

# ***K2 Summit/Solo/SAN Release Notes and Upgrade Instructions Software version 8.1.10***

This document contains the most recent information and supersedes previous publications. Check the Grass Valley website at [www.grassvalley.com/docs](http://www.grassvalley.com/docs) for an updated version that contains additional important information.

# Contacting Grass Valley

<b>International Support Centers</b>	<b>France 24 x 7</b>	+800 8080 2020 or +33 1 48 25 20 20	<b>United States/Canada 24 x 7</b>	+1 800 547 8949 or +1 530 478 4148
<b>Local Support Centers (available during normal business hours)</b>	<b>Asia</b>	<b>Hong Kong, Taiwan, Korea, Macau:</b> +852 2531 3058 <b>Indian Subcontinent:</b> +91 22 24933476 <b>Southeast Asia/Malaysia:</b> +603 7492 3303 <b>Southeast Asia/Singapore:</b> +65 6379 1313 <b>China:</b> +861 0660 159 450 <b>Japan:</b> +81 3 5484 6868		
		<b>Australia and New Zealand:</b> +61 1300 721 495	<b>Central/South America:</b> +55 11 5509 3443	
		<b>Middle East:</b> +971 4 299 64 40 <b>Near East and Africa:</b> +800 8080 2020 or +33 1 48 25 20 20		
	<b>Europe</b>	<b>Belarus, Russia, Tadzikistan, Ukraine, Uzbekistan:</b> +7 095 2580924 225 <b>Switzerland:</b> +41 1 487 80 02 <b>S. Europe/Italy-Roma:</b> +39 06 87 20 35 28 <b>-Milan:</b> +39 02 48 41 46 58 <b>S. Europe/Spain:</b> +34 91 512 03 50 <b>Benelux/Belgium:</b> +32 (0) 2 334 90 30 <b>Benelux/Netherlands:</b> +31 (0) 35 62 38 42 1 <b>N. Europe:</b> +45 45 96 88 70 <b>Germany, Austria, Eastern Europe:</b> +49 6150 104 444 <b>UK, Ireland, Israel:</b> +44 118 923 0499		

Copyright © Grass Valley USA, LLC. All rights reserved.  
This product may be covered by one or more U.S. and foreign patents.

## Grass Valley Web Site

The <http://www.grassvalley.com/support> web site offers the following:

**Online User Documentation** — Current versions of product catalogs, brochures, data sheets, ordering guides, planning guides, manuals, and release notes in .pdf format can be downloaded.

**FAQ Database** — Solutions to problems and troubleshooting efforts can be found by searching our Frequently Asked Questions (FAQ) database.

**Software Downloads** — Download software updates, drivers, and patches.



## END-OF-LIFE PRODUCT RECYCLING NOTICE

Grass Valley's innovation and excellence in product design also extends to the programs we've established to manage the recycling of our products. Grass Valley has developed a comprehensive end-of-life product take back program for recycle or disposal of end-of-life products. Our program meets the requirements of the European Union's WEEE Directive, the United States Environmental Protection Agency, and U.S. state and local agencies.

Grass Valley's end-of-life product take back program assures proper disposal by use of Best Available Technology. This program accepts any Grass Valley branded equipment. Upon request, a Certificate of Recycling or a Certificate of Destruction, depending on the ultimate disposition of the product, can be sent to the requester.

Grass Valley will be responsible for all costs associated with recycling and disposal, including freight. However, you are responsible for the removal of the equipment from your facility and packing the equipment to make it ready for pickup.



For further information on the Grass Valley product take back system please contact Grass Valley at + 800 80 80 20 20 or +33 1 48 25 20 20 from most other countries. In the U.S. and Canada please call 800-547-8949, and ask to be connected to the EH&S Department. Additional information concerning the program can be found at: [www.grassvalley.com/about/environmental-policy](http://www.grassvalley.com/about/environmental-policy)

001187401

# Contents

Release Summary.....	5
Release note revisions for this release.....	5
What's new in version 8.1.10.....	5
Feature limitations in this release.....	5
Not supported in this release.....	5
Changes and features in previous releases.....	6
Additional notes.....	8
Passwords and security on Grass Valley systems.....	8
Password changes and compatibility.....	8
About application security on the K2 SAN.....	9
About proxy/live streaming.....	10
Managing the write filter.....	11
K2 Summit/Solo formats.....	13
Installing and configuring support for Windows 7 generic iSCSI clients.....	14
Extent Manager for K2 SANs.....	16
Operation considerations.....	17
Version compatibility.....	19
Compatible K2 Summit/Solo components.....	19
Compatible K2 Media Server components.....	22
Compatible K2 Control Point PC components.....	23
Compatible HP ProCurve GigE switch components.....	23
Compatible K2 RAID components.....	24
Compatible K2 RAID disk drive firmware.....	25
Compatible Grass Valley products.....	29
Compatible recovery applications.....	31
Upgrading K2 systems.....	32
Upgrading a K2 SAN.....	32
About upgrading the K2 SAN with SiteConfig.....	32
Make recovery images.....	33
Prepare SiteConfig for software deployment to K2 SAN devices.....	33
Deploy control point PC software.....	34
Take SAN clients offline.....	35
Manage multiple K2 Media Servers.....	35
Upgrade K2 Media Server.....	37
Verify/upgrade switch firmware.....	45
Upgrade RAID controller microcode.....	46
Upgrade RAID disk drive firmware.....	46
Reset Capture Services.....	47
Update Broadcom driver.....	48
Configure fsnameservers on servers-class devices.....	49
Manage redundancy on K2 Media Servers.....	51
Upgrade remaining K2 Media Servers.....	52
Upgrade K2 client.....	52
Upgrade STRATUS and Aurora Playout systems.....	60
Upgrade other SAN clients.....	60
Make recovery images.....	60
Upgrading stand-alone K2 systems with SiteConfig.....	61
About upgrading stand-alone K2 systems with SiteConfig.....	61
Make recovery images.....	61

Prepare for K2 system upgrade.....	62
Configure SNFS default.cfg file on stand-alone K2 system.....	62
Prepare SiteConfig for software deployment to stand-alone K2 systems.....	64
Check all currently installed software on stand-alone K2 systems.....	64
Add software package to deployment group for stand-alone K2 systems.....	65
Unlock K2 Summit Production Clients or K2 Solo Media Servers.....	65
Upgrade software on stand-alone K2 systems.....	66
Install required Windows updates.....	69
Upgrade disk drive firmware on stand-alone K2 system.....	71
Configure RTIO.....	72
Reset Capture Services.....	73
Lock K2 Summit Production Clients.....	74
Install MPEG-2/AVC-Intra field kit.....	74
Make recovery images.....	75
Deploy control point PC software.....	75
Upgrading stand-alone K2 systems without SiteConfig.....	75
Make recovery images.....	75
Prepare for K2 system upgrade.....	76
Disable write filter.....	76
Configure SNFS default.cfg file on stand-alone K2 system.....	76
Uninstall K2 software from stand-alone K2 system.....	77
Uninstall SNFS from K2 client.....	78
Install K2 software.....	78
Install SNFS on stand-alone K2 system.....	81
Verify upgraded software.....	81
Install required Windows updates.....	82
Upgrade disk drive firmware on stand-alone K2 system.....	84
Configure RTIO.....	85
Reset Capture Services.....	86
Upgrade remaining stand-alone K2 systems.....	87
Enable write filter.....	87
Install MPEG-2/AVC-Intra field kit.....	87
Make recovery images.....	87
Licensing K2 products.....	88
K2 licenses.....	88
About K2 system software licensing.....	89
Requesting a license.....	90
Adding a license.....	91
Deleting licenses.....	92
Archiving licenses.....	92
Known Problems.....	93
Trademarks and agreements.....	97
Trademarks.....	97
JPEG acknowledgment.....	97

---

# Release Summary

## Release note revisions for this release

This release of software has multiple versions of release notes, as follows:

Part number	Description
071-8781-08	Initial release notes for K2 version 8.1.10 software
071-8781-09	Topics added/modified as follows: <ul style="list-style-type: none"><li>• SNFS version updated to 3.5.3.b27171.</li><li>• Compatible GV STRATUS version updated to 2.5</li></ul>
071-8902-00	Topics added/modified as follows: <ul style="list-style-type: none"><li>• <a href="#">Install required Windows updates</a> on page 56</li></ul>

## What's new in version 8.1.10

- **K2 Dyno** — Compatibility with K2 Dyno version 2.0.3. Refer to "K2 Dyno Controller Release Notes" for more information on the following:
  - **Simplified SuperOut setup in AppCenter** – Channel properties can still be turned on or off, but their screen positions are now fixed. This reduces the number of decisions that need to be made at setup time and eliminates configurations that cause properties to overlap.
  - **SuperOut reflects the information on the Dyno screen** – Dyno status information is now available on the SuperOut monitor.
  - **Larger SuperOut font** – The font is larger and the outline is thicker.

## Feature limitations in this release

- The following features are documented in customer manuals but are absent in the AppCenter user interface. They will be enabled in a future release:
  - Record AFD as clip property
  - CEA-608 to DTV CC transcoder

## Not supported in this release

The following devices and functionality are not supported with this version of K2 software. Check with your Grass Valley representative regarding availability.

- K2 Media Client — Compatible with 3.x versions of K2 software only.

## Changes and features in previous releases

The following sections describe changes and features in past releases.

### Version 8.1.9

- **STRATUS** — Compatibility with STRATUS 2.0.
- **Solo** — Support K2 Solo systems with 300GB drives.
- **Documentation** – Use K2/STRATUS Documentation Set 063-8289-09 June 2012, in addition to these release notes, with this release of K2 software. The following manuals are new/revised:
  - K2 Summit/Solo Field Kit Upgrade Instructions 071-8721-03

### Version 8.1

- **K2 Summit 3G Production Client** — The next generation K2 Summit Production Client. Supports the same feature set and expands upon it as follows:
    - AVCHD play output (decode) support as an option.
    - 3G codec module hosts codec option cards that are programmable for multiple formats and functions, including multi-cam configurations with XDCAM HD format, Super Slow-motion in both DVCPRO HD and AVC-Intra formats, and playback of H.264 clips.
    - Ready for 1080p 50/60 fps applications in the future with a software only upgrade.
    - 2.5 inch internal storage media storage drives. Capacity increased by 50% (12 x 600GB).
    - mSATA SSD system drive with larger capacity, protected by a file-based write filter.
    - USB 3.0 interface for file exchange
- NOTE: K2 Transmission Clients/Servers and K2 Solo models continue to be available and are not replaced by K2 Summit 3G Production Client.**
- **SNFS file system** — Upgrade to version 3.5.3.b21398 is required.
  - **Documentation** – Use K2/STRATUS Documentation Set 063-8289-08 February 2012, in addition to these release notes, with this release of K2 software. The following manuals are new/revised:
    - K2 AppCenter User Manual 071-8723-03
    - K2 System Guide 071-8726-03
    - K2 Summit 3G Service Manual 071-8725-02
    - K2 SAN Installation and Service Manual 071-8779-01
    - K2 Storage Cabling Guide 071-8780-01
    - K2 Summit 3G Client Quick Start Guide 071-8722-03
    - K2 Summit/Solo Field Kit Upgrade Instructions 071-8721-03
    - K2 Summit 3G Field Kit Upgrade Instructions 071-8826-00

### Version 8.0.x

- **STRATUS** — Support for Grass Valley's STRATUS™ Media Workflow Application Framework.

- **Proxy/live streaming** — When licensed and configured to do so, the K2 Summit system creates low-resolution representations of high-resolution media. The system generates a live stream at inputs and outputs. The system also creates proxy files for recorded assets. Proxy/live streaming functionality is included in AppCenter Pro and AppCenter Elite licenses. This functionality requires the currently shipping Type II carrier module. To access proxy/live streaming for application workflows, you must use a supported STRATUS system configuration, which includes a separate proxy server. Direct access on a K2 Summit system alone is not supported.
- **Unified file system** — The media file system supports direct access and interchange with the STRATUS™ Media Workflow Application Framework.
- **Credentials** — Default user accounts and passwords change for better integration across all Grass Valley products. Refer to [Password changes and compatibility](#) on page 8.
- **USB Recovery Flash Drive** — The size increased to 16 GB.
- **Upgrade** — Upgrading existing K2 Summit systems to software version 8.0.x is a disk image process and requires upgraded hardware as well. Software-only upgrade is not supported. Therefore, you must procure an upgrade field kit from Grass Valley, as follows:
  - K2-XDP-CPU-FK — Includes a Type II carrier module with the new higher performance CPU/COM Express board. Order this field kit if you require proxy/live streaming support and your K2 Summit system does not already have a Type II carrier module.
  - K2-XDP-V8x-FK — Does not include a Type II carrier module. Order this field kit if your K2 Summit system already has a Type II carrier module or if you do not require proxy/live streaming support.

Both field kits include the disk image, CompactFlash, USB Recovery Flash Drive, and documentation required for the upgrade to version 8.0.x software.

- **Documentation** – Use K2/STRATUS Documentation Set 063-8289-07 October 2011, in addition to these release notes, with this release of K2 software. The following manuals are revised:
  - K2 AppCenter User Manual 071-8723-02
  - K2 System Guide 071-8726-02
  - K2 Solo Media Server Quick Start Guide 071-8710-02
  - K2 Summit Client Quick Start Guide 071-8722-02
  - K2 Summit/Solo Field Kit Upgrade Instructions 071-8721-02
  - K2 TimeDelay User Manual 071-8727-01
  - SiteConfig User Manual 071-8693-03

---

# Additional notes

The following sections contain additional information about this release.

## Passwords and security on Grass Valley systems

To provide a basic level of security, Grass Valley systems recognize three different security levels based on Windows users and groups, and the systems ship from the factory with accounts pre-configured accordingly. To access the system you must login with the username and password for one of the pre-configured accounts.

The following table shows the different types of users and their privileges. Passwords are case sensitive.

	Windows administrator	Grass Valley product administrator	Grass Valley product user
Login	Administrator	GVAdmin	GVUser
Password	adminGV!	adminGV!	userGV!
AppCenter Configuration Manager	Full access	Full access	Can view
AppCenter	Full access	Full access	Full access; requires an account on the K2 Summit/Solo system
Storage Utility	Full access	Full access	Can't access
K2Config	Full access	Full access	Can't access
Server Control Panel	Full access	Can view	Can view
Windows Operating System	Full access	Limited access (based on Windows login privileges). Not a member of the Administrators group.	Limited access (based on Windows login privileges)

To support legacy FTP and security features, K2 systems also have *movie*, *mxfmovie*, *mpgmovie*, and *video\_fs* accounts. Do not use these accounts to log in to the Windows operating system on K2 systems.

## Password changes and compatibility

With currently released products, default accounts and passwords are unified across Grass Valley systems. This includes K2, STRATUS, and Aurora products. However, some previous versions of Grass Valley products had default accounts and passwords that were not unified with other Grass Valley products. For example, the Administrator account on previous versions of K2 products had a password of `adminK2`, rather than the unified password of `adminGV!`.

Therefore, when combining newer, currently released Grass Valley products with older, previously released products, you must manage your passwords for system and operational compatibility. Grass Valley recommends the following:

- Ensure that a user account that is the same on all systems has the same password.
- Change all passwords to the newer unified passwords. This applies especially to the Administrator account, where you would change the password on your older systems from `adminK2` to `adminGV!`.
- If your site policies prohibit changing your passwords, then you may change the passwords on your newer systems to match your older systems. In the case of the Administrator account, on your newer systems you would change the password from `adminGV!` to `adminK2`.
- Do not change the password for the GVadmin account. This account must retain the default password of `adminGV!`. Grass Valley applications and services use this account/password for program interactions.

Consider the following as you change passwords:

- SiteConfig provides default credentials for each device type. If you have not overridden these default credentials in SiteConfig, whenever your SiteConfig access requires authentication, SiteConfig uses the default credentials. When you upgrade SiteConfig, it is possible that the newer version of SiteConfig has newer default credentials. If this is the case, authentication can fail when SiteConfig uses the new default credentials to access a device still configured for the old default credentials. Therefore, refer to SiteConfig Release Notes when upgrading and if default credentials change, reconcile by overriding default credentials in SiteConfig as necessary.
- Transfers between K2 systems require that the same user account and password be on both systems. The transfer uses the credentials with which you are logged in to the application initiating the transfer to authenticate the transfer on the other K2 system. If a password has changed and is no longer the same or an account is not present, the transfer fails. Therefore, when initiating transfers use accounts and passwords that are the same on all systems.

## **About application security on the K2 SAN**

The K2Config application and the Storage Utility application both require that you be logged in to the application with administrator privileges in order to modify any settings. These privileges are based on the Windows account that you use when you log in to the K2Config application. When you open Storage Utility from within the K2Config application, the account information is passed to Storage Utility, so you do not need to log in separately to Storage Utility.

In SiteConfig you configure global and/or device-type credentials for device access. These credentials are likewise based on Windows accounts.

You must use a Windows account that has local administrator privileges on the machine to be configured. For example, when you are on a control point PC and you run the K2Config application for the purpose of configuring a K2 Media Server, the account with which you log in to the K2Config application must be present on the K2 Media Server and must have administrator privileges on the K2 Media Server.

For initial setup and configuration, you can use the default Windows Administrator username and password to log in to applications and machines as you work on your K2 SAN. However, for ongoing security you should change the username/password and/or create unique accounts with similar

privileges. When you do this, you must ensure that the accounts are present locally on all K2 SAN machines, including control point PCs, K2 Media Servers, K2 Media Clients, K2 Summit Production Clients, and other iSCSI clients.

NetCentral also has accounts for security levels, as follows:

- NetCentral Administrator
- NetCentral Technician
- NetCentral User

Grass Valley recommends mapping the NetCentral administrator with product administrator accounts for your K2 and other Grass Valley products. This allows you to log on to NetCentral as administrator using the product administrator logon. You can also assign other NetCentral groups to users, as necessary for your site's security policies. You need Windows administrator privileges to add or modify a user's privileges. For more on NetCentral security, see NetCentral documentation.

## **About credentials in SiteConfig**

SiteConfig requires administrative privileges on devices in order to perform most of the network configuration and deployment tasks. For known device types, SiteConfig has a default administrator login and password. These default credentials depend on the SiteConfig version, so check your SiteConfig Release Notes for any changes. When you add a device based on a known device type, SiteConfig references the default administrator login and password. Then, when you use remote desktop or perform software deployment to the device, SiteConfig automatically uses these credentials. These credentials are called "global" credentials for the device since the same credentials are used on all devices of that type in the system.

You can choose to override the default credentials for a given device type. For example, if you have specified a different administrator account or a different password on the devices when commissioning the system, then you want SiteConfig to use these modified credentials.

It is possible to also override the default credentials for a single device.

## **About proxy/live streaming**

The K2 Summit system writes proxy files to a CIFS share, using credentials GVAdmin. A proxy file contains the video track, up to eight audio tracks, and timecode. The file is a fragmented MPEG-4 file, which can record/play in chunks. This allows you to play a growing proxy file while it is still recording.

Each K2 Summit system channel multicasts a low-resolution live stream. The K2 Summit system has an HTTP server over which it makes the SDP file available to applications that play the live stream.

A Type II carrier module is required to support proxy/live streaming.

An AppCenter Pro or AppCenter Elite license on the K2 Summit system enables proxy/live streaming. If licensed for AppCenter Pro, a live stream is available from each of the four channels. If licensed for AppCenter Elite, ChannelFlex features allow you to configure up to eight inputs/outputs, so up to eight live streams are similarly available. When a K2 Summit system is licensed, in Configuration Manager (a part of the K2 AppCenter application) you can configure proxy/live streaming for each

channel. You can turn proxy file recording on or off, and you can turn live network streaming on or off. When you turn proxy file recording on, you can then select up to eight audio tracks to include in the proxy file. You can also turn automatic scene detection on or off. When you turn scene detection on, you can configure the minimum scene length. When you turn proxy live network streaming on, you can then select two audio tracks (one pair) to include in the proxy stream.

If licensed for AppCenter Elite, a ChannelFlex channel generates proxy/live streaming as follows:

- **Multi-cam Recorder** — Both high-resolution assets have their own proxy file. Two live streams are also available. If shared audio, the proxy file and live stream are generated as follows: the first input includes video, audio, and timecode; the second input includes video but does not include audio and timecode. If shared audio, the proxy file and live stream are generated as follows: the first input includes video, audio, and timecode; the second input includes video and audio but no timecode.
- **3D / Video + Key** — A proxy file is generated with one video. Two live streams are available as follows: the first input/output includes video, audio, and timecode; the second input/output includes video but does not include audio and timecode.
- **Super Slo-Mo Recorder** — A video-only proxy file and a video-only live stream are generated that are normal speed, which means that they are one half or one third the Super Slo-Mo record rate.

Proxy recording is not supported for continuous record mode.

Network switches and firewalls must be configured to allow the multicast live streaming traffic.

Grass Valley's STRATUS product accesses proxy files through a shared CIFS folder. There is a limit to the number of proxy access connections on the server that hosts the share. Therefore full proxy recording is only supported using one of the recommended STRATUS configurations with a proxy server. Recording and storing proxy on the local media storage on a K2 Summit/Solo system is not recommended.

## Managing the write filter

The following topics describe the K2 Summit Production Client and K2 Solo Media Client write filter.

### About the write filter

The K2 Summit/Solo system has a file-based write filter, which is a feature of the Windows embedded operating system. With the write filter enabled, files can be created, modified, and deleted, but these changes are held in a memory cache. When the K2 system restarts, these changes are lost and the K2 system returns to its original state. This protects the K2 system from changes and increases on-air reliability. For any system configuration change the write filter must be disabled otherwise changes are lost at the next restart.

Some directories, such as *C:\logs*, *C:\Profile\config*, and *C:\Profile\ChannelSuites*, are excluded from write filter protection, so that channel configuration and logs are saved. Do not attempt to alter this list of excluded directories. If you suspect that write filter configuration has been altered, use the recovery image process to restore to the default configuration.

To enable the write filter, the K2 system must be restarted. Likewise, to disable the write filter, the K2 system must be restarted. You can enable/disable the write filter remotely using the K2Config application or by using the SiteConfig application lock/unlock feature. The SiteConfig lock/unlock feature applies to one K2 system at a time or on a group of K2 systems all at once. You can also enable/disable the write filter from a local K2 system, but if you use the local method, do not also use the SiteConfig method. If you enable/disable the write filter locally, the change is not automatically sent to SiteConfig, so SiteConfig can not reliably indicate the current lock/unlock state.

#### **Local software installation and the write filter**

When you manually install K2 client software at the local K2 Summit Production Client or K2 Solo Media Server, the installation program helps you manage the write filter. Both the uninstall program and the install program have the same behavior. When you run either the uninstall or the install program, the program behaves as follows:

- If the write filter is enabled, the program notifies you and sets the write filter to disabled, then prompts you to restart. To continue the uninstall or install process, you must restart and then run the program again, this time with the write filter disabled.
- If the write filter is disabled, the program sets it to be enabled so that after next restart the K2 system starts up with the write filter enabled.

In this way the write filter is disabled while software is installed. Changes made to system settings or to the system drive before the restart following an install are preserved.

Once you have uninstalled or installed K2 Client software, at the next restart the write filter is enabled. If you want to keep the write filter disabled after an install, run the Write Filter Utility and disable the write filter before restarting.

#### **SiteConfig software installation and the write filter**

When you use SiteConfig to install K2 client software on a K2 Summit Production Client or K2 Solo Media Server, SiteConfig helps you manage the write filter. The SiteConfig "Lock" feature enables the write filter and the "Unlock" feature disables the write filter. In addition, both uninstall deployment tasks and install deployment tasks behave the same way in how they manage the write filter, as follows:

- If the write filter is enabled (the K2 system is locked), SiteConfig does not allow the task to be deployed. To deploy software, you must first disable (unlock) the write filter on the K2 system.
- If the write filter is disabled (the K2 system is unlocked), when the deployment task completes SiteConfig keeps the write filter disabled. If you then restart the K2 system, the write filter is still disabled after the restart. This allows you to deploy additional software.

When you are finished deploying software, use SiteConfig to enable (lock) the write filter on the K2 system.

## Disable write filter

Prerequisite:

- K2 software must be installed on the K2 Summit/Solo system.
1. If you have not already done so, log on to the K2 Summit/Solo system with Windows administrator privileges.
  2. From the Windows desktop, click **Start | All Programs | Grass Valley | Write Filter Utility**.  
FBWF Manager opens.
  3. Under Filter Settings, set Filter to **Disable**.  
Do not modify other settings.
  4. Click **OK**.
  5. When prompted, restart the K2 system.

## Enable write filter

Prerequisite:

- K2 software must be installed on the K2 Summit/Solo system.
1. If you have not already done so, log on to the K2 Summit/Solo system with Windows administrator privileges.
  2. From the Windows desktop, click **Start | All Programs | Grass Valley | Write Filter Utility**.  
FBWF Manager opens.
  3. Under Filter Settings, set Filter to **Enable**.
  4. Under Protected Volumes, set C: to **Protected**.  
Do not modify other settings.
  5. Click **OK**.
  6. When prompted, restart the K2 system.

## K2 Summit/Solo formats

Formats are supported as in the following table.

Formats	K2 Summit/Solo	K2 Summit 3G
DVCPRO 25/50	Standard	Standard
DVCPRO HD	Requires HD license	HD license is standard

<b>Formats</b>	<b>K2 Summit/Solo</b>	<b>K2 Summit 3G</b>
MPEG-2	Decode is standard	Encode/decode is standard
	Encode requires codec option card	Multi-Cam requires codec option card
	HD requires HD license	3D/Video + Key requires codec option card HD license is standard
AVC-Intra	Requires HD license	Requires AVC license
	Requires codec option card	HD license is standard
AVCHD	Not supported	Decode only
		Requires AVC license

## **Installing and configuring support for Windows 7 generic iSCSI clients**

With the Windows 7 operating system, additional steps are required for generic iSCSI clients, to support configuration via SiteConfig and K2Config. The system requirement for .NET is version 4.0 update KB2468871. The complete procedure is as follows:

1. On the PC that hosts the SiteConfig application, navigate to the directory at which SiteConfig is installed.  
By default the location is *C:\Program Files\Grass Valley\SiteConfig*.
2. Copy the contents of the *ConnectivityKit* directory and the *DiscoveryAgent Setup* directory to a USB thumb drive, network drive, or some other shared location to make it easier to distribute to each PC.

3. To install and configure SiteConfig support locally at a control network PC, do the following:
  - a) Copy the contents of the *ConnectivityKit* directory and the *DiscoveryAgent Setup* directory to the control network PC.
  - b) On the control network PC, check the Microsoft .NET Framework version and compare to system requirements for the software you intend to deploy with SiteConfig.
  - c) If necessary, install .NET software and the required Windows update.  
You can find the installation file for a .NET version in the *ConnectivityKit* directory.
  - d) On the control network PC, run `\DiscoveryAgent Setup\setup.exe`.  
The install wizard opens.
  - e) Work through the install wizard and when prompted to select the device type, select **GenericDevice**.
  - f) Finish the install wizard.
  - g) Open firewall port settings on the PC as follows.

<b>137</b>	UDP: Used by SiteConfig. File and printer sharing.
<b>138</b>	UDP: Used by SiteConfig. File and printer sharing.
<b>139</b>	TCP: Used by SiteConfig. File and printer sharing.
<b>445</b>	TCP: Used by SDB and XMOS Server and NAS. Used by SiteConfig. File and printer sharing.
<b>3389</b>	TCP: Used by Remote Desktop for use by SiteConfig.
<b>18262</b>	TCP: Used by GV ProductFrame Configuration Service, ProductFrame Discovery Agent Service for use by SiteConfig. Used by GV NetConfig Service. gv-pf. UDP: Used by GV NetConfig Service. gv-pf.
<b>18263</b>	UDP: Used by ProductFrame Discovery Agent Service for GV NetConfig Device Broadcast/Unicast Protocol. Used by SiteConfig. Sent by ControlPoint, received by Devices
<b>18264</b>	UDP: Used by ProductFrame Discovery Agent Service for GV NetConfig Controller Protocol. Used by SiteConfig. Sent by Devices, received by ControlPoint
<b>49168</b>	HTTP: Used by Grass Valley K2 Config for K2Config application connection between a control point PC and the K2 system device configured. Used for most functions.
<b>49169</b>	TCP: Used by Grass Valley K2 Config for K2Config application connection between a control point PC and the K2 system device configured. Used for a few functions that require longer time periods.

When you run `\Connectivity Kit\setup.exe` it attempts to configure the Windows firewall, but because firewalls vary on different systems, you must verify and configure the PC's firewall.

- h) Run the following at the Windows operating system command line:

```
netsh int ipv4 set dynamicport tcp start=52152 num=13383
netsh int ipv4 set dynamicport udp start=52152 num=13383
```

- i) Check system requirements for .NET software and if necessary install the required Windows update.
- j) Restart the control network PC.

## **Extent Manager for K2 SANs**

Extent Manager is a service that reclaims hard drive disc space that might be lost by the creation of proxy media files. It runs automatically on standalone K2 Summit systems. You must run it manually on your online or production K2 SAN system if you store proxy media files in the same storage (on the V: drive) as your high-resolution media files.

You should run Extent Manager periodically as instructed below during times when system performance is not critical, such as while the system is off the air. To see how many proxy files are in queue to be operated on by the Extent Manager service, look in the default proxy location `v:\proxy\journal\`. Each journal file in that location represents a proxy file in the queue. A large number of files indicates that you should run Extent Manager.

1. Open the Windows **Services** Control Panel.
2. Start the **Grass Valley Extent Manager Service**.  
A message notifies you that the service started successfully.
3. Monitor progress by observing files in `v:\proxy\journal\`. A decreasing number of files indicates the service is working. You can estimate 4 minutes per 1000 files.
4. If desired, you can safely stop and start Extent Manager at any time, using the Windows **Services** Control Panel.
5. When the journal folder is empty or contains only a few files, the Extent Manager process is complete.

---

# Operation considerations

- If you have problems using SiteConfig to discover a Windows Server 2008 K2 Media Server, make sure the server has an IP address. SiteConfig cannot discover Windows Server 2008 systems that do not have an IP address, such as those configured for DHCP.
- When installing MPIO on a 64-bit K2 Media Server (required only for a redundant nearline SAN), the file name is *gdsminstall64.exe*.
- Do not neglect to make a “first birthday” image of each K2 product shortly after installation and configuration is complete.
- Changing system video standards (NTSC/PAL) requires a restart as part of the channel changes as soon as the new standard is selected. Configuration Manager causes an immediate restart of the K2 client if the system reference standard is changed and AppCenter is being used.
- Refer to the “Remote control protocols” appendix in the *K2 System Guide* for operation considerations related to AMP, VDCP, BVW, Harris, RS-422, etc.
- To import/export between systems using AppCenter, in Configuration Manager on the Remote tab, add each system that you want to have available as a source or a destination. Do this for K2 systems as well as non-K2 systems, such as Profile XP.
- When transferring between K2 systems and other types of systems, such as Profile XP, you must specify the IP address, path, and file name to initiate a transfer.
- Constrain media names and filepaths for support across systems. While AppCenter allows you to create bin names and clip names longer than 32 characters, names of this length are not supported on all products.
- Before configuring audio tracks on a channel, eject all clips. This is required to put changes into effect.
- K2 Summit/Solo systems and K2 Media Servers can operate continuously for a long period of time, but the recommended operational practice is to restart at least once every three to six months.
- Mix effects (an AppCenter Pro feature) are not supported between different compression formats.
- A 3D/Video+Key player channel does not support agile playback or transition (mix) effects.
- A 3D/Video+Key player channel does not support a two-head player model.
- A 3D/Video+Key player channel does not support offspeed play greater than 1 or less than -1. During these offspeed play operations the video is not synchronized between the two video tracks. However, both video outputs will resync when recued.
- On a K2 Solo Media Server, before making a new file system, first upgrade drive firmware to the latest version, as specified in *Compatible K2 Summit/Solo components* on page 19. Failure to do so generates a Storage Utility error.
- Grass Valley recommends that you use a frame synchronizer on incoming video sources that are recorded in AVC-Intra format.
- If Dyno PA connects to an internal storage first generation K2 Summit system, there are special requirements for media disk labels. Refer to the *Dyno Production Assistant Configuration Manual*.
- When configuring editors on a K2 SAN with 1 Gig TOEs, do not assign editors and K2 clients (K2 Summit or K2 Media Client) to the same TOE. Instead, assign editors to their own TOE.
- To export AVI format files to a shared CIFS drive, first export to the local disk, then copy the file to the share.
- A K2 10G RAID controller connected to a Fibre Channel switch must have its "Link Attach" parameter set to "Point-to-Point". A K2 10G RAID controller connected directly to a K2 Summit system must have its "Link Attach" parameter set to "LOOP". When you purchase your K2 10G RAID system from Grass Valley, it comes configured correctly for your intended use. If you re-use a K2 10G RAID system and change the way it is connected, contact Grass Valley for instructions to change the Fiber Channel port configuration.

- A best practice is to check the K2 Summit log weekly to monitor the database size. Every 15 minutes the K2 Summit system reports a "Completed database backup..." message that includes the database size. If the size exceeds 50 MB, reduce the number of markers and/or the amount of metadata in clips.
- If you have a first generation K2 Summit system with a Type II (ADLINK) CPU carrier module or a 3G codec, consult "K2 Summit 3G Production Client Service Manual" when doing any service work or replacing any Field Replaceable Units (FRUs). This is true even if replacing an original FRU that has not been upgraded. System dependencies involving FRUs require procedures found only in "K2 Summit 3G Production Client Service Manual".
- It is not recommended to use 720p tri-level sync for interlace output formats (such as SD and 1080i) Output timing can be off by a field.
- You can configure internal media drives as RAID 0, RAID 1, or RAID 10 in a K2 Summit 3G system. The "K2 Summit 3G Production Client Service Manual" contains procedures for RAID 1 only. Adapt these procedures for RAID 0 and RAID 10.

---

# Version compatibility

Versions qualified for compatibility with this version 8.1 release of K2 software are summarized in the following sections.

## Compatible K2 Summit/Solo components

The following components are part of K2 Summit Production Client, K2 Solo Media Server, or K2 Summit Transmission Client/Server products. Components are compatible with this release of K2 software as listed in the following table. Compatible versions are pre-installed on the K2 system when you receive it new from Grass Valley. For microcode and firmware filenames, refer to tables later in this section.

### Component versions

Component	Version	Comments
GrassValley K2 Client software	8.1.10	Includes AppCenter
Media File System (SNFS)	3.5.3.b27171	—
SiteConfig Discovery Agent, also known as SiteConfig Network Configuration Connect Kit	2.0.0.195 and higher	A minimum version of 1.0.8 is required to support device discovery. Then when you deploy software to the device, the SiteConfig application prompts you to upgrade to the correct version of the Discovery Agent on the device.
Windows Operating System	Windows XP embedded 2002 SP3	—
Windows update	2.0.50727.4022	—
Microsoft .NET Framework	2.0 SP2, 3.0 SP2, 3.5 SP1, 4.0	—
QuickTime	7.6 and higher	—
Intel Network Connections	13.3	—
Microsoft iSCSI Initiator	2.08	—
MS XML	4.0 SP2, 6.0	—
MegaRAID Storage Manager (internal storage only)	v2.91-05	—
RAID controller microcode (internal storage only)	1.40.242-1083 or 1.40.322-1445	Both version are compatible. Upgrade to one of these versions is required.
RAID disk drive firmware Hitachi ViperB drives	570	First generation Summit internal storage only
RAID disk drive firmware Hitachi ViperC drives	510	First generation Summit internal storage only

Component	Version	Comments
RAID disk drive firmware Hitachi CobraD drives	360	Summit 3G and Solo internal storage only. 10K
RAID disk drive firmware 7.2K SAS drives	N004	Summit Transmission storage only. This version is still compatible.
	N104	Summit Transmission storage only. This is the currently shipping version. Upgrade is not required and not recommended.
	N002	Summit Transmission storage only. Muskie Plus (+)
RAID disk drive firmware	4101	Solo internal storage only
RAID disk drive firmware	2269	Solid State drives. Solo internal storage only
LSI RAID controller driver	3.10.0.32	Internal storage only. First generation Summit.
LSI RAID controller driver	4.33.0.32	Internal storage only. Summit 3G.
LSI Adaptor 4GbFC driver Models 7104,7204, 7404W, 949X	1.26.1.0	—

#### K2 Summit Production Client internal storage RAID controller microcode file names

Find files at *C:\profile\microcode\Internal Storage\LSI Controller*.

Version	Microcode file
1.40.52-0629	SAS1078_FW_Image_1.40.52.0629.rom
1.40.242-1083	SAS1078_FW_1.40.242.1083.rom

#### First generation K2 Summit Production Client internal storage drive firmware file names

Find files at *C:\profile\microcode\Internal Storage\Hitachi*.

Drive type	Drive size	Storage Utility Identifier	Version	Firmware file
ViperB	300GB	HUS154530VLS300	570	HITACHI_ViperB_15K_A570.bin
	450GB	HUS154545VLS300	570	HITACHI_ViperB_15K_A570.bin
ViperC	300GB	HUS156030VLS600	510	HITACHI_ViperC_15K_A510.bin
	450GB	HUS156045VLS600	510	HITACHI_ViperC_15K_A510.bin
	600GB	HUS156060VLS600	510	HITACHI_ViperC_15K_A510.bin

#### K2 Summit 3G Production Client internal storage drive firmware file names

Find files at *C:\profile\microcode\Internal Storage\Hitachi*.

Drive type	Drive size	Storage Utility Identifier	Version	Firmware file
CobraD	600GB	HUC106060CSS600	360	HITACHI_CobraD_10K_A360.bin

### K2 Solo Media Server drive firmware file names

Find files at *C:\profile\microcode\Internal Storage\Hitachi*.

Drive type	Drive size	Storage Utility Identifier	Version	Firmware file
CobraD	300GB	HUC106030CSS600	360	HITACHI_CobraD_10K_A360.bin

Find files at *C:\profile\microcode\Internal Storage\Fujitsu*.

Drive size	Storage Utility Identifier	Version	Firmware file
136GB	MBE2147RC	4101	FUJITSU_15K_25_4101.frm

### K2 Summit Transmission internal storage 7.2K SAS Muskie drives

Find files at *C:\profile\microcode\External Storage\K2\_L10-L40 Condor\Drive\7.2K\Muskie*.

Disk Drive	Storage Utility Identifier	Firmware Version	Firmware file
500G	ST3500414SS	N004	MU_7K_SAS_1T_500G_N004.bin
		N104	MU_7K_SAS_1T_500G_N104.bin
1TB	ST31000424SS	N004	MU_7K_SAS_1T_500G_N004.bin
		N104	MU_7K_SAS_1T_500G_N104.bin
2TB	ST32000444SS	N004	MU_7K_SAS_2T_N004.bin
		N104	MU_7K_SAS_2T_N104.bin

### K2 Summit Transmission internal storage 7.2K SAS Muskie+ drives

Find files at *C:\profile\microcode\External Storage\K2\_L10-L40 Condor\Drive\7.2K\Muskie+*.

Disk Drive	Storage Utility Identifier	Firmware Version	Firmware file
500G	ST500NM0001	N002	MUP_7K_SAS_500G_N002.bin
500G and 1TB	ST1000NM0001	N002	MUP_7K_SAS_1T_N002.bin. Available via FTP download.
2TB	ST2000NM0001	N002	MUP_7K_SAS_2T_N002.bin

## Compatible K2 Media Server components

The following components reside on the K2 Media Server and are compatible with this release of K2 software as listed in the following table. Compatible versions are pre-installed on the K2 Media Server when you receive it new from Grass Valley.

Component	Version	Comments
Grass Valley K2 Server software	8.1.10	—
Media File System (SNFS)	3.5.3.b27171	—
SiteConfig Discovery Agent, also known as SiteConfig Network Configuration Connect Kit	2.0.0.195 and higher with Windows 2008 Server	This version required for device discovery on systems with the Microsoft® Windows® Server 2008 operating system
	2.0.0.195 and higher with Windows 2003 Server	A minimum version of 1.0.8 is required to support device discovery on systems with the Microsoft® Windows® Server 2003 operating system. Then when you deploy software to the device, the SiteConfig application prompts you to upgrade to the correct version of the Discovery Agent on the device.
Windows Operating System	Windows 2003 Server	With the latest update
	Windows 2008 Server	With the latest update
Windows update	2.0.50727.4022	—
Microsoft .NET Framework	2.0 SP2, 3.0 SP2, 3.5 SP1, 4.0	—
QuickTime	7.6 and higher	—
Adobe Acrobat Reader	7.0 and higher	—
ATI Display Driver	8.24.3.0	—
Dell OpenManage	6.5.0	—
J2SE Runtime Environment	6, Update 3	—
MSXML	4.0 and higher	—
Dell Server Models	R610, 2950, 1950	As provided by Grass Valley for specific K2 storage levels and applications.
LSI Adaptor 4GbFC driver Models 7104,7204, 7404W, 949X	1.25.7.0	—
Broadcom driver	7.0.11.0	—

## Compatible K2 Control Point PC components

The following components reside on the K2 Control Point PC and are compatible with this release of K2 software as listed in the following table. Compatible versions are pre-installed on the K2 Control Point PC when you receive it new from Grass Valley.

Software	Version	Comments
K2 control point	8.1.10	—
Windows operating system	Server 2003 SP 1	—
Windows update	2.0.50727.4022	—
NetCentral	5.2.0.25	Check with your Grass Valley representative for the specific version.
SQL Server Express	2005	—
.NET Framework	1.1, 1.1 Hotfix, 2.0 SP2, 3.0 SP2, 3.5 SP1, Version 4.0 update KB2468871	—
QuickTime	7.6 and higher	—
MS XML	4.0	—
Windows Installer	3.1	—
SiteConfig application	2.1.1.516 and higher	Upgrade to this version before deploying software to any devices.
SiteConfig Discovery Agent, also known as SiteConfig Network Configuration Connect Kit	2.0.0.195 and higher	A minimum version of 1.0.8 is required to support device discovery. Then when you deploy software to the device, the SiteConfig application prompts you to upgrade to the correct version of the Discovery Agent on the device.
7-ZIP	—	—
Adobe Reader	9.0	—

## Compatible HP ProCurve GigE switch components

Components that reside on the HP ProCurve 3400cl series GigE switch and the HP ProCurve 29xx series GigE switch are compatible with this release of K2 software as follows:

Product	Version	Comments
HP ProCurve 2910al series firmware	W_14_30	This is the only version available on this model of switch.
HP ProCurve 2900 series firmware	T.11.12	This older version is no longer recommended.

Product	Version	Comments
	T.13.23	Upgrade to this version is required. After upgrade, configure QOS settings.
HP ProCurve 3400cl series firmware	M.08.66	This older version is still compatible
	M.08.86	Upgrade to this version is recommended

**Related Topics**

[Upgrading firmware on HP switch](#)

[Configuring QOS on the GigE switch](#)

[Verify/upgrade switch firmware](#) on page 45

## Compatible K2 RAID components

This compatibility specification applies to K2 Lx0 RAID (Condor with 4 Gig controllers) and K2 10G RAID (Condor with 8 Gig controllers) on a K2 SAN, both basic and redundant. RAID firmware is compatible with this release of K2 software as follows:

Find firmware on the K2 client (for direct-connect storage) or the K2 Media Server (for shared storage) at `C:\profile\microcode\External Storage\K2_L10-L40 Condor\Controller`.

Component	Version	File Name	Comments
Level 10/20 controller firmware for primary chassis with 15K SAS drives or SATA drives	07VS	D1_07VS.BIN	This version is still compatible for 300 and 450 GB drives
	07VV	D1_07VV.BIN	This version is still compatible for 300 and 450 GB drives
	07VW	D1_07VW.BIN	This version required for 600 GB drives, recommended for 300 and 450 GB drives. Requires version 050B for expansion chassis.
Level 10/20 controller firmware for expansion chassis with 15K SAS drives or SATA drives	030F	ENCL_030F.BIN	This version is still compatible for 300 and 450 GB drives with 07VS or 07VV controller firmware.
	050B	ENCL_050B.BIN	This version is compatible for 300 and 450 GB with 07VS, 07VV, or 07VW controller firmware. Required for 600 GB drives with 07VW controller firmware.
Level 10/20 controller firmware for primary chassis with 7.2K SAS drives	07VV	D1_07VV.BIN	7.2K SAS drives are used in K2 Production Storage and K2 Nearline Storage.
Level 10/20 controller firmware for expansion chassis with 7.2K SAS drives	050B	ENCL_050B.BIN	

Component	Version	File Name	Comments
Level 30/35 controller firmware for primary chassis with 15K SAS drives or SATA drives	07VS	D3_07VS.BIN	This version is still compatible for 300 and 450 GB drives
	07VV	D3_07VV.BIN	This version is still compatible for 300 and 450 GB drives
	07VW	D3_07VW.BIN	This version required for 600 GB drives, recommended for 300 and 450 GB drives. Requires 050B for expansion chassis.
Level 30/35 controller firmware for expansion chassis with 15K SAS drives or SATA drives	030F	ENCL_030F.BIN	This version is still compatible for 300 and 450 GB drives with 07VS or 07VV controller firmware.
	050B	ENCL_050B.BIN	This version is compatible for 300 and 450 GB with 07VS, 07VV, or 07VW controller firmware. Required for 600 GB drives with 07VW controller firmware.
Level 30/35 controller firmware for primary chassis with 7.2K SAS drives	07VV	D3_07VV.BIN	7.2K SAS drives are used in K2 Production Storage and K2 Nearline Storage.
Level 30/35 controller firmware for expansion chassis with 7.2K SAS drives	050B	ENCL_050B.BIN	
10G controller firmware for primary chassis with either 7.2K or 15K drives	01VP	D4_01VP.BIN	—
10G controller firmware for primary chassis with either 7.2K or 15K drives	01VR	D4_01VR.BIN	Upgrade to this version is recommended but not required. Supports NetCentral/SNMP monitoring.
10G controller firmware for expansion chassis with either 7.2K or 15K drives	020F	ENCL_020F.BIN	—

## Compatible K2 RAID disk drive firmware

This compatibility specification applies to K2 Lx0 RAID (Condor with 4 Gig controllers) and K2 10G RAID (Condor with 8 Gig controllers) on a K2 SAN, both basic and redundant.

Be aware that Storage Utility can report inconsistent disk drive firmware versions. This can be a normal condition, since the RAID system supports multiple drive capacities and firmware versions. Be sure to compare the version numbers with this table, and update only as required.

Disk drive firmware is compatible with this release of K2 software as summarized in the following tables:

**15K SAS Cheetah 5 drives with 4G controllers compatible versions**

Find files for these versions at *C:\profile\microcode\External Storage\K2\_L10-L40 Condor\Drive\15K\Cheetah 5*. Refer to "Firmware file names" below to identify files.

Disk Drive	Storage Utility Identifier	Firmware Version	Comments
73G	ST373685SS	0002	—
146G	ST3146685SS	0002	—
300G	ST3300655SS	0002	—

**15K SAS Cheetah 6 drives with 4G controllers compatible versions**

Find files for these versions at *C:\profile\microcode\External Storage\K2\_L10-L40 Condor\Drive\15K\Cheetah 6*. Refer to "Firmware file names" below to identify files.

Disk Drive	Storage Utility Identifier	Firmware Version	Comments
146G	ST3146356SS	0004	This version is still compatible
		N005	This is the currently shipping version. Upgrade is recommended but not required.
300G	ST3300656SS	0004	This version is still compatible
		N005	This is the currently shipping version. Upgrade is recommended but not required.
450G	ST3450856SS	0004	This version is still compatible
		N005	This is the currently shipping version. Upgrade is recommended but not required.

**15K SAS Cheetah 7 drives with 4G controllers compatible versions**

Find files for these versions at *C:\profile\microcode\External Storage\K2\_L10-L40 Condor\Drive\15K\Cheetah 7*, except for N005<sup>1</sup> versions. The files for these N005 versions are removed from *C:\profile\microcode\...* directories when you upgrade your K2 software. Refer to "Firmware file names" below to identify files.

Disk Drive	Storage Utility Identifier	Firmware Version	Comments
300G	ST3300657SS	N005	N005 is compatible with 4G controllers only. Not compatible with 8G controllers.

---

<sup>1</sup> Do not use file CH\_15K7\_SAS.N005 for any drive

Disk Drive	Storage Utility Identifier	Firmware Version	Comments
		N006	This is the currently shipping version and is compatible with 4G controllers. Upgrade is recommended. If you must load disk firmware, load version N006.
450G	ST3450857SS	N005	N005 is compatible with 4G controllers only. Not compatible with 8G controllers.
		N006	This is the currently shipping version and is compatible with both 4G and 8G controllers. Upgrade is recommended. If you must load disk firmware, load version N006.
600G	ST3600057SS	N005	N005 is compatible with 4G controllers only. Not compatible with 8G controllers.
		N006	This is the currently shipping version and is compatible with both 4G and 8G controllers. Upgrade is recommended. If you must load disk firmware, load version N006.

#### 15K SAS Cheetah 7 drives with 8G controllers compatible versions

Find files for these versions at *C:\profile\microcode\External Storage\K2\_L10-L40 Condor\Drive\15K\Cheetah 7*. Refer to "Firmware file names" below to identify files.

Disk Drive	Storage Utility Identifier	Firmware Version	Comments
450G	ST3450857SS	N006	This is the currently shipping version and is compatible with both 4G and 8G controllers.
600G	ST3600057SS	N006	This is the currently shipping version and is compatible with both 4G and 8G controllers.

#### 7.2K SAS drives with 4G controllers compatible versions

Find files for these versions at *C:\profile\microcode\External Storage\K2\_L10-L40 Condor\Drive\7.2K*. Refer to "Firmware file names" below to identify files.

Disk Drive	Storage Utility Identifier	Firmware Version	Comments
500G	ST3500620SS	N001	—
1TB	ST31000640SS	N001	—

### 7.2K SAS Muskie drives with 8G controllers compatible versions

Find files for these versions at *C:\profile\microcode\External Storage\K2\_L10-L40 Condor\Drive\7.2K\Muskie*. Refer to "Firmware file names" below to identify files.

Disk Drive	Storage Utility Identifier	Firmware Version	Comments
500G	ST3500414SS	N004	This version is still compatible. Upgrade is not required and not recommended, because upgrading bound disks takes a very long time, degrades performance, and puts the file system at risk if a disk fails.
		N104	
2TB	ST32000444SS	N004	
		N104	

### 7.2K SAS Muskie+ drives with 8G controllers compatible versions

Find files for these versions at *C:\profile\microcode\External Storage\K2\_L10-L40 Condor\Drive\7.2K\Muskie+*. Refer to "Firmware file names" below to identify files.

Disk Drive	Storage Utility Identifier	Firmware Version	Comments
500G	ST500NM0001	N002	This is the currently shipping version.
500G and 1TB	ST1000NM0001	N002	
2TB	ST2000NM0001	N002	

### Firmware file names

Disk Drive	Firmware Version	Firmware Type	Firmware File Name
Cheetah 5 15K SAS 73G	0002	Interface	CT15K5SAS.01_
		Servo	CT15K5SAS_73._1
Cheetah 5 15K SAS 146G	0002	Interface	CT15K5SAS.01_
		Servo	CT15K5SAS_146._1
Cheetah 5 15K SAS 300G	0002	Interface	CT15K5SAS.01_
		Servo	CT15K5SAS_300._1
Cheetah 6 15K SAS 146G	0004	Interface/Servo	CH_15K6_SAS.N004
	N005	Interface/Servo	CH_15K6_SAS.N005
Cheetah 6 15K SAS 300G	0004	Interface/Servo	CH_15K6_SAS.N004
	N005	Interface/Servo	CH_15K6_SAS.N005
Cheetah 6 15K SAS 450G	0004	Interface/Servo	CH_15K6_SAS.N004
	N005	Interface/Servo	CH_15K6_SAS.N005
Cheetah 7 15K SAS 300G	N006	Interface/Servo	CH_15K7_SAS_300G_N006.bin

Disk Drive	Firmware Version	Firmware Type	Firmware File Name
Cheetah 7 15K SAS 450G	N006	Interface/Servo	CH_15K7_SAS_450G_N006.bin
Cheetah 7 15K SAS 600G	N006	Interface/Servo	CH_15K7_SAS_600G_N006.bin
7.2K SAS 500G	N001	Interface	BA_7K_Interface.N001
		Servo	BA_7K_ST3500620SS_Servo.C30D
7.2K SAS 1TB	N001	Interface	BA_7K_Interface.N001
		Servo	BA_7K_ST31000640SS_Servo.B30D
7.2K SAS 500G Muskie	N004	Interface/Servo	MU_7K_SAS_1T_500G_N004.bin
	N104	Interface/Servo	MU_7K_SAS_1T_500G_N104.bin
7.2K SAS 2TB Muskie	N004	Interface/Servo	MU_7K_SAS_2T_N004.bin
	N104	Interface/Servo	MU_7K_SAS_2T_N104.bin
7.2K SAS 500G Muskie+	N002	Interface/Servo	MUP_7K_SAS_500G_N002.bin
7.2K SAS 500G/1TB Muskie+	N002	Interface/Servo	MUP_7K_SAS_1T_N002.bin. Available via FTP download.
7.2K SAS 2TB Muskie+	N002	Interface/Servo	MUP_7K_SAS_2T_N002.bin

## Compatible Grass Valley products

Grass Valley products are compatible with this version 8.1.10 release of K2 software as follows:

Product	Version	Comments
STRATUS	2.5	—
K2 Dyno Replay Controller	2.0.3 and higher	—
K2 Dyno PA	2.0.2	—
Aurora Browse	Not supported	The STRATUS product now provides this functionality.
Aurora Suite	Not supported	
Aurora Ingest	Not supported	
Aurora Payout	8.0.0.9	—
Profile XP Media Platform	5.4.8 or higher	Media assets can be transferred to/from a Profile XP system but cannot be browsed.
NetCentral	5.2.0.25 and higher	—
SiteConfig application	2.1.1.516 and higher	—
UIM	2.1.1	—
K2 TimeDelay	8.1.0.19	—

---

## Version compatibility

Product	Version	Comments
K2 InSync	4.0.3.15	Check with your Grass Valley representative for version availability
K2-AvidTM	7.0.0.128	Interplay Transfer Engine 2.4 NewsCutter 9.0.4 Media Composer 5.5.2 Omnibus Driver version 0.10.0.15 for software version 0.0.0.7 Contact Grass Valley Support for additional information and version availability. On the Avid Editor install the <i>K2AvidIngest</i> module and on the device that runs the Avid Transfer Manager/Interplay Engine install the <i>K2AvidDhm</i> module.
K2 FCP Connect	2.0	—
Grass Valley LDK8300 Super SloMo Camera	—	3x and 2x frame rates supported. Requires AppCenter Elite license.
Grass Valley LDK8000 SportElite HD Super SloMo Camera	—	2x frame rate. Requires AppCenter Elite license.
Sony 3300 Super SloMo Camera	—	3x frame rate only; 2x is not supported. Requires AppCenter Elite license.
Edius	6.06	—
Kayenne/Karrera	4.1.0	Check with your Grass Valley representative for version availability.

## Compatible recovery applications

To create a recovery image of a K2 device, use compatible versions of the recovery application, as follows:

<b>Product</b>	<b>Recovery application and version</b>	<b>Comments</b>
K2 Summit Production Client	Recovery Flash Drive part number 86205900	Use the Recovery Flash Drive that you received with the product. It is identified with the product's serial number and is to be used on that specific K2 Summit Production Client only.
K2 Media Server	Recovery CD part number 063-8246-04	—
Grass Valley Control Point PC	Recovery CD part number 063-8246-04	—

---

# Upgrading K2 systems

This section contains the tasks necessary for a software-only upgrade on standalone and SAN K2 systems.

The following are supported for software-only upgrade:

- Upgrading K2 Summit 3G systems
- Upgrading first generation K2 Summit systems currently at a 8.x version to a higher version

The following are not supported for software-only upgrade:

- Upgrading first generation K2 Summit systems currently at a 7.x version to a 8.x version
- Upgrading first generation K2 Summit systems to the Type II CPU carrier module and/or the 3G Codec

For these upgrades you must procure and follow instructions in one of the following K2 Summit Field Kits:

- K2-XDP-V8x-FK — Upgrades a system with a Type I (Kontron) CPU carrier module currently at a software version lower than 8.0 to software version 8.x.
- K2-XDP-CPU-FK — Upgrades a system with a Type I (Kontron) CPU carrier module to the Type II (ADLINK) CPU carrier module and software version 8.x.
- K2-XDP-3G1-FK — Upgrades a system with a Type I (Kontron) CPU carrier module to the Type II (ADLINK) CPU carrier module, 3G codec module, and software version 8.x.
- K2-XDP-3G2-FK — Upgrades a system with a Type II (ADLINK) CPU carrier module and first-generation codec module to the 3G codec module and software version 8.x.

K2 software downgrade is supported only via the recovery image process. If you must downgrade and you do not have a recovery image at the desired software version, obtain a recovery image from Grass Valley Support.

## Upgrading a K2 SAN

This section contains the tasks necessary to upgrade a K2 SAN to this release of K2 software. Work through the tasks sequentially to complete the upgrade.

***NOTE: These upgrade instructions assume that on your SAN-attached K2 Summit systems, the current K2 software is at version 8.x or higher. If the current K2 software is at a version lower than 8.x, you must upgrade K2 Summit systems using the appropriate Grass Valley Field Kit, which includes a disk image and hardware. Once upgraded via the field kit to an 8.x version, you can then use these upgrade instructions.***

## About upgrading the K2 SAN with SiteConfig

This section provides instructions to upgrade the following K2 SAN devices:

- K2 Media Servers
- K2 Summit Production Clients

With these upgrade instructions, you use SiteConfig from a network connected control point PC and remotely upgrade software simultaneously on multiple K2 devices. This is the required process for software upgrades. Do not upgrade software on a K2 SAN locally at each device or via any other process.

If this is the first time using SiteConfig for software upgrade, follow instructions in *K2 SAN Installation and Service Manual* rather than instruction in these release notes. You must first have SiteConfig set up for system management and software deployment of the K2 SAN. Also refer to the *SiteConfig User Manual* or *SiteConfig Help Topics*. Then, after you have completed this initial SiteConfig set up, you can follow the instructions in this section to upgrade software.

**NOTE:** *If this is the first time using SiteConfig for software upgrade do not follow instructions in these release notes alone.*

**NOTE:** *Do not attempt to upgrade software incrementally across the devices of a K2 SAN while media access is underway. Online software upgrading is not supported.*

The following installation tasks provide information specifically for the upgrade to this 8.1 version of software. Read the information in these sections carefully before attempting any upgrade to software on any of the devices of a K2 SAN, including K2 systems, Aurora Edit systems, or other clients.

## Make recovery images

Do not do this task if:

- You previously made a recovery image at the current software version for each computer you are upgrading.

Do this task if:

- You do not have a recovery image at the current software version for one or more of the computers you are upgrading.

The recommended procedure is to make a recovery image immediately after a software upgrade. If you neglected to do this when you last upgraded software you should make the recovery image now, before upgrading to the new version.

Refer to the Grass Valley product's *Service Manual* for recovery image procedures.

**⚠ CAUTION:** *If you upgrade and then decide you do not want to stay with this version of K2 system software, you must use the recovery disk image process to downgrade to your previous version.*

## Prepare SiteConfig for software deployment to K2 SAN devices

Do the following to prepare SiteConfig for the software upgrade.

1. Make the following files accessible to the SiteConfig control point PC:
  - K2 Summit Client SAN software installation (\*.cab) file.
  - K2 Media Server software installation (\*.cab) file. Use file with *x86* in filename for 32-bit systems and file with *x64* in filename for 64-bit systems.
  - SNFS software installation (\*.cab) file. Use file with *x86* in filename for 32-bit systems and file with *x64* in filename for 64-bit systems.
  - Summit SNFS software installation (\*.cab) file.
  - Control Point software installation (\*.cab) file.

2. On the K2 Media Server, check for the `C:\SNFS` directory and then proceed as follows:
  - If `C:\SNFS` exists on the K2 Media Server, then SNFS 3.5.1 is on the C: drive. In this case you must move SNFS to the D: drive. To do this you must procure the `35c235d.reg` file and use it as instructed with special tasks in the upgrade process below. The `35c235d.reg` file is on the version 8.1.x.xxxx K2 software CD in the SNFS directory. It can also be obtained at <http://www.grassvalley.com/downloads>.
  - If `C:\SNFS` does not exist on the K2 Media Server, continue with this procedure. No special tasks are required.
3. If a newer version of SiteConfig is available for upgrade and you have not yet upgraded SiteConfig, do the following:
  - a) From Windows Add/Remove programs, uninstall the current version of SiteConfig from the control point PC.
  - b) Install the new version of SiteConfig on the control point PC.
4. If not already present in the SiteConfig system description, configure deployment groups as follows:
  - A deployment group that contains your SAN K2 clients
  - A deployment group that contains your K2 Media Servers
  - A deployment group that contains your control point PC

## Deploy control point PC software

Use SiteConfig to upgrade control point software on the K2 control point PC. In most cases, the K2 control point PC is also the SiteConfig control point PC, so you are in effect using SiteConfig to upgrade software on its own local system.

For this release of K2 software, the install task identifies the control point software in the Managed Package column as follows:

- GrassValleyControlPoint 8.1.x.xxxx

The software deployment process for the control point PC is similar to that used to upgrade software on other K2 devices. Use similar procedures and adjust accordingly to do the following:

1. Add the K2 control point software package to the deployment group that contains the control point PC.
2. Check software on the control point PC.
3. Configure and run deployment tasks to upgrade software.

## Unlock K2 Summit Production Clients

This task disables the write filter on one or more K2 Summit Production Clients.

Prerequisites for this task are as follows:

- The device or all the devices in the group are communicating correctly in SiteConfig. This is indicated by the green star icon overlay.

- The device or all the devices in the group are currently locked. This is indicated by the gray lock icon overlay.
- 1. If you have not already done so, stop all media access on the K2 systems. This includes record, play, and transfer operations.
- 2. In either the **Network Configuration | Devices** tree view or the **Software Deployment | Deployment Groups** tree view, identify the device or the group of devices that you intend to unlock.
- 3. Right-click the device or the group and select **Unlock**.  
A "...may require restart..." message appears.
- 4. Click **Yes** to allow SiteConfig to restart the device or devices.  
The Set Administrative Credentials dialog box opens.
- 5. Enter a username and password with administrator level privileges on the device or devices and click **OK**.  
The Unlocking Devices window opens and displays progress.
- 6. When the Unlocking Devices window reports that the unlock process completed successfully, click **Close**.

The device or devices are now unlocked. For K2 Summit Production Clients, this also disables the write filter, which enforces a restart.

### Take SAN clients offline

When upgrading software on a K2 SAN, you upgrade software on K2 Media Servers before you upgrade software on the connected SAN clients. This includes K2 clients, K2 appliances, Aurora clients, and generic clients. While you are upgrading software on K2 Media Servers you must keep all connected client devices offline (all media access stopped) or shut down. Do not power up or start media access on connected devices until the upgrade on K2 Media Servers is complete and the media file system/database server is fully operational.

1. If you have not already done so, stop all media access on SAN clients. This includes all record, play, and transfer operations
2. For K2 Summit Production Clients, if you have not already done so, disable (unlock) the write filter.
3. Shutdown all the SAN K2 clients on the SAN. To do this in SiteConfig, right-click a client device in the tree view and select **Shutdown**.

Next upgrade K2 Media Servers. If you have multiple K2 Media Servers you must manage them properly for the upgrade process.

### Manage multiple K2 Media Servers

Do not do this task if:

- You are upgrading a K2 SAN with only one K2 Media Server. Skip ahead and begin upgrading your K2 Media Server.

Do this task if:

- You are upgrading a basic (non-redundant) K2 SAN with multiple servers. This means you have just one K2 Media Server that takes the role of media file system/database server and one or more other K2 Media Servers dedicated to other roles, such as FTP server.

- You are upgrading a redundant K2 SAN. This means you have two K2 Media Servers (primary and backup) that take the role of media file system/database server.

**NOTE: If the K2 SAN has multiple K2 Media Servers, you must upgrade all to the same version.**

**If you are upgrading a basic K2 SAN with multiple servers:**

1. Upgrade the server that takes the role of media file system/database server first.
2. After the media file system/database server is upgraded and when instructed to do so in a later task, upgrade your other servers.

**If you are upgrading a redundant K2 SAN:**

Use the following steps to manage primary/backup roles and upgrade your two media file system/database servers in the proper sequence. This avoids triggering a failover event.

1. Determine the current primary/backup roles of the servers. You can use Server Control Panel (via the K2 System Configuration application or on the local K2 Media Server) or NetCentral to make this determination.
2. Shut down the backup server.
3. Upgrade the primary server.
4. Continue with upgrade tasks on your two K2 Media Servers that take the role of media file system/database server. If you have additional servers, upgrade them later, when instructed to do so in a later task.

## Upgrade K2 Media Server

Prerequisites for the upgrade are as follows:

- From the SiteConfig control point PC, you must have access to the software installation files for this release.

### Install required Windows update

Do this task if:

- A K2 Media Server, Control Point PC, or K2 Coder with Windows update at a version lower than 2.0.50727.4022.

**NOTE: In addition to this required update, Grass Valley recommends that you also install "High Priority" updates.**

- If you are not sure of the Windows update version currently installed, do the following:
  - Navigate to `C:\Windows\Microsoft.NET\Framework\v2.0.50727`.
  - Check file properties. The following properties indicate that version 2.0.50727.4022 is already installed:

File name	File version	File size	Date	Time	Platform
mscordacwks.dll	2.0.50727.4022	989,000	11-Mar-2009	04:56	x86
mscorlib.dll	2.0.50727.4022	4,550,656	11-Mar-2009	04:56	x86
mscorwks.dll	2.0.50727.4022	5,812,544	11-Mar-2009	04:56	x86
sos.dll	2.0.50727.4022	388,936	11-Mar-2009	04:56	x86

- If your properties are different than those specified above, the update is necessary. This is true even if your version numbers are higher or your dates are later. Continue with this procedure.

**NOTE: You must update even if your version numbers are higher or your dates are later.**

- Access the upgrade files and double-click `NDP20SP2-KB968760-x86.exe`.  
The installation wizard opens.
- Work through the wizard, accepting all default settings, and finish.
- Restart as prompted.

### Install High Priority Windows updates (recommended)

- Windows "High Priority" updates are recommended, but not required. While you have devices in an offline state to upgrade software, you should check to see if there are any new updates that you need to install. Use standard Windows procedures.

**⚠ CAUTION: Only "High Priority Updates" should be installed. Do not install other Windows or driver updates unless specifically directed by product documentation or by Grass Valley Support.**

### Upgrade QuickTime

Do not do this task if:

- QuickTime is currently at version 7.6 or higher.

Do this task if:

- QuickTime is at a version lower than 7.6.
1. Access the QuickTime installation files.
  2. Locate and open the following QuickTime install file:

*QuickTimeInstaller-7.6.exe*

3. Work through the install wizard.

Configure settings so that the software does not automatically update Quicktime and other Apple software.

**NOTE: Unless instructed to do so by Grass Valley, do not update or install Apple software.**

Accept the default destination folder and other default settings.

### Configure GlobalSuperUser in SNFS default.cfg file on K2 Media Servers

In this task you open the media file system (SNFS) configuration file and verify/modify settings.

Do not do this task if:

- You have already modified the configuration file with the required settings.

Do this task if:

- The configuration file does not have the required settings.

Prerequisites for this task are as follows:

- K2 systems must be offline

You can verify and, if necessary, modify the media file system (SNFS) configuration file and still keep your media file system intact if you carefully follow the steps in this procedure.

As an alternative to manually modifying the configuration file, if you need to make a new file system after upgrading K2 software, the required values are set automatically by the upgraded version of Storage Utility.

This task applies to the following devices:

- K2 Media Servers with role of file system server. If a redundant SAN, you must do this task on both primary and backup K2 Media Server.

1. On a K2 Media Server, using Notepad, open the media file system (SNFS) configuration file:

The configuration file can be either *D:\SNFS\config\default.cfg*. or

*D:\SNFS\config\gvfs\_hostname.cfg*, where *hostname* is the name of the primary file system server (FSM).

2. On a K2 Media Server, verify, and if necessary modify, settings for required values as follows:

```
# *****
# A global section for defining file system-wide parameters
# *****
GlobalSuperUser Yes
.
.
.
.
.

InodeDeleteMax 1000

.

BufferCacheSize 64M
.
.
.
.
InodeCacheSize 32K
.
ReservedSpace No
```

3. Close, and if necessary save, the SNFS configuration file.

If you made changes, the K2 system must be restarted for the changes to take effect.

The restart later in this upgrade procedure is sufficient to put the changes into effect.

**Configure Macintosh access in SNFS configuration file on K2 Media Servers**

In this task you open the media file system (SNFS) configuration file and verify/modify settings.

Do not do this task if:

- The K2 SAN has no iSCSI or Fibre Channel connected Macintosh clients
- The K2 SAN has iSCSI connected or Fibre Channel connected Macintosh clients and Windows Security is configured to Yes on the SNFS file system.

Do this task if:

- The K2 SAN has iSCSI connected or Fibre Channel connected Macintosh clients and Windows Security is configured to No on the SNFS file system.

Prerequisites for this task are as follows:

- The Macintosh client connection requires K2 FCP Connect.
- The K2 SAN must be offline

You can verify and, if necessary, modify the media file system (SNFS) configuration file and still keep your media file system intact if you carefully follow the steps in this procedure.

This task applies to the following devices:

- K2 Media Servers with role of file system server. If a redundant SAN, you must do this task on both primary and backup K2 Media Server.

1. On a K2 Media Server, using Notepad, open the media file system (SNFS) configuration file:

The configuration file can be either `D:\SNFS\config\default.cfg`. or  
`D:\SNFS\config\gvfs_hostname.cfg`, where `hostname` is the name of the primary file system server (FSM).

2. On a K2 Media Server, verify, and if necessary modify, settings for required values as follows:

```
# *****  
# A global section for defining file system-wide parameters  
# *****  
.  
.  
WindowsSecurity No  
  
UnixDirectoryCreationModeOnWindows 0777  
UnixFileCreationModeOnWindows 0666
```

3. Close, and if necessary save, the SNFS configuration file.

If you made changes, the K2 system must be restarted for the changes to take effect.

The restart later in this upgrade procedure is sufficient to put the changes into effect.

If you made changes to `UnixDirectoryCreationModeOnWindows` and `UnixFileCreationModeOnWindows` parameters, to apply changes to existing assets you must delete and then re-create files and/or bins, such as HotBins.

#### If SNFS is on C: uninstall SNFS manually

Do not do this task if:

- SNFS is on the D: drive of the K2 Media Server.

Do this task if:

- SNFS 3.5.1 is on the C: drive of the K2 Media Server. If `C:\SNFS` exists on the K2 Media Server, then SNFS 3.5.1 is on the C: drive.

If SNFS 3.5.1 is on the C: drive of the K2 Media Server, you must move it to the D: drive. This is best accomplished as part of the upgrade process. After you uninstall SNFS, you must reset registry settings, install SNFS, then copy files from C: to D:. To do this, use the following procedure and other steps as instructed later in the upgrade process.

1. If you have not already done so, procure the `35c235d.reg` file.

The `35c235d.reg` file is on the version 8.1.x.xxxx K2 software CD in the SNFS directory. It can also be obtained at <http://www.grassvalley.com/downloads>.

2. Copy `35c235d.reg` to the local K2 Media Server.
3. On the local K2 Media Server open Windows **Add/Remove Programs** and uninstall SNFS.
4. Double-click `35c235d.reg` to run the file.

The file resets registry entries in preparation for moving SNFS from C: to D:.

5. When prompted "Are you sure...", answer **Yes**.

6. When a message confirms the registry change, dismiss the message.
7. Restart the K2 Media Server.

**Check all currently installed software on K2 Media Servers**

Prerequisites for this task are as follows:

- The device is assigned in the SiteConfig system description and network connectivity is present.
- SiteConfig is able to log in to the device using the username/password credentials assigned to the device.
- The SiteConfig PC does not have a network drive mapped to an administrative share (such as C\$) on a device on which you are checking software.

Do the following steps on the K2 Media Servers that you are upgrading.

1. In the **Software Deployment | Deployment Groups** tree view, right-click the top-most node for the group or any individual device and select **Check Software**.

***NOTE:** If you have access problems, verify that the administrator account on the device has credentials as currently configured in SiteConfig.*

The Check Software dialog box appears. SiteConfig searches for software on the selected device or devices and gathers information. Progress is reported.

2. When the check is complete, close the Check Software dialog box.

An updated list of all currently installed software is displayed in the **Software Deployment | Devices | Installed Software** list view. If software is a SiteConfig managed software package, information is displayed in the Managed Package and Deployment Group columns.

**Add software package to deployment group for K2 Media Servers**

Prerequisites for this task are as follows:

- You can access the software package file from the SiteConfig control point PC.
- The K2 Media Servers to which you are deploying software are in a deployment group.

Use the following procedure to add one or more software packages to the deployment group that contains your K2 Media Servers. For this release of K2 software, identify and add software installation files as follows:

Software	File name
K2 Server software for 32-bit systems	<i>GrassValleyK2Server_x86_8.1.x.xxxx.cab</i>
K2 Server software for 64-bit systems	<i>GrassValleyK2Server_x64_8.1.x.xxxx.cab</i>
SNFS software for 32-bit systems	<i>SNFS_x86_3.5.3.b27171.cab</i>
SNFS software for 64-bit systems	<i>SNFS_x64_3.5.3.b27171.cab</i>

You can add files for both 32 bit and 64 bit systems because when SiteConfig deploys software it automatically deploys the 32 bit or 64 bit software appropriate for the target device.

1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
2. Click the **Add** button.  
The Add Package(s) dialog box opens.
3. Do one of the following to select the software package:
  - Select from the list of packages then click **OK**.
  - Click **Browse**, browse to and select the package, then click **Open**.
4. If one or more EULAs are displayed, accept them to proceed. If you do not accept a EULA, the associated software is not assigned to the deployment group.  
SiteConfig adds the package to the deployment group.

The package appears in the Managed Packages list for the selected deployment group. SiteConfig creates new software deployment tasks for the package and displays them in the Tasks list view.

#### Upgrade software on K2 Media Servers

Prerequisites for this task are as follows:

- The devices that you are upgrading are in a deployment group.
- For the software you are upgrading, you have added a newer version of that managed software package to the deployment group.
- If SNFS was on C:, you have uninstalled SNFS manually as instructed earlier in this upgrade procedure.
- You have recently done the SiteConfig "Check Software" operation on the devices you are upgrading.
- **NOTE: On a K2 system, if a SNFS version lower than 3.0 is installed, do not uninstall using SiteConfig. You must manually uninstall using a special batch file. Follow instructions in the release notes for your current version of K2 software.**

If you are upgrading multiple software components for which there is a required sequence, you must check and uncheck tasks and run multiple deployment sessions to control the sequence. For some software components, SiteConfig aids you by enforcing dependencies. For each individual software component, SiteConfig enforces an uninstall of the current version of software before installing the upgrade version. SiteConfig provides uninstall deployment tasks and install deployment tasks to indicate the taskflow. SiteConfig can do the uninstall/install in a single deployment session.

1. In the **Software Deployment | Deployment Groups** tree view, select the device or the group of devices to which you are deploying software.  
The corresponding software deployment tasks are displayed in the Tasks list view.
2. For the software you are deploying, select the **Deploy** check box in the row for the uninstall task.

- For the software you are installing, select the **Deploy** check box in the row for the install task.

For upgrading a K2 Media Server to this release, deploy the following tasks:

Deploy	Managed Package	Action
✓	GrassValleyK2Server xxxxx.xxxx or GrassValleyK2Server_x86 xxxxx.xxxx or GrassValleyK2Server_x64 xxxxx.xxxx	Uninstall
✓	GrassValleyK2Server_x86 8.1.x.xxxx	Install
✓	GrassValleyK2Server_x64 8.1.x.xxxx	Install

You can deploy packages for both 32 bit and 64 bit systems because when SiteConfig deploys software it automatically deploys the 32 bit or 64 bit software appropriate for the target device. You must install SNFS as a separate cab file.

Also, when upgrading SNFS, configure deployment tasks to upgrade (uninstall/install) SNFS. Deploy the following tasks to K2 Media Servers with role of file system server:

Deploy	Managed Package	Action
✓	SNFS xxxxxx or SNFS x86 xxxxxx or SNFS x64 xxxxxx	Uninstall
✓	SNFS x86 3.5.3.b27171	Install
✓	SNFS x64 3.5.3.b27171	Install

If you previously uninstalled SNFS manually and then did a Check Software operation, only the install task is present.

You can deploy packages for both 32 bit and 64 bit systems because when SiteConfig deploys software it automatically deploys the 32 bit or 64 bit software appropriate for the target device. You must install SNFS as a separate cab file.

If using K2-Aurora FTP and an upgrade to a compatible version is required, deploy the K2-Aurora FTP software while you are upgrading K2 software. Refer to [Compatible Grass Valley products](#) on page 29 to determine if an upgrade is required.

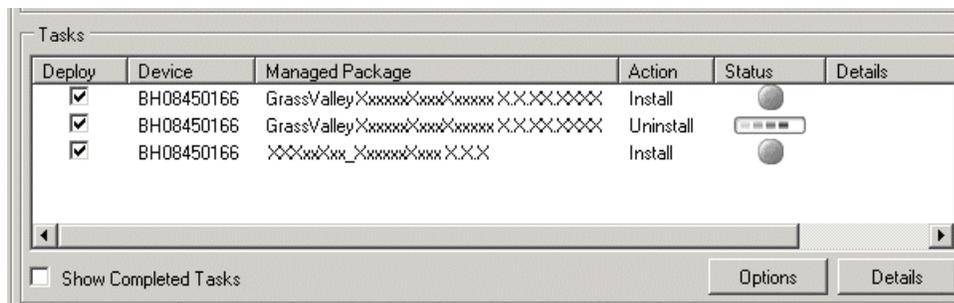
**NOTE:** *If there are dependencies, SiteConfig can enforce that some tasks be deployed together.*

4. Check the area next to the Start Deployment button for a message.



If a message instructs you to upgrade the Discovery Agent, on the control point PC go to the directory to which SiteConfig is installed, find the *DiscoveryAgent\_x.x.x.x.cab* file, add it to the deployment group, and deploy the Discovery Agent software as well.

5. Click the **Start Deployment** button.



Deployment tasks run and software is uninstalled. Progress is reported and next steps are indicated in both the Status and Details columns. If an error appears regarding prerequisite software, install the prerequisite files on the control point PC and then repeat this step.

When upgrading both K2 and SNFS software, SiteConfig uninstalls both in the proper sequence.

6. When the Status or Details columns indicate next steps, identify the software in the row, then do one of the following:

- For K2 software, when Details displays a **Restart required** link (but not "Visible dialog pending..."), click the link and when prompted "...are you sure...", click **Yes**.

The K2 Media Server restarts. This restart is required by the K2 software uninstall.

When upgrading SNFS software, this is also the restart required by the SNFS uninstall.

Deployment tasks run and software is installed. Progress is reported and next steps are indicated in both the Status and Details columns.

If upgrading both K2 and SNFS software, SiteConfig uninstalls both in the proper sequence.

7. When the Status or Details columns indicate next steps, identify the software in the row, then do one of the following:

- For K2 software, when Details displays a **Restart required** link (but not "Visible dialog pending..."), click the link and when prompted "...are you sure...", click **Yes**.

The K2 Media Server restarts. This restart is required by the K2 software install.

If upgrading both K2 and SNFS software, SiteConfig uninstalls both in the proper sequence.

8. Monitor progress as indicated by both the Status and Details column. When finished, the Status column indicates complete.

9. If you previously uninstalled SNFS manually because SNFS was on C:, copy directories/files from C: to D:, overwriting files on D:, as follows.
  - a) Copy the `C:\SNFS\config` directory to `D:\SNFS\config`.
  - b) Copy the `C:\SNFS\data` directory to `D:\SNFS\data`. This directory can be large, so allow adequate time to complete the copy operation.
  - c) A restart is required to put the change into effect. If you do a subsequent upgrade task that also requires a restart, that restart is sufficient. Otherwise restart now.
  - d) After the entire K2 SAN upgrade process is complete, test media access. If successful, delete the `C:\SNFS` directory and its files on the K2 Media Server.

### Upgrading the Discovery Agent

Do this task if SiteConfig does not prompt you to upgrade to the compatible version of the Discovery Agent when you deploy software.

Prerequisites for this task are as follows:

- Your devices are in one or more deployment groups
  - A check software operation has been performed either on the device or the deployment group that you are upgrading
1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
  2. Click **Add Package**
  3. Click **Browse** in the add package dialog and browse to the Discovery Agent Setup folder under your SiteConfig install location on the SiteConfig PC.
  4. Select the required `DiscoveryAgent_<version>.cab` file and click **Open**.  
SiteConfig generates deployment tasks to uninstall the existing version and installs the selected version and enables the **Start Deployment** button.
  5. Check the uninstall and install deploy tasks for the Discovery Agent and click the **Start Deployment** button when you are ready to deploy.  
SiteConfig runs the deployment tasks.

### Verify/upgrade switch firmware

Do not do this task if:

- Your HP ProCurve 29xx series switch already has the current required firmware version.

Do this task if:

- Your HP ProCurve 29xx series switch does not have the current required firmware version.

Refer to compatibility information earlier in these release notes for firmware version requirements.

1. Telnet to the switch and login with the administrator username and password.
2. At the switch console command (CLI) prompt, type the following, then press **Enter**:  
menu  
If prompted to save the current configuration, answer no (press the n key) to proceed.  
The main menu opens.

3. From the main menu, tab to **Command Line (CLI)** and press **Enter**. The command prompt appears.
4. Check the version of firmware on the switch. To do this, type the following, then press **Enter**:

show flash

Information is displayed similar to the following example:

```
HP_iSCSI_switch1# show flash
Image                Size(Bytes)  Date        Version
-----
Primary Image       : 6737518     07/25/08    T.13.23
Secondary Image     : 5886358     10/26/06    T.11.12
Boot Rom Version:   K.12.12
Current Boot        : Primary
```

5. Check the Primary Image Version and refer to compatibility information earlier in these release notes. If instructed to change the firmware on the switch, do so before continuing.

#### Related Topics

[Upgrading firmware on HP switch](#)

[Configuring QOS on the GigE switch](#)

[Compatible HP ProCurve GigE switch components](#) on page 23

## Upgrade RAID controller microcode

Do not do this task if:

- The K2 RAID controller and expansion chassis microcode is already at compatible versions, as listed in [Compatible K2 RAID components](#) on page 24.
- The K2 RAID is a Level 2 or Level 3.

Do this task if:

- The K2 RAID controller and/or expansion chassis microcode is at a version that is not compatible.

The microcode files are copied on to the K2 Media Server when the K2 system software is installed.

1. Refer to the K2 RAID compatibility specifications earlier in these release notes for the version to which you must upgrade and for the file names for the microcode files.
2. Use Storage Utility to upgrade microcode.  
Refer to the *K2 SAN Installation and Service Manual* for procedures.
3. On 100% completion, proceed as follows:
  - If the RAID controller chassis has redundant controllers, power cycle the RAID controller chassis, then restart the K2 Media Server.
  - If the RAID controller chassis does not have redundant controllers, no power cycle is required. The firmware download is complete.

## Upgrade RAID disk drive firmware

Do not do this task if:

- The K2 RAID disk drive firmware is already at compatible versions, as listed in [Compatible K2 RAID disk drive firmware](#) on page 25.

- The K2 RAID is Level 2 or Level 3 SAN.

Do this task if:

- The K2 RAID disk drive firmware is at a version that is not compatible.

Prerequisites:

- The RAID system is offline.
- Only the primary K2 Media Server is powered up.
- K2 software has been upgraded on the K2 Media Server. This is required because the firmware files are copied onto the K2 Media Server when the K2 software is installed.

1. Determine if disk drive firmware upgrades are required as follows:
  - a) Select a disk drive icon in the Storage Utility tree view, then note the drive properties reported in the right-hand pane.
  - b) Refer to the K2 RAID compatibility specifications earlier in these release notes for drive-type identifiers and firmware versions.

2. If an upgrade is required, continue with this procedure to upgrade disk drive firmware.

Refer to the *K2 SAN Installation and Service Manual* for complete procedures.

3. In Storage Utility, right-click a controller in the tree view, then select **Advanced | Download Disk Firmware** in the context menu.

**NOTE:** *You can download firmware to a single disk by right-clicking a disk icon in the tree view.*

The Open File dialog box opens.

4. In the Open File dialog box, browse to the desired firmware file for your disks, select the file, and click **OK**.

As instructed by a message that appears, watch the lights on the drives. For each drive, one at a time, the lights flash as firmware loads. Wait until the lights on all the drives on which you are downloading firmware have completed their flashing pattern. This can take several minutes.

The Progress Report window appears showing the disk firmware download task and the percentage complete.

5. When finished, restart the K2 Media Server.

## Reset Capture Services

Do not do this task if:

- You do not use any of the K2 Capture Services.

Do this task if:

- You are using one or more K2 Capture Services, such HotBin, Pathfire, DG, XML Import, Export, P2, etc

Do this task on the K2 system running your K2 Capture Service, which is the K2 system that receives the media to be imported into K2 storage. This can be a K2 Solo Media Server, a stand-alone K2

Summit Production Client, or the K2 Media Server with the role of primary FTP server on a K2 SAN.

When you configure a K2 Capture Service for the first time, the service is set to startup type Automatic. However, if you upgrade or otherwise re-install your K2 System Software, the service is re-set to startup type Manual. Therefore, you must re-configure the service after K2 System Software upgrade/ reinstall in order to set the startup type back to Automatic.

1. From the **Start** menu, access the **Programs** menu and select **Grass Valley | K2 Capture Services**.  
On a K2 Summit/Solo system, if the write filter is enabled, a message appears that informs you about the write filter and prompts you to restart. Restart as prompted, then repeat this step.  
The K2 Capture Services utility dialog box is displayed.
2. Click **Apply**.  
On a K2 Summit/Solo system, a message appears that informs you about the write filter and prompts you to restart. Click **OK** and the K2 Summit/Solo system restarts.  
For import capture services, the service checks the source directory for files. If files are present, the service moves them to the Archive sub-directory. It does not import the files into the destination bin on the K2 system.

## Update Broadcom driver

This task applies to the following:

- All Dell platform GV STRATUS servers and K2 Media Servers with Microsoft Windows Server 2008 R2 operating system.

Do not do this task if:

- In Device manager under Network Adapters, the Broadcom driver version is 7.0.11.0.

Do this task if:

- In Device manager under Network Adapters, the Broadcom driver version is earlier than 7.0.11.0.

Before doing this task, procure the following file:

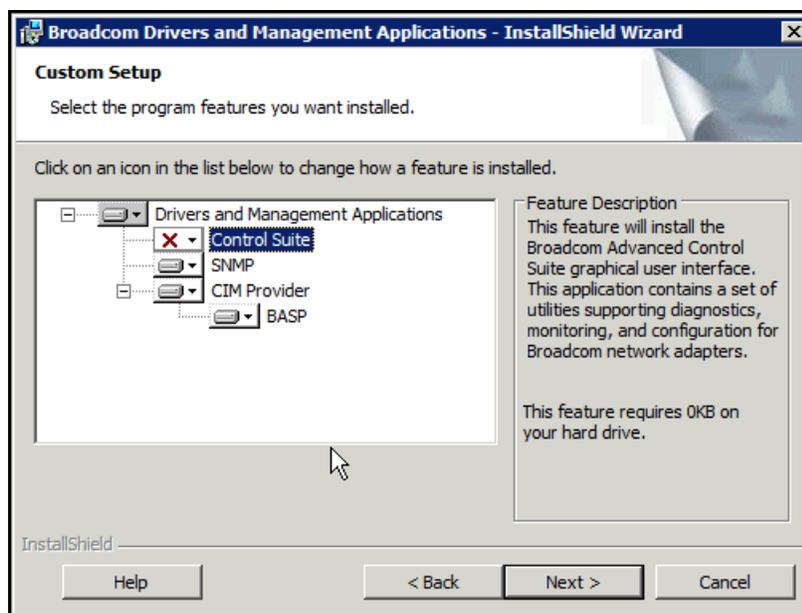
- *Network\_Driver\_2T17H\_WN32\_17.0.1\_A00.EXE*

The file is available on the Grass Valley website GV STRATUS version download page. It is in *StratusMiscellaneousSoftware2.0.zip*.

This task fixes potential network and performance problems.

1. Login to the server as Administrator.
2. Double-click *Network\_Driver\_2T17H\_WN32\_17.0.1\_A00.EXE*.  
A Dell Update Package dialog box opens.
3. Click **Install**.  
The Broadcom Drivers and Application Management Applications wizard opens.

4. Work through the wizard, clicking **Next**, **I accept**, and **Next**.  
The Custom Setup page opens.



5. For each of the following nodes, click the drop-down list and select **This Feature, and all sub-features, will be installed on the local hard drive:**

- **SNMP**
- **CIM Provider**

**NOTE:** *Do not install Control Suite.*

6. Click **Next** and **Install**.
7. If prompted to enable System TCP Chimney Offload, click **Yes**.
8. Click **Finish** to complete the wizard.  
The Dell Update Package dialog box appears.
9. Click **OK**.
10. Restart the server to put changes into effect.

Next, configure `fsnameservers.cfg` files. This is required when updating the Broadcom driver.

### Configure `fsnameservers` on servers-class devices

This task applies to SAN systems with one or more SNFS servers that have had their Broadcom driver updated to version 7.0.11.0. On those SAN systems, all devices with a `v:` drive to the SAN's

storage (all SNFS servers and SNFS clients) must have their *fnameservers* file configured. This includes the following type of SAN systems:

- An online or production K2 SAN — If the SAN's SNFS server, which is the K2 Media Server with role of media file system server (FSM), has had its Broadcom driver updated to version 7.0.11.0, then this task applies to the following server-class devices on that SAN:
  - The one K2 Media Server (if non-redundant) or two K2 Media Servers (if redundant). This device is the SAN's SNFS server.
  - If a STRATUS system, the STRATUS Proxy Encoder. This device is an SNFS client on the SAN.
  - If an A1 STRATUS system, the STRATUS Proxy Server. This device is an SNFS client on the SAN.
  - Any other SAN-attached server-class devices, such as NH FTP servers. This device is an SNFS client on the SAN.
- A nearline K2 SAN — If the SAN's SNFS server, which is the K2 Media Server with role of media file system server, has had its Broadcom driver updated to version 7.0.11.0, then this task applies to the following server-class devices on that SAN:
  - The one K2 Media Server (if non-redundant) or two K2 Media Servers (if redundant). This device is the SAN's SNFS server.
  - Any other SAN-attached server-class devices, such as NH FTP servers. This device is an SNFS client on the SAN.
- A STRATUS Proxy Storage system — If the SAN's SNFS server, which is the Proxy Storage file system server, has had its Broadcom driver updated to version 7.0.11.0, this task applies to the following server-class device:
  - The Proxy Storage file system server. This device is the SAN's SNFS server.

The SAN must be in an offline mode before doing this task.

You must know your server's names and IP addresses.

1. On the SAN's SNFS server that has had its Broadcom driver updated, login to the server as Administrator.
2. In Notepad, open the following file:  
`D:\SNFS\config\fnameservers`
3. In the file, identify the server name of the local server.  
If a redundant SAN, identify the server names of both of the redundant servers.
4. Edit the line of text and replace the server name with the server's IP address.  
If a redundant SAN, replace both server names with their IP addresses.  
Make sure you leave text lines intact. Do not alter the line returns, spaces, other elements of the text line.
5. Save the file.
6. Copy the *fnameservers* file to an external location, such as a network share or a USB drive, that allows access by the other devices of the SAN.
7. Restart the server.

8. If redundant SNFS servers, do the following on the other redundant server:
  - a) Copy (overwrite) the *fsnameservers* file onto the device.  
On SNFS servers, the file's location is *D:\SNFS\config\fsnameservers*.
  - b) Restart the device.
9. On other server-class devices that are SNFS clients, do the following:
  - a) Copy (overwrite) the *fsnameservers* file onto the device.  
On SNFS clients, the file's location is *C:\SNFS\config\fsnameservers*.
  - b) Restart the device.

You must also configure *fsnameservers* on all remaining SNFS clients on the SAN. Refer to the related topic later in the upgrade process.

## Manage redundancy on K2 Media Servers

Do not do this task if:

- You are upgrading a basic (non-redundant) K2 SAN. This means you have just one K2 Media Server that takes the role of media file system/database server. Skip ahead and begin upgrading your other K2 Media Servers or SAN K2 clients.

Do this task if:

- You are upgrading a redundant K2 SAN. To prevent triggering failover mechanisms, you must manage primary/backup roles as instructed.

### If primary upgrade only is complete

If you have completed the upgrade to the primary server but you have not yet upgraded the backup server, do the following:

1. Make sure the backup server is still shut down.
2. Put the primary server in service as follows:
  - a) On the primary server, run Server Control Panel. You can do this at the local server or through the K2 System Configuration application.
  - b) Use the **Start** button on Server Control Panel. This makes the primary server qualified to take the role of media file system/database server.
  - c) Make sure that Server Control Panel shows green LEDs and that the server on which you have upgraded software is indeed the current primary server.
3. Power up the backup server. Wait until startup processes complete before continuing.  
The Failover Monitor should currently be off, as this is the normal state of the service at system startup.

Next upgrade the backup server. Perform all K2 Media Server upgrade tasks on the backup server.

### If primary and backup upgrades are complete

If you have completed the upgrade to both the primary and backup servers, do the following:

1. Make sure the primary server is powered up.

2. Run Server Control Panel. You can do this at the local server or through the K2 System Configuration application. Make sure Server Control Panel shows green LEDs and that the first server on which you upgraded software is still the current primary server.
3. Put the backup server in service as follows:
  - a) Run Server Control Panel. You can do this at the local server or through the K2 System Configuration application.

The Failover Monitor should currently be off on the backup server, as this is the normal state of the service at system startup.
  - b) Use the **Start** button on Server Control Panel. This makes the backup server qualified to take the role of media file system/database server.
  - c) Make sure that Server Control Panel shows green LEDs and that servers are correctly taking primary/backup roles.

Next upgrade any remaining K2 Media Servers.

### Upgrade remaining K2 Media Servers

Do not do this task if:

- All the K2 Media Servers on the K2 SAN have been upgraded.

Do this task if:

- There are K2 Media Servers that do not take the role of media file system/database server on the K2 SAN that have not yet been upgraded.

Perform all upgrade tasks on the remaining K2 Media Servers.

### Upgrade K2 client

Work through the following topics sequentially to upgrade K2 clients.

***NOTE: These upgrade instructions assume that on your SAN-attached K2 Summit systems, the current K2 software is at version 8.x or higher. If the current K2 software is at a version lower than 8.x, you must upgrade K2 Summit systems using the appropriate Grass Valley Field Kit, which includes a disk image and hardware. Once upgraded via the field kit to an 8.x version, you can then use these upgrade instructions.***

#### Prepare for K2 system upgrade

Before upgrading K2 systems, do the following:

- Procure the software installation files for this release via the appropriate distribution method, such as download, USB Recovery Flash Drive, network drive, or external drive.
- Start up the K2 systems you are upgrading, if they are not already started.
- For K2 Summit Production Client or K2 Solo Media Server, if you have not already done so, disable (unlock) the write filter.
- Stop all media access on K2 systems.

- Shut down all applications on K2 systems.

#### Check all currently installed software on SAN K2 clients

Prerequisites for this task are as follows:

- The device is assigned in the SiteConfig system description and network connectivity is present.
- SiteConfig is able to log in to the device using the username/password credentials assigned to the device.
- The SiteConfig PC does not have a network drive mapped to an administrative share (such as C\$) on a device on which you are checking software.

Do the following steps on the SAN K2 clients that you are upgrading.

1. In the **Software Deployment | Deployment Groups** tree view, right-click the top-most node for the group or any individual device and select **Check Software**.

**NOTE:** *If you have access problems, verify that the administrator account on the device has credentials as currently configured in SiteConfig.*

The Check Software dialog box appears. SiteConfig searches for software on the selected device or devices and gathers information. Progress is reported.

2. When the check is complete, close the Check Software dialog box.

An updated list of all currently installed software is displayed in the **Software Deployment | Devices | Installed Software** list view. If software is a SiteConfig managed software package, information is displayed in the Managed Package and Deployment Group columns.

#### Add software package to deployment group for SAN K2 clients

Prerequisites for this task are as follows:

- You can access the software package file from the SiteConfig control point PC.
- The SAN K2 clients to which you are deploying software are in a deployment group.

Use the following procedure to add one or more software packages to the deployment group that contains your SAN K2 clients. For this release of K2 software, identify and add software installation files as follows:

Software	File name
K2 client software	<i>GrassValleyK2SummitSANClient_8.1.x.xxxx.cab</i>
SNFS software	<i>SNFS_Summit_3.5.3.b27171.cab</i>

1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
2. Click the **Add** button.  
The Add Package(s) dialog box opens.
3. Do one of the following to select the software package:
  - Select from the list of packages then click **OK**.
  - Click **Browse**, browse to and select the package, then click **Open**.

4. If one or more EULAs are displayed, accept them to proceed. If you do not accept a EULA, the associated software is not assigned to the deployment group.

SiteConfig adds the package to the deployment group.

The package appears in the Managed Packages list for the selected deployment group. SiteConfig creates new software deployment tasks for the package and displays them in the Tasks list view.

#### Upgrade software on SAN K2 clients

Prerequisites for this task are as follows:

- The devices that you are upgrading are in a deployment group.
- For the software you are upgrading, you have added a newer version of that managed software package to the deployment group.
- You have recently done the SiteConfig "Check Software" operation on the devices you are upgrading.
- For the K2 Summit Production Client, the write filter is disabled (unlocked).
- **NOTE: On a K2 system, if a SNFS version lower than 3.0 is installed, do not uninstall using SiteConfig. You must manually uninstall using a special batch file. Follow instructions in the release notes for your current version of K2 software.**

If you are upgrading multiple software components for which there is a required sequence, you must check and uncheck tasks and run multiple deployment sessions to control the sequence. For some software components, SiteConfig aids you by enforcing dependencies. For each individual software component, SiteConfig enforces an uninstall of the current version of software before installing the upgrade version. SiteConfig provides uninstall deployment tasks and install deployment tasks to indicate the taskflow. SiteConfig can do the uninstall/install in a single deployment session.

1. In the **Software Deployment | Deployment Groups** tree view, select the device or the group of devices to which you are deploying software.  
The corresponding software deployment tasks are displayed in the Tasks list view.
2. For the software you are deploying, select the **Deploy** check box in the row for the uninstall task.

- For the software you are installing, select the **Deploy** check box in the row for the install task.

For upgrading SAN K2 clients to this release, configure **Deploy** check boxes as follows:

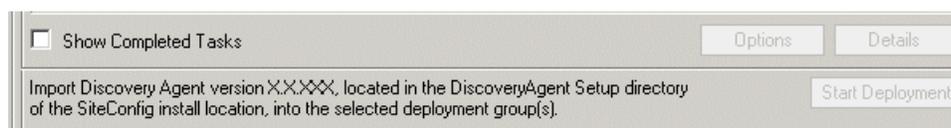
Deploy	Managed Package	Action
✓	GrassValleyK2SummitSANClient xxxx.xxxx	Uninstall
✓	GrassValleyK2SummitSANClient 8.1.x.xxxx	Install
✓	WRegMon_SummitSANClient x.x.x	Install (there is no uninstall task for this software)

Also, when upgrading SNFS, configure deployment tasks to upgrade (uninstall/install) SNFS. Deploy the following tasks at the same time:

Deploy	Managed Package	Action
✓	SNFS Summit xxxxxx	Uninstall
✓	SNFS Summit 3.5.3.b27171	Install

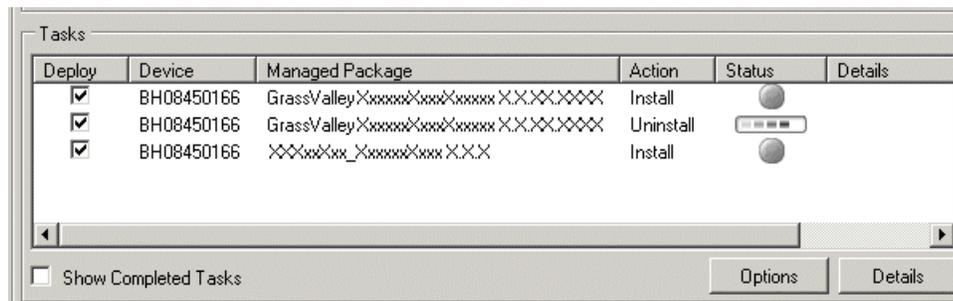
**NOTE:** *If there are dependencies, SiteConfig can enforce that some tasks be deployed together.*

- Check the area next to the Start Deployment button for a message.



If a message instructs you to upgrade the Discovery Agent, on the control point PC go to the directory to which SiteConfig is installed, find the *DiscoveryAgent\_x.x.x.x.cab* file, add it to the deployment group, and deploy the Discovery Agent software as well.

- Click the **Start Deployment** button.



Deployment tasks run and software is uninstalled. Progress is reported and next steps are indicated in both the Status and Details columns. If an error appears regarding prerequisite software, install the prerequisite files on the control point PC and then repeat this step.

When upgrading both K2 and SNFS software, SiteConfig uninstalls both in the proper sequence.

- When the Status or Details columns indicate next steps, identify the software in the row, then do one of the following:
  - For SNFS software, when Details displays a **Restart required** link, click the link and when prompted "...are you sure...", click **Yes**. After this restart, continue with other restarts as indicated.
  - For K2 software, if the version from which you are upgrading is 8.0 or higher, when Details displays a **Restart required** link, click the link and when prompted "...are you sure...", click **Yes**.
- Monitor progress as indicated by both the Status and Details column. When finished, the Status column indicates complete.

#### Install required Windows updates

Do this task if:

- You have a K2 Summit, K2 Summit 3G, K2 Solo, K2 Solo 3G system with Windows XP.
- You wish to install Windows XP Security Updates.

Before doing this task, obtain a new 16GB CompactFlash Drive (GV part number 050-3493-00) from Grass Valley Service at <http://www.grassvalley.com/support>.

**NOTE: Do not install general Windows updates as available from Microsoft. Update only as directed by Grass Valley.**

**Refer to "K2 Summit Production Client Service Manual" to accomplish the steps in this procedure.**

- Download Windows update batch files from Grass Valley website; *RunUpdates.zip*, *RunUpdates2011.zip*, *RunUpdates2012.zip*, and *RunUpdates2013Q1.zip*.
- Save the batch files to a USB drive.
- Create a recovery image of the K2 Summit/Solo system and save the image to a USB drive.  
This is a system-specific recovery image for restoring that specific K2 Summit/Solo system only.

4. If you have a K2 Summit 3G or K2 Solo 3G, skip steps 5 and 6, and proceed to step 7.
5. Remove the CompactFlash boot media to replace the existing 4GB or 8GB CompactFlash drive with the new 16GB CompactFlash drive.
6. Restore from the system-specific recovery image you created in step 3.  
When using Acronis, select **No Free Space** on the Restored Partition Size page. Refer to the related topic in "K2 Summit Production Client Service Manual".
7. Turn off the write filter, then restart.
8. From the USB drive, extract the contents of the *RunUpdates.zip* file into the *C:\Temp* directory.  
This creates a folder named *RunUpdates* that includes Windows update files.
9. Within the *RunUpdates* folder, run *RunUpdates.exe*.  
A command shell starts.
10. When prompted, enter *Y* to start the update process.  
For each of the security updates, the shell displays a line showing the update installing. A window showing the progress of an update opens and then closes when complete. The shell then updates with the completion status of the update.
11. If you interrupt the Windows update process, run *RunUpdates.exe* to start it again. Updating continues from the point of interruption.
12. When updates complete and the shell displays the prompt **Do you want to reboot now?**, enter *Y* to restart.
13. Proceed to the *RunUpdates2011.zip* batch file.
14. From the USB drive, extract the contents of the *RunUpdates2011.zip* file into the *C:\Temp* directory.  
This creates a folder named *RunUpdates2011* that includes Windows update files.
15. Within the *RunUpdates2011* folder, run *RunUpdates.exe*.  
A command shell starts.
16. If the batch script stalls, press **Ctrl + C** at the command prompt to stop the process and restart *RunUpdates.exe* from *RunUpdates2011* folder until all files are successfully processed.  
It takes about one hour to finish the updates.
17. When updates complete and the shell displays the prompt **Do you want to reboot now?**, enter *Y* to restart.
18. Proceed to the *RunUpdates2012.zip* batch file.
19. From the USB drive, extract the contents of the *RunUpdates2012.zip* file into the *C:\Temp* directory.  
This creates a folder named *RunUpdates2012* that includes Windows update files.
20. Within the *RunUpdates2012* folder, run *RunUpdates.exe*.  
A command shell starts.  
**NOTE: *RunUpdates2012* batch script will automatically reboot the system in the middle of the updates**
21. Restart the batch script to finish the updates.

22. When updates complete and the shell displays the prompt **Do you want to reboot now?**, enter Y to restart.
23. If the batch script stalls, press **Ctrl + C** at the command prompt to stop the process and restart *RunUpdates.exe* from *RunUpdates2012* folder until all files are successfully processed.  
It takes about one hour to finish the updates.
24. Proceed to the *RunUpdates2013Q1.zip* batch file.
25. From the USB drive, extract the contents of the *RunUpdates2013Q1.zip* file into the *C:\Temp* directory.  
This creates a folder named *RunUpdates2013Q1* that includes Windows update files.
26. Within the *RunUpdates2013Q1* folder, run *RunUpdates.exe*.  
A command shell starts.
27. If the batch script stalls, press **Ctrl + C** at the command prompt to stop the process and restart *RunUpdates.exe* from *RunUpdates2013Q1* folder until all files are successfully processed.  
It takes about one hour to finish the updates.
28. When updates complete and the shell displays the prompt **Do you want to reboot now?**, enter Y to restart.  
The installed security files from each RunUpdates batch are now located in the *Installed* folder in *C:\temp* folder.
  - *RunUpdates* folder: *C:\temp\RunUpdates\Installed\*.
  - *RunUpdates2011* folder: *C:\temp\RunUpdates2011\Installed\*.
  - *RunUpdates2012* folder: *C:\temp\RunUpdates2012\Installed\*.
  - *RunUpdates2013Q1* folder: *C:\temp\RunUpdates2013Q1\Installed\*.
29. To recover some disk space, you may delete the *.zip files*, *extracted folders*, and the *Installed* folder.

### Upgrading the Discovery Agent

Do this task if SiteConfig does not prompt you to upgrade to the compatible version of the Discovery Agent when you deploy software.

Prerequisites for this task are as follows:

- Your devices are in one or more deployment groups
  - A check software operation has been performed either on the device or the deployment group that you are upgrading
1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
  2. Click **Add Package**
  3. Click **Browse** in the add package dialog and browse to the Discovery Agent Setup folder under your SiteConfig install location on the SiteConfig PC.
  4. Select the required *DiscoveryAgent\_<version>.cab* file and click **Open**.  
SiteConfig generates deployment tasks to uninstall the existing version and installs the selected version and enables the **Start Deployment** button.

5. Check the uninstall and install deploy tasks for the Discovery Agent and click the **Start Deployment** button when you are ready to deploy.  
SiteConfig runs the deployment tasks.

### Configure fsnameservers on SNFS clients

This task applies to SAN systems with one or more SNFS servers that have had their Broadcom driver updated to version 7.0.11.0. On those SAN systems, all devices with a v: drive to the SAN's storage (all SNFS servers and SNFS clients) must have their *fsnameservers* file configured. This includes the following type of SAN systems:

- An online or production K2 SAN — If the SAN's SNFS server, which is the K2 Media Server with role of media file system server (FSM), has had its Broadcom driver updated to version 7.0.11.0, then this task applies to the following SNFS clients of that SAN:
  - All K2 Summit systems attached to the K2 SAN
  - Any STRATUS high resolutions client PCs attached to the K2 SAN
  - Any Macintosh (K2 FCP Connect) clients attached to the K2 SAN
  - Any other SNFS client devices attached to the K2 SAN

The SNFS clients must be in an offline mode before doing this task.

You must know your SNFS client's names and IP addresses.

You must have access to the *fsnameservers* file that you copied from the SAN's SNFS server.

1. On the SNFS client, login to as Administrator.
2. Copy (overwrite) the *fsnameservers* file onto the device.  
On SNFS clients, the file's location is *C:\SNFS\config\fsnameservers*.
3. Restart the SNFS client.
4. Repeat these steps on all the SAN's SNFS client devices.

### Lock K2 Summit Production Clients

This task enables the write filter on a K2 Summit Production Client or on a group of K2 Summit Production Clients.

Prerequisites for this task are as follows:

- The device or all the devices in the group are communicating correctly in SiteConfig. This is indicated by the green star icon overlay.
  - The device or all the devices in the group are currently unlocked. This is indicated by the red lock icon overlay.
1. In the **Network Configuration | Devices** tree view or the **Software Deployment | Deployment Groups** tree view, identify the device or the group of devices that you intend to lock.
  2. Right-click the device or the group and select **Lock**.  
A "...may require restart..." message appears.
  3. Click **Yes** to allow SiteConfig to restart the device or devices.  
The Locking Devices window opens and displays progress.

4. When the Locking Devices window reports that the lock process completed successfully, click **Close**.

The device or devices are now locked. For K2 Summit/Solo, this also enables the write filter, which enforces the restart.

#### **Install MPEG-2/AVC-Intra field kit**

If you are installing an MPEG-2 or AVC-Intra field kit upgrade on one or more of your K2 Summit Production Clients or K2 Solo Media Servers, do so now. Follow the procedure in the Field Kit Upgrade Instructions document that you received with the field kit.

### **Upgrade STRATUS and Aurora Playout systems**

Prerequisites for this task are as follows:

- K2 systems are upgraded to the compatible version of K2 system software.
- All STRATUS and Aurora Playout devices are offline (all media access stopped) or shut down.

Upgrade your STRATUS and Aurora Playout systems to the compatible versions of software. This includes the STRATUS Proxy Storage system, if present in your system. Refer to each product's documentation for procedures.

### **Upgrade other SAN clients**

Do this task if:

- You have clients on the K2 SAN that have not yet been upgraded. This is the case if you have K2 appliances or other products that use the shared storage of the K2 SAN.

Prerequisites for this task are as follows:

- You have access to the software installation files for this release. Procure the files via the appropriate distribution method, such as download, CD-ROM, network drive, or external drive.

Refer to upgrade procedures for K2 clients and similarly upgrade all remaining client devices on the K2 SAN.

**NOTE:** *You must restart after installing K2 software.*

### **Make recovery images**

After you have upgraded software as instructed in these procedures and verified that your system is working properly, you should always make a recovery image of each of your upgraded computers. Use a sequence of tasks similar to those you followed for upgrading software so that as you take systems offline you manage redundancy, servers, and clients, as appropriate for your system.

Refer to the Grass Valley product's *Service Manual* for recovery image procedures.

## Upgrading stand-alone K2 systems with SiteConfig

This section contains the tasks for using SiteConfig to upgrade stand-alone K2 systems to this release of K2 software.

Work through the tasks sequentially to complete the upgrade.

**NOTE:** *These upgrade instructions assume that on your K2 Summit/Solo system, the current K2 software is at version 8.x or higher. If on a K2 Summit system the current software is at a version lower than 8.x, you must upgrade it using a Grass Valley Field Kit, which includes a disk image and hardware. K2 Solo systems are available with 8.x software only as shipped from Grass Valley.*

### About upgrading stand-alone K2 systems with SiteConfig

These upgrade instructions apply to stand-alone K2 systems as follows:

- K2 Summit Production Client internal storage
- K2 Summit Production Client direct-connect storage
- K2 Solo Media Server

With these upgrade instructions, you use SiteConfig from a network connected control point PC and remotely upgrade software simultaneously on multiple K2 systems.

**NOTE:** *A control point PC is required.*

This is the recommended process for software upgrades. If you choose to upgrade manually instead, you can go to each local K2 system and use keyboard, monitor, and mouse to upgrade software. You can find instructions for a manual upgrade without SiteConfig at [Upgrading stand-alone K2 systems with SiteConfig](#) on page 61 in these release notes.

If this is the first time using SiteConfig for software upgrade, follow instructions in *K2 System Guide* rather than instruction in these release notes. You must first have SiteConfig set up for system management and software deployment of the stand-alone K2. Also refer to the *SiteConfig User Manual* or *SiteConfig Help Topics*. Then, after you have completed this initial SiteConfig set up, you can follow the instructions in this section to upgrade software.

**NOTE:** *If this is the first time using SiteConfig for software upgrade do not follow instructions in these release notes alone.*

The following installation tasks provide information specifically for the upgrade to this version of 8.1 software. Read the information in these sections carefully before attempting any upgrade to software on a stand-alone K2 system.

### Make recovery images

Do not do this task if:

- You previously made a recovery image at the current software version for each computer you are upgrading.

Do this task if:

- You do not have a recovery image at the current software version for one or more of the computers you are upgrading.

The recommended procedure is to make a recovery image immediately after a software upgrade. If you neglected to do this when you last upgraded software you should make the recovery image now, before upgrading to the new version.

Refer to the Grass Valley product's *Service Manual* for recovery image procedures.

**△ CAUTION:** *If you upgrade and then decide you do not want to stay with this version of K2 system software, you must use the recovery disk image process to downgrade to your previous version.*

## Prepare for K2 system upgrade

Before upgrading K2 systems, do the following:

- Procure the software installation files for this release via the appropriate distribution method, such as download, USB Recovery Flash Drive, network drive, or external drive.
- Start up the K2 systems you are upgrading, if they are not already started.
- For K2 Summit Production Client or K2 Solo Media Server, if you have not already done so, disable (unlock) the write filter.
- Stop all media access on K2 systems.
- Shut down all applications on K2 systems.

## Configure SNFS default.cfg file on stand-alone K2 system

In this task you open the media file system (SNFS) configuration file and verify/modify settings.

Do not do this task if:

- You have already modified the configuration file with the required settings.

Do this task if:

- The configuration file does not have the required settings.

Prerequisites for this task are as follows:

- K2 systems must be offline

You can verify and, if necessary, modify the media file system (SNFS) configuration file and still keep your media file system intact if you carefully follow the steps in this procedure.

As an alternative to manually modifying the configuration file, if you need to make a new file system after upgrading K2 software, the required values are set automatically by the upgraded version of Storage Utility.

This task applies to the following devices:

- K2 Solo Media Servers and stand-alone K2 Summit Production Clients. This includes internal storage and direct-connect storage K2 Summit Production Clients.

**NOTE: Make sure the write filter is disabled.**

1. On a stand-alone K2 system, using Notepad, open the media file system (SNFS) configuration file:

On a stand-alone K2 system, the configuration file can be either `C:\SNFS\config\default.cfg` or `C:\SNFS\config\gvfs_hostname.cfg`, where `hostname` is the name of the K2 system.

2. On a stand-alone K2 system, verify, and if necessary modify, settings for required values as follows:

```
# *****
# A global section for defining file system-wide parameters
# *****
GlobalSuperUser Yes
.
.
.
.
.

InodeDeleteMax 1000
.
ReservedSpace No
```

3. Close, and if necessary save, the SNFS configuration file.

If you made changes, the K2 system must be restarted for the changes to take effect.

The restart later in this upgrade procedure is sufficient to put the changes into effect.

## Uninstall K2 Dyno Server software

Do not do this task if:

- The K2 Summit Production Client is not controlled by a K2 Dyno Controller.

Do this task if:

- The K2 Summit Production Client is controlled by a K2 Dyno Controller and you are upgrading the K2 Dyno Controller from a 1.x version to a 2.x or higher version of Dyno software.

If you have not already done so, disable the write filter on the K2 Summit Production Client or K2 Solo Media Server.

On the K2 Summit Production Client or K2 Solo Media Server, use the Windows **Add/Remove Programs** control panel and uninstall K2 Dyno Server software.

The display name of the software is **K2 Dyno**.

The K2 Dyno Server software is now uninstalled, and it should not be re-installed on the K2 Summit/Solo system. It is not required for control by a K2 Dyno Controller at version 2.x or higher.

Do not restart the K2 Summit Production Client or K2 Solo Media Server.

**Related Topics**

[Upgrade K2 Summit/Solo for use with K2 Dyno Controller](#)

[About K2 Dyno software](#)

## Prepare SiteConfig for software deployment to stand-alone K2 systems

Do the following to prepare SiteConfig for the software upgrade.

1. Make the following files accessible to the SiteConfig control point PC:
  - K2 Summit Client Standalone software installation (\*.cab) file.
  - Summit SNFS software installation (\*.cab) file.
2. If a newer version of SiteConfig is available for upgrade and you have not yet upgraded SiteConfig, do the following:
  - a) From Windows Add/Remove programs, uninstall the current version of SiteConfig from the control point PC.
  - b) Install the new version of SiteConfig on the control point PC.
3. If not already present in the SiteConfig system description, configure deployment groups as follows:
  - A deployment group that contains your stand-alone K2 systems
  - A deployment group that contains your control point PC

## Check all currently installed software on stand-alone K2 systems

Prerequisites for this task are as follows:

- The device is assigned in the SiteConfig system description and network connectivity is present.
- SiteConfig is able to log in to the device using the username/password credentials assigned to the device.
- The SiteConfig PC does not have a network drive mapped to an administrative share (such as C\$) on a device on which you are checking software.

Do the following steps on the stand-alone K2 systems that you are upgrading.

1. In the **Software Deployment | Deployment Groups** tree view, right-click the top-most node for the group or any individual device and select **Check Software**.

**NOTE:** *If you have access problems, verify that the administrator account on the device has credentials as currently configured in SiteConfig.*

The Check Software dialog box appears. SiteConfig searches for software on the selected device or devices and gathers information. Progress is reported.

2. When the check is complete, close the Check Software dialog box.

An updated list of all currently installed software is displayed in the **Software Deployment | Devices | Installed Software** list view. If software is a SiteConfig managed software package, information is displayed in the Managed Package and Deployment Group columns.

## Add software package to deployment group for stand-alone K2 systems

Prerequisites for this task are as follows:

- You can access the software package file or files from the SiteConfig control point PC.
- The stand-alone K2 systems to which you are deploying software are in a deployment group.

Use the following procedure to add one or more software packages to the deployment group that contains your stand-alone K2 systems. For this release of K2 software, identify and add software installation files as follows:

Software	File name
K2 Client software	<i>GrassValleyK2SummitStandalone_8.1.x.xxxx.cab</i>
SNFS software	<i>SNFS_Summit_3.5.3.b27171.cab</i>

1. In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
2. Click the **Add** button.  
The Add Package(s) dialog box opens.
3. Do one of the following to select the software package:
  - Select from the list of packages then click **OK**.
  - Click **Browse**, browse to and select the package, then click **Open**.
4. If one or more EULAs are displayed, accept them to proceed. If you do not accept a EULA, the associated software is not assigned to the deployment group.  
SiteConfig adds the package to the deployment group.

The package appears in the Managed Packages list for the selected deployment group. SiteConfig creates new software deployment tasks for the package and displays them in the Tasks list view.

## Unlock K2 Summit Production Clients or K2 Solo Media Servers

This task disables the write filter on one or more K2 Summit Production Clients or K2 Solo Media Servers.

Prerequisites for this task are as follows:

- The device or all the devices in the group are communicating correctly in SiteConfig. This is indicated by the green star icon overlay.
- The device or all the devices in the group are currently locked. This is indicated by the gray lock icon overlay.

1. If you have not already done so, stop all media access on the K2 systems. This includes record, play, and transfer operations.
2. In either the **Network Configuration | Devices** tree view or the **Software Deployment | Deployment Groups** tree view, identify the device or the group of devices that you intend to unlock.
3. Right-click the device or the group and select **Unlock**.  
A "...may require restart..." message appears.

4. Click **Yes** to allow SiteConfig to restart the device or devices.  
The Set Administrative Credentials dialog box opens.
5. Enter a username and password with administrator level privileges on the device or devices and click **OK**.  
The Unlocking Devices window opens and displays progress.
6. When the Unlocking Devices window reports that the unlock process completed successfully, click **Close**.

The device or devices are now unlocked. For K2 Summit Production Clients, this also disables the write filter, which enforces a restart.

## Upgrade software on stand-alone K2 systems

Prerequisites for this task are as follows:

- The devices that you are upgrading are in a deployment group.
- For the software you are upgrading, you have added a newer version of that managed software package to the deployment group.
- You have recently done the SiteConfig "Check Software" operation on the devices you are upgrading.
- For the K2 Summit Production Client or K2 Solo Media Server, the write filter is disabled (unlocked).
- **NOTE: On a K2 system, if a SNFS version lower than 3.0 is installed, do not uninstall using SiteConfig. You must manually uninstall using a special batch file. Follow instructions in the release notes for your current version of K2 software.**

If you are upgrading multiple software components for which there is a required sequence, you must check and uncheck tasks and run multiple deployment sessions to control the sequence. For some software components, SiteConfig aids you by enforcing dependencies. For each individual software component, SiteConfig enforces an uninstall of the current version of software before installing the upgrade version. SiteConfig provides uninstall deployment tasks and install deployment tasks to indicate the taskflow. SiteConfig can do the uninstall/install in a single deployment session.

1. In the **Software Deployment | Deployment Groups** tree view, select the device or the group of devices to which you are deploying software.  
The corresponding software deployment tasks are displayed in the Tasks list view.
2. For the software you are deploying, select the **Deploy** check box in the row for the uninstall task.

- For the software you are installing, select the **Deploy** check box in the row for the install task.

For upgrading stand-alone K2 systems to this release, configure **Deploy** check boxes as follows:

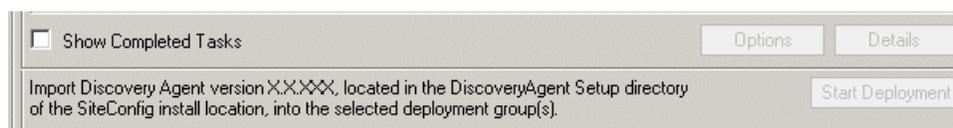
Deploy	Managed Package	Action
✓	GrassValleyK2SummitStandalone xxxx.xxxx	Uninstall
✓	GrassValleyK2SummitStandalone 8.1.x.xxxx	Install
✓	WRegMon_SummitStandalone x.x.x	Install (there is no uninstall task for this software)

Also, when upgrading SNFS, configure deployment tasks to upgrade (uninstall/install) SNFS. Deploy the following tasks at the same time:

Deploy	Managed Package	Action
✓	SNFS Summit xxxxxx	Uninstall
✓	SNFS Summit 3.5.3.b27171	Install

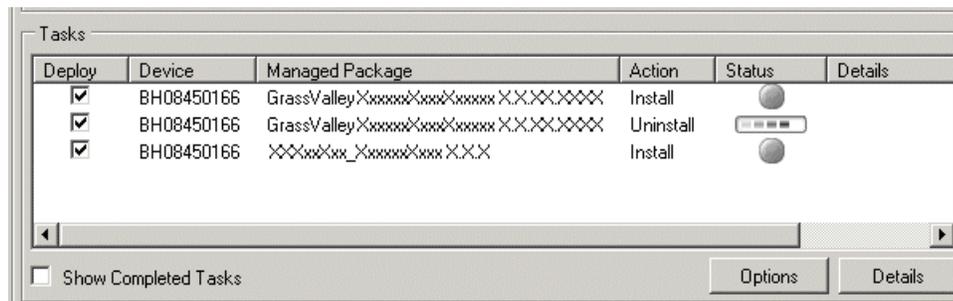
**NOTE:** *If there are dependencies, SiteConfig can enforce that some tasks be deployed together.*

- Check the area next to the Start Deployment button for a message.



If a message instructs you to upgrade the Discovery Agent, on the control point PC go to the directory to which SiteConfig is installed, find the *DiscoveryAgent\_x.x.x.x.cab* file, add it to the deployment group, and deploy the Discovery Agent software as well.

- Click the **Start Deployment** button.



Deployment tasks run and software is uninstalled. Progress is reported and next steps are indicated in both the Status and Details columns. If an error appears regarding prerequisite software, install the prerequisite files on the control point PC and then repeat this step.

When upgrading both K2 and SNFS software, SiteConfig uninstalls both in the proper sequence.

- When the Status or Details columns indicate next steps, identify the software in the row, then do one of the following:
  - For SNFS software, when Details displays a **Restart required** link, click the link and when prompted "...are you sure...", click **Yes**. After this restart, continue with other restarts as indicated.
  - For K2 software, if the version from which you are upgrading is 8.0 or higher, when Details displays a **Restart required** link, click the link and when prompted "...are you sure...", click **Yes**.
- Monitor progress as indicated by both the Status and Details column. When finished, the Status column indicates complete.

## Upgrading the Discovery Agent

Do this task if SiteConfig does not prompt you to upgrade to the compatible version of the Discovery Agent when you deploy software.

Prerequisites for this task are as follows:

- Your devices are in one or more deployment groups
  - A check software operation has been performed either on the device or the deployment group that you are upgrading
- In the **Software Deployment | Deployment Groups** tree view, select a deployment group.
  - Click **Add Package**
  - Click **Browse** in the add package dialog and browse to the Discovery Agent Setup folder under your SiteConfig install location on the SiteConfig PC.
  - Select the required *DiscoveryAgent\_<version>.cab* file and click **Open**.

SiteConfig generates deployment tasks to uninstall the existing version and installs the selected version and enables the **Start Deployment** button.

5. Check the uninstall and install deploy tasks for the Discovery Agent and click the **Start Deployment** button when you are ready to deploy.  
SiteConfig runs the deployment tasks.

## Install required Windows updates

Do this task if:

- You have a K2 Summit, K2 Summit 3G, K2 Solo, K2 Solo 3G system with Windows XP.
- You wish to install Windows XP Security Updates.

Before doing this task, obtain a new 16GB CompactFlash Drive (GV part number 050-3493-00) from Grass Valley Service at <http://www.grassvalley.com/support>.

**NOTE: Do not install general Windows updates as available from Microsoft. Update only as directed by Grass Valley.**

**Refer to "K2 Summit Production Client Service Manual" to accomplish the steps in this procedure.**

1. Download Windows update batch files from Grass Valley website; *RunUpdates.zip*, *RunUpdates2011.zip*, *RunUpdates2012.zip*, and *RunUpdates2013Q1.zip*.
2. Save the batch files to a USB drive.
3. Create a recovery image of the K2 Summit/Solo system and save the image to a USB drive.  
This is a system-specific recovery image for restoring that specific K2 Summit/Solo system only.
4. If you have a K2 Summit 3G or K2 Solo 3G, skip steps 5 and 6, and proceed to step 7.
5. Remove the CompactFlash boot media to replace the existing 4GB or 8GB CompactFlash drive with the new 16GB CompactFlash drive.
6. Restore from the system-specific recovery image you created in step 3.  
When using Acronis, select **No Free Space** on the Restored Partition Size page. Refer to the related topic in "K2 Summit Production Client Service Manual".
7. Turn off the write filter, then restart.
8. From the USB drive, extract the contents of the *RunUpdates.zip* file into the *C:\Temp* directory.  
This creates a folder named *RunUpdates* that includes Windows update files.
9. Within the *RunUpdates* folder, run *RunUpdates.exe*.  
A command shell starts.
10. When prompted, enter *Y* to start the update process.  
For each of the security updates, the shell displays a line showing the update installing. A window showing the progress of an update opens and then closes when complete. The shell then updates with the completion status of the update.
11. If you interrupt the Windows update process, run *RunUpdates.exe* to start it again. Updating continues from the point of interruption.
12. When updates complete and the shell displays the prompt **Do you want to reboot now?**, enter *Y* to restart.
13. Proceed to the *RunUpdates2011.zip* batch file.

14. From the USB drive, extract the contents of the *RunUpdates2011.zip* file into the *C:\Temp* directory.  
This creates a folder named *RunUpdates2011* that includes Windows update files.
15. Within the *RunUpdates2011* folder, run *RunUpdates.exe*.  
A command shell starts.
16. If the batch script stalls, press **Ctrl + C** at the command prompt to stop the process and restart *RunUpdates.exe* from *RunUpdates2011* folder until all files are successfully processed.  
It takes about one hour to finish the updates.
17. When updates complete and the shell displays the prompt **Do you want to reboot now?**, enter *Y* to restart.
18. Proceed to the *RunUpdates2012.zip* batch file.
19. From the USB drive, extract the contents of the *RunUpdates2012.zip* file into the *C:\Temp* directory.  
This creates a folder named *RunUpdates2012* that includes Windows update files.
20. Within the *RunUpdates2012* folder, run *RunUpdates.exe*.  
A command shell starts.  
***NOTE: RunUpdates2012 batch script will automatically reboot the system in the middle of the updates***
21. Restart the batch script to finish the updates.
22. When updates complete and the shell displays the prompt **Do you want to reboot now?**, enter *Y* to restart.
23. If the batch script stalls, press **Ctrl + C** at the command prompt to stop the process and restart *RunUpdates.exe* from *RunUpdates2012* folder until all files are successfully processed.  
It takes about one hour to finish the updates.
24. Proceed to the *RunUpdates2013Q1.zip* batch file.
25. From the USB drive, extract the contents of the *RunUpdates2013Q1.zip* file into the *C:\Temp* directory.  
This creates a folder named *RunUpdates2013Q1* that includes Windows update files.
26. Within the *RunUpdates2013Q1* folder, run *RunUpdates.exe*.  
A command shell starts.
27. If the batch script stalls, press **Ctrl + C** at the command prompt to stop the process and restart *RunUpdates.exe* from *RunUpdates2013Q1* folder until all files are successfully processed.  
It takes about one hour to finish the updates.

28. When updates complete and the shell displays the prompt **Do you want to reboot now?**, enter Y to restart.

The installed security files from each RunUpdates batch are now located in the *Installed* folder in *C:\temp* folder.

- *RunUpdates* folder: *C:\temp\RunUpdates\Installed\*.
- *RunUpdates2011* folder: *C:\temp\RunUpdates2011\Installed\*.
- *RunUpdates2012* folder: *C:\temp\RunUpdates2012\Installed\*.
- *RunUpdates2013Q1* folder: *C:\temp\RunUpdates2013Q1\Installed\*.

29. To recover some disk space, you may delete the *.zip files*, *extracted* folders, and the *Installed* folder.

## Upgrade disk drive firmware on stand-alone K2 system

Do not do this task if:

- A K2 system with disk drive firmware already at a compatible version, as listed in compatibility specifications.

Do this task if:

- A K2 system with disk drive firmware that you need to upgrade, as listed in compatibility specifications.

For internal storage K2 Summit/Solo systems, find compatibility specifications at [Compatible K2 Summit/Solo components](#) on page 19. For a K2 Summit Production Client with direct-connect storage, find compatibility specifications at [Compatible K2 RAID components](#) on page 24.

**NOTE: The disk drives are upgraded one at a time which can take as long as 2 minutes per drive. Take this into consideration when scheduling the upgrade.**

1. Open AppCenter Workstation, either on the local K2 system or on the control point PC and logon.  
Make sure you logon to AppCenter with appropriate privileges, as this logon is passed to Storage Utility. Administrator-level permission is necessary for most Storage Utility operations. If you log in with user-level permissions, the Storage Utility menu item is disabled.
2. If you are running AppCenter from a control point PC and you have channels from multiple K2 systems in your channel suite, select a channel from the stand-alone K2 system whose storage you intend to configure with Storage Utility. This is important as Storage Utility automatically connects to the K2 system that hosts the currently selected channel.  
**NOTE: Make sure you are connecting to a stand-alone K2 system. You should never connect Storage Utility directly to a K2 system that uses shared (SAN) storage.**
3. From the AppCenter **System** menu, select **Storage Utility**.  
Storage Utility opens.
4. If you are connecting from a control point PC, you should verify that you are connected to the correct K2 system. To verify this, use the Identify feature to flash the disks on the K2 system.
5. Select a disk drive icon in the Storage Utility tree view, then note the firmware version in drive properties reported in the right-hand pane. Proceed if you need to download disk drive firmware.

6. Right-click a disk in the tree view, then select **Advanced | Download Disk Firmware** in the context menu.
7. If online, messages appear "...offline mode now?" and "...continue?". Click **Yes** to put the K2 system in offline mode.

AppCenter channels go offline. The Open File dialog box opens.
8. In the Open File dialog box browse to the directory and file as listed in compatibility tables earlier in these release notes. You must select the correct file for the device, storage type, and drive size/type.
9. Click **OK**.

For internal drives, watch the lights on the drive to which you are downloading firmware. The lights flash as firmware loads. Wait until the lights have completed their flashing pattern. This can take several minutes.

The Progress Report window appears showing the disk firmware download task and the percentage completion.
10. Repeat this procedure on each drive.
11. When finished, exit Storage Utility.
12. Put AppCenter channels back online.
13. Restart.

## Configure RTIO

In this task you set the Real Time Input/Output (RTIO) value for the SNFS file system to support K2 software features. This setting is required for all stand-alone K2 systems.

Do not do this task if:

- A shared storage (SAN client) K2 system.
- A stand-alone K2 system that was installed new with K2 software version 7.2 or higher. On these systems the RTIO setting is already at the required value.
- A stand-alone K2 system on which you have already set RTIO to the required value.

Do this task if:

- The K2 software from which you are upgrading is version 7.1.x or lower.
- — OR —
- You are not sure if the RTIO setting is already at the required value.

Prerequisites for this task are as follows:

- K2 systems must be offline

In this task you manually modify the SNFS configuration file. You can do this and still keep your media file system intact if you carefully follow the steps in this procedure.

If you need to make a new file system after upgrading K2 software, the values are set automatically by the upgraded version of Storage Utility.

This task applies to the following devices:

- Stand-alone K2 Summit Production Clients. This includes internal storage and direct-connect storage K2 Summit Production Clients.

- K2 Solo Media Server
1. Open Storage Utility on the K2 Solo Media Server or stand-alone K2 Summit Production Client.
  2. In Storage Utility click **Tools | Modify File System**.
  3. When prompted "...offline mode now?" click **Yes**.
  4. When prompted "...continue?" click **Yes**.  
The Modify File System window opens and displays the text of the configuration file.
  5. In the text of the configuration file, identify the RTIO setting as in the following example:

```
# *****
# A stripe section for defining stripe groups.
# *****
[StripeGroup VStripe]
.
.
.
Rtios 370
.
```

If necessary modify the value as follows:

- On a K2 Summit Production Client the required RTIO value is 370.
  - On a K2 Solo Media Server with standard Hard Disk Drives (HDD) the required RTIO value is 170.:
  - On a K2 Solo Media Server with optional Solid State Drives (SSD) or on a K2 Summit Production Client the required RTIO value is 250.
  - On a K2 Solo Media Server with 300G 10K Hitachi the required RTIO value is 200.
6. Do one of the following:
    - If you modified the configuration file, click **Modify** and when prompted "...restarted now" click **OK**. The K2 system restarts.
    - If you did not modify the configuration file, click **Cancel** and then exit Storage Utility. When prompted "...back to online mode?" click **Yes**.

## Reset Capture Services

Do not do this task if:

- You do not use any of the K2 Capture Services.

Do this task if:

- You are using one or more K2 Capture Services, such HotBin, Pathfire, DG, XML Import, Export, P2, etc

Do this task on the K2 system running your K2 Capture Service, which is the K2 system that receives the media to be imported into K2 storage. This can be a K2 Solo Media Server, a stand-alone K2 Summit Production Client, or the K2 Media Server with the role of primary FTP server on a K2 SAN.

When you configure a K2 Capture Service for the first time, the service is set to startup type Automatic. However, if you upgrade or otherwise re-install your K2 System Software, the service

is re-set to startup type Manual. Therefore, you must re-configure the service after K2 System Software upgrade/ reinstall in order to set the startup type back to Automatic.

1. From the **Start** menu, access the **Programs** menu and select **Grass Valley | K2 Capture Services**.  
On a K2 Summit/Solo system, if the write filter is enabled, a message appears that informs you about the write filter and prompts you to restart. Restart as prompted, then repeat this step.  
The K2 Capture Services utility dialog box is displayed.

2. Click **Apply**.

On a K2 Summit/Solo system, a message appears that informs you about the write filter and prompts you to restart. Click **OK** and the K2 Summit/Solo system restarts.

For import capture services, the service checks the source directory for files. If files are present, the service moves them to the Archive sub-directory. It does not import the files into the destination bin on the K2 system.

## Lock K2 Summit Production Clients

This task enables the write filter on a K2 Summit Production Client or on a group of K2 Summit Production Clients.

Prerequisites for this task are as follows:

- The device or all the devices in the group are communicating correctly in SiteConfig. This is indicated by the green star icon overlay.
  - The device or all the devices in the group are currently unlocked. This is indicated by the red lock icon overlay.
1. In the **Network Configuration | Devices** tree view or the **Software Deployment | Deployment Groups** tree view, identify the device or the group of devices that you intend to lock.
  2. Right-click the device or the group and select **Lock**.  
A "...may require restart..." message appears.
  3. Click **Yes** to allow SiteConfig to restart the device or devices.  
The Locking Devices window opens and displays progress.
  4. When the Locking Devices window reports that the lock process completed successfully, click **Close**.

The device or devices are now locked. For K2 Summit/Solo, this also enables the write filter, which enforces the restart.

## Install MPEG-2/AVC-Intra field kit

If you are installing an MPEG-2 or AVC-Intra field kit upgrade on one or more of your K2 Summit Production Clients or K2 Solo Media Servers, do so now. Follow the procedure in the Field Kit Upgrade Instructions document that you received with the field kit.

## Make recovery images

After you have upgraded software as instructed in these procedures and verified that your system is working properly, you should always make a recovery image of each of your upgraded computers. Use a sequence of tasks similar to those you followed for upgrading software so that as you take systems offline you manage redundancy, servers, and clients, as appropriate for your system.

Refer to the Grass Valley product's *Service Manual* for recovery image procedures.

## Deploy control point PC software

Use SiteConfig to upgrade control point software on the K2 control point PC. In most cases, the K2 control point PC is also the SiteConfig control point PC, so you are in effect using SiteConfig to upgrade software on its own local system.

For this release of K2 software, the install task identifies the control point software in the Managed Package column as follows:

- GrassValleyControlPoint 8.1.x.xxxx

The software deployment process for the control point PC is similar to that used to upgrade software on other K2 devices. Use similar procedures and adjust accordingly to do the following:

1. Add the K2 control point software package to the deployment group that contains the control point PC.
2. Check software on the control point PC.
3. Configure and run deployment tasks to upgrade software.

## Upgrading stand-alone K2 systems without SiteConfig

This section contains the tasks for upgrading stand-alone K2 systems to this release of K2 software.

With these instructions you go to each local K2 system and upgrade software using locally connected keyboard, monitor, and mouse. Work through the tasks sequentially to complete the upgrade.

**NOTE:** *These upgrade instructions assume that on your K2 Summit/Solo system, the current K2 software is at version 8.x or higher. If on a K2 Summit system the current software is at a version lower than 8.x, you must upgrade it using a Grass Valley Field Kit, which includes a disk image and hardware. K2 Solo systems are available with 8.x software only as shipped from Grass Valley.*

## Make recovery images

Do not do this task if:

- You previously made a recovery image at the current software version for each computer you are upgrading.

Do this task if:

- You do not have a recovery image at the current software version for one or more of the computers you are upgrading.

The recommended procedure is to make a recovery image immediately after a software upgrade. If you neglected to do this when you last upgraded software you should make the recovery image now, before upgrading to the new version.

Refer to the Grass Valley product's *Service Manual* for recovery image procedures.

**△ CAUTION:** *If you upgrade and then decide you do not want to stay with this version of K2 system software, you must use the recovery disk image process to downgrade to your previous version.*

## Prepare for K2 system upgrade

Before upgrading K2 systems, do the following:

- Procure the software installation files for this release via the appropriate distribution method, such as download, USB Recovery Flash Drive, network drive, or external drive.
- Start up the K2 systems you are upgrading, if they are not already started.
- For K2 Summit Production Client or K2 Solo Media Server, if you have not already done so, disable (unlock) the write filter.
- Stop all media access on K2 systems.
- Shut down all applications on K2 systems.

## Disable write filter

Prerequisite:

- K2 software must be installed on the K2 Summit/Solo system.
1. If you have not already done so, log on to the K2 Summit/Solo system with Windows administrator privileges.
  2. From the Windows desktop, click **Start | All Programs | Grass Valley | Write Filter Utility**.  
FBWF Manager opens.
  3. Under Filter Settings, set Filter to **Disable**.  
Do not modify other settings.
  4. Click **OK**.
  5. When prompted, restart the K2 system.

## Configure SNFS default.cfg file on stand-alone K2 system

In this task you open the media file system (SNFS) configuration file and verify/modify settings.

Do not do this task if:

- You have already modified the configuration file with the required settings.

Do this task if:

- The configuration file does not have the required settings.

Prerequisites for this task are as follows:

- K2 systems must be offline

You can verify and, if necessary, modify the media file system (SNFS) configuration file and still keep your media file system intact if you carefully follow the steps in this procedure.

As an alternative to manually modifying the configuration file, if you need to make a new file system after upgrading K2 software, the required values are set automatically by the upgraded version of Storage Utility.

This task applies to the following devices:

- K2 Solo Media Servers and stand-alone K2 Summit Production Clients. This includes internal storage and direct-connect storage K2 Summit Production Clients.

**NOTE: Make sure the write filter is disabled.**

1. On a stand-alone K2 system, using Notepad, open the media file system (SNFS) configuration file:

On a stand-alone K2 system, the configuration file can be either `C:\SNFS\config\default.cfg` or `C:\SNFS\config\gvfs_hostname.cfg`, where `hostname` is the name of the K2 system.

2. On a stand-alone K2 system, verify, and if necessary modify, settings for required values as follows:

```
# *****
# A global section for defining file system-wide parameters
# *****
GlobalSuperUser Yes
.
.
.
.
.

InodeDeleteMax 1000
.
ReservedSpace No
```

3. Close, and if necessary save, the SNFS configuration file.

If you made changes, the K2 system must be restarted for the changes to take effect.

The restart later in this upgrade procedure is sufficient to put the changes into effect.

## Uninstall K2 software from stand-alone K2 system

1. Disable the write filter, if not already disabled.
2. Open the Windows **Add/Remove Programs** control panel.
3. Select **GrassValleyK2Client**. and click **Remove**.
4. When prompted "Are you sure...?", click **Yes**.
5. When prompted to restart, do not restart.

While a restart is required after installing K2 Client software, you can delay the restart until after other tasks are complete.

6. On a K2 Summit Production Client or K2 Solo Media Server, disable the write filter.  
Disabling the write filter at this point keeps it disabled after the required restart. This is helpful because it must be disabled in order to uninstall or install software, which you will be doing after the restart.
7. Manage the required restart as follows:
  - Restart now.

### Uninstall SNFS from K2 client

Do not do this task if:

- The desired version of SNFS is already installed and the installation (including required restarts) is complete.

Do this task if:

- A SNFS version lower than 3.5.3.b27171 is currently installed

If you have not already done so, disable the write filter on the K2 Summit Production Client or K2 Solo Media Server.

1. Make sure you are logged in with an administrator account.
2. Use the Windows **Add/Remove Programs** control panel and uninstall SNFS.
3. Disable the write filter.  
Disabling the write filter at this point keeps it disabled after the required restart. This is helpful because it must be disabled in order to install software, which you will be doing after the restart.
4. Restart using the Windows operating system restart procedure.

### Install K2 software

Prerequisites for this task are as follows:

- If you uninstalled the previous version of K2 software, you must restart the K2 client at least once before installing the new version of K2 software.

1. Log in with a local administrator account. This is required to support K2 System Software licensing.

***NOTE: When installing K2 system software, you must be logged in with a local administrator account. Do not install software using a domain account.***

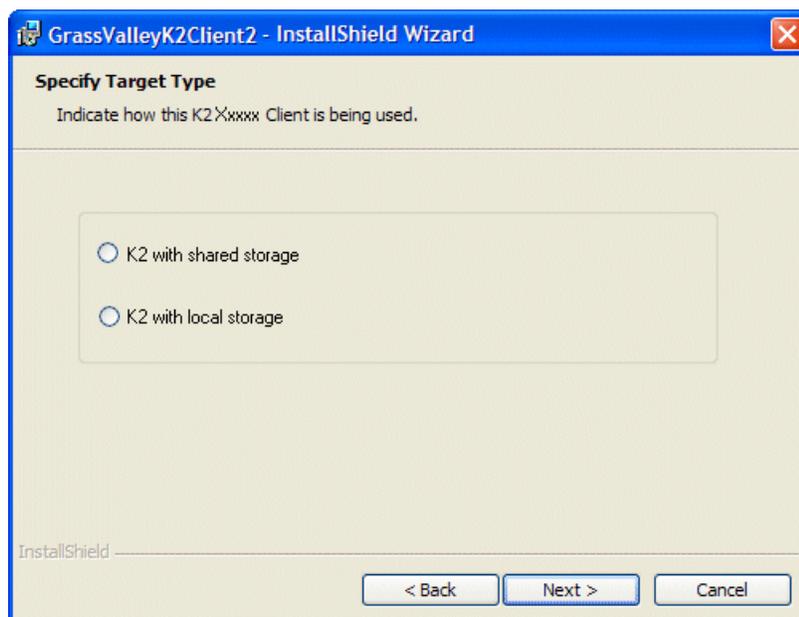
2. Disable the write filter, if not already disabled.
3. If installation files are on a connected external USB drive, copy the installation files to the local drive before proceeding.
4. Access the installation files.

## 5. Locate and open the following file:

For K2 Summit Production Client or K2 Solo Media Server — *K2SummitClient.exe*

- If a message appears informing you that you must install writer filter and/or restart, click **OK** to restart. If an external USB drive is currently connected, disconnect it before startup processes begin. Then repeat previous steps as necessary to run the install program again before continuing with the next step in this procedure.
- If no message appears, the install wizard opens. Continue with the next step in this procedure.

## 6. Follow the install wizard onscreen instructions, and work through each page.



## 7. When you arrive at the Specify Target Type page, select the option as follows:

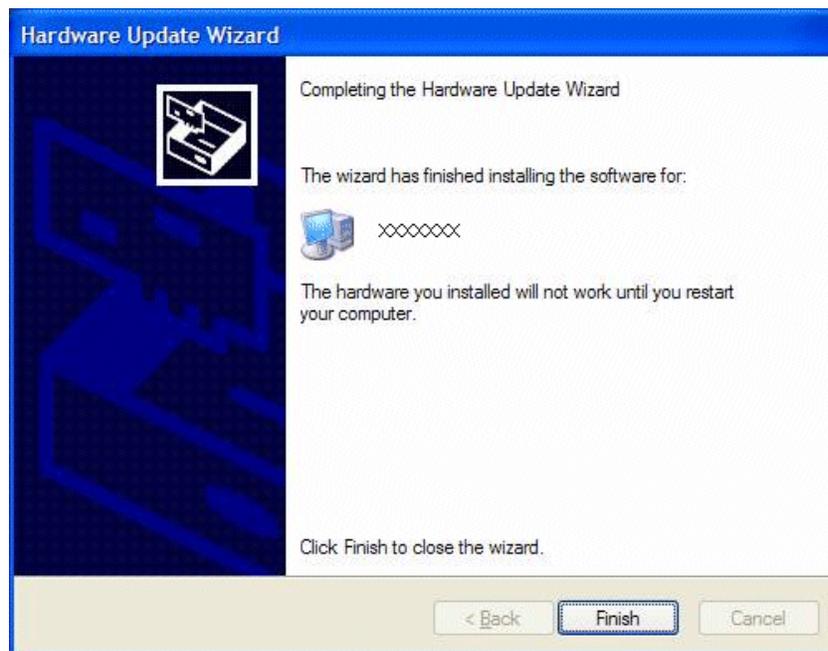
Option	Description
<b>K2 with local storage</b>	For installing on an internal storage K2 system or on a direct-connect storage K2 system.

8. Depending on the state of the system when upgrading, you might see one or more of the following screens or messages as you work through the installation wizard. Proceed as instructed, and then continue with this procedure:
  - a) If one or more messages appear referring to "...has not passed Windows logo testing...", you can safely continue. This is a normal part of the upgrade.



Click **Yes** or Continue... to allow the installation to progress.

- b) If installation progress stops after about a minute and does not proceed, look in the Windows taskbar for a Hardware Update Wizard window that has opened.



Click **Finish** on the Hardware Update Wizard to continue installation. If multiple Hardware Update Wizards open, finish them similarly.

9. Click **Next** and **Finish** to complete the installation.
10. When prompted, proceed as follows:
  - Disable the write filter.
 

Disabling the write filter before the restart keeps it disabled after restart. This is helpful because it must be disabled in order to install software, which you will be doing after the restart.
  - If prompted to restart, do not restart. The restart after you install SNFS in a later task is sufficient.

## Install SNFS on stand-alone K2 system

Prerequisites for this task are as follows:

- Before installing a new version of SNFS software, make sure that the computer has been restarted at least once since the previous version of SNFS software was uninstalled.
1. Access the installation files.
  2. Locate and open the file for your system:
 

Use the 32-bit (x86) installation files for a K2 Summit system.

File	Description
<i>gvSnfs353SetupSummit.bat</i>	For K2 Summit/Solo system

The command window appears. After a pause, messages confirm setup complete.

3. Press any key to proceed.
4. Restart media file system services as follows:
  - a) Click **Start | Programs | SNFS File System | Services Stop**.
  - b) Click **Start | Programs | SNFS File System | Services Start**.
5. Restart the computer using the Windows operating system restart procedure.

## Verify upgraded software

When the K2 client starts up, you can verify that the correct versions of software are installed as follows:

1. Log on to AppCenter.
2. In AppCenter click **Help | About**.
 

The About dialog box opens.
3. Identify versions as follows

System Version	8.1.xxx	These should both report the same version number. This is the K2 System Software version number.
RTS Version	8.1.xxx	
Media File System	3.5.3.b27171	This is the SNFS version.

## Install required Windows updates

Do this task if:

- You have a K2 Summit, K2 Summit 3G, K2 Solo, K2 Solo 3G system with Windows XP.
- You wish to install Windows XP Security Updates.

Before doing this task, obtain a new 16GB CompactFlash Drive (GV part number 050-3493-00) from Grass Valley Service at <http://www.grassvalley.com/support>.

**NOTE: Do not install general Windows updates as available from Microsoft. Update only as directed by Grass Valley.**

**Refer to "K2 Summit Production Client Service Manual" to accomplish the steps in this procedure.**

1. Download Windows update batch files from Grass Valley website; *RunUpdates.zip*, *RunUpdates2011.zip*, *RunUpdates2012.zip*, and *RunUpdates2013Q1.zip*.
2. Save the batch files to a USB drive.
3. Create a recovery image of the K2 Summit/Solo system and save the image to a USB drive.  
This is a system-specific recovery image for restoring that specific K2 Summit/Solo system only.
4. If you have a K2 Summit 3G or K2 Solo 3G, skip steps 5 and 6, and proceed to step 7.
5. Remove the CompactFlash boot media to replace the existing 4GB or 8GB CompactFlash drive with the new 16GB CompactFlash drive.
6. Restore from the system-specific recovery image you created in step 3.  
When using Acronis, select **No Free Space** on the Restored Partition Size page. Refer to the related topic in "K2 Summit Production Client Service Manual".
7. Turn off the write filter, then restart.
8. From the USB drive, extract the contents of the *RunUpdates.zip* file into the *C:\Temp* directory.  
This creates a folder named *RunUpdates* that includes Windows update files.
9. Within the *RunUpdates* folder, run *RunUpdates.exe*.  
A command shell starts.
10. When prompted, enter *Y* to start the update process.  
For each of the security updates, the shell displays a line showing the update installing. A window showing the progress of an update opens and then closes when complete. The shell then updates with the completion status of the update.
11. If you interrupt the Windows update process, run *RunUpdates.exe* to start it again. Updating continues from the point of interruption.
12. When updates complete and the shell displays the prompt **Do you want to reboot now?**, enter *Y* to restart.
13. Proceed to the *RunUpdates2011.zip* batch file.
14. From the USB drive, extract the contents of the *RunUpdates2011.zip* file into the *C:\Temp* directory.  
This creates a folder named *RunUpdates2011* that includes Windows update files.

15. Within the *RunUpdates2011* folder, run *RunUpdates.exe*.  
A command shell starts.
16. If the batch script stalls, press **Ctrl + C** at the command prompt to stop the process and restart *RunUpdates.exe* from *RunUpdates2011* folder until all files are successfully processed.  
It takes about one hour to finish the updates.
17. When updates complete and the shell displays the prompt **Do you want to reboot now?**, enter **Y** to restart.
18. Proceed to the *RunUpdates2012.zip* batch file.
19. From the USB drive, extract the contents of the *RunUpdates2012.zip* file into the *C:\Temp* directory.  
This creates a folder named *RunUpdates2012* that includes Windows update files.
20. Within the *RunUpdates2012* folder, run *RunUpdates.exe*.  
A command shell starts.  
**NOTE: *RunUpdates2012* batch script will automatically reboot the system in the middle of the updates**
21. Restart the batch script to finish the updates.
22. When updates complete and the shell displays the prompt **Do you want to reboot now?**, enter **Y** to restart.
23. If the batch script stalls, press **Ctrl + C** at the command prompt to stop the process and restart *RunUpdates.exe* from *RunUpdates2012* folder until all files are successfully processed.  
It takes about one hour to finish the updates.
24. Proceed to the *RunUpdates2013Q1.zip* batch file.
25. From the USB drive, extract the contents of the *RunUpdates2013Q1.zip* file into the *C:\Temp* directory.  
This creates a folder named *RunUpdates2013Q1* that includes Windows update files.
26. Within the *RunUpdates2013Q1* folder, run *RunUpdates.exe*.  
A command shell starts.
27. If the batch script stalls, press **Ctrl + C** at the command prompt to stop the process and restart *RunUpdates.exe* from *RunUpdates2013Q1* folder until all files are successfully processed.  
It takes about one hour to finish the updates.
28. When updates complete and the shell displays the prompt **Do you want to reboot now?**, enter **Y** to restart.  
The installed security files from each *RunUpdates* batch are now located in the *Installed* folder in *C:\temp* folder.
  - *RunUpdates* folder: *C:\temp\RunUpdates\Installed\*.
  - *RunUpdates2011* folder: *C:\temp\RunUpdates2011\Installed\*.
  - *RunUpdates2012* folder: *C:\temp\RunUpdates2012\Installed\*.
  - *RunUpdates2013Q1* folder: *C:\temp\RunUpdates2013Q1\Installed\*.
29. To recover some disk space, you may delete the *.zip files*, *extracted* folders, and the *Installed* folder.

## Upgrade disk drive firmware on stand-alone K2 system

Do not do this task if:

- A K2 system with disk drive firmware already at a compatible version, as listed in compatibility specifications.

Do this task if:

- A K2 system with disk drive firmware that you need to upgrade, as listed in compatibility specifications.

For internal storage K2 Summit/Solo systems, find compatibility specifications at [Compatible K2 Summit/Solo components](#) on page 19. For a K2 Summit Production Client with direct-connect storage, find compatibility specifications at [Compatible K2 RAID components](#) on page 24.

**NOTE:** *The disk drives are upgraded one at a time which can take as long as 2 minutes per drive. Take this into consideration when scheduling the upgrade.*

1. Open AppCenter Workstation, either on the local K2 system or on the control point PC and logon.  
Make sure you logon to AppCenter with appropriate privileges, as this logon is passed to Storage Utility. Administrator-level permission is necessary for most Storage Utility operations. If you log in with user-level permissions, the Storage Utility menu item is disabled.
2. If you are running AppCenter from a control point PC and you have channels from multiple K2 systems in your channel suite, select a channel from the stand-alone K2 system whose storage you intend to configure with Storage Utility. This is important as Storage Utility automatically connects to the K2 system that hosts the currently selected channel.

**NOTE:** *Make sure you are connecting to a stand-alone K2 system. You should never connect Storage Utility directly to a K2 system that uses shared (SAN) storage.*

3. From the AppCenter **System** menu, select **Storage Utility**.  
Storage Utility opens.
4. If you are connecting from a control point PC, you should verify that you are connected to the correct K2 system. To verify this, use the Identify feature to flash the disks on the K2 system.
5. Select a disk drive icon in the Storage Utility tree view, then note the firmware version in drive properties reported in the right-hand pane. Proceed if you need to download disk drive firmware.
6. Right-click a disk in the tree view, then select **Advanced | Download Disk Firmware** in the context menu.
7. If online, messages appear "...offline mode now?" and "...continue?". Click **Yes** to put the K2 system in offline mode.  
AppCenter channels go offline. The Open File dialog box opens.
8. In the Open File dialog box browse to the directory and file as listed in compatibility tables earlier in these release notes. You must select the correct file for the device, storage type, and drive size/type.

9. Click **OK**.

For internal drives, watch the lights on the drive to which you are downloading firmware. The lights flash as firmware loads. Wait until the lights have completed their flashing pattern. This can take several minutes.

The Progress Report window appears showing the disk firmware download task and the percentage completion.

10. Repeat this procedure on each drive.
11. When finished, exit Storage Utility.
12. Put AppCenter channels back online.
13. Restart.

## Configure RTIO

In this task you set the Real Time Input/Output (RTIO) value for the SNFS file system to support K2 software features. This setting is required for all stand-alone K2 systems.

Do not do this task if:

- A shared storage (SAN client) K2 system.
- A stand-alone K2 system that was installed new with K2 software version 7.2 or higher. On these systems the RTIO setting is already at the required value.
- A stand-alone K2 system on which you have already set RTIO to the required value.

Do this task if:

- The K2 software from which you are upgrading is version 7.1.x or lower.
- — OR —
- You are not sure if the RTIO setting is already at the required value.

Prerequisites for this task are as follows:

- K2 systems must be offline

In this task you manually modify the SNFS configuration file. You can do this and still keep your media file system intact if you carefully follow the steps in this procedure.

If you need to make a new file system after upgrading K2 software, the values are set automatically by the upgraded version of Storage Utility.

This task applies to the following devices:

- Stand-alone K2 Summit Production Clients. This includes internal storage and direct-connect storage K2 Summit Production Clients.
  - K2 Solo Media Server
1. Open Storage Utility on the K2 Solo Media Server or stand-alone K2 Summit Production Client.
  2. In Storage Utility click **Tools | Modify File System**.
  3. When prompted "...offline mode now?" click **Yes**.
  4. When prompted "...continue?" click **Yes**.

The Modify File System window opens and displays the text of the configuration file.

5. In the text of the configuration file, identify the RTIO setting as in the following example:

```
# *****  
# A stripe section for defining stripe groups.  
# *****  
[StripeGroup VStripe]  
. . .  
Rtios 370  
.
```

If necessary modify the value as follows:

- On a K2 Summit Production Client the required RTIO value is 370.
  - On a K2 Solo Media Server with standard Hard Disk Drives (HDD) the required RTIO value is 170.:
  - On a K2 Solo Media Server with optional Solid State Drives (SSD) or on a K2 Summit Production Client the required RTIO value is 250.
  - On a K2 Solo Media Server with 300G 10K Hitachi the required RTIO value is 200.
6. Do one of the following:
    - If you modified the configuration file, click **Modify** and when prompted "...restarted now" click **OK**. The K2 system restarts.
    - If you did not modify the configuration file, click **Cancel** and then exit Storage Utility. When prompted "...back to online mode?" click **Yes**.

## Reset Capture Services

Do not do this task if:

- You do not use any of the K2 Capture Services.

Do this task if:

- You are using one or more K2 Capture Services, such HotBin, Pathfire, DG, XML Import, Export, P2, etc

Do this task on the K2 system running your K2 Capture Service, which is the K2 system that receives the media to be imported into K2 storage. This can be a K2 Solo Media Server, a stand-alone K2 Summit Production Client, or the K2 Media Server with the role of primary FTP server on a K2 SAN.

When you configure a K2 Capture Service for the first time, the service is set to startup type Automatic. However, if you upgrade or otherwise re-install your K2 System Software, the service is re-set to startup type Manual. Therefore, you must re-configure the service after K2 System Software upgrade/ reinstall in order to set the startup type back to Automatic.

1. From the **Start** menu, access the **Programs** menu and select **Grass Valley | K2 Capture Services**.  
On a K2 Summit/Solo system, if the write filter is enabled, a message appears that informs you about the write filter and prompts you to restart. Restart as prompted, then repeat this step.  
The K2 Capture Services utility dialog box is displayed.

2. Click **Apply**.

On a K2 Summit/Solo system, a message appears that informs you about the write filter and prompts you to restart. Click **OK** and the K2 Summit/Solo system restarts.

For import capture services, the service checks the source directory for files. If files are present, the service moves them to the Archive sub-directory. It does not import the files into the destination bin on the K2 system.

## Upgrade remaining stand-alone K2 systems

For stand-alone storage K2 systems, repeat the previous steps to upgrade your remaining stand-alone storage K2 systems.

For the K2 Summit Production Client or K2 Solo Media Server, after you are done with the upgrade process, enable the write filter.

## Enable write filter

Prerequisite:

- K2 software must be installed on the K2 Summit/Solo system.
1. If you have not already done so, log on to the K2 Summit/Solo system with Windows administrator privileges.
  2. From the Windows desktop, click **Start | All Programs | Grass Valley | Write Filter Utility**. FBWF Manager opens.
  3. Under Filter Settings, set Filter to **Enable**.
  4. Under Protected Volumes, set C: to **Protected**.  
Do not modify other settings.
  5. Click **OK**.
  6. When prompted, restart the K2 system.

## Install MPEG-2/AVC-Intra field kit

If you are installing an MPEG-2 or AVC-Intra field kit upgrade on one or more of your K2 Summit Production Clients or K2 Solo Media Servers, do so now. Follow the procedure in the Field Kit Upgrade Instructions document that you received with the field kit.

## Make recovery images

After you have upgraded software as instructed in these procedures and verified that your system is working properly, you should always make a recovery image of each of your upgraded computers. Use a sequence of tasks similar to those you followed for upgrading software so that as you take systems offline you manage redundancy, servers, and clients, as appropriate for your system.

Refer to the Grass Valley product's *Service Manual* for recovery image procedures.

## Licensing K2 products

The following sections contain instructions for managing K2 product licenses.

### K2 licenses

The Grass Valley licenses available at the time of this writing that can be installed on a K2 product are as follows. Contact your Grass Valley representative for more information about licenses.

#### K2 Summit/Solo system licenses

License	License type	1 <sup>st</sup> Gen Summit	Solo	Summit 3G
K2 System Software	SabreTooth	X	X	X
HD license for two channels of High Definition input/output	SabreTooth	X	X	X
H.264 license for two channels of AVC-Intra input/output and AVCHD output	SabreTooth			X
AppCenter Pro	SabreTooth	X	X	X
AppCenter Elite	SabreTooth	X	X	X
K2 FCP Connect	SabreTooth	X	X	X
K2 TimeDelay	SabreTooth	X	X	X
K2 InSync	SabreTooth	X	X	X
K2 XML Import Capture Service	SabreTooth	X	X	X
Avid-TM	SabreTooth	X	X	X

License	License type	1 <sup>st</sup> Gen Summit	Solo	Summit 3G
K2 HotBin Export Service	SabreTooth	X	X	X

#### K2 Media Server licenses

License	License type
K2 SAN bandwidth	SabreTooth

## About K2 system software licensing

K2 system software version 8.1 requires a license from Grass Valley. Licensing is enforced at the K2 Summit Production Client or K2 Solo Media Server, so every K2 client running version 8.1 must have a valid license in place. No software version license is required on the control point PC. The K2 Media Server can be licensed for K2 SAN bandwidth, but no K2 system software version license is required on the K2 Media Server.

K2 clients shipping new from the factory have version 8.1 pre-installed with a permanent license in place, so no licensing tasks are required unless you want to add optional features such as AppCenter Pro/Elite. When upgrading from a 7.0.x version to version 8.1, you do not need to obtain a new HD license or AppCenter Pro/Elite license. If these licenses were permanent and valid before the upgrade, the licenses are still valid after the upgrade.

Licenses are requested through email and managed through the SabreTooth License Manager, which is installed on the Grass Valley product with the Grass Valley software. The SabreTooth License Manager must be located on the Grass Valley product.

License information is stored in XML files that you can manage just like any other file on your system. Node-locked licenses are unique to the system for which they are requested and cannot be used on any other machine. A floating license can be used on multiple machines, one at a time. You should back up the license text files to a separate drive or as part of a recovery image.

Licenses are based on your system's unique identifier, which is partially derived from your system's Media Access Control (MAC) address. If you change your system's MAC address by performing operations such as changing the System Processor card, you must obtain a new license based on the new MAC address.

#### After temporary licenses expire

After the temporary license expires, if you have not yet obtained a permanent license, the following occurs:

- The K2 system software temporary license will expire. You will not be able to start AppCenter once the license has expired. If running, AppCenter will not stop working, and any remote control protocols will continue to function. However, you will not be able to make any changes in AppCenter, such as altering the configuration.

- The AppCenter Pro temporary license will expire and the AppCenter Pro features will stop functioning.

## Requesting a license

This topic applies to Grass Valley Sabretooth licenses. For the system you are licensing, you must provide a generated unique ID to Grass Valley. Grass Valley uses the ID to create your unique license.

1. Log on to the device that you want to license.

You must log in as a Windows administrator with a local account, not a domain account.

2. Open the License Request Wizard.

Find the License Request shortcut on the Windows desktop.

The License Request Wizard displays.

3. Read the on-screen instructions, then click **Next**.

The Customer dialog box displays.

4. Enter the information requested on this page then click **Next**.

You must provide a valid email address to receive your license file.

The Sales Number dialog box displays.

5. Enter the Sales Order Number in the field then click **Next**.

Typically the Sales Order Number is found on the Software License sheet that you received from Grass Valley.

The Summary dialog box displays.

6. Review the License Request information and click **Finish**.

A License Request text file, *License\_Request\_<SalesNumber>.txt*, is generated and saved to the Windows Desktop.

**NOTE:** *If you are requesting licenses for more than one application, be sure to modify the name of the first License Request text file before saving it to your desktop. (In Notepad, use the Save As command.) Otherwise, the second License Request text file will overwrite it.*

7. If a K2 Summit/Solo system and the write filter is currently enabled, be aware that files on the desktop are lost on restart. Therefore do one of the following:

- Save the License Request text file(s) to a different location.
- Keep the K2 system running (do not restart) until after you have requested the license(s).

8. Do one of the following:

- Attach the License Request text file to an email.
- Paste the text directly into an email message.

You might want to keep a copy of the message for your records.

9. Send the email as instructed by the License Request Wizard.

An email will be sent from Grass Valley to the return email address you specified; your SabreTooth software license will be provided as a text file.

10. Save this email in case you ever need to re-image this machine.

Next add the license to the SabreTooth License Manager.

#### **If you encounter difficulties when requesting a license**

If you encounter difficulties running the License wizard, or the License wizard is not available, try this alternate method:

1. Generate a unique ID of the device where you will install software, as follows:
  - a) Double click on the License Manager icon on the Windows Desktop.  
The SabreTooth License Manager opens.
  - b) Choose **File | Generate Unique Id** the License Manager.
  - c) Click **Copy to clipboard** to copy the generated ID, and **OK** to exit.
2. Prepare an email that includes the following information:
  - Customer Name
  - Customer Email
  - Sales Order Number
  - Unique ID of the device where you will install software.
3. Send the email to [K2License@grassvalley.com](mailto:K2License@grassvalley.com).

The SabreTooth license number will be emailed to the email address you specified.

#### **Adding a license**

Your software license, *Licenses\_<SalesNumber>.txt*, is provided as a text file. Use the License Manager to add this file to your system and enable the desired feature.

1. If adding a license on a K2 Summit/Solo system, if you have not already done so, disable the write filter.
2. Double click on the License Manager icon on the Windows Desktop.  
The SabreTooth License Manager opens.
3. Do one of the following:
  - Choose **File | Import License** and navigate to the file location to open the text file.
  - Drag and drop the text file onto the License Manager.

You will now see the permanent license in SabreTooth, as well as any other licenses, permanent or temporary, that have been installed on this machine.

4. On a K2 Summit/Solo system, if you have completed your changes, enable the write filter.

You should archive the permanent license to a backup system.

## Deleting licenses

Deleting a license disables the feature that it enabled. You might want to delete a temporary license prior to its expiry if you have decided not to purchase the feature. You can delete a temporary license after the permanent license has been installed without disabling the licensed product.

1. If deleting a license on the K2 Summit Production Client, if you have not already done so, disable the write filter.
2. Select the license in the SabreTooth License Manager.
3. Use the Delete key on your keyboard or right click with your mouse and select **Delete**.
4. On the K2 Summit Production Client, if you have completed your changes, enable the write filter.

## Archiving licenses

You can archive your licenses to a secure external location. This allows you to quickly re-install a license should it be deleted or should you have to downgrade and then re-license the software. You can archive multiple licenses at the same time.

***NOTE: If you downgrade to an earlier version of the licensed software, make sure to archive the licenses first.***

1. In the SabreTooth License Manager, select the license or licenses.
2. Choose **File | Export License** to open the Save As dialog box.
3. Assign a meaningful name to the file, and save it to the desired location. Grass Valley recommends saving the license file to a USB drive or other external location.

---

# Known Problems

The following limitations are present in this release of software. If you wish to obtain more information about these limitations, please mention the reference numbers.

## AppCenter

ncb00003440	Description:	Bins nested more than nine levels deep are not supported. Database errors can occur.
	Workaround:	Constrain bins to nine levels deep or less. This includes the top-most bin.
ncb00003457	Description:	Closed captioning and/or ancillary data not present in the last few seconds of a growing clip's playout. This occurs when playing out a clip that is being recorded, and the recording stops.
	Workaround:	Stop playout of growing clip before stopping recording. In any case the closed captioning and/or ancillary data is full-length in the recorded clip and present in subsequent playout.
ncb00039062	Description:	The system clock may not update when the TimeOfDay source is changed.
	Workaround:	If this happens reboot after the TimeOfDay source change.
ncb00003919	Description:	When reconfiguring channel security settings on Configuration Manager Security tab, AppCenter does not allow username/password fields to be blank.
	Workaround:	Enter username/password for a valid user account. Once configured, the fields require valid information.
ncb00004073	Description:	Recorded video is one frame late relative to timecode. This occurs if you record using Time-of-day timecode and the source is from channel four's LTC input.
	Workaround:	Connect the house LTC input to channel 1 and use it as the Time-of-day source.
ncb00002648	Description:	AppCenter does not allow a clip to be deleted if the clip is associated with a playlist, program, or subclip.
	Workaround:	First use the "Consolidate Media" feature on the clip, then delete the clip.
ncb00002781	Description:	Video faults continue to occur if Super Slo-Mo inputs lose and then regain phase alignment while recording is underway.
	Workaround:	If inputs lose phase alignment, first restore phase alignment and then stop and restart the recording.
ncb00035282	Description:	On K2 Summit Transmission models, only two audio tracks can be created for new Playlist.
	Workaround:	As designed.
ncb00038746	Description:	Audio errors occur when playing a clip while importing from a USB device.

	Workaround:	Copy first, then play. Playback while importing from USB not supported.
ncb00061447	Description:	After a cold boot AppCenter does not start. The log shows errors “System channel.cpp: Unknown error” followed by “AppService: Could not create controller”.
	Workaround:	Reboot.
ncb00061803	Description:	Remote AppCenter errors on 64-bit PC.
	Workaround:	As designed. Remote AppCenter supported on 32-bit PC only.

### Storage Utility

ncb00004104	Description:	Storage Utility does not open for a nearline SAN. This occurs when in K2 Config you select the name of the K2 SAN, which is the top node of the storage system tree, when attempting to open Storage Utility.
	Workaround:	In K2Config tree view, under the nearline SAN's K2 Media Server, select the <b>File System Server</b> node to open its property page. On the property page click <b>Launch Storage Utility</b> .

### System

ncb00017096	Description:	The K2 Media Server displays an error because the Dell OpenManage server log fills up.
	Workaround:	Manually clear the log and then configure OpenManage to overwrite the log when full.
ncb00003449	Description:	Slow operations after restarting with a USB device connected.
	Workaround:	Disconnect then reconnect USB device. Normal operation speed is restored.
ncb00002672	Description:	Macintosh systems cannot write to a HotBin directory on the V: drive of an iSCSI or Fibre Channel connected K2 SAN. GV Connect export to the HotBin fails.
	Workaround:	Delete the HotBin, configure Macintosh access in the SNFS configuration file, then recreate the HotBin from the K2 Media Server. Configure the SNFS configuration file as part of the upgrade to this version of K2 software, as instructed in the upgrade procedure earlier in these release notes. If not upgrading, take systems offline, make the change as instructed in the upgrade procedure, then restart the K2 Media Server to put the change into effect.
ncb00004203	Description:	On a K2 Media Server with SNFS on the C: drive, media is lost if you re-image the C: drive
	Workaround:	Before re-imaging, copy C:\SNFS\config and C:\SNFS\data to another location. After re-imaging, copy back to the C: drive.
ncb00004242	Description:	AppService fails to start after software installation.

---

	Workaround:	Restart the K2 system.
ncb00060531	Description:	When configuring a HotBin Export destination folder and entering credentials, a "...cannot start service..." error message appears.
	Workaround:	In Windows Services Control Panel, for Grass Valley Import Service, enter the credentials and start the service.
ncb00038588	Description:	The K2Config application does not open.
	Workaround:	On the PC that hosts the K2Config application, disable the control network interface card, then open the K2Config application, then enable the control network interface card.
ncb00064016	Description:	AFD property is not passed with AVC clips.
	Workaround:	Add an ancillary data track to the AVC clip to carry the AFD property.
ncb00063992	Description:	Some USB 3.0 devices are not recognized as USB 3.0 on the front connectors.
	Workaround:	If the USB 3.0 device is recognized as a USB 2.0 device when plugged in, remove it and plug it in again to be recognized as a USB 3.0 device. If the USB 3.0 device is not recognized at all, plug in a USB 2.0 device, then plug in the USB 3.0 device again to use it. This only needs to be done once after booting. Thereafter the device will be recognized as a USB 3.0 device.
DE1427 ncb00074726	Description:	In STRATUS Playlist Editor, when dragging clips to the lower section of the panel, some clips are not visible.
	Workaround:	Eject and reload playlist.

---

### Proxy/live streaming

---

ncb00041093	Description:	Live streaming can fail when the K2 Summit system's IP address is changed.
	Workaround:	On the K2 Summit system navigate to <code>V:\live streaming</code> and use Notepad or a similar text editor to open a <code>*.sdp</code> file. Check the first IP address listed in the file, on the <code>o=</code> line. If it is not the K2 Summit system's Control Connection IP address, delete the <code>*.sdp</code> files in the directory and restart the K2 Summit system.
ncb00061128	Description:	Remote desktop connections cause live streaming errors and audio/video sync problems.
	Workaround:	Do not use Remote Desktop on K2 Summit systems that are generating live streams. To restore live streaming audio/video sync, disable the proxy recording and live streaming for that channel, then re-enable live streaming.

---

### Installation

---

ncb00003885	Description:	If uninstalling or installing K2 client software while applications or connections to AppService are open, the installation program becomes unresponsive.
	Workaround:	Use Task Manager to stop AppService. To prevent the problem from occurring, shutdown all applications and connections before uninstalling or installing.
ncb00040814	Description:	Error messages appear during Generic iSCSI software install. This occurs when doing a manual (not SiteConfig) install on a Windows 7 PC. The error messages are similar to "The installation of VS2005.762 appears to have failed..." and "Setup could not find the update.inf file...".
	Workaround:	Ignore the error messages and continue with installation. The software installs successfully. The error messages are caused because the installation program tries to install components that are already present in Windows 7.

---

### Compatibility

---

ncb00008524	Description:	M-Series iVDR transfers fail.
	Workaround:	Do not attempt to transfer to/from M-Series iVDR.
ncb00025753	Description:	MXF streaming transfer to XDCAM recorder fails.
	Workaround:	None. Some Sony deck models do not comply with the MXF standard.

---

### Dyno PA

---

ncb00002810	Description:	On a stand-alone K2 Summit/Solo configured for K2 Dyno PA, the V: drive is not available. This occurs if the K2 system is started without a network connection or otherwise used outside of the Dyno PA system.
	Workaround:	Remove the DLC configuration from the K2 Summit/Solo as instructed in Dyno PA documentation. Verify that the loopback adapter is at the top of the adapter order list. This is required for a stand-alone K2 system that is not part of a Dyno PA system.

---

### K2Config

---

DE2192 ncb00075556	Description:	In K2Config, when using the <b>Check</b> button on a File System Server Configuration page or a File System Client Configuration page, an error is displayed about changing the name of the File System Servers. This occurs if the fsnameservers file contains IP addresses rather than hostnames.
	Workaround:	Do not use the <b>Check</b> button. If you do and the error is displayed on a File System Server Configuration page, K2Config writes hostnames to the fsnameservers file. Open the fsnameservers file and remove the hostnames, so the file contains only IP addresses.

---

---

# Trademarks and agreements

## Trademarks

Grass Valley, STRATUS, K2, Aurora, Summit, ChannelFlex, Dyno, Solo, ClipStore, Infinity, Turbo, Profile, Profile XP, NetCentral, NewsBrowse, NewsEdit, NewsQ, NewsShare, NewsQ Pro, and Media Manager are either registered trademarks or trademarks of Grass Valley USA, LLC. in the United States and/or other countries. Grass Valley USA, LLC. products are covered by U.S. and foreign patents, issued and pending. Additional information regarding Grass Valley USA, LLC. trademarks and other proprietary rights may be found at [www.grassvalley.com](http://www.grassvalley.com). Other trademarks and logos used in this document are either registered trademarks or trademarks of the manufacturers or vendors of the associated products, such as Microsoft® Windows® operating system, Windows Media® player, Internet Explorer® internet browser, and SQL Server™. QuickTime and the QuickTime logo are trademarks or registered trademarks of Apple Computer, Inc., used under license therefrom. AVCHD and the AVCHD logo are trademarks of Panasonic Corporation and Sony Corporation



## JPEG acknowledgment

This software is based in part on the work of the Independent JPEG Group.