

IT Hardware Maintenance / Services

Menu

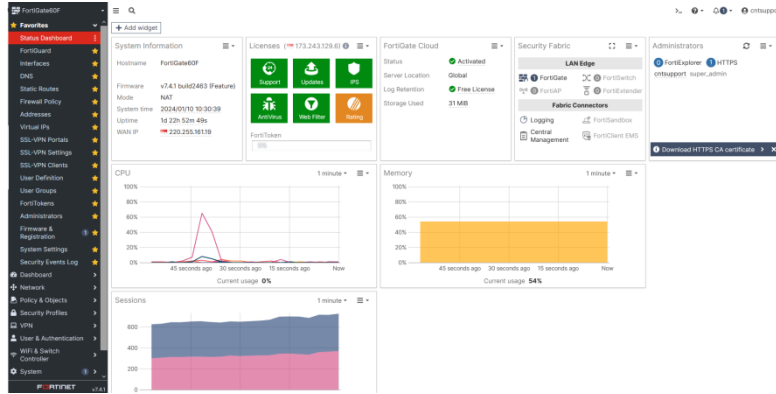


1.1 Firewall Maintenance	2
1.2 Windows Server Maintenance	6
1.3 NAS Maintenance	10
1.4 UPS Maintenance	12
1.5 Managed Switch Maintenance	13
1.6 Access Point Maintenance	15
1.7 CCTV Maintenance	17

1.1 Firewall Maintenance

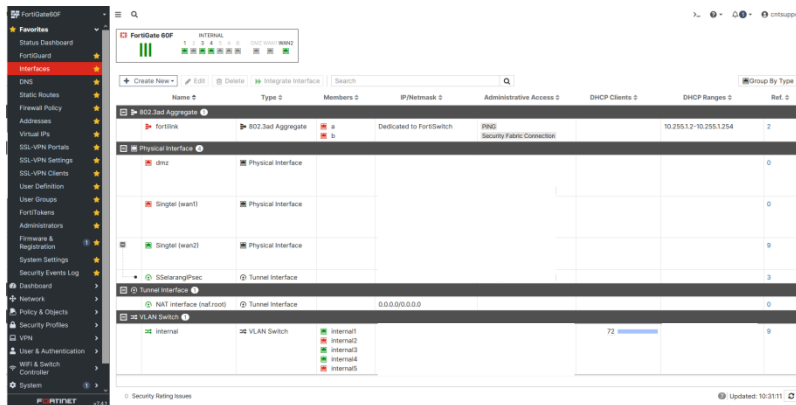
Firewall System Performance Status

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.



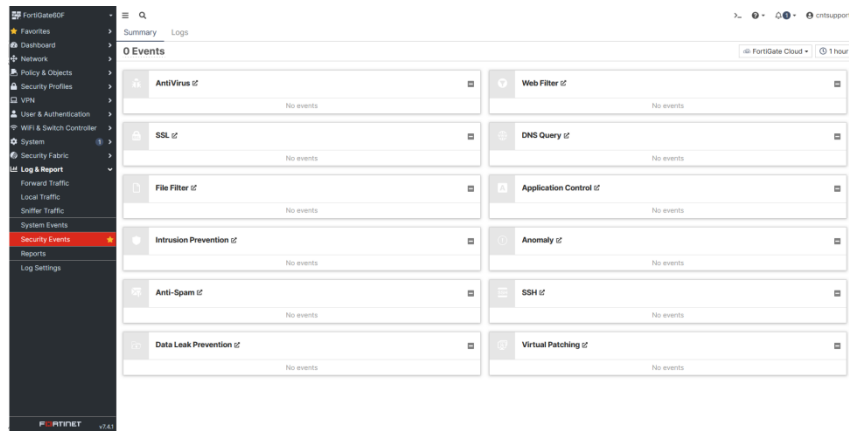
Firewall Port Status

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.

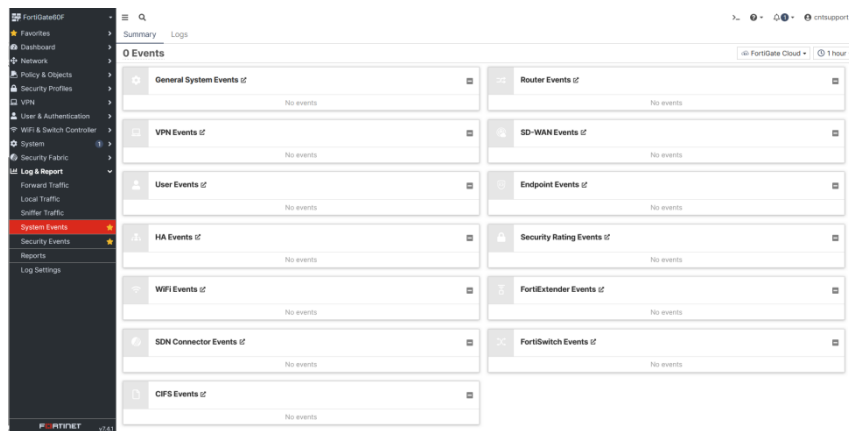


Firewall Security / System Events Summary & Logs

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.

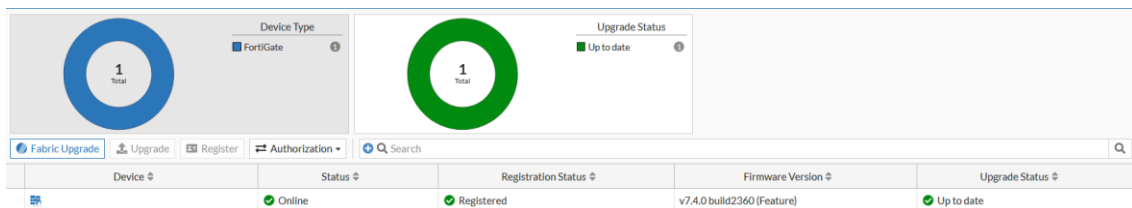


We will check system events Summary and Logs are a comprehensive collection of records that detail the operational status, security incidents, and other significant events that occur within a network protected by a FortiGate firewall. These logs are essential for network administrators to ensure ongoing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



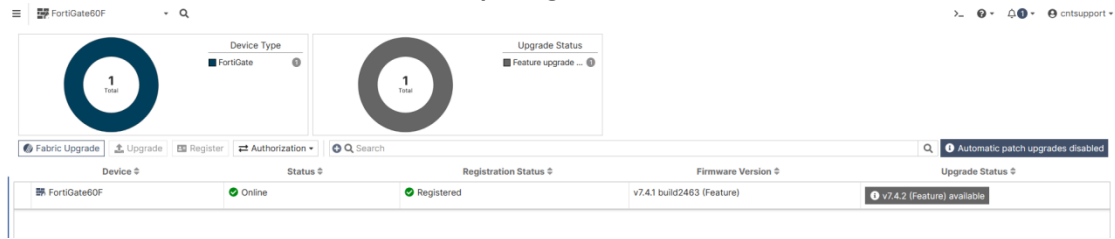
Firewall System Firmware

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.



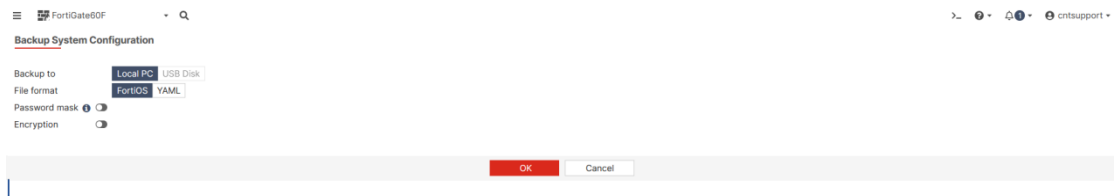
Case Study:

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

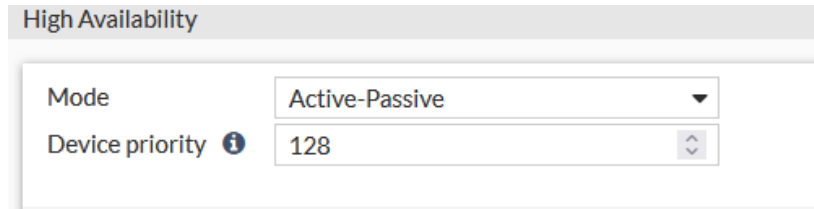
Identify login attempt. This includes details such as IP address, usernames and timestamps and number of failed login attempts.

The screenshot shows the 'Logs' section of the FortiGate60F management console. The logs table displays the following data:

Date/Time	Level	User	Message	Log Description
2023/08/10 17:32:41	Warning		of 3 bad attempts	Admin login disabled
2023/08/10 17:32:41	Warning		of 3 bad attempts	Admin login disabled
2023/08/10 17:32:41	Warning		of 3 bad attempts	Admin login disabled
2023/08/10 17:32:41	Warning		of 3 bad attempts	Admin login disabled
2023/08/10 17:32:40	Warning		of 3 bad attempts	Admin login disabled
2023/08/10 17:32:40	Warning		of 3 bad attempts	Admin login disabled
2023/08/10 17:32:39	Warning		of 3 bad attempts	Admin login disabled
2023/08/10 17:32:39	Warning		of 3 bad attempts	Admin login disabled

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.



The screenshot shows the FortiGate HA cluster status table. The table has columns for Status, Priority, Hostname, Serial No., Role, System Uptime, Sessions, and Throughput. Two devices are listed, both in a 'Synchronized' state with a priority of 128. The Primary device has a system uptime of 16h 57m, 711 sessions, and a throughput of 11.05 Mbps. The Secondary device has a system uptime of 16h 57m, 340 sessions, and a throughput of 37.00 kbps.

Status	Priority	Hostname	Serial No.	Role	System Uptime	Sessions	Throughput
Synchronized	128			Primary	16h 57m	711	11.05 Mbps
Synchronized	128			Secondary	16h 57m	340	37.00 kbps

Case Study:

3. Ensuring Network Continuity with Firewall High Availability

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

Troubleshoot:

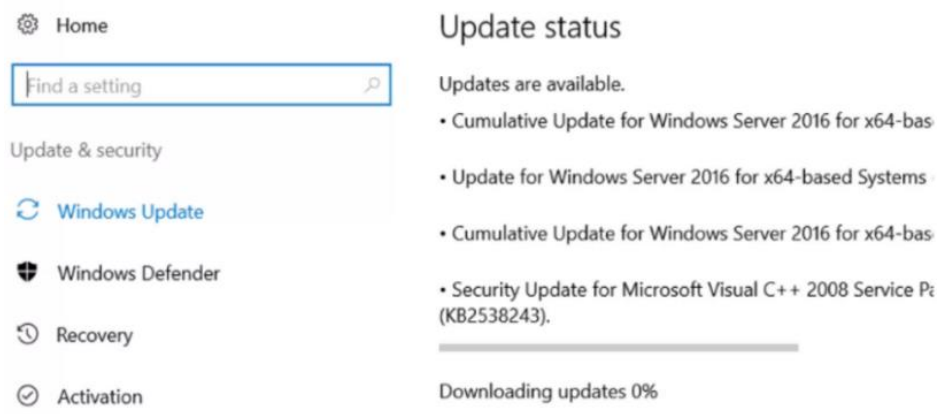
High Availability Response:

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

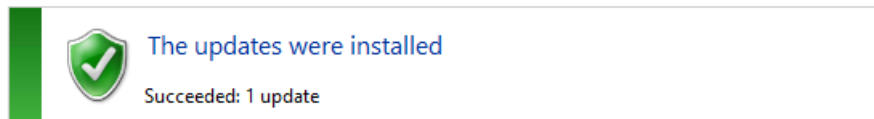
Windows Server Update & Patches

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.



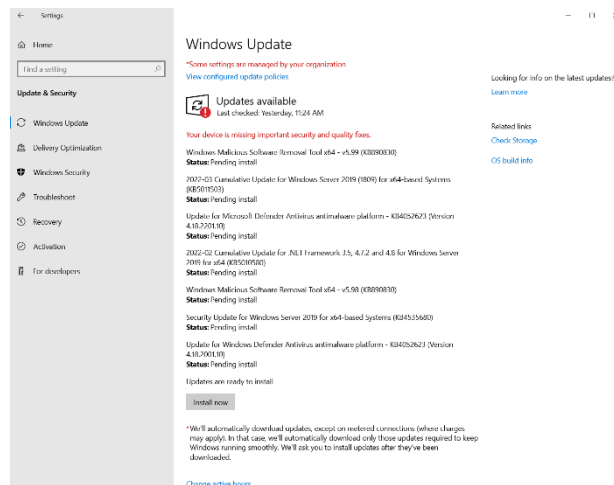
Quality updates include bug fixes, improvements, and optimizations for various aspects of the Windows Server OS. Quality updates are aimed at providing a smoother and more reliable operating system environment.

Windows Update



Most recent check for updates: Today at 2:58 PM
Updates were installed: Today at 4:36 PM.
You receive updates: For Windows only.

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:**

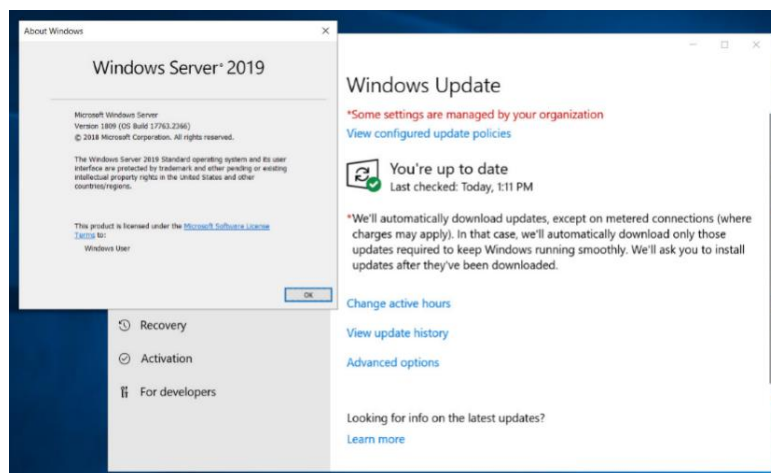
Without the latest security patches, the system becomes more susceptible to malware infections, such as viruses, ransomware, and spyware. Malware can cause data loss, system damage, and compromise sensitive information.

- **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.

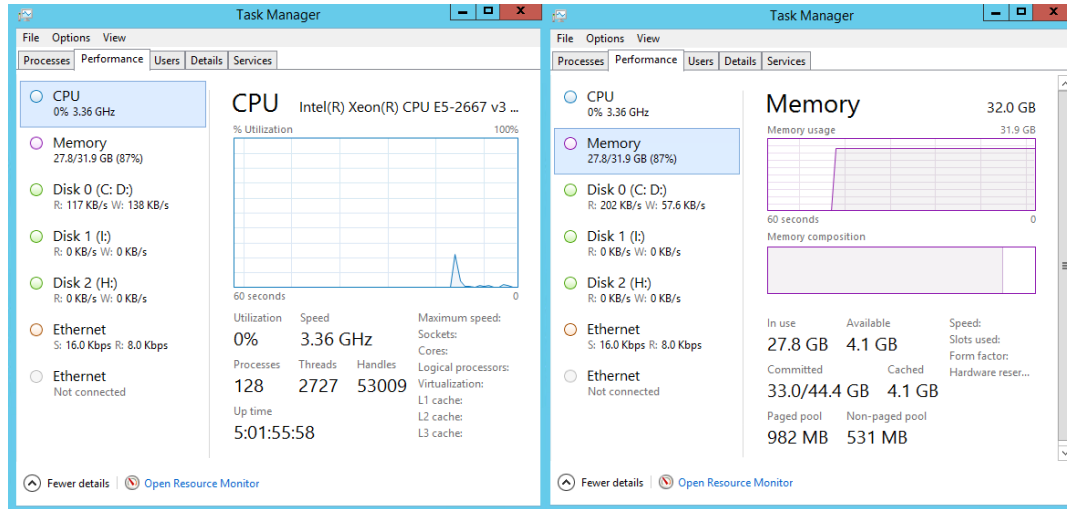
- **Software Compatibility Problems:**

Newer software applications and drivers may not be fully compatible with an outdated operating system, resulting in compatibility issues and potential crashes.

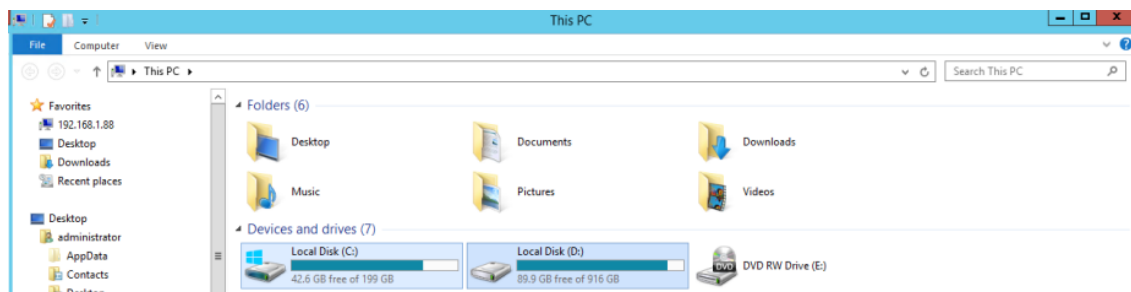
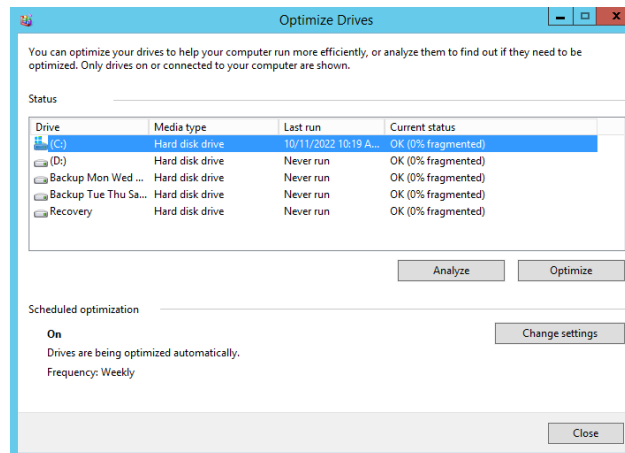


Windows Server Performance Optimizations

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:

The screenshot shows the 'Storage' section of the iDRAC interface. The 'Controllers' tab is selected, displaying a table of RAID controllers. Below the table, the 'Controller Battery' status is shown as 'Ready'.

Rollup Status	Name	Device Description	PCI Slot	Firmware Version	Driver Version	Cache Memory Size	Actions
+	PERC H755 Adapter	RAID Controller in Slot 1	1	62.21.0-4606	7.722.02.00	8192 MB	Actions

Status	Battery Name	Device Description	State	Controller Name
+	Battery	Battery on RAID Controller in Slot 1	Ready	PERC H755 Adapter

Server Power Supply Status Picture:

The screenshot shows the 'System' section of the iDRAC interface. The 'Power' tab is selected, displaying a table of power supplies and a power usage graph.

Health	Name	Status	Input Wattage	Rated	Actual	FW Version	Part Number	Input Line Type	Type
+	PS1 Status	Present	927	800	800	00.1B.53	DMGPPCA02	High line	AC
+	PS2 Status	Present	927	800	800	00.1B.53	DMGPPCA02	High line	AC

Power

Capacity: 17.95%

Raw Power Reading: 190 Watts
Warning Threshold: 840 Watts
Failure Threshold: 936 Watts

Historical Trends:

- Average Usage: 182 Watts | 621 BTU/hr
- Max Peak: 198 Watts | 678 BTU/hr
- Max Peak Time: Wed Jan 10 17:32:21 2024
- Min Peak: 179 Watts | 611 BTU/hr
- Min Peak Time: Wed Jan 10 16:40:05 2024

Present Power Reading and Thresholds

Probe Status	Probe Name	Present Reading	Warning Threshold	Failure Threshold
+	System Board Pwr Consumption	168 Watts 573 BTU/hr	840 Watts 2867 BTU/hr	936 Watts 3196 BTU/hr

Server Cooling Fan Status Picture:

The screenshot shows the 'System' section of the iDRAC interface. The 'Cooling' tab is selected, displaying a 'Cooling Overview' and a 'Temperature Overview'.

Cooling Overview

- Fan Status: ✔
- Redundancy Status: Full
- Average Fan Speed: 28% PWM
- Net System Airflow: N/A
- Thermal Profile Optimization: Default Thermal Profile Settings (Maximum Performance)
- Fan Speed Offset: Off
- Minimum Fan Speed: Default (28% PWM)
- PCIe Airflow Settings: Automatic

Temperature Overview

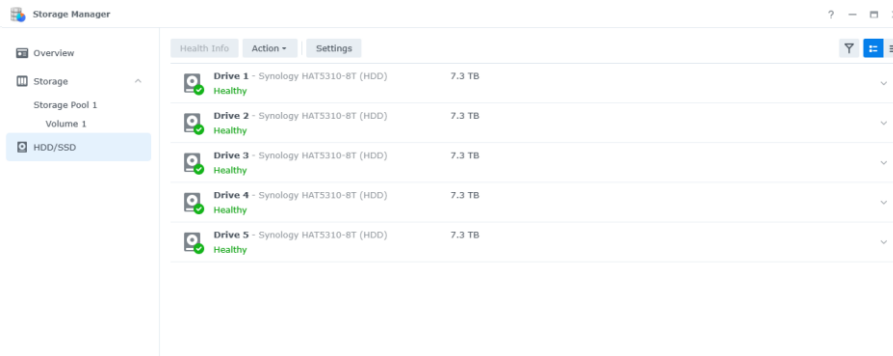
- Temperature Status: ✔
- System Inlet Temperature: 20 °C (68.0 °F)
- System Inlet Temperature Support Limit for this configuration: 35 °C (95.0 °F)
- ASHRAE Category: A2

1.3 NAS Maintenance

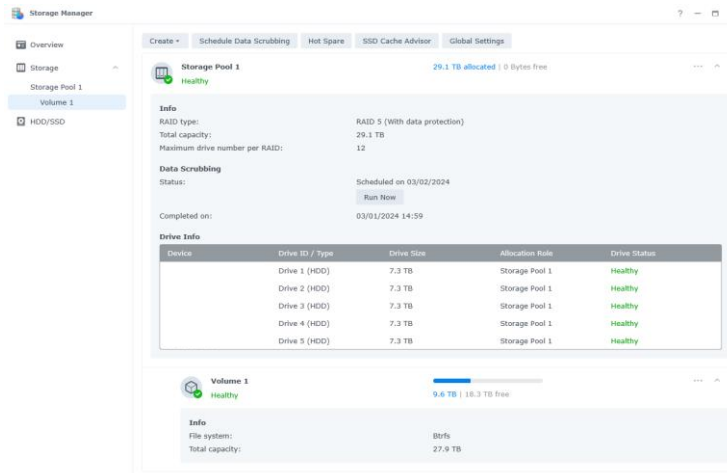
NAS Storage Manager Status

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:



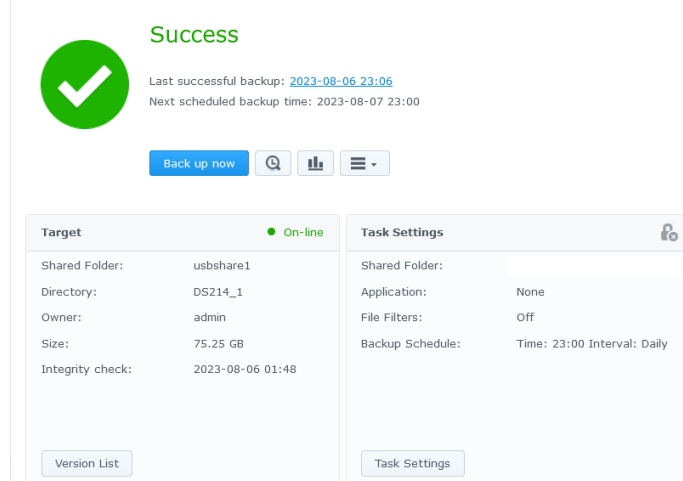
RAID Controller Status Picture:



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:



The screenshot displays the Synology Backup Status interface. At the top, a large green checkmark icon is accompanied by the word "Success" in green. Below this, the text indicates the last successful backup was on 2023-08-06 at 23:06, and the next scheduled backup is for 2023-08-07 at 23:00. A "Back up now" button is visible, along with search, bar chart, and menu icons. The interface is divided into two main sections: "Target" and "Task Settings".

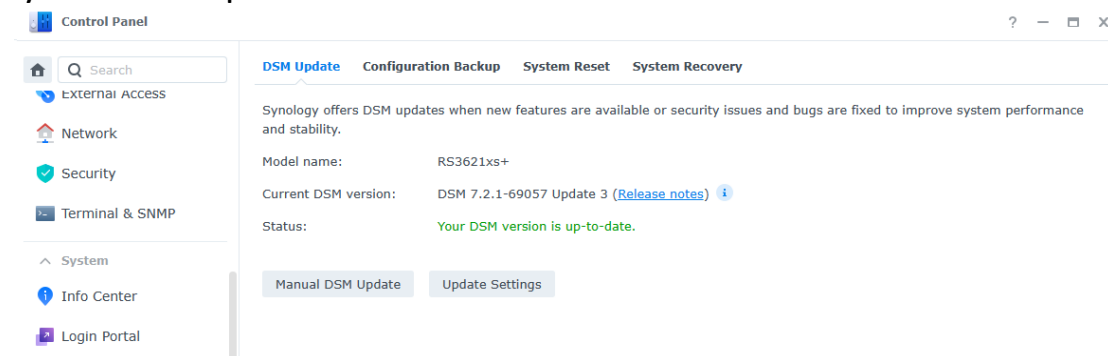
Target	Task Settings
Shared Folder: usbshare1	Shared Folder:
Directory: DS214_1	Application: None
Owner: admin	File Filters: Off
Size: 75.25 GB	Backup Schedule: Time: 23:00 Interval: Daily
Integrity check: 2023-08-06 01:48	

Buttons for "Version List" and "Task Settings" are located at the bottom of their respective sections.

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:



The screenshot shows the "DSM Update" page within the Synology Control Panel. The page title is "Control Panel" and it includes standard window controls. The navigation menu on the left includes External Access, Network, Security, Terminal & SNMP, System, Info Center, and Login Portal. The main content area has tabs for "DSM Update", "Configuration Backup", "System Reset", and "System Recovery". The "DSM Update" tab is active, displaying the following information:

- Synology offers DSM updates when new features are available or security issues and bugs are fixed to improve system performance and stability.
- Model name: RS3621xs+
- Current DSM version: DSM 7.2.1-69057 Update 3 ([Release notes](#))
- Status: Your DSM version is up-to-date.

Buttons for "Manual DSM Update" and "Update Settings" are located at the bottom of the page.

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:

The screenshot shows a dashboard with three main sections: BATTERY, DEVICE, and FIRMWARE. The BATTERY section displays four metrics: RUNTIME (7 mins), CHARGE (100%), TEMPERATURE (24°C), and REPLACE BY (Jan 26, 2025). The FIRMWARE section shows the current version (v 03.7 (1015)) and a status message: "Your firmware is up to date with the latest version." with a "VIEW MORE" button.

BATTERY			
RUNTIME	CHARGE	TEMPERATURE	REPLACE BY
7 mins	100%	24°C	Jan 26, 2025

DEVICE

FIRMWARE

CURRENT VERSION

v 03.7 (1015)

✔ Your firmware is up to date with the latest version.

[VIEW MORE](#)

UPS Battery Diagnostics Picture:

The screenshot shows the "DIAGNOSTICS" section with two tabs: "UPS SELF TEST" and "AUDIBLE ALARM". The "UPS SELF TEST" tab is active, displaying the "Last Test Result: PASSED" in green text. Below the result is a blue button labeled "RUN NEW TEST".

DIAGNOSTICS

UPS SELF TEST | AUDIBLE ALARM

Last Test Result:
PASSED

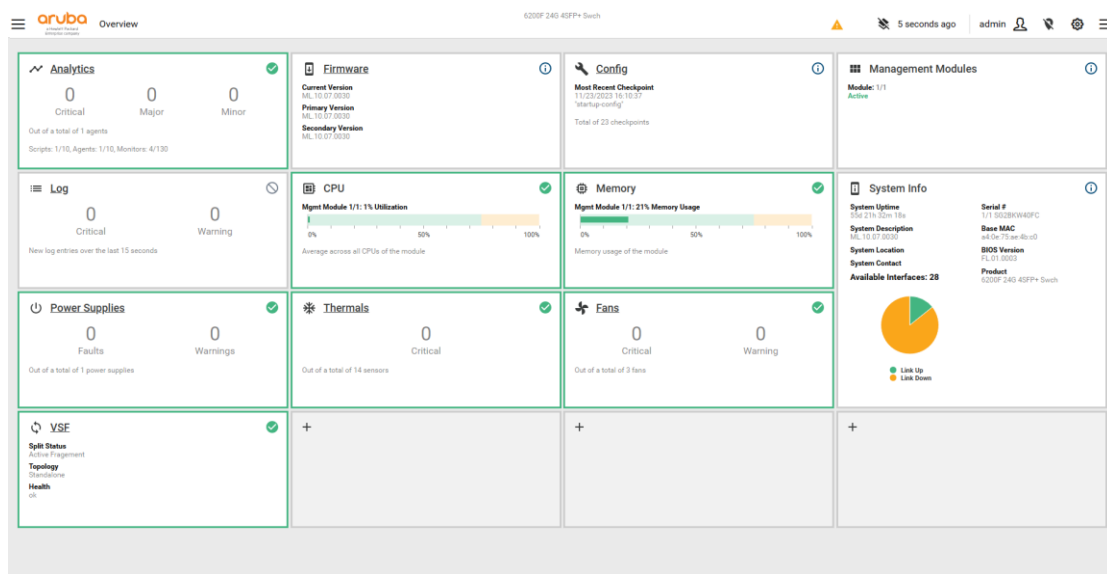
[RUN NEW TEST](#)

1.5 Managed Switch Maintenance

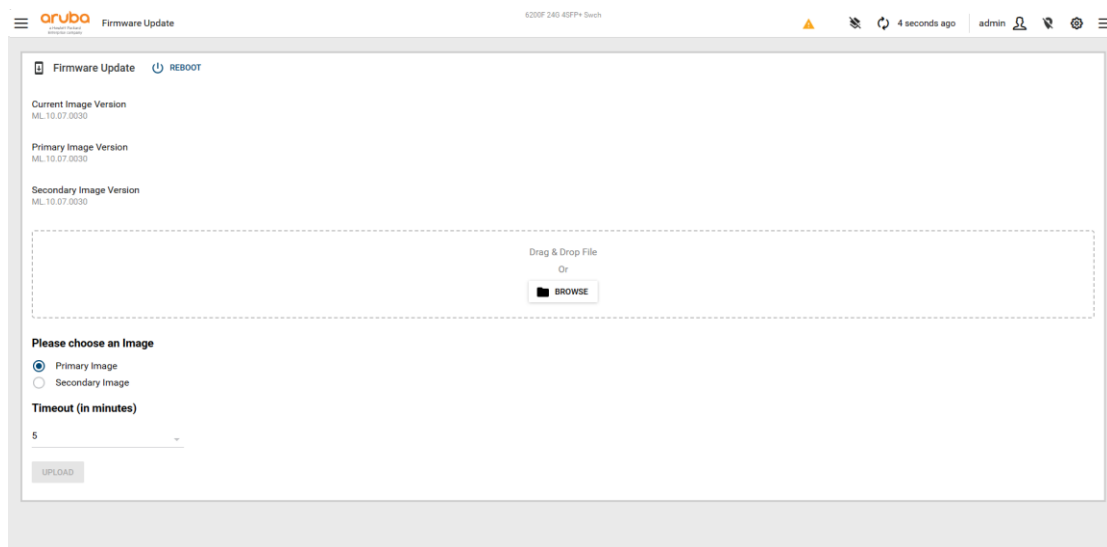
We will check network performance monitoring, firmware updates, configuration backups, security audits, and redundancy checks. We will use network management tools to monitor the performance of the switch. Look for anomalies such as high collision rates, CRC errors, or unexpected traffic patterns. We 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:

The screenshot shows the Aruba Config Mgmt interface for a switch (6200F 240 4SFP+ Swch). The 'Checkpoints' section displays a table of configuration backups:

Name	Date	Version
startup-config	01/11/24 13:37:56	ML.10.07.0030
CPC20230721183727_6200	07/22/23 02:37:27	ML.10.07.0030
CPC20230721182527_6200	07/22/23 02:25:27	ML.10.07.0030
CPC20230721165029_6200	07/22/23 00:50:29	ML.10.07.0030
CPC20230721155622_6200	07/21/23 23:56:22	ML.10.07.0030
CPC20230721151650_6200	07/21/23 23:16:50	ML.10.07.0030
CPC20230614094842_6200	06/14/23 17:48:42	ML.10.07.0030
CPC20230614092045_6200	06/14/23 17:20:45	ML.10.07.0030
CPC20230614090655_6200	06/14/23 17:06:55	ML.10.07.0030
CPC20230614085646_6200	06/14/23 16:56:46	ML.10.07.0030
CPC20230614071237_6200	06/14/23 15:12:37	ML.10.07.0030
CPC20230614070201_6200	06/14/23 15:02:01	ML.10.07.0030
CPC20230614064204_6200	06/14/23 14:42:04	ML.10.07.0030

Below the table is an 'Upload' section with a dashed box for file upload, a 'BROWSE' button, and an 'UPLOAD' button.

Managed Switch Log Report Status Picture:

The screenshot shows the Aruba Analytics Dashboard for the same switch. It features several panels:

- Agents:** Shows 'system_resource_monitor.default' with a status of 'Normal'.
- Scripts:** Shows 'system_resource_monitor'.
- Alerts:** A table of recent alerts:

Time	Agent	Rule	Action(s)
06/09/23 14:14:43	system_resource_mon-	Medium-Term Normal CI	ALERT_LEVELSNMPYSLOG
06/09/23 14:14:31	system_resource_mon-	Medium-Term High CPU	ALERT_LEVELCL(3)SNMP-
05/17/23 14:48:11	system_resource_mon-	Medium-Term Normal CI	ALERT_LEVELSNMPYSLOG
05/17/23 14:48:06	system_resource_mon-	Medium-Term High CPU	ALERT_LEVELCL(3)SNMP-

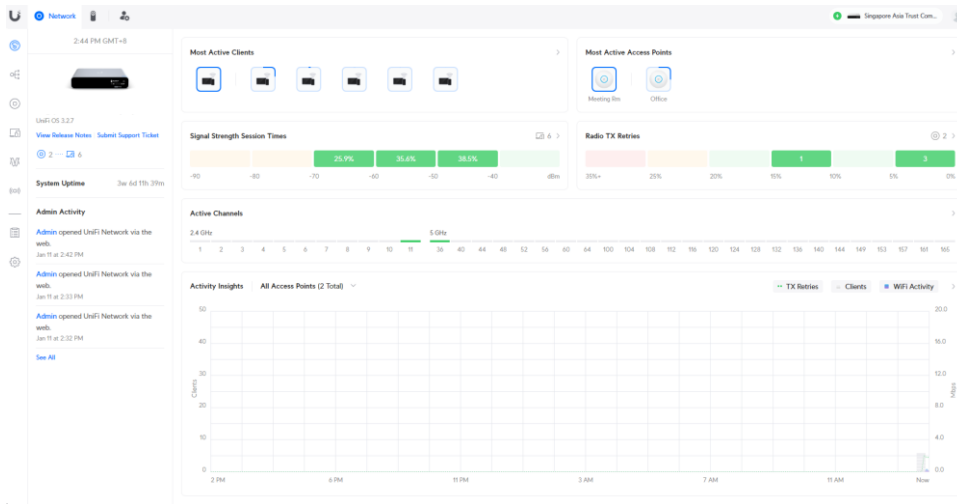
There is also a line graph for 'system_resource_mon...' showing data points over time (13:35 to 13:41). The dashboard includes an 'ARUBA EXCHANGE' banner and several placeholder charts.

1.6 Access Point Maintenance

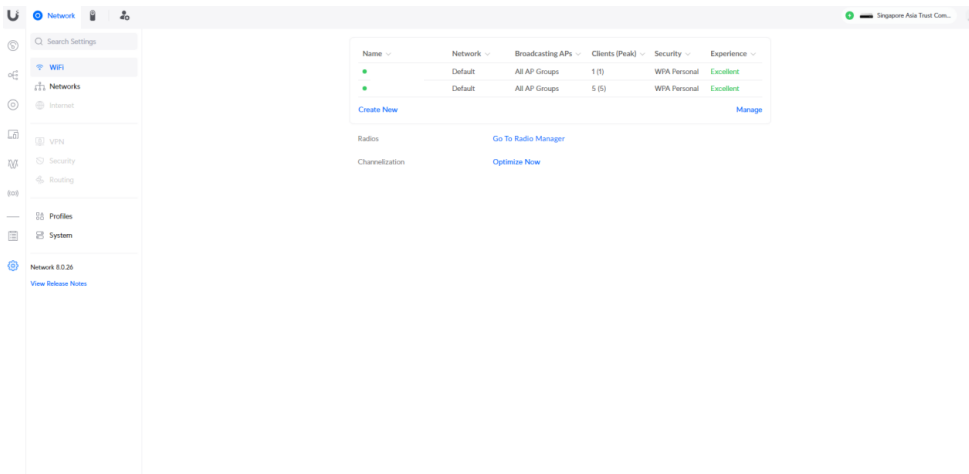
We will check AP performance monitoring, configuration management, network analysis, security audits and firmware updates. We will be monitoring the performance of access points to ensure they are providing the expected coverage and speed. This can involve checking signal strength, noise levels, and 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

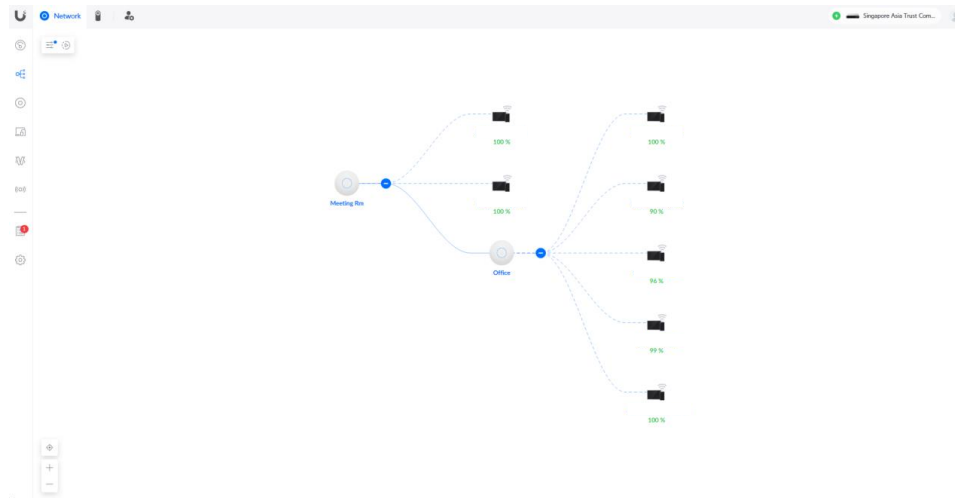
Ubiquiti AP Controller Performance Monitoring Picture:



Ubiquiti AP Controller Wi-Fi configuration management Picture:



Ubiquiti AP Controller Network Analysis Picture:



Ubiquiti AP Controller Log Report Status Picture:

This screenshot displays the 'Critical' log report in the Ubiquiti AP Controller. The report lists several system critical events, including IP address conflicts and power-related issues for the 'Office' and 'Meeting Rm' nodes. Each entry includes a description, a date, and a time. A search bar is visible at the top of the log area.

Description	Date / Time
1 Unresolved System Critical Event	
Multiple devices are using the same IP address. Please check each device's configuration to ensure none are communicating with a rogue DHCP server.	Today at 2:59 PM
Office is offline. Please ensure it's receiving sufficient power. If so, but it's still offline, replace the power cable to confirm that the original isn't damaged. Learn more	Dec 16, 2023 7:48 AM
Office is offline. Please ensure it's receiving sufficient power. If so, but it's still offline, replace the power cable to confirm that the original isn't damaged. Learn more	Dec 16, 2023 5:02 AM
Multiple devices have reconnected. Click to view them.	Dec 15, 2023 6:06 PM
Meeting Rm has reconnected.	Dec 15, 2023 11:36 AM
Multiple devices have reconnected. Click to view them.	Dec 15, 2023 10:01 AM
Meeting Rm has reconnected.	Dec 15, 2023 8:35 AM
Meeting Rm is offline. Please ensure it's receiving sufficient power. If so, but it's still offline, replace the power cable to confirm that the original isn't damaged. Learn more	Dec 15, 2023 7:57 AM
Office has reconnected. This has happened multiple times in the past 24 hours. Please ensure that it has sufficient power and its cabling is not damaged. Learn more	Dec 15, 2023 7:29 AM
Multiple devices have reconnected. Click to view them.	Dec 15, 2023 6:09 AM
Office is offline. Please ensure it's receiving sufficient power. If so, but it's still offline, replace the power cable to confirm that the original isn't damaged. Learn more	Dec 15, 2023 5:25 AM
Meeting Rm has reconnected.	Dec 15, 2023 5:04 AM
Meeting Rm is offline. Please ensure it's receiving sufficient power. If so, but it's still offline, replace the power cable to confirm that the original isn't damaged. Learn more	Dec 15, 2023 4:26 AM
Multiple devices have reconnected. Click to view them.	Dec 15, 2023 3:38 AM
Office is offline. Please ensure it's receiving sufficient power. If so, but it's still offline, replace the power cable to confirm that the original isn't damaged. Learn more	Dec 15, 2023 3:19 AM
Meeting Rm is offline. Please ensure it's receiving sufficient power. If so, but it's still offline, replace the power cable to confirm that the original isn't damaged. Learn more	Dec 12, 2023 4:53 AM
Office is offline. Please ensure it's receiving sufficient power. If so, but it's still offline, replace the power cable to confirm that the original isn't damaged. Learn more	Dec 11, 2023 11:45 AM
Multiple devices are using the same IP address. Please check each device's configuration to ensure none are communicating with a rogue DHCP server.	Dec 7, 2023 3:11 PM
Multiple devices are using the same IP address. Please check each device's configuration to ensure none are communicating with a rogue DHCP server.	Dec 6, 2023 9:09 AM
Multiple devices are using the same IP address. Please ensure they are not communicating with a rogue DHCP server.	Dec 1, 2023 9:16 AM
Multiple devices are using the same IP address. Please ensure they are not communicating with a rogue DHCP server.	Nov 28, 2023 9:10 AM
Multiple devices are using the same IP address. Please check each device's configuration to ensure none are communicating with a rogue DHCP server.	Nov 28, 2023 9:07 AM

Ubiquiti AP Controller Firmware Status Picture:

This screenshot shows the 'Updates' section of the Ubiquiti AP Controller. It displays a list of firmware updates for the 'Office' and 'Meeting Rm' nodes. The 'Office' node was updated to version 6.6.55 at 2:33 PM today, and the 'Meeting Rm' node was updated to the same version at 2:33 PM today. A search bar is located at the top of the updates list.

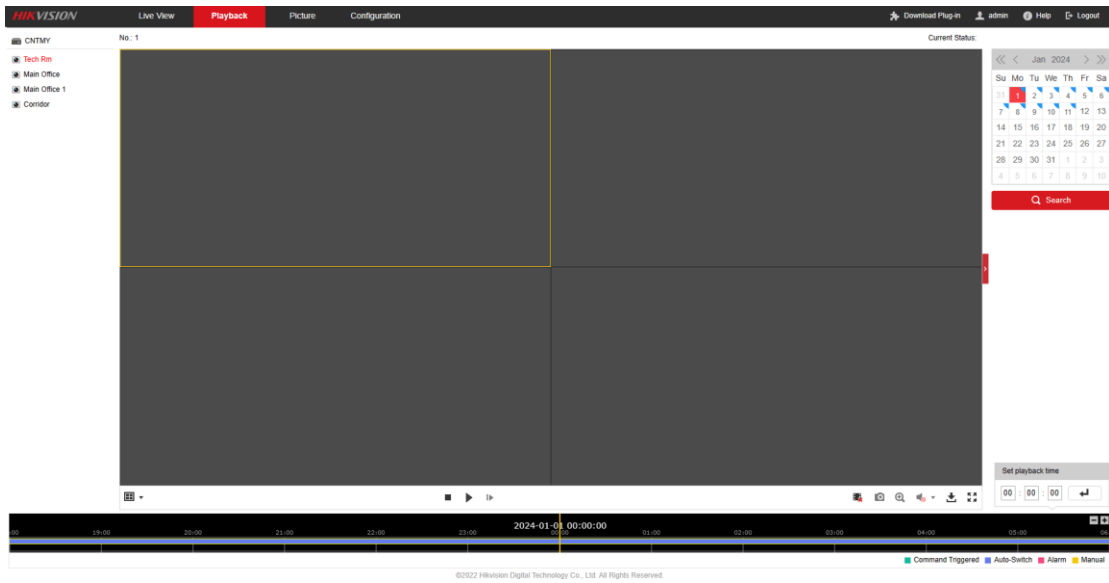
Description	Date / Time
Office has updated to 6.6.55.	Today at 2:33 PM
Meeting Rm has updated to 6.6.55.	Today at 2:33 PM

1.7 CCTV Maintenance

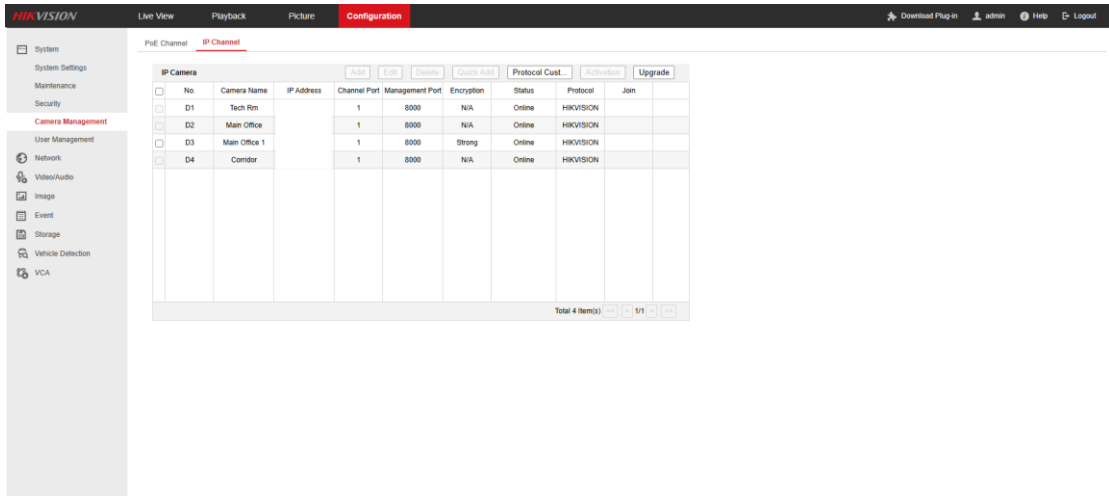
We will check CCTV record performance review, CCTV camera network communication, CCTV storage management, CCTV software update and CCTV security audit. We will check the recording and playback quality to ensure that the system is performing as expected. We will ensure that the network settings are correct, 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:

The screenshot shows the 'Configuration' tab of the Hikvision web interface, specifically the 'HDD Management' section. The page includes a navigation menu on the left with options like System, Network, Video/Audio, Image, Event, Storage, and Storage Management. The main content area displays a table with the following data:

HDD No.	Capacity	Synchronization S.	Remaining Space	Status	Type	Character	Progress
1	7452.040B	Normal	0.000B	Normal	Local	RW	

Below the table, there are buttons for 'See', 'Format', 'Rebuild Vol', and 'Rebuild All'. At the bottom of the page, the copyright notice reads: ©2022 Hikvision Digital Technology Co., Ltd. All Rights Reserved.

CCTV Software Firmware & Log report Status Picture:

The screenshot shows the 'Upgrade & Maintenance' section of the Hikvision web interface. The page includes a navigation menu on the left with options like System, System Settings, Maintenance, Security, Camera Management, User Management, Network, Video/Audio, Image, Event, Storage, Vehicle Detection, and VCA. The main content area displays the following options:

- Reboot:** A 'Reboot' button with the description 'Reboot the device'.
- Default:** Two buttons: 'Simple Restore' (Reset all the parameters, except the IP parameters and user information, to the default settings.) and 'Default' (Restore all device parameters to default settings.).
- Export:** A 'Device Parameters' button.
- Import Config. File:** A text input field for the file path, with 'Browse' and 'Import' buttons.
- Upgrade:** A 'Firmware' dropdown menu, a text input field for the file path, and 'Browse' and 'Upgrade' buttons.

Below the upgrade section, there is a status field and a note: 'Note: The upgrading process will be 1 to 10 minutes, please don't disconnect power to the device during the process. The device reboots automatically after upgrading.'