grass valley

071-8464-01

Monitoring the K2 Media Client with NetCentral

This document describes how to set up the K2 Media Client for monitoring with NetCentral software.

For information about the overall NetCentral system, read the *NetCentral User Guide*.

Table of Contents

Before you begin monitoring with NetCentral

The following systems must be in place before you can begin monitoring your K2 Media Client with NetCentral:

- NetCentral manager software must be installed and operating correctly on the NetCentral server. Refer to the *NetCentral User Guide*.
- The NetCentral server and the K2 Media Client must be on the network and be able to communicate with one another. To verify, use the *ping* command at the MS-DOS command prompt.
- The K2 Media Client device provider must be installed on the NetCentral server PC. In NetCentral manager, click **File | New | Device Provider** and follow the on-screen instructions to install the **K2 Client** device provider. Refer to the *NetCentral User Guide* for a detailed procedure.
- A license is required for the K2 Media Client SNMP agent. Contact your Grass Valley representative to obtain a license.

When these pre-requisites are met, continue with the next procedure "Adding the K2 Media Client to NetCentral".

Adding the K2 Media Client to NetCentral

There are two ways to add a K2 Media Client to NetCentral, as explained in the following sections:

Generating the K2 Storage System view automatically

If the K2 Media Client has external storage as part of a K2 Storage System, the K2 System Configuration application can automatically send information about K2 Storage System devices, such as the K2 Media Client, to NetCentral. This information is sent via a SNMP trap message. When NetCentral receives this information, it automatically adds the K2 Storage System device, creating a unified view for monitoring of the K2 Storage System. When this view is automatically created in NetCentral, it is not necessary to individually add K2 Media Clients or other K2 Storage System devices.

Use the following procedure to automatically generate the K2 Storage System view, which includes adding the K2 Media Client:

1. Monitor (with NetCentral) the control point PC that runs the K2 System Configuration application.

   You must do this before using the K2 System Configuration application to define the K2 Storage System or configure any K2 Storage System devices. This especially means that the control point PC must have its SNMP trap destination set to the NetCentral server PC, so that NetCentral receives the SNMP traps sent by the control point PC. This is true even if the control point PC and the NetCentral server PC are the same machine.

2. Define and configure the K2 Storage System using the K2 System Configuration

application.

As you click **Finish** at the conclusion of each configuration wizard, the K2 System Configuration application sends an SNMP trap message to NetCentral. and NetCentral adds the configuration information.A folder created this way displays blue in NetCentral.

Refer to the *K2 Storage System Instruction Manual* for installation instructions that incorporate these steps.

When you use the K2 System Configuration application to reconfigure a K2 Storage system or device, upon saving the configuration the changes are automatically sent to NetCentral, which then updates accordingly. This means that if you manually change K2 Storage System information in NetCentral (designated by the blue folder color), your changes could later be overwritten by an automatic update from the K2 System Configuration application.

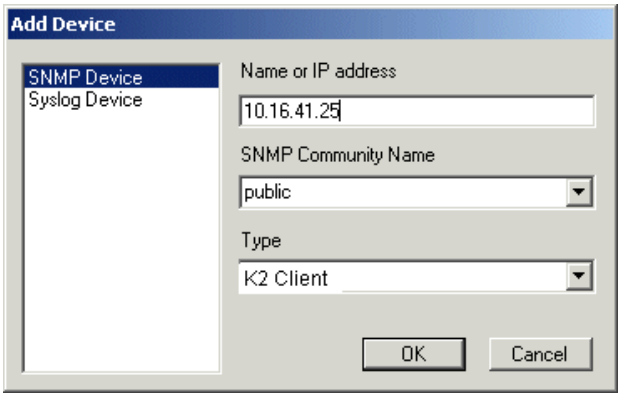
Manually adding the K2 Media Client to NetCentral

When it is necessary to individually add a K2 Media Client to the NetCentral system, use the following procedure. This adds the K2 Media Client to the NetCentral manager tree view and automatically sets the SNMP trap destination on the K2 Media Client. Setting the SNMP trap destination ensures that K2 Media Client status messages are sent to the NetCentral server.

To add the K2 Media Client to the NetCentral tree view:

1. If you have not already done so, log on to NetCentral manager with NetCentral administrator-level access rights. Refer to the *NetCentral User Guide* for information about logging on and application security.
2. In NetCentral, click **File | New | Device**.

   The Add Device dialog box opens.



3. Enter the K2 Media Client IP address.
4. Select **K2 Client** in the Device Type drop-down list, then click **OK**.

   NetCentral Manager attempts to communicate with the K2 Media Client. When contact is made, the K2 Media Client is added to the NetCentral tree view and NetCentral automatically sets the SNMP trap destination address on the K2 Media Client. This may take a few moments.

5. In the tree view, hover your cursor over the K2 Media Client, identify the tooltip displayed, and proceed as follows:
   - If the tooltip only identifies the device as a K2 Media Client and has no message regarding trap validation, it means that NetCentral successfully entered the IP address of the NetCentral server as an SNMP trap destination on the K2 Media Client and then successfully received a test trap message from the device. A K2 Media Client with this tooltip is fully monitored by NetCentral and requires no further steps.
   - If a K2 Media Client has a "…Traps not validated…" tooltip message, one of the following conditions applies. In the Messages view, check the K2 Media Client's SNMP Trap Target Status message to determine which condition applies and then proceed as indicated:
     - NetCentral is in the process of testing the K2 Media Client to validate its SNMP trap messages. After a few minutes check the K2 Media Client again for a change in its SNMP Trap Target Status message reflecting the test results.
     - NetCentral tried to configure SNMP properties but was not successful. In most cases this means you must configure SNMP properties manually as in "What if NetCentral cannot validate K2 Media Client SNMP messages?" on page 4.

What if NetCentral cannot validate K2 Media Client SNMP messages?

If message reporting (SNMP trap messages) is not automatically validated, there may be a problem with the SNMP configuration settings on the K2 Media Client. Use the following procedure to check and configure K2 Media Client SNMP settings. You'll need the IP address or host name of the NetCentral server PC.

To check SNMP settings on the K2 Media Client:

1. Connect a mouse and keyboard to the K2 Media Client, then restart Windows.
2. In Windows, select **Start | Settings | Control Panel**, then open **Administrative Tools**.
3. In the Administrative Tools dialog, open **Services**.
4. Double-click **SNMP Service** to view the properties dialog box.
5. Select the Traps tab.
6. For the community name, enter `public` or the SNMP community name that you use, then click **Add to list**. Also, the SNMP community should have RW access permissions. Do not configure permission settings otherwise.
7. Under "Trap destinations", click **Add**.
8. Enter the IP address or host name of the NetCentral server PC, then click **Add**.
9. On the Security tab, verify that **Send authentication trap** is selected.
10. Click **OK** to save changes and close.
11. On the NetCentral server PC, in the NetCentral tree view, right-click the K2 Media Client and select **Validate Trap Messages**.

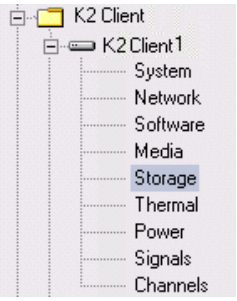
12. In the tree view, hover your cursor over the K2 Media Client, identify the tooltip displayed, and proceed as follows:
    - If the tooltip only identifies the device as a K2 Media Client and has no message regarding trap validation, it means that NetCentral successfully received a test trap message from the device. A K2 Media Client with this tooltip is fully monitored by NetCentral and requires no further steps.
    - If a K2 Media Client has a "…Traps not validated…" tooltip message, NetCentral is still not able to receive messages from the K2 Media Client. Refer to the troubleshooting information in the *NetCentral User Guide*.

Monitoring the K2 Media Client with NetCentral

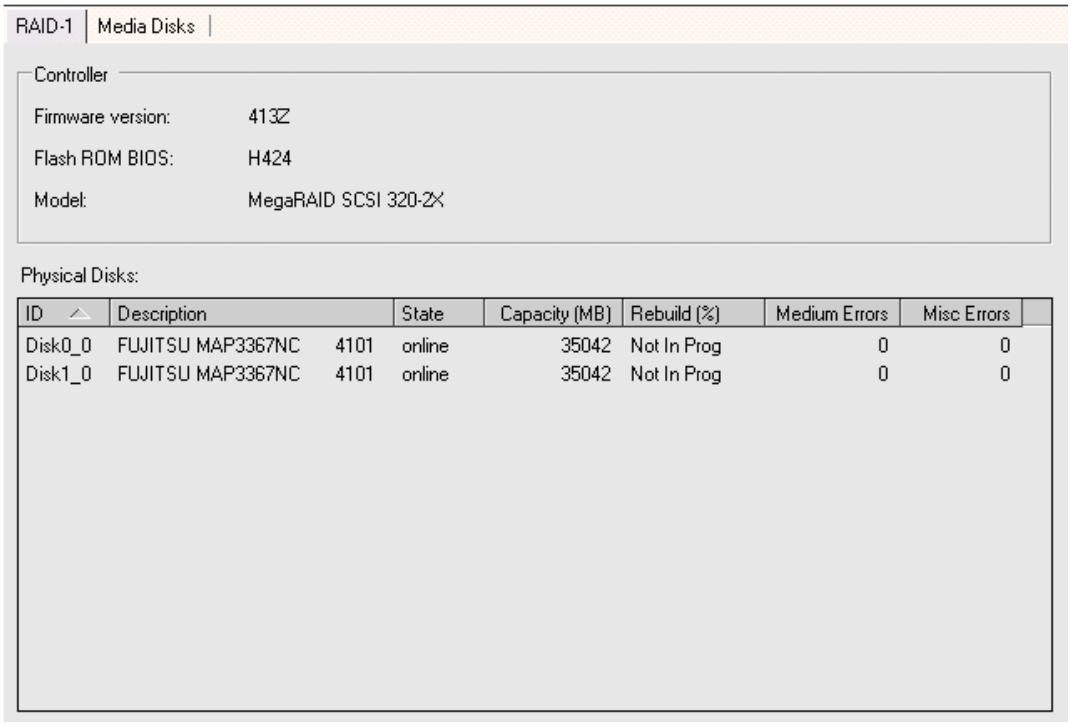
After completing the setup procedure, you are ready to monitor the K2 Media Client using NetCentral. Most monitoring features are common for all types of monitored devices and are explained in the *NetCentral User Guide*. The monitoring features explained in the following sections are unique to the K2 Media Client.

Monitoring K2 Media Client storage

1. In NetCentral, select **Facility**.
2. Expand the NetCentral tree view and locate the K2 Media Client device icon.

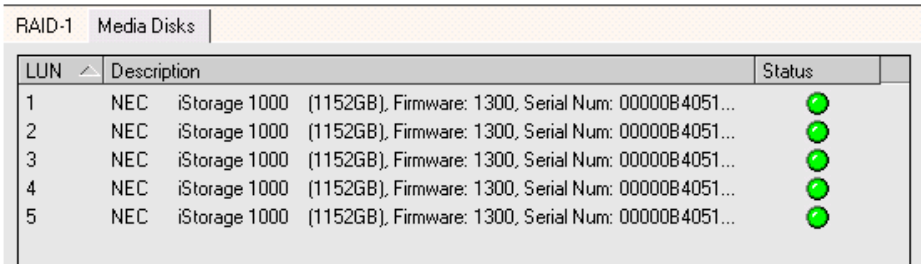


3. Expand the K2 Media Client device icon, then select the **Storage** subsystem.
4. Click the **RAID-1** tab.



This subsystem property page provides information on the disks in the K2 Media Client chassis. On both internal storage and external storage models, two disks (Disk0_0 and Disk 0_1) are displayed. These two disks provide the functionality of the K2 Media Client system drive. The screen shot above illustrates an external storage model. On internal storage models, 10 additional disks are displayed that provide the functionality of media storage drives.

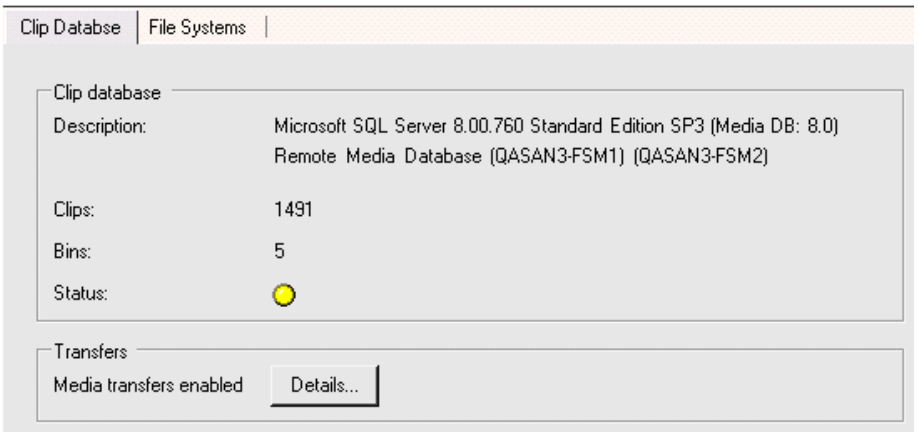
5. Click the **Media Disks** tab.



This subsystem property page provides information on logical drives that provide the media storage. A logical drive consists of one or more physical disks that are bound as a RAID Logical Unit Number (LUN). On internal storage models, these logical drives are the RAID 1 LUNs, each of which is made up of two physical disks that reside in the K2 Media Client chassis. On external storage models, these logical drives are RAID 1, 3, or 5 LUNs, each of which is made up of multiple physical disks that reside in the RAID storage device chassis. The screen shot above illustrates an external storage model.

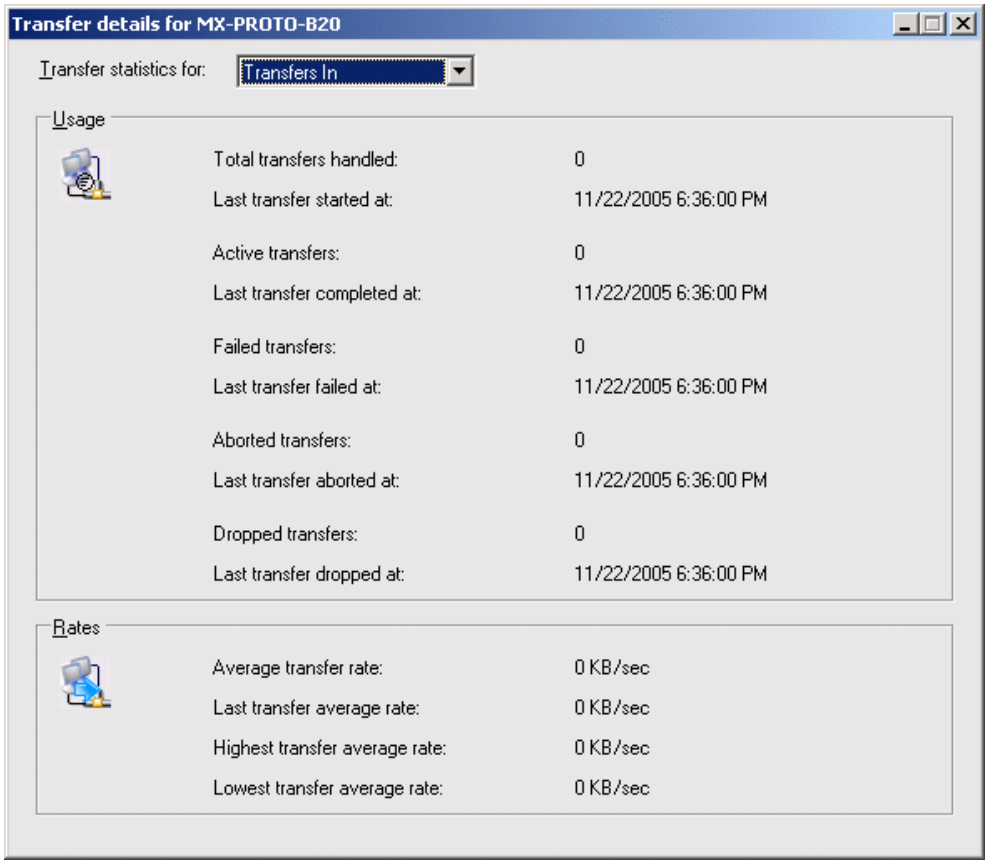
Monitoring K2 Media Client media

1. In NetCentral, select **Facility**.
2. Expand the NetCentral tree view and locate the K2 Media Client device icon.
3. Expand the K2 Media Client device icon, then select the **Media** subsystem.
4. Click the **Clip Database** tab.



This subsystem property page provides information on the SQL database that holds the records of the clips in the media storage accessed by the K2 Media Client. If the K2 Media Client is an external storage model, as shown in the screenshot above, the K2 Media Server that is in the role of media database server is displayed. If a redundant K2 Storage System, the redundant media database servers are displayed.

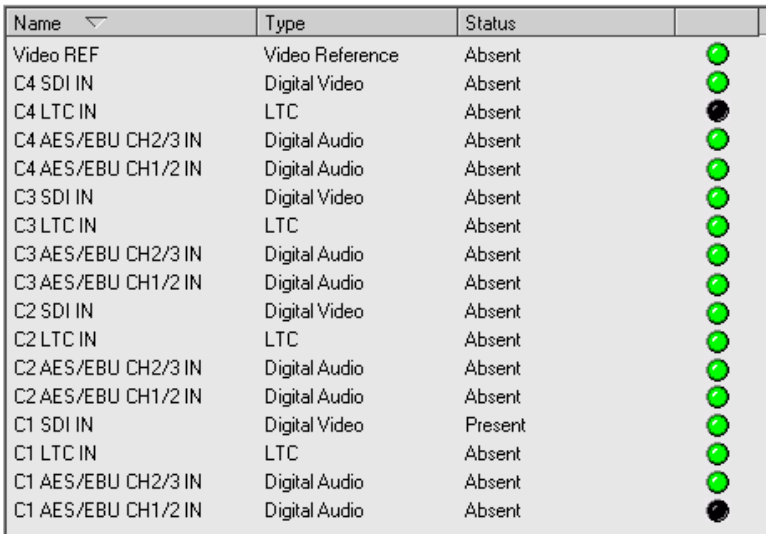
5. Click the **Details** button. The Transfer Details page opens.



This page provides information on transfers in and out of the K2 Media Client.

Monitoring K2 Media Client signals

1. In NetCentral, select **Facility**.
2. Expand the NetCentral tree view and locate the K2 Media Client device icon.
3. Expand the K2 Media Client device icon, then select the **Signals** subsystem.

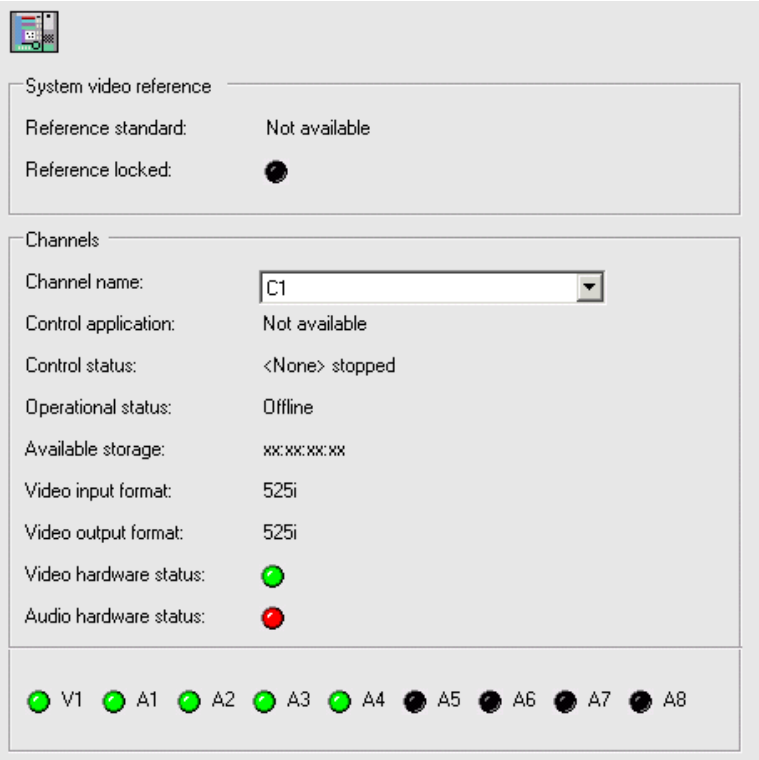


Name	Type	Status	
Video REF	Video Reference	Absent	
C4 SDI IN	Digital Video	Absent	
C4 LTC IN	LTC	Absent	
C4 AES/EBU CH2/3 IN	Digital Audio	Absent	
C4 AES/EBU CH1/2 IN	Digital Audio	Absent	
C3 SDI IN	Digital Video	Absent	
C3 LTC IN	LTC	Absent	
C3 AES/EBU CH2/3 IN	Digital Audio	Absent	
C3 AES/EBU CH1/2 IN	Digital Audio	Absent	
C2 SDI IN	Digital Video	Absent	
C2 LTC IN	LTC	Absent	
C2 AES/EBU CH2/3 IN	Digital Audio	Absent	
C2 AES/EBU CH1/2 IN	Digital Audio	Absent	
C1 SDI IN	Digital Video	Present	
C1 LTC IN	LTC	Absent	
C1 AES/EBU CH2/3 IN	Digital Audio	Absent	
C1 AES/EBU CH1/2 IN	Digital Audio	Absent	

This page provides information on the signals present at the input and output connectors of the K2 Media Client. A green indicator means a signal is present. A black indicator means no signal detected. A red indicator means there is a problem with the signal.

Monitoring K2 Media Client channels

1. In NetCentral, select **Facility**.
2. Expand the NetCentral tree view and locate the K2 Media Client device icon.
3. Expand the K2 Media Client device icon, then select the **Channels** subsystem.


System video reference
Reference standard:
Not available
Reference locked:
Channels
Channel name:
C1
Control application:
Not available
Control status:
<None> stopped
Operational status:
Offline
Available storage:
xx:xx:xx:xx
Video input format:
525i
Video output format:
525i
Video hardware status:
Audio hardware status:
V1
A1
A2
A3
A4
A5
A6
A7
A8

This page provides information on the current operation and status of the channels of the K2 Media Client. V1 indicates video. A1 through A8 indicate audio.

Monitoring K2 Media Client Trends

Click the **Trends** button to see the Trends view. The Trends view pulls specific device parameters and provides you with a daily, weekly, monthly, and yearly view of selected parameters. The following table lists the Trends view graphs for the K2 Media Client and provides explanations:

Name of Trend graph	Explanation of Trend graph
System\ Up Time	Up time essentially is an ever incrementing value that indicates the system is up and running and is measured as an absolute value in minutes; given that the polling rate is more than a minute. Though the value itself is of less significance, it is the ramp graph obtained by plotting these values that proves significant where a downward edge on the ramp indicates a device going offline and a flat line at zero indicating the device downtime. Multiple ramps indicate how often the device was taken down for activities like maintenance or servicing, or simply how many times it was restarted to handle a complete device failure. If the ramps do not coincide when the device was taken down, it could indicate conditions like automatic restarts, and the device may need attention.
System\ Processor Usage[*CPUn*]	Processor usage is a primary indicator of processor activity. It is the average percentage of elapsed time that the processor spends executing non-idle programs during that sampling period. Sustained value over 90% (5 minutes or more) indicates an excessively busy system and may result in the system appearing unresponsive. If the usage is associated with a single program, the program may be faulty and need a restart. Upper Threshold: 90
System\ Processes	Processes indicates the number of processes running on the system during that sampling interval. A Windows system creates one or more “process” when a program is run. A process contains computer instructions. The number of processes running on the system is a secondary indicator of the processor loading. A sustained increase in the number of processes indicates suspicious processing activity on the system.

Name of Trend graph	Explanation of Trend graph
System\ Memory Usage	Memory usage is the percentage of total (physical memory and page file space) memory used by programs running on the system during that sampling period. Sustained increase in this value could indicate a memory leak in one or more running programs and might eventually lead to system failure due to unavailability of more memory. Upper Threshold: 90
Storage\ Disk Usage[*diskname*]	Disk usage is the percentage of the total usable storage space on the logical fixed (hard) disk that was used to store programs and data during that sampling period. Sustained increase in this value over 90% may start degrading system performance and eventually lead to a disk full condition causing failures while saving data to the disk. Note, this also includes media disk usage. Upper Threshold: 90
Network\ Network Link Usage[*linkname*]	Network link usage is the percentage of the attained throughput on the network link compared with its maximum operational capacity during that sampling period. This helps measure congestion (or potential congestion) through the network. A sustained high value is not necessarily bad. However over utilization occurs when there is more traffic queued to pass over the link than it can handle, there will be latency implications. Note, this also includes network links used for media transfers.
Network\ Network Link Bandwidth[*linkname*]	Network link bandwidth is the amount of actual data transferred on the port during that sampling period measured in bits per second. Bandwidth is used to measure the quality of service (QoS) of the network link. Higher values indicate faster data transfers and better performance. Note, this also includes network links used for media transfers.

Name of Trend graph	Explanation of Trend graph
Network\ Network Link Errors [*linkname*]	Network link errors is the percentage of error occurrences on the link when receiving network data during that sampling period. Note that transmit errors are not accounted because a network interface never knowingly places frames with errors on the network. This is indicative of network problems. When errors occur, typically attempts would be made to retransmit the data potentially causing more errors. Sustained values above 10% are indicative of faulty network cabling, or a suspicious Ethernet controller, or port. Note, this also includes network links used for media transfers. Upper Threshold: 10
Thermal\ Motherboard Temperature[*location*]	Motherboard Temperature indicates the current temperature value in degrees Centigrade read by the temperature probe at the specific location on the motherboard during that sampling period. If this value starts rising consistently, it could indicate malfunctioning hardware or HVAC. Values above 55 degrees Centigrade can damage the system. Upper Threshold: 55
Thermal\ Real-time System Temperature	Real-time system temperature indicates the maximum reading in degrees Centigrade obtained from all the temperature probes installed on the Real-time system assembly. If this value starts rising consistently, it could indicate malfunctioning hardware or HVAC. Values above 55 degrees Centigrade can damage the system. Upper Threshold: 55
Video\ Video Drops[*channel*]	Video drops indicate the number of times that the video processing subsystem on the channel started dropping video. When video is dropped by a recorder channel, black video is written to the disks. When video is dropped by a player channel, black or frozen video is played back. This should always be zero. Consistent ramps could indicate bad disks or bad media.
Storage\ RAID Controller IO Errors	RAID Controller IO Errors indicates the rate of IO error occurrence tracked by the RAID controller. This should typically be zero. A persistent IO occurrence indicates problems with the RAID controller and the associated disk hardware.

Name of Trend graph	Explanation of Trend graph
Storage\ Logical Disk IO	Logical Disk IO indicates the rate at which disk read and write requests being made to the logical disk per second. This provides an estimate of the disk IO activity.

Troubleshooting the K2 Media Client with NetCentral

NetCentral reports status, warnings, and alarms using messages that are easy to understand. Suggested corrective actions are presented along with failure information. If you have any trouble interpreting any of the problems or suggested solutions, contact Grass Valley Support.

For more information

For more information about NetCentral, how it works, and how to configure and use its features, refer to the *NetCentral User Guide*. You can find an online Help version of this manual on the NetCentral Help menu.