vantageo™

VANTAGEO & VEEAM HARDENED REPOSITORY HARDWARE SETUP QUICK GUIDE

Planning / Implementation

Abstract

The Veeam Hardened Repository offers an effective way to safeguard business-critical backups through immutable storage technology. By utilizing Linux-based WORM capabilities, organizations can ensure backup data remains protected against cyber threats, malicious changes, and accidental data loss. The solution runs on standard server hardware, providing a cost-effective and flexible approach to building a secure backup repository.

The **Vantageo 2240 Server** is engineered to deliver the performance, reliability, and storage flexibility required for modern data protection environments. Featuring enterprise-class architecture, advanced security capabilities, and scalable storage options, the platform is an ideal foundation for Veeam backup repositories and other mission-critical workloads.

This document serves as a practical hardware setup guide for deploying a Veeam Hardened Repository on the Vantageo 2240 Server. The guide covers recommended installation practices, storage planning, firmware updates, RAID configuration, security controls, and operational considerations to help ensure successful deployment.

Organizations today require more than traditional backup solutions to defend against increasingly sophisticated cyber threats. The Veeam Hardened Repository provides a secure, Linux-based backup storage platform that protects backup data through immutability controls. By utilizing a Write Once, Read Many (WORM) approach, backup files can be preserved in a protected state for a specified retention period, ensuring that critical recovery points cannot be altered, encrypted, or removed by unauthorized users or malicious software.

Built on the principles of cyber resilience, Veeam Data Platform helps organizations strengthen their ability to safeguard data, respond effectively to security incidents, and restore business operations with confidence. The platform combines advanced threat detection, secure backup storage, and streamlined recovery workflows to reduce operational risk and improve overall resilience against ransomware and other cyberattacks.

Key Benefits

- Identify potential security threats before they impact business operations.
- Accelerate recovery processes following ransomware or cyber incidents.
- Maintain secure, compliant, and reliable protection for critical data assets.

Core Capabilities

Intelligent Threat Detection

Advanced analytics continuously examine backup activity and data characteristics during backup operations, helping administrators detect unusual patterns and potential malware activity at an early stage.

Reduced Risk of Reinfection

Detailed analysis of backup content assists in identifying affected systems and suspicious data, enabling teams to restore from known clean recovery points and minimize the possibility of reintroducing threats.

Immutable Data Protection

Backup integrity is protected through immutable storage policies, zero-trust security principles, and enhanced administrative controls that help prevent unauthorized deletion or modification of recovery data.

Integrated Security Visibility

Security-related backup events and anomalies can be shared with monitoring, incident management, and security analytics platforms, enabling security teams to investigate and respond more efficiently.

Coordinated Recovery Operations

Automated recovery workflows help organizations restore applications, systems, and infrastructure in a structured and controlled manner, reducing downtime and operational disruption.

Compliance and Security Validation

Built-in assessment tools help verify that backup environments align with established security and data protection best practices, supporting stronger governance and compliance initiatives.

Enhanced Incident Awareness

External security platforms can integrate with backup operations to provide additional context regarding identified threats, allowing backup administrators to make more informed recovery decisions.

Granular Point-in-Time Recovery

Organizations can restore workloads to specific moments before an incident occurred, minimizing data loss and improving recovery accuracy for mission-critical systems.

Centralized Threat Insights

A unified security dashboard provides visibility into backup security posture, threat indicators, operational risks, and overall resilience metrics, helping organizations continuously improve their cyber readiness.

For detailed deployment, configuration, and operational guidance related to Veeam Hardened Repository implementations, administrators should refer to the applicable Veeam product documentation and best-practice resources for their platform version.

Introduction

The Vantageo 2240 is a 2U rackmount server designed for enterprise workloads, cloud infrastructure, virtualization, edge computing and backup repository deployments. This guide provides a recommended hardware deployment workflow for Veeam Hardened Repository environments.

Recommended Server Platform

Key capabilities include dual 4th/5th Gen Intel Xeon Scalable processors, up to 32 DDR5 DIMMs, flexible SATA/SAS/NVMe storage, redundant power supplies, TPM 2.0 security and Redfish-enabled management.

Figure 1: Vantageo 2240 2U rackmount server

Firmware Update Procedures

Update server firmware before production deployment. Apply BMC updates first, validate management access, then update BIOS/UEFI, RAID controllers, storage devices and network adapters.

Figure 2: Login to BMC with IP Address

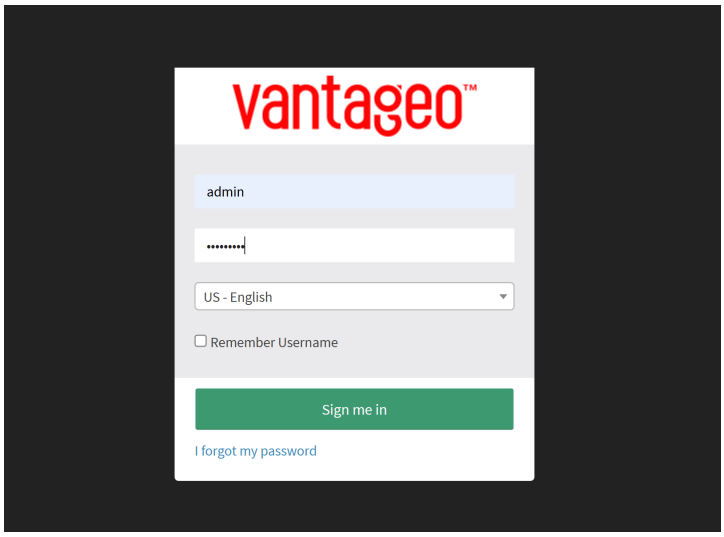


Figure 3: Go to Maintenance and click on the Firmware Update

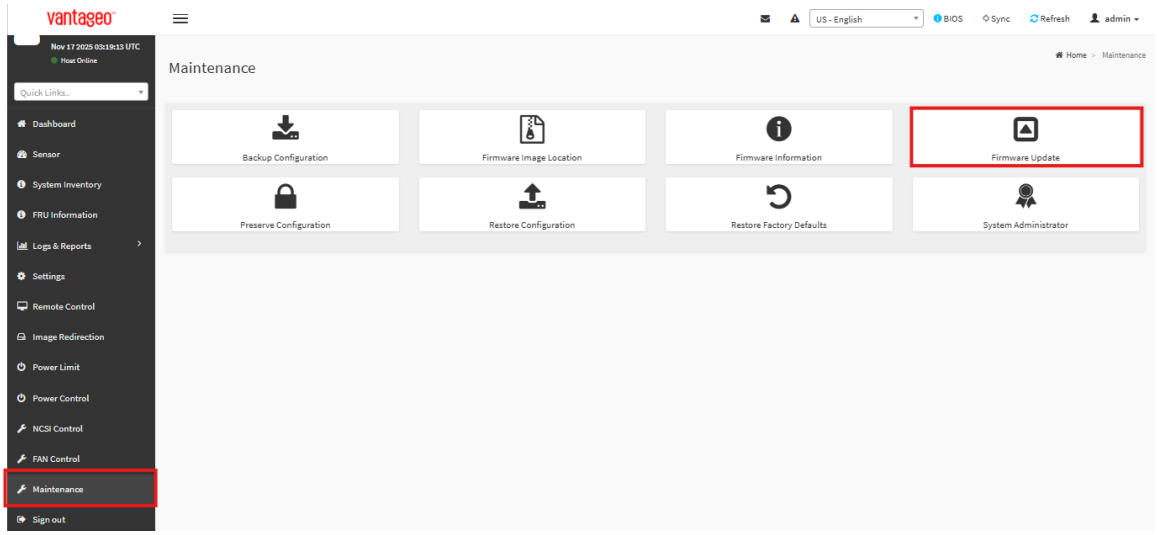
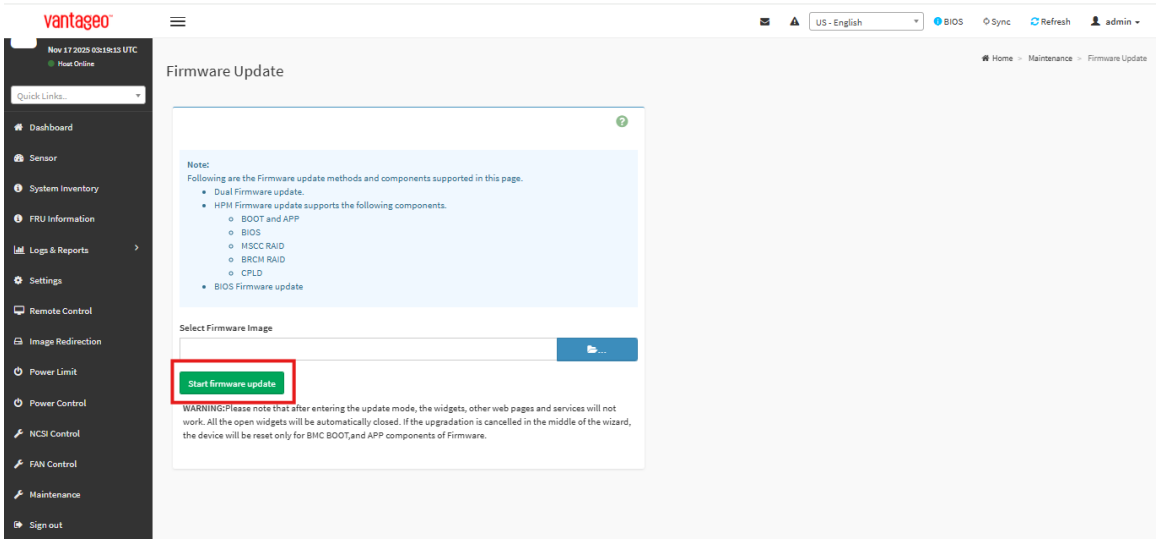


Figure 4: Select the File and Click on Start Firmware Update



Recommended Update Sequence

1. Install hardware
2. Update BMC firmware
3. Reboot management controller
4. Update BIOS/UEFI
5. Reboot server
6. Update remaining components
7. Validate system health

RAID Setup for Logical Drives

Create virtual disks according to repository requirements. Common RAID levels include RAID 1 for operating systems and RAID 6 or RAID 60 for large-capacity backup repositories.

Figure 5: Go to Setting and Click on the RAID Management

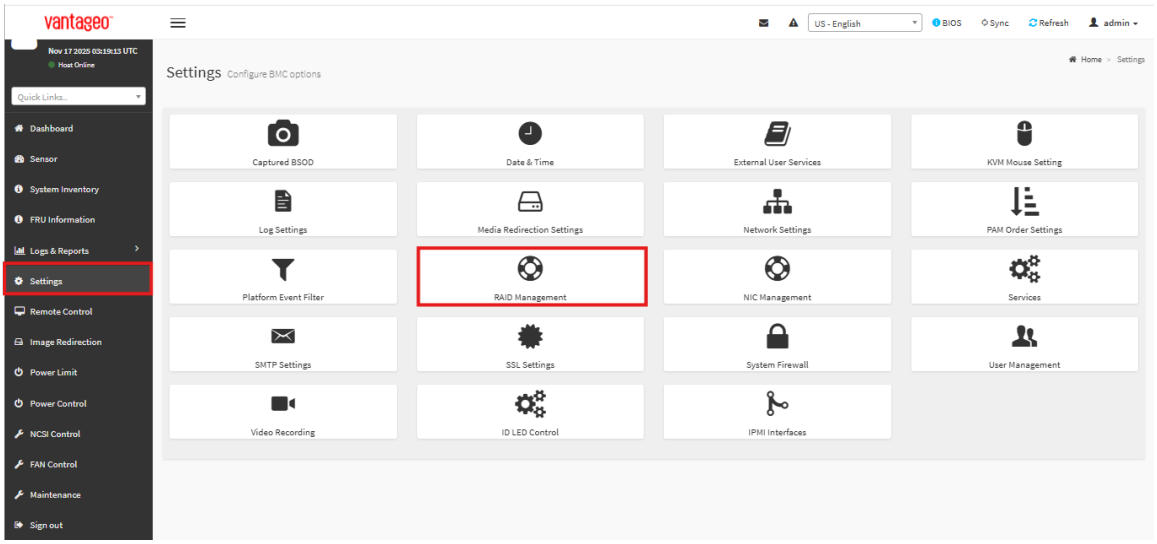


Figure 6: Click on the Raid Controller Information

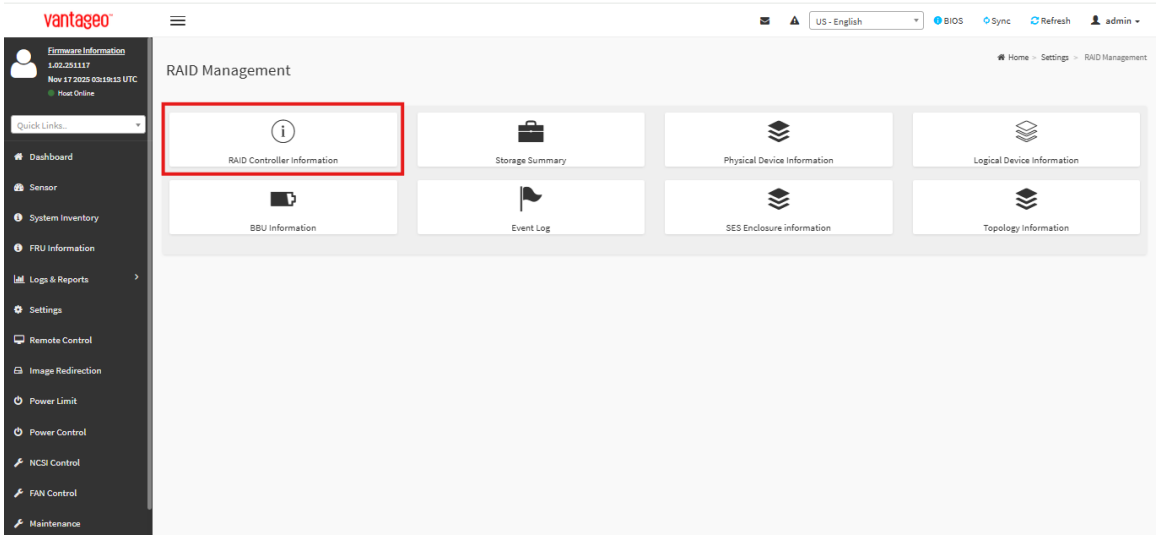


Figure 7: Raid Controller Information

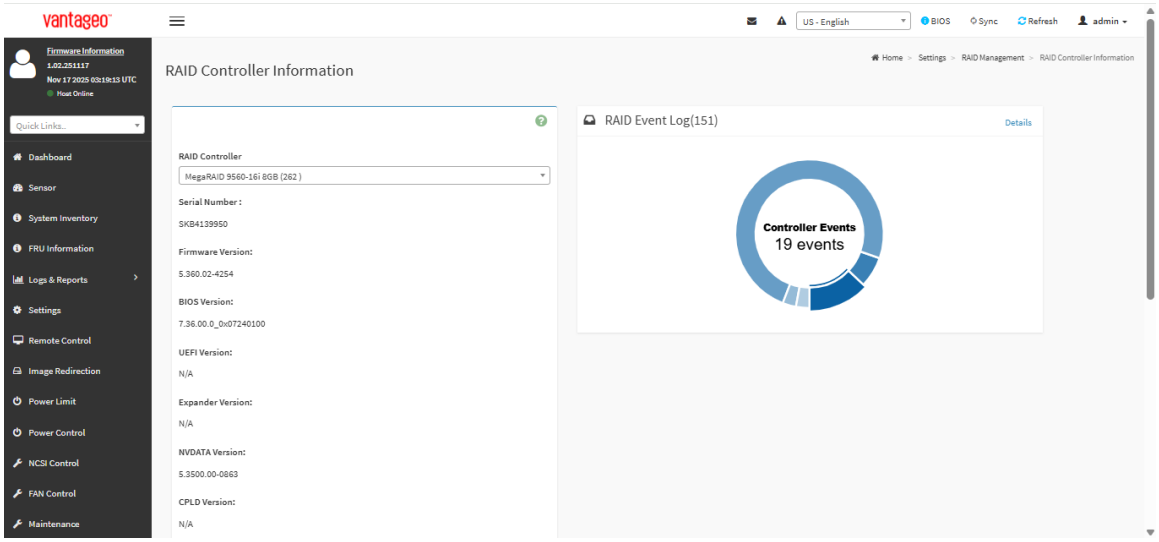


Figure 8: Click on the Physical Device Information

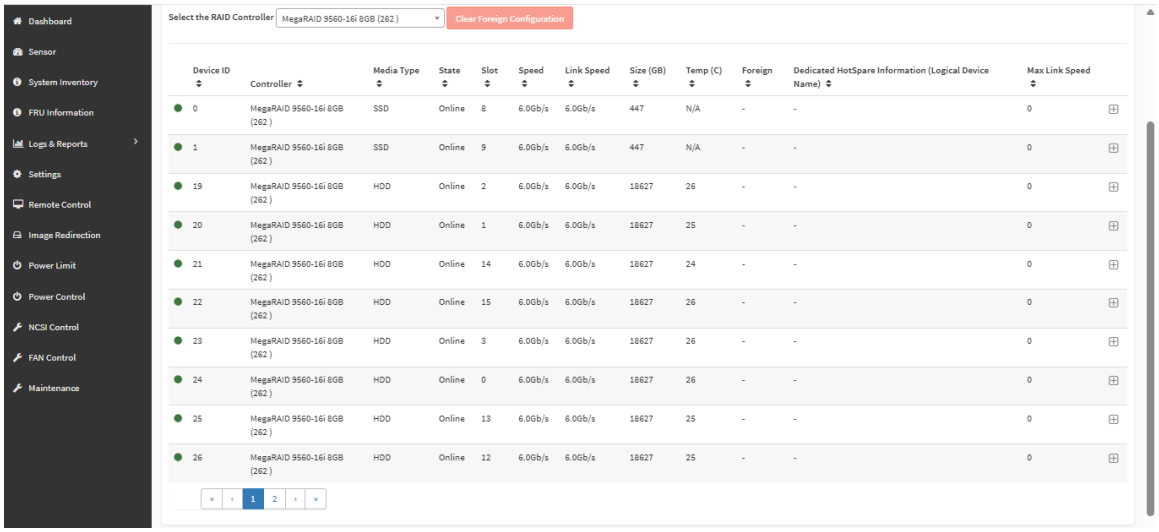


Figure 9: Click on the Logical Device Information and click on the Create Virtual Drive

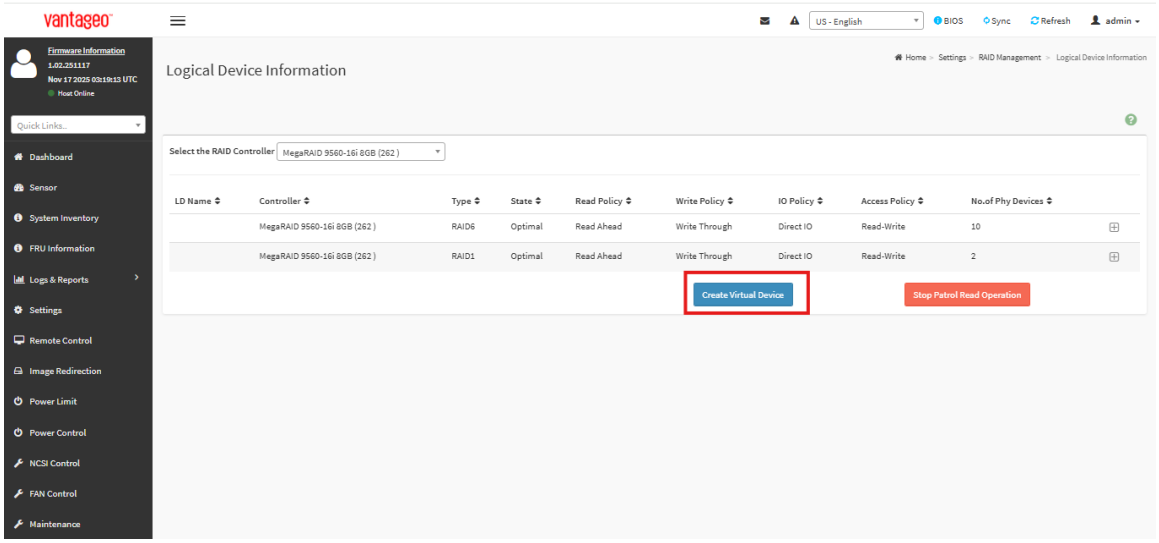
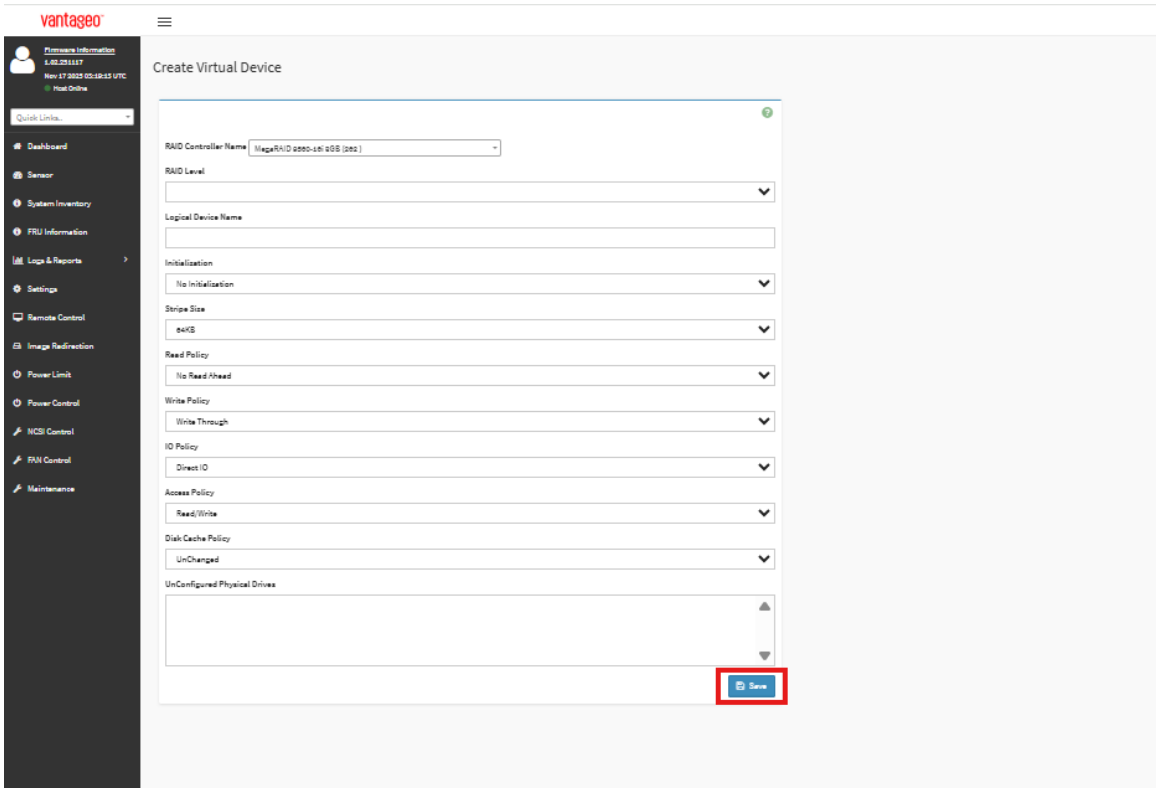


Figure 10: Select requried details and click on Save to Create Virtual Drive



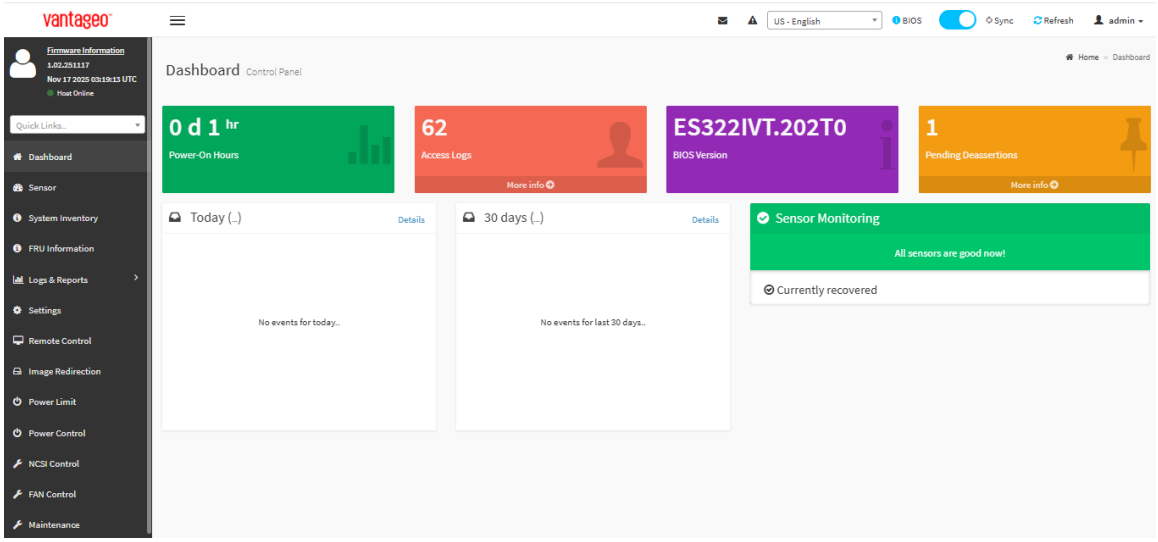
Redfish API Integration

The platform supports industry-standard Redfish and IPMI interfaces for monitoring, automation and lifecycle management.

System Health Monitoring

Monitor hardware status, events, utilization, storage health, thermal readings and alert notifications through the baseboard management controller.

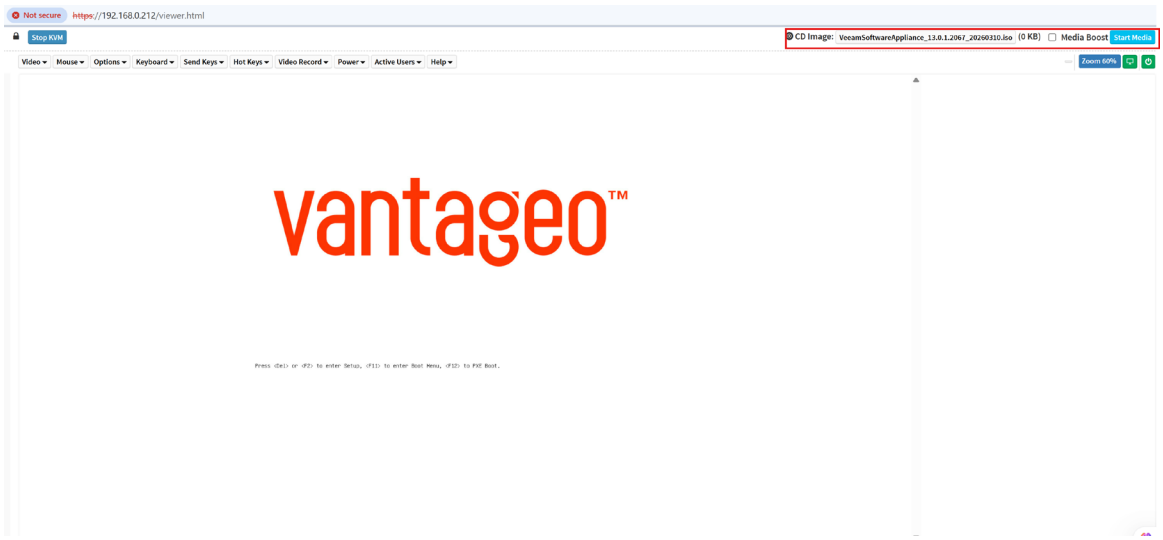
Figure 8: Dashboard of the Server



Remote Console and OS Deployment

Use KVM-over-LAN remote console functionality to mount ISO images, perform unattended deployments and troubleshoot systems remotely.

Figure 9: Remote Console and OS Deployment



For More Information

Visit https://vantageo.com/products/vantageo-2240-serverand consult product datasheets and support documentation.

Legal Notices and Trademarks

Technical Modifications: Information, specifications, and images in this document are subject to continuous technical updates and modification without notice. Vantageo India Pvt. Ltd. assumes no responsibility for operational interruptions or technical discrepancies resulting from reliance on this publication.

Availability: Hardware configurations, firmware revisions, and component availability may vary by region and production schedule.

Intellectual Property: All third-party trademarks, service marks, trade names, and copyrights cited in this document remain the property of their respective holders. Reference to third-party products does not constitute endorsement or affiliation.