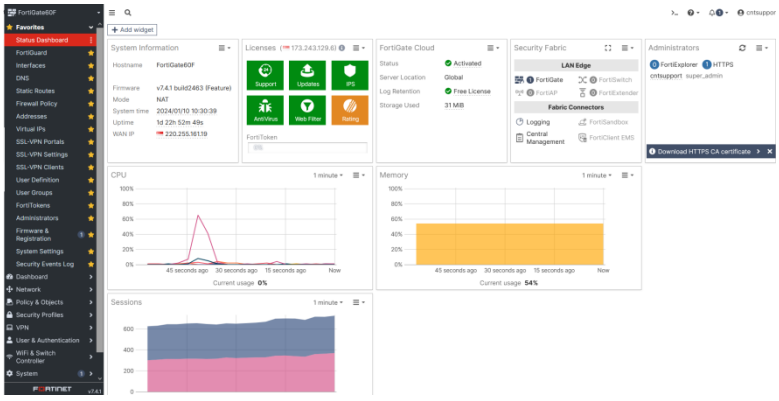
IT Hardware Maintenance / Services

Menu

1.1 Firewall Maintenance

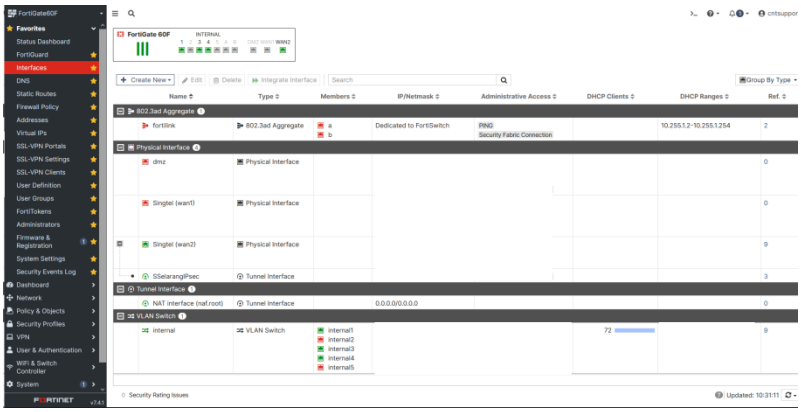
Firewall System Performance Status

We will review the firewall dashboard status to ensure that the widgets accurately present the Forti-Web appliance's details, such as the serial number, current system status, uptime, system resource usage, hostname, firmware version, system time, and the status of policy sessions.



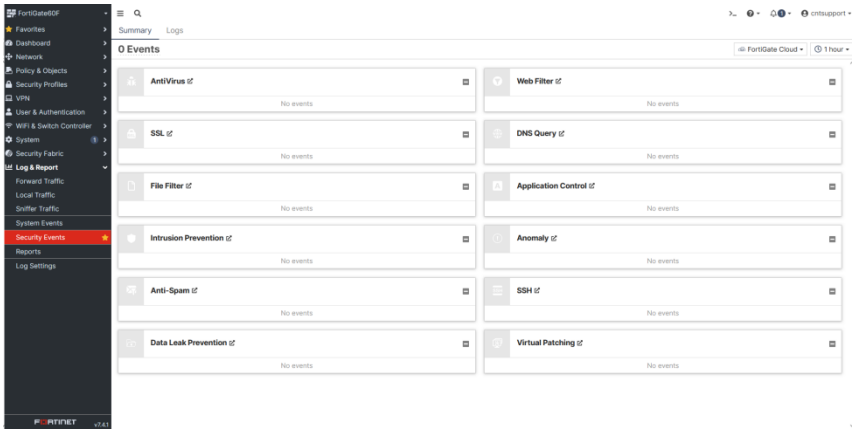
Firewall Port Status

We will check the status of ports on a FortiGate firewall can refer to whether the individual network ports are enabled, disabled, or in a particular state such as up or down.

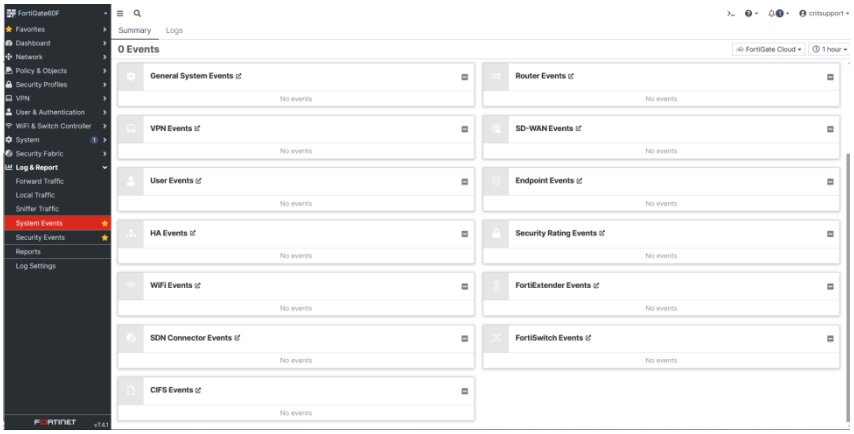


Firewall Security / System Events Summary & Logs

We will check security events summary & Logs in the context of FortiGate refer to the consolidated records that detail the activities and incidents detected by the firewall. These logs are crucial for network administrators and security professionals to monitor, analyze, and respond to potential security events.

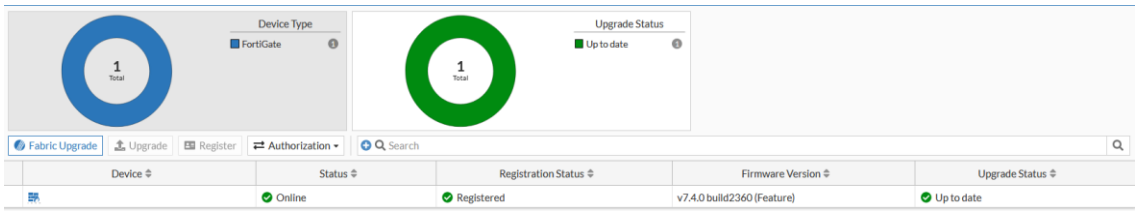


We will check system events Summary and Logs are a comprehensive collection of records that detail the operational status, security incidents, and other significant events that occur within a network protected by a FortiGate firewall. These logs are essential for network administrators to ensure ongoing network health, security, and compliance with various regulatory standards.



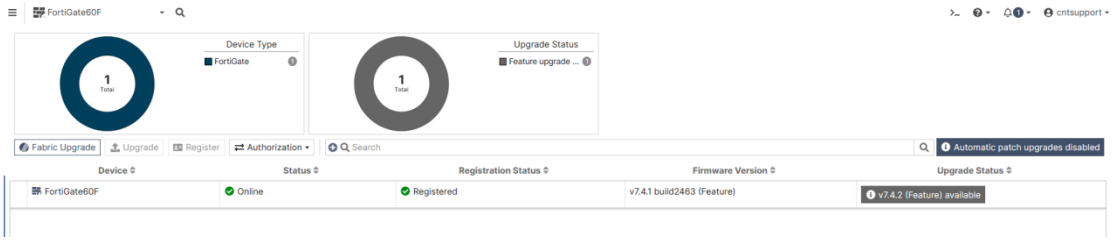
Firewall System Firmware

We will regularly release firmware upgrades that include security patches to address known vulnerabilities. Upgrading the firmware ensures that the firewall is equipped to defend against new and emerging threats.



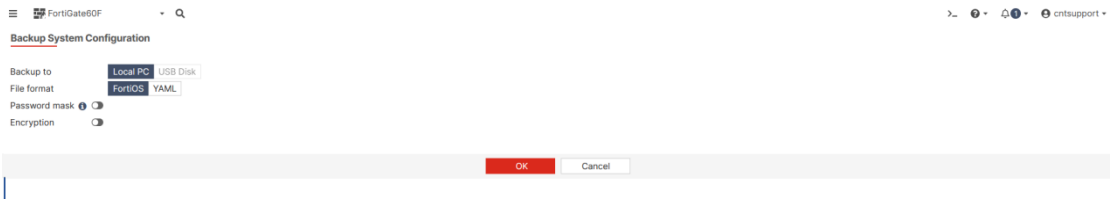
Case Study:

1. Outdated Firewall Firmware Exposing Vulnerabilities



Firewall Backup Configuration File

Create a backup of the current firewall configuration. This backup will act as a fail-safe mechanism in case anything goes wrong during the firmware update process.



Case Study:

Problem: Unauthorized access to a firewall result in malicious configuration changes that compromise a client or company.

Solution:

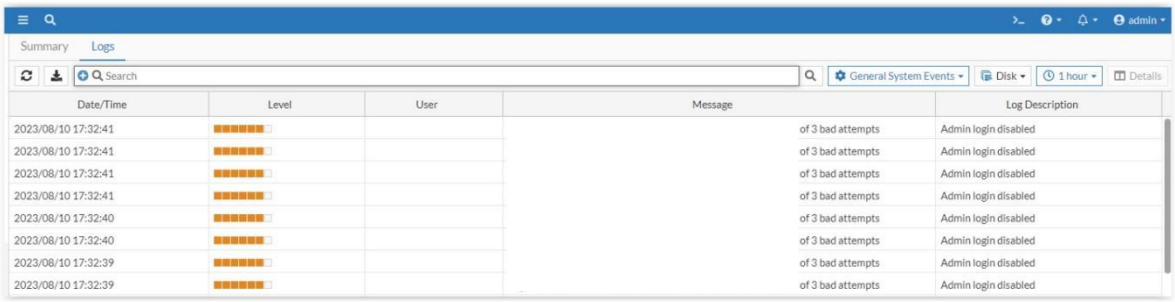
Configuration Restoration

CNT Team leveraged the latest configuration backup, which was taken before the breach, to restore the firewall to its previous secure state. This process ensured that any unauthorized changes made by the hacker were overwritten by the trusted configuration.

2. Check the logs file for threats.

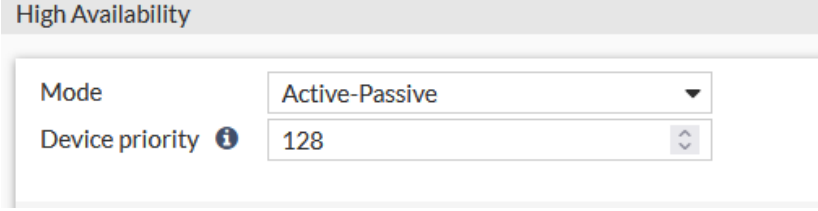
A. Unauthorized login attempts

Identify login attempt. This includes details such as IP address, usernames and timestamps and number of failed login attempts.



B. Synchronization & HA

The active firewall continuously synchronizes its state and configuration with the passive firewall devices. This synchronization ensures that the passive nodes are up-to-date and ready to take over the active role if needed.



HA clusters communicate with each other through a heartbeat mechanism. They constantly exchange signals to verify each other's availability and health status.

Case Study:

3. Ensuring Network Continuity with Firewall High Availability

Problem Statement: Hardware failure or unexpected disruptions to Firewall will interrupt network operations.

Troubleshoot:

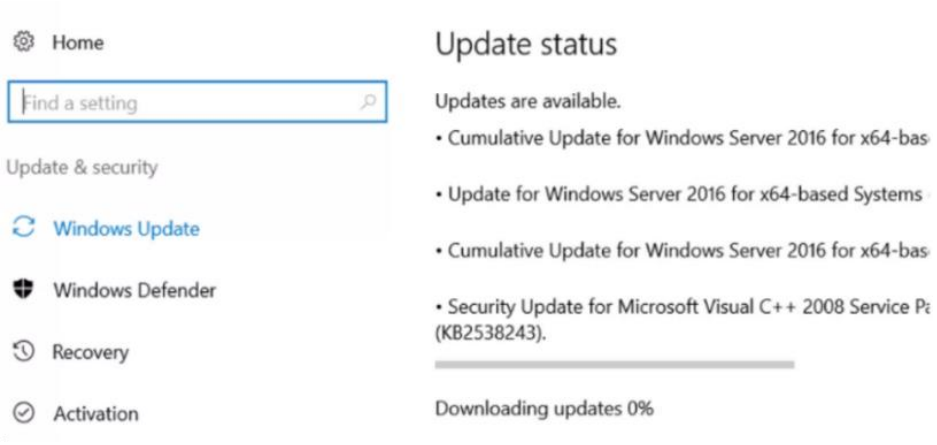
High Availability Response:

As the primary firewall went down, the secondary firewall detected the absence of heartbeat signals within the predefined time frame. It swiftly assumed control and took over the network responsibilities, including handling VPN connections and managing internet traffic.

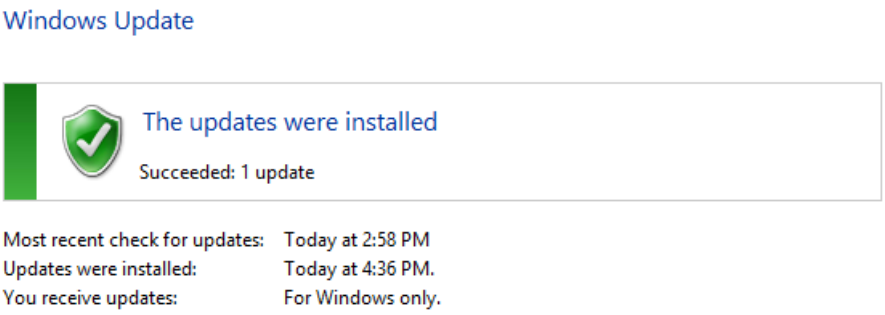
1.2 Windows Server Maintenance

Windows Server Update & Patches

Security updates are released to address known vulnerabilities and weaknesses in the Windows Server operating system. These vulnerabilities could potentially be exploited by hackers and malicious software to compromise the server's security. Microsoft releases these updates as a response to emerging threats.

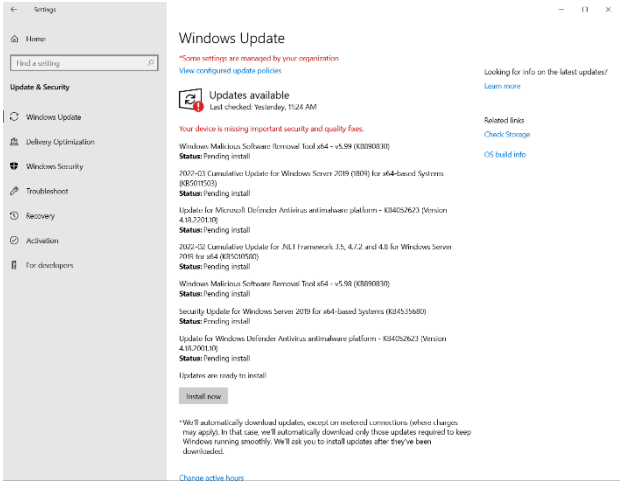


Quality updates include bug fixes, improvements, and optimizations for various aspects of the Windows Server OS. Quality updates are aimed at providing a smoother and more reliable operating system environment.



Case Study:

Windows Server Update:



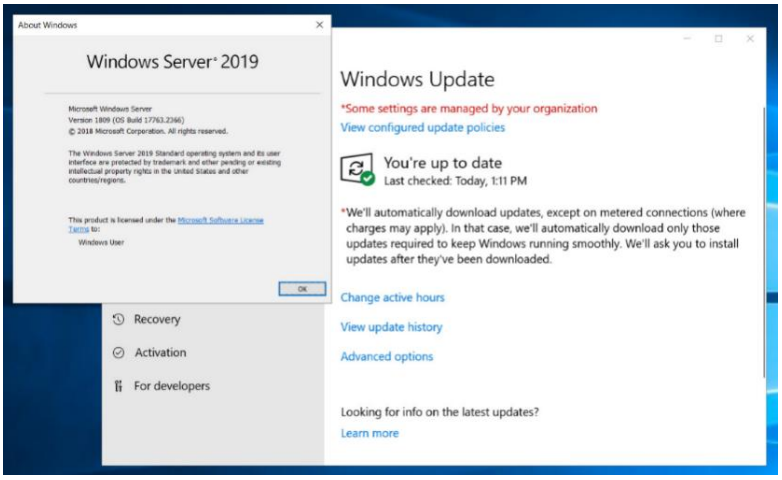
Many Windows updates are missing from the server it could lead to:

- **Security Vulnerabilities:**
  Outdated software can contain known security vulnerabilities. Hackers and cybercriminals often exploit these weaknesses to gain unauthorized access to systems, steal data, or carry out other malicious activities.

- **Malware Infections:**
  Without the latest security patches, the system becomes more susceptible to malware infections, such as viruses, ransomware, and spyware. Malware can cause data loss, system damage, and compromise sensitive information.

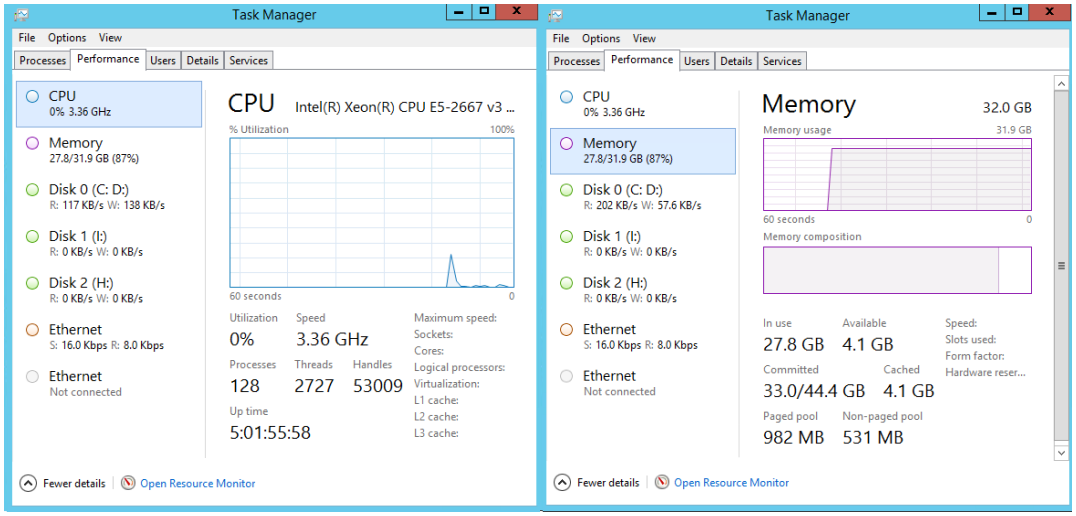
- **Performance Issues:**
  Updates often include performance improvements and bug fixes, which can enhance system stability and responsiveness. Not updating Windows may lead to performance degradation or instability over time.

- **Software Compatibility Problems:**
  Newer software applications and drivers may not be fully compatible with an outdated operating system, resulting in compatibility issues and potential crashes.

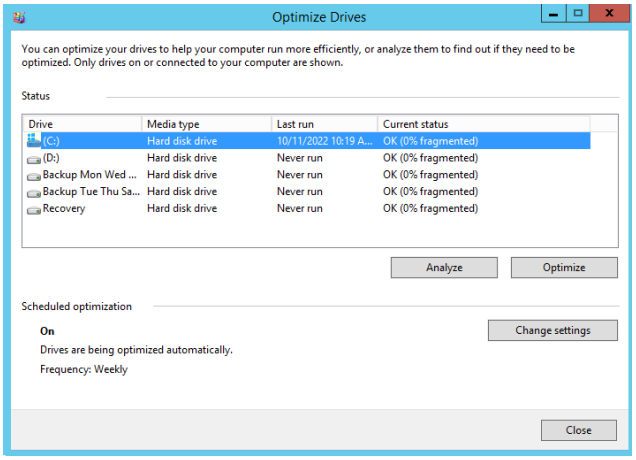


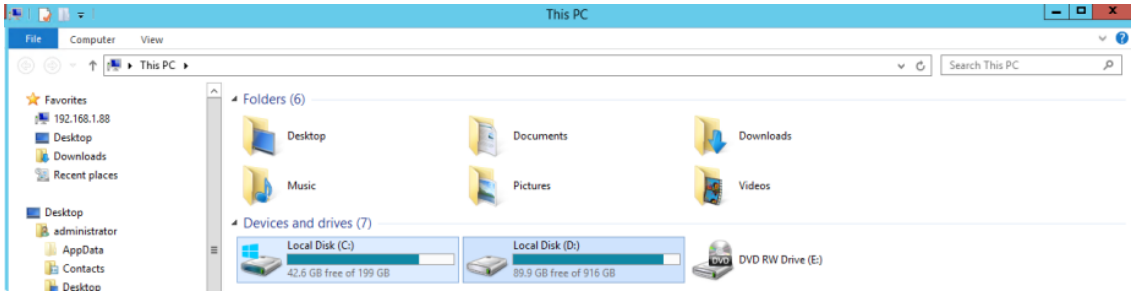
Windows Server Performance Optimizations

We will check hardware optimization to ensure that the server has sufficient RAM and CPU resources to handle the expected workload.



We will check storage optimization do defragmenting disks regularly and ensuring that there is enough free space.



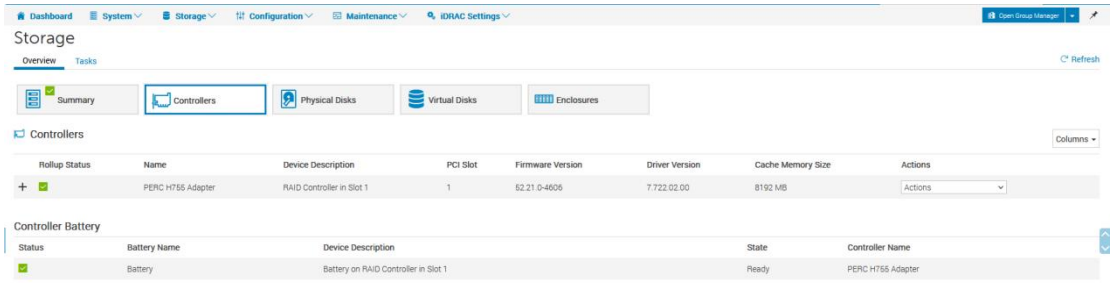


Windows Server Monitoring

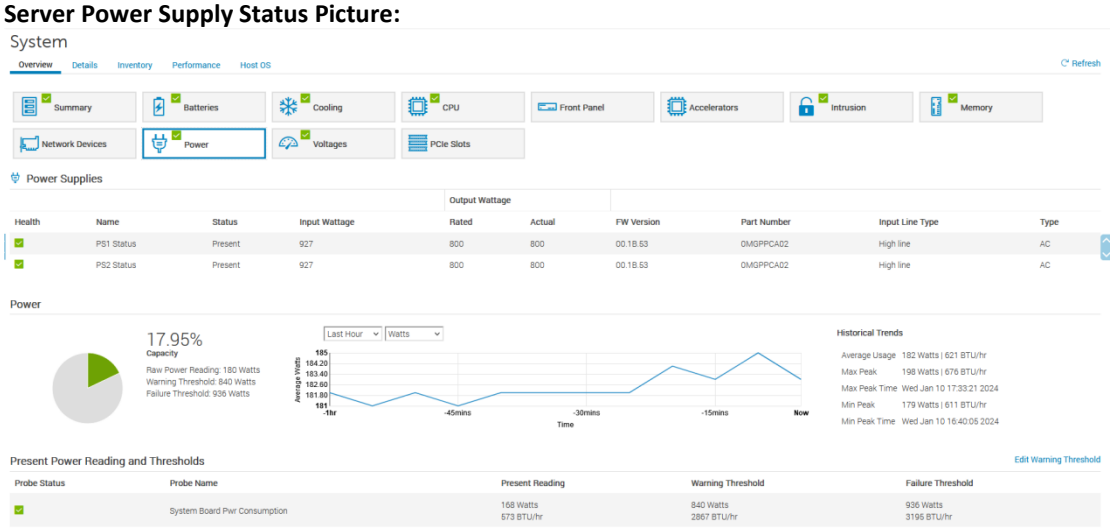
We will check the server hardware health, if the server is on-premises, check the hardware status, including RAID systems, power supplies, and temperature, to prevent hardware failure.

Dell EMC Power Edge Server Status

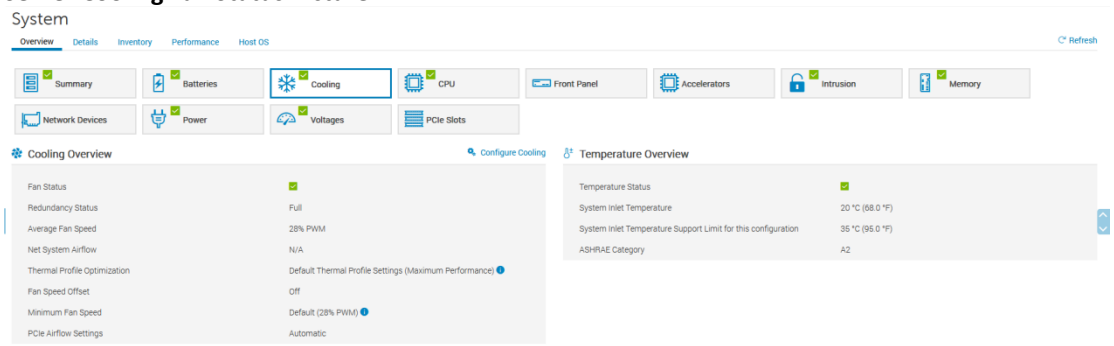
Server RAID Controller Status Picture:



Server Power Supply Status Picture:



Server Cooling Fan Status Picture:

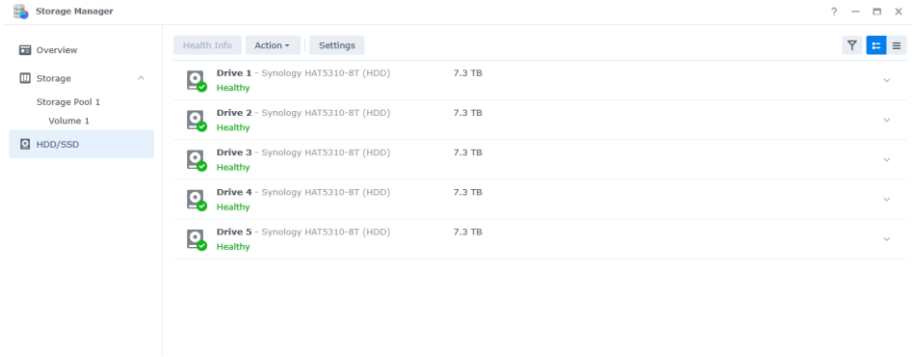


1.3 NAS Maintenance

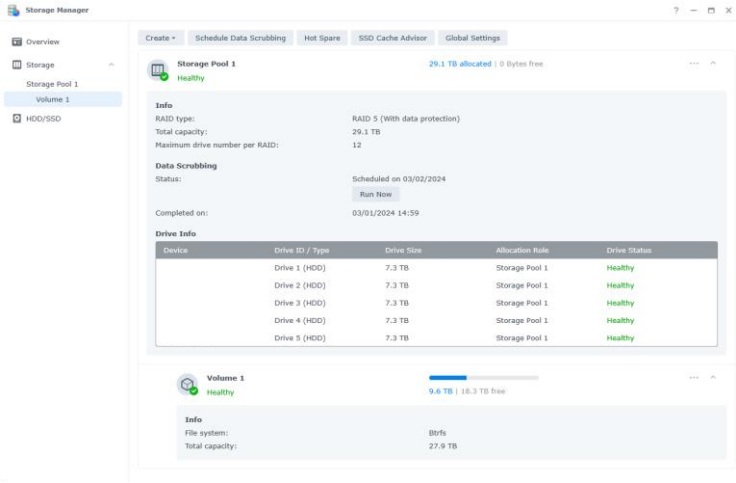
NAS Storage Manager Status

We will check disk health looking for signs of potential failure such as self-monitoring, analysis and reporting warnings message. We will check the storage volumes, including expanding volumes, RAID configuration and ensuring efficient use of storage space.

Disk Health Status Picture:



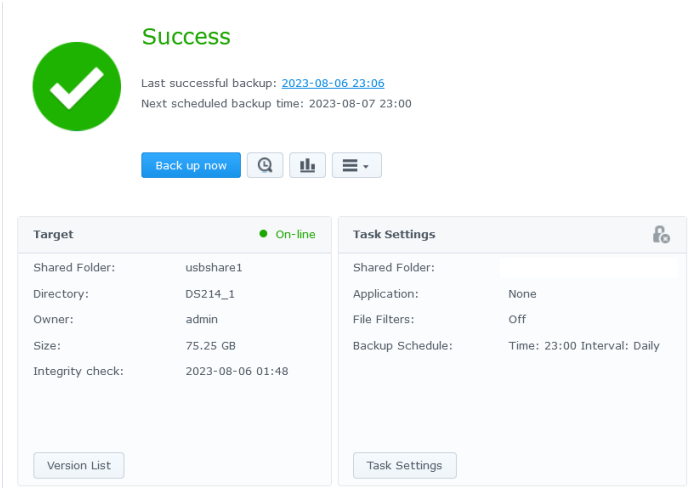
RAID Controller Status Picture:



NAS Backup Status

We will check data backup ensuring that the data stored on the cloud or backup media is regularly backed up to prevent data loss in the event of hardware failure or another issue.

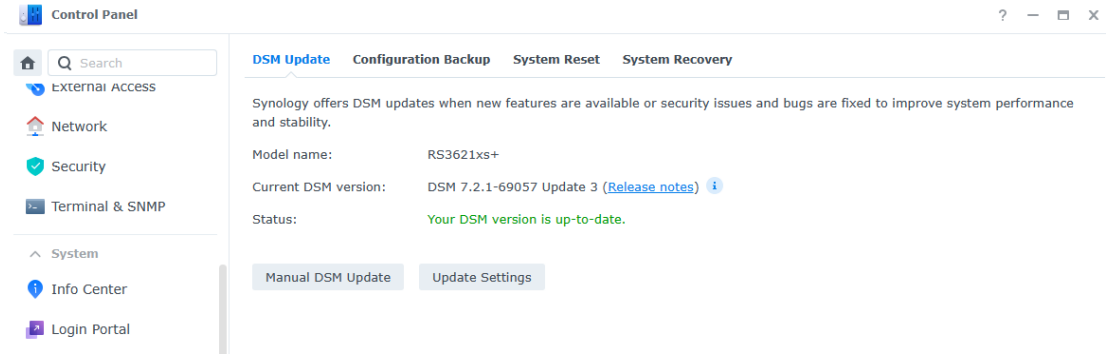
Backup Status Picture:



NAS Firmware Update

We will check NAS firmware to improve performance, security enhancements and bug fixes. The updates can optimize the way the device operates, potentially making it faster or more efficient. If there are known issues or bugs in the firmware, updates can resolve these, leading to a more stable and reliable NAS. New firmware often patches known vulnerabilities that could be exploited by malware or hackers.

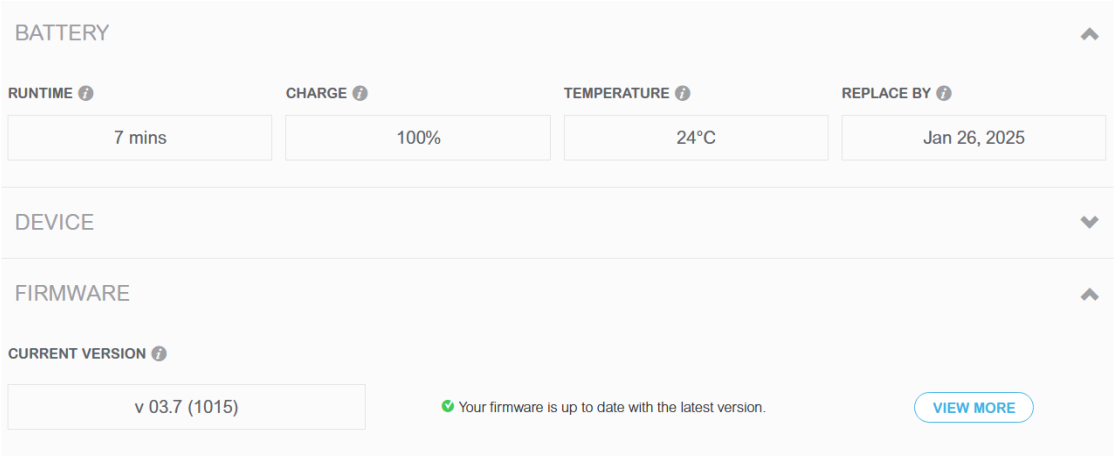
System Firmware Update Picture:



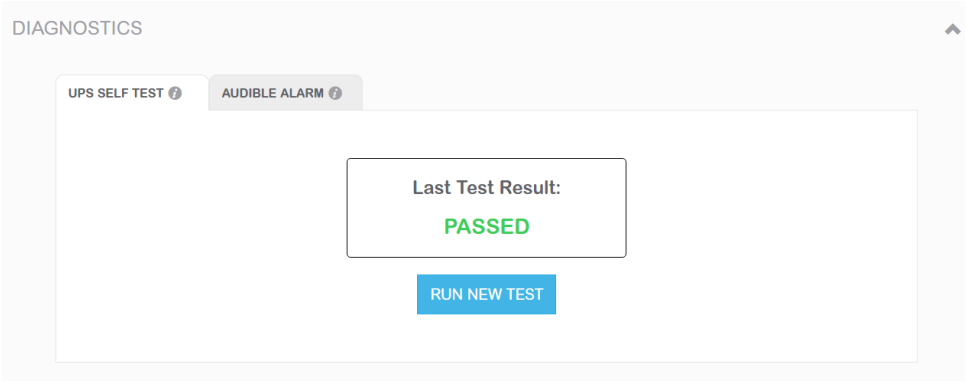
1.4 UPS Maintenance

We will check battery maintenance and firmware updates. UPS batteries are a critical component of a UPS. Maintenance includes checking battery charge levels, testing for capacity, and replacing batteries that are no longer holding a charge. Keeping the UPS firmware up to date to ensure compatibility with connected devices and to improve functionality.

UPS Dashboard & Firmware Status Picture:



UPS Battery Diagnostics Picture:

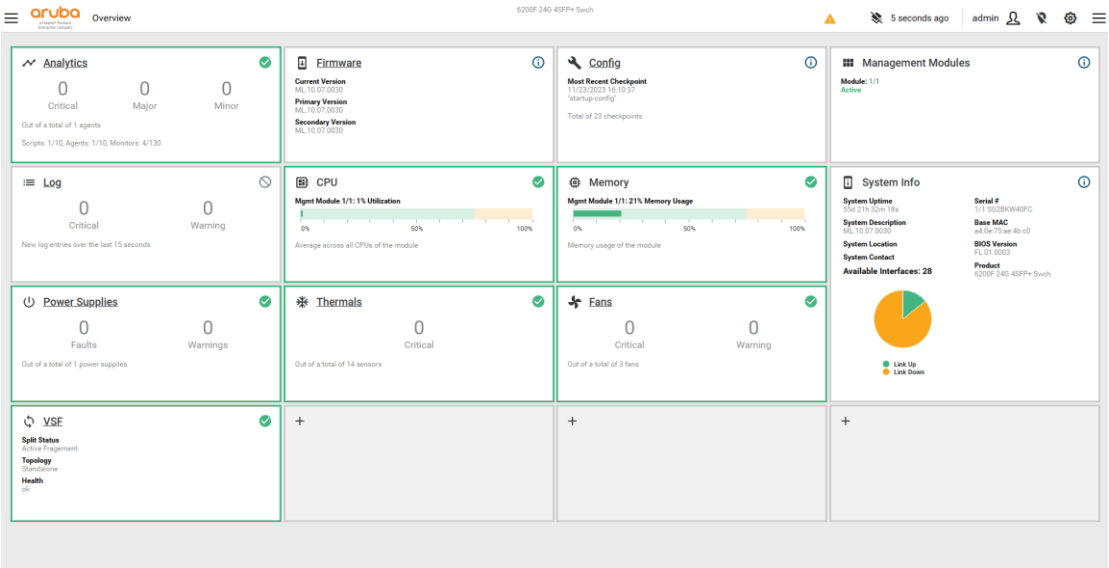


1.5 Managed Switch Maintenance

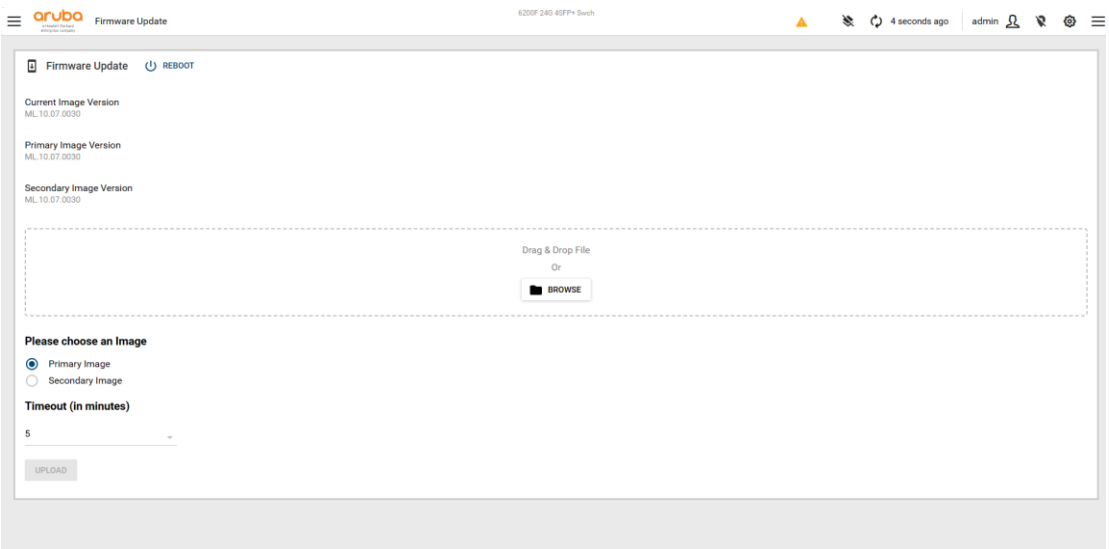
We will check network performance monitoring, firmware updates, configuration backups, security audits, and redundancy checks. We will use network management tools to monitor the performance of the switch. Look for anomalies such as high collision rates, CRC errors, or unexpected traffic patterns. We will regularly save the current configuration of the switch. In case of a failure, you can restore the switch to a known good state. We will regularly review security settings, update access control lists, and ensure that all default passwords have been changed. Monitor logs for unauthorized access attempts. If the switch is part of a redundant setup, test failover mechanisms to ensure they work as expected.

Aruba Core Switch Device

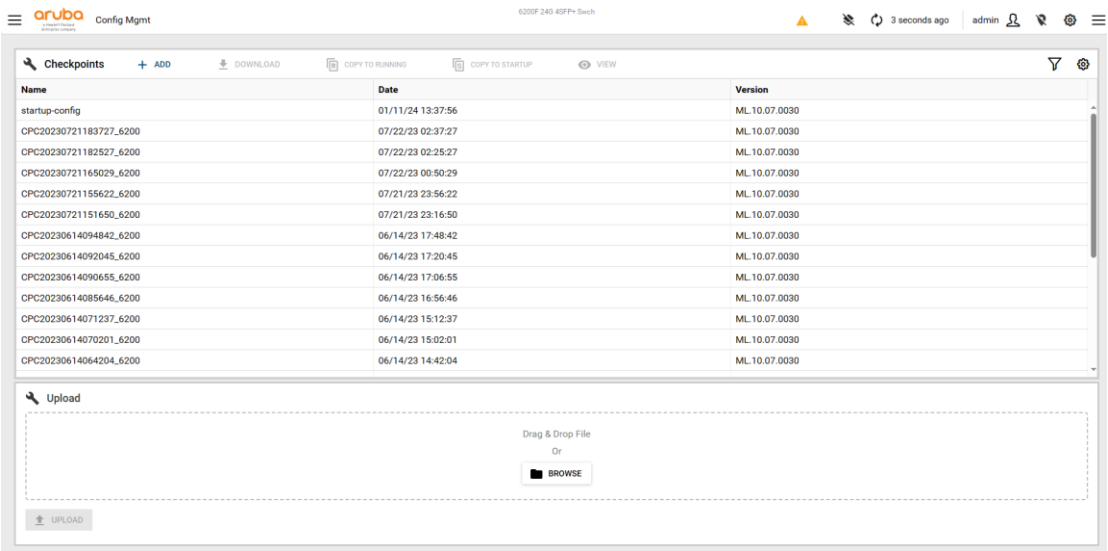
Managed Switch Performance Monitoring Picture:



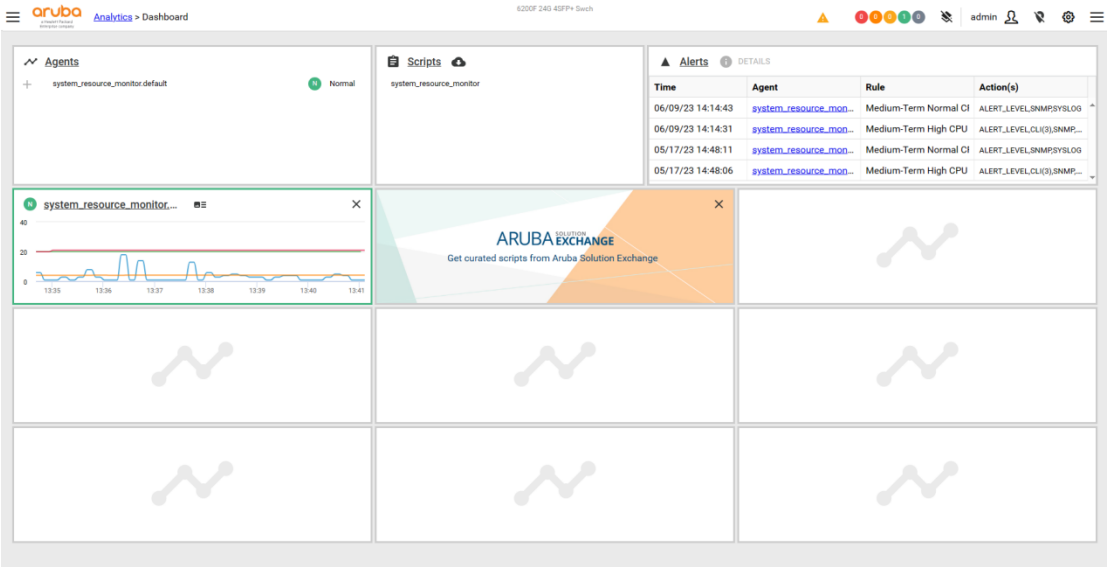
Managed Switch Firmware Update Status Picture:



Managed Switch Configuration Backup Status Picture:



Managed Switch Log Report Status Picture:

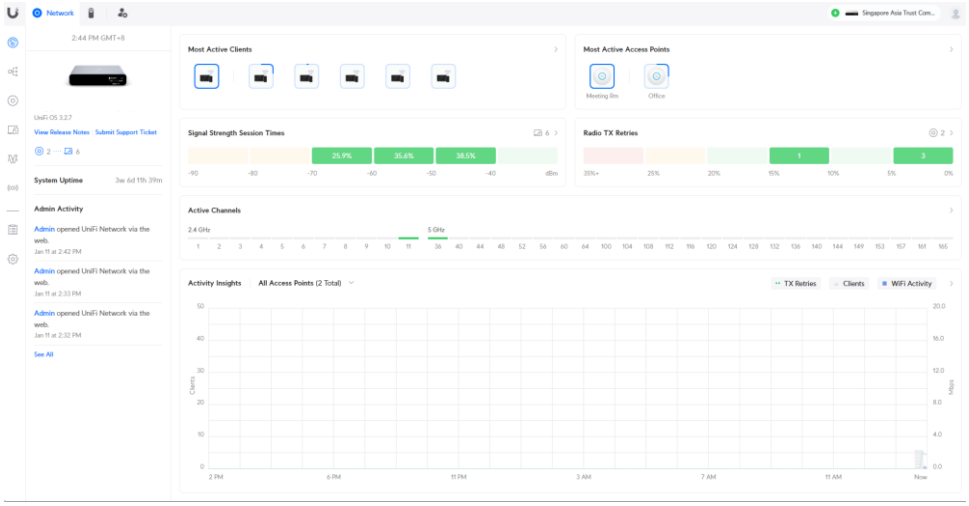


1.6 Access Point Maintenance

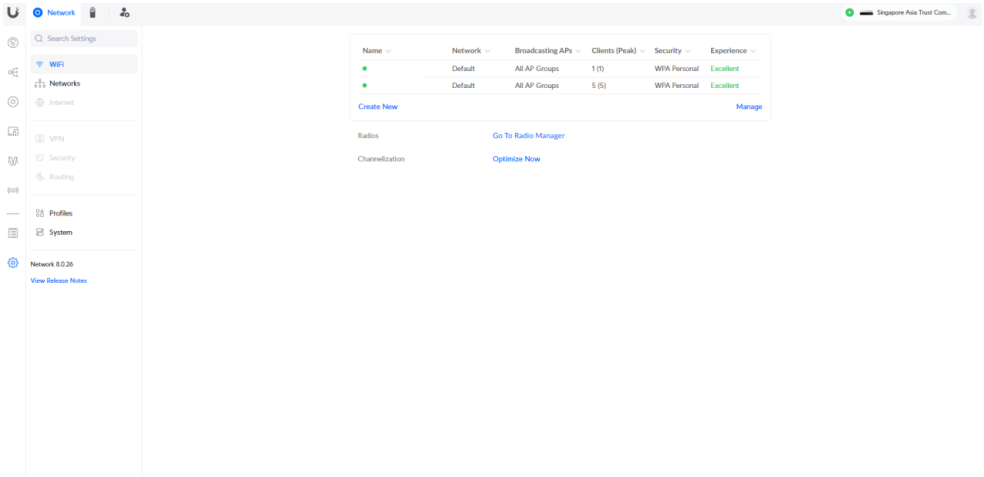
We will check AP performance monitoring, configuration management, network analysis, security audits and firmware updates. We will be monitoring the performance of access points to ensure they are providing the expected coverage and speed. This can involve checking signal strength, noise levels, and the number of connected devices. We will review and optimise the configuration settings, such as SSID settings, security protocols, and channel selection to prevent interference and improve performance. We will use network analysis tools to identify and resolve any issues such as dead zones, interference, or over utilization of certain access points. We will regularly conduct security audits to ensure that the network is protected against unauthorized access or attacks. This includes checking for and addressing any vulnerabilities. We will regularly update the firmware of access points to the latest version to ensure they have the latest features and security patches.

Ubiquiti Access Point Controller Device

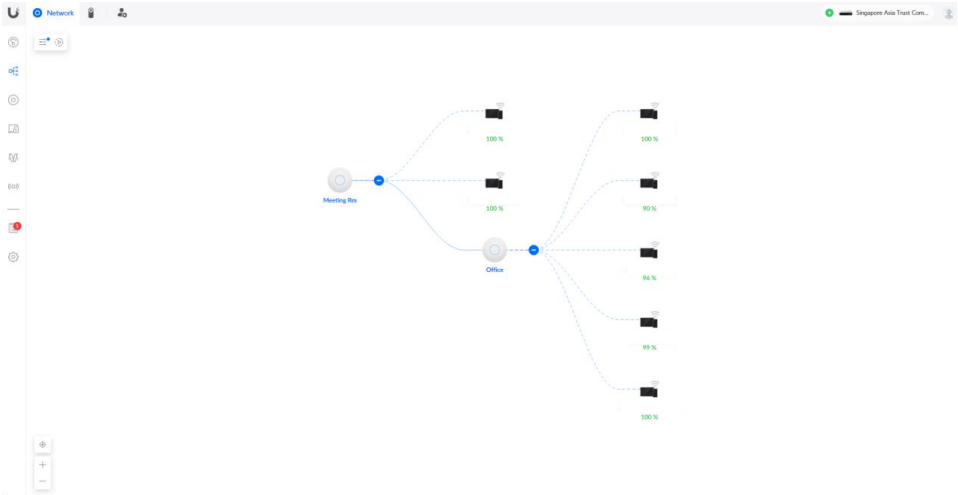
Ubiquiti AP Controller Performance Monitoring Picture:



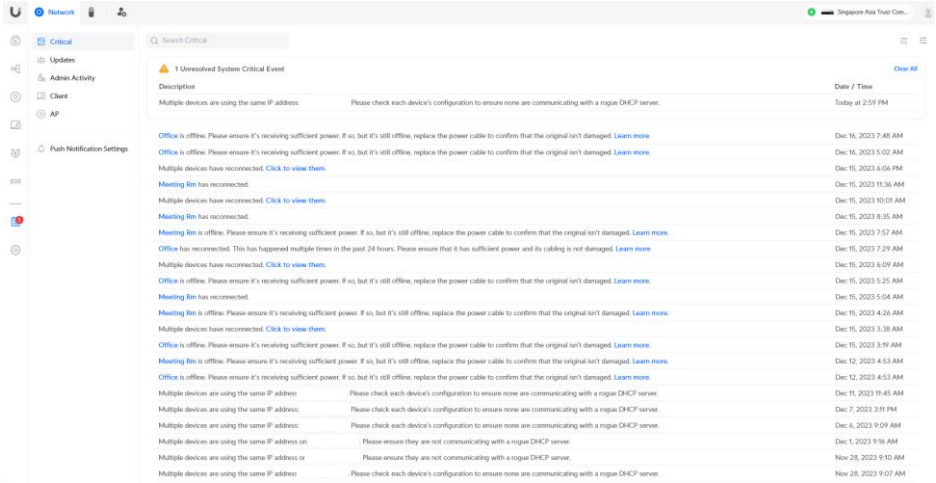
Ubiquiti AP Controller Wi-Fi configuration management Picture:



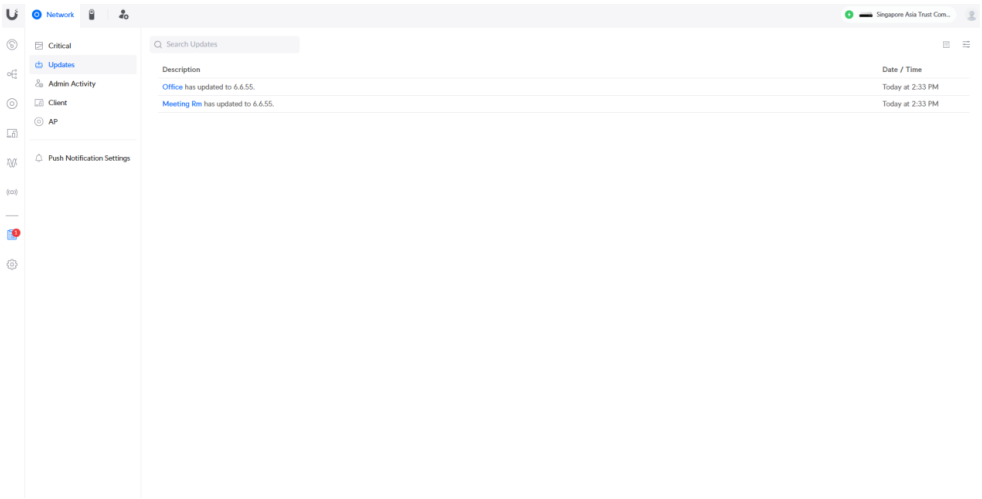
Ubiquiti AP Controller Network Analysis Picture:



Ubiquiti AP Controller Log Report Status Picture:



Ubiquiti AP Controller Firmware Status Picture:

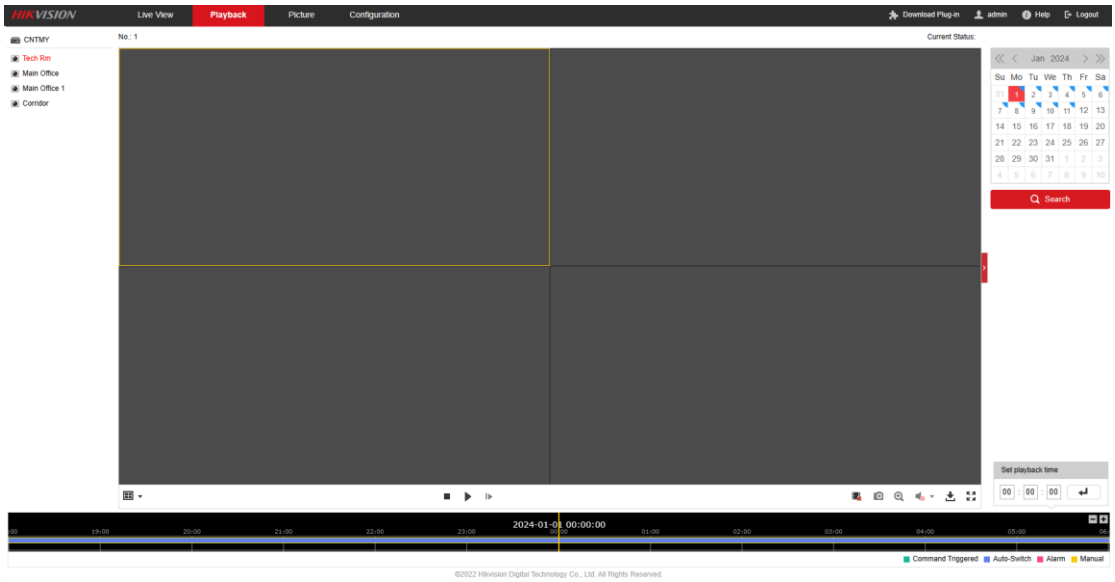


1.7 CCTV Maintenance

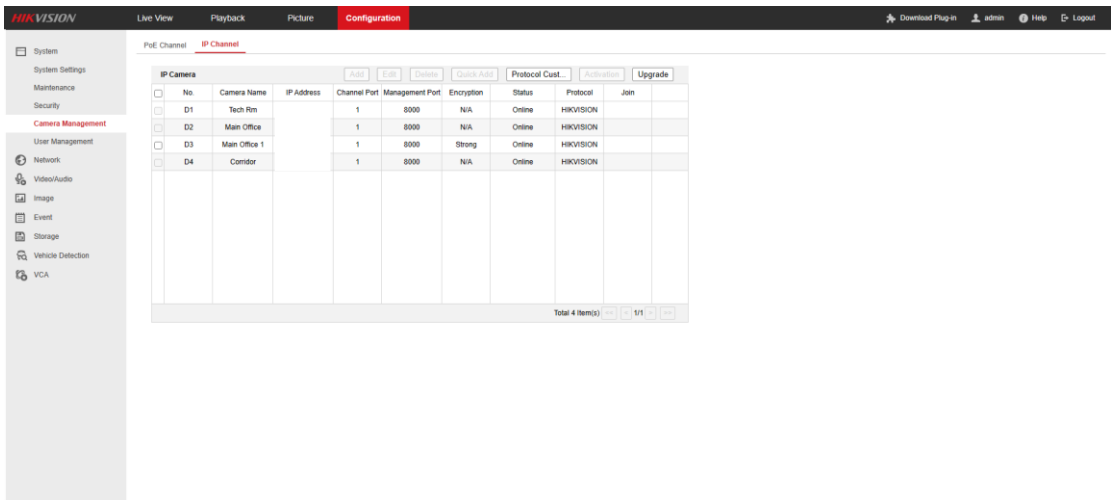
We will check CCTV record performance review, CCTV camera network communication, CCTV storage management, CCTV software update and CCTV security audit. We will check the recording and playback quality to ensure that the system is performing as expected. We will ensure that the network settings are correct, and that the NVR is communicating effectively with the cameras and any other integrated systems. We will check the available storage space and manage old recordings to ensure that the system does not run out of space, which could prevent new recordings. We will check if CCTV systems require software updates or patches to improve functionality and security. We will review user access logs, check for unauthorized access attempts, and ensure that the system is secure from potential cyber threats.

Hikvision NVR CCTV Device

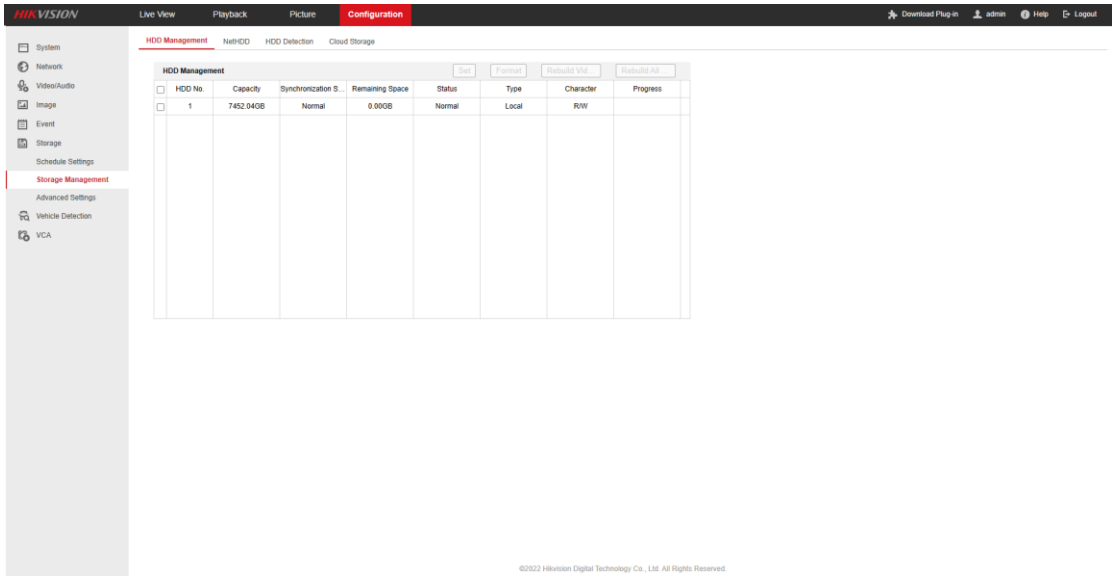
CCTV Record Performance Review Picture:



CCTV Camera Network Communication Status Picture:



CCTV Storage Management Status Picture:



CCTV Software Firmware & Log report Status Picture: