AMULET HOTKEY

UM

Amulet Hotkey CoreStation HX5

Management Console User Manual

Contents

Version 1.0

1. Introduction

1.1 Management System Overview

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

- 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

1.2 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

1.3 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 Windows 11 Pro to report dynamic details.	• OS State reporting • Network connectivity • IP Address and hostname • Driver versions

2. Accessing the Management Console

2.1 Accessing the Management Console using web browser

The Management Console can be accessed using a web browser 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 Ubuntu 24.04

2.2 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.

2.3 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 (port 443) and will re-direct all HTTP (port 80) access to the HTTPS version of the login page.

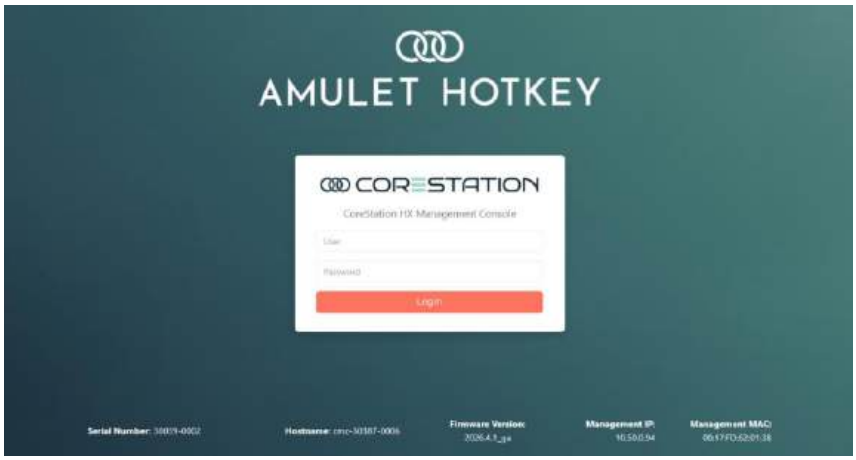


Figure 1 - Management Console Login Screen

2.4 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 permissions on their local machine to dismiss the browser warning and continue to load the page.

2.5 Default login credentials

The system ships with a unique default password which 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.

3. Enclosure Information and Status

3.1 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.

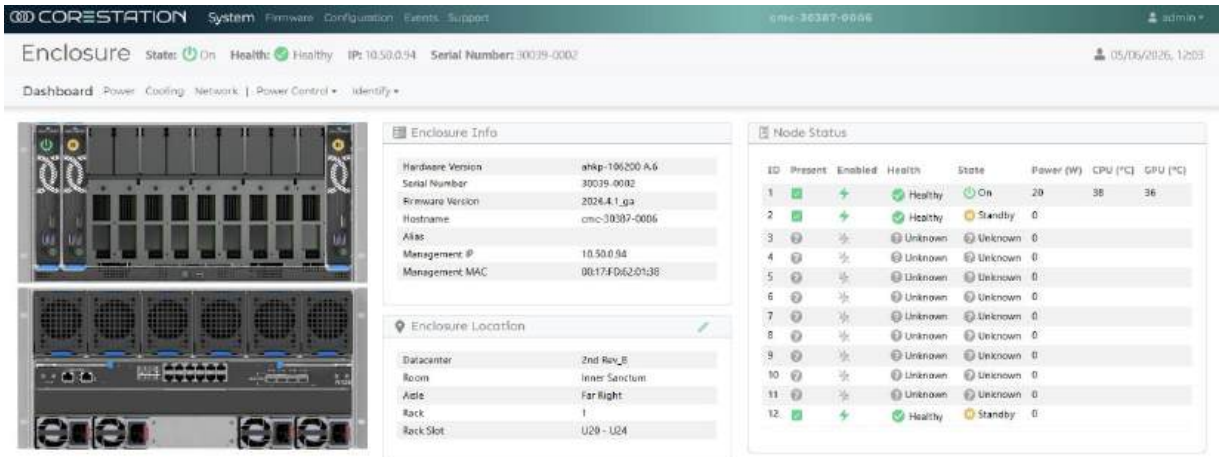


Figure 2 - Management Console System Dashboard

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. **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 **Degraded** - 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 (if a discrete GPU is fitted)

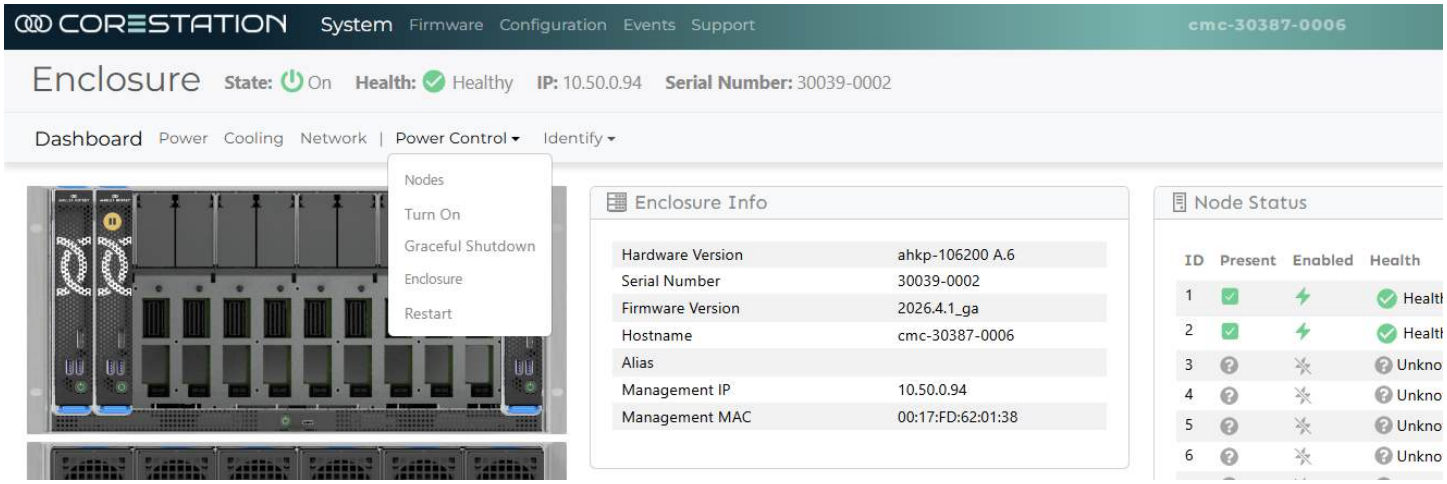


Figure 3 - Dashboard Power Actions

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. This also restarts the internal network switch and interrupts node network connections using the switched ports via the SFP connections, but it does not restart the nodes.
Action - Identify	• Flash the Enclosure LEDs in order to identify this system Enclosure to a technician who intends to work on this system.

3.2 Power System

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

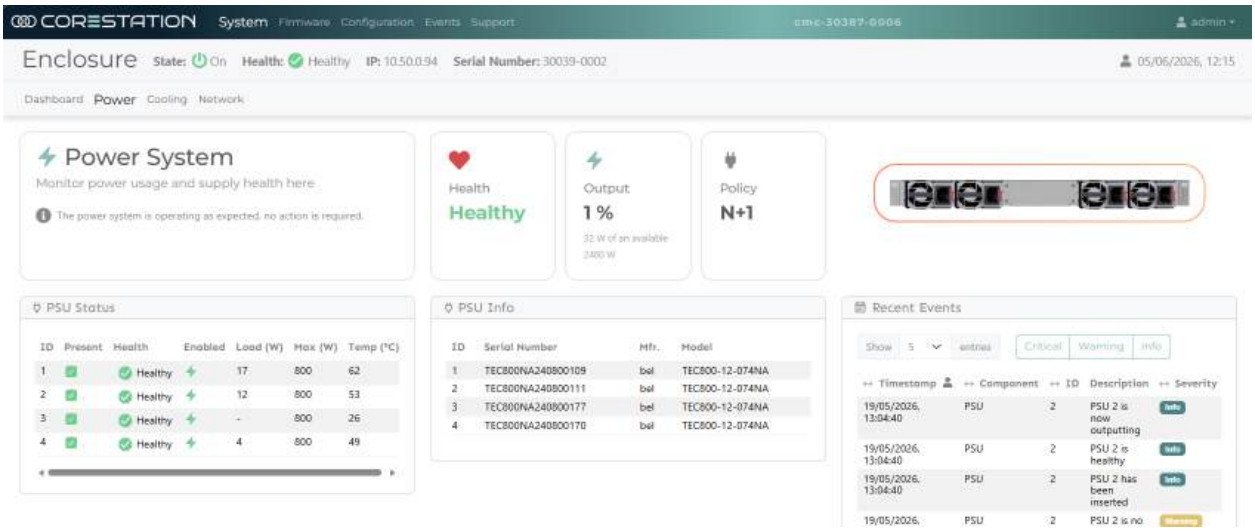


Figure 4 - Power System

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 • N+2 – Loss of two PSUs will not affect system operation, typically when the PSUs are connected to two separate power feeds.
Recent Events	List of recent events and log message related to system power and PSU modules.

3.3 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 operating temperature. Contact Amulet Hotkey to verify the deployment environment for a specific system configuration before install.

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.

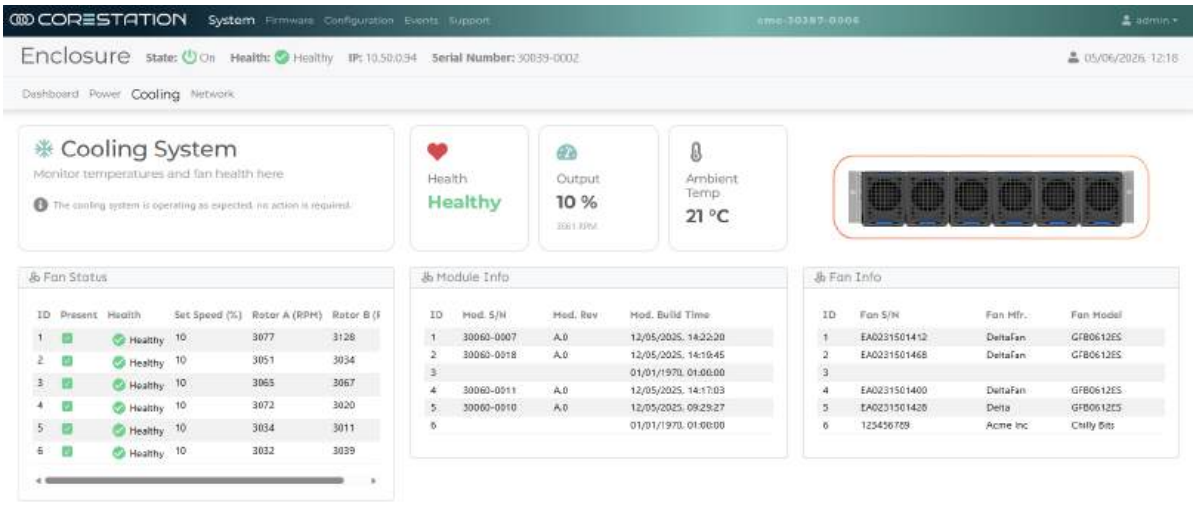


Figure 5- Cooling System

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

3.4 Fan Control Mode

The fans default to automatic mode in which the fan speed increases in response to the temperature of the nodes, but they can alternatively be set to manual mode where the fan speed stays fixed, regardless of the node temperature. Automatic mode is the best choice for typical deployments, but fixed mode is useful when the enclosure is temporarily operated in environments where noise is a concern, such as an IT test lab.

When running in fixed mode at a low speed, the nodes may overheat and throttle back which can reduce their overall lifetime. As such, fixed mode is not recommended for production deployments.

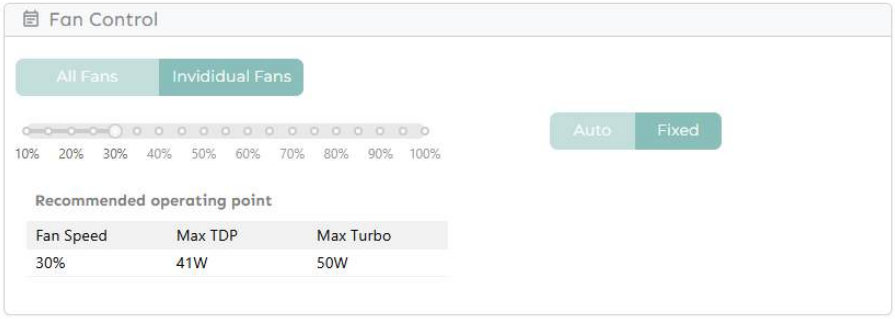


Figure 6 - Fan Control dialog

Control Item	Description
All Fans/Individual Fans	Sets the Fan Control dialog for common (Single slider, controls all fans) or individual (six sliders, one for each fan)
Auto/Fixed	Sets the Control Mode for the fans – Automatic or Fixed mode
Speed Slider	When in manual mode, sets the speed of the target fans in 5% increments relative to the maximum possible speed for each fan.
Recommended operating point	Provides an indication of the continuous power draw which can be successfully cooled at this fan speed. This is for information only and does not affect any node configuration.

3.5 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 7 - 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, 1G, 2.5G, 10G –** Port active and operational
Link Aggregation (LAG)	Configuration for Network Uplink ports on N120: • Disabled – Uplink ports are not active • Enabled – All four uplink ports are configured as a single link aggregation group Live network link status for the uplink ports on the N120 • Present – Is an SFP module fitted to this port • Link Speed – Live link status and speed reported for this port **DOWN** – No link detected **UNKNOWN** – No link speed reported by the SFP Module **1G, 10G** - Port active and operational
Recent Events	List of recent events and log message related to system network and management

4. Firmware information and updates

4.1 Firmware Status

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

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

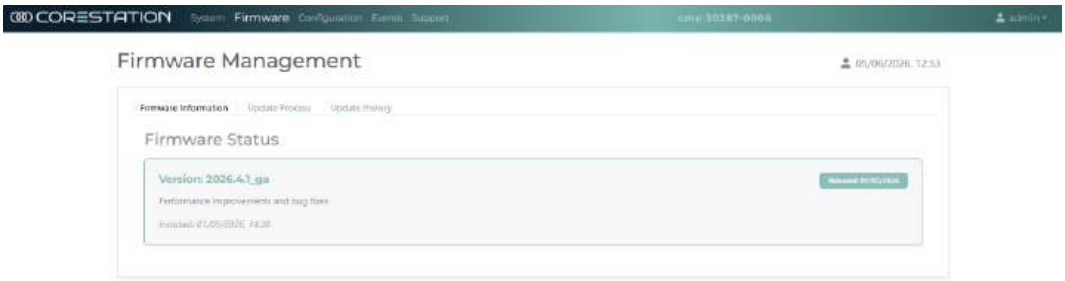


Figure 8 - Firmware Information

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 NIC/SSD Firmware	Updated using AHK Firmware update application, deployed via the OS

4.2 System firmware updates

Amulet Hotkey regularly release updated management firmware for CoreStation HX, and this is made available on the Amulet Hotkey 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.

See Knowledge Base Article (KBA 224) for details of the firmware update process and a step-by-step guide.

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 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 9 - 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. The firmware update will update dialog will not proceed unless the nodes are all in the Standby power state.

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

4.3 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 downgrade to a previous version using the same process as an upgrade.

Amulet Hotkey recommend running the latest GA firmware version in production which may contain critical bug fixes.

Figure 10 - Firmware History

5. System Configuration

5.1 Management Network Configuration

The network settings for the Management Controller can be configured either from the serial port or from the Management Console. Typically, DHCP or Static IP assignment would be configured from the serial port during initial deployment as this may be required before the Management Console can be accessed over the network.

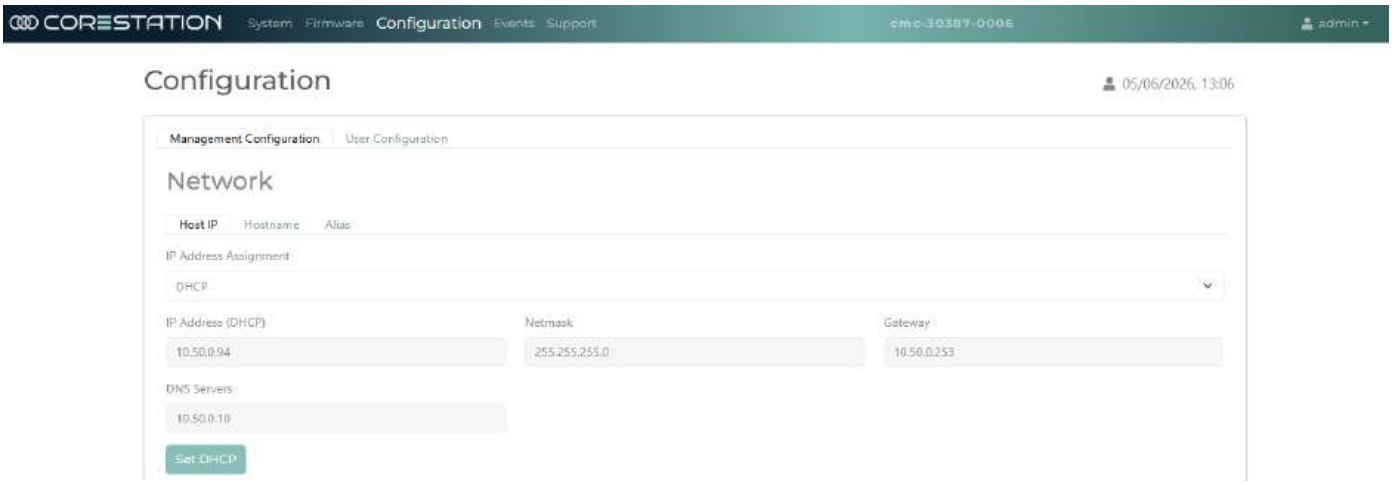


Figure 11 - Network Configuration

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 12 - Hostname Configuration

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

5.2 System time

The Management Controller contains a battery-backed Real-Time clock which 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 13 - 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.

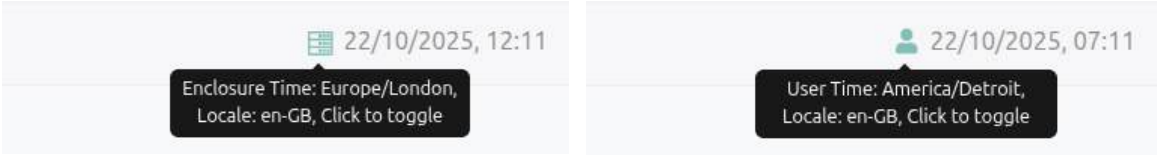


Figure 14 - Display time toggle

5.3 TLS Certificates

The TLS certificate is used by the Management Console website to authenticate and encrypt the connection between the CoreStation HX web server and the client's browser. 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.

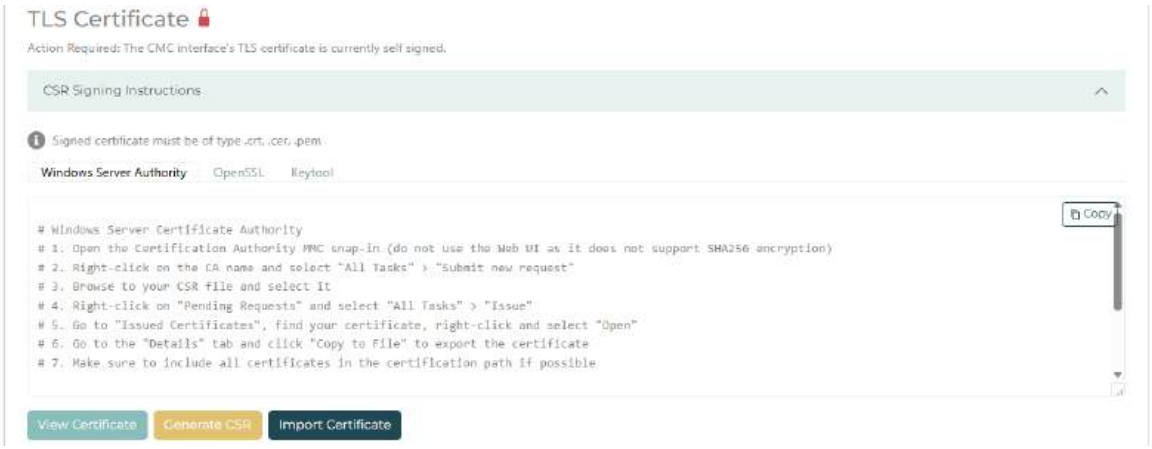


Figure 15 - HTTPS Certificate export and import

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”

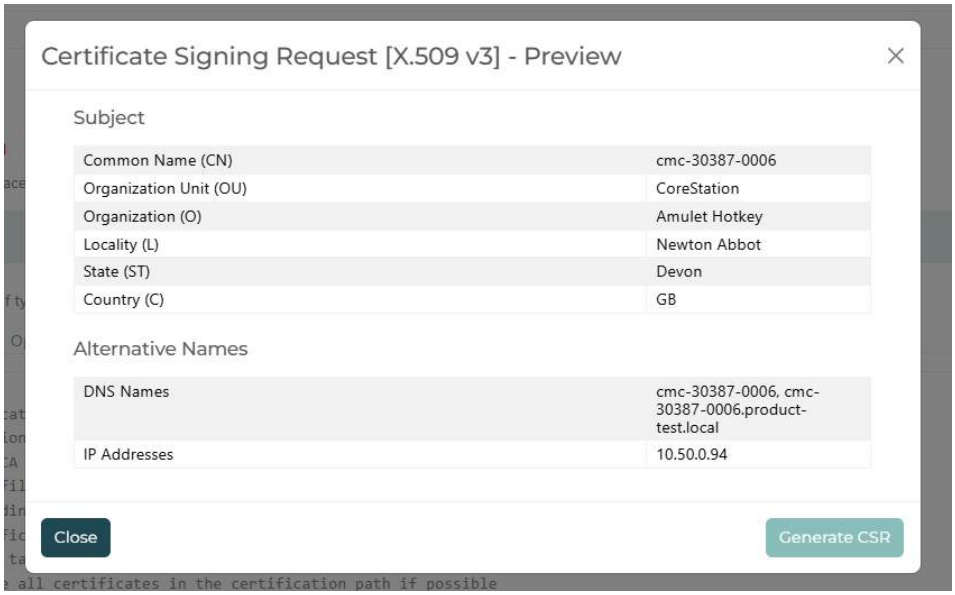


Figure 16 - CSR Export dialogue

If the new certificate correctly matches the CSR export, the new certificate will replace the existing self-signed certificate, all users will be signed out, and the management controller will restart. Any running Nodes will remain operational, but there will be a temporary interruption to network connections using the internal switch via the SFP interfaces.

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

The TLS/SSL certificate can be reset to the factory-issued self-signed version by confirming “Reset Certificates” or by following the Factory Reset process.

5.4 Remote Console

This controls access to the Remote Console feature for all users and all nodes together. If this is disabled, the Remote Console feature is not available. If enabled, the Remote Console is enabled on all nodes, and access is based on the user role.

5.5 Factory Reset

The Factory Reset function erases the Management Controller configuration and returns the system to the state and firmware version 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 30 minutes to complete, and the Management Console will be unavailable during this time. Once the process is complete, the firmware should be upgraded to the latest released version to ensure all features are available and bug fixes are applied In some cases, Nodes may not be operational until the firmware has been updated from the Factory Reset Version to a more recent release.

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 Management Controller	The version that was installed at the time of Enclosure Management Controller manufacture
Node	No change to Node OS, BIOS or configuration

5.6 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 17 - Access control for serial and SSH access

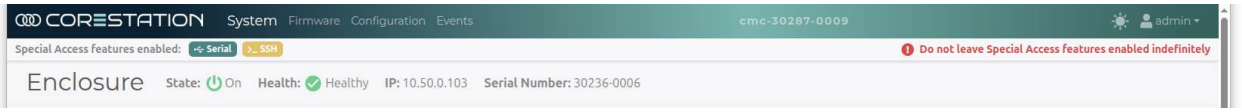


Figure 18 - Banner showing Serial and SSH features enabled

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

6. User Configuration

6.1 Local user configuration

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

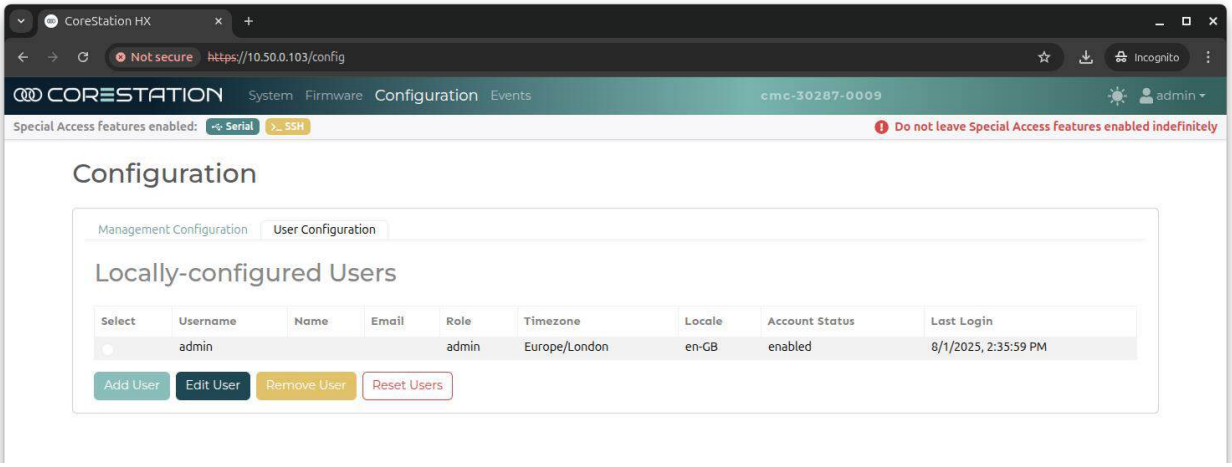


Figure 19 - Local user Configuration

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).

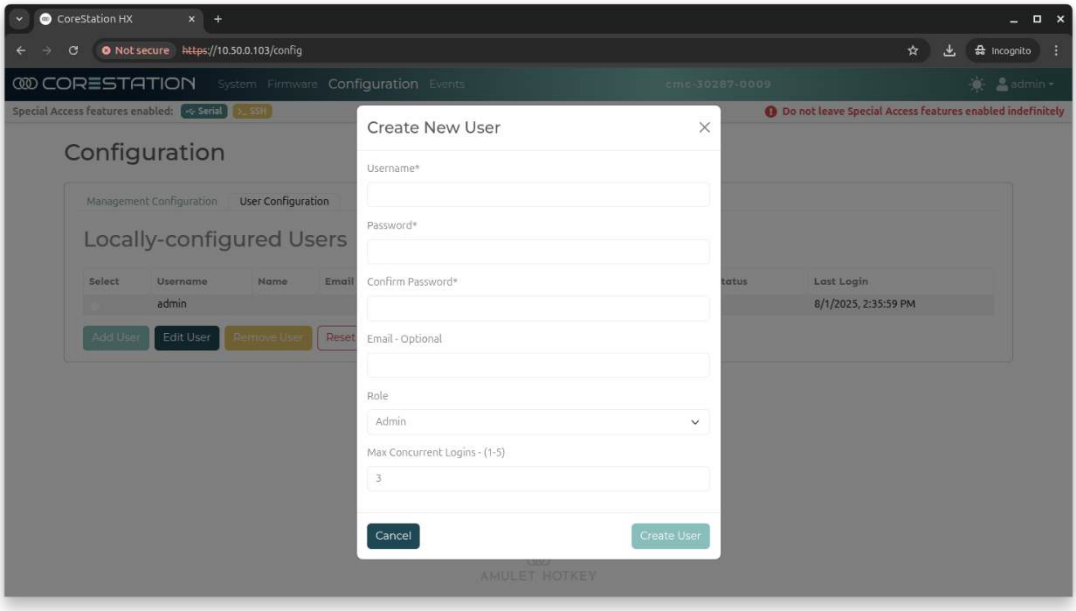


Figure 20 – New User dialog

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.

6.2 Domain user setup with LDAP

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.

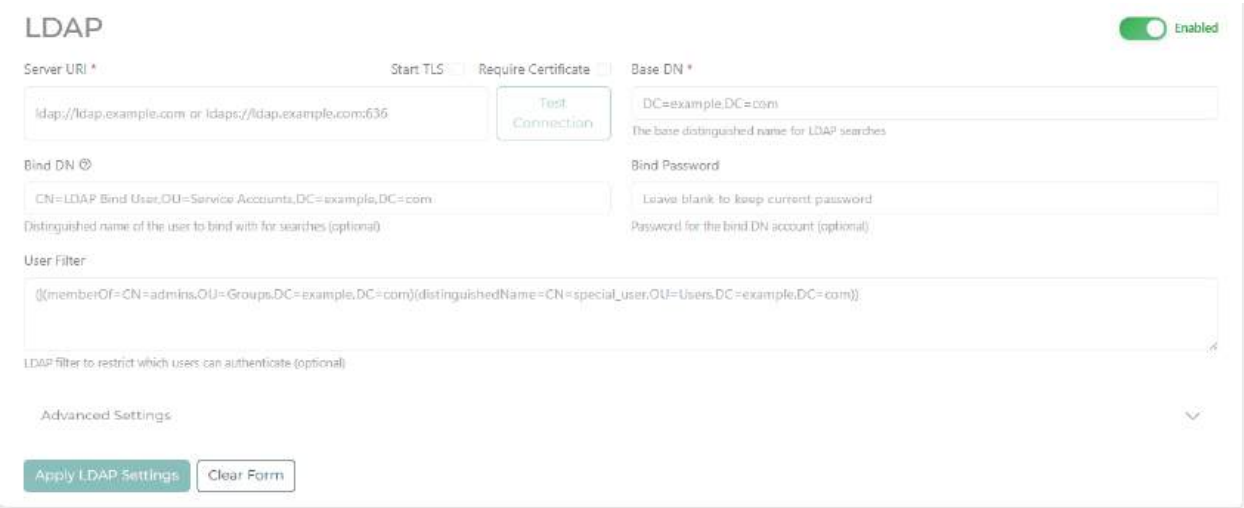
The Management Controller user list maintains an entry for every user who has successfully authenticated via LDAP and keeps track of their last login and user role.

LDAP Settings

Configuration path: Management Console web > Configuration > User Configuration tab.

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.



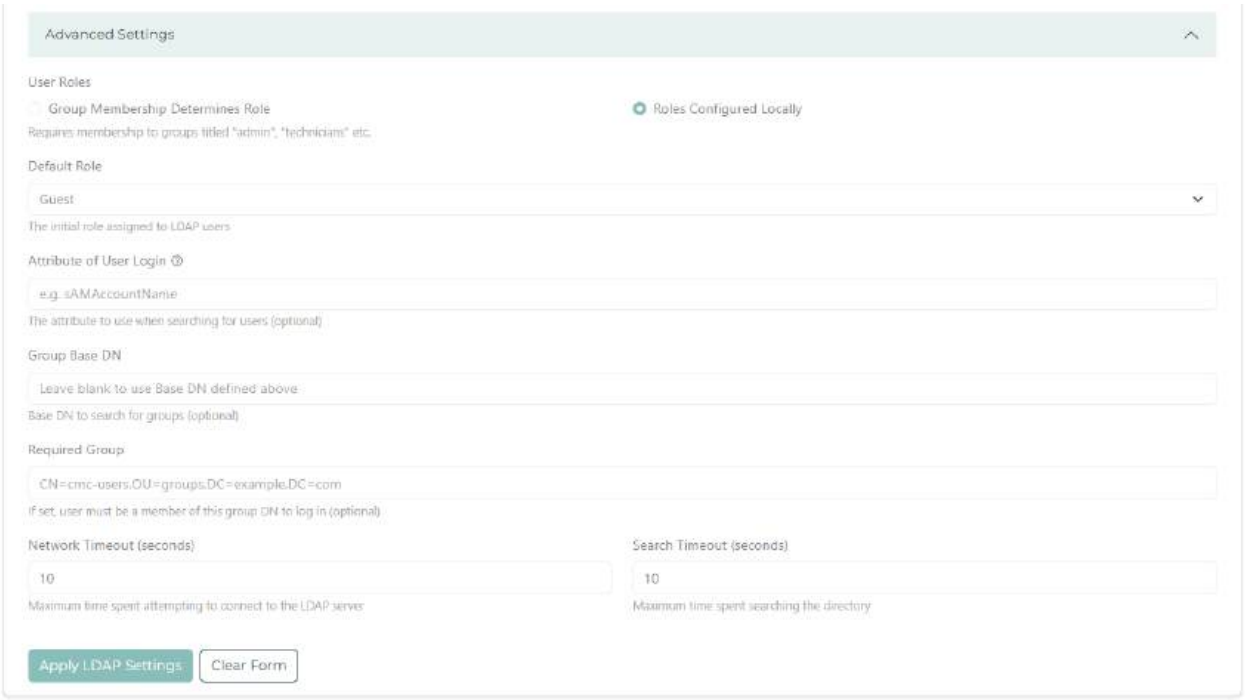
Advanced LDAP Settings

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.



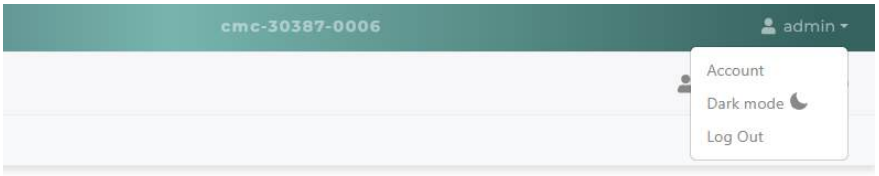
6.3 User Roles and access restrictions

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	Limited day-to-day access operations	View information only
System	Full Access	Full Access	Limited	View Only
Node	Full Access	Full Access	Limited	View Only
Remote Console	Full Access	Full Access	Not available	Not available
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)

6.4 User Menu

The user menu is shown on all pages of the Management Console in the top right corner.



Account Settings

Link to the account settings page for the current user showing their details and provides means to edit a subset of their information if the user is a local user. For LDAP/directory users, this page is for information only, any changes must be made on the central corporate directory

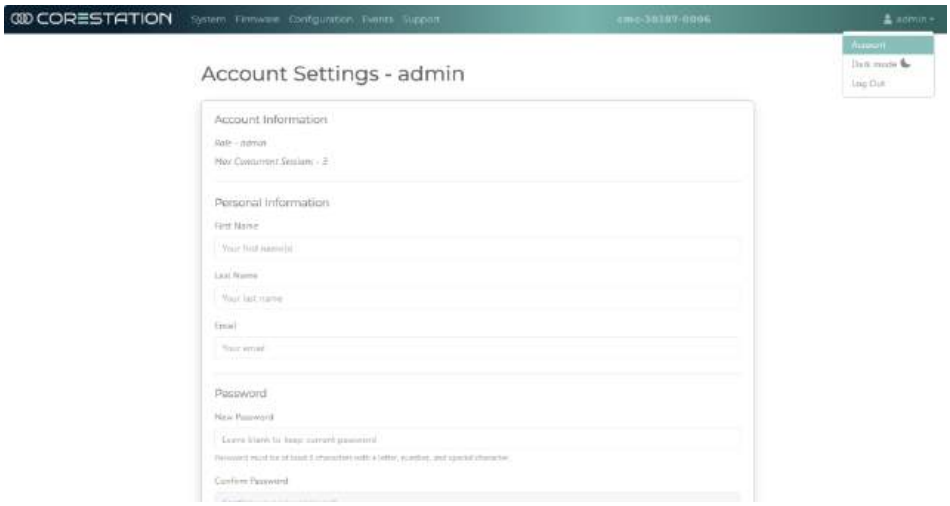


Figure 21 - User account settings

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.
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

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 22 - Light mode

Figure 23 - Dark Mode

Logout

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

7. Node Management

7.1 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.

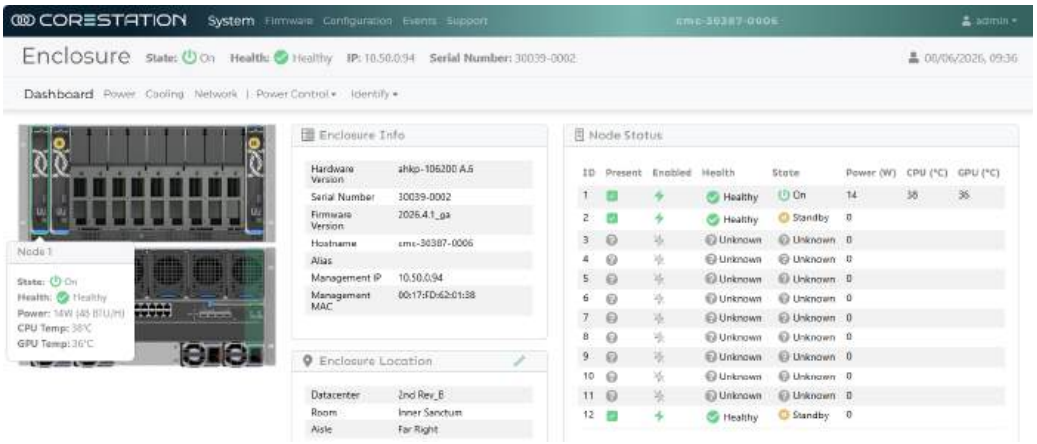


Figure 24 - System Dashboard with node 1 hover-over

7.2 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.

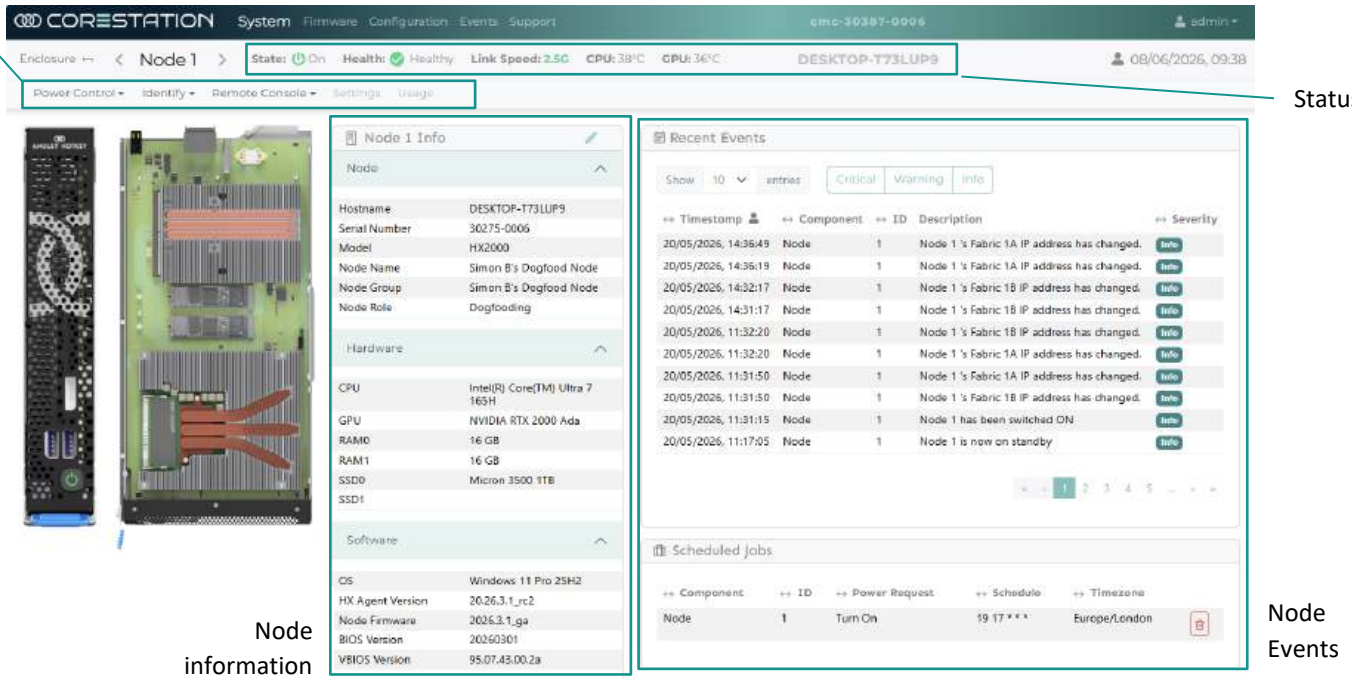


Figure 25 - Node page

Node Status Information

This status information is reported live and gathered out-of-band from each node, with the exception of hostname which requires the CoreStation HX Agent to be installed. The CPU and GPU temperatures are shown live without any averaging or filtering, so give a real-time view of the node health and status.

Node Status item	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 **Degraded** - Minor issue, slightly affecting performance **Error** - Major issue, seriously affecting performance or functionality
Link Speed	Current network link speed for this node. If the node has multiple active network connections, this will report the highest individual speed. Possible values include **DOWN**, **100M**, **1G**, **2.5G** and **10G**
CPU	Live CPU package core temperature
GPU	Live GPU core temperature, only shown when a discrete GPU is fitted.
OS Host Name	Current or last known hostname for the Operating System on this node.

Node Action Bar

The Node Action Bar provides a way to perform actions which would be typically performed in front of a physical desktop.

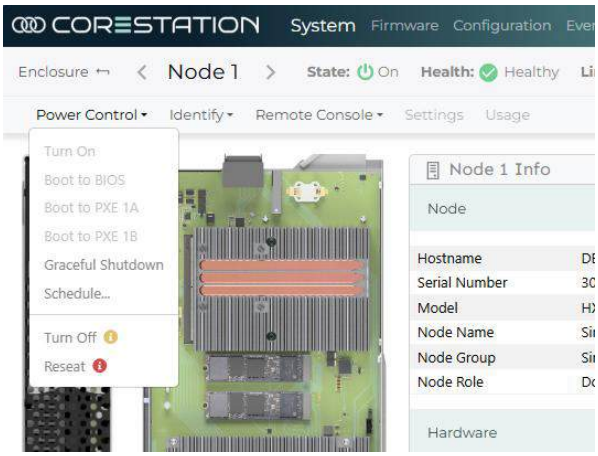
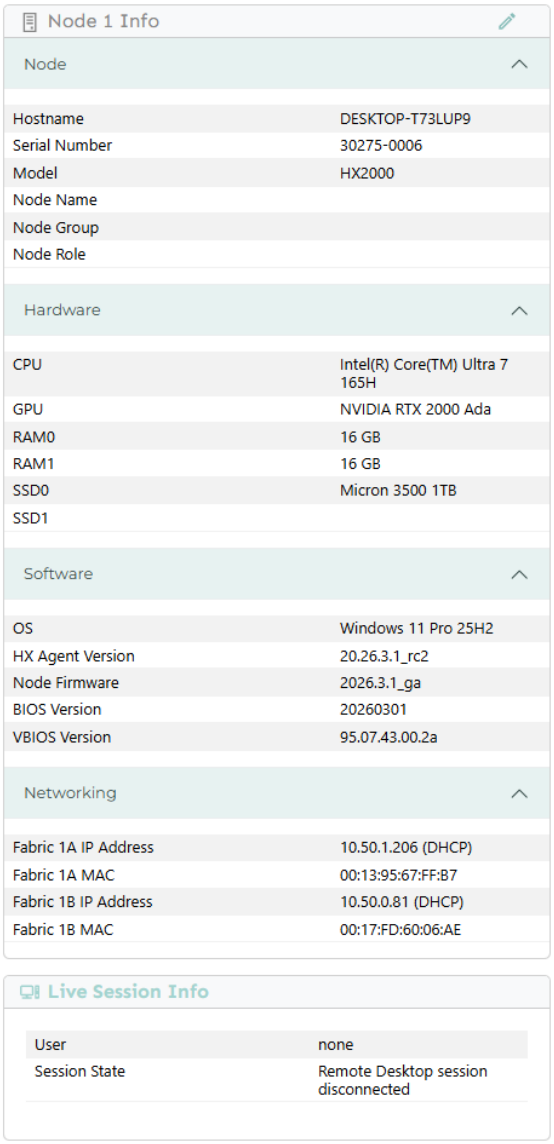


Figure 26 - Node Action - Power Control Menu

Action Menu	Description
Power Control	Provides power control for this node. All the actions to turn off and restart a node ask for confirmation before performing the action to avoid accidental interruption to a user session. **Turn On** - Initiates the power-up process on this node. Only available if the node is currently powered-down. This is equivalent to pressing the power button on the front of a physical desktop **Boot to BIOS -** Turns the node on and boots to the BIOS Setup menu to allow configuration of individual settings, view information and select a boot device. Each node uses a unique BIOS admin password, so it is not possible to access the BIOS setup menu using other routes. **Boot to PXE 1A/ Boot to PXE 1B -** Turns the node on and initiates PXE boot using Fabric 1A or Fabric 1B network connection. The node will contact the DHCP server and report as an EFI x64 client (Opt 93) with PXEClient:Arch:00007:UNDI:003016 vendor class (Opt 60). It will then attempt to download and execute an image from the server provided in options 66/67. **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. This is equivalent to a short press on the power button of a physical desktop. **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 physical desktop. If this action is performed repeatedly, the OS may enter a recovery state or experience data 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 whilst the OS is running, the OS may enter a recovery state or experience corruption. This is similar to pulling the power cord on a physical machine.
Identify	Blink 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** B**linking** – Stop the identification and revert to the standard LED indicator The blinking state is reflected in the system Dashboard.
Remote Console	Open a Remote Console KVM session to this node for interactive control with video, keyboard and mouse access. This opens a new browser tab and connects to the node using an HTML5-based video session running completely within the browser This feature is intended for interactive Operating System install, repair and diagnosis of issues, rather than daily interactive use so the resolution, frame rate and colour accuracy are limited.

Node Information



Static Node Information

This information is gathered from the Node out-of-band and is available without an OS installed.

- Serial Number
- Node Model
- CPU Model
- GPU
- Memory (RAM)
- Storage (SSD)
- Network MAC addresses for each interface
- Node firmware
- BIOS version
- VBIOS version

Static

These are free-text fields for customer use. The content is stored on the node and moves with the node if it is removed.

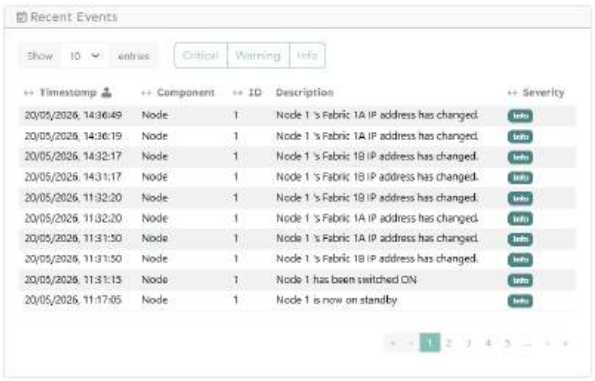
- Node Name
- Node Group
- Node Role

Dynamic Node Information

This information is provided by the CoreStation Agent whilst the node is operating. The CoreStation agent is supported on Windows 11 only.

- HX Agent Version
- Hostname
- Operating System and Version
- IP Addresses for each network interface
- User – Username of the current login session
- Session State – Current Windows session state for this node

7.3 Node Events



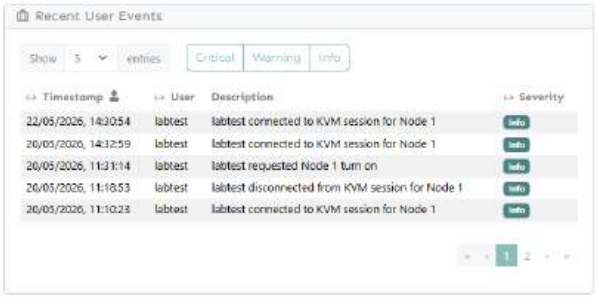
Recent Events

This includes all observed state changes relevant to the node whether they were the result of an identifiable user action or physical interaction with the enclosure.

- Power On/Off
- Health Status for Node
- Insertion and Removal
- Enable and Disable
- Automated Node provisioning and configuration
- Changes in node network state, speed or IP address

Scheduled Jobs

If any scheduled tasks have been created for this node, they are shown here with brief details. The schedule field shows short-form cron-style notation, in the attached example, the node will turn on at 17:19 every day.



Recent User Events

This shows actions related to this node which can be attributed to a user, including:

- Power, identify and reseat actions
- Remote Console session start and stop
- Scheduled event creation

Node events are recorded in the event logs based on the action and the outcome and all events relating to node will be shown on the relevant node page, the Dashboard page and in the system-wide event logs.

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)

The events are recorded at the time they happen, so a jobs event for power action is recorded as the user clicks on the action, but the resulting change in power state typically happens a few seconds later and the event is created at that time. Some actions such as graceful shutdown can take several minutes to complete depending on the OS response, so the event for recording the power action job and the event acknowledging the changed power state would be recorded with that delay.

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
Assign/Change node IP or hostname	Node 1 's Fabric 1A IP address has changed.
Network Link Status Change	CoreStation - Node 1 - Fabric 1A Link UP CoreStation - Node 1 - Fabric 1A Link DOWN
Session Login/Logout/Lock	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

7.4 Scheduled Job creation

The Node Action Bar -> Schedule… action allows power actions to be run automatically based on a defined schedule. This can be used for operations such as turning all Nodes off at night to save power, forcing a restart to ensure OS updates are applied out of hours or scheduling work to happen when the enclosure is quiet. All scheduled jobs are setup as recurring forever, so if a single run is required then the scheduled job must be deleted once it is completed. All times and dates in this dialog use the enclosure time zone, rather than the current user time zone.

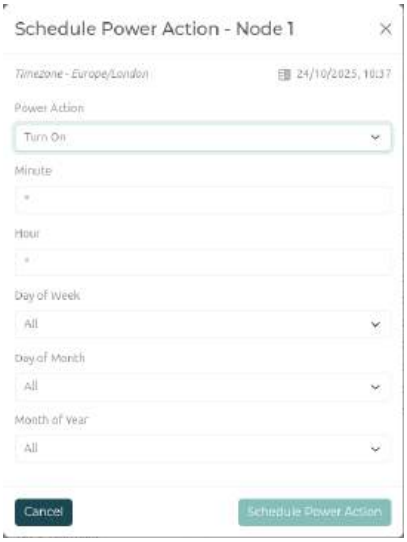


Figure 27 - Schedule dialog

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 of the day or use * 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. In this case the task would generate the same error or warning as trying to perform the action directly, if the node is already powered on then the scheduled task would be considered successful and generate no further events

7.5 Automated Provisioning and Configuration

When a Node is first inserted into an Enclosure, there is an automated process to setup and configure the Node to match the Enclosure. This process takes several minutes, during which the Node is not available for use and Power actions are disabled. During this time, the Provisioning progress bar is displayed with a progress counter and at the end of the process, there is an event to confirm the outcome. If the process is interrupted part-way through then it will restart again when the node is next inserted.

Part of this process configures a unique BIOS Admin password for each Node which is securely stored in the Node Management Controller. This password is entered automatically when using the *Boot to BIOS* power action on the node page, but not if a user directly enters BIOS Setup by another route.

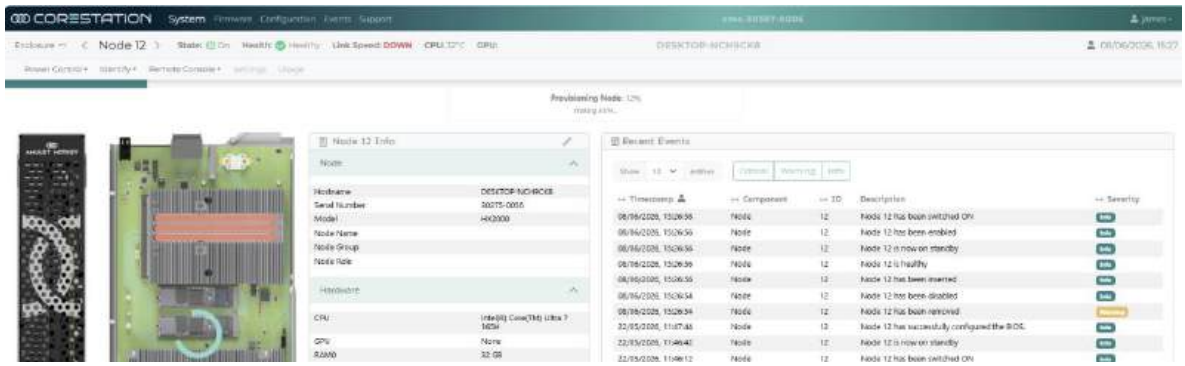


Figure 28 - Node Provisioning

8. Remote Console

The Remote Console feature provides direct access to each Node providing KVM (Keyboard, Video and Mouse) within the Management Console browser session. This feature is intended for installation, configuration and fixing issues, particularly when it is not possible to use OS-native remote access routes such as RDP. The Remote Console feature operates at the hardware level and so works without any Operating System installed, allows access to the BIOS setup and operates even when the node has no network connection.

There is an enclosure-wide setting for Remote Console on the Config page which defaults to Enabled.

8.1 Launching Remote Console

Remote Console is available to users with the Admin and Technician roles and is launched from the Node Action Bar on the Node page and opens in a new tab. It is possible to start the Remote Console session when the Node is turned off, but there will be no visible output until a Turn On action is sent.

1. Launch Remote Console KVM from Node Action Bar

Figure 29 - Launching Remote Console KVM

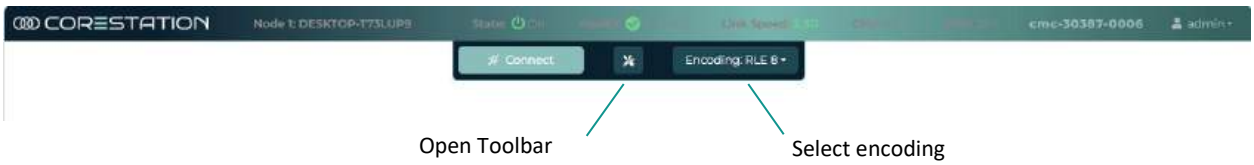
2. Remote Console showing new tab on the pre-connect screen

Connect – start the Remote console session to the node

Toolbar – open the in-session toolbar for hotkeys and virtual media

Encoding – Provides options for session colour depth - Use RLE8 for lower bandwidth connections and RLE16 when more bandwidth is available for higher colour accuracy.

Pressing the Connect button starts the KVM session to the Node and records an event in the user events log.



3. In Session

Once connected, the Remote Console session behaviour is very similar to a physical desktop PC with a locally-connected monitor, keyboard and mouse. As such, the KVM session would typically boot to a Windows login screen and require the user to authenticate using the username and password of a valid user on that desktop. If there is another user already using that Node, then Windows will display a message to warn that the existing user will be logged out if the new login goes ahead.

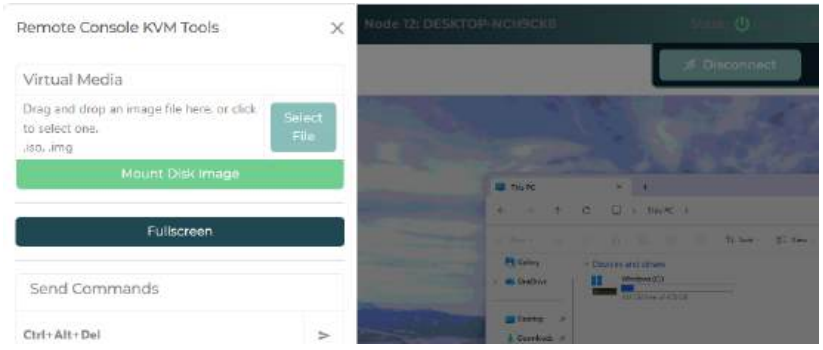
If a Remote Console session is disconnected whilst the Windows user is at the desktop, then a subsequent Remote Console session will bypass the login screen and connect straight to that desktop with the same user account. This is the same behaviour as walking away from a physical machine, so it is recommended to sign out or lock the OS before terminating the Remote Console session.

To end the Remote Console session cleanly and generate an event, click the Disconnect button in the Remote Console window. If the tab is closed without disconnecting, other users may be blocked from starting Remote Console on this node for up to 30 minutes and the event log entry for session disconnect will not be generated.

8.2 Virtual Media, Fullscreen and in-session keys

Virtual Media

Remote Console Virtual Media is a method to share files with the Node OS when there is no network connection, or the files are not easily accessible via typical routes. This is especially useful for installing key system drivers or loading client certificates that may be required to enable a working network connection.



The Virtual media dialog in the in-session toolbar accepts disk images in standard .iso format and works well with images up 250MB in size. Larger images can be used, but access can be slow and less reliable, especially on a low-bandwidth connection.

To mount a disk image, use the *Select File* button to choose an ISO file from the local machine, then click *Mount Disk Image* to connect the selected image to the target Node.

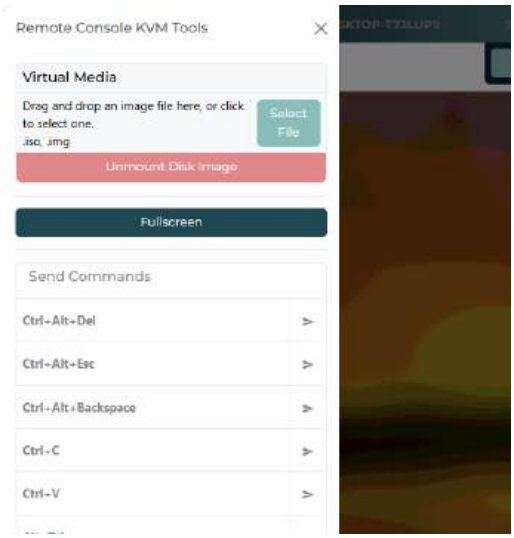
The disk image shared using virtual media appears as a CD-ROM drive to Node OS and is accessible in file explorer like any other drive. The disk image is mounted read-only, so the Node OS can copy files from the disk to the local machine, but files cannot be written back to the virtual media disk.

Fullscreen

The Fullscreen button expands the video window to use the full display of the local user's desktop. This is useful when working with small text or highly detailed information if there are issues when viewing the content in a scaled window.

To exit full screen mode, press <Esc>

Combination Key Commands



The In-session tool bar provides a dialog to send specific keyboard combinations to the remote session which would otherwise be captured and interpreted by the local OS of the user who is accessing the Management Controller.

The keys are sent immediately and interpreted by the Node OS in the same way as pressing those keys on a locally attached keyboard.

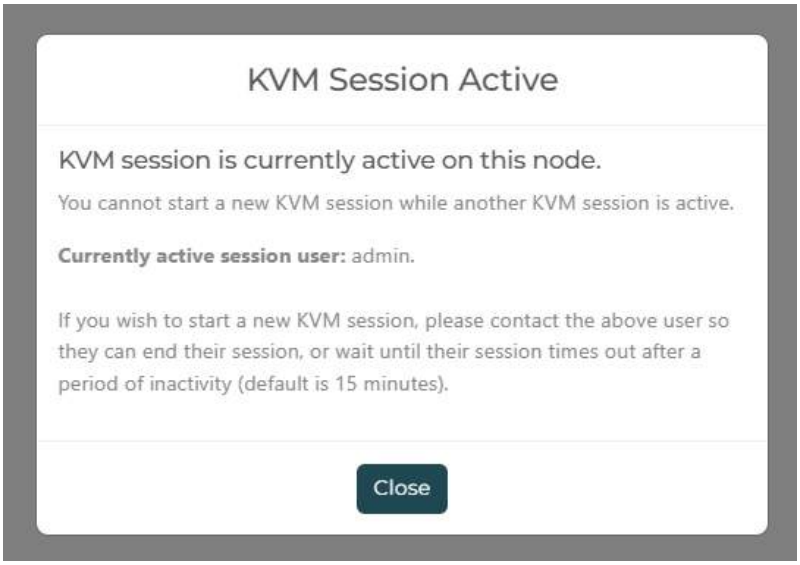
8.3 Multi-user interaction

Role-based access

The Remote Console feature is only available to Administrator and Technician user rules, Guest and Operator users are blocked when attempting to load the Remote Console page.

Remote Console session in progress on this node

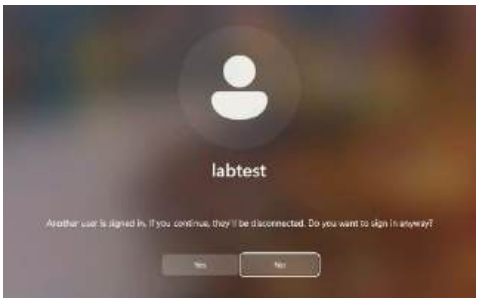
It is not possible to have more than one concurrent Remote Console session running on a specific Node, but within the enclosure, multiple Nodes can be running a Remote Console session simultaneously. For example, User A has a running session to node 1 and node 2 and at the same time, User B has a running session to node 3. If another user tries to connect to node 1, 2 or 3 using Remote Console, they will be blocked.



Windows desktop session in progress

When starting a Remote Console session to a Node which is in use (e.g. by a remote user over RDP), the session will connect and show the Windows login screen prompting for valid credentials for the Node OS. Since Windows Pro only allows a single concurrent user, the existing user will be disconnected if the Remote Console user continues. Windows Pro provides a warning before this happens.

A. Different user accounts (existing RDP user A, Remote Console user B) – The Remote Console user will see a warning message after entering correct credentials, giving them the choice to disconnect the existing remote user. The Remote user will be shown a similar warning, giving them the chance to continue their session.



Message shown to the Remote Console user

Message shown to the existing (RDP) user

B. Same user accounts (existing RDP user A, Remote Console user A) – If the same user account is used in both cases, there is no warning message and the Remote Console user will silently disconnect the existing session.

In either case, the reverse is also true – If a user attempts to connect to a Node over RDP whilst there is already a Remote Console session in progress, then they will see similar warnings.

Depending on the Windows OS settings, available memory and time elapsed, if a user reconnects to a machine from which they were previously disconnected, the desktop will be exactly as it was when they were last connected.

9. Events and Reporting

The Event Log provides an 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.

The Management Controller treats the initiation of an action and the result of an action separately because the same action can be initiated in different ways and initiating an action does not always result in a successful outcome.

9.1 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
- Automated Node provisioning and configuration
- Changes in node network state, speed or IP address

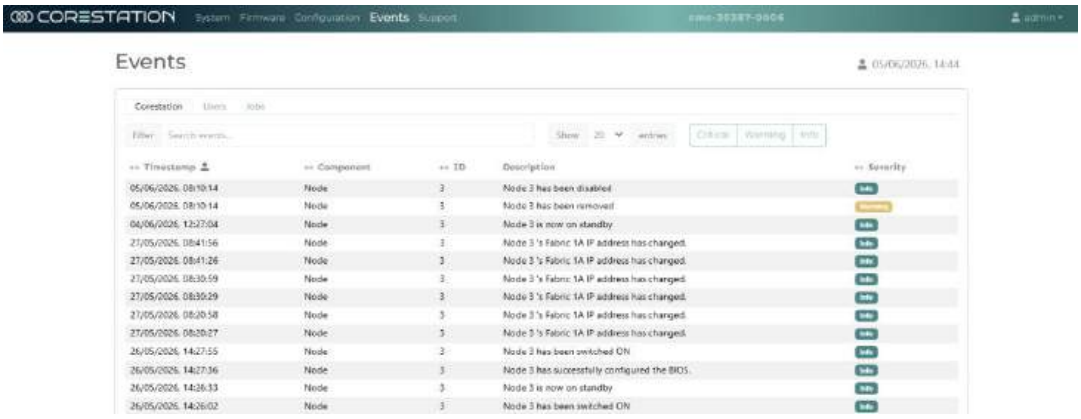


Figure 30 - CoreStation event history

9.2 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.

- Changes to system settings and configuration
- Enclosure and Node power up/down, identify and reseat actions
- Remote Console session start and stop
- Firmware Updates
- Support bundle export
- Changes to Special access configuration

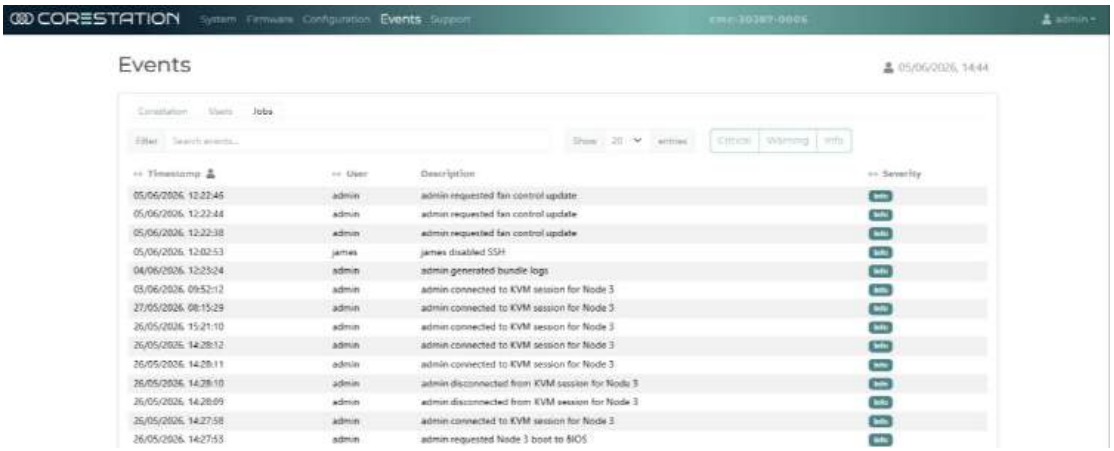


Figure 31 - Job event history

9.3 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
- Login Token grant and refresh
- Failed login attempts including username and the source IP address
- User account creation and modification
- User password changes

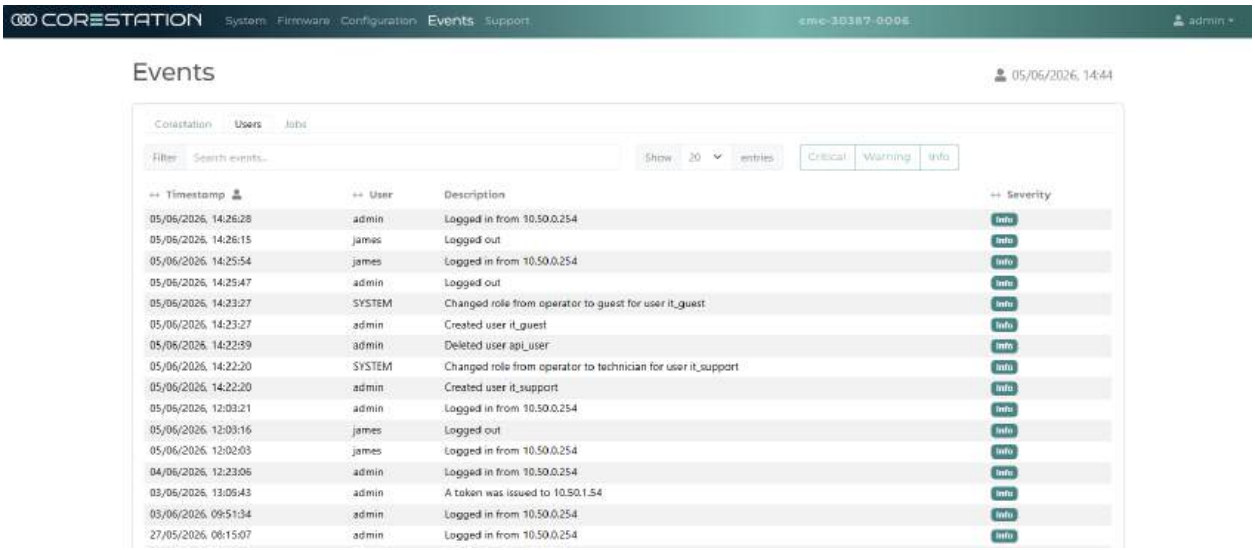


Figure 32 – User event history

9.4 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.

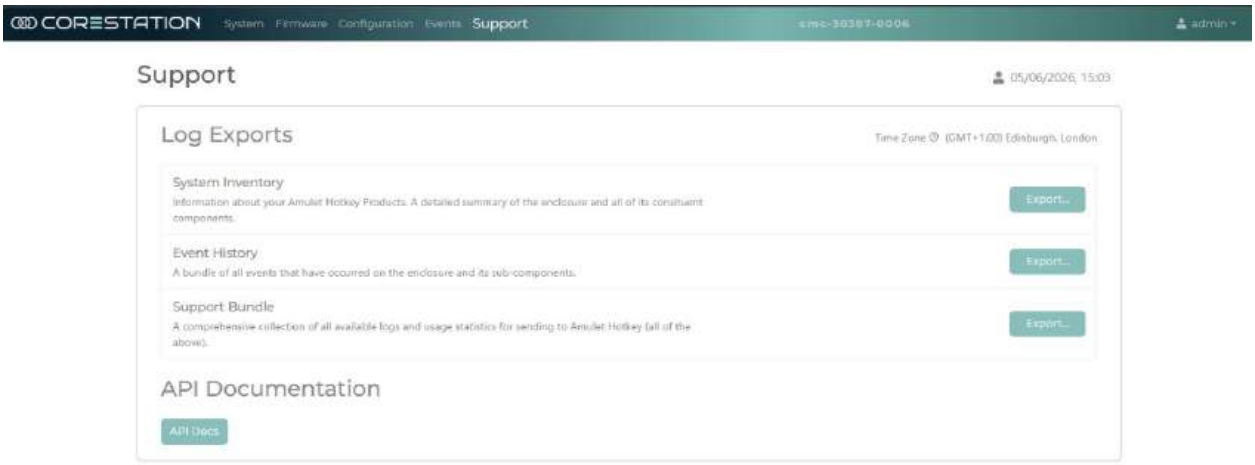


Figure 33 - log exports

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

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. The support bundle contains a wide range of information about the system:

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

Resources
www.amulethotkey.com

EMEA Support
+44(0)20 7960 2400
eurosupport@amulethotkey.com

North America Support
+1(212)269 9300
ussupport@amulethotkey.com
casupport@amulethotkey.com

Asia Pacific Support
apsupport@amulethotkey.com

Latin America Support
latamsupport@amulethotkey.com