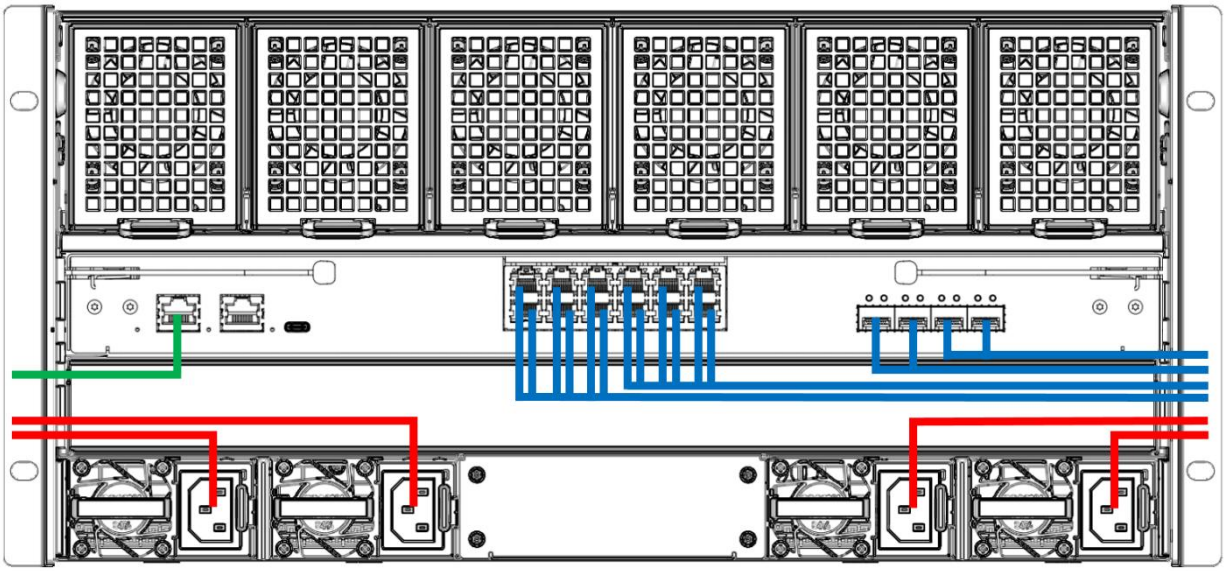


Figure 9 - Typical Cable connections

Red	Power
Green	Management Network
Blue	Data Network

Management Console - Status and Information

Management System Overview

The CoreStation HX Management Console is a system management platform which runs on the system using a dedicated ARM CPU. This platform provides the following services:

- Closed-loop thermal control using fans and performance throttling
- Node power control based on available power
- System health summary with detail of warnings and errors
- Detailed system telemetry for power, temperature and system load
- Admin control for power, settings and performance for each workstation node
- Out-of-band KVM access to the desktop of each workstation node, including BIOS and early boot (Planned for 2025.12 firmware release).

Interfaces for Managing CoreStation HX

The Management Console provides access and notifications via the following methods

Access method	Intended Use	Features Available
Web Browser	• Interactive users for day-to-day management	All management features
Serial Port	• Initial setup • Recovery and Erase	• Basic system info • Management network configuration • System reset
REST API	• API for integration with other systems	Most management features, excluding: • Firmware update • Log bundle export

Key components of the management system

The CoreStation HX Management Controller operates as one system, but is made up from several distinct hardware and software components

Component	Location	Description	Functionality
CoreStation Management Controller	HX5 I/O Module	Amulet Hotkey management software platform running on an embedded Linux-based Operating System, powered by an embedded ARM-based processor.	• Management Console • APIs • Communication with other system components • Power and cooling control • Maintains system status database • Gathers system telemetry
CoreStation Node Management Controller	Node system board	Amulet Hotkey management software running on an embedded Real-Time Operating System, powered by an embedded ARM-based processor.	• Node CPU power control • Node status and sensor monitoring • Node BIOS interaction
CoreStation Agent	Running on Node OS	Amulet Hotkey agent software running on the Workstation OS to report dynamic details.	• OS State reporting • Network connectivity • IP Address and hostname • Driver versions

Accessing the Management Console using web browser

The Management Console can be accessed over HTTPS using the system's assigned IP address or hostname (If DNS name resolution service is running on the network).

First find the address of the system using the serial port or DHCP log for the network. The network administrator will be able to advise how to use the DHCP logs.

The Management Console is based on responsive web technologies and will attempt to display information in the most suitable way for a wide variety of display resolutions in both portrait and landscape orientation. It is tested on a variety of browsers and fully supported on the following:

Browser	Platform
Microsoft Edge	Windows 11 Pro
Google Chrome	Windows 11 Pro Android 13 and later
Apple Safari	iOS 18 and later

Lookup system address using the serial port

The management controller will default to using DHCP to acquire an IP address and on first boot will request an IP address from the DHCP server on the network.

If the DHCP server does not respond, it will re-try the DHCP request every 60 seconds until an address is granted successfully, or the serial port is used to set a static IP address.

The default management system host name is based on the serial number of the management controller and is printed on a label on the IO Module but can be changed later.

Management Console Login page

Point the web browser to the IP address or hostname of the system to see the login page.

The Management Console uses HTTPS by default and will re-direct all HTTP access to the HTTPS version of the login page.

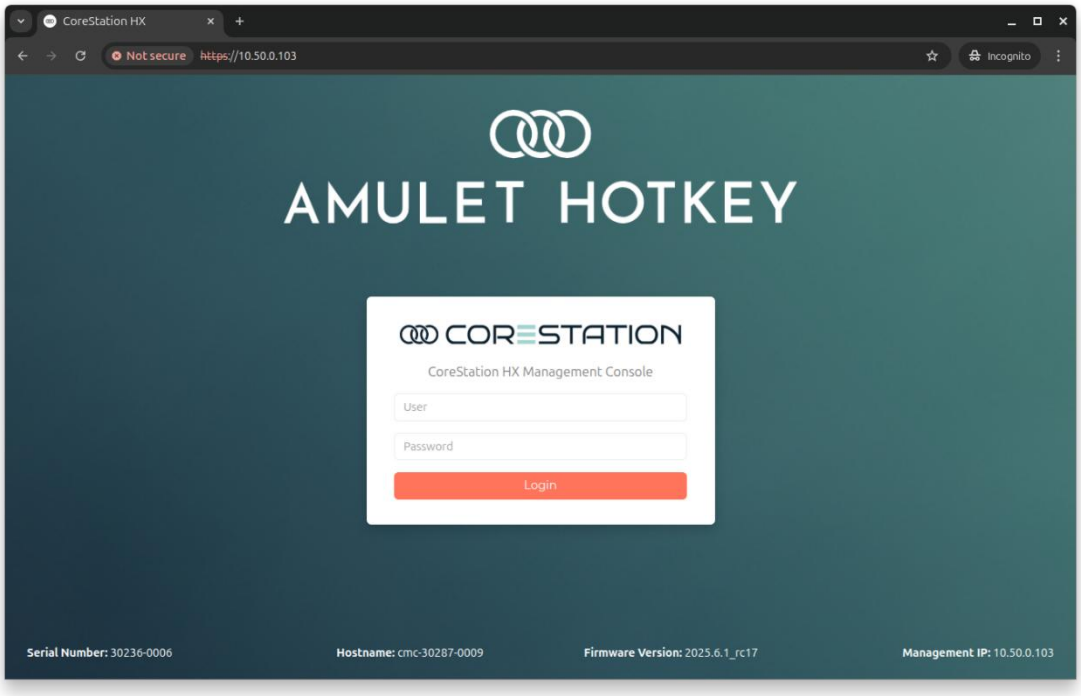


Figure 10 - Management Console Login Screen

HTTPS Self-signed certificate

The management console ships with a self-signed HTTPS TLS/SSL certificate issued by Amulet Hotkey which is used to encrypt the traffic over the management interface. As part of the initial setup and configuration, this should be replaced with a company-signed certificate signed by a corporate CA certificate authority.

For the initial login using the self-signed certificate, the browser will generate a warning that the site is not secure. The details of the self-signed certificate can be viewed in the page details (typically next to the address bar) to confirm the reason for the warning. The user who performs the initial setup will need sufficient access to dismiss the browser warning and continue to load the page.

Default login credentials

The system ships with a unique default login but should not be treated as secure since it is printed on the management controller and is visible to anyone who has handled the system. The admin password should be changed as soon as is practical.

Following a system reset, these default credentials will be re-instated, so they should not be discarded or removed from the system. Contact support if these credentials are lost.

username: *admin*

password: *Unique password for each system from label on IO Module*

Enter these default credentials to login to the system for the first time.

System Dashboard

After successful login, the users are shown the System Dashboard page. This provides a summary of the system information, component health and shows details of the modules and nodes currently fitted.

The image on the left of the page shows a representative image of the system based on the current hardware configuration. Clicking on any system component leads to a page with more specific information on that component.

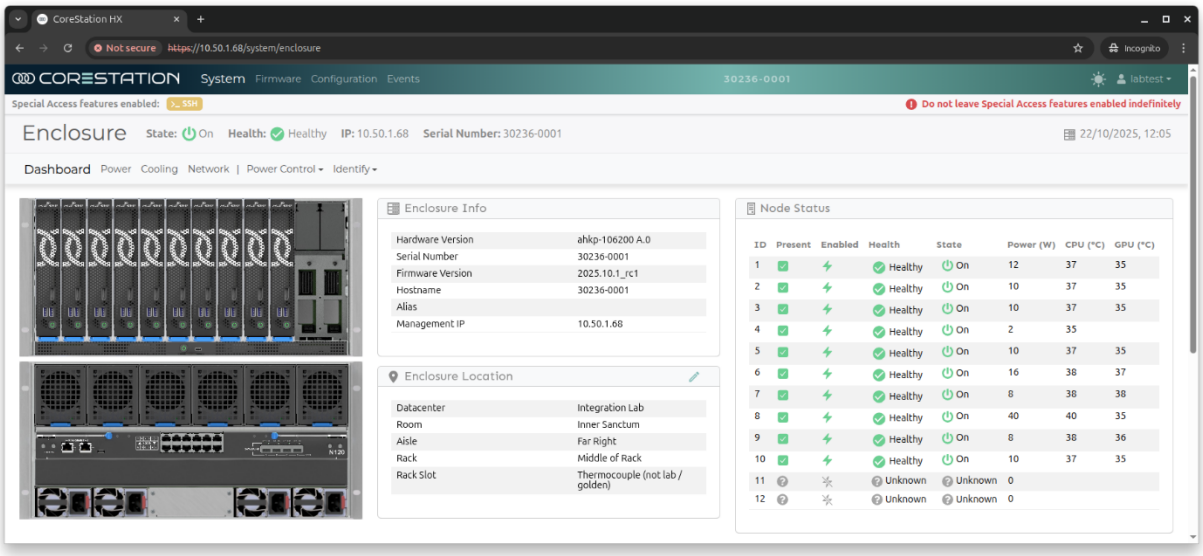


Figure 11 - Management Console System Dashboard

Main Page Items	Description
Notification Bar	Shows critical messages such as firmware update progress. These notifications are visible to all users and shown on every page.
State	Overall System Power State: **On** - Main power enabled and operational **Standby** - Management controller is operational, but all workstation nodes are turned off. All power can be safely removed from the system in this state. The system will automatically enter this state if all nodes are turned off. **Restarting** - The management controller is about to restart due to a configuration change or firmware update.
Health	Overall system health summary: **Healthy** - System and all components are operating normally **Warning** - At least one component has a minor issue which is reducing functionality or performance or may become an issue in the near future. **Error** - At least one component has a serious issue which is preventing normal operation or significantly impacting performance
System Image	Images of the system showing the components currently fitted. • Hover over any component for a summary • Click on any component to see more details
Enclosure Info	Static information about this system
Enclosure Location	Details about the location of this specific system. These can be edited using the pencil icon.
Node Status	For each node, provides a summary of the node status: • Present - Is a node fitted in this slot • Enabled: **Enabled** - This node can power up and operate normally **Disabled** - This node cannot operate due to an Enclosure restriction, e.g. insufficient power • Health - Summary of health status for this node **Healthy** - Operating Normally **Warning** - Minor issue **Error** - Major issue • State - Current node power state **On** - Powered on and operating **Standby** - Powered down • Power (W) – Live power draw for this node • CPU (°C) – Live temperature of the CPU package for this node • GPU (°C) – Live temperature of the GPU for this node

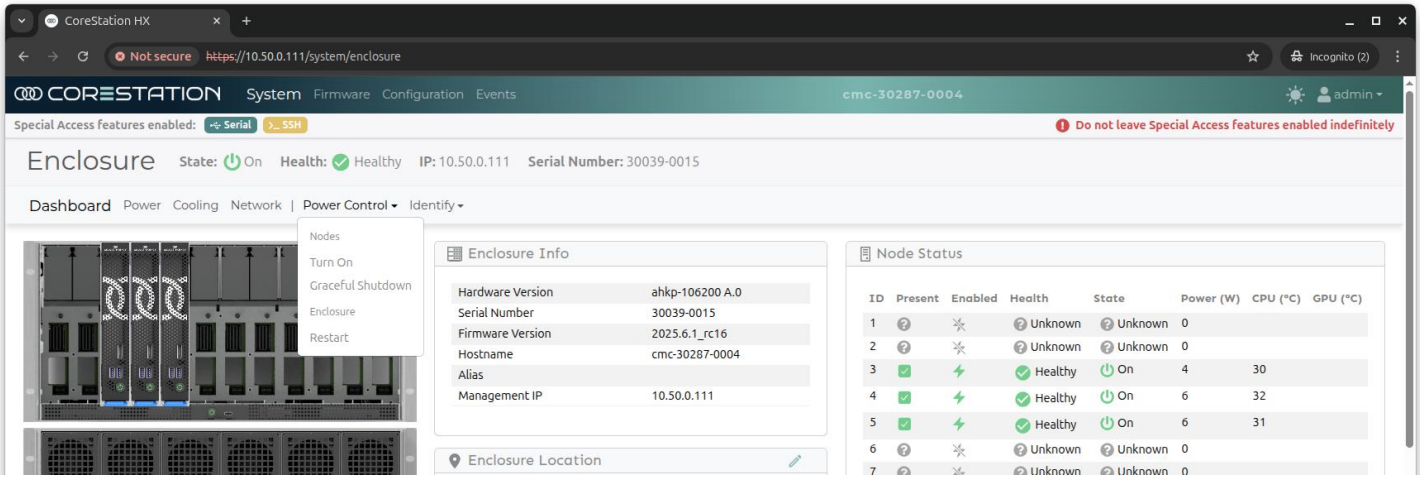


Figure 12 - Dashboard Power Actions

Components and Action Bar	Description
Power	Link to the Power management page for details of the power consumption, PSU status and power configuration. This is equivalent to clicking on any of the power supply modules in the system image.
Cooling	Link to the cooling and thermal management page for details of the fans and thermal configuration. This is equivalent to clicking on any of the fan modules in the system image.
Network	Link to the Network status and configuration page. This is equivalent to clicking on the HX5 I/O Module in the system image
Action - Power Control	• **Nodes – Turn On** - Enable and turn on all nodes in the enclosure. • **Nodes – Graceful Shutdown** - Request all running nodes to shut down and turn off. This is an OS-driven shutdown and so may not succeed if there is an active user or updates need to be installed on a node. • **Enclosure – Restart** – Restarts the Management Controller and completes any pending updates.
Action - Identify	• Flash the Enclosure LEDs in order to identify this system Enclosure to a technician who intends to work on this system.

Power

The power page shows the power supplies currently fitted to the system and for each supply provides the power rating and health status.

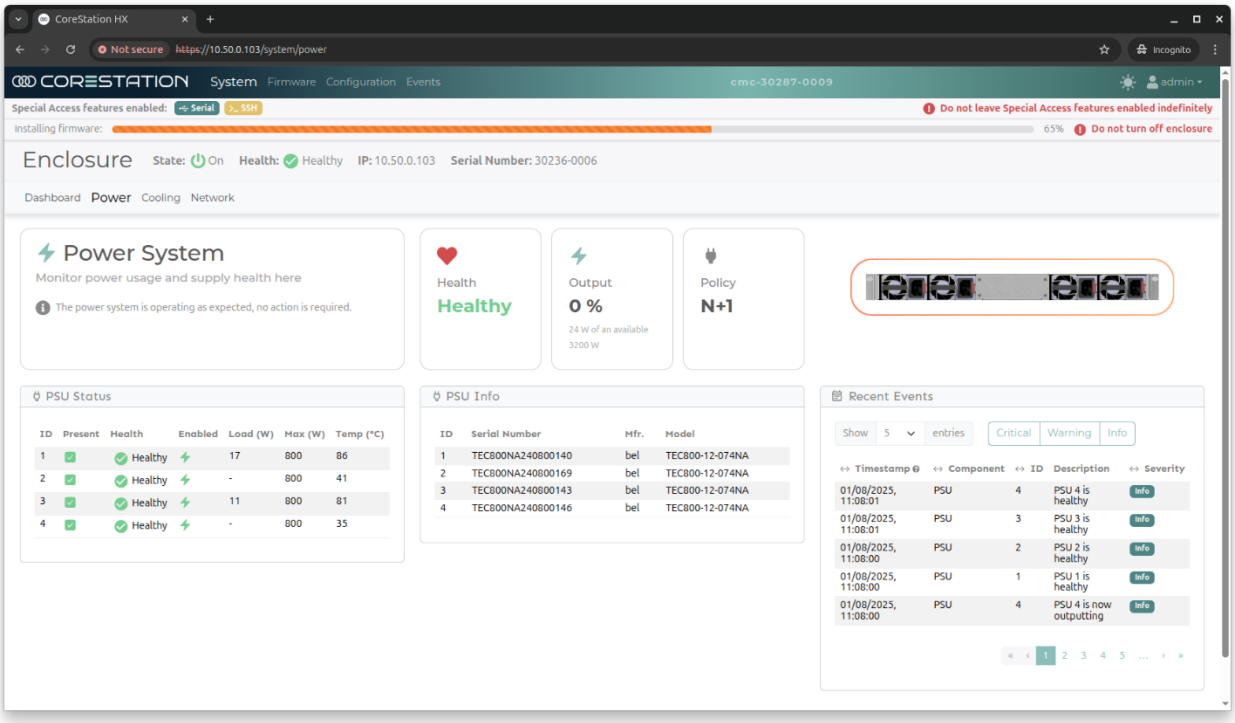


Figure 13 - Power System

Status and Information displayed on Power Page

Main Page Items	Description
Enclosure image	Rear view of the Enclosure showing the Power Supplies which are currently fitted and the slots they are using. Any PSUs with a Yellow or Red health status will be highlighted. Hover over an individual PSU to highlight information specific to that module.
PSU Status	• Present - Is a PSU module fitted in this location • Health: **Healthy** - Operating Normally **Warning** - Minor issue, output power may be slightly reduced **Error** - Major issue, this PSU is unable to supply power • Output Enabled - Is this PSU currently contributing to the system power - At light load, some PSUs may be automatically turned off to improve overall efficiency.

	• Output Load - How much of the PSU capacity is currently used • Temperature - What is the internal temperature of the PSU?
System Power Status	Overall status of the power system **Healthy** - Operating Normally **Warning** - Minor issue **Error** - Major issue
Output Load	Live enclosure power consumption and maximum power available
Power Policy	Redundancy level - Level of PSU redundancy at the current configuration • Non-redundant - Loss of a single PSU may cause the system to turn off immediately • N+1 - Loss of a single PSU will not affect system operation
Recent Events	List of recent events and log message related to system power and PSU modules.

Cooling System

The Cooling page shows details of the fans modules fitted to the system and their status.

The Management Controller automatically controls the speed of the fans to maintain the temperature of the components and nodes. As the system load increases the fans are driven at a higher speed to provide more cooling and as the system load decreases, the fans spin slower to reduce noise and increase operating lifetime.

Each of the fans are controlled independently and their speed is based on the current heat load within their cooling channel, with some consideration to the heat in adjacent cooling channels.

Recommended Maximum Temperature

For any system configuration, there is a recommended maximum ambient temperature. This is based on Amulet Hotkey validation and can be determined before install using the CoreStation HX power estimation tool.

These recommendations are based on reliably cooling the system with a maximum load on all workstation nodes and the fans running at around 90% of their maximum speed. This provides a good balance of fan operation lifetime and ambient temperature range. It is acceptable to exceed this ambient recommendation for short periods, but running above the recommended limit continuously will reduce fan operating lifetime.

If the system is operated above the recommended maximum ambient temperature for a given configuration, the fans will first increase at maximum speed, then the performance of nodes will be reduced to maintain a safe operating temperature for the key components.

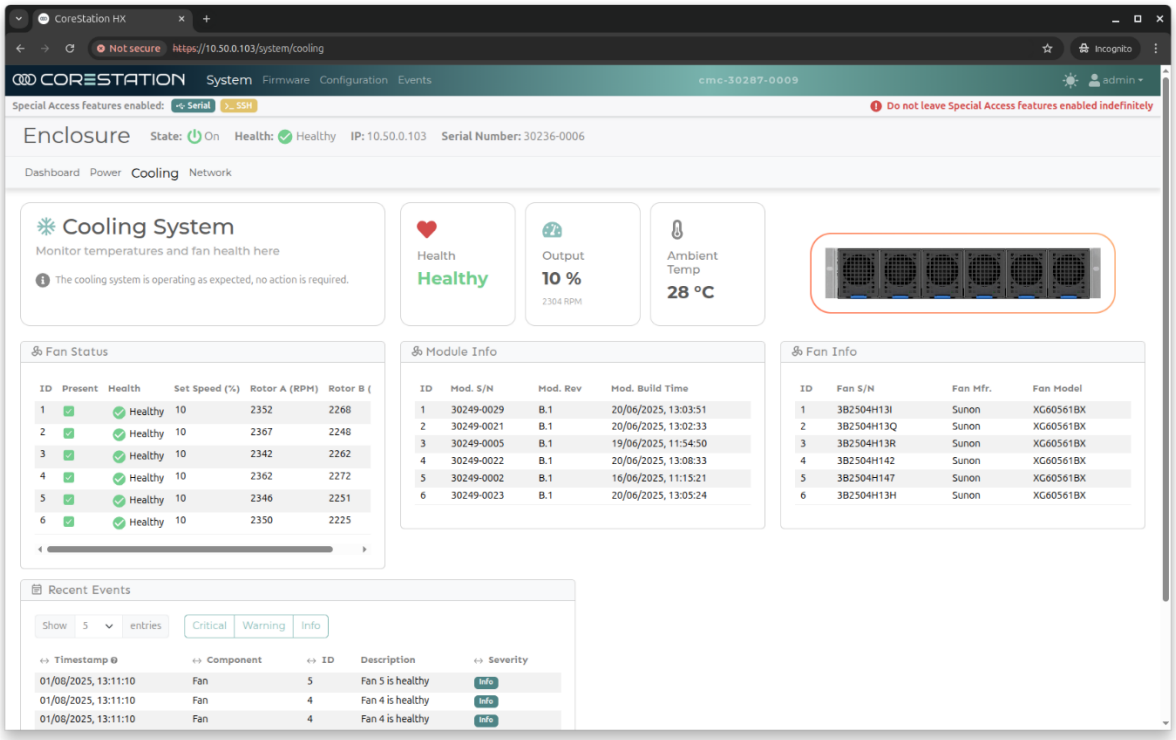


Figure 14- Cooling System

Main Page Items	Description
Enclosure Image	Rear view of the Enclosure showing the Fan modules which are currently fitted and the slots they are using. Any module with a yellow or red health status will be highlighted.
Ambient Temp	• Live measurement of ambient temperature at the front of the system
Fan Status	• Present - Is a Fan module fitted in this location • Health: **Healthy** - Operating Normally **Warning** - Partial failure with a small effect on node performance **Error** - Failure with significant effect on node performance or functionality • Set speed - The target speed percentage requested for this fan based on thermal load and ambient temperature • Rotor A - Live speed of the front rotor for this fan • Rotor B - Live speed of the rear rotor for this fan
Module and Fan Info	Details of the fan modules fitted to each location
Recent Events	List of recent events and log message related to system cooling and fan modules

Network

The network page provides details of the CoreStation HX5 I/O module and the status of the external ports. Depending on the module variant in use, there may be additional configuration options available.

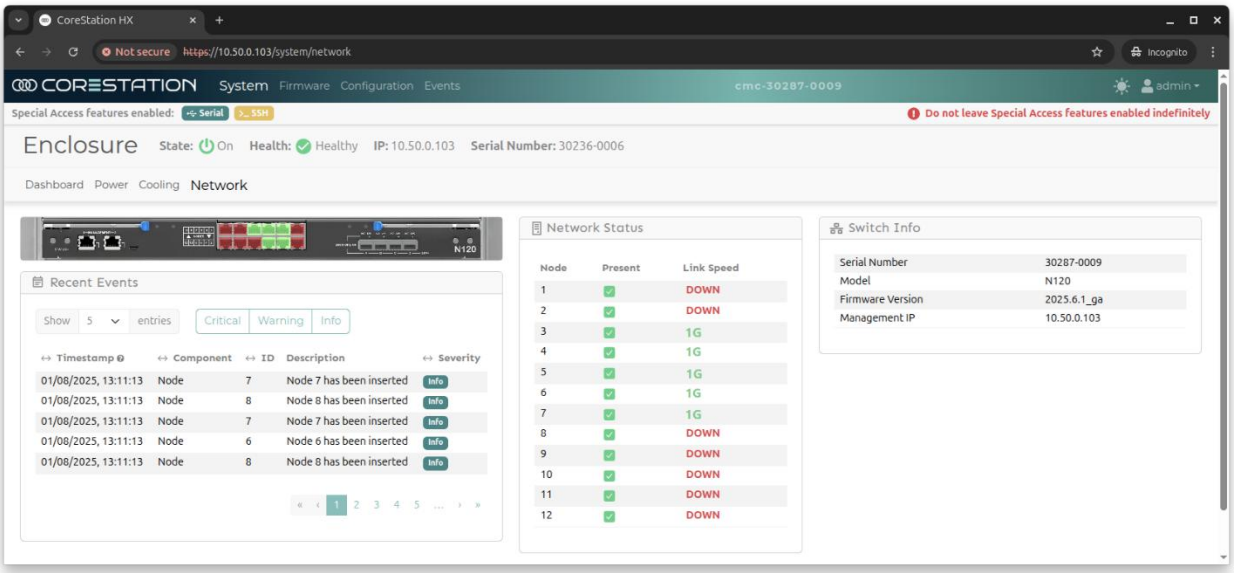


Figure 15 - Network Status

Main Page Items	Description
Image	Rear image of the HX5 I/O module showing the live status of the ports
Switch Info	• Serial Number – Serial number as printed on the label of the IO Module • Model – IO Module variant fitted • Firmware Version – Current system firmware version. The System firmware is updated together, and this version will match the version of the management controller. • Management IP – The Live IP address assigned to the management network interface.
Network Status	Live network link status for the passthrough port on each node • Present – Is a node fitted to this slot • Link Speed – Live link status and speed reported for this port **DOWN** – No link detected or node network interface not active **100M** – Link established at 100Mbit/s **1G** – Link established at 1000Mbit/s **2.5G** – Link established at 2500Mbit/s
Recent Events	List of recent events and log message related to system network and management

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.

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

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

Available commands

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 syntax

Command	Example syntax

help	`> 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`

info	`> 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`
	`Network mode: DHCP`

net	`> 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`

system reboot	`> system reboot`
	`About to reboot Corestation Management Controller...`
	`Contiune (yes/no) > yes`

system reset	`> 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`

system format	`For use in firmware recovery under guidance from Amulet Hotkey support`
fw	

Management Console - Configuration

Firmware Status

The Firmware page shows the version of the firmware running on the system and when it was installed.

Firmware versions are named as year.month.version with a suffix describing either general availability (GA) or a customer specific variant.

The system firmware is updated together, and the update package contains firmware images for:

- HX5 Management Controller
- HX5 integrated network Switch in N120
- Node Management Controller
- PSU Controller

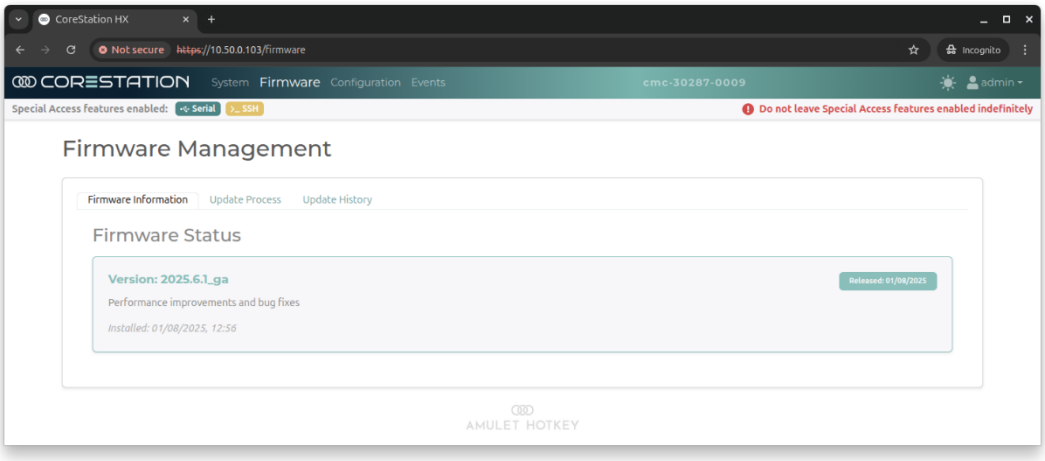


Figure 16 - Firmware Information

Other firmware and software components are updated independently:

Node BIOS	Updated via the OS or directly over USB
Node Operating System	Updated using standard OS-specific methods
Node Operating System Drivers	Updated using AHK Baseline driver packs, deployed via the OS.
Node SSD Firmware	Updated via the OS

System firmware updates

Amulet Hotkey regularly release updated management firmware for CoreStation HX, and this is made available on the Amulet Hotkey resources website. The firmware update is delivered as a single compressed (.zst) file which is cryptographically signed and contains all the firmware required by the system. The compressed update file is approximately 1GB in size.

Amulet Hotkey provide an email notification service for updates so that all customers are aware of updates as soon as they are released.

The system firmware update process would typically follow the following pattern:

1. Receive notification of new firmware update release
2. Read the release notes and plan the firmware roll-out schedule
3. Download the firmware update file from the Amulet Hotkey resources website
4. Validate the download using the provided SHA-256 hash value
5. Shutdown and turn off all nodes
6. Open the CoreStation HX management console and open the Firmware page
7. Upload the firmware update file using the dialog
8. The firmware file is validated by the management console
9. The system offers the options to perform the firmware update now or Cancel

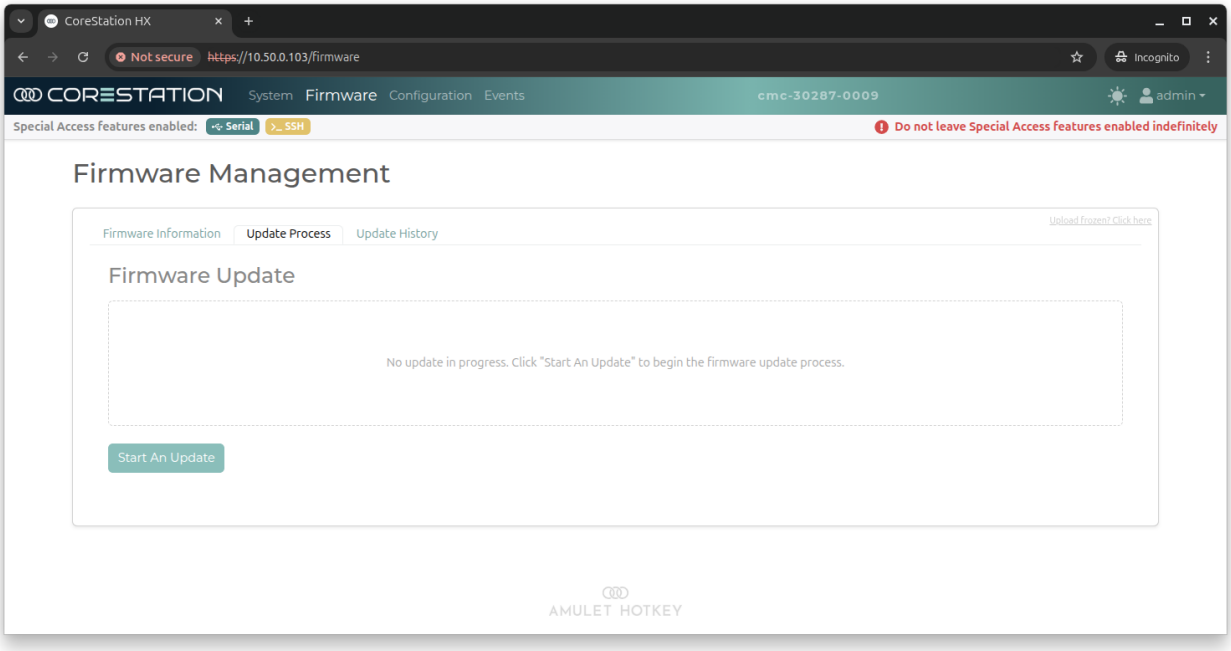


Figure 17 - Firmware Update

Once the process has started, the Management Controller will install the firmware and show a message once it's ready to restart. The nodes must all be shut down and turned off before the restart in order that the node management controller can be updated at the same time.

If new nodes are added to the system, they will be updated to the latest running firmware before they are enabled for use.

Firmware update history

The Update History page shows the dates and times of previously installed updates for information. It is not possible to directly revert to a previous version using this page, but the standard firmware update dialog can be used to update to a previous version.

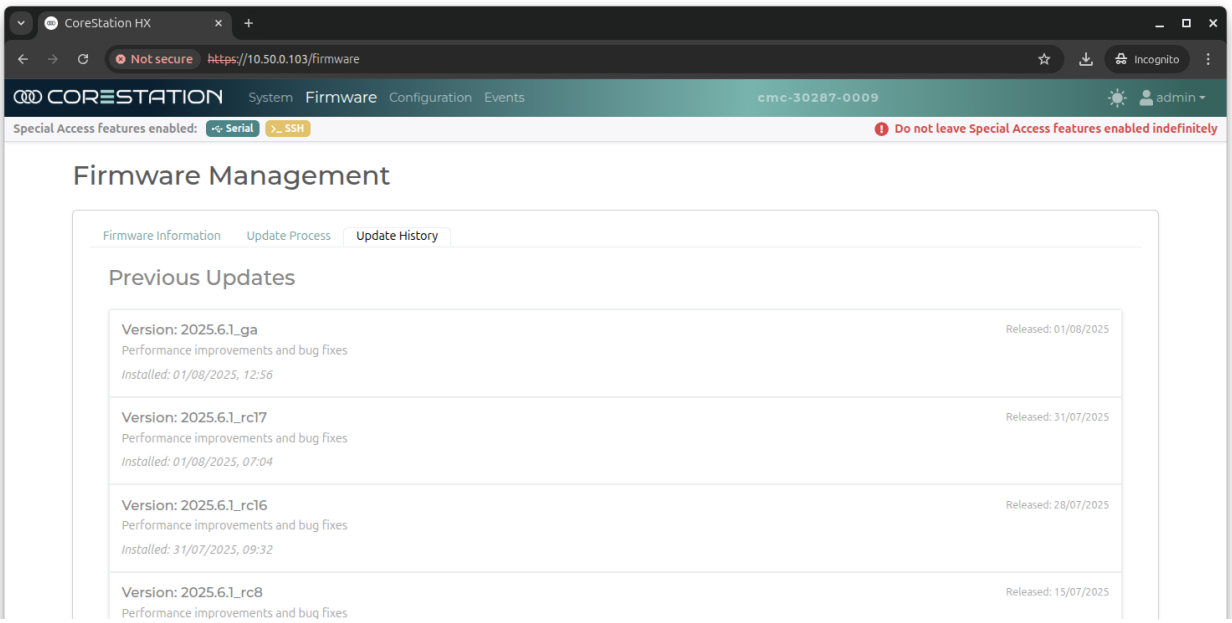


Figure 18 - Firmware History

System time

The time is set at the Amulet Hotkey factory and uses the network time protocol (NTP) if available to update the time regularly. The NTP server address defaults to the public pool.ntp.org cluster, but can be configured to use a local server for tighter control.

The Enclosure time zone should be set to the time zone matching the geographical location of the enclosure. This time zone is used when recording all enclosure events so that physical operations and external factors can be aligned.

Enclosure time zone is separate to user time zone to make it easier to track multiple users who are in different geographical locations to the enclosure.

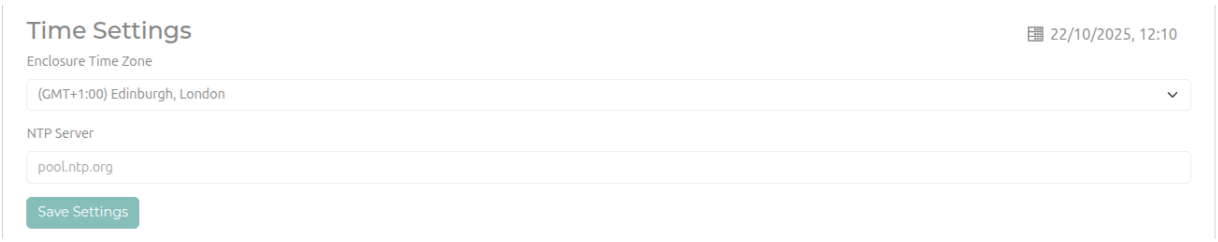


Figure 19 - Time Settings

Many pages in the Management Controller display the time in the top-right corner. The time displayed can be toggled between Enclosure time zone and User time zone by clicking the Icon. There is additional detail provided in the hover-over popup.

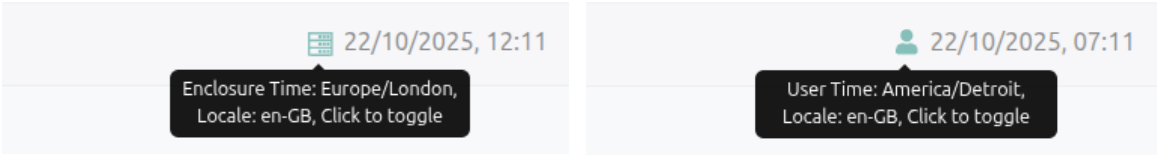


Figure 20 - Display time toggle

Management Network Configuration

The network settings for the Management Controller can be configured either from the serial port or from the Management Console.

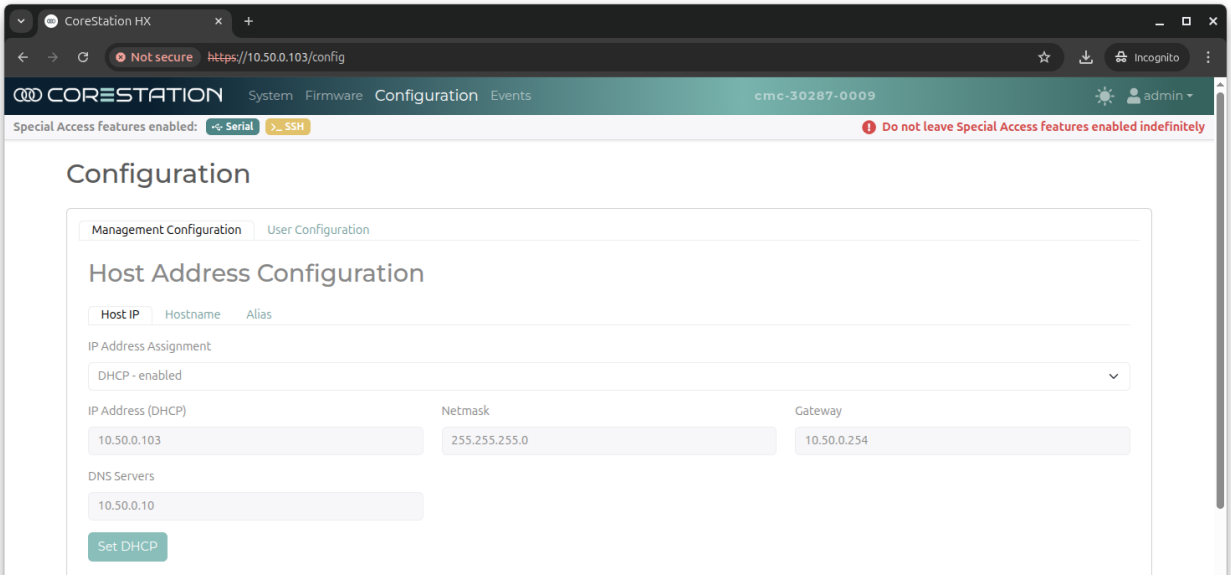


Figure 21 - Network Configuration

The Management Controller can be configured to either use DHCP or a static IP with manually specified netmask, gateway and DNS servers. Once this is confirmed, the Management Controller will restart and appear on the new address.

The system hostname can also be changed to a specified value. The default hostname is based on the serial number of the Management Module.

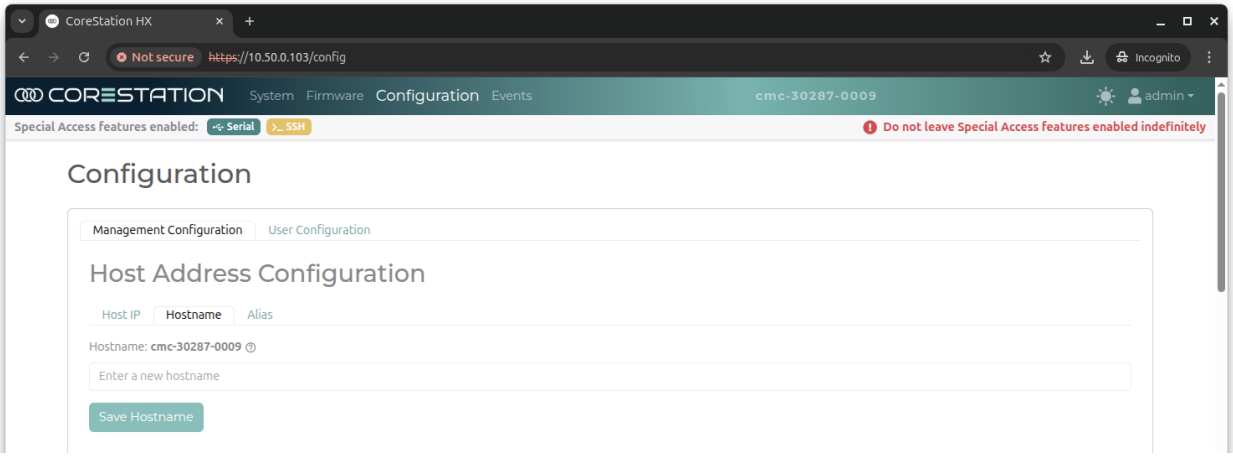


Figure 22 - Hostname Configuration

Following a system reset, the Management Controller will return to the default hostname and attempt to use DHCP to acquire an IP address.

HTTPS Certificates

The default self-signed TLS/SSL certificate can be replaced by a new certificate generated and signed by a local or corporate Certificate Authority (CA) using a certificate signing request (CSR) process.

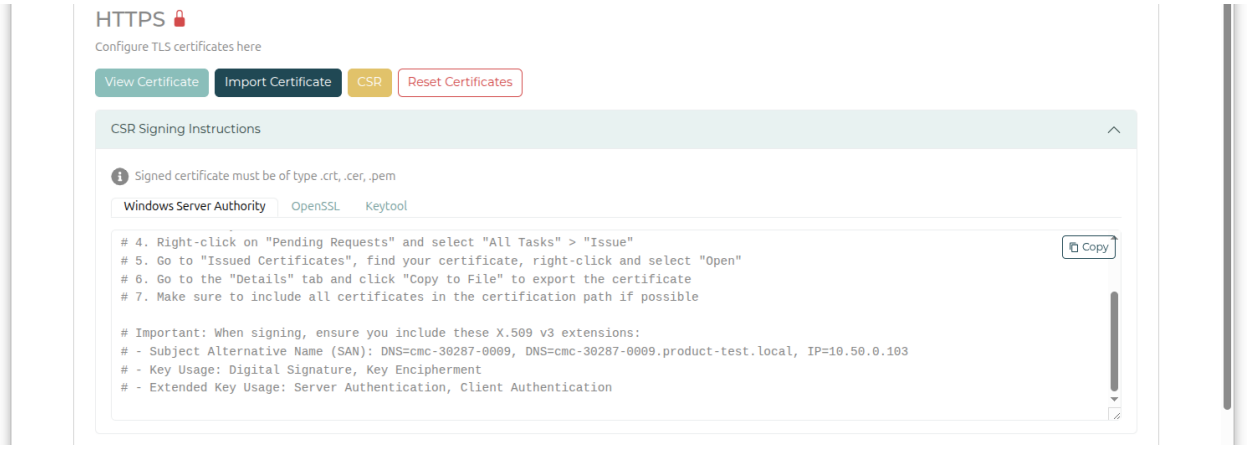


Figure 23 - HTTPS Certificate export and import

1. Navigate to Configuration > Management Configuration
2. Generate a CSR using the “Export CSR” button and save the downloaded file
3. Request a unique certificate matching this CSR from the internal company CA server
4. When the new certificate is available, add the new certificate using “Import certificate”

If the new certificate correctly matches the CSR, the new certificate will replace the existing self-signed certificate, all users will be signed out and the management controller will restart.

Next time any user tries to access the management console, they will be presented with the updated TLS/SSL certificate.

If there is an issue, the TLS/SSL certificate can be reset to the factory-issued self-signed version by confirming “Reset Certificates”

Factory Reset

The Factory Reset function erases the Management Controller configuration and returns the system to the state as it was when it left the factory. This includes all user data and network configuration, so before performing this reset, be sure to have the default login credentials to hand – these can be found on the label on the management controller module.

During the factory reset process, all usage data and history is erased from the Management Controller using a simple erase process. If the system is destined for disposal, contact Amulet Hotkey for information on a fully secure process to destroy all data and ensure it cannot be recovered.

The reset process takes up to 15 minutes to complete and the Management Console will be unavailable during this time.

Item	State after Factory Reset
Management Console User Accounts	Admin account only. Default password as printed on IO Module label
Management Controller hostname	Default hostname as printed on IO Module label
IP Address	Use DHCP to acquire IP address
System Firmware Version	The version that was installed at the time of manufacture
System Firmware History	Erased
Event history	Erased
HTTPS Certificates	Self-signed certificate
Node	No change to Node OS, BIOS or configuration

Special Access

The special access features are intended for diagnosing or repairing exceptional issues with the help of Amulet Hotkey support, they are not intended for general customer use. The features and commands available via these interfaces are likely to change between versions with no notice, so it is recommended to use the CoreStation API for integration and scripting.

If these special features are required, they should be enabled for a short time and then disabled again once the investigation is complete. Because these features enable access to the system without the standard login credentials, they are shown as a warning banner on the top of all pages on the Management Console when enabled.

Both special access methods require a login using a fixed user and password which cannot be changed. Logins using these special access methods do not appear in the system event logs so Special Access methods should always be disabled unless explicitly required.

Figure 24 - Access control for serial and SSH access

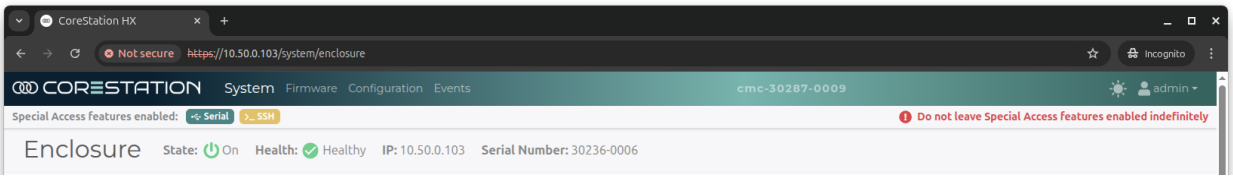


Figure 25 - Banner showing Serial and SSH features enabled

Special Access	When enabled	When disabled
Serial	Front and Rear system serial ports present a direct, privileged login to the embedded Linux operating system running on the Management Controller and the pre-boot environment.	Front and Rear system serial ports present a restricted interface for configuring IP address and performing factory reset
SSH	Secure shell access is enabled over the network on port 22 on the IP address of the management controller. This provides a direct, privileged login to the embedded Linux operating system running on the Management Controller	Port 22 is closed, does not answer requests and SSH login is not possible

Local user configuration

This page provides a table of the current local users for the management controller.

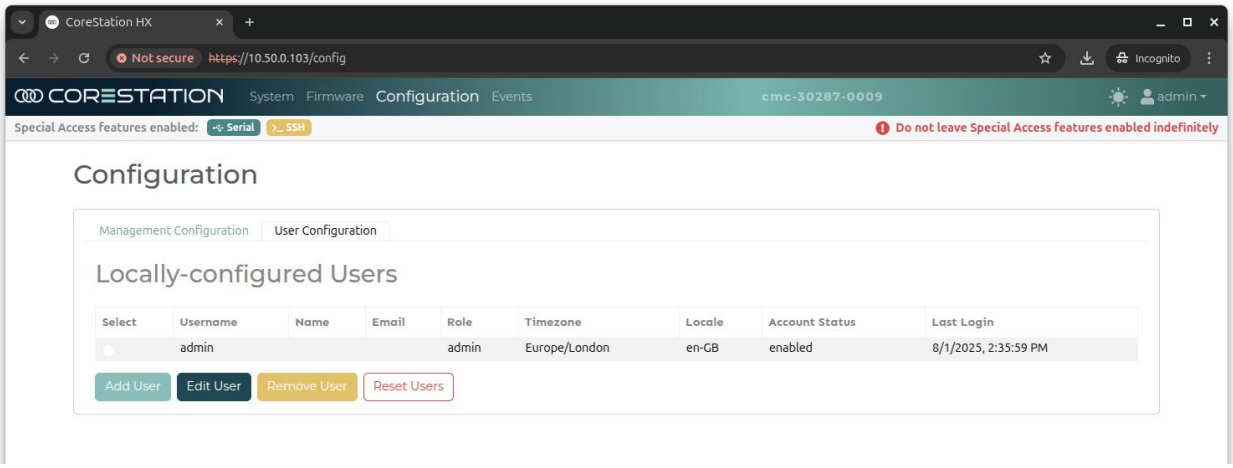


Figure 26 - Local user Configuration

Up to 25 local user accounts can be created with usernames including letters, numbers, diacritics and other characters typically found in email addresses (@, ., -, _). The usernames are not case sensitive and the add user dialog will fail if a user already exists with the same letters (e.g. admin and ADMIN).

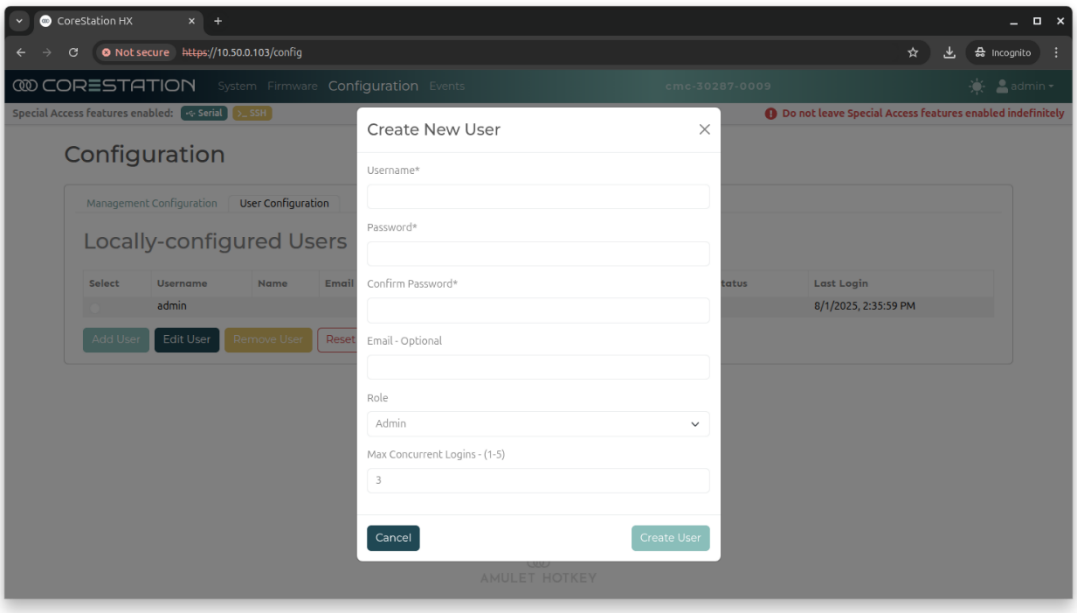


Figure 27 – New User dialog

The in-built Administrator account with username admin cannot be deleted but can be disabled as long as another local admin has been created or domain user integration has been correctly setup.

Domain user setup with LDAP (BETA)

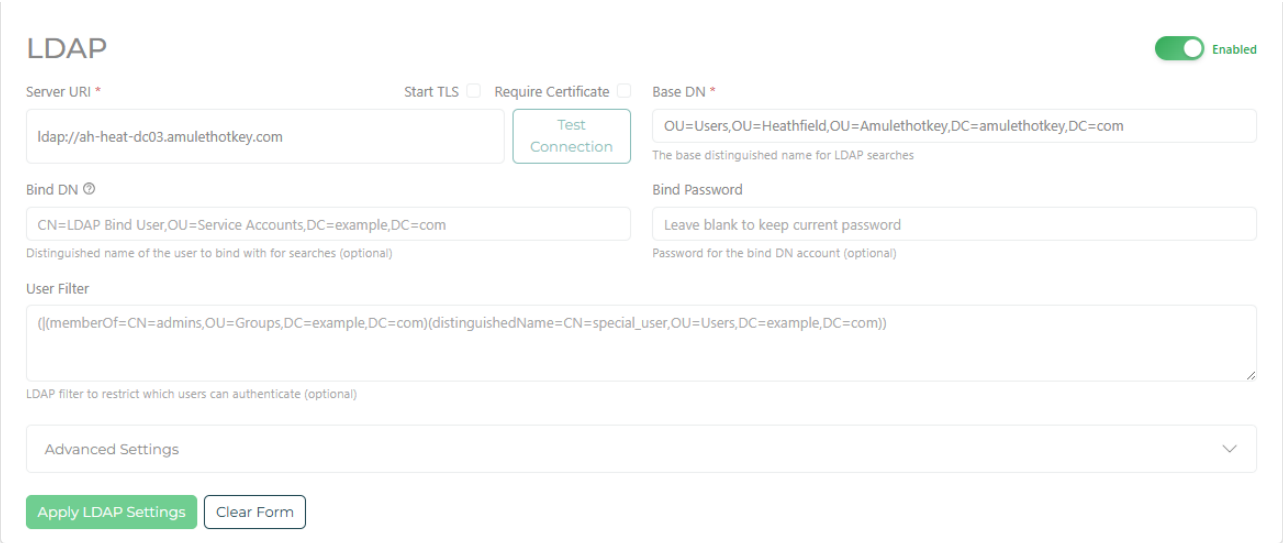
The Management controller can be setup to allow user authentication with a centrally-managed service using the Lightweight Directory Access Protocol (LDAP) for connection to services such as Microsoft Active Directory. There are multiple settings which make up the LDAP configuration in order to support a wide range of possible deployments and directory services, but not all fields need to be configured for all deployments.

The Management Controller user list maintains an entry for every user who has successfully authenticated via LDAP and keeps track of their last login and user role.

LDAP Settings

Configuration	Option	Description
Enabled	En/Dis	If Enabled, the Management Console will check login attempts against directory service if configured. Local accounts can still login if this is disabled or cannot be reached.

Server URI	URI string	The network address of the server running the LDAP directory service. This can be a network name or IP address which can be reached from the Management Controller. Prefix this entry with the protocol used to connect (ldap:// or ldaps:// for connections using TLS).
Start TLS	Yes/No (Opt)	If yes, attempt to negotiate an encrypted connection to the LDAP server. Encrypted connection is always used if the URI prefix is https://
Require Certificate	Yes/No (Opt)	When set, the Management Controller will validate the certificate from the LDAP server against a local stored certificate if the connection uses TLS.
Upload Certificate	Upload (Opt)	Upload a certificate to be used for validating the LDAP server when establishing a secure connection using TLS.
Base DN	String	The location to find users within the directory service database, provided in X.500 Distinguished Name format. E.g. “OU=Users,DC=example,DC=com”
Bind DN (User)	String (opt)	This is a specific user account which has permissions to search the directory service. E.g. “CN=BindUser,OU=Users,DC=example,DC=com” If this left blank, the search will be performed with the credentials of the user who is attempting to login.
Bind Password	String (opt)	
User Filter	String (opt)	A set of requirements on the user account to allow login, presented in DN format and can combine OR and AND operators. E.g. must be a member of the facilities group: “memberOf=CN= facilities,OU=Groups,DC=example,DC=com”. If this filter is highly complex, it can add significant time to the login process. Consider using the Required Group filter instead. If this field is left blank, any user in the directory will be authenticated.

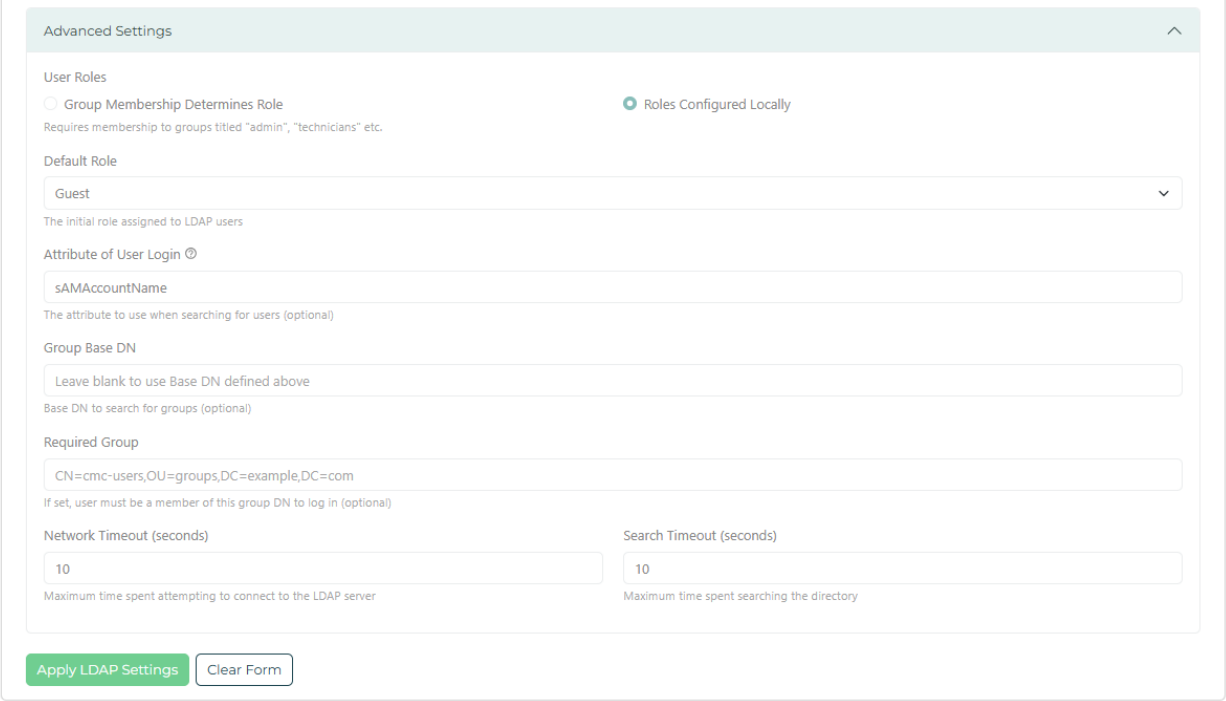


Advanced LDAP Settings

There are also a set of advanced LDAP settings for matching directory users to one of the four user roles in the Management Console. By default, the first time a new user completes a successful login, they are added to the user list with the guest role. An admin can subsequently promote that user to a higher role and the Management Console will remember this setting in future.

Alternatively, the role for a user can be automatically determined at login if the directory service contains groups defining members of each access role.

Configuration	Option	Description
User Roles	**Group Membership Determines Role** At every login, search the LDAP directory service for the role the user should be assigned. **Roles Configured Locally (default)** The first time a user successfully logs in, assign them to the default Role. This can subsequently be changed by an administrator on the Management Console and is retained for subsequent logins.	
Default Role	Role (req)	The role assigned to a user when they first login to the Management Controller using LDAP (Guest, Operator, Technician, Admin)
Attribute of User Login	String (opt)	Defines the field or fields in the LDAP directory to check against the username entered at login time. Directory users may be listed as first.last@domain or first.last or else the database structure has changed over time. The username entered on the Management Controller login screen name must match one of these fields exactly. By default, the username will be checked against “sAMAccountName”, “userPrincipalName” and “uid”.
Group Base DN	String (req)	The location to find groups in the directory for assigning user roles. There must be groups defined here for each Management Console User Role (Admin, Operator, Technician, Guest). The authenticating user will be assigned a role based on the group of which they are a member. If they are a member of multiple groups, they will be assigned the highest role.
Required Group	String (opt)	If populated, the authenticating user must be a member of this group. This is applied in addition to the user filter and can be a simpler way to control access if there is a suitable group with all the users who should be given access.
Network Timeout	Seconds	Maximum time to wait for a successful connection to the LDAP directory server. After this timeout, the login attempt will be rejected. Default 10 seconds.
Search Timeout	Seconds	Maximum time to spend searching the directory to confirm user credentials are valid. Default 10 seconds.



User Roles and access restrictions

Each user account is assigned to one of four defined roles which determines the level of privilege that user is granted.

Role	Administrator	Technician	Operator	Guest
Intended use	Setup and configuration	Day-to-day operations	Restricted Operations	View information only
System	Full Access	Full Access	Limited	View Only
Node	Full Access	Full Access	Limited	View Only
Firmware	Full Access	View Only	View Only	Hidden
Configuration	Full Access	View Only	View Only	Hidden
Events	Full Access	View and Filter	View and Filter	View and Filter
Exports	Full Access	Hidden	Hidden	Hidden
Account	Full Access	Full Access	Full Access	View Only (Cannot Change password)

Dark/Light Mode

Allows the user to choose their preferred visual style and takes effect immediately

- Light mode - Dark text on light background
- Dark mode - Light text on dark background

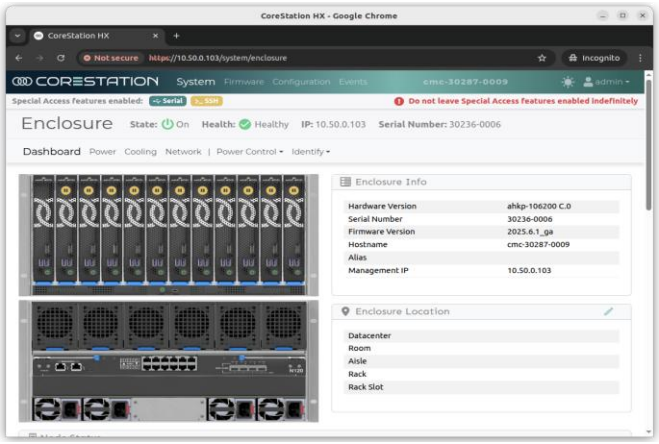


Figure 28 - Light mode

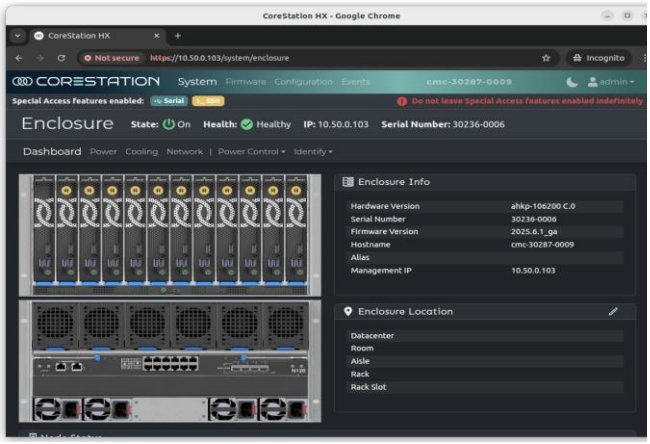


Figure 29 - Dark Mode

User Menu

This menu is present on all pages of the management console.

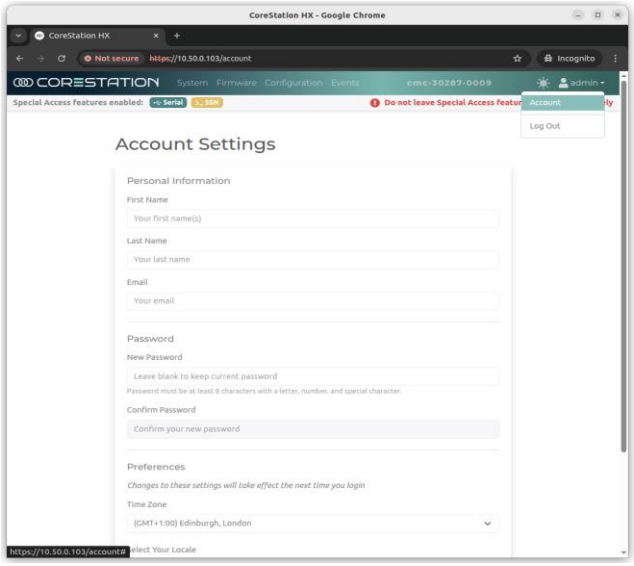


Figure 30 - User account settings

Account Settings

Link to the account settings page for the current user which allows editing a subset of their information.

First Name **Last Name**	Used for display and keeping track of local users in the user database and event logs.
Email	Used to link the user account to a specific company individual. In future used for pre-login password reset and email-based alerts and notifications.
Password	Allows the current user to change their password. No specific password complexity is enforced on new passwords. The password change will happen immediately, and the user will be required to sign in again.
Time Zone	Allows the current user to set their time zone for future system event reporting and alerting.
Locale	Allows the current user to select their preferred display format for dates and units within the management console. This does not change the language used for text. For example: English (United Kingdom) - dates use DD/MM/YYYY, Temperatures use °C English (United States) - dates use MM/DD/YYYY, Temperatures use °F

Logout

Sign out of the management console, close the session and delete the session token.

Management Console – Events and Reporting

The Event Log provides a audit trail and report for all actions which affect the system. This is split into three sections:

CoreStation Events – Changes to component state or health

User Events – Authentication actions and Account changes

Jobs Events – Actions performed by a user

Each of the event logs can be viewed in Enclosure time or User time to provide a clearer understanding of timing when the user and enclosure are in different time zones.

CoreStation (System) Events

This is a list of all the notable events which the system monitors for module status, health and presence. They can be filtered by severity and searched to locate specific actions. This includes all observed state changes whether they were the result of an identifiable user action or physical interaction with the enclosure.

- Power On/Off for enclosure and components
- Health Status for components
- Insertion and Removal of system components
- Enable and Disable status for system components

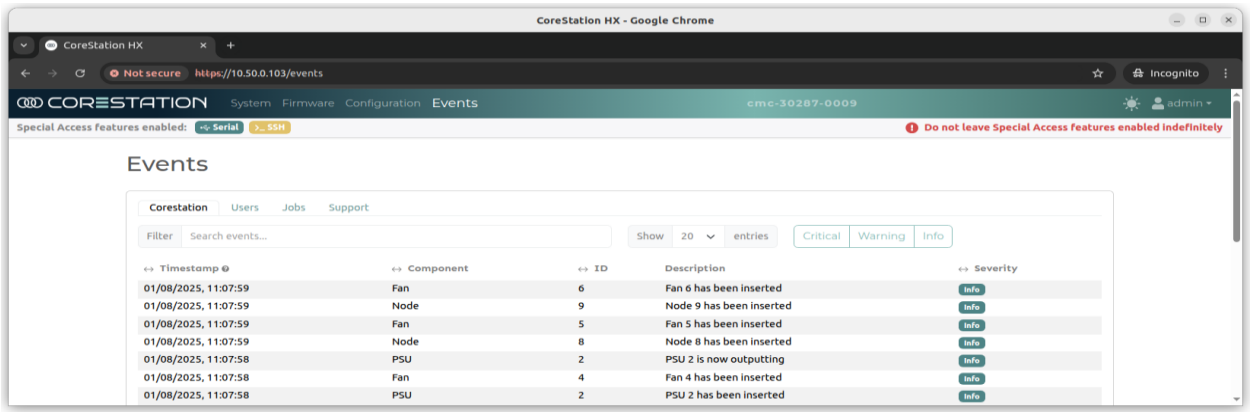


Figure 31 - CoreStation event history

Jobs Events

The jobs event log provides a history of all actions performed on the system and the user who initiated the action. Actions which are not attributable to a user (e.g. physical interaction with the system) do not appear in this list.

- Enclosure and Node power up/down actions
- Identify actions
- Firmware Updates
- Support bundle export

- Changes to API and Special access configuration

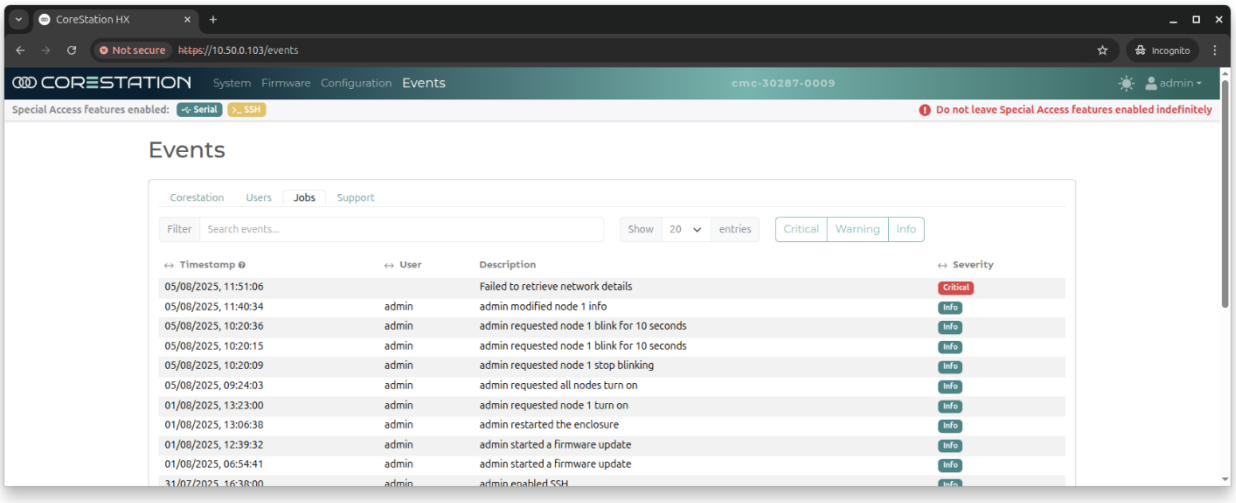


Figure 32 - Job event history

User Events

This is a history of all actions related to a user or initiated by an identifiable user including failed attempts to login.

- Successful Login by a user and the source IP address
- Successful Logout by a user
- Failed login attempts and the source IP address
- User account creation and modification
- User password changes

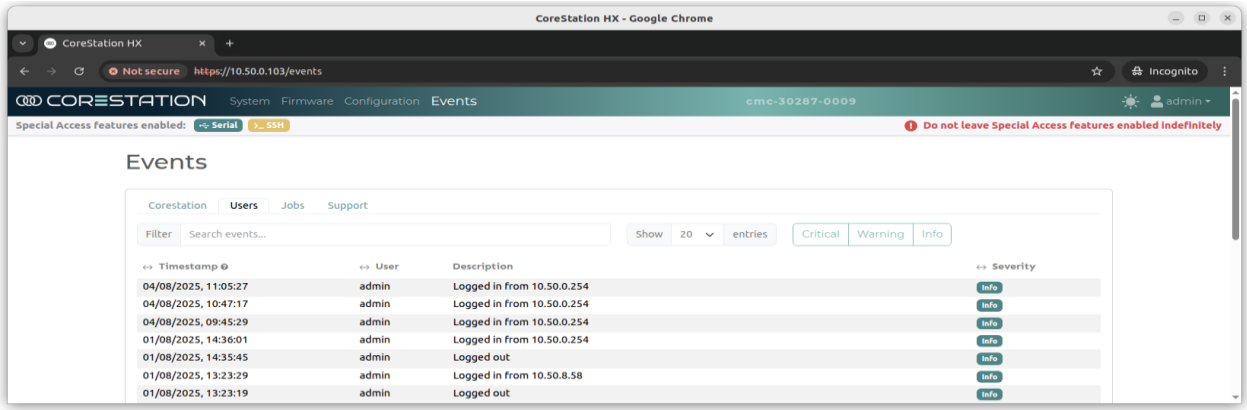


Figure 33 – User event history

Support

The support page provides a route to export information from the system for audit or diagnosis.

Amulet Hotkey support teams will often request a Support Bundle export as part of any investigation.

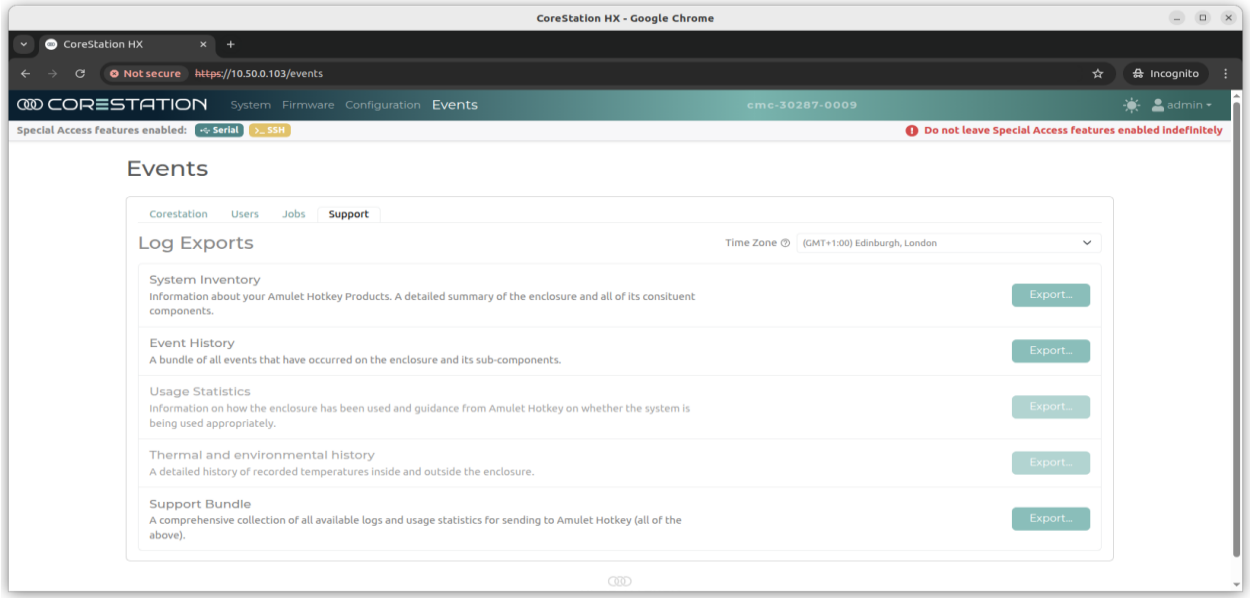


Figure 34 - log exports

The process may take a few seconds, following which the user will be prompted to save the file locally.

System inventory

- Detail of the modules and nodes currently fitted to the system

Event history

- Recent Event Logs for system and users

Usage Statistics and Thermal and Environmental History

- These will be added in a future update

Support Bundle

The support bundle uses the common .tar.gz compressed container file type to reduce the size of the file download. It is possible to open this file using Windows PowerShell or common archive management applications, so the content can be reviewed prior to sharing with Amulet Hotkey support.

- System Inventory
- Recent Event Logs
- Management Console web server logs
- Management Controller Operating System logs
- Management Controller application logs

Management Console – Node Management

System Dashboard

The System Dashboard page provides an overview of the nodes in the system and shows specific info when hovering over the node. Clicking on any node in the image leads to the detailed page for that node.

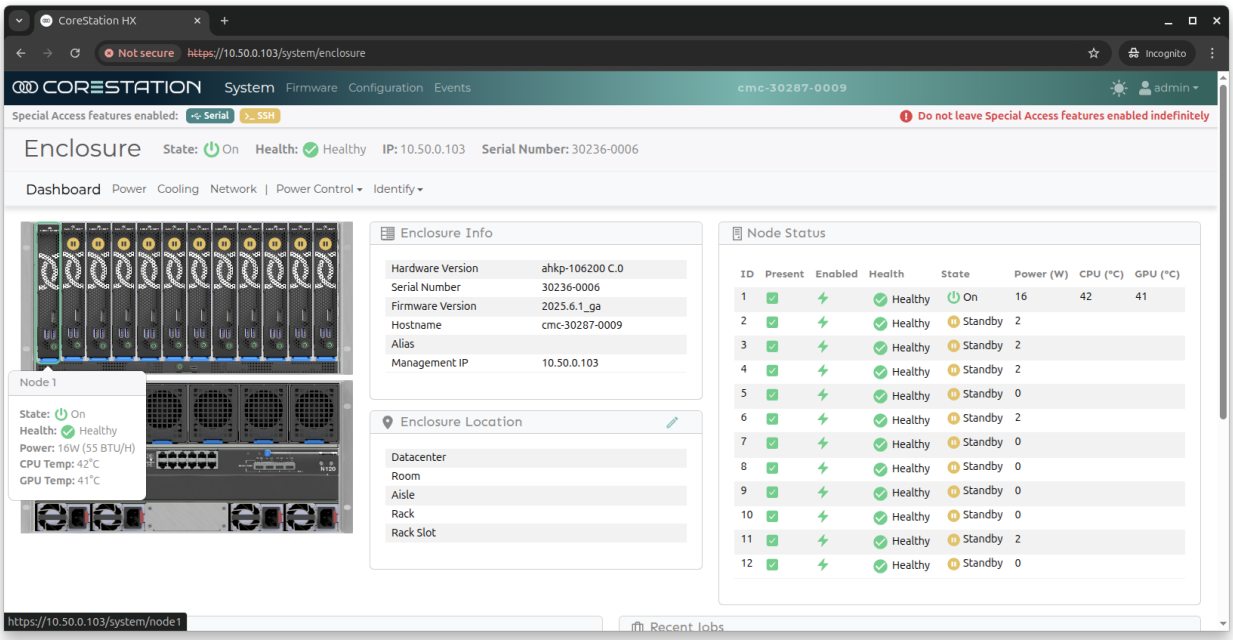


Figure 35 - System Dashboard with node 1 hover-over

Node management page

The management page for an individual node shows the specific information about that node. A complete system can be comprised of a range of different nodes, each with their own unique mix of components and settings.

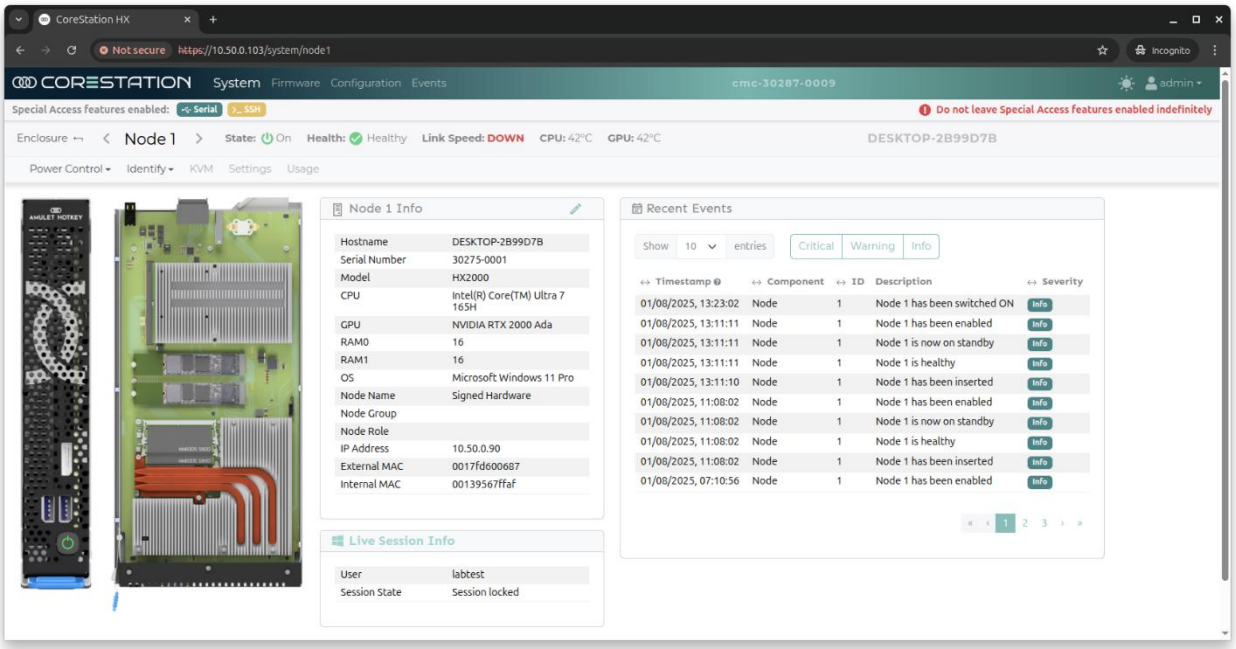


Figure 36 - Node status

Main Page Items	Description
State	Current node power state **On** - Powered on and operating **Standby** - Powered down
Health	Health - Summary of health status for this node **Healthy** - Operating Normally **Warning** - Minor issue, slightly affecting performance **Error** - Major issue, seriously affecting performance or functionality
Link Speed	Current network link speed for this node
CPU	Live CPU package core temperature
GPU	Live GPU core temperature
Front Image	Image of the node to help with locating it within an enclosure
Side Image	Image with the cover removed to help identify components, especially in the event of failure.
Node Info (static)	This information is gathered from the Node out-of-band and is available without an OS installed. • Serial Number • Model • CPU • GPU

	• RAM • OS • External MAC – Hardware address for Fabric 1B • Internal MAC – Hardware address for Fabric 1A
Node Info (Dynamic)	This information is provided by the CoreStation Agent whilst the node is operating. The latest values are cached when the node is not running. • Hostname – Workstation network host name • OS - Operating System name • IP Address
Node Info (User Fields)	These are free-text fields for customer use • Node Name • Node Group • Node Role
Live Session Info	This information provided by the CoreStation Agent whilst the node is operating. • User – Username of the current login session • Session State – Current Windows session state for this node
Recent Events	List of recent events and log message related to this node with filters for severity

Node Actions and Operations

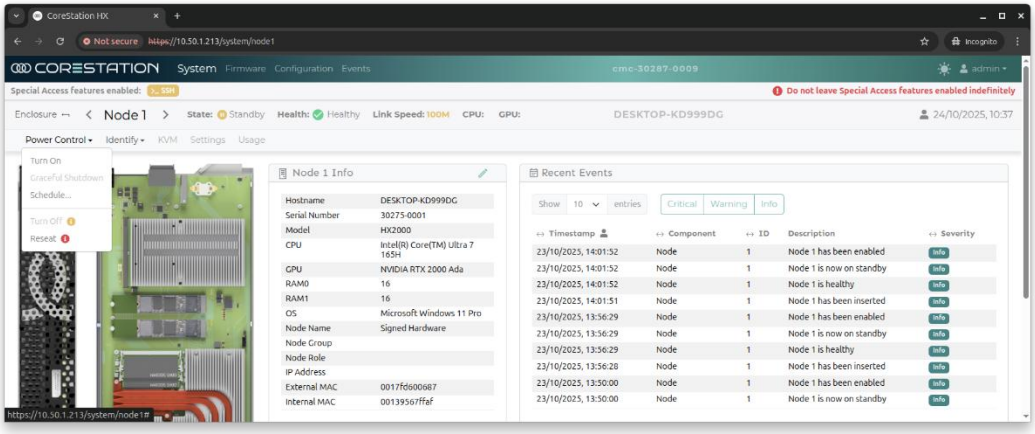
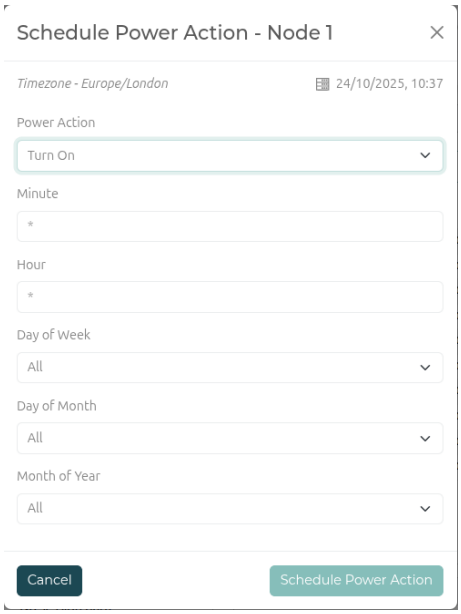


Figure 37 - Node Actions

Settings and Action Bar	Description
Power Control - Action Menu	Provides power control for this node. All the actions to turn off and restart a node ask for confirmation before performing the action. **Turn On** - Initiates the power-up process on this node. Only available if the node is currently powered-down. **Graceful Shutdown** - Initiates the Operating System shutdown process and turns the node off. This action may not succeed or may take some time to complete, depending on the operating system – e.g. User may cancel the request, an application may block shutdown, or Updates may need to be installed before shutdown. **Schedule** – Configures a power action to be performed at a specific time and repeat as required, for example configure nodes to power up each day before users start work. **Turn Off** - Forces the node to turn off without notifying the Operating System. This is equivalent to holding the power button for 4 seconds on a typical PC. If this action is performed repeatedly, the OS may enter a recovery state or experience corruption. **Reseat –** Equivalent to physically removing and re-inserting the node, this disconnects, then re-connects all power to the node and restarts the node management controller. If this action is performed repeatedly, the OS may enter a recovery state or experience corruption.
Identify – Action Menu	Flash the Node LED blue in order to identify this node to a technician who intends to work on this system. **10 seconds / 1 minute / 10 minutes** - flash the LED for a set period **Stop flashing** – Stop the identification and revert to the standard LED indicator The flashing state is reflected in the System Dashboard.

Schedule Action dialog	Setting
 *Figure 38 - Schedule dialog*	**Power Action –** The action to perform (Turn On, Graceful Shutdown, Turn Off, Reseat, Reboot). **Minute/Hour** – The time-of-day to perform the action. This can be a specific hour/minute or * to perform the action every hour. **Day of Week/Month/Year** – This can be a specific date to perform the action or All for a repeating action every day, week or month as required. **Schedule Power Action –** Once the action has been setup, this will appear as a scheduled Job on the node page. This can be cancelled from the Scheduled Jobs section of the node page. Some actions can only be performed if the node is in an appropriate starting state and the scheduled task will be ignored if it cannot be performed, for example a scheduled task to Turn On a node which is already Powered on.

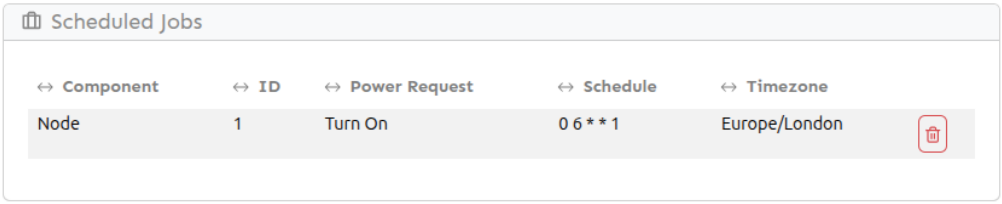


Figure 39 - Node Scheduled task card

Node Firmware Updates

Firmware Item	Update Route	Restrictions
Node Management Controller	Updated automatically as part of system firmware at next restart	Management controller and nodes must run the same firmware version
Node BIOS	Updated from the OS using BIOS Capsule updater from AHK Resources site	Node BIOS version must be the same as or earlier than the Management controller firmware.
CPU Microcode	Included in BIOS image	No Restrictions
Intel ME Firmware	Included in BIOS Image	No Restrictions
SSD Firmware	Updated from the OS using vendor-specific update tool	A minimum version is required for some drives to operate correctly. Do not downgrade below shipping firmware versions.

Node Events

Node events are recorded in the event logs based on the action and the outcome.
If an action is performed by a known user, then the Events > Jobs log will show an event attributable to that user. If the action is not attributable to a user, then the event will be recorded in Events > CoreStation log, but there will not be an associated job.

For example, a node can be powered on in several ways:

- Using the action menu on the Management Console (Known user)
- Using the power button on the front of the node
- When the node is inserted (If the BIOS is set to auto-power up)

Not all node-related activities and actions are recorded in the system event logs.

Action	Related Events
Turn On, Turn Off	Jobs - *user* requested node 1 turn on CoreStation - Node 1 has been switched ON
Turn On (From Front panel button)	CoreStation - Node 1 has been switched ON
Schedule/delete an action	Jobs - *user* scheduled Node 1 to turn on Jobs - *user* deleted a scheduled power action
Graceful Shutdown	Jobs – *user* requested node 1 shutdown gracefully CoreStation - Node 1 is now on standby
Reseat	Jobs – *user* requested node 1 reseat CoreStation - Node 1 has been inserted
Physical Insertion	CoreStation - Node 1 has been inserted
Physical Removal	CoreStation - Node 1 has been removed
Ready for use (Present, Healthy)	CoreStation - Node 1 has been enabled

Identity blink	Jobs - *user* requested node 1 blink for 10 seconds
Identify Stop	Jobs - *user* requested node 1 stop blinking
Change text fields for node info	Jobs - *user* modified node 1 info
Heath Status	CoreStation - Node 1 is healthy
Session Login/Logout/Lock	Not recorded as an event
Assign/Change node IP or hostname	Not recorded as an event
Network Link Status Change	Not recorded as an event
Connection to front panel USB/Video	Not recorded as an event
Change in Node OS or version	Not recorded as an event

CoreStation Agent for Windows

The CoreStation Agent provides integration between the CoreStation Management Controller and the node OS to provide key system information on the Management Console. The Agent runs as a background service on the node OS and communicates with the Management Controller directly using a serial port. It does not communicate over the network or internet in any way.

Installation of the Agent is optional and if not installed then the information it provides is not available in the Management Console, but no errors or warnings are generated.

The Agent is provided as a signed installer package for Windows 11 Pro on the resources page.

Item	Details	Where it is displayed
Hostname	Workstation Hostname set on the OS - to make it easy to find in other management tools	Shown on Node Info page
IP Address	Current IP address assigned to the workstation	Shown on Node Info page
OS Name	Current OS Product Name as reported by the OS	Shown on Node Info page
OS Version	Current OS Version and release running on this Node	Not currently shown
User	The username for the current desktop session	Shown on Node Info page
Session Status	Current state of the workstation and session as reported by Windows • No session data • Remote Desktop session connected • Remote Desktop session disconnected • User logged on • User logged off • Session locked • Session unlocked • Session created • Session terminated	Shown on Node Info page
Agent Version	Current version of the installed agent	Not currently shown

HX2000 Workstation Node

Overview

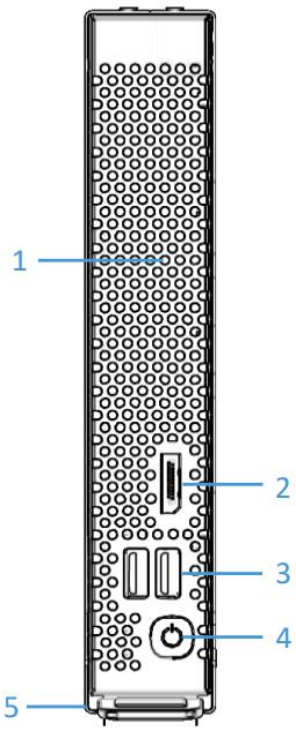
The CoreStation HX Workstation nodes are complete desktop computers which operate independently from one another and rely on support services delivered by the Enclosure and system management.

There is a system-level interaction between workstation nodes based on available system power and cooling, but otherwise the nodes can be removed and inserted without any consideration to the workload and status of others.

Figure 40 - HX2000 Workstation Node

Figure 41- HX2000 Workstation Node front

Workstation Node front view



1	Cooling air inlet	Cool air is drawn into the front of the workstation node over the full height of the front panel. Take care not to obstruct this inlet air when using the front panel ports.
2	Local Video Output (DisplayPort)	Used for direct connection to the local video output of the workstation for initial setup or diagnosis if out-of-band KVM is not available.
3	Local USB ports (USB-A, 3.0 5Gbps)	Used for direct connection of local USB devices to the Workstation for initial OS install when a network boot source or out-of-band KVM is not available.
4	Power button and status indicator	Power Button is used for manual shutdown when a workstation node must be removed without access to the management console. Power indicator shows a summary of the workstation node state and any serious health warnings which affect the node.
5	Latch handle	Physical handle used to latch the node into the Enclosure.

Workstation Node internal view

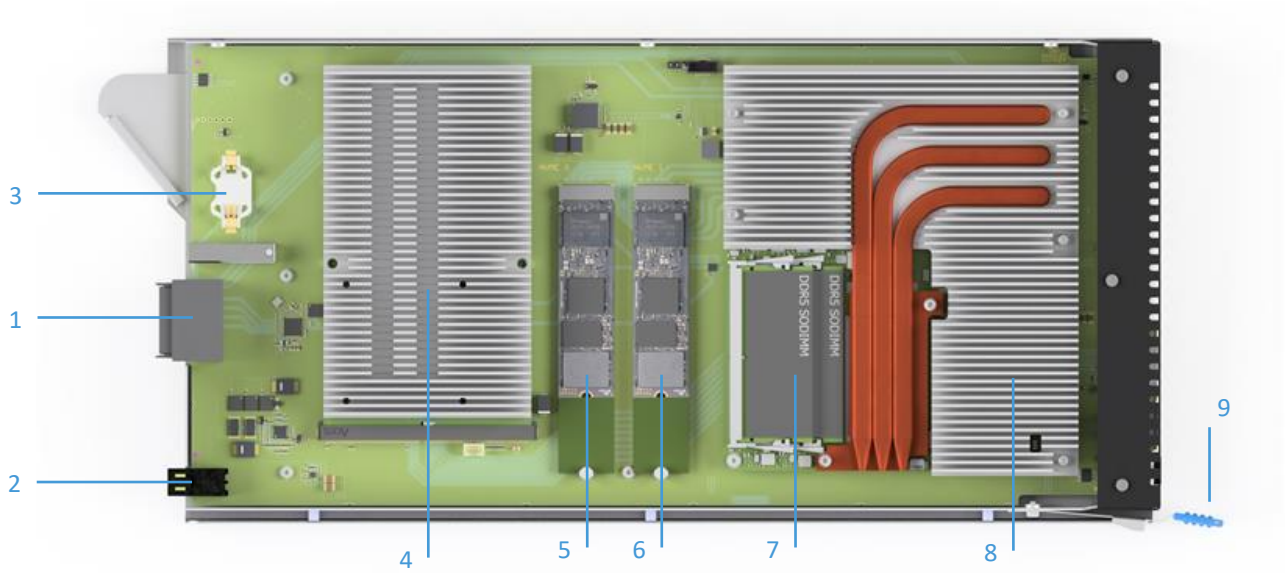


Figure 42 HX2000 Workstation Node with discrete GPU

1	Data Connector	Provides connection to Management controller module for network and system management services
2	Power Connector	Provides 12V input power to the workstation node
3	RTC Battery	Maintains Real-time clock and BIOS settings when node is removed from the Enclosure.
4	Discrete GPU	Optional discrete GPU for higher performance on graphically intensive tasks. Standard MXM 3.1 type modular GPU form factor.
5	Storage position A	Primary M.2 storage
6	Storage position B	Secondary M.2 storage
7	Memory modules	Dual-channel DDR5 SODIMM CPU Memory
8	Processor module	Workstation Node Processor module containing fixed solder-down CPU, support and power circuitry.
9	Latch handle	Physical handle used to latch the node into the Enclosure.

Node Status Indicator

Colour and Cadance	Workstation Node State
Off	No power is provided to the node
Solid Amber	Shutdown
Solid Green	Healthy and operational
Blinking Green (Once per second)	Main Operating System is booting, or other operation is in progress such as firmware or BIOS update.
Flashing Amber	Error or health alert on this node
Flashing Blue	Node ID - The identification request has been enabled from the management console in order to signal to a technician that this workstation node needs attention. This persists until the ID request has been cancelled.

Node power button

Workstation node power states would typically be controlled from the management console but can also be manually changed using the power button. The power button has similar functionality to a desktop PC.

Workstation Node State	Power button function
Enclosure not powered	No effect
Shutdown/Standby	Instructs node to power on and boot
Active	Short press (< 4 seconds) - Instruct OS to perform graceful shutdown Long press (> 4 seconds) - Power off immediately

Insertion and Removal

Workstation nodes can be inserted and removed at any time.

When a node is inserted, the System management controller will establish communication with the node BMC and check if it is possible to power up the node based on the power required by the node configuration and the power available in the system according to the current power policy. It may not be possible to safely power on the new node if it would exceed the available power.

It is recommended to power down a node before removal to avoid corruption to the operating system and also to avoid excessive wear on the power connector and power circuitry.

Before removing an operating node, first long press the power button to power off the node and observe the status indicator in the solid amber state.

CPU

Each workstation node has its own CPU module board which contains the CPU, memory, BIOS and supporting circuitry. The module is fitted and configured at the factory and is not user-replaceable.

The CPU has an integrated AI co-processor and GPU for accelerating workloads.

Workstation Node Series	Processor family	CPU Options	Core Count	Integrated GPU	AI Co-processor
CoreStation HX2000	Intel Core Ultra 100 series “Meteor Lake H”	Core Ultra 7 165H	16 Cores 22 threads 6P+8E+2E_{LP}	Intel Arc Graphics (Alchemist architecture)	Intel AI Boost NPU3 11.5 TOPS
	Intel Core Ultra 200 series “Arrow Lake H”	Core Ultra 9 285H	16 Cores 16 threads 6P+8E+2E_{LP}	Intel Arc 140T GPU (Battlemage architecture)	Intel AI Boost NPU3 13 TOPS

Memory

The CPU module supports dual-channel memory, where each channel has one SODIMM connector. Both channels should be populated for maximum performance.

The SODIMM memory can be replaced and upgraded by the customer using compatible modules supplied by Amulet Hotkey.

SODIMM modules with hardware error correction (ECC) are not compatible, but the workstation node can be configured to use in-band ECC. This slightly reduces the memory capacity and bandwidth available to the operating system and applications to provide additional resilience.

The following configurations are supported using unbuffered, non-ECC DDR5 SODIMMs operating at 1.1V. Use of modules rated for a lower speed will reduce the available memory bandwidth and system performance.

Workstation Node Series	Total Memory	Memory Modules	Memory interface speed
HX2000 Meteor Lake	16GB	Two 8GB DDR5-5600	5,600 MT/s
	32GB	Two 16GB DDR5-5600	5,600 MT/s
	64GB	Two 32GB DDR5-5600	5,600 MT/s
	96GB	Two 48GB DDR5-5600	5,600 MT/s
HX2000 Arrow Lake	16GB	Two 8GB DDR5-6400	6,400 MT/s
	32GB	Two 16GB DDR5-6400	6,400 MT/s
	64GB	Two 32GB DDR5-6400	6,400 MT/s
	96GB	Two 48GB DDR5-6400	6,400 MT/s

GPU

HX2000 makes use of the integrated GPU as part of the Intel system-on-chip and HX2000 series can also be fitted with a discrete GPU module. When an external GPU is fitted, both the integrated GPU and external GPU are available to the Operating System and applications for graphical workloads.

The Integrated GPU on the HX2000 series is based on the Intel Arc Graphics Alchemist architecture, generation 12.7, but the GPU is branded differently based on the core count.

Discrete GPUs on HX2000 series are connected directly to the CPU via PCIe using the PEG (PCI Express Graphics) port with a x8 lane count and transfer speed up to Gen 4.0 (16 GT/s)

GPU	GPU Memory	Core count	PCIe	FP32 Peak Performance	Graphics Power
Intel 'Arrow Lake' Arc Graphics	Shared DDR memory with CPU	8 Iris Xe cores 128 EUs	Integrated with CPU package	4.61 TFLOPS	Part of CPU power, max 25W for GPU-only workloads
Intel Arc 140T	Shared DDR memory with CPU	8 Iris Xe cores 128 EUs	Integrated with CPU package	4.8 TFLOPS	Part of CPU power, max 25W for GPU-only workloads
NVIDIA RTX 2000 Ada Lovelace architecture	8GB dedicated GDDR6	3072 CUDA cores 96 Tensor cores 24 RT cores	PCIe x8 Gen4.0	14.5 TFLOPS	60W TGP

Storage

There are two positions for M.2 22110 PCIe expansion cards which are available for high speed NVMe storage devices supporting PCIe/NVMe Gen 4 with x4 link width.

RAID Configuration

If both devices are fitted, these can be used as either two separate storage drives or combined into a single RAID volume using Intel VMD RAID in the CPU system-on-chip. When configured as RAID 1, the storage array is tolerant to the failure of either M.2 drive and this failed drive can be replaced at the next suitable maintenance window. The M.2 storage devices are not possible to hot-swap whilst the workstation node is operating, it must be removed from the Enclosure and powered-down.

The configuration of the RAID array must be performed before the OS installation and cannot be changed without re-imaging. When configured for VMD RAID, the windows installation requires the Intel VMD RAID driver as part of the installation.

Storage Config	OS Storage Driver mode
Two separate devices	AHCI
Single RAID 0 volume	VMD RAID
Single RAID 1 volume	VMD RAID

Storage Devices

HX2000 nodes are tested and validated with specific M.2 NVMe SSDs which can be supplied at purchase and also later as upgrades or replacement.

The following drives are supplied with the workstation nodes and are supported for upgrade and replacement

Capacity	Drive Model	Interface	Seq. read	Seq. write	Endurance (5yrs)	Minimum Firmware
512GB	Micron 3500	NVMe Gen 4	7000MB/s	5100MB/s	300 TB / 0.32 DWPD	P8MA002
1TB	Micron 3500	NVMe Gen 4	7000MB/s	6900MB/s	600 TB / 0.32 DWPD	P8MA002
2TB	Micron 3500	NVMe Gen 4	7000MB/s	7000MB/s	1,200 TB / 0.32 DWPD	P8MA002

Network

The HX2000 workstation node uses a pair of Intel i226 Network Controllers to provide network and management services. Management services use fabric A, whilst data connections to the OS can use either fabric A or B.

Connectivity	Network Controller	Capabilities	Uses
Fabric 1A	Intel i226	2.5GBase-T Ethernet 100/1000/2500 Mbit/s	Out-of-band management Data network connection to the operating system when using N120 uplinks.
Fabric 1B	Intel i226	2.5GBase-T Ethernet 100/1000/2500 Mbit/s	Data network connection to the operating system when using N120 passthrough network.
Fabric 2A	No Connection	-	
Fabric 2B	No Connection	-	

Operating Systems

CoreStation nodes are shipped with an operating system installed for ease of deployment and setup.

Operating System	Version	Driver Pack	Status
Microsoft Windows 11 Pro	24H2	Available on Amulet Hotkey Resources website	Available pre-installed and supported for customer install
Ubuntu Desktop Linux	Ubuntu 24.04.2 LTS (HWE Kernel 6.11+)	Integrated in mainline kernel	Available pre-installed and supported based on customer requirements
Red Hat Enterprise Linux Workstation	RHEL 9.6+ RHEL 10.0+	Integrated in RHEL packages	Available pre-installed and supported based on customer requirements

Servicing and Maintenance

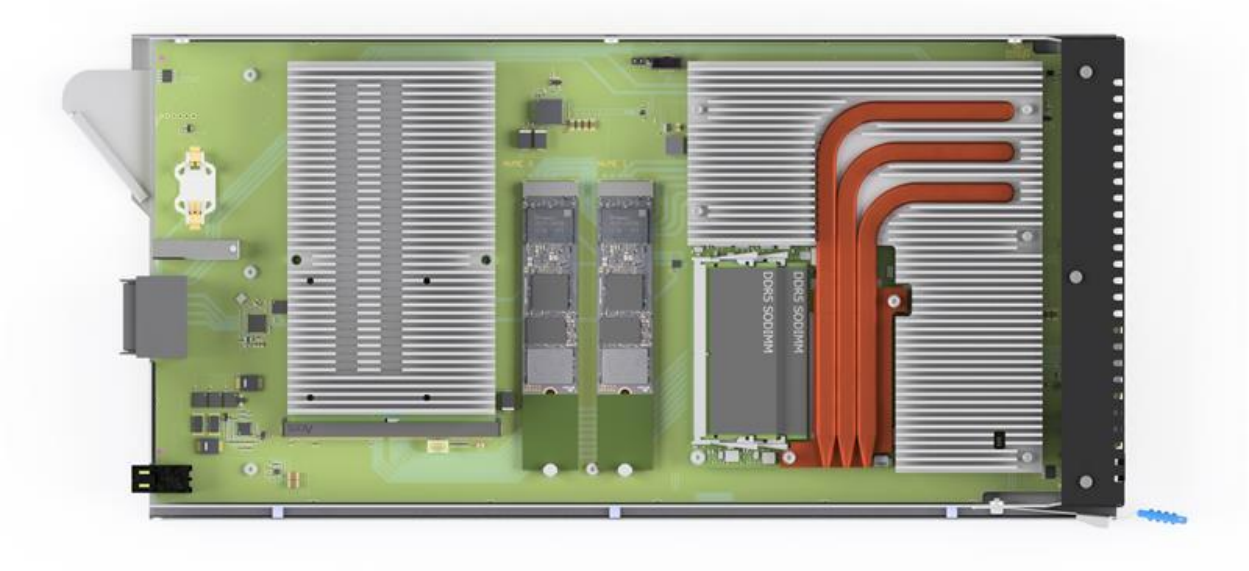


Figure 43 - HX2000 Workstation Node with discrete GPU

Replacement items are available from Amulet Hotkey as individual spares for customer use or as part of an on-site service contract.

Component	Details	Requirements
Storage	One or Two M.2 Flash-based storage devices for Operating System, Applications and User Data. For RAID 1 setup using two drives, it is recommended to use two drives of the same model and size. Located on carrier top-side	• Standard NVMe M.2 SSD in 2280 or 22110 form factors • PCIe Gen 3 or Gen 4 • PCIe interface width x4 • Max active power consumption 12W
Memory	Two modules providing primary CPU system memory. Populate both memory sockets using modules of the same type and capacity. Memory modules are fitted to the CPU module, one top-side, one bottom-side	• DDR5-5600 SODIMM (165H) • DDR5-6400 CSODIMM (285H) • non-ECC • Single Rank or Dual Rank • 8GB, 16GB, 32GB, 48GB or 64GB (285H only) capacity
RTC Battery	Coin cell battery to maintain system time when the node is not powered. The battery is expected to last for approximately ten years of normal operation or three years of un-powered storage.	• CR2032 Coin-cell battery • 20 mm diameter, 3.2 mm height • Nominally 3V, approx. 220 mAh capacity • Primary cell, not rechargeable

HX2000 Dimensions

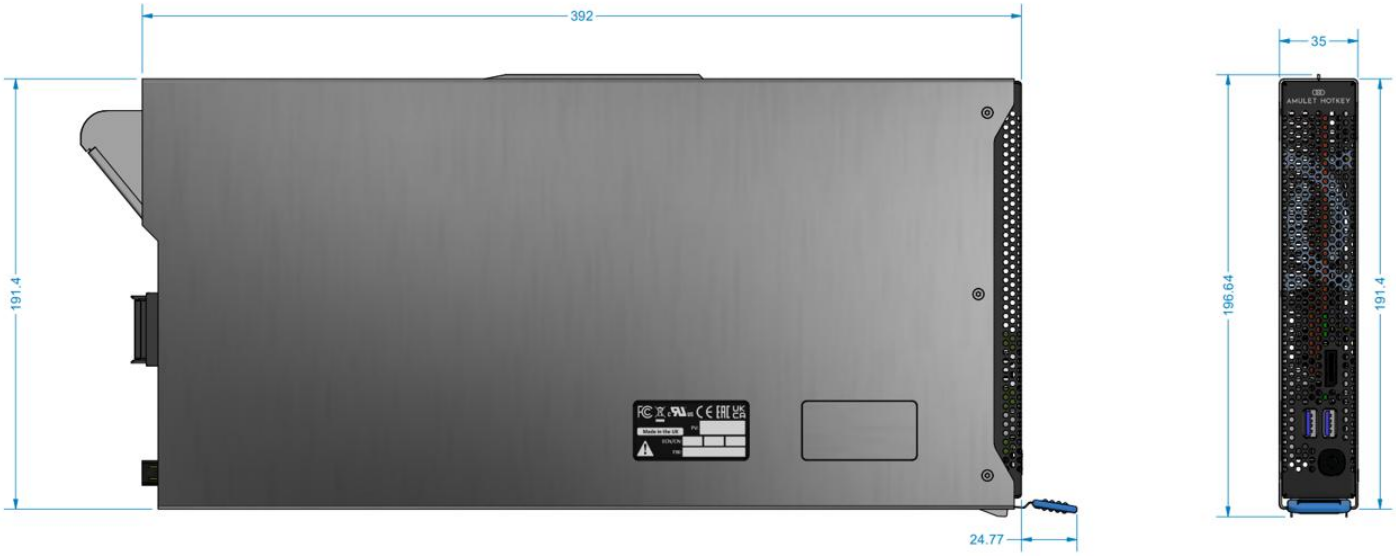


Figure 44 - HX2000 node dimensions

HX2000 BIOS Features and OS

HX2000 Nodes use AMI Aptio V UEFI firmware for the initial bootloader BIOS and system configuration. This works like the standard boot firmware on a desktop PC to initialise the system, load firmware for the CPU and provide boot devices.

Accessing the BIOS Setup Menu

The BIOS Setup menu is accessible via the front-panel ports on each node. Connect a keyboard and display, reboot the node and press <F2> when prompted.

The BIOS setup menu is like any desktop PC and is driven interactively by the keyboard to change settings and save to non-volatile storage.

BIOS Configuration Options

There are a larger number of possible settings and customisations available in the BIOS, some of which are exposed and some of which are pre-configured by Amulet Hotkey based on the design of the node.

The following settings are supported for customer configuration and persist through BIOS updates. These can be pre-configured in production to reduce the required configuration on-site.

Setting	Description	Options
Integrated Components	Advanced ⟶ Processor (Integrated Components)⟶	
Enable VMD Controller (VMD Setup)	The VMD RAID controller is a high-performance RAID controller integrated into the chipset to provide RAID 0 and RAID 1 with NVMe drives. Enable both settings to create RAID volumes on the two M.2 storage drives or disable if the drives should be used individually	• Enabled (Default) • Disabled
Enable VMD Global Mapping (VMD Setup)		• Enabled (Default) • Disabled
ECC Support (Memory Config)	When enabled, configures the memory to use in-band ECC. This reserves around 5% of the memory capacity and bandwidth for error checking and correction.	• Enabled • Disabled (Default)
Primary Display (Graphics Config)	Set the Primary display used for boot-time output. Hybrid Graphics is the preferred option for CoreStation HX to enable BIOS output on the front panel ports. Windows OS has independent settings to select the appropriate GPU for each application.	• Auto [Discrete GPU if available] • IGD [Integrated Graphics] • HG [Hybrid Graphics] (Default)
Internal Graphics Device (Graphics Config)	Enable or Disable the Integrated Intel Arc GPU in the CPU Package.	• Auto [Enabled] • Disabled • Enabled (Default)
Port 12 (x8 PEG)	Advanced ⟶ PCI Express Configuration⟶	
PCI Express Root Port 12 (x8 PEG)	Enable or disable the PCIe port connected to the MXM GPU.	• Enabled (Default) • Disabled
Config TDP Configurations	Advanced ⟶ Power & Performance ⟶ CPU - Power Management Control ⟶ Config TDP Configurations	•
Power Limit 1 (Custom Settings Level2)	CPU Package TDP Limit - Maximum power use for steady-state operation	Range: • Ultra 5/7 CPUs: 20W - 65W

		• Ultra 9 CPUs: 28W - 65W
Power Limit 2 (Custom Settings Level2)	CPU Package Turbo Power Limit - Maximum power use for short-duration peaks	Range: • Min: Power Limit 1 • Max: 115W
Power Limit 1 Time Window (Custom Settings Level2)	Duration for which the CPU Package power can exceed PL1 in a single burst. Also known as Turbo Duration.	Range: • Min: 0 (Turbo disabled) • Max: 128s (Default)
	Advanced→	
Wake on LAN Enable (PCH)	Allow the node to be powered up from sleep using Wake-on-LAN Magic Packets. Check if WoL packets are compatible with the intended network setup.	• Enabled (Default) • Disabled
USB Mass Storage Driver Support (USB)	When enabled, allows USB devices to populate the list of bootable devices. Only USB Mass storage devices which are formatted and written as UEFI-compatible can be selected as boot targets.	• Enabled (Default) • Disabled
UEFI Network Stack (UEFI Network Stack)	When enabled, allows PXE and HTTPS network boot modes to be selected as boot targets in the boot menu	• Enabled (Default) • Disabled
Security	Security→	
Secure Boot (Secure Boot)	If enabled, the BIOS will only boot to images which are signed with a valid key which matches those in the allowed list (db list). When disabled, BIOS will boot any UEFI compatible image.	• Enabled (Default) • Disabled
Secure Boot Mode (Secure Boot)	Standard – Use the default AHK Secure Boot keys, allow list (db) and exclude lists (dbx). Custom – Use customer-specific Secure boot keys, lists and settings	• Standard (Default) • Custom
Secure Boot Keys (Secure Boot)	Option to upload customer-specific Secure Boot keys (PK, KEK, DB and DBX). Factory defaults are AHK keys.	• Factory Keys (Default) • Custom keys
Boot	Boot→	
Power Loss Control	Action to take when power is restored. Typically, the result of sudden loss of power to the enclosure	• Remain Off • Turn On • Last State (Default)
Boot Priority Selection	Selects the order to try boot devices.	• Local Disk • Local RAID Volume • USB Mass storage • HTTPS (If enabled) • PXE (If enabled)
USB Support	When enabled, allows USB devices to populate the list of bootable devices. Only USB Mass storage devices which are formatted and written as UEFI-compatible can be selected as boot targets.	• Enabled (Default) • Disabled
Network Stack Driver Support	When enabled, allows PXE and HTTPS network boot modes to be selected as boot targets in the boot menu	• Enabled • Disabled (Default)

BIOS firmware updates

The BIOS update package is a collection of firmware for different elements of the CPU, GPU and chipset as well as the BIOS Setup menu and UEFI boot firmware. These are all updated together as part of the BIOS firmware update tool running from Windows.

Following a BIOS update, only some settings are preserved, others are reset to defaults.

Refer to the BIOS update KBA for further information about BIOS updates.

OS Deployment

There are several supported routes for OS deployment:

Route	OS Installation	Description
Windows Autopilot	AHK factory	Windows 11 Pro Pre-installed with hardware hash ready to upload to Microsoft Intune for cloud management
Manual Setup	AHK factory	Windows 11 Pro pre-installed with standard Out-of-box experience for manual setup or on-prem domain join
PXE/HTTPS	Using WinPE via Microsoft MDT or TFTP/HTTPS server	Customer image installs using PXE boot. Requires HX2000 pre-install driver pack for network and RAID drivers.
USB	Using .wim or WinPE from local USB media	Customer image installs using local USB ports on the node. Requires HX2000 pre-install driver pack for network and RAID drivers.

Windows OS Settings and Customisation

HX2000 requires some specific OS customisation to operate correctly with the Management Controller and out-of-band management functions.

Customisation	Description
HX2000 Baseline driver pack	• Latest validated drivers for all system components
HX2000 GPU Drivers	• Latest drivers for Intel integrated GPU and NVIDIA discrete GPU (if fitted)
HX2000 BIOS (CGOS) Capsule driver	• Enables BIOS firmware updates from Windows with Secure Boot enabled
CoreStation Agent	• Install the CoreStation Agent to provide richer integration with the Management Console
HX2000 Power and sleep settings	• Disable Fast Boot, Hibernation • Disable sleep and screen lock

Security Features and Best Practice

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.

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 • Disable unused switch ports	• 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 resources page	• Make sure the system is running the latest security patches and fixes • Avoid exposure to known vulnerabilities

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

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.

Specifications and Compliance

Dimensions

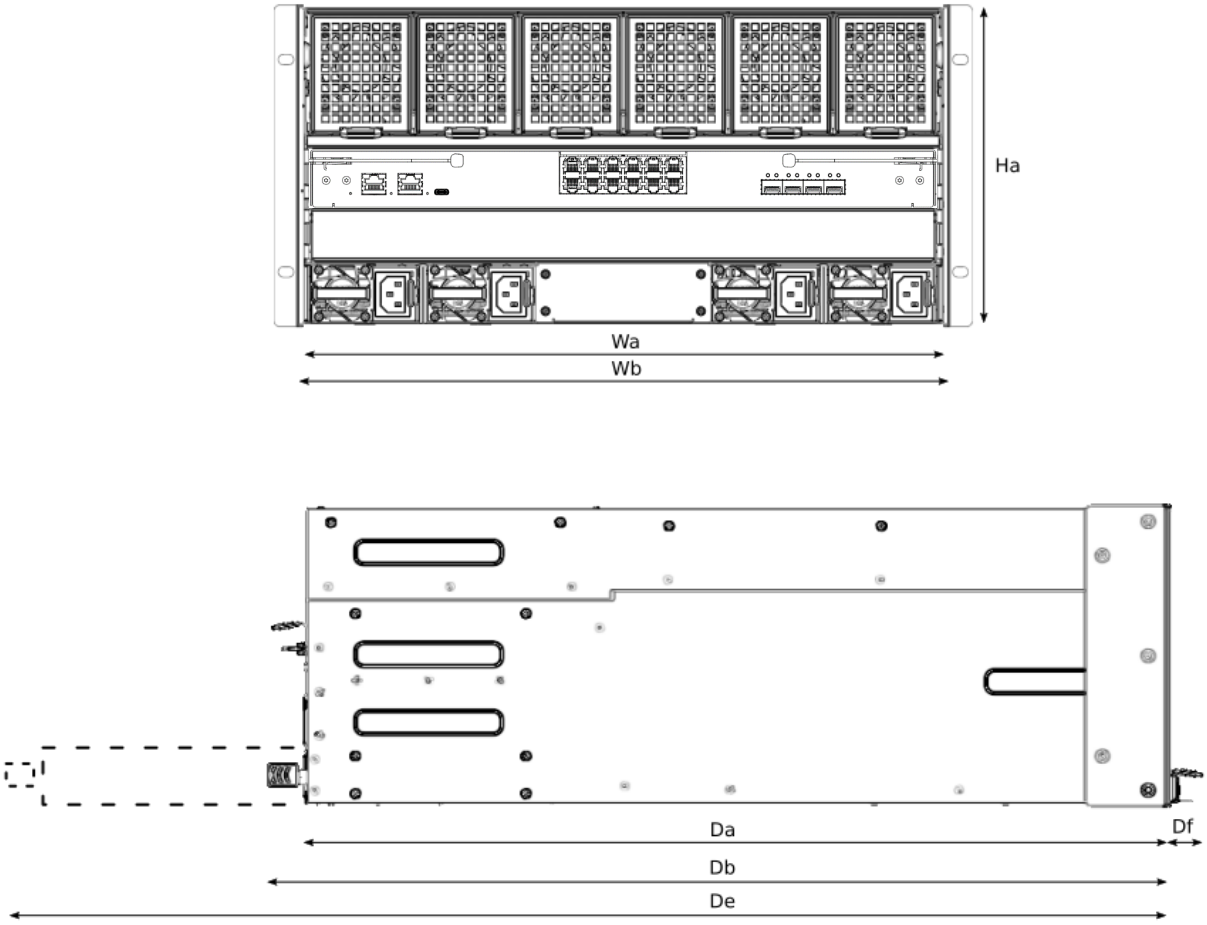


Figure 45 - CoreStation HX enclosure dimensions

Symbol	Description	Measurement
Da	Depth of system enclosure	602mm / 23.7in
Db	Depth to furthest point (PSU handles)	627mm / 24.7in
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

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.		

Weights

Empty enclosure: 12.2 kg (26.9 lbs)

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

HX2000 Workstation Node with integrated GPU: 3.0 kg (6.6 lbs)

Fully populated system: 59.4 kg (131 lbs)

Fully populated shipping weight: 72.0kg (159 lbs)

Resources
https://amulethotkey.force.com/support/s/resources

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