Technical Note NVT-0039

Release date: 12/2025

Technical Note Description;

The notes below contain instructions to aid identifying common faults with Dedicated Micros / NetVu third generation (Gen3) DVR and NVR units.

Product Models Covered;

DM/SD/xx/yy, DM/SDA/xx/yy, DM/SDACP/xx/yy, DM/DVIP/xx/yy, DM/SDANVR/xx/yy, DM/NVRM/xx/yy, DM/SDHDA/xx/yy, DM/ECS2/xx/yy, DM/ECS1/xx/yy, DM/ECO4/xx/yy, DM/NV1/xx/yy.

Introduction;

All NetVu third generation units load their application software in three stages, these are;

1. Initial boot loader from internal boot ROM.
2. Intermediate loader from FLASH memory.
3. Main application from an internal micro SD card.

For the unit to boot successfully all of the above steps must be completed correctly.

Steps 1 and 2 occur almost instantly at power on. If they fail to complete then the unit will present as “dead”. Depending on the model it may display some LED activity on its front panel as there is a small microcontroller on this panel that attempts to “talk to” the unit’s main CPU and will indicate if it can not establish communication by flashing the RED LED.

The front panel also contains a small “beeper” which should emit a single “beep” when mains power is applied.

If you do not hear a beep and there are no LED’s illuminated on the front panel the prime suspect is the power supply, on all units except the Ecosense, Eco4, NVR Media Server, SDANVR, and NV1 this is a 1U 350W ATX PC power supply. These can be tested with a PC power supply tester to confirm correct operation and if found to be faulty can be replaced with an off the shelf unit.

The Ecosense, Eco4 and NV1 units use a 12v external supply, whose pinout is uncommon, so replacement supplies should be purchased from NetVu Ltd.

The NVR Media Server and SDANVR units use an external 48V power supply as this is also used to deliver the 48v POE power to the cameras. Replacement supplies should be obtained from NetVu Limited.

If the unit “beeps” and the LED on the front panel flashes RED continually then the power supply is probably OK, but the unit is failing to complete its boot sequence for some reason. This can be caused by several things, the most common being a failed system micro SD card, or failed CODEC (video input) card.

The easiest way to establish the failure mode at this point is to use “Serial Debug”. All Gen3 Dedicated Micros / NetVu units output debug information on serial port 1 at 115200 Baud, 8,N,1 however it is appreciated that not all engineers have access to a PC with a serial port, or USB to serial converter as well as the required “null modem” cross over serial lead (one of which was supplied with every unit at the time of manufacture, but not many seem to have remained available), so this guide will attempt to progress without reference to serial debug unless absolutely required.

Some idea as to whether the fault is with the system micro SD card or the CODEC’s can be obtained by watching the flashing LED on the front panel. The LED on most units is “Bicolour” which means it can flash RED or GREEN.

If the unit is reading the micro SD card the LED will change colour from RED to GREEN as the main software application loads and runs. If it then returns to flashing RED again rather than turning solid GREEN this indicates that the unit has reset and the boot sequence has restarted. This is more likely to be a CODEC failure. See the next section to help identify which CODEC has failed.

If the unit is failing to read the micro SD card then the LED will not change from RED to GREEN, it will continually flash RED. Depending on the failure mode of the micro SD card you may see the text “Initialising Bootloader” displayed on the main MON A output, This text usually clears within 15 - 20 seconds of initial power up. If the card has only partially failed the unit can sometimes read the initial loader from the card, but fails to load the rest of the software. More often than not nothing is displayed on the main monitor and the LED remains flashing RED.

With the front panel LED just flashing RED and never turning GREEN the next step should be to test and replace the system micro SD card. The easiest way to do this is by removing the card from the card slot on the DVR / NVR main board. There is only one micro SD card slot in all of the desktop models, it is either located on the front right hand corner of the main board (in the SD Advance range), towards the rear centre (NVR Media Server, SDANVR), or in the front left hand corner (Ecosense).

The quickest way to test the micro SD card is to remove it from the unit and place it in a card reader on a PC. The card is formatted FAT32 so should be visible on any computer operating system (Windows, Linux, MacOS). If the card can not be read via a card reader then it will not work in a DVR / NVR.

However some cards can partially fail and can still be accessed via a PC, cards that have failed in this manner will usually take very long periods to respond, and show signs of data corruption on the PC with obviously corrupt file names. If a card is not accessible “instantly”, and contains corrupt file names then it is also faulty.

If in doubt try a replacement card.

Instructions on how to create a new system micro SD card for the system can be found in FAQ NVT-001 at www.netvu.org.uk (https://netvu.org.uk/wp-content/uploads/2022/02/NVT-001-NVT-Replace-SD-Card.pdf).

If the micro SD card is still partially accessible using a PC card reader then it is recommended that you copy the following files to the PC as a backup, and to allow you to easily restore the system settings in the event of a future failure.

From the /etc folder on the micro SD card copy the file USER.DB this contains the usernames and passwords.

From the /frm_data folder on the micro SD card copy the file master.sfm this contains all system settings.

If you are working on an NVR Media Server, or SDANVR copy the file closediptv.sql from the /sql folder. This contains the closedip camera database.

If your unit has any additional features (3rd party IP camera support, tripwire, object left and removed Etc) then you should also copy the file license.txt from the /etc/lic folder. If you can not copy this file then you will need to contact NetVu for a copy of the license key.

If the card has failed completely and you are unable to copy these three files then when you install the replacement card the unit will start up in factory shipping condition, and you will have to add user accounts, configure camera names, alarm inputs and responses, ARC settings Etc manually.

The unit should detect and configure NetVu IP cameras automatically. You will have to add any third party cameras manually.

None Volatile settings (Network configuration, System name, Drive mappings, Etc) are not affected by micro SD card failure, so the unit should still be accessible remotely.

If you deal with a large estate containing the same model of unit it is advisable to carry a “test card” containing the correct software for the unit. This can effectively be inserted as a quick go / no go test.

To sum up identifying micro SD card issues with no access to serial debug, the card is probably faulty if any of the following symptoms are present.

1. Flashing RED light on the front panel that never goes green.
2. A black screen on the main monitor displaying “Initialising Bootloader”, that never clears.
3. Failure to complete the boot process with no access to the unit available, and the main monitor output freezing part way through the process, either displaying a white screen, or partial display.

CODEC Issues;

The analogue / hybrid Gen3 units (SDA, SDACP, SDAHD, and DVIP) all contain a number of plug in CODEC cards, these are video digitizers that convert the analogue (composite video) into a digital format that can then be stored on the internal hard drive/s or streamed via a network.

The number of cards (and card type) varies depending on the model number of the unit. As a rule of thumb the more "powerful" the unit the more CODEC cards it contains. An eight channel unit can contain as few as two CODEC cards, as each card can contain a quad video encoder (digitizer). A thirty two channel real time unit (DVIPRT) will contain 16 CODEC cards (each card contains two encoders to provide real time performance).

However all of these systems perform in the same way as far as fault finding is concerned.

When the main software starts up it checks its “unlock code” which tells it how many CODEC cards it should have, it then attempts to load software into each of these cards and verify that they are operating correctly.

If a card fails to start up the software will trigger a reboot in an attempt to reload the software into the unresponsive card.

If this fails five times in a one hour period then the unit will enter “safe mode” (boot loader), whereby it does not attempt to load any CODEC software and remains accessible with a “cut down” version of the operating system running for fifteen minutes to allow engineering access.

After this fifteen minute period the unit will begin another cycle, attempting again to boot up. If it succeeds it will operate normally, if it fails to load the CODEC software then it will return to “safe mode” after five attempts.

This can be seen to be occurring by watching the flashing LED on the front panel of the unit.

If the LED starts off flashing RED, but then turns to flashing GREEN for a short period of time before returning to flashing RED again this usually indicates a failure to successfully load the software into one or more CODEC cards.

The flashing GREEN indicates that the main application has started and is loading the CODEC cards. If they all load successfully then the LED will stop flashing and illuminate GREEN permanently.

A loop of flashing RED, then flashing GREEN, returning to flashing RED again usually indicates a CODEC issue.

Each CODEC card has a RED status LED situated to the left hand side of the card slot. If the lid is removed from the unit and the startup process observed you should see each of these card status LED’s start flashing as the boots up.

If any one of the LED’s is not flashing then the unit will reboot as described above.

It is highly unlikely that the CODEC card is actually faulty. The most common issue is dirt / contamination of the contacts on the card and card slot. The unit contains cooling fans that pull air over the CODEC cards and main board components. After many years of operation (depending on how clean the operating environment is) the card slots become contaminated with debris, and communication between the main board and cards becomes unreliable.

If the unit is suffering from CODEC issues then the first thing to try is removing the card with the issue and cleaning the card edge connectors with a solvent cleaner (Isopropyl Alcohol recommended, but other electronic cleaners / solvents can be used), then applying a little of the cleaner into the socket before blowing it clear with some compressed air. Following this insert and remove the card from its socket a number of times (approx 10) to remove any build up of contamination from the sprung fingers of the card sockets.

You may need to perform this operation several times to attain stability.

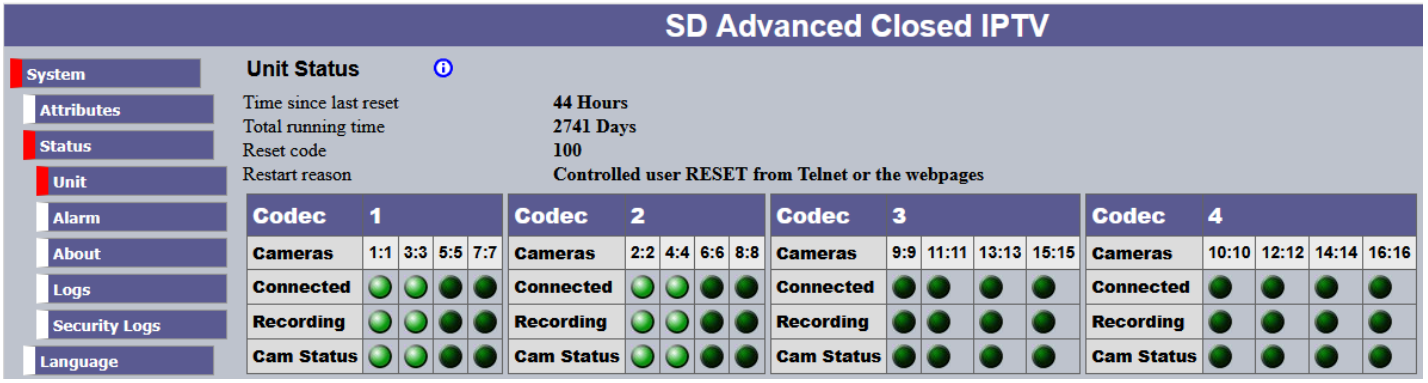
Also it is recommended that even if just a single card is showing an issue to clean and re-seat all of the CODEC cards, as if one is contaminated the rest will soon begin to show the same symptoms.

There is also one (or possibly two depending on the model number, the SDAHD, DVIPRT and NV8 have two as they have two HDMI video outputs) larger CODEC card nearest the rear of the unit. This is the Framestore (Graphics Card) that drives the monitor output. This card can occasionally cause issues with poor connections as well as the video CODECS. If you have an issue with posterized video output (looks like an early 80’s pop video with missing colours Etc) on the monitor output across ALL cameras then suspect the Framestore connected to the monitor in question, of having bad connections.

If the poor (posterized) video is only visible on some cameras then the issue will be with the video input CODEC associated with the channel/s in question rather than the Framestore.

You can see which CODEC cards have which cameras connected to them by using the System/Status/Unit webpage.

In the image below you can see that cameras 1 and 3 are connected to CODEC 1, 2 & 4 to CODEC 2.



There are only four cameras connected to the unit that was used to create the image above, however it can be seen that the unit contains four quad input CODECS, with the four cameras being split over CODECS one and two. Cameras that are not connected show in dark green, connected cameras show in light green, and failed cameras (there are none on this system) show as red. A failed camera is one that has been added on the camera setup web page but is not providing any video.

Therefore if you are experiencing poor / distorted video on cameras 1, 3, 5 and 7 then you should suspect an issue with CODEC one.

Again this can be used as a useful guide as to the fault location.

From this we can see that CODECS can fail in more than one way. A CODEC that is not being detected by the software application can cause the unit to never boot up correctly. However a CODEC that is being detected correctly by the system can also create poor / no video faults.

The CODEC cards are numbered from the rear of the unit, with CODEC 1 being the card nearest the rear and CODEC 16 being nearest the front.

The Framestore (video out / graphics) card/s are larger and sit nearer the rear of the unit behind the input cards. These are secured in place with small cable ties threaded through the card retaining latches and should not need removing under most circumstances.

However, if you do need to remove the Framestore card/s then it is acceptable not to replace the cable ties, they were fitted to prevent the cards from becoming disconnected from the slots during transit. Once the unit is installed these fixings are not required.

The system log files (see log file section below) can indicate CODEC related issues, usually 131, this will also identify which card is causing the issue. After the error code the CODEC which failed will be shown in brackets.

So to sum up, CODECS can fail in two ways. These are;

1. Failure to initialise which prevents the unit from booting up. This can be diagnosed by looking for the flashing status LED next to CODEC card slot. No LED indicates that the card is not running.
2. VIdeo issues. The card is identified and runs its software correctly, but causes no / bad video on the channels that it is digitizing the video from. The CODEC allocation can be determined from the System/Status/Unit webpage.

Hard Drive Issues;

Desktop units can contain up to four hard disk drives. Most units contain one or two. These are used to store recorded video and associated “metadata” consisting of Alarm information, VMD / motion data, Audio, and debugging information.

The drives are formatted as FAT32 allowing them to be removed and played back if required on any operating system, Windows, Linux, Macos Etc.

The information is recorded using the NetVu PAR file system; this has several advantages in allowing the metadata to be preserved as evidence alongside the video images. However it does mean that recordings need to be played back using NetVu viewing software, which can be an issue in some circumstances where “standard” video files are required for evidence.

NetVu provides a 100% FREE PAR file replay viewer (NetVu VCR) with no purchase necessary. This is installed with the free version of our Enterprise Observer software, and has no restriction in its use. It can be copied onto replay media (CD/ DVD / USB) with the PAR files and freely distributed.

For short video clips you can use the screen recorder facility built into Enterprise Observer to create an AVI, or MP4 file however this is done in “real time” so can be impractical for large video segments.

NetVu can provide software and instructions on how to convert a large number of PAR files to “standard” video, please contact tech support if this is required.

PLEASE NOTE, NetVu do not recommend converting video from PAR files to “standard” media video formats as doing so will remove all of the embedded metadata, preventing any alarm data, motion detection information Etc from being available.

Hard drives these days are generally very reliable and will provide recordings for many years, however they are mechanical devices and inevitably wear out. A complete hard drive failure can be identified easily. The unit will display “Warning Not Recording” on the main monitor output, along with the “RECORD” LED on the front panel extinguishing indicating that recording has ceased.

Partial drive failure can be more difficult to diagnose, you may see intermittent recording, corrupt video during playback, or even intermittent rebooting of the unit.

Intermittent rebooting due to drive failure is actually not a fault in itself, it is caused by the unit attempting to restart the failing drive. If cameras are selected to be recorded and the unit can not record to the selected drive for more than 15 minutes it will reboot in an attempt to “wake up” the failed drive. This can be quite a successful recovery method, and some drives will recover and allow continued recording for many days / weeks before the next reboot. However, as the drive deteriorates further the reboots become more and more frequent until intervention is required.

If you have a unit that reboots intermittently check the system log files (see log file section below) for error 121, or 125 errors. Both of these are drive related restarts.

The units have the ability to collect S.M.A.R.T health data from the hard drives. This can be very useful in determining the state of the drives. Unfortunately this is not available via the web interface. You need to access the unit's “command shell”. This is done either through the serial interface (but as discussed above we will avoid venturing too far with this) via COM1 at 115200,8,N,1 or via a TELNET session.

TELNET used to be a very common way of connecting over a network to obtain a remote command shell from one device to another, but due to security vulnerabilities has been depreciated by Microsoft after Windows 7, and requires enabling in the control panel (usually by a system administrator or IT department).

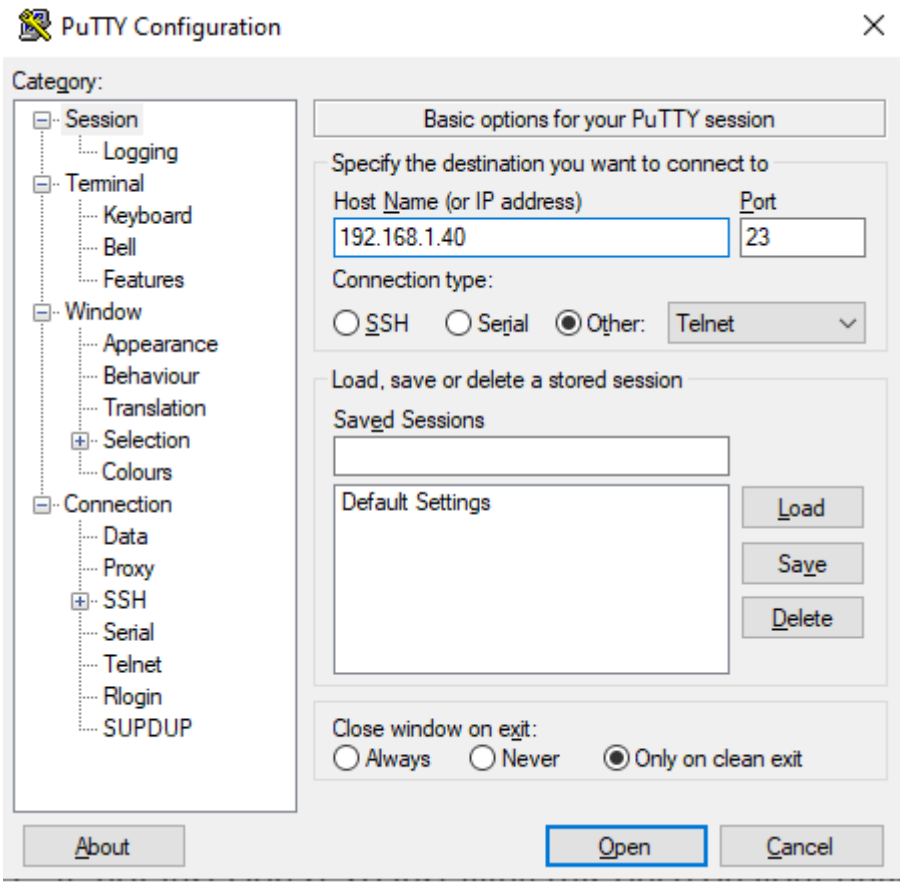
Therefore it is easier to use a third party TELNET client on your PC rather than attempting to enable Windows built in client.

NetVu recommends PUTTY as a combined Serial (RS232), SSH, and TELNET client, as this can be used to access all NetVu servers (Gen1 - 4, not just Gen3), so installing this once on your engineering PC should be regarded as essential. However you can use any serial, SSH or TELNET clients that you prefer. PUTTY is third party software and as such NetVu can provide no support for it.

PUTTY can be downloaded here;

https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html

Once installed run the PUTTY software and select the connection type as “other”, leave the dropdown box set to “Telnet”, leave the “Port” set to “23” and enter the IP address of your DVR / NVR into the “Host Name (or IP address)” box, in the example below 192.168.1.40



Then click “Open”. This will open a command shell on your NetVu / Dedicated Micros unit. If you have set up a TELNET user account on the unit you will be prompted for a username and password enter these now. If you do not know them please refer to the password removal FAQ’s NVT-003, and / or NVT025 detailing password removal.

If you have not set up any user accounts then a box will open displaying the units command shell, which will be the units model followed by >

For example SD Advanced Closed IPTV16>

At this point enter the command “drive smart” followed by the hard drive that you wish to check the health of. The primary drive in all units is usually set to DH0, so to check the smart health of the primary drive you would enter;

drive smart dh0

```
SD Advanced Closed IPTV16> drive smart dh0
SMART for drive DH0
SMART Data Structure Revision: 0x00 0x10
ID   Name                      Flags  Value  Vendor Specific                    Raw Value
==== ========================  ====== ===    --------------------------------
0x01 Raw_Read_Error_Rate       0x000b  95     95   1   0   9   0   0   0   0  (589825)
0x02 Throughput_Performance    0x0005 135    135  96   0   0   0   0   0   0  (96)
0x03 Spin_Up_Time              0x0007 115    115 200   0 199   0   4   0   0  (200 (Average 199))
0x04 Start_Stop_Count          0x0012 100    100  64   2   0   0   0   0   0  (576)
0x05 Reallocated_Sector_Ct     0x0033 100    100   0   0   0   0   0   0   0  (0)
0x07 Seek_Error_Rate           0x000b 100    100   0   0   0   0   0   0   0  (0)
0x08 Seek_Time_Performance     0x0005 138    138  31   0   0   0   0   0   0  (31)
0x09 Power_On_Hours            0x0012  88     88 139  75   1   0   0   0   0  (84875)
0x0a Spin_Retry_Count          0x0013 100    100   0   0   0   0   0   0   0  (0)
0x0c Power_Cycle_Count         0x0032 100    100  64   2   0   0   0   0   0  (576)
0xc0 Power-Off_Retract_Count   0x0032 100    100  72   2   0   0   0   0   0  (584)
0xc1 Load_Cycle_Count          0x0012 100    100  72   2   0   0   0   0   0  (584)
0xc2 Temperature_Celsius       0x0002 200    200  30   0   0   0  49   0   0  (30 (Min/Max 0/49))
0xc4 Reallocated_Event_Count   0x0032 100    100   0   0   0   0   0   0   0  (0)
0xc5 Current_Pending_Sector    0x0022 100    100   0   0   0   0   0   0   0  (0)
0xc6 Offline_Uncorrectable     0x0008 100    100   0   0   0   0   0   0   0  (0)
0xc7 UDMA_CRC_Error_Count      0x000a 200    200   0   0   0   0   0   0   0  (0)


Offline collection status:       (0x84) : Offline data collection suspended by host command
Self-test execution status:      0x00
Offline collection duration:     4831 seconds
Offline collection capability:   0x5b
SMART Capability:                0x0003
Short self test polling time:    1 minutes
Extended self test polling time: 81 minutes


SMART Health 100%

SD Advanced Closed IPTV16>
```

This will display the S.M.A.R.T. health data for the drive. A new drive starts off with all of the “Raw data” as “0”, these figures will increase as the drive ages. The important indicators of poor drive health are numbers greater than zero in “Reallocated_Sector_Ct”, “Seek_Error_Rate”, “Spin_Retry_Count”, “Reallocated_Event_Count”, “Current_Pending_Sector”, Offline_Uncorrectable” and “UDMA_CRC_Error_Count”.

Anything greater than “0” in any of these fields should be treated as a symptom of poor drive health. It will also cause the “SMART Health” percentage to report as less than 100%.

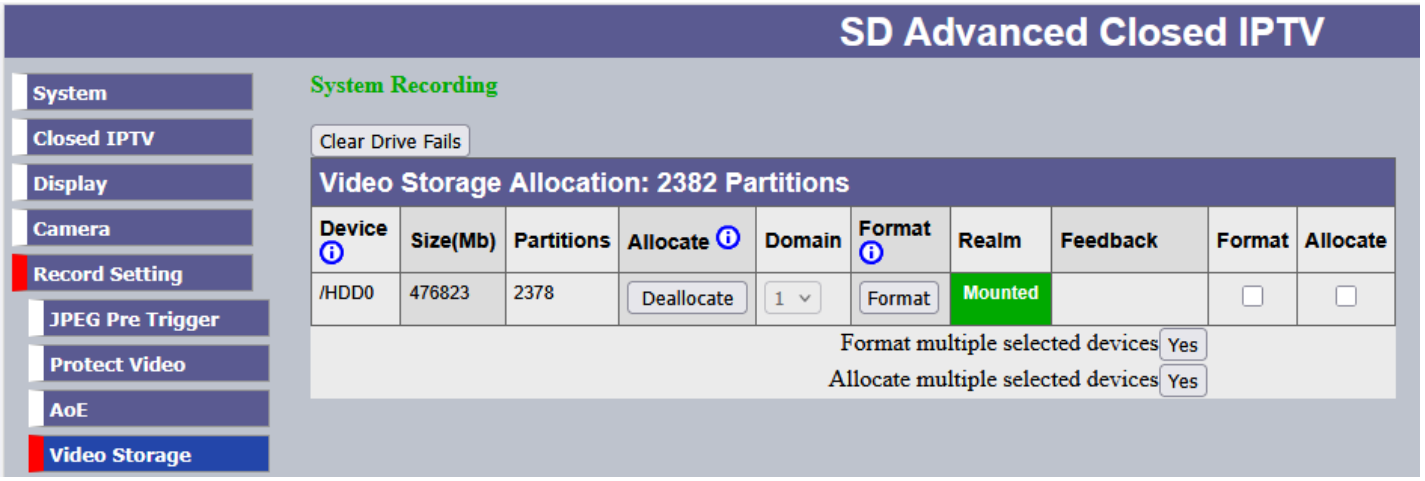
Any hard drive reporting less than 100% should ideally be replaced, anything reporting less than 80% health MUST be replaced.

All drives connected to a system should be checked regularly.

The secondary drive mapping varies somewhat from system to system. The second drive (if fitted) on a SD Advanced, and SDACP is dh5, so the command to check it is “drive smart dh5”.

The second drive (if fitted) on an NVR Media server, and an SDANVR is di0, so the command to check it is “drive smart di0”.

You can see which drives are available to the unit on the “Record Settings / Video Storage” web page. This page lists all available drives and their “mount points”.



This page also allows you to format and allocate / deallocate the drive/s from the unit. Normally all available drives should be formatted and allocated.

If you fit a replacement drive to your system you should go to this page and click “Format” (then wait for the process to complete (it takes approx 45 seconds depending on drive capacity)), then click on the “Allocate” button to begin the process of creating the video files on the unit.

When you format a drive greater than 2Tb the unit will split it into 2Tb virtual drives, this is due to the fact that 2Tb is the limit for the FAT32 file system, so for example if you fit a 6Tb hard drive after formatting you will see “hdd0”, “hdd0a” and “hdd0b” as drives ready for allocation. Once allocated the unit will use all of the drive capacity as a single large array.

It is best to do this manually for each drive partition as the tick boxes to format and allocate multiple drives have been seen not to work correctly in some web browsers.

Allocating a drive can take a relatively long period of time, as it pre creates all of the video partitions on the drive. The pre-creation of the files makes the file system extremely resilient to corruption in the event of power failures Etc. If you have other maintenance work to do on the site it is advisable that you fit the replacement drives first, that way you can leave the unit creating the video whilst other tasks are performed.

As an example it takes approximately an hour for a 6Tb drive to allocate.

Please ensure that all available drives are allocated for maximum record time.

Please note that if you fit a replacement micro SD card to a unit then by default only the first partition of hdd0 will be allocated and available for recording, so for example if a 6Tb drive were fitted and the micro SD card subsequently replaced then you will only see 2Tb available for recording. If fitting a replacement card, or

formatting an existing card you must always go to the “Video Storage” web page and re-allocate the remaining partitions.

It is possible to manually re-map drives from the command line. This is sometimes done remotely by tech support operators to stop the unit “looking for” failed hard drives and rebooting. Allowing the unit to operate with a reduced recording capacity until the failed drive can be replaced. Once the failed drive has been replaced the drive mapping should be returned to the factory default to prevent “none standard” units being present in the field.

The correct drive mapping for all Gen3 units is;

APPDRIVE: mdd0 (mdd0)
FTPDRIVE: mdd0 (mdd0)
NVRDRIVE: nvd0 (nvd0)
WEBDRIVE: mdd0 (mdd0)
DATADRIVE: hdd0 (hdd0)
TEMPDRIVE: rdd0 (rdd0)
PCAPPDRIVE: mdd0 (mdd0)
LOGDRIVE: hdd0 (hdd0)
DBASEDRIVE: hdd0 (hdd0)

The mapping can be changed from the command line using the commands shown before the mapping, so for example if the primary hard drive “hdd0” had failed the unit can be changed to use it;s secondary drive “hdd5” for the Data, Logs, and Alarm Database by issuing the following commands;

EscM\DATADRIVE\hdd5
EscM\LOGDRIVE\hdd5
EscM\DBASEDRIVE\hdd5
reset *** To restart the unit so that changes take effect ***

Note that all NetVu units commands to make changes to the system must start with EscM\ this is the “Escape” (Esc) key in the top left hand corner of your keyboard followed by the “m” key then the “\” key (bottom left hand side of your keyboard).

After the unit has rebooted it will start writing video, logs, and database entries to the secondary drive (hdd5). This will prevent a unit with a failed primary drive from resetting.

The same thing can be done if the micro SD card fails. The unit can be told to use the hard drive to store its application and web pages using the commands;

EscM\APPDRIVE\hdd0
EscM\WEBDRIVE\hdd0
reset *** To restart the unit so that changes take effect ***

However you will have to install a copy of the application and web pages onto the hard drive as by default it does not contain them.

Once the failed drive/s have been replaced then all of the drive mapping should be returned to their default settings.

To check the drive mappings plus the rest of the non-volatile settings (settings not contained on the micro SD card that will be retained in the event of a card / drive failure) you can use the following command from the unit's command line via TELNET or serial.

EscM\STATUS

This will return the following information;

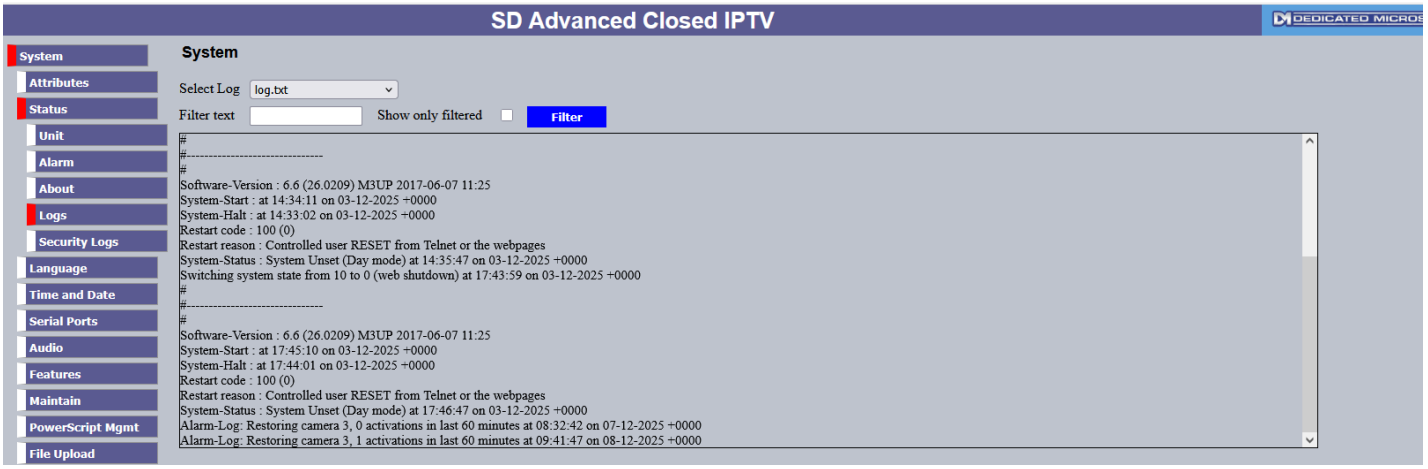
```
SD Advanced Closed IPTV status: current data (user modified)
PPP Configuration :
   BASE_IP: 10.0.0.1 (10.0.0.1)
Eth0 Configuration :
   MAC ID: 00 D0 D9 07 AD 22  ( 00 D0 D9 07 AD 22 )
   GATEWAY: 0.0.0.0 (0.0.0.0)
   SUBNET: 255.255.255.0 (255.255.255.0)
   ETHER_IP: 192.168.240.1 (192.168.240.1)
   Autonegotiation
SYSTEM: 1-ND2506001N006 (1-ND2506001N006)
APPLICATION: M3UP.ELF (M3UP.ELF)
APPDRIVE: mdd0 (mdd0)
FTPDRIVE: mdd0 (mdd0)
NVRDRIVE: nvd0 (nvd0)
WEBDRIVE: mdd0 (mdd0)
DATADRIVE: hdd0 (hdd0)
TEMPDRIVE: rdd0 (rdd0)
PCAPPDRIVE: mdd0 (mdd0)
LOGDRIVE: hdd0 (hdd0)
DBASEDRIVE: hdd0 (hdd0)
ACCOUNT: XXX000 (XXX000)
VIDSTD: 0 (0)
COM1: Debug (Debug)
COM2: Text In Image (Text In Image)
COM3: Telemetry (Telemetry)
COM4: Telemetry (Telemetry)
SECURITY: Eng Telnet access: PASSWORD (PASSWORD)
SECURITY: Debug port access: PASSWORD (PASSWORD)
USERNAME: SDAV (SDAV)
ARC_HOST:  ()
ARC_ID: HQ-Training-SDA (HQ-Training-SDA)
ARC_PROFILE:  ()
```

The EscM\STATUS command is very useful, allowing all of the system configuration settings to be viewed from one place.

System Log Files:

When a NetVu unit reboots for any reason it creates a “Logfile” containing the reason for the reboot and any debugging information associated with the issue to aid the software development team in resolving the issue and improving the software.
When you speak to tech support they may ask you to provide the logs to help with your issues.
To download the log files goto the “System / Status / Logs” web page, and initially select “log.txt” from the

drop down menu of available files. This will display something similar to the image below;



The text can be filtered if required to isolate a particular key word, or can be copied and pasted into an Email for support.
It can be seen in the log file above that the unit was deliberately restarted on two occasions (Restart Code 100), plus the time and date of the restart and the software version the unit was running.
A restart code (100) is a fairly common code caused when someone clicks on a”Reset” button in the web pages, or types “reset” from the command console.

However the log extract below is from a unit with a failed internal temperature sensor, showing debug information allowing the fault to be isolated;

Software-Version : 6.0 (32.0006) NBMB 2025-07-25 19:49
System-Start : at 13:46:03 on 19-11-2025 +0000
System-Halt : at 13:45:25 on 19-11-2025 +0000
Restart code : 127 (3)
Restart reason : Automatic maintenance restart
System-Status : System Startup at 13:46:00 on 19-11-2025
System-Error : Variable 7, value 0x1003A458
System-Error : Variable 8, value 0x1003A458
System-Error : Variable 9, value 0x1003A454
System-Error : Variable 10, value 0x1003A454
System-Error : Variable 11, value 0x60000013
System-Status : System Unset (UNSET mode) at 13:46:25 on 19-11-2025 +0000

Log files are a powerful tool allowing tech support to provide information on software and hardware issues. There are several other log files that may also be useful. These are;

bak.txt (this is the earlier log.txt file, log.txt is limited to 2Kb in size, when it exceeds 2Kb the bak.txt file is created)

startup.txt (this is a copy of the debug output from the last startup of the unit, and may be requested by the tech support operator)

seclog.txt (Logs inbound and outbound network connections to the unit, can be useful in determining if the unit has been the victim of a DDOS attack, or ensuring that the unit is secure)

There may be an occasion when the unit's web pages are inaccessible due to the fact that it is either in “safe mode” or that the micro SD card containing the application software has failed.

It is still possible to view / download the log files from the command line in this situation.

This is achieved via the following commands;

cd /hdd0/logs
list log.txt

This will print the contents of the file “log.txt” to the command console (TELNET or serial) it can then be copied from there into an Email and provided to tech support.

The above assumes that the log files are stored on hdd0 which is the default drive, if the unit is configured with the LOGDRIVE set to a drive other than hdd0 then use the correct drive name in the command above (see previous section on drive mapping).

Command Console;

NetVu Gen3 units have a comprehensive command console, most of the file system commands are the same as those used for MSDOS, valid file system commands are CD, MKDIR, RMDIR, DIR, RENAME, LIST, COPY, DEL, DELTREE

So for example to display and modify the files in the logs directory you can use the following commands;

CD /HDD0/LOGS	*** Change directory to the LOGS directory on drive HDD0 ***
DIR	*** Show a directory listing of all files in the LOGS directory ***
LIST LOG.TXT	*** Display the file LOG.TXT in the console window ***
RENAME LOG.TXT MYLOG.TXT	*** Rename the file LOG.TXT to MYLOG.TXT ***
MKDIR OLDLOGS	*** Make a directory in LOGS called OLDLOGS ***
COPY LOG.TXT OLDLOGS/LOG.TXT	*** Copy the file LOG.TXT from LOGS to OLDLOGS ***
DEL LOG.TXT	*** Delete the file LOG.TXT from the current directory ***
DELTREE OLDLOGS	*** Delete the contents of the OLDLOGS directory and remove the directory **
RMDIR OLDLOGS	*** Remove the OLDLOGS directory. The directory must be empty for this *** *** Command to work ***

The complete list of commands available can be found by entering “help” at the command console. Most of these commands should only be used by NetVu tech support personnel, or run only when asked to do so by a support engineer. Improper use of commands can leave the unit in a non-functional state and require it to be returned to NetVu Limited for repair / re-configuration.

There are some commands that may prove useful for service personnel, aside from the ones already listed in the drive mapping section above, in no particular order these are;

CD MDD0/ETC
RENAME USER.DB USER.OLD
RESET

This command renames the USER.DB file which contains the usernames and passwords on the unit to USER.OLD which has the effect of temporarily removing all of the user accounts. This can be very useful if you need to make changes to a system but do not know the usernames / passwords.
However if the unit has been configured correctly then TELNET access will be protected by an account as well as the web pages, so to enter the command console you would have to use serial access via COM1 (115200 Baud, 8,N,1). The unit will prompt for serial login before the main application is started. This is obtained by pressing "+++" three times, to stop the unit from booting and allow access to the command console.

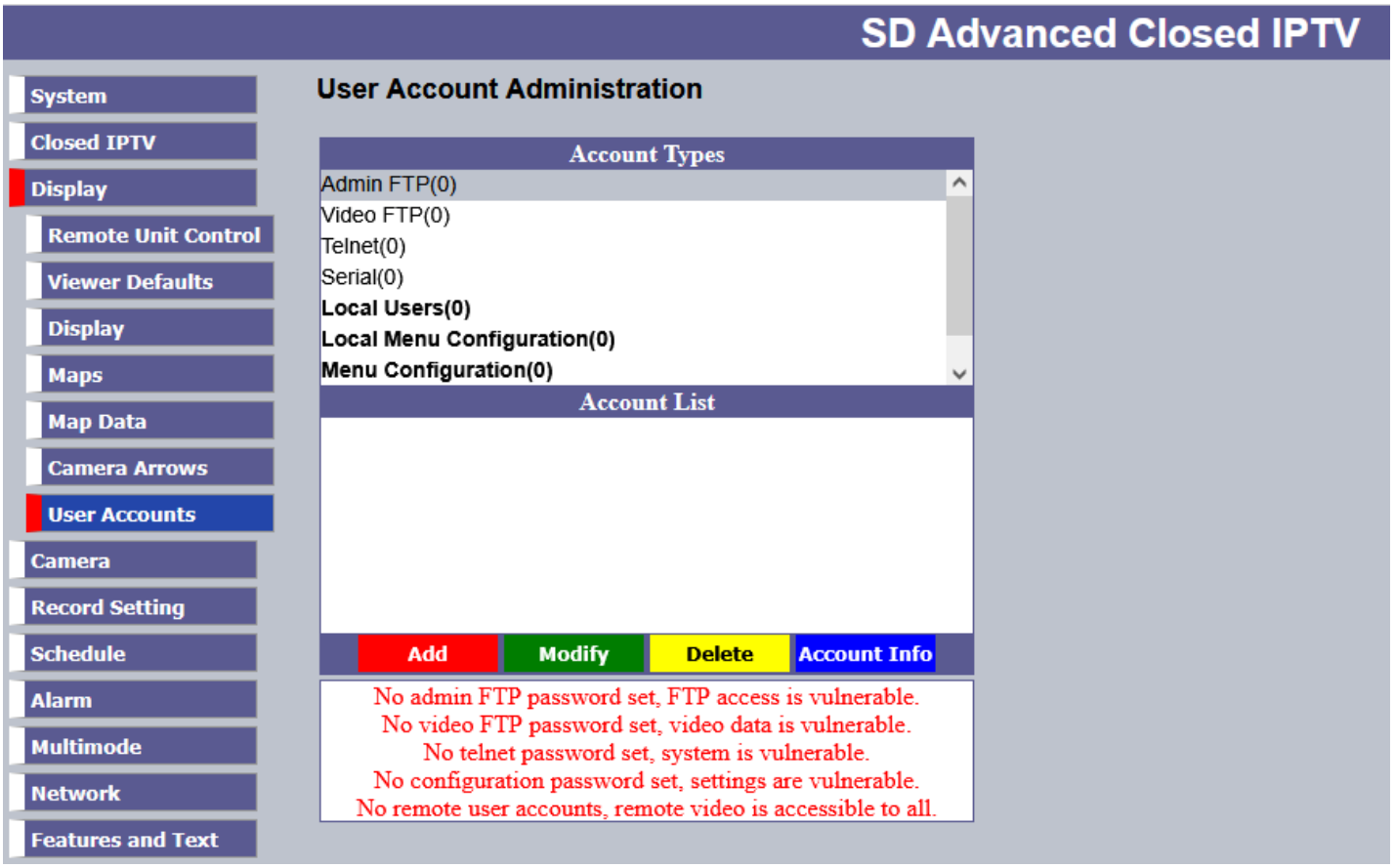
However it is worth trying a TELNET connection first as a lot of systems do not have TELNET user accounts setup.

Once you have renamed the USER.DB file and reset the unit it will startup with no user accounts.
You can then make the required changes and reinstate the accounts as follows;

CD MDD0/ETC
RENAME USER.OLD USER.DB
RESET

The unit will then restart with the original user accounts restored.

If you do not want to restore the old accounts you can simply set up new accounts from the User Accounts web page. There is no way to discover the passwords from the USER.DB file, they are encrypted. You can only delete or rename the file.



CD MDD0/FRM_DATA
RENAME MASTER.SFM MASTER.OLD
DEL SAFEVARS.SFM
RESET

This set of commands restores the unit to the factory default shipping condition except for the non-volatile settings (Network details, System Name, ARC details). The file MASTER.SFM and the associated backup file SAFEVARS.SFM contain all of the settings made via the web pages.

Renaming the MASTER.SFM file and deleting the backup makes the unit start up in the factory condition. This is especially handy if you suspect that something you changed in the web pages has created a fault on the unit. It allows you to quickly revert to a known good state for testing.

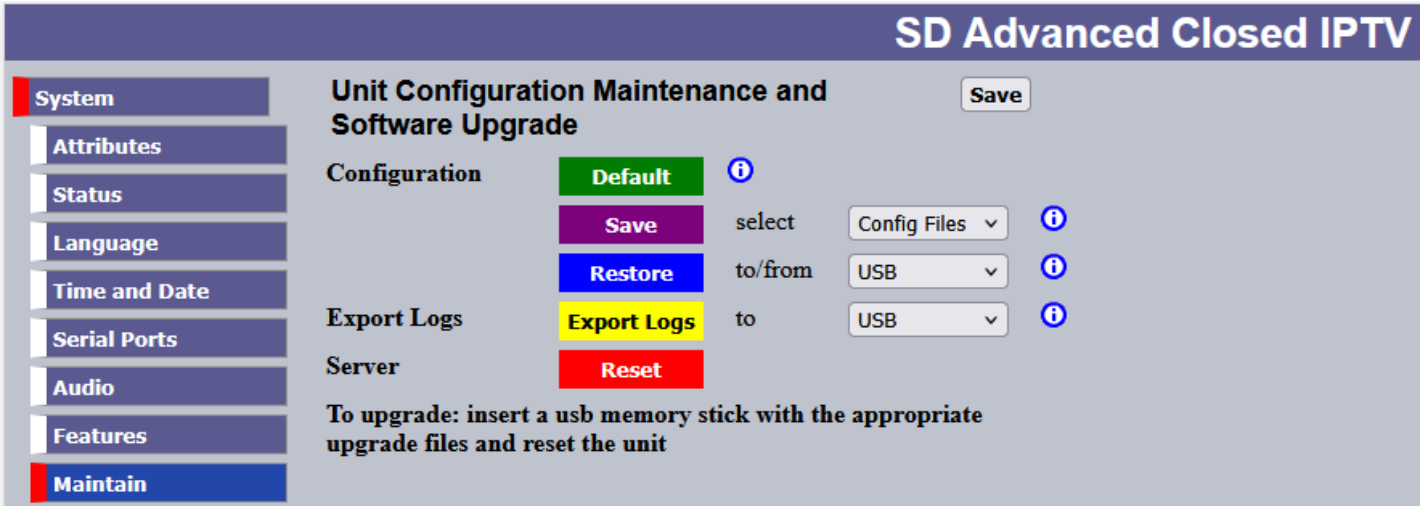
You can revert to the customers original configuration using the reverse of the commands above;

CD MDD0/FRM_DATA
DEL MASTER.SFM
DEL SAFEVARS.SFM
RENAME MASTER.OLD MASTER.SFM
RESET

This will delete the new MASTER.SFM and SAFEVARS.SFM files created by the system and rename the backup file created above MASTER.OLD as MASTER.SFM

If you do not want to return to the original settings simply set up the unit as you wish using the web interface. The unit will automatically create new MASTER.SFM and SAFEVARS.SFM files.

You can also backup and restore (clone) systems from the “System / Maintain” web page. This copies the MASTER.SFM files to a USB stick or CD/DVD so that it can be restored in the event of a unit failure.
It is always good practice to keep a recent backup copy of the unit's configuration somewhere accessible near the unit in case there is a need to restore the configuration, or fit a replacement unit. NetVu suggests that a USB stick is stored in the comms rack with the unit or fixed to the rear of the unit with a cable tie or similar if it is installed in a desktop environment. This will allow quick and easy recovery of a unit in the event of failure. It is also very useful if a unit should require a replacement system micro SD card as the configuration settings are stored on the micro SD card, so if it fails and there is no backup available all of the configuration will have to be entered again from scratch.



Finally, if you have an NVR Media Server, or SDANVR that is having problems detecting cameras correctly this can be caused by the camera SQL database becoming corrupted. Renaming this from the command line and allowing the unit to detect the cameras again resolves the vast majority of camera issues on any of our CloseIPTV systems. The commands to clear the database and restart detection is as follows;

CD /MDD0/SQL
RENAME CLOSEDIPTV.SQL CLOSEDIPTV.OLD
RESET

The unit should then start up and rescan the camera network creating a new database. This will add any NetVu Connected cameras discovered by the system. Any cameras added via third party switches or on the corporate network will have to be added manually.

Please note that the CLOSEDIPTV.SQL file can not be deleted, it is read only, but can be renamed. Once it has been renamed and the unit rebooted you can delete the renamed file if required.

There are some “hidden” files on both the micro SD card and the HDD that can also affect closedIPTV detection, so the above process may not resolve every scenario, however it is the first thing to try before proceeding to a full system format and restore, or micro SD and HDD replacement.

Web Page Tricks;

The browser can be made to display live debug information and system variables which may be useful in locating a fault, these are accessed by adding a “port number” to the end of the IP address of the unit.

Port 5201 provides debug, and port 5202 provides system variables, so if I want to view the debug from a unit you can enter the following into your web browser;

http://aaa.bbb.ccc.ddd:5201

Where aaa.bbb.ccc.ddd is the IP address of the unit that you wish to view the debug output from.

http://aaa.bbb.ccc.ddd:5202

Where aaa.bbb.ccc.ddd is the IP address of the unit whose system variables you wish to view.

The monitor output from a unit can be viewed directly in a web browser, this is useful if you do not have a local monitor connected and you wish to see what is being displayed on the monitor, this can be viewed using the command;

http://aaa.bbb.ccc.ddd/cgi-bin/monitor.cgi?monitor=1&fields=1

Will display the local monitor output from the unit with IP address aaa.bbb.ccc.ddd in a web browser. This is a still image so you will have to keep refreshing if you are looking for something that is not permanently displayed.

You can use the web browser to download and backup the MASTER.SFM system settings file directly to your PC if you do not have a USB stick available. Enter the following into your browser;

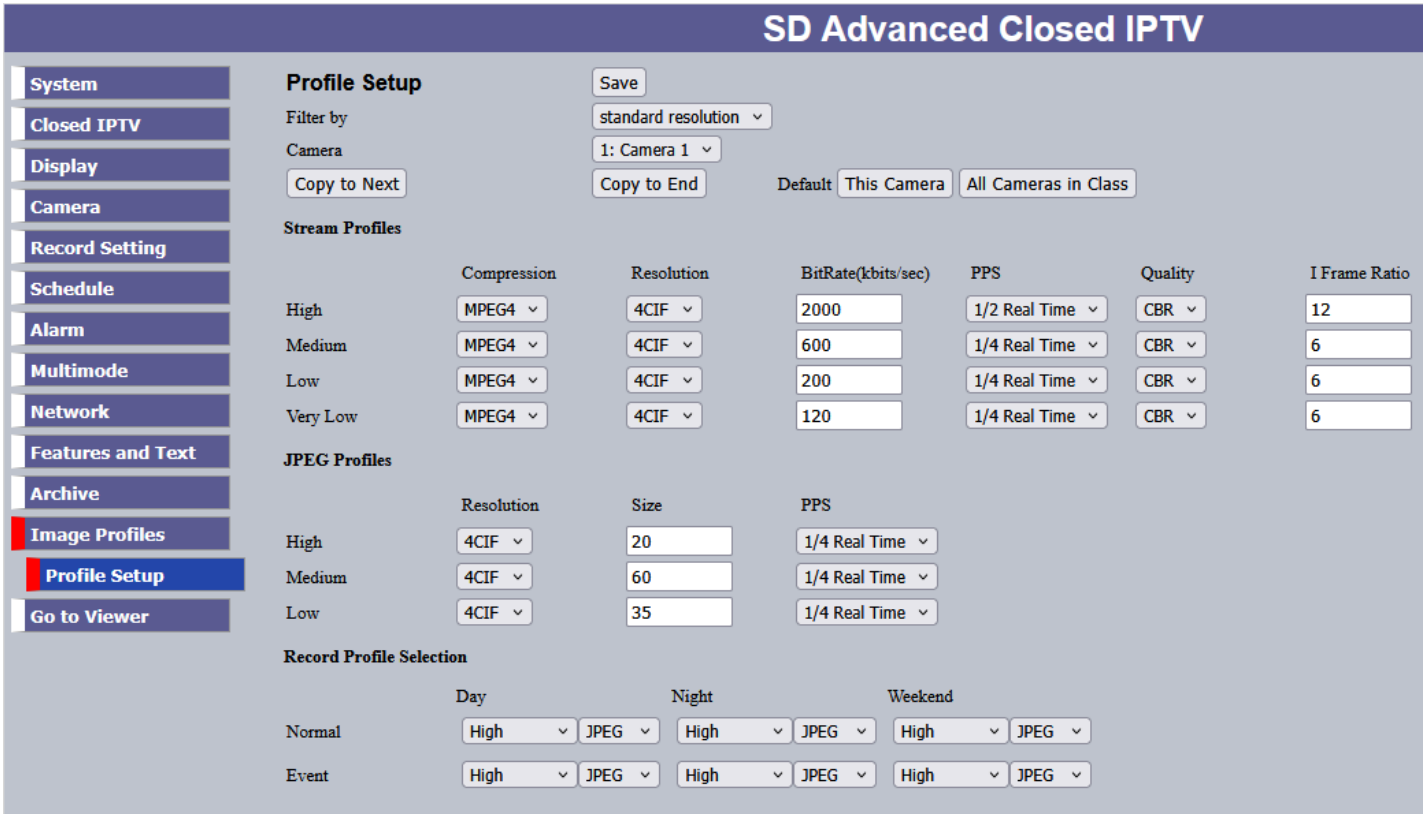
http://aaa.bbb.ccc.ddd/frm_data/master.sfm

This will download the file, then click “save page as” in your browser and save it as MASTER.SFM

Configuring a closedIPTV camera connected to an NVR Media Server or SDANVR from the NVR;

Once a system is deployed the normal practice is to only allow the IP address of the NVR through the external router, so it may not be obvious at first how you configure the connected cameras.

The answer is twofold. All everyday configuration, image resolution, compression rates Etc are controlled from the NVR, you do not need to access the camera directly. You use the “Image Profiles” web page.



From here you can set the image quality, stream type, and resolution for each camera, or copy the same profile to all of the connected cameras.

However there may be situations when you wish to access the camera configuration directly, such as wanting to flip and mirror an image depending on camera mounting position, adjust the illumination settings, white balance, or other camera specific settings.

To do this you use the Closed IP Proxy setting from the “System / Features / Network” web page.

Navigate to the web page and you will see a box to input the “Closed IP Proxy Target Camera”, and a second box containing the “Closed IP Proxy Port”.

To access a camera's web page remotely enter the address of the camera you wish to access into the “Closed IP Proxy Target Camera” box and click “Save” (top right hand corner).

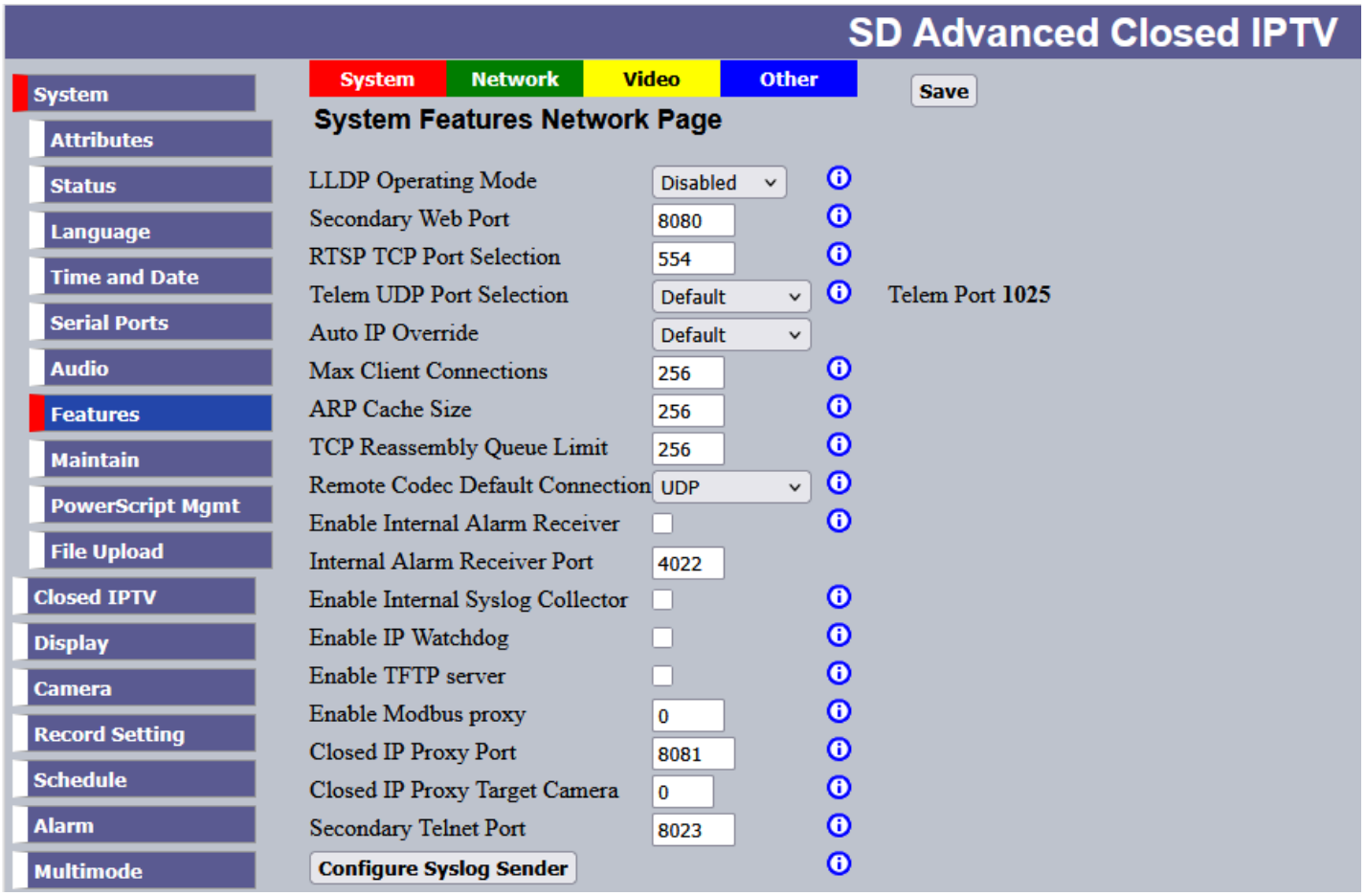
Leave the “Closed IP Proxy Port” set to 8081 unless instructed by NetVu tech support.

Then to view the camera's configuration page enter the IP address of the NVR into your web browser followed by a “:” and 8081 (the Closed IP Proxy Port Number). This will then open the camera's configuration page via a proxy port so that you can configure the camera directly. To setup camera 2 for example you would enter 2 into the “Closed IP Proxy Target Camera” box, click save, and enter the following into your browser;

http://aaa.bbb.ccc.dd:8081

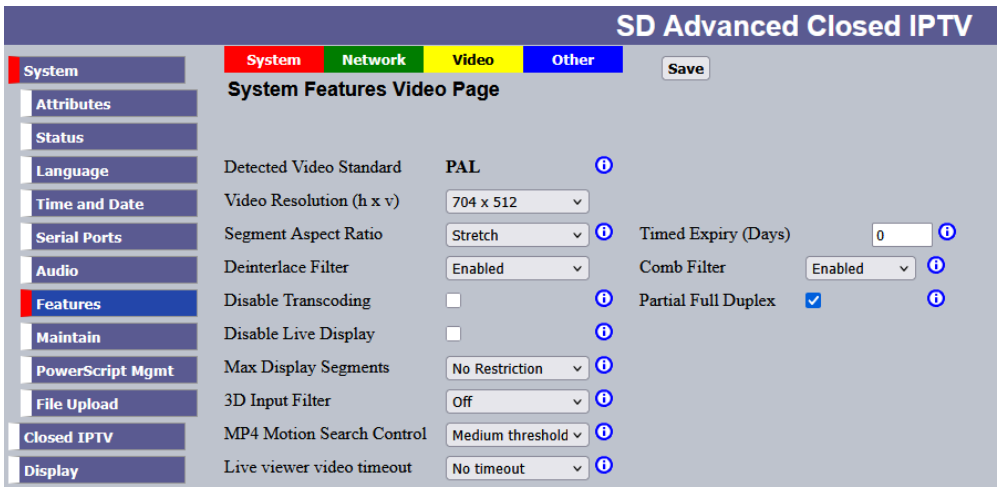
Where aaa.bbb.ccc.ddd is the IP address of your NVR. This will open the camera's configuration web page.

That way you only need to expose the address of the NVR plus port 8081 to provide access to all cameras.

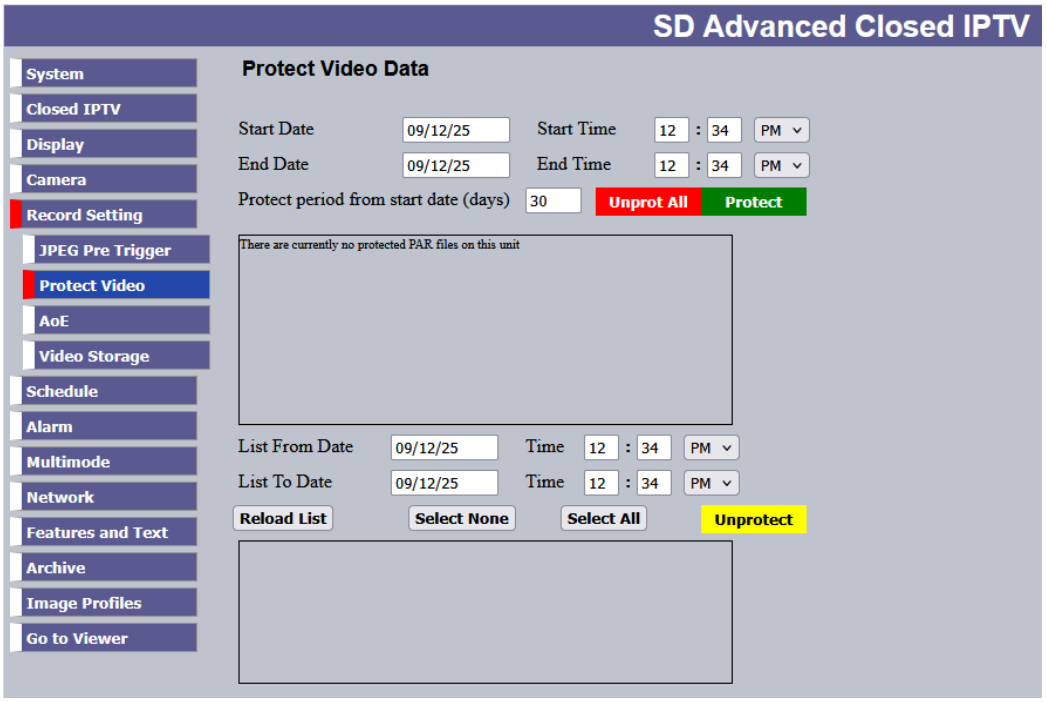


Another feature that is commonly requested, especially by European installers is the ability to retain images for a set amount of time, in both France and Italy recordings can only be retained for 24 hours unless there is notification of an incident.

The setting is referred to as “timed expiry” and it is set on the “System / Features / Video” web page. This is accessed by navigating to System / Features, then clicking on the YELLOW Video button. On this page you can set the “Timed Expiry” in days, so to comply with French and Italian law this should be set to 1 day.



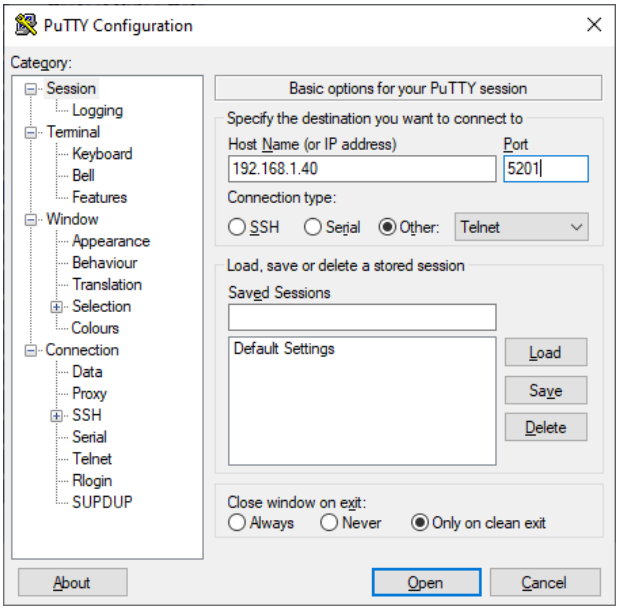
If you have set “Timed Expiry” and there is an incident then you must either download the footage before the expiry ends or protect the recording. You can protect the recorded video using the “Record Settings / Protect Video” web page. Protected video will not expire until the protection period has elapsed, providing time to download any evidential footage required.



Interpreting Debug;

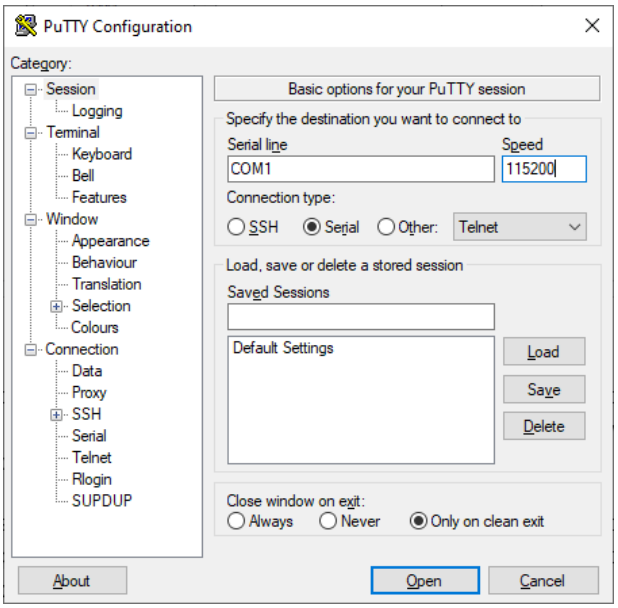
All NetVu units output a stream of debug information to enable the software team to diagnose the cause of performance issues, and unexpected behaviour.

This debug can be accessed in three ways, these being via serial (RS232) from com port one (115200 Baud, 8,N,1) via TELNET on port 5201 or via the web pages also on port 5201. To access the serial debug simply enter the IP address of your unit into Putty, select “Other” , leave the drop down box set to TELNET, but change the port from 23 to 5201. This will open a window displaying the unit's debug output.

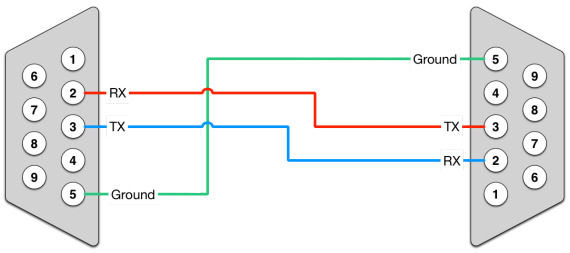


Or as mentioned in the web page section above enter http://aa.bbb.ccc.ddd:5201 into your web browser. The web based debug can be awkward to use as you need to keep refreshing the browser to load the latest debug output, so serial or telnet debug may be preferred.

Putty can also be used to access serial debug, simply select the connection type as “Serial”, set the Baud rate (Speed) to 115200 and select the PC COM port you are using (you can see what COM port number has been assigned to a USB to serial converter by opening device manager on you PC and looking at the “Ports (COM & LPT)” section when you plug in your converter;



You will need a “null modem” lead from your PC serial port to COM 1 on the NetVu / Dedicated micros unit.



These can be brought from many sources, one was originally supplied with each of the units, or assembled prior to visiting the site using the diagram above. All that is required are two female nine pin D-Type sockets and a length of three core cable.

Serial debug is by far the most useful for advanced, in depth, fault location as the debug is produced immediately after power is applied, whereas debug from the unit via the network is only available after the unit has booted far enough to initialise the network controller. Sometimes this never happens, so no debug information is available. Other times the unit will start in “safe mode” (engineering boot loader), which will initialise the network, but not provide any useful debug as the unit will not be running the main software application, so the root cause of the issue will be difficult to identify.

With serial debug the unit will output information right up to the point of failure, whether it be before or after the network is initialised, so any fault early in the startup process can only be seen using serial debug.

Even if the site engineer does not intend to utilise serial debugging in person it can still be an invaluable tool for remote support, as our technical support engineers can use it remotely via team viewer, any desk or other remote desktop software to enable a much higher level of support than otherwise available. To that

end NetVu strongly suggests that anyone attending site to work on any of our platforms be equipped with a PC with a serial port, or USB to Serial converter, plus a “null modem” lead.

Once you are able to view the unit debug from power up you should be able to determine the root cause of many failures. On most occasions the last piece of information output via debug is the reason that the unit has failed (or more likely rebooted), so for example if a CODEC card CW3 is failing to start up you will see a line of debug starting CW3: followed by an error message defining the cause. After this you would see the unit reboot, whereupon it will try to boot again until it reaches the same point of failure. CODEC cards are initialised before the network controller so you will never see the relevant debug information via TELNET or the web interface. The CODEC cards are also not started up during “safe mode”, so you would not see the card failure information being output when viewing debug in safe mode.

The same goes for many other issues which can be reasonably simple to resolve if complete access to the debug stream is possible.

It is possible to interrupt the serial debug stream in order to enter commands. To enter the command interface type “+++” into the serial terminal window.

When you have completed your command entry you can resume debug monitoring by pressing CTRL+D

NetVu supplies a free debug monitoring tool called the “Debug Parser”, downloadable from the software section of our web site. Contained in the “Engineering and Support Toolkit” download. This allows you to filter the debug data stream enabling you to isolate specific key words and display any debug containing the word in a separate window. For example you could filter debug from each of the CODEC cards by applying a filter for CW0: CW1: CW2: CW3: and CW8: so that you could check that all of the cards are operating correctly. Or filter by the word MAIN which is output once per minute and contains performance related information on how many images have been recorded in the last minute, any cameras showing as failed, the CPU load on the main and CODEC processors, and the amount of memory in use.

All of this information is present in the main debug data stream, but the ability to filter and search for specific text makes fault location easier.

If serial debug is not available the “Debug Parser” can work nearly as effectively with network debug data via TELNET, however as mentioned above the network debug is dependent on the network interface starting up, so any debug from early in the boot process will not be visible.

Useful (case sensitive) filter keywords to use when examining debug from a unit are;

MAIN - Displays the unit status once per minute

CWx - Displays the status of the plugin CODEC cards where x is the card number from 0 through 9

VID_REC1 - is the record thread displays useful info on record rates Etc

ERROR - Most processes that have a problem will output the word ERROR in the debug

RTC - Any issues with the real time clock will generally contain the word RTC

Fsimage - Is the record process thread, hard drive issues usually show up here

DATABASE - Any database actions will create a debug entry containing this keyword, alarms, set / unset, VMD events, text keywords captured from point of sale equipment, Etc.

ALARM - Any state change of an alarm input will generate an alarm event in the debug, even if the alarm has not been set up in the web pages. This can be a good way of testing the alarm port hardware if you are not receiving alarms and suspect that the issue is hardware rather than configuration related. No matter how the unit is configured you will still see alarm transitions in the debug if the state changes, either from open to closed, or closed to open. These transitions can also be seen on the “System / Status / Alarm” web page.

Software Updating;

There are several ways to perform software updates on our Gen3 units, these vary in complexity depending on the existing state of the unit's software. If a unit is already running a software application upgrading using either our Enterprise Observer viewing software or the web interface is the preferred method. However if the unit needs to be given a complete new install of software then you will either need to use a micro SD card reader, or third party FTP software (NetVu Recommends Filezilla).

The reason for this being that if no application software is running on the unit then the web interface and Enterprise Observer connections will be unavailable.

Either upgrade method starts with obtaining the correct software to install on your unit. All Gen3 (and indeed Gen1, Gen2 & Gen4) software can be found on the NetVu web site at,
https://netvu.org.uk/new-software-release-area/

Scroll down to the bottom of the page and you will see a section called “LEGACY PRODUCT SOFTWARE”. Below this is a drop box where you can select the software for your unit. We will use an SD Advance ClosedIP in the example below, but substitute the model for that which you require.

From the drop down box select “SD Advanced Closed IPTV (M3U)” This is the product description and main board type / Platform (M3U)

Note. Some units may have more than one Platform, ensure you select the correct one for your hardware, the sticker on the underside of the unit will identify the “Platform”, alternately if the sticker has been removed or is unreadable there will be a sticker on the main board itself identifying the board. Installing the wrong software on a blank micro SD card will not harm the unit, but it will not function until the correct software is installed. Upgrading to the wrong software via the web interface or Enterprise Observer will simply not upgrade. The unit will continue to run whatever software version it was previously running.. The only thing that will happen is that space on the internal micro SD card will be taken up holding the wrong files, which may impact the unit's ability to accept the correct files depending on what capacity card is fitted. (you may need to manually delete the wrong files to free up space, this will be explained at the end of the section).

When you select the product a new section will open showing all available software downloads. This has three background colours, Grey, for old software versions, Green for the latest stable release, and Pink for Beta releases. Under normal circumstances unless instructed otherwise by technical support, select the software with the Green background and click “Show Files”.

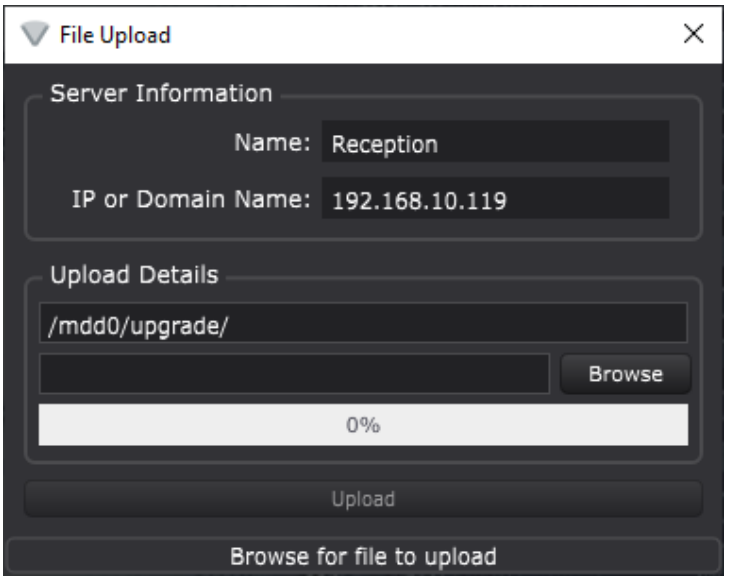
This will take you to the download page for the software release. Click on the “download” button for each file you require (you only need to download the web pages for your region (NTSC for the USA, Canada and Japan. PAL for the UK, Europe, and the rest of the world)). Some of the files are only required to reprogram specific boards / chips, and are not needed for a simple software upgrade, although downloading them all will not cause any issue.

For a simple upgrade you require the Main Application, CODEC Application, Framestore Application, Web Page Core, and Unit specific regional web pages. The remaining files are optional but should be downloaded for completeness.

Note. The Main Application, CODEC, Framestore, and Web Pages should always be installed together. Do not just attempt to upgrade one file in isolation as the software is released as a package. For example if you just upgrade the web pages, and not the application, you may find new features displayed that do not work, as they require a corresponding update to the application. This can at best be frustrating, and at worst actually prevent the unit from booting up correctly, if for example you try to enable a feature that is unsupported by an old application the unit may crash because it can not "find" the required code.

Once you have downloaded the ZIP files you then need to copy them to the unit. They need to be copied to /mdd0/upgrade/

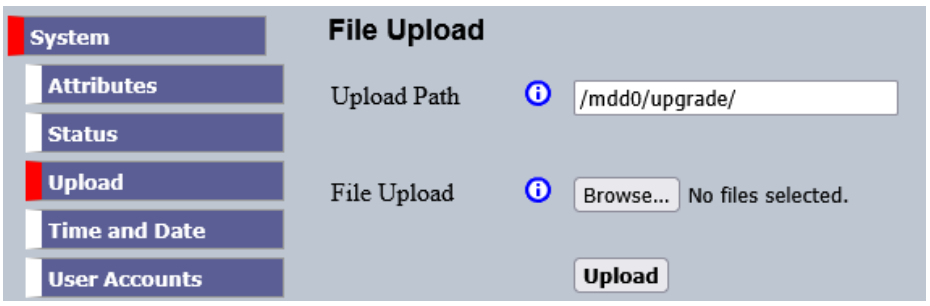
If you are using Enterprise Observer, right click on the server that you wish to upgrade and select "File Upload", this will open the following window. As you can see the upgrade path /mdd0/upgrade/ is pre filled, leave this as is and browse to the ZIP files you downloaded above;



Then click on the "Upload" button. You need to do this for each of the ZIP files, Main Application, CODEC, Framestore and Web Pages.

Once all of the files have been uploaded, reset the unit (DO NOT power cycle it, it must be a soft reset from the web interface, or command line, as the uploaded files are stored in RAM, they will be lost if the unit is power cycled and the unit will not upgrade).

To upload the files via the web interface goto the "System / Upload" web page and select the ZIP files to upload using the "Browse" button followed by "Upload".



Once all of the files have been uploaded, reset the unit.

You can check to see if the software update has been successful by visiting the “Attributes” web page and clicking on the “Software” button, or typing “Version” into the command shell. The reported versions should match the ones that you just downloaded.

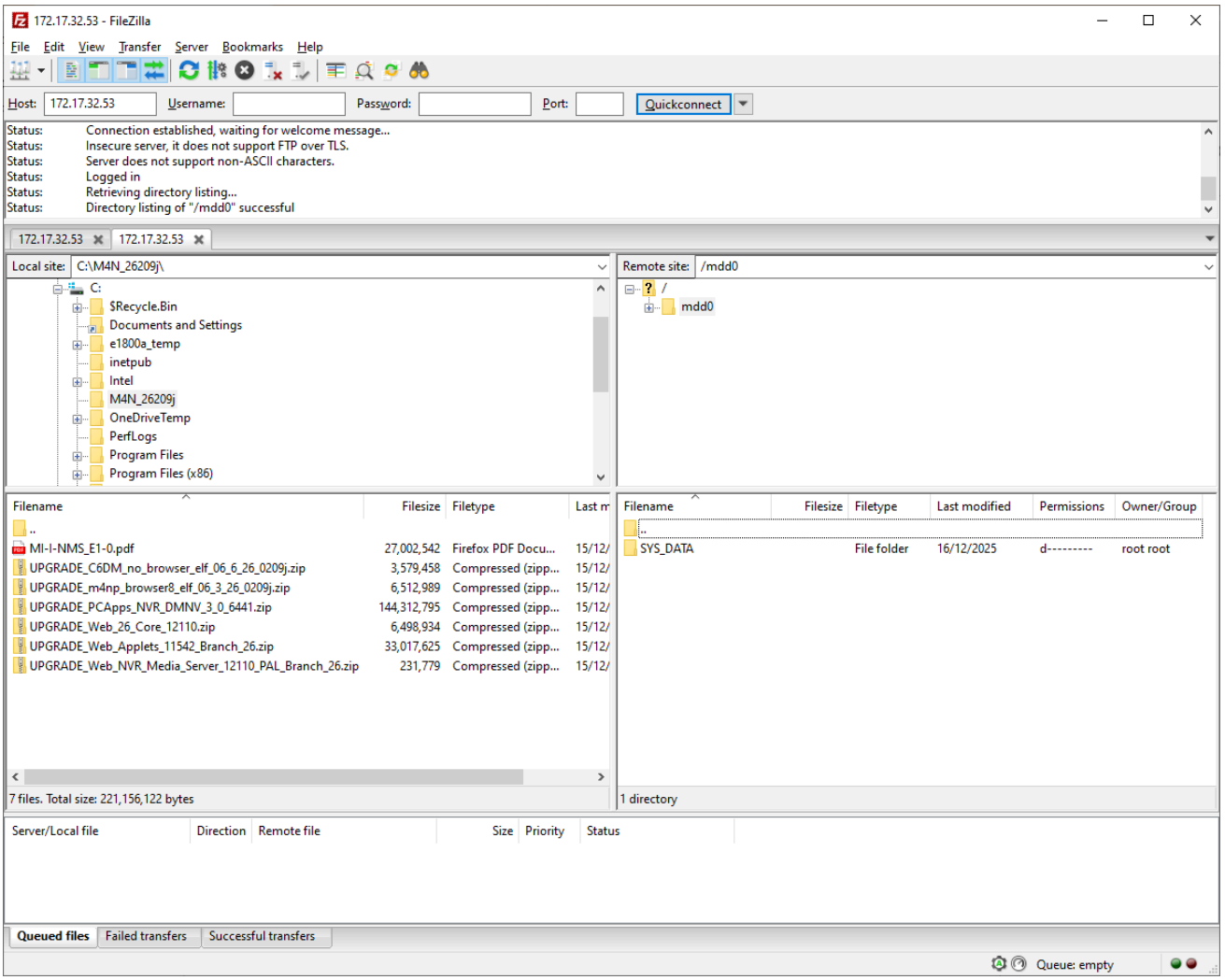
If the micro SD card in the unit is being replaced (I.E. It is blank and contains no software to upgrade) then you will need to either insert the blank card into a card reader in a PC and unzip the files to the card using windows, or copy the files to the card using an FTP client and unzip them from the command line of the unit.

If using Windows make sure that you unzip the files to the card, not just copy them, The files will automatically be placed into the correct directories (folders) on the card.

To transfer the files to the card using FTP, install an FTP client on your PC (NetVu recommends Filezilla https://filezilla-project.org/), start the software and enter the IP address of your unit into the “Host” box, and fill in any username and password to match the unit (if any accounts have been set up) then click “Quickconnect”.

This will open a window displaying two main panes, your PC will be on the left hand side and the unit's micro SD card contents will be shown in the right hand window.

To transfer the files from the PC navigate to the location that you downloaded the files to (in the left hand pane) highlight them and drag them over to the SD Card (in the right hand pane).



In the example above the unit's IP address is 172.17.32.53 and the files are in the PC folder C:\M4N_26209J These are the latest files for the SD Advance NVR and NVR Media server. Selecting these files and dragging them from left to right will copy them to the unit's micro SD card /mdd0. The folder SYS_DATA is automatically created on a blank card, you do not need to do anything with this folder.

Once the files have been copied open a command console via a TELNET connection to the unit (or use the serial port) and type the following;

CD /MDD0	To change directory to the micro SD card
UNZIP *.*	To unzip all of the files on the card (the ones you just copied to it)
DEL *.ZIP	To remove the zip files and make space on the card for future upgrades
RESET	To reboot the unit and run the software

Note. Remember to visit the "Video Storage" web page when the unit has restarted, and enable any additional drives (and video partitions) after re-installing the software on a blank card, as only the first partition of the first drive will be enabled by default. The unit will work but the recording capacity will be limited.

Note. If the wrong files are uploaded to the unit via the web interface or Enterprise Observer then they will not be "used" by the unit, however they will remain in the /MDD0/UPGRADE/ directory consuming storage space and may prevent further upgrades from being performed as there may not be enough remaining space for the correct files. This has become less of an issue over the years, but can cause issues on early units with 1 and 2Gb micro SD cards installed. Late model production units, and all units that have been returned to NetVu's service center will have been fitted with either 4 or 8Gb cards which have enough capacity to hold many incorrectly uploaded files without causing any issues. If you have a unit that fails to upgrade correctly it may have run out of storage space on the micro SD card. If you unzip the files from the command console and receive an error "There were errors during unzip" then you have most probably run out of space on the micro SD card. To free up storage space proceed as follows.

Connect to the unit via TELNET, or serial and open a command console. Type the following;

CD /MDD0/UPGRADE	***Change directory to the UPGRADE folder***
DEL *.ZIP	***Removes all ZIP files from the UPGRADE folder***
CD /MDD0	***Change directory to the ROOT directory can sometimes contain ZIP files***
DEL *.ZIP	***Delete any ZIP files from the ROOT directory***
RESET	***Restart the unit to recover free space***

Then try uploading the upgrade files again.

If this does not work then you can try uploading one file at a time, unzipping it and then deleting the ZIP file. This will take up less space on the card, as once unzipped the ZIP file is no longer required. If you still encounter issues then either install a higher capacity card, NetVu recommend a minimum of 4Gb, or leave out the non-essential ZIP files, such as help videos, web applets, and PC Apps. These will not affect the day to day operation of the unit. The help videos are only played when you click on the "i" icon for further information in a web page, the web applets do not work in any modern browsers (they were used for camera viewing in the web pages, but have been depreciated, you would have to install an old

unsupported web browser to make use of them), and the PC Apps file contains the user manuals and copies of the viewing software Etc, that can be downloaded separately from our web site if required. These are also included for multiple operating systems, Windows, Macos, Linux and Solaris, so it is unlikely that you will need them in most situations.

Password Removal;

NetVu / Dedicated Micros units do not have a default username / password, this is inherently insecure, as the vast majority of users do not change the passwords from the default. Instead the units are accessible from the local network with no username / password checking by default, but will not accept a connection from outside the local subnet (network) unless the user has a valid username / password combination configured. This allows local access for initial configuration, but prevents anyone accessing externally from the Internet, or another network segment on the same site.

It is recommended that an engineering user account is set up during initial configuration and that the installation engineer keeps this information stored as part of their installation documentation so that they have a known login when performing maintenance on the system.

If the password information is lost there is no way to access the unit remotely, or even locally, via the network to reset it. The information is stored in an encrypted file and NetVu has no way to recover / change the user accounts.

If the login information has been lost then the only way to regain access to the unit is to remove the password file and re enter new user account information.

This can only be achieved with “physical access” to the unit in question. There is no way to reset, or remove the passwords remotely. This is part of the secure by design ethos applied to the product range, and although it can cause frustration to both the end user and installer, it is deliberately designed in this manner for maximum security.

There are two methods of removing the password file, which one is used is the choice of the engineer, and depends on what equipment they have available at the time. However both methods achieve the same result.

If the engineer has a serial port and “null modem” cable available then the quickest and easiest way to remove the password is via the unit’s debug port.

If no serial access is available then the file can be deleted directly from the unit’s micro SD card, however this will entail removing the cover from the unit to access the card, as well as access to a card reader (note that most, but not all modern laptops have a micro SD card reader. If choosing a new PC for engineering work on DM / NetVu equipment it is strongly suggested that you check that the PC has one available, or if not buy a USB to micro SD “dongle” to keep as part of the tool kit). This can be time consuming and cumbersome if the unit is rack mounted as it will involve having to disconnect all of the cabling and removal of the unit to allow access.

Serial Password Removal;

To remove the password file via serial, connect the PC to the debug port (COM1) on the unit and using a serial terminal (PUTTY Recommended) open a connection at 115200,8,N,1

You will see various debug messages in the terminal window.

At this point highlight the terminal window and enter “+++” into the window. If you are “lucky” you will get a command prompt, as very few installers bother to set up a serial password. If you get a command prompt you can skip the next section and proceed straight to entering the commands in bold below.

If you are prompted for a username / password when trying to login via serial then you will need to reboot the unit and prevent it from starting the main application and reading the password file. To do this keep the serial lead connected to COM1 on the unit and cycle the power. You will immediately see debug in the serial terminal, watching this carefully you will see a prompt that says “****** serial login to cancel ******”.

At this point enter “+++” and you should see the command prompt SD Advanced Closed IPTV16 (SAFE MODE User) >

Or whatever the model of your unit is in place of “SD Advanced Closed IPTV16”. “SAFE MODE” indicates that the unit has been halted in the loader and will not run the main application.

The serial login prompt is only visible for 2 seconds and easy to miss, so the easier way to enter safe mode is to continually hit the “+” key as soon as you apply power, and continue until you get to the “SAFE MODE” command prompt.

If you miss this window of opportunity then the unit will continue to boot the main application and read the password file so you will be presented with a password request and not be able to log in.

If you miss the prompt simply power cycle and try again. With practice it is possible to access the prompt with just three key presses at the correct point, but continually hitting “++++++++++” is just as effective.

Once you get the ***SD Advanced Closed IPTV16 (SAFE MODE User) >*** prompt then enter the following commands;

CD /MDD0/ETC

DEL USER.DB

RESET

This will remove the password file and restart the unit with no user accounts configured.

At first the serial method may seem more complex, but it can be completed in under a minute with no need to remove the unit from its location, and no need to strip it down.

SD Card Password Removal;

Power down the unit, and remove the lid.

Remove the micro SD card from the unit, you will see it mounted in a slot on the main board either in the front right, or left hand corners, or centrally towards the rear depending on the model. There is only one card, so you can not remove the wrong one.

Once removed, place the card into a card reader, either built into your PC, or USB, and delete the USER.DB file from the ETC folder on the card.

Replace the card and refit the lid.

Power up the unit and it will restart with no user accounts configured.