grass valley

K2

Media Platform

System Guide

Software version 9

www.grassvalley.com

071-8726-04
November 2012

CERTIFICATE

Certificate Number: 510040.001

The Quality System of:

Grass Valley USA, LLC and its Grass Valley Affiliates

Headquarters:
400 Providence Mine Road
Nevada City, CA 95945
United States

15655 SW Greystone Ct.
Beaverton, OR 97006
United States

Kapittelweg 10
4827 HG Breda
The Nederlands

2300 So. Decker Lake Blvd.
Salt Lake City, UT 84119
United States

Including its implementation, meets the requirements of the standard:

ISO 9001:2008

Scope:
The design, manufacture and support of video and audio hardware and software products and related systems.

This Certificate is valid until: June 14, 2015
This Certificate is valid as of: June 14, 2012
Certified for the first time: June 14, 2000

H. Pierre Sallé
President
DEKRA Certification, Inc

The method of operation for quality certification is defined in the DEKRA General Terms And Conditions For Quality And Environmental Management Systems Certifications. Integral publication of this certificate is allowed.

DEKRA Certification, Inc.
4377 County Line Road
Chalfont, PA 18914
Ph: (215)997-4519
Fax: (215)997-3809
CRT 001 042108

Accredited By:
ANAB

grass valley

K2

Media Platform

System Guide

Software version 9

www.grassvalley.com

071-8726-04
November 2012

Contacting Grass Valley

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

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.

grass valley

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

001187401

Contents

Safety Summaries

Safety Summary

Read and follow the important safety information below, noting especially those instructions related to risk of fire, electric shock or injury to persons. Additional specific warnings not listed here may be found throughout the manual.

⚠	***WARNING: Any instructions in this manual that require opening the equipment cover or enclosure are for use by qualified service personnel only. To reduce the risk of electric shock, do not perform any servicing other than that contained in the operating instructions unless you are qualified to do so.***

Safety terms and symbols

Terms in this manual

Safety-related statements may appear in this manual in the following form:

⚠	***WARNING: Warning statements identify conditions or practices that may result in personal injury or loss of life.***
⚠	***CAUTION: Caution statements identify conditions or practices that may result in damage to equipment or other property, or which may cause equipment crucial to your business environment to become temporarily non-operational.***

Terms on the product

These terms may appear on the product:

DANGER — A personal injury hazard is immediately accessible as you read the marking.

WARNING — A personal injury hazard exists but is not immediately accessible as you read the marking.

CAUTION — A hazard to property, product, and other equipment is present.

Symbols on the product

The following symbols may appear on the product:

⚠	Indicates that dangerous high voltage is present within the equipment enclosure that may be of sufficient magnitude to constitute a risk of electric shock.
⚠	Indicates that user, operator or service technician should refer to product manual(s) for important operating, maintenance, or service instructions.
⚠	This is a prompt to note fuse rating when replacing fuse(s). The fuse referenced in the text must be replaced with one having the ratings indicated.

	Identifies a protective grounding terminal which must be connected to earth ground prior to making any other equipment connections.
	Identifies an external protective grounding terminal which may be connected to earth ground as a supplement to an internal grounding terminal.
	Indicates that static sensitive components are present which may be damaged by electrostatic discharge. Use anti-static procedures, equipment and surfaces during servicing.

Warnings

The following warning statements identify conditions or practices that can result in personal injury or loss of life.

Dangerous voltage or current may be present — Disconnect power and remove battery (if applicable) before removing protective panels, soldering, or replacing components.

Do not service alone — Do not internally service this product unless another person capable of rendering first aid and resuscitation is present.

Remove jewelry — Prior to servicing, remove jewelry such as rings, watches, and other metallic objects.

Avoid exposed circuitry — Do not touch exposed connections, components or circuitry when power is present.

Use proper power cord — Use only the power cord supplied or specified for this product.

Ground product — Connect the grounding conductor of the power cord to earth ground.

Operate only with covers and enclosure panels in place — Do not operate this product when covers or enclosure panels are removed.

Use correct fuse — Use only the fuse type and rating specified for this product.

Use only in dry environment — Do not operate in wet or damp conditions.

Use only in non-explosive environment — Do not operate this product in an explosive atmosphere.

High leakage current may be present — Earth connection of product is essential before connecting power.

Dual power supplies may be present — Be certain to plug each power supply cord into a separate branch circuit employing a separate service ground. Disconnect both power supply cords prior to servicing.

Double pole neutral fusing — Disconnect mains power prior to servicing.

Use proper lift points — Do not use door latches to lift or move equipment.

Avoid mechanical hazards — Allow all rotating devices to come to a stop before servicing.

Cautions

The following caution statements identify conditions or practices that can result in damage to equipment or other property

Use correct power source — Do not operate this product from a power source that applies more than the voltage specified for the product.

Use correct voltage setting — If this product lacks auto-ranging power supplies, before applying power ensure that the each power supply is set to match the power source.

Provide proper ventilation — To prevent product overheating, provide equipment ventilation in accordance with installation instructions.

Use anti-static procedures — Static sensitive components are present which may be damaged by electrostatic discharge. Use anti-static procedures, equipment and surfaces during servicing.

Do not operate with suspected equipment failure — If you suspect product damage or equipment failure, have the equipment inspected by qualified service personnel.

Ensure mains disconnect — If mains switch is not provided, the power cord(s) of this equipment provide the means of disconnection. The socket outlet must be installed near the equipment and must be easily accessible. Verify that all mains power is disconnected before installing or removing power supplies and/or options.

Route cable properly — Route power cords and other cables so that they ar not likely to be damaged. Properly support heavy cable bundles to avoid connector damage.

Use correct power supply cords — Power cords for this equipment, if provided, meet all North American electrical codes. Operation of this equipment at voltages exceeding 130 VAC requires power supply cords which comply with NEMA configurations. International power cords, if provided, have the approval of the country of use.

Use correct replacement battery — This product may contain batteries. To reduce the risk of explosion, check polarity and replace only with the same or equivalent type recommended by manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Troubleshoot only to board level — Circuit boards in this product are densely populated with surface mount technology (SMT) components and application specific integrated circuits (ASICS). As a result, circuit board repair at the component level is very difficult in the field, if not impossible. For warranty compliance, do not troubleshoot systems beyond the board level.

Sicherheit – Überblick

Lesen und befolgen Sie die wichtigen Sicherheitsinformationen dieses Abschnitts. Beachten Sie insbesondere die Anweisungen bezüglich

Brand-, Stromschlag- und Verletzungsgefahren. Weitere spezifische, hier nicht aufgeführte Warnungen finden Sie im gesamten Handbuch.

⚠ ***WARNUNG: Alle Anweisungen in diesem Handbuch, die das Abnehmen der Geräteabdeckung oder des Gerätegehäuses erfordern, dürfen nur von qualifiziertem Servicepersonal ausgeführt werden. Um die Stromschlaggefahr zu verringern, führen Sie keine Wartungsarbeiten außer den in den Bedienungsanleitungen genannten Arbeiten aus, es sei denn, Sie besitzen die entsprechende Qualifikationen für diese Arbeiten.***

Sicherheit – Begriffe und Symbole

In diesem Handbuch verwendete Begriffe

Sicherheitsrelevante Hinweise können in diesem Handbuch in der folgenden Form auftauchen:

⚠	***WARNUNG: Warnungen weisen auf Situationen oder Vorgehensweisen hin, die Verletzungs- oder Lebensgefahr bergen.***
⚠	***VORSICHT: Vorsichtshinweise weisen auf Situationen oder Vorgehensweisen hin, die zu Schäden an Ausrüstungskomponenten oder anderen Gegenständen oder zum zeitweisen Ausfall wichtiger Komponenten in der Arbeitsumgebung führen können.***

Hinweise am Produkt

Die folgenden Hinweise können sich am Produkt befinden:

GEFAHR – Wenn Sie diesen Begriff lesen, besteht ein unmittelbares Verletzungsrisiko.

WARNUNG – Wenn Sie diesen Begriff lesen, besteht ein mittelbares Verletzungsrisiko.

VORSICHT – Es besteht ein Risiko für Objekte in der Umgebung, den Mixer selbst oder andere Ausrüstungskomponenten.

Symbole am Produkt

Die folgenden Symbole können sich am Produkt befinden:

	Weist auf eine gefährliche Hochspannung im Gerätegehäuse hin, die stark genug sein kann, um eine Stromschlaggefahr darzustellen.
	Weist darauf hin, dass der Benutzer, Bediener oder Servicetechniker wichtige Bedienungs-, Wartungs- oder Serviceanweisungen in den Produkthandbüchern lesen sollte.
	Dies ist eine Aufforderung, beim Wechsel von Sicherungen auf deren Nennwert zu achten. Die im Text angegebene Sicherung muss durch eine Sicherung ersetzt werden, die die angegebenen Nennwerte besitzt.
	Weist auf eine Schutzerdungsklemme hin, die mit dem Erdungskontakt verbunden werden muss, bevor weitere Ausrüstungskomponenten angeschlossen werden.
	Weist auf eine externe Schutzerdungsklemme hin, die als Ergänzung zu einem internen Erdungskontakt an die Erde angeschlossen werden kann.
	Weist darauf hin, dass es statisch empfindliche Komponenten gibt, die durch eine elektrostatische Entladung beschädigt werden können. Verwenden Sie antistatische Prozeduren, Ausrüstung und Oberflächen während der Wartung.

Warnungen

Die folgenden Warnungen weisen auf Bedingungen oder Vorgehensweisen hin, die Verletzungs- oder Lebensgefahr bergen:

Gefährliche Spannungen oder Ströme – Schalten Sie den Strom ab, und entfernen Sie ggf. die Batterie, bevor sie Schutzabdeckungen abnehmen, löten oder Komponenten austauschen.

Servicearbeiten nicht alleine ausführen – Führen Sie interne Servicearbeiten nur aus, wenn eine weitere Person anwesend ist, die erste Hilfe leisten und Wiederbelebungsmaßnahmen einleiten kann.

Schmuck abnehmen – Legen Sie vor Servicearbeiten Schmuck wie Ringe, Uhren und andere metallische Objekte ab.

Keine offen liegenden Leiter berühren – Berühren Sie bei eingeschalteter Stromzufuhr keine offen liegenden Leitungen, Komponenten oder Schaltungen.

Richtiges Netzkabel verwenden – Verwenden Sie nur das mitgelieferte Netzkabel oder ein Netzkabel, das den Spezifikationen für dieses Produkt entspricht.

Gerät erden – Schließen Sie den Erdleiter des Netzkabels an den Erdungskontakt an.

Gerät nur mit angebrachten Abdeckungen und Gehäuseseiten betreiben – Schalten Sie dieses Gerät nicht ein, wenn die Abdeckungen oder Gehäuseseiten entfernt wurden.

Richtige Sicherung verwenden – Verwenden Sie nur Sicherungen, deren Typ und Nennwert den Spezifikationen für dieses Produkt entsprechen.

Gerät nur in trockener Umgebung verwenden – Betreiben Sie das Gerät nicht in nassen oder feuchten Umgebungen.

Gerät nur verwenden, wenn keine Explosionsgefahr besteht – Verwenden Sie dieses Produkt nur in Umgebungen, in denen keinerlei Explosionsgefahr besteht.

Hohe Kriechströme – Das Gerät muss vor dem Einschalten unbedingt geerdet werden.

Doppelte Spannungsversorgung kann vorhanden sein – Schließen Sie die beiden Anschlußkabel an getrennte Stromkreise an. Vor Servicearbeiten sind beide Anschlußkabel vom Netz zu trennen.

Zweipolige, neutrale Sicherung – Schalten Sie den Netzstrom ab, bevor Sie mit den Servicearbeiten beginnen.

Fassen Sie das Gerät beim Transport richtig an – Halten Sie das Gerät beim Transport nicht an Türen oder anderen beweglichen Teilen fest.

Gefahr durch mechanische Teile – Warten Sie, bis der Lüfter vollständig zum Halt gekommen ist, bevor Sie mit den Servicearbeiten beginnen.

Vorsicht

Die folgenden Vorsichtshinweise weisen auf Bedingungen oder Vorgehensweisen hin, die zu Schäden an Ausrüstungskomponenten oder anderen Gegenständen führen können:

Gerät nicht öffnen – Durch das unbefugte Öffnen wird die Garantie ungültig.

Richtige Spannungsquelle verwenden – Betreiben Sie das Gerät nicht an einer Spannungsquelle, die eine höhere Spannung liefert als in den Spezifikationen für dieses Produkt angegeben.

Gerät ausreichend belüften – Um eine Überhitzung des Geräts zu vermeiden, müssen die Ausrüstungskomponenten entsprechend den Installationsanweisungen belüftet werden. Legen Sie kein Papier unter das Gerät. Es könnte die Belüftung behindern. Platzieren Sie das Gerät auf einer ebenen Oberfläche.

Antistatische Vorkehrungen treffen – Es gibt statisch empfindliche Komponenten, die durch eine elektrostatische Entladung beschädigt werden können. Verwenden Sie antistatische Prozeduren, Ausrüstung und Oberflächen während der Wartung.

CF-Karte nicht mit einem PC verwenden – Die CF-Karte ist speziell formatiert. Die auf der CF-Karte gespeicherte Software könnte gelöscht werden.

Gerät nicht bei eventuellem Ausrüstungsfehler betreiben – Wenn Sie einen Produktschaden oder Ausrüstungsfehler vermuten, lassen Sie die Komponente von einem qualifizierten Servicetechniker untersuchen.

Kabel richtig verlegen – Verlegen Sie Netzkabel und andere Kabel so, dass Sie nicht beschädigt werden. Stützen Sie schwere Kabelbündel ordnungsgemäß ab, damit die Anschlüsse nicht beschädigt werden.

Richtige Netzkabel verwenden – Wenn Netzkabel mitgeliefert wurden, erfüllen diese alle nationalen elektrischen Normen. Der Betrieb dieses Geräts mit Spannungen über 130 V AC erfordert Netzkabel, die NEMA-Konfigurationen entsprechen. Wenn internationale Netzkabel mitgeliefert wurden, sind diese für das Verwendungsland zugelassen.

Richtige Ersatzbatterie verwenden – Dieses Gerät enthält eine Batterie. Um die Explosionsgefahr zu verringern, prüfen Sie die Polarität und tauschen die Batterie nur gegen eine Batterie desselben Typs oder eines gleichwertigen, vom Hersteller empfohlenen Typs aus. Entsorgen Sie gebrauchte Batterien entsprechend den Anweisungen des Batterieherstellers.

Das Gerät enthält keine Teile, die vom Benutzer gewartet werden können. Wenden Sie sich bei Problemen bitte an den nächsten Händler.

Consignes desécurité

Il est recommandé de lire, de bien comprendre et surtout de respecter les informations relatives à la sécurité qui sont exposées ci-après, notamment les consignes destinées à prévenir les risques d'incendie, les décharges électriques et les blessures aux personnes. Les avertissements complémentaires, qui ne sont pas nécessairement repris ci-dessous, mais présents dans toutes les sections du manuel, sont également à prendre en considération.

⚠ ***AVERTISSEMENT: Toutes les instructions présentes dans ce manuel qui concernent l'ouverture des capots ou des logements de cet équipement sont destinées exclusivement à des membres qualifiés du personnel de maintenance. Afin de diminuer les risques de décharges électriques, ne procédez à aucune intervention d'entretien autre que celles contenues dans le manuel de l'utilisateur, à moins que vous ne soyez habilité pour le faire.***

Consignes et symboles de sécurité

Termes utilisés dans ce manuel

Les consignes de sécurité présentées dans ce manuel peuvent apparaître sous les formes suivantes :

⚠ ***AVERTISSEMENT: Les avertissements signalent des conditions ou des pratiques susceptibles d'occasionner des blessures graves, voire même fatales.***

⚠ ***MISE EN GARDE: Les mises en garde signalent des conditions ou des pratiques susceptibles d'occasionner un endommagement à l'équipement ou aux installations, ou de rendre l'équipement temporairement non opérationnel, ce qui peut porter préjudice à vos activités.***

Signalétique apposée sur le produit

La signalétique suivante peut être apposée sur le produit :

DANGER — risque de danger imminent pour l'utilisateur.

AVERTISSEMENT — Risque de danger non imminent pour l'utilisateur.

MISE EN GARDE — Risque d'endommagement du produit, des installations ou des autres équipements.

Symboles apposés sur le produit

Les symboles suivants peut être apposés sur le produit :

	Signale la présence d'une tension élevée et dangereuse dans le boîtier de l'équipement ; cette tension peut être suffisante pour constituer un risque de décharge électrique.
	Signale que l'utilisateur, l'opérateur ou le technicien de maintenance doit faire référence au(x) manuel(s) pour prendre connaissance des instructions d'utilisation, de maintenance ou d'entretien.
	Il s'agit d'une invite à prendre note du calibre du fusible lors du remplacement de ce dernier. Le fusible auquel il est fait référence dans le texte doit être remplacé par un fusible du même calibre.
	Identifie une borne de protection de mise à la masse qui doit être raccordée correctement avant de procéder au raccordement des autres équipements.
	I dentifie une borne de protection de mise à la masse qui peut être connectée en tant que borne de mise à la masse supplémentaire.
	Signale la présence de composants sensibles à l'électricité statique et qui sont susceptibles d'être endommagés par une décharge électrostatique. Utilisez des procédures, des équipements et des surfaces antistatiques durant les interventions d'entretien.

Avertissements

Les avertissements suivants signalent des conditions ou des pratiques susceptibles d'occasionner des blessures graves, voire même fatales :

Présence possible de tensions ou de courants dangereux — Mettez hors tension, débranchez et retirez la pile (le cas échéant) avant de déposer les couvercles de protection, de défaire une soudure ou de remplacer des composants.

Ne procédez pas seul à une intervention d'entretien — Ne réalisez pas une intervention d'entretien interne sur ce produit si une personne n'est pas présente pour fournir les premiers soins en cas d'accident.

Retirez tous vos bijoux — Avant de procéder à une intervention d'entretien, retirez tous vos bijoux, notamment les bagues, la montre ou tout autre objet métallique.

Évitez tout contact avec les circuits exposés — Évitez tout contact avec les connexions, les composants ou les circuits exposés s'ils sont sous tension.

Utilisez le cordon d'alimentation approprié — Utilisez exclusivement le cordon d'alimentation fourni avec ce produit ou spécifié pour ce produit.

Raccordez le produit à la masse — Raccordez le conducteur de masse du cordon d'alimentation à la borne de masse de la prise secteur.

Utilisez le produit lorsque les couvercles et les capots sont en place — N'utilisez pas ce produit si les couvercles et les capots sont déposés.

Utilisez le bon fusible — Utilisez exclusivement un fusible du type et du calibre spécifiés pour ce produit.

Utilisez ce produit exclusivement dans un environnement sec — N'utilisez pas ce produit dans un environnement humide.

Utilisez ce produit exclusivement dans un environnement non explosible — N'utilisez pas ce produit dans un environnement dont l'atmosphère est explosible.

Présence possible de courants de fuite — Un raccordement à la masse est indispensable avant la mise sous tension.

Deux alimentations peuvent être présentes dans l'équipement — Assurez vous que chaque cordon d'alimentation est raccordé à des circuits de terre séparés. Débranchez les deux cordons d'alimentation avant toute intervention.

Fusion neutre bipolaire — Débranchez l'alimentation principale avant de procéder à une intervention d'entretien.

Utilisez les points de levage appropriés — Ne pas utiliser les verrous de la porte pour lever ou déplacer l'équipement.

Évitez les dangers mécaniques — Laissez le ventilateur s'arrêter avant de procéder à une intervention d'entretien.

Mises en garde

Les mises en garde suivantes signalent les conditions et les pratiques susceptibles d'occasionner des endommagements à l'équipement et aux installations :

N'ouvrez pas l'appareil — Toute ouverture prohibée de l'appareil aura pour effet d'annuler la garantie.

Utilisez la source d'alimentation adéquate — Ne branchez pas ce produit à une source d'alimentation qui utilise une tension supérieure à la tension nominale spécifiée pour ce produit.

Assurez une ventilation adéquate — Pour éviter toute surchauffe du produit, assurez une ventilation de l'équipement conformément aux instructions d'installation. Ne déposez aucun document sous l'appareil – ils peuvent gêner la ventilation. Placez l'appareil sur une surface plane.

Utilisez des procédures antistatiques - Les composants sensibles à l'électricité statique présents dans l'équipement sont susceptibles d'être endommagés par une décharge électrostatique. Utilisez des procédures, des équipements et des surfaces antistatiques durant les interventions d'entretien.

N'utilisez pas la carte CF avec un PC — La carte CF a été spécialement formatée. Le logiciel enregistré sur la carte CF risque d'être effacé.

N'utilisez pas l'équipement si un dysfonctionnement est suspecté — Si vous suspectez un dysfonctionnement du produit, faites inspecter celui-ci par un membre qualifié du personnel d'entretien.

Acheminez les câbles correctement — Acheminez les câbles d'alimentation et les autres câbles de manière à ce qu'ils ne risquent pas d'être endommagés. Supportez correctement les enroulements de câbles afin de ne pas endommager les connecteurs.

Utilisez les cordons d'alimentation adéquats — Les cordons d'alimentation de cet équipement, s'ils sont fournis, satisfont aux exigences de toutes les réglementations régionales. L'utilisation de cet équipement à des tensions dépassant les 130 V en c.a. requiert des cordons d'alimentation qui satisfont aux exigences des configurations NEMA. Les cordons internationaux, s'ils sont fournis, ont reçu l'approbation du pays dans lequel l'équipement est utilisé.

Utilisez une pile de remplacement adéquate — Ce produit renferme une pile. Pour réduire le risque d'explosion, vérifiez la polarité et ne remplacez la pile que par une pile du même type, recommandée par le fabricant. Mettez les piles usagées au rebut conformément aux instructions du fabricant des piles.

Cette unité ne contient aucune partie qui peut faire l'objet d'un entretien par l'utilisateur. Si un problème survient, veuillez contacter votre distributeur local.

Certifications and compliances

Canadian certified power cords

Canadian approval includes the products and power cords appropriate for use in the North America power network. All other power cords supplied are approved for the country of use.

FCC emission control

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. Changes or modifications not expressly approved by Grass Valley can affect emission compliance and could void the user's authority to operate this equipment.

Canadian EMC Notice of Compliance

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A préscrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

EN55103 1/2 Class A warning

This product has been evaluated for Electromagnetic Compatibility under the EN 55103-1/2 standards for Emissions and Immunity and meets the requirements for E4 environment.

This product complies with Class A (E4 environment). In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

FCC emission limits

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesirable operation.

Laser compliance

Laser safety requirements

This product may contain a Class 1 certified laser device. Operating this product outside specifications or altering its original design may result in hazardous radiation exposure, and may be considered an act of modifying or new manufacturing of a laser product under U.S. regulations contained in 21CFR Chapter 1, subchapter J or CENELEC regulations in HD 482 S1. People performing such an act are required by law to recertify and reidentify this product in accordance with provisions of 21CFR subchapter J for distribution within the U.S.A., and in accordance with CENELEC HD 482 S1 for distribution within countries using the IEC 825 standard.

Laser safety

Laser safety in the United States is regulated by the Center for Devices and Radiological Health (CDRH). The laser safety regulations are published in the "Laser Product Performance Standard," Code of Federal Regulation (CFR), Title 21, Subchapter J.

The International Electrotechnical Commission (IEC) Standard 825, "Radiation of Laser Products, Equipment Classification, Requirements and User's Guide," governs laser products outside the United States. Europe and member nations of the European Free Trade Association fall under the jurisdiction of the Comité Européen de Normalization Electrotechnique (CENELEC).

Safety certification

This product has been evaluated and meets the following Safety Certification Standards:

Standard	Designed/tested for compliance with:
ANSI/UL 60950-1	Safety of Information Technology Equipment, including Electrical Business Equipment (Second edition 2007).
IEC 60950-1 with CB cert.	Safety of Information Technology Equipment, including Electrical Business Equipment (Second edition, 2005).
CAN/CSA C22.2 No. 60950-1	Safety of Information Technology Equipment, including Electrical Business Equipment (Second edition 2007).
BS EN 60950-1	Safety of Information Technology Equipment, including Electrical Business Equipment 2006.

ESD Protection

Electronics today are more susceptible to electrostatic discharge (ESD) damage than older equipment. Damage to equipment can occur by ESD fields that are smaller than you can feel. Implementing the information in this section will help you protect the investment that you have made in purchasing Grass Valley equipment. This section contains Grass Valley's recommended ESD guidelines that should be followed when handling electrostatic discharge sensitive (ESDS) items. These minimal recommendations are based on the information in the *Sources of ESD and Risks* on page 21 area. The information in *Grounding Requirements for Personnel* on page 22 is provided to assist you in selecting an appropriate grounding method.

Recommended ESD Guidelines

Follow these guidelines when handling Grass Valley equipment:

- Only trained personnel that are connected to a grounding system should handle ESDS items.
- Do not open any protective bag, box, or special shipping packaging until you have been grounded.

  NOTE: When a Personal Grounding strap is unavailable, as an absolute minimum, touch a metal object that is touching the floor (for example, a table, frame, or rack) to discharge any static energy before touching an ESDS item.
- Open the anti-static packaging by slitting any existing adhesive tapes. Do not tear the tapes off.
- Remove the ESDS item by holding it by its edges or by a metal panel.
- Do not touch the components of an ESDS item unless it is absolutely necessary to configure or repair the item.
- Keep the ESDS work area clear of all nonessential items such as coffee cups, pens, wrappers and personal items as these items can discharge static. If you need to set an ESDS item down, place it on an anti-static mat or on the anti-static packaging.

Sources of ESD and Risks

The following information identifies possible sources of electrostatic discharge and can be used to help establish an ESD policy.

Personnel

One of the largest sources of static is personnel. The static can be released from a person's clothing and shoes.

Environment

The environment includes the humidity and floors in a work area. The humidity level must be controlled and should not be allowed to fluctuate over a broad range. Relative humidity (RH) is a major part in determining the level of static that is being generated. For example, at 10% - 20% RH a person walking across a carpeted floor can develop 35kV; yet when the relative humidity is increased to 70% - 80%, the person can only generate 1.5kV.

Static is generated as personnel move (or as equipment is moved) across a floor's surface. Carpeted and waxed vinyl floors contribute to static build up.

Work Surfaces

Painted or vinyl-covered tables, chairs, conveyor belts, racks, carts, anodized surfaces, plexiglass covers, and shelving are all static generators.

Equipment

Any equipment commonly found in an ESD work area, such as solder guns, heat guns, blowers, etc., should be grounded.

Materials

Plastic work holders, foam, plastic tote boxes, pens, packaging containers and other items commonly found at workstations can generate static electricity.

Grounding Requirements for Personnel

The information in this section is provided to assist you in selecting a grounding method. This information is taken from ANSI/ESD S20.20-2007 (Revision of ANSI/ESD S20.20-1999).

Product Qualification

Personnel Grounding Technical Requirement	Test Method	Required Limits
Wrist Strap System*	ANSI/ESD S1.1 (Section 5.11)	$< 3.5 \times 10^7$ ohm
Flooring / Footwear System – Method 1	ANSI/ESD STM97.1	$< 3.5 \times 10^7$ ohm
Flooring / Footwear System – Method 2 (both required)	ANSI/ESD STM97. 1ANSI/ESD STM97.2	$< 10^9$ ohm
	ANSI/ESD STM97.2	< 100 V

Product qualification is normally conducted during the initial selection of ESD control products and materials. Any of the following methods can be used: product specification review, independent laboratory evaluation, or internal laboratory evaluation.

Compliance Verification

Personnel Grounding Technical Requirement	Test Method	Required Limits
Wrist Strap System*	ESD TR53 Wrist Strap Section	$< 3.5 \times 10^7$ ohm
Flooring / Footwear System – Method 1	ESD TR53 Flooring Section and ESD TR53 Footwear Section	$< 3.5 \times 10^7$ ohm
Flooring / Footwear System – Method 2 (both required)	ESD TR53 Flooring Section and ESD TR53 Footwear Section	$< 1.0 \times 10^9$ ohm

* For situations where an ESD garment is used as part of the wrist strap grounding path, the total system resistance, including the person, garment, and grounding cord, must be less than 3.5×10^7 ohm.

Preface

About this document

This manual describes K2™ systems and provides the information you need to go beyond factory default settings and customize your system's configuration to meet your site-specific needs. The manual covers first generation K2 Solo™ Media Server, K2 Solo™ 3G Media Server, first-generation K2 Summit™ models, and K2 Summit™ 3G models, including ChannelFlex™ Suite features and K2 SAN devices.

For more information

The following sections help you find the information you need in product manuals and elsewhere.

For the installer of a standalone K2 product with internal storage

If you are installing a K2 system, such as a K2 Summit/Solo system, with standalone internal storage, refer to documentation in the following sequence:

	Find this document…	In these locations…	In these formats:
1	K2 Release Notes	Grass Valley Website	PDF file
2	Quick Start Guide for the K2 product	K2 product shipping box	Printed
		K2 Documentation Set	PDF file
		Grass Valley Website	PDF file
3	K2 System Guide	K2 Documentation Set	PDF file
		Grass Valley Website	PDF file

For the installer of a K2 product with direct connect storage

If you are installing a standalone K2 system, such as a K2 Summit system, with direct connect external RAID storage, refer to documentation in the following sequence:

	Find this document…	In these locations…	In these formats:
1	K2 Release Notes	Grass Valley Website	PDF file
2	K2 Storage Cabling Guide	K2 RAID shipping box	Printed
		K2 Documentation Set	PDF file
		Grass Valley Website	PDF file

	Find this document…	In these locations…	In these formats:
3	Quick Start Guide for the K2 product	K2 product shipping box	Printed
		K2 Documentation Set	PDF file
		Grass Valley Website	PDF file
4	K2 System Guide	K2 Documentation Set	PDF file
		Grass Valley Website	PDF file

For the installer of K2 Summit systems with K2 SAN shared storage

If you are installing a K2 SAN with connected K2 Summit systems, refer to documentation in the following sequence:

	Find this document…	In these locations…	In these formats:
1	K2 Release Notes	Grass Valley Website	PDF file
2	K2 Storage Cabling Guide	K2 RAID shipping box	Printed
		K2 Documentation Set	PDF file
		Grass Valley Website	PDF file
3	Quick Start Guide for the K2 product	K2 product shipping box	Printed
		K2 Documentation Set	PDF file
		Grass Valley Website	PDF file
4	K2 SAN Installation and Service Manual	K2 Documentation Set	PDF file
		Grass Valley Website	PDF file
5	K2 System Guide	K2 Documentation Set	PDF file
		Grass Valley Website	PDF file

K2 Release Notes

Contains the latest information about the software shipped on your system, including software upgrade instructions, software specifications and requirements, feature changes from the previous releases, and any known problems. You should always check the Grass Valley Website to determine if there is an updated version of release notes available.

Quick Start Guides

The Quick Start Guide is a printed document, shipped in the product packaging with K2 Summit/Solo systems and K2 Dyno Replay Controllers. The Quick Start Guide provides step-by-step installation instructions for basic installation and operation of the product.

K2 Storage Cabling Guide

The K2 Storage Cabling Guide is a printed document, shipped in the product packaging with the primary RAID storage chassis. The cabling guide provides instructions for K2 Storage Area Network (SAN) cabling and external configuration. The cabling guide provides instructions for each level of K2 SAN and covers both redundant and basic (non-redundant) systems. It also provides instructions for connecting direct-connect external RAID storage to K2 Summit systems.

K2 Documentation Set

Except for the release notes, the full set of support documentation, including this manual, is available in the K2 or K2/STRATUS Documentation Set. You can find the Documentation Set on the Grass Valley website. The following URL allows you to browse by K2 software version:

http://www.grassvalley.com/dl/k2_summit

You can also find the Documentation Set on the USB Recovery Flash drive that ships with your K2 Summit/Solo system.

The Documentation Set includes the following K2 product documents:

K2 AppCenter User Manual	Provides instructions for configuring and operating the media channels of product.
Quick Start Guides	The Quick Start Guide provides step-by-step installation instructions for basic installation and operation of the product.
K2 System Guide	Contains the product specifications and instructions for modifying system settings.
K2 Service Manuals	Contains information on servicing and maintaining the K2 product.
K2 SAN Installation and Service Manual	Contains installation, configuration, and maintenance procedures for shared storage options.
K2 Storage Cabling Guide	The cabling guide provides instructions for K2 Storage Area Network (SAN) cabling and external configuration. The cabling guide provides instructions for each level of K2 SAN and covers both redundant and basic (non-redundant) systems. It also provides instructions for connecting direct-connect external RAID storage to K2 Summit systems.
Fibre Channel Switch Installation Manual	Contains information on configuring and servicing the Fibre Channel switch.

On-line Help Systems

You can find documentation online with products as follows:

K2 AppCenter Help	Contains information on using K2 AppCenter. In the AppCenter user interface menu bar select **Help**, then choose **AppCenter Help Topics** from the drop-down menu.

SiteConfig Help	Contains information on using SiteConfig. In the SiteConfig user interface menu bar select **Help**, then choose **SiteConfig Help Topics** from the drop-down menu.

K2 FCP Connect documentation

The K2 FCP Connect product has its own documentation set, described as follows:

GV Connect User Manual	Provides instructions for using GV Connect, which is a Final Cut Pro plugin, to access and work with K2 assets. GV Connect is part of the K2 FCP Connect product.
GV Browse User Manual	Provides instructions for using GV Browse, which is a Final Cut Pro plugin, to access and work with assets on a MediaFrame server in an Aurora Browse system. GV Connect is part of the K2 FCP Connect product.
K2 FCP Connect Installation Manual	Provides detailed instructions to install and configure the K2 FCP Connect product.
K2 FCP Connect Release Notes	Contains the latest information about the K2 FCP Connect product, including software upgrade instructions, software specifications and requirements, feature changes from the previous releases, and any known problems. You should always check the Grass Valley Website to determine if there is an updated version of release notes available.

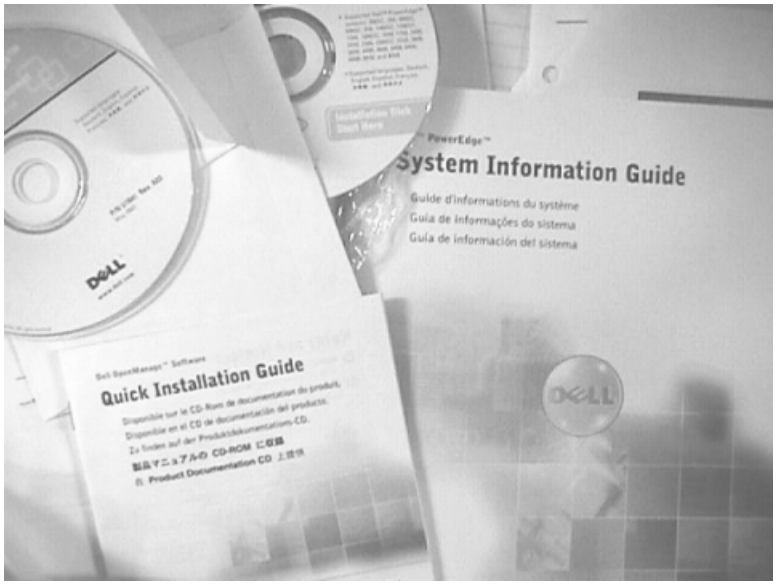
Grass Valley Website

This public Web site contains all the latest manuals and documentation, and additional support information. Use the following URL.

http://www.grassvalley.com

Dell Server Documentation

If your system includes a Grass Valley product on a Dell server platform, refer to the applicable Grass Valley product manual for installation and configuration information. However, a full set of Dell server documentation has been provided on the *Dell Product Documentation* CD-ROM. Refer to the documents on this CD-ROM only as required by procedures in Grass Valley product manual.



Information referenced on the *Dell Product Documentation* CD-ROM includes, but is not limited to:

- Unpacking and rack-mounting
- Important safety and regulatory information
- Status indicators, messages, and error codes
- Troubleshooting help

⚠ ***CAUTION: Do not use the Dell Quick Installation Guide provided with the Dell CD-ROM package. This guide includes instructions for using the OpenManage software CD-ROM to install an operating system, which is not necessary on the Grass Valley product.***

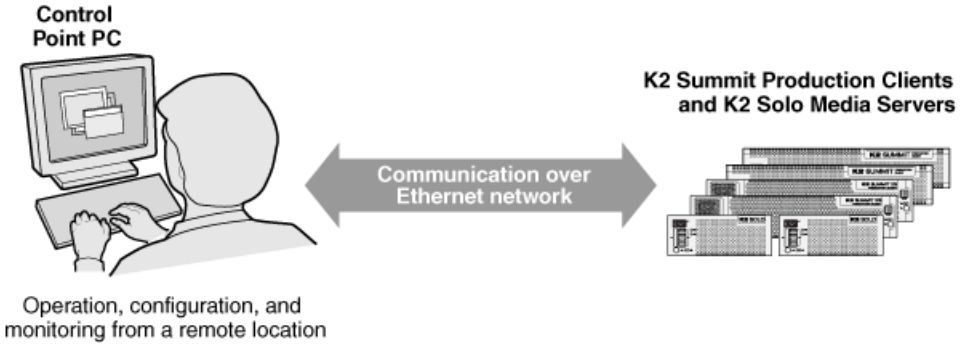
Chapter 1

Product description

This section contains the following topics:

About K2 systems

The K2 Summit/Solo system is a cost-effective Broadcast Enterprise Server that incorporates IT server platform and storage technologies to deliver a networked solution to facilities for ingest, playout, news integration, sports, and media asset management. Each K2 system model is a comprehensive platform that provides a suite of user applications, system tools, and the largest range of third-party interactivity in the industry.



The K2 Summit/Solo system is designed for "headless" operation from a remote control point using Grass Valley Control Point software. You can also use the Microsoft Windows Remote Desktop Connection application on your PC to connect to the K2 system for configuration or administration.

The K2 Summit/Solo system is further described in the following topics. Also refer to topics on Transmission models for information unique to those products.

K2 Summit 3G system features

The following features apply to the K2 Summit 3G Production Client:

- Windows 7 64-bit embedded operating system
- Embedded Security for protection against viruses and other unauthorized programs.
- Bidirectional channels (channel can be either an input channel or it can be an output channel)
- Two or four channels per chassis
- SDI video inputs and outputs
- AES/EBU or embedded audio inputs and outputs.
- Standard Definition (SD) video formats and High Definition (HD) video formats
- AVCHD and H.264 play output (decode) as an option.
- 3G codec module hosts codec option cards that are programmable for multiple formats and functions.
- Mixed format playback of SD or HD clips on the same timeline
- Up/down/cross HD/SD conversion (e.g. SD and HD clips ingested, then played back as SD or HD clips) or as a different SD or HD format (e.g. 720p to 1080i).
- VGA monitoring capability
- Redundant power supply, cooling fans for reliability

- 2.5 inch media storage drives
- mSATA SSD system drive
- Type III CPU carrier module with 8 GB RAM
- USB 3.0 interface for file exchange
- Ability to create nested bins, i.e. sub-bins within bins
- Freeze mode can be frame or field
- Various video mix effects (e.g. dissolves between two video and audio tracks on the same channel, or fade thru matte color)
- Remote operation and configuration via AppCenter
- Gigabit Ethernet
- AMP, VDCP, and BVW remote control protocols supported
- Remote control over RS-422 or Ethernet
- Super Slo-Mo, Multi-cam, and 3D/Video + Key features are available as part of the ChannelFlex Suite
- Low-resolution proxy files created during record and live streaming from SDI In/out are available as part of the AppCenter Pro and Elite licenses
- RAID media storage
- Stand-alone internal storage, stand-alone external direct-connect storage, and external shared (SAN) storage

Related Topics

Specifications on page 215

K2 Summit system features

The following features apply to the first-generation K2 Summit Production Client:

- Bidirectional channels (channel can be either an input channel or it can be an output channel)
- Two or four channels per chassis
- SDI video inputs and outputs
- AES/EBU or embedded audio inputs and outputs.
- Standard Definition (SD) video formats and High Definition (HD) video formats
- Mixed format playback of SD or HD clips on the same timeline
- Up/down/cross HD/SD conversion (e.g. SD and HD clips ingested, then played back as SD or HD clips) or as a different SD or HD format (e.g. 720p to 1080i).
- VGA monitoring capability
- Redundant power supply, cooling fans for reliability
- 3.5 inch media storage drives
- CompactFlash system drive
- Ability to create nested bins, i.e. sub-bins within bins
- Freeze mode can be frame or field
- Various video mix effects (e.g. dissolves between two video and audio tracks on the same channel, or fade thru matte color)
- Remote operation and configuration via AppCenter
- Gigabit Ethernet

- AMP, VDCP, and BVW remote control protocols supported
- Remote control over RS-422 or Ethernet
- Super Slo-Mo, Multi-cam, and 3D/Video + Key features are available as part of the ChannelFlex Suite.
- Low-resolution proxy files created during record and live streaming from SDI In/out are available as part of the AppCenter Pro and Elite licenses. This requires the Type II carrier module.
- RAID media storage
- Stand-alone internal storage, stand-alone external direct-connect storage, and external shared (SAN) storage

Related Topics

Specifications on page 215
K2 Summit Transmission models features on page 198

K2 Solo 3G system features

The following features apply to the K2 Solo 3G Media Server:

- Windows 7 64-bit embedded operating system
- Embedded Security for protection against viruses and other unauthorized programs.
- Bidirectional channels (channel can be either an input channel or it can be an output channel)
- Two channels per chassis
- SDI video inputs and outputs
- AES/EBU or embedded audio inputs and outputs.
- Standard Definition (SD) video formats and High Definition (HD) video formats
- AVCHD and H.264 play output (decode) as an option.
- 3G codec module. Codec option card not supported on K2 Solo system.
- Mixed format playback of SD or HD clips on the same timeline
- Up/down/cross HD/SD conversion (e.g. SD and HD clips ingested, then played back as SD or HD clips) or as a different SD or HD format (e.g. 720p to 1080i). Aspect ratios are adjusted.
- VGA monitoring capability
- Compact Flash System drive
- Type III CPU carrier module with 8 GB RAM
- USB 3.0 interface for file exchange
- Ability to create nested bins, i.e. sub-bins within bins
- Freeze mode can be frame or field
- Various video mix effects (e.g. dissolves between two video and audio tracks on the same channel, or fade thru matte color)
- Remote operation and configuration via AppCenter
- Gigabit Ethernet
- AMP, VDCP, and BVW remote control protocols supported
- Remote control over RS-422 or Ethernet
- ExpressCard
- Super Slo-Mo, Multi-cam, and 3D/Video + Key features are available as part of the ChannelFlex Suite.

- Low-resolution proxy files created during record and live streaming from SDI In/out are available as part of the AppCenter Pro and Elite licenses. This requires the Type II carrier module.
- RAID 0 internal media storage
- Support for Dyno S.

K2 Solo system features

The following features apply to the first-generation K2 Solo Media Server:

- Bidirectional channels (channel can be either an input channel or it can be an output channel)
- Two channels per chassis
- SDI video inputs and outputs
- AES/EBU or embedded audio inputs and outputs.
- Standard Definition (SD) video formats and High Definition (HD) video formats
- Mixed format playback of SD or HD clips on the same timeline
- Up/down/cross HD/SD conversion (e.g. SD and HD clips ingested, then played back as SD or HD clips) or as a different SD or HD format (e.g. 720p to 1080i). Aspect ratios are adjusted.
- VGA monitoring capability
- CompactFlash system drive
- Ability to create nested bins, i.e. sub-bins within bins
- Freeze mode can be frame or field
- Various video mix effects (e.g. dissolves between two video and audio tracks on the same channel, or fade thru matte color)
- Remote operation and configuration via AppCenter
- Gigabit Ethernet
- AMP, VDCP, and BVW remote control protocols supported
- Remote control over RS-422 or Ethernet
- ExpressCard
- Super Slo-Mo, Multi-cam, and 3D/Video + Key features are available as part of the ChannelFlex Suite.
- Low-resolution proxy files created during record and live streaming from SDI In/out are available as part of the AppCenter Pro and Elite licenses. This requires the Type II carrier module.
- RAID 0 internal media storage

K2 Summit/Solo formats, models, licenses, and hardware support

Formats are supported as in the following tables.

Table 1: First-generation K2 Summit/Solo system

Formats	Compression	1x	Multi-Cam, 3D/Video + Key	Super Slo-Mo
SD	DV	Encode/decode	Encode/decode	Not supported.

Formats	Compression	1x	Multi-Cam, 3D/Video + Key	Super Slo-Mo
	MPEG-2	Decode is standard. Encode requires codec option card.	Not supported.	Not supported.
	AVCHD	Not supported.	Not supported.	Not supported.
1080i/720p	DV	Encode/decode. Requires HD license.	Encode/decode. Requires HD license.	Encode/decode. Requires HD license.
	MPEG-2	Decode is standard. Encode requires codec option card. Requires HD license.	Not supported.	Not supported.
	AVC-Intra	Encode/decode. Requires coded option card. Requires HD license.	Encode/decode. Requires coded option card. Requires HD license.	Not supported.
	AVCHD	Not supported	Not supported	Not supported

Table 2: K2 Summit 3G system

Formats	Compression	1x	Multi-Cam, 3D/Video + Key	Super Slo-Mo
SD	DV	Encode/decode	Encode/decode	Not supported.
	MPEG-2	Encode/decode	Encode/decode. Requires codec option card.	Not supported.
	AVCHD/H.264	Decode only. Requires AVC license.	Not supported	Not supported
1080i/720p	DV	Encode/decode. HD license is standard.	Encode/decode. HD license is standard.	Encode/decode. HD license is standard.
	MPEG-2	Encode/decode. HD license is standard.	Encode/decode. Requires codec option card. HD license is standard.	Not supported.
	AVC-Intra	Encode/decode. Requires AVC license. HD license is standard.	Encode/decode. Requires AVC license. HD license is standard.	Encode/decode. Requires AVC license. HD license is standard.

Formats	Compression	1x	Multi-Cam, 3D/Video + Key	Super Slo-Mo
	AVCHD/H.264	Decode only. Requires AVC license.	Not supported	Not supported

Table 3: K2 Solo 3G system

Formats	Compression	1x	Multi-Cam, 3D/Video + Key	Super Slo-Mo
SD	DV	Encode/decode	Encode/decode	Not supported.
	MPEG-2	Encode/decode	Not supported	Not supported
	AVCHD/H.264	Decode only. Requires AVC license.	Not supported	Not supported
1080i/720p	DV	Encode/decode. HD license is standard.	Encode/decode. HD license is standard.	Encode/decode. HD license is standard.
	MPEG-2	Encode/decode. HD license is standard.	Not supported	Not supported
	AVC-Intra	Encode/decode. Requires AVC license. HD license is standard.	Encode/decode. Requires AVC license. HD license is standard.	Encode/decode. Requires AVC license. HD license is standard.
	AVCHD/H.264	Decode only. Requires AVC license.	Not supported	Not supported

Features of internal storage models

K2 Summit/Solo systems have media drives as follows:

- First generation K2 Summit system — Up to eight media drives
- K2 Summit 3G system — Up to twelve media drives
- K2 Solo Media Server — Two media drives
- K2 Solo 3G Media Server — Two media drives

This makes the internal storage K2 system a self-contained, stand-alone unit, with no external devices for storage connections required. You can transfer media in and out of the internal storage K2 system via Gigabit Ethernet. You can also export media to a mapped drive or USB-attached storage. With the K2 Solo Media Server, you can also export media via an ExpressCard.

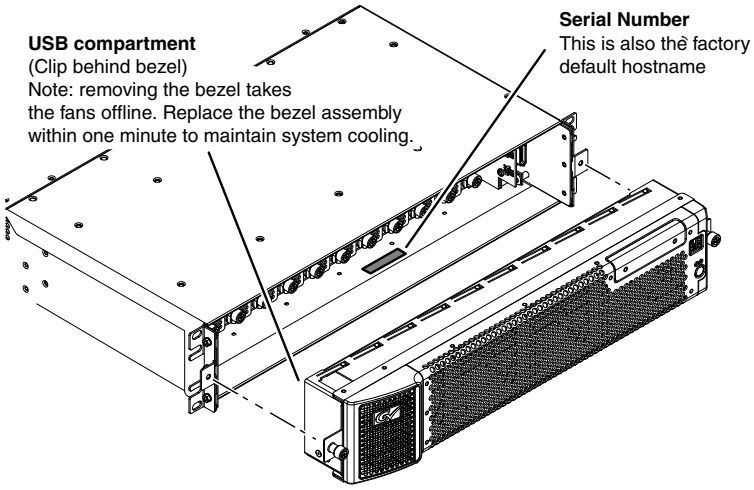
Features of external storage models

The external storage K2 Summit system contains only the system drive. There are no media drives in an external storage K2 Summit system. There are two types of external storage for media, as follows:

- Shared storage — Multiple external storage K2 Summit systems connect to the K2 SAN via Gigabit Ethernet or Fibre Channel to share a common pool of storage.
- Direct-connect storage — A single K2 Summit system with the optional Fibre Channel board installed connects directly to its own external (non-shared) RAID storage device. This makes the direct-connect K2 Summit system a self-contained, stand-alone unit, with no additional devices for storage connections required. You can transfer media in and out of the direct-connect K2 Summit system via Gigabit Ethernet.

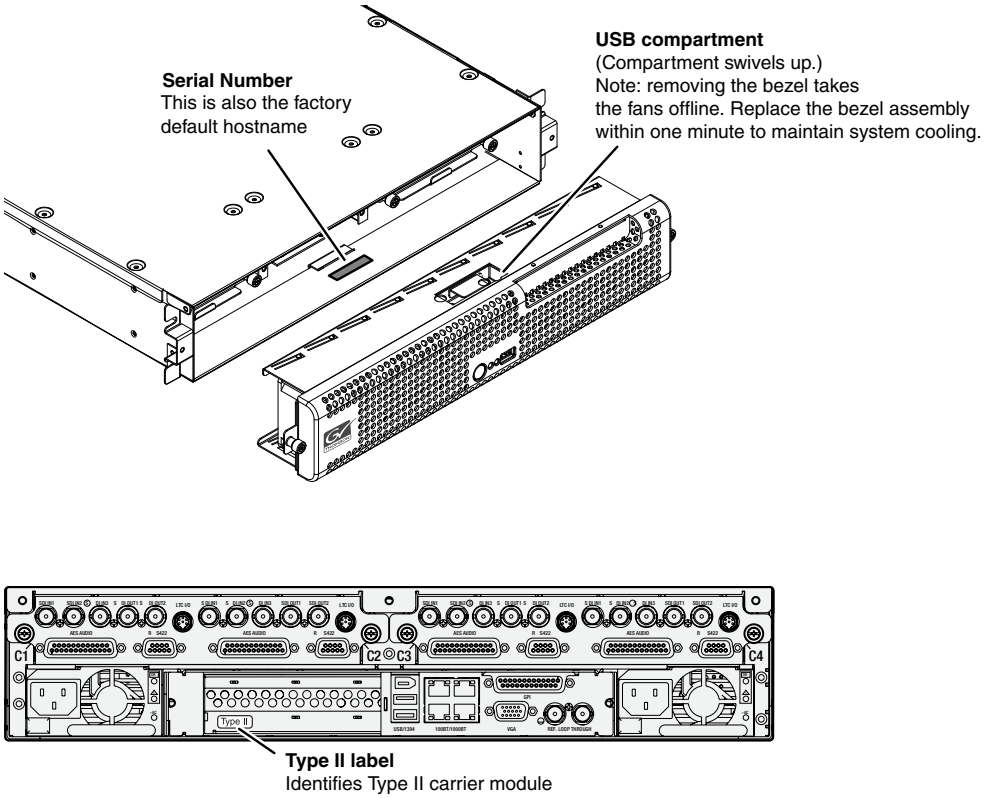
Product identification K2 Summit 3G

The K2 Summit 3G system has labels affixed to the chassis that provide product identification as illustrated:



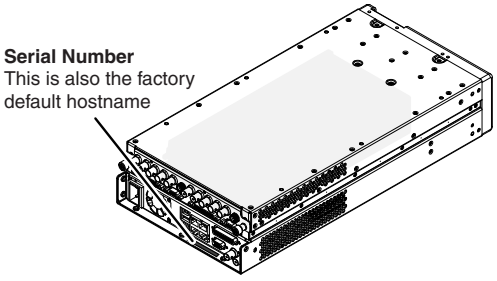
Product identification first generation K2 Summit

The first generation K2 Summit system has labels affixed to the chassis that provide product identification as illustrated:



Product identification K2 Solo

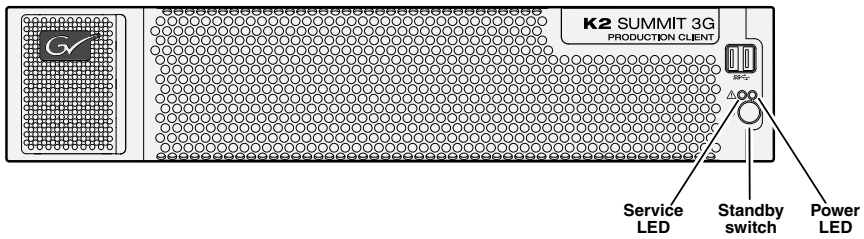
K2 Solo system have labels affixed to the chassis that provide product identification as illustrated:



Front panel indicators K2 Summit 3G system

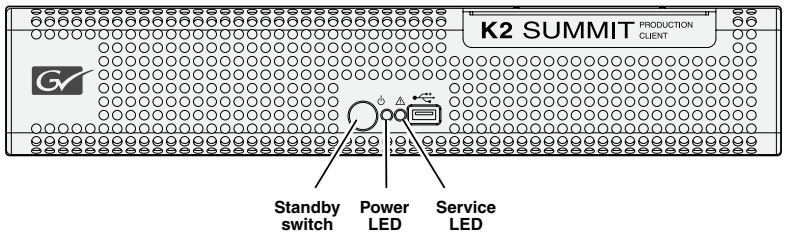
With the front bezel in place, the indicator LEDs are visible. The LEDs indicate the status of the machine. For example, when the Service LED is a steady yellow light, this could signify that one

of the power cables is unplugged. For more information on indicator LEDs, see the service manual for your K2 product.



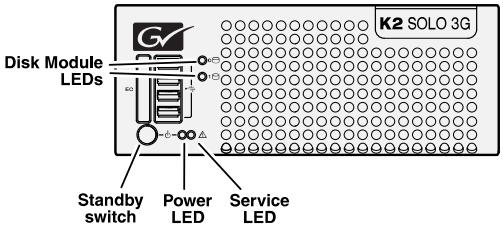
Front panel indicators first-generation K2 Summit

With the front bezel in place, the indicator LEDs are visible. The LEDs indicate the status of the machine. For example, when the Service LED is a steady yellow light, this could signify that one of the power cables is unplugged. For more information on indicator LEDs, see the service manual for your K2 product.



Front panel indicators K2 Solo

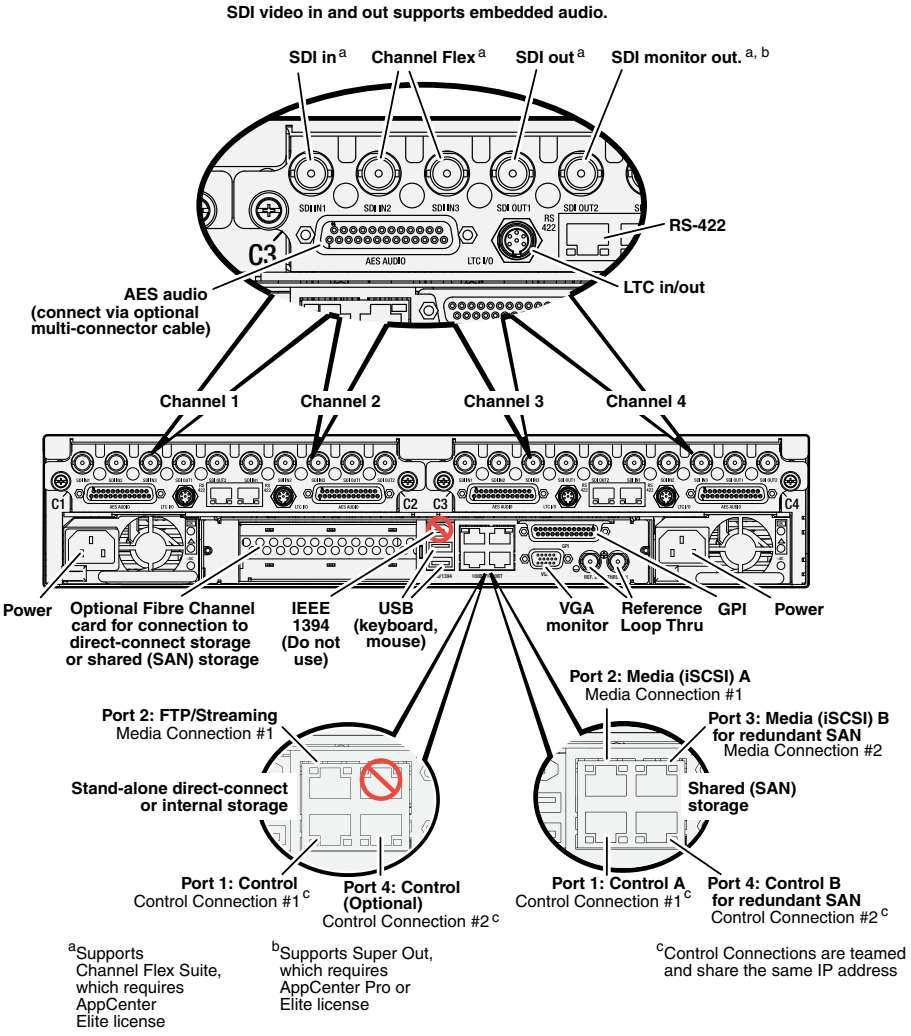
Both the first-generation K2 Solo system and the K2 Solo 3G system have the same front panel indicators. With the front bezel in place, the indicator LEDs are visible. The LEDs indicate the status of the machine. For example, when the Service LED is a steady yellow light, this could signify that one of the power cables is unplugged. For more information on indicator LEDs, see the service manual for your K2 product.



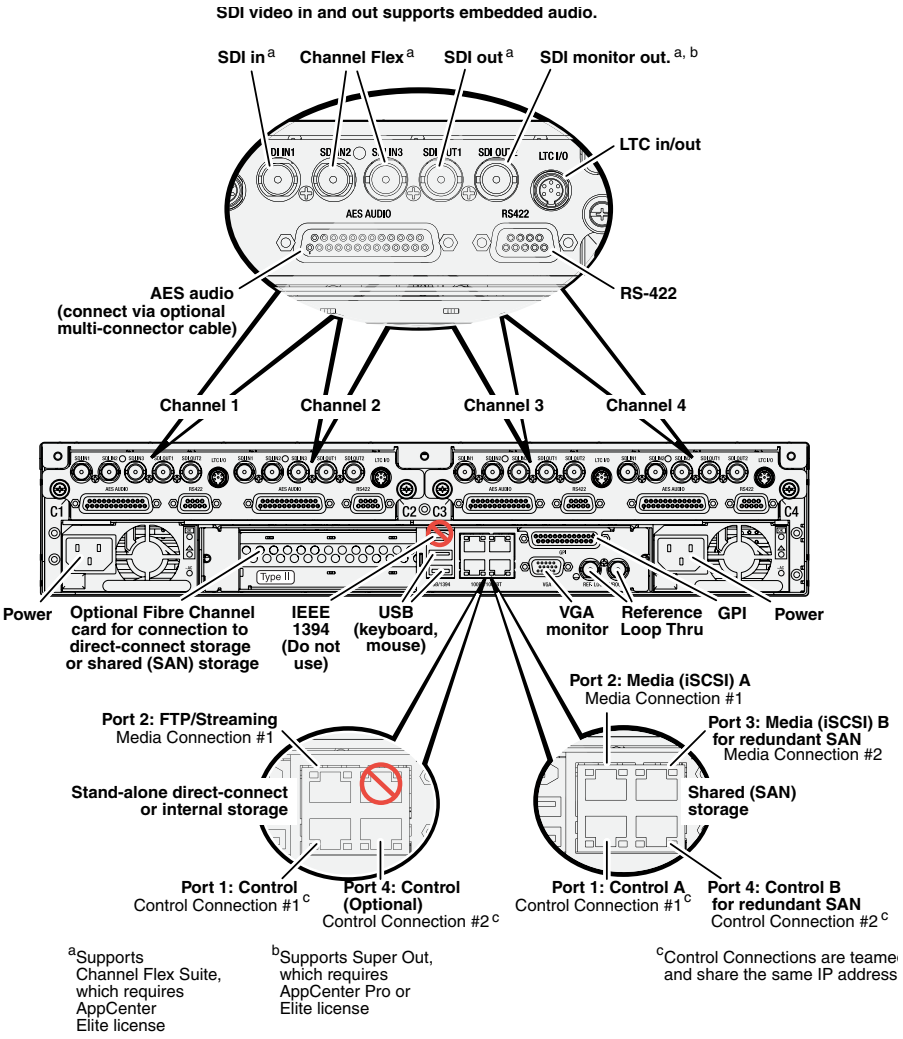
Rear panel view

The following illustrations identify the rear panel connectors and components.

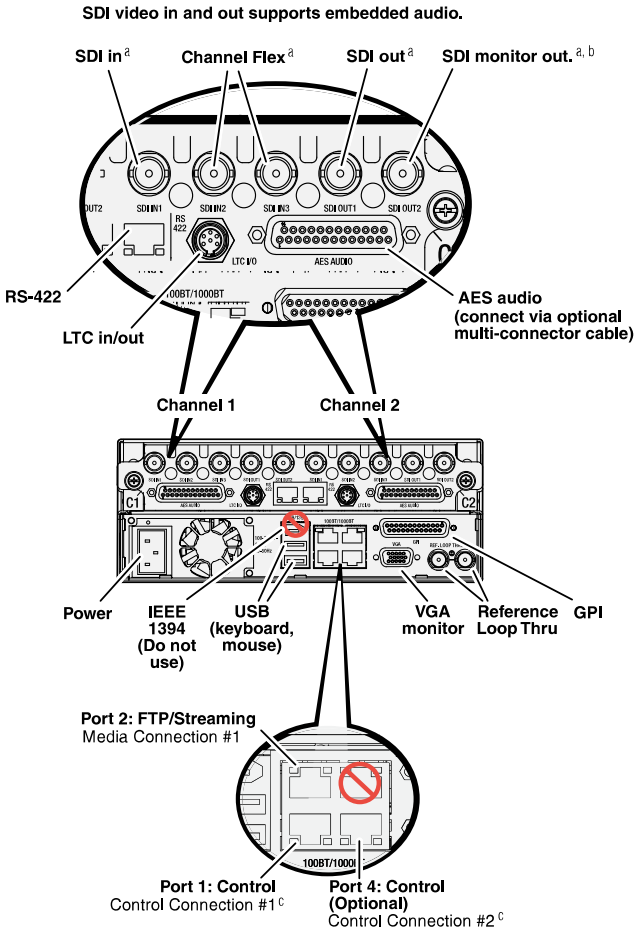
K2 Summit 3G models rear panel



K2 Summit first generation models rear panel



K2 Solo 3G Media Server rear panel

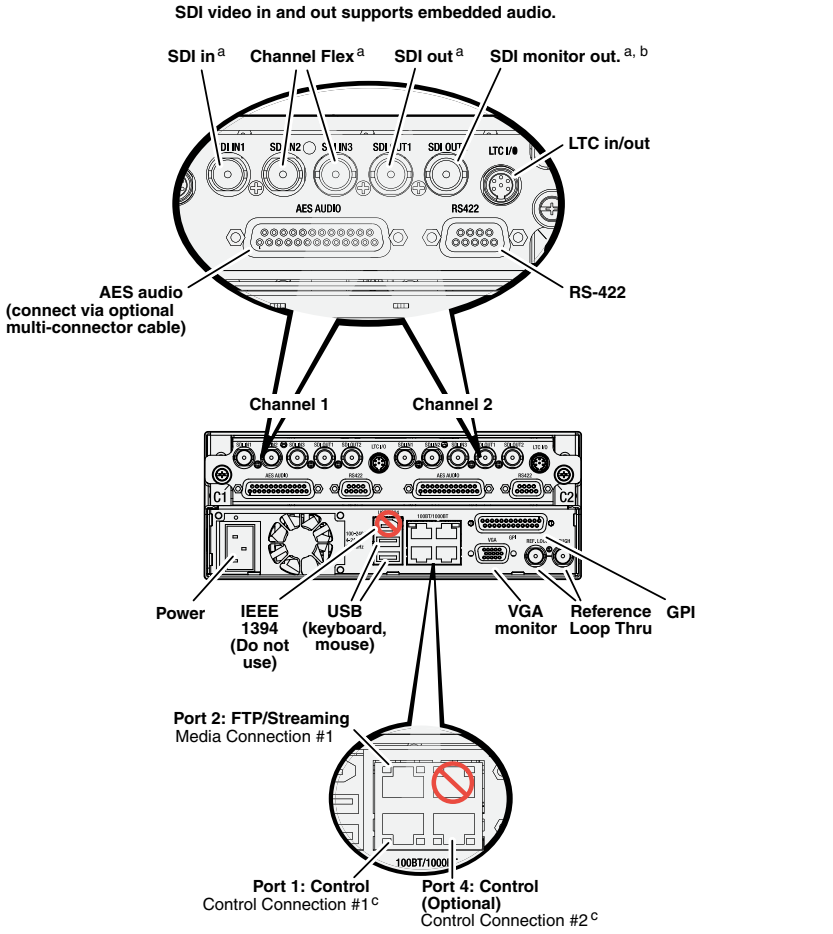


[a] Supports Channel Flex Suite, which requires AppCenter Elite license

[b] Supports Super Out, which requires AppCenter Pro or Elite license

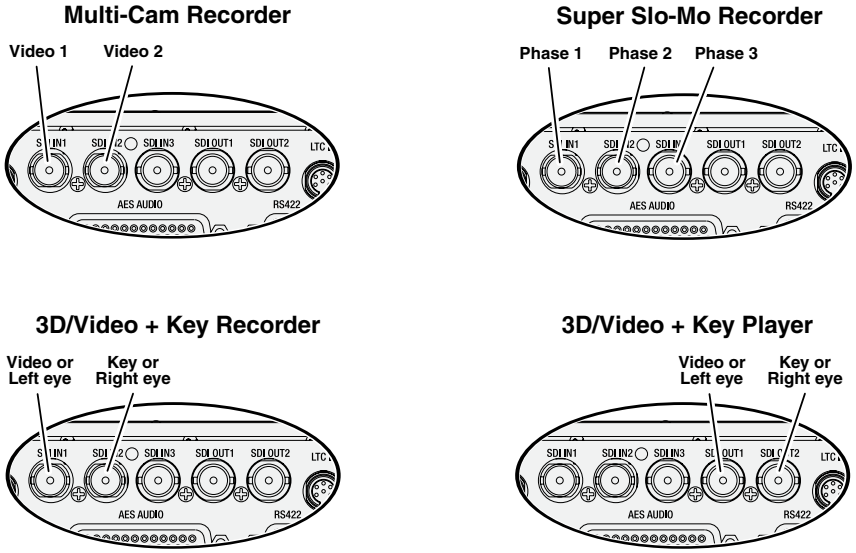
[c] Control Connections are teamed and share the same IP address

K2 Solo Media Server rear panel



ChannelFlex rear panel connections

ChannelFlex Suite features require the AppCenter Elite license. Super Slo-Mo also requires the HD license. When configured for these features, channel connections are as follows:



Refer to the *K2 AppCenter User Manual* for more information on ChannelFlex Suite features.

Considerations for first startup out of box

When you receive a K2 system from the factory, one or more End User License Agreements (EULAs) appear on the screen at first startup. Software licensing agreements require that you accept these EULAs. When you do so, start up processes can proceed. This behavior occurs only at first startup. Subsequent startups do not exhibit this behavior.

K2 Summit/Solo system overview

The K2 Summit/Solo system are purpose-built clients based on COM Express compact computer with dedicated systems to provide the video disk recorder functionality. This section explains the major architectural blocks.

Related Topics

Application System on page 44
Real Time System on page 44
Media control and processing on page 44
Loop through, E to E, and feeds on page 45

Application System

The K2 Summit Production Client and K2 Solo Media Server application system architecture uses the COM Express form factor to provide functionality similar to that of standard PC-type computers. The carrier module contains a CPU module, built in Ethernet, and USB ports. On the K2 Summit Production Client, the carrier module also includes one PCIe board slot for expansion.

The Application system uses a Windows embedded operating system upon which all internal storage K2 system applications run for configuration and control of the unit.

Real Time System

Each channel hosts a complete Real Time system that provides the core video disk recorder functionality. Primary components are as follows:

- Dedicated processor for media access and processing.
- Codec circuits responsible for encoding/decoding video and processing audio and timecode, including the media-related input and output connectors.

The Real Time system uses a dedicated operating system. This operating system manages all the hardware involved in controlling the flow of video, audio, timecode, genlock, and GPI in and out of the K2 system.

Media control and processing

The following section explains how the Application system and the Real Time system work together to provide K2 system functionality.

The high processing requirements of digital video can overwhelm the processor on a standard desktop PC, resulting in wait-times that destroy the video's essential real-time aspect. The K2 system avoids this problem by providing dedicated systems that isolate processing needs. The components that work together to provide this functionality are as follows:

Application system — Dedicated to control, configuration, and networking functions that do not require real-time accuracy. The Application system has the following components:

- Application software provides the user interface for operating the K2 system. The software runs as Windows programs.
- The Media File system manages clips. It includes a database that associates the clip with its video, audio, and timecode files and a dedicated file system (separate from the Windows file system) that controls access to the raw data that makes up each file. Any reading and writing of clips, be it through play and record operations or through file transfers and media streaming, is managed by the database. The database and file system run as Windows programs.

Storage system — Includes the media disk drives, controllers, drivers, and adapters necessary for access and movement of the data. While the primary data flow is within the overall control of the Real Time system, some components and their communication pathways cross over into the Application system. For example, the media drives appear as the V: drive to the Windows operating system.

Real Time system — Manages the media flow between the Storage system and the inputs and outputs. The Real Time system has dedicated processors and time-sensitive mechanisms to serve media processing needs while maintaining real-time accuracy.

When you control play and record operations from within the Application system you trigger a chain of events that eventually crosses over into the Real Time system and results in media access. The following sequence is an example of this type of chain of events:

1. A user operates the Player application to play a particular clip. The Player application asks the Media File system for permission to access the clip. The Media File system grants access. In shared storage models, the Media File system enforces shared storage policies in order to grant the access. When access is granted, the Player application initiates play access to the clip.
2. The database identifies the files that make up the clip and the file system instructs the Storage system to open access to the files.
3. The Storage system finds the raw data and opens the appropriate read access. At this point both the Application system and the Real Time system are involved. Windows controls the media drives and controllers, so the Real Time system makes file requests to Windows and it causes the data to be transferred to buffers on the Real Time processor. The data is then available to the Real Time system so that it can be processed at exactly the right time.
4. The Real Time system processes the media, decompresses it, adjusts its timing, and moves it as required to play the clip as specified by the user.

Loop through, E to E, and feeds

Behaviors related to input signals routed to output connectors are described in the following topics.

Related Topics

Remote control protocols on page 209

Recording synchronous and asynchronous feeds

For best results in all workflows, use synchronous feeds, defined as follows:

- All outputs are locked to the house reference
- All inputs are genlocked to the house reference and at zero time

The K2 Summit Production Client and K2 Solo Media Server can record inputs that are asynchronous, with the following considerations:

- The encoder clock and the audio clock are derived from the input signal, which enables frame accurate recording of all inputs.
- Outputs are timed to the reference and if no reference is present, the output runs free.
- If the input video rate does not equal the output video rate (asynchronous) then video tearing or jumping can occur when input/output synch is critical, such as in the following:
  - K2 TimeDelay
  - SD-00 or Summit E-to-E (LoopThru) mode
  - HD-00 Loopback

Loop through on K2 Summit/Solo

The Player/Recorder application has a "E-to-E (LoopThru) mode" selection on the Control menu. This mode applies when the channel is under local AppCenter control as well as when it is under remote control, for all protocols.

This "E-to-E (LoopThru) mode" feature allows you to monitor the video that is being recorded. The video is routed back essentially untouched. Any audio or timecode that is on the input video stream is still there on the loop through output. The K2 Summit/Solo system and the loop through videos must be locked to a video reference for the loop through feature to work properly. This "E-to-E (LoopThru) mode" feature should not be confused with true E to E. True E to E is not supported on the K2 Summit/Solo system.

When "E-to-E (LoopThru) mode" is not selected, the channel behaves as follows:

- "PB" is displayed on the channel pane, next to the Timecode Source indicator.
- When no clip is loaded, black plays out.
- When a record operation stops, Recorder becomes Player and the clip remains in the Player. The clip's last frame plays out.

When "E-to-E (LoopThru) mode" is selected, the channel behaves as follows:

- "EE" is displayed on the channel pane, next to the Timecode Source indicator.
- When no clip is loaded, the signal that is currently present at the channel input plays out.
- When a record operation stops, Recorder stays Recorder and the clip remains in the Recorder. The signal that is currently present at the channel input plays out.

Ports used by K2 services

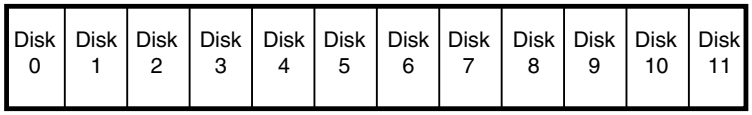
The following ports are used by the applications and system tools of the K2 family of products:

20	TCP: Used by mpgsession.exe, mxfsession.exe, gxfsession.exe, or ftpd.exe for FTP.
21	TCP: Used by ftpd.exe for FTP data.
161	UDP: Used by snmp.exe for SNMP.
162	UDP: Used by snmptrap.exe for SNMP trap.
3389	TCP: Used by Remote Desktop for use by SiteConfig.
3811	TCP: Used by Grass Valley AppService for 3rd party applications to communicate using AMP protocol. Used by SDB and XMOS Server AMP Communication.
8080	HTTP: Used by STRATUS Summit Services.
8100	HTTP: Used by Macintosh systems for the SabreTooth licensing web service to check out licenses
8732	HTTP: Used by Site Config data service .
8733	HTTP: Used by K2 Config data service .
8734	HTTP: Used by Site Config data service .
8735	HTTP: Used by K2 Config data service.

18262	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.
18263	UDP: Used by ProductFrame Discovery Agent Service for GV NetConfig Device Broadcast/Unicast Protocol. Used by SiteConfig. Sent by ControlPoint, received by Devices
18264	UDP: Used by ProductFrame Discovery Agent Service for GV NetConfig Controller Protocol. Used by SiteConfig. Sent by Devices, received by ControlPoint
31820	UDP: Used for live streaming from K2 Summit/Solo systems. This is the default base for UDP ports, with the range being 31820 to 31827. Other ranges are possible, depending on the UDP port base configured on the K2 Summit/Solo system.
49168	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.
49169	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.
49170	HTTP: Used by Grass Valley Transfer Queue Service for Transfer Manager connection between source system and destination system.
49171	TCP: Used by Grass Valley AppService for AppCenter connection between control point PC and K2 client/Solo.
49172	HTTP: Used by Grass Valley Storage Utility Host for connection for Storage Utility between the control point PC and the K2 system being configured.
50872	UDP: Used by K2 Appcenter to discover K2 systems on the network.

RAID drive numbering K2 Summit 3G system

In the K2 Summit 3G system, internal RAID drives are numbered as follows. This numbering is displayed in Storage Utility.



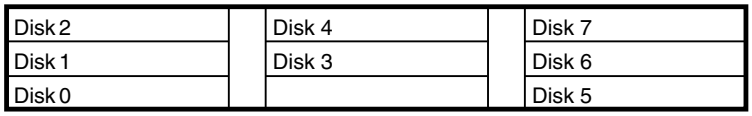
Drives are configured as RAID 1.

Drive numbering	Explanation
Disk 0	These two RAID drives make up LUN 0.
Disk 1	
Disk 2	These two RAID drives make up LUN 1.
Disk 3	

Drive numbering	Explanation
Disk 4	These two RAID drives make up LUN 2.
Disk 5	
Disk 6	These two RAID drives make up LUN 3.
Disk 7	
Disk 8	These two RAID drives make up LUN 4.
Disk 9	
Disk 10	These two RAID drives make up LUN 5.
Disk 11	

RAID drive numbering first generation K2 Summit system

In the first generation K2 Summit system, internal RAID drives are numbered as follows. This numbering is displayed in Storage Utility. You cannot see the labeling on the K2 Summit Production Client chassis RAID drive when you remove the fan module.

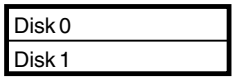


Drive numbering	Explanation
Disk 0	When configured as RAID 1, these two RAID drives make up LUN 0.
Disk 1	
Disk 2	When configured as RAID 1, these two RAID drives make up LUN 1.
Disk 3	
Disk 4	When configured as RAID 1, these two RAID drives make up LUN 2.
Disk 5	
Disk 6	When configured as RAID 1, these two RAID drives make up LUN 3.
Disk 7	

When drives are configured as RAID 0, each drive is considered its own LUN. As such, the order of LUNs and drive numbers as displayed in Storage Utility does not always correlate with the position of drives in the chassis.

RAID drive numbering K2 Solo system

In the K2 Solo system, internal RAID drives are numbered as follows.



NOTE: **K2 Solo system** ***drives are always configured as RAID 0.***

When drives are configured as RAID 0, each drive is considered its own LUN. As such, the order of LUNs and drive numbers as displayed in Storage Utility does not always correlate with the position of drives in the chassis.

Chapter 2

Overview of K2 System Tools

This section contains the following topics:

Configuration Manager

The Configuration Manager is the primary configuration tool for a K2 Summit/Solo system. It makes settings that apply to the overall internal storage K2 Summit/Solo system as well as settings that apply to individual channels.

Configuration Manager settings are stored in a database. When the K2 Summit/Solo system starts up it reads the current settings from the database and configures itself accordingly. When you modify a setting in Configuration Manager you must save the setting in order to update the database and reconfigure the K2 Summit/Solo system.

You can also save settings out of Configuration Manager into a configuration file, which is a stand-alone XML file. Likewise, you can load settings into Configuration Manager from a configuration file. However, you must use Configuration Manager as the means to save the settings to the database before the settings actually take effect. Configuration files are not linked directly to the database.

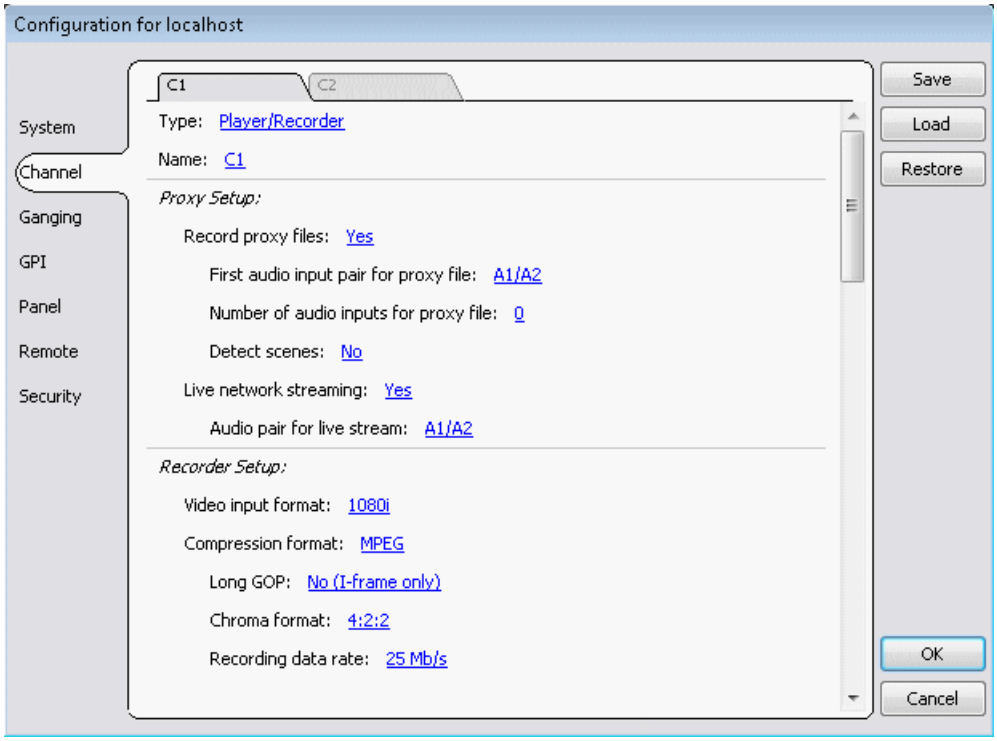
You can use configuration files as a means to back up your settings. You can also use configuration files to save several different groups of customized settings, each with a unique name, so that you can quickly load settings for specialized applications.

If you save a configuration file and then upgrade your K2 system software, there can be compatiblity issues. If the upgraded software version has new features, the saved configuration file might not be compatible.

Accessing Configuration Manager

You access Configuration Manager through the K2 AppCenter application from the local K2 Summit/Solo system or from the Control Point PC.

To access the configuration settings, open AppCenter and select **System | Configuration**.



Saving and restoring Configuration Manager settings

Settings can be saved as a configuration file. You can save any number of uniquely named custom configuration files. You can load a configuration file to restore system settings.

To save custom settings:

1. In the Configuration Manager, click the **Save** button.

   The Save As dialog opens.
2. Use the up arrow or select folders to navigate to the folder in which you want to save the configuration file.
3. Enter a name for the configuration file.

   Do not name the file *Default*Config.xml, as this name is reserved for the factory default configuration file. Otherwise, standard Windows 2000 and up file naming restrictions apply.
4. Click **Save** and **Close**.

To restore custom settings:

1. If you want to save current settings, you should save them as a configuration file before continuing.
2. In the Configuration Manager, click the **Load** button.

   The Open dialog opens.
3. Use the up arrow or select folders to navigate to the custom configuration file.
4. Select the custom configuration file.
5. Click **Open**.

   The custom settings are loaded into Configuration Manager, but they have not been saved and put into effect.
6. Click **OK** to save and apply settings, and to close the Configuration Manager.

Restoring default Configuration Manager settings

You can restore factory default settings as follows:

- Restore some individual settings or groups of settings by selecting the **Default** button which appears below the settings in the configuration screen.
- Restore all the settings in Configuration Manager at once to their default values as explained in the following procedure.

1. If you want to save current settings you should do so before proceeding.
2. In the Configuration Manager dialog, click **Restore**.

   The default settings are loaded into Configuration Manager, but they have not yet been saved and put into effect.
3. Click **OK** to save settings and close Configuration Manager.

Related Topics

Saving and restoring Configuration Manager settings on page 53

K2Config

The K2 System Configuration application (K2Config) is the primary tool for configuring systems in the category of a K2 SAN, which include online or production K2 SANs, K2 Nearline systems, and STRATUS Proxy Storage systems. Once the devices of the storage system are cabled and are communicating on the control network, you can do all the configuration required to create a working K2 SAN using the K2Config application. When you use SiteConfig for network configuration, you can import the SiteConfig system description file into the K2Config application to get you started with your SAN configuration.

After your K2 SAN is initially installed and configured, if you need to reconfigure the system you should do so using SiteConfig and the K2Config application. This enforces consistent policy and sequencing for configuration tasks, which makes the system easier to maintain and aids in troubleshooting should a problem arise.

The K2Config application runs on a control point PC and accesses the devices of the K2 SAN via the control network. You can configure the devices of the K2 SAN as follows:

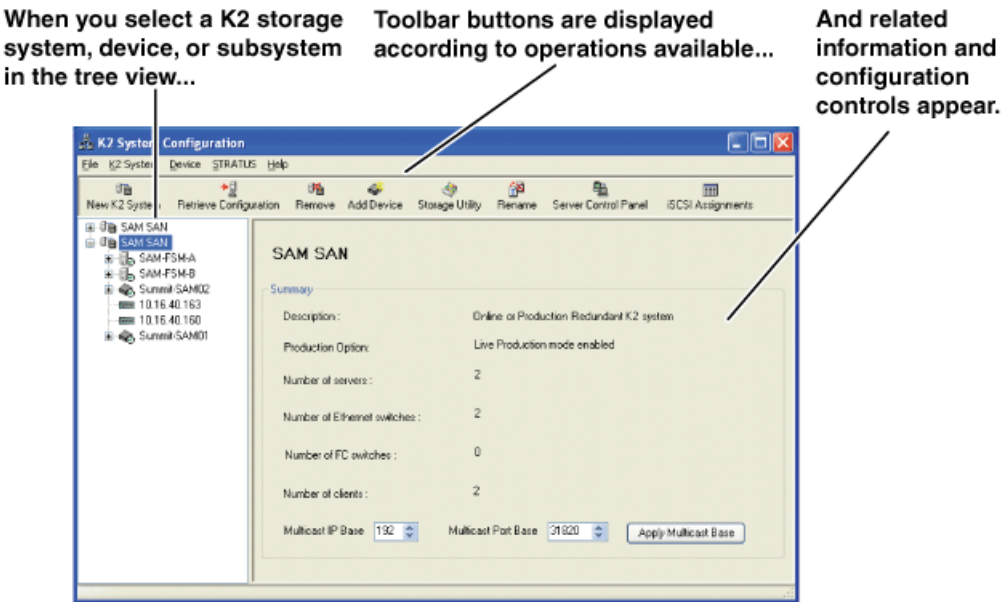
- SAN-attached K2/Summit systems and K2 Media Server — These devices are configured directly by the K2Config application.
- K2 RAID storage devices — The K2Config application launches a remote instance of Storage Utility, which configures RAID storage devices. Storage Utility components run on the K2 Media Server and the configuration actually takes place via the Fibre Channel connection between the K2 Media Server and the RAID storage device.
- Ethernet switches — The K2Config application can launch a switch's web-based configuration application.

You can expand and select nodes in the tree view to view K2 SANs, individual devices, and configuration settings. The configuration file is saved on the V: drive, along with the media files in the shared storage system. The configuration file is updated and saved whenever you change a configuration using the K2Config application. That is why you must always use the K2Config application to change settings on the storage system, so the most recently changed configurations will always be stored in the configuration file and displayed.

Opening the K2Config application

1. On the control point PC open the K2Config application shortcut on the desktop. The K2Config application log in dialog box opens.
2. Log in using the designated administrator account for configuring K2 SAN devices.

3. The K2Config application opens.



If you have one or more K2 SANs currently configured, the K2Config application displays the systems in the tree view.

If you have not yet configured a K2 SAN, the K2Config application opens with the tree view blank.

Storage Utility for standalone K2 Summit/Solo system

There are two versions of Storage Utility:

- Storage Utility for the K2 SAN
- Storage Utility for stand-alone K2 systems

This manual explains Storage Utility for stand-alone K2 Summit/Solo system. Refer to the *K2 SAN Installation and Service Manual* to learn about Storage Utility for the K2 SAN.

NOTE: For shared storage, run Storage Utility only via the* K2Config *application.

The Storage Utility is your primary access to the media file system, the media database, and the media disks of the K2 Summit/Solo system for configuration, maintenance, and repair. It is launched from the K2 AppCenter application.

⚠ ***CAUTION: Use the Storage Utility only as directed by a documented procedure or by Grass Valley Support. If used improperly, the Storage Utility can render your K2 system inoperable or result in the loss of all your media.***

NOTE: Do not use the MegaRAID utility on a K2 system. This utility is for use by qualified Grass Valley Service personnel only. When this utility is opened it scans the SCSI bus and interferes with record and play operations.

Remote Desktop Connection

You can use the Microsoft Windows Remote Desktop Connection application to make a remote connection to a Grass Valley system that runs the Windows operating system.

Take the following into consideration when connecting to K2 systems:

- Before you can use the Remote Desktop Connection, you need network access and permissions to connect to the K2 system.
- You can use either the name or the IP address to access the K2 system.
- Do not use the Remote Desktop Connection to access the PC running the Control Point software or to access the AppCenter application; results may be unreliable.
- Take care when accessing an online K2 system on which media access is underway. The additional load on network and system resources could cause unpredictable results.
- Lack of robust video/graphic support can cause video display problems. Remote desktop connections can interrupt proxy and live streaming. AppCenter video monitoring is not supported through Remote Desktop Connection.

Accessing Remote Desktop Connection

1. Do one of the following:
   - Click the **Start** button on the Windows task bar
   - Press the Windows key on the keyboard.
2. Select **Programs | Accessories | Communications | Remote Desktop Connection**.

   The Remote Desktop dialog box opens.
3. Enter the name or IP address of the system to which you are making the remote connection and click **Connect**.

About SiteConfig

SiteConfig is Grass Valley's tool for network configuration and software deployment. SiteConfig is a ProductFrame application. ProductFrame is an integrated platform of tools and product distribution processes for system installation and configuration.

You can use SiteConfig as a stand-alone tool for planning and system design, even before you have any devices installed or cabled. You can define networks, IP addresses, hostnames, interfaces, and other network parameters. You can add devices, group devices, and modify device roles in the system.

As you install and commission systems, SiteConfig runs on a designated PC. It discovers devices, configures their network settings, and manages host files. SiteConfig also manages software installations and upgrades and provides a unified software package with compatible versions for deployment across multi-product systems.

You should use SiteConfig for network configuration and software deployment at installation and throughout the life of the system in your facility. This enforces consistent policy and allows SiteConfig

to keep a record of changes, which makes the system easier to maintain and aids in troubleshooting should a problem arise.

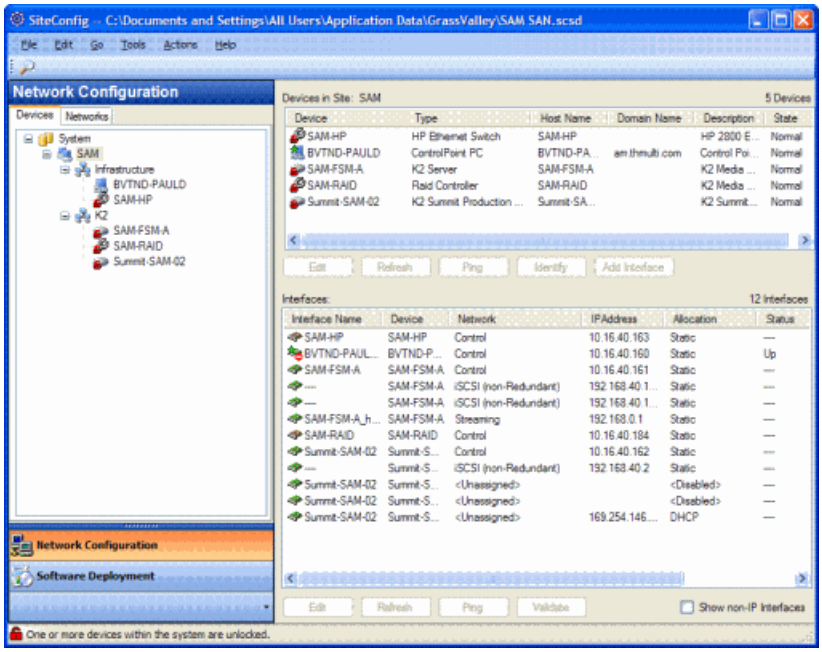
SiteConfig displays information from a system description file, which is an XML file.

Opening SiteConfig

1. Do one of the following: Use the SiteConfig shortcut on the Windows desktop or in the Start menu to open SiteConfig.
   - On the Windows desktop, click the **Grass Valley SiteConfig** shortcut.
   - On the Windows **Start** menu, in the **Grass Valley** folder, click the **SiteConfig** shortcut.
2. SiteConfig opens as follows:
   - If you have previously opened SiteConfig, the SiteConfig main window opens with the most recently used system description loaded.
   - If you have not previously used SiteConfig or if SiteConfig does not have access to a system description file, you are prompted to create a new system description or to import an existing system description.
3. Respond as appropriate.

SiteConfig main window

The SiteConfig main window is as follows:



The left side of the screen shows the tree view of the currently loaded system description. The Network Configuration and Software Deployment buttons at the bottom of the tree view activate either the network configuration workspace or the software deployment workspace.

The network configuration workspace on the left has two tabs: a Devices tab to display the tree of devices in the system and a Networks tab to show the hierarchy of networks defined in the system.

The software deployment workspace also has two tabs: a Devices tab that displays the same tree view of devices but provides information about the software roles assigned to the devices and the software currently installed on devices. The Deployment Groups tab provides the interface to manage software deployment tasks.

Select an item in the tree and the view on the right side of the screen shows details about the item selected. Select a site or group to show information about all the items that fall under the selected item.

Right-click an item to access a context menu of operations.

Icon overlays on items and tooltips provide status and warning feedback.

Chapter 3

System connections and configuration

This section contains the following topics:

About networks

The following section describe networks as they apply to K2 systems. Also refer to the *K2 SAN Installation and Configuration Guide* for more detailed information about K2 SAN networking.

Control network description

The control network is for communication between devices and components. It does not have real-time media traffic or streaming/FTP media traffic. The control network must be on a different subnet than the streaming/FTP network and the media (iSCSI) network. The control network and the streaming/FTP network may be on the same VLAN. The control network and the media (iSCSI) network must not be on the same VLAN. Static IP addresses with name resolution via host files are recommended for the control network.

Streaming/FTP network description

The streaming/FTP network is for media transfers and FTP traffic. It must be on a different subnet than the control network and the media (iSCSI) network. The control network and the streaming/FTP network may be on the same VLAN. The control network and the media (iSCSI) network must not be on the same VLAN. Static IP addresses with name resolution via host files are recommended for the streaming/FTP network. Hostnames of network adapters that are dedicated to the streaming/FTP network must be aliased in the hosts file with the `_he0` suffix. This directs the streaming traffic to the correct port.

Media (iSCSI) network description

The media network is exclusively for real-time iSCSI traffic on a K2 SAN. It must be on a different subnet than the control network and the streaming/FTP network. Furthermore, its traffic is kept physically separate from that of other networks. This separation is provided by dedicated ports, cables, and by a dedicated VLAN on the Ethernet switch or by separate switches. Static IP addresses are required for the media network. Name resolution is not necessary, so media network IP addresses are not required in host files.

Network considerations and constraints

- Do not use any 10.1.0.n or 10.2.0.n IP addresses. These are used by the K2 RAID maintenance port and must be reserved for that purpose. If these addresses are otherwise used, maintenance port communication errors occur.

Network connections

Use the information in this section as appropriate to connect the Gigabit (1GBaseT) Ethernet network for your application:

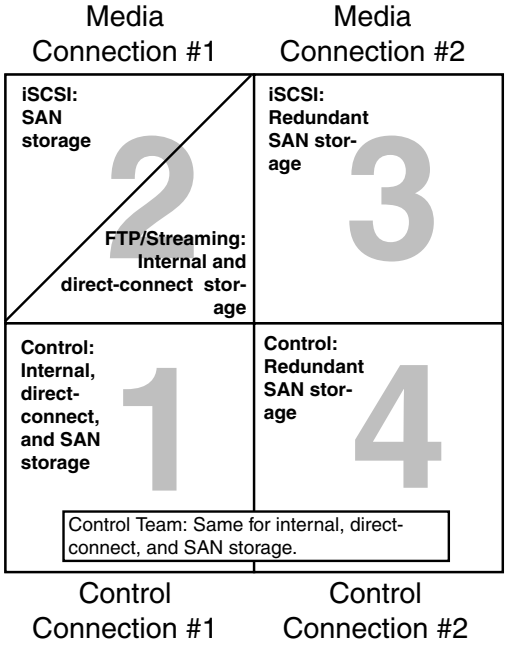
Ethernet cable requirements

For making Ethernet connections, cabling must meet the following requirements:

- Use CAT5e or CAT6 cables. The maximum cable length is 50 meters for CAT5e and 100 meters for CAT6.

About network ports

When you receive a K2 Summit Production Client or K2 Solo Media Server from the factory, it has a specific network configuration, including a loopback adapter and two of the four Gigabit Ethernet ports configured as a teamed pair. The Gigabit Ethernet ports, as viewed when looking at the rear panel, are represented in the following illustration.

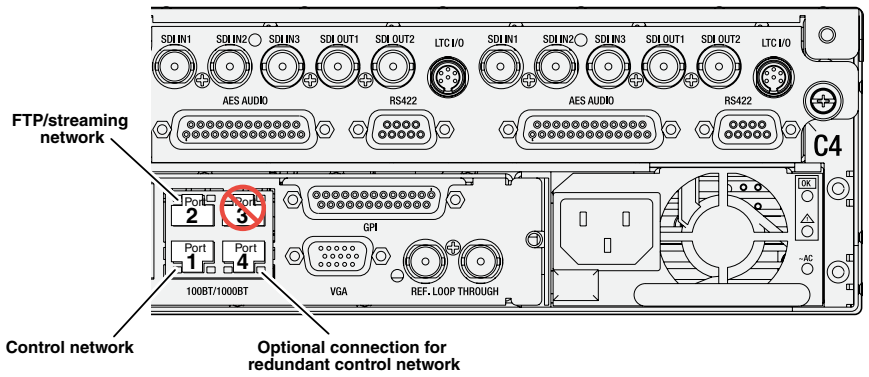


The K2 Solo Media Server is not supported for SAN (shared storage) connection.

Making network connections

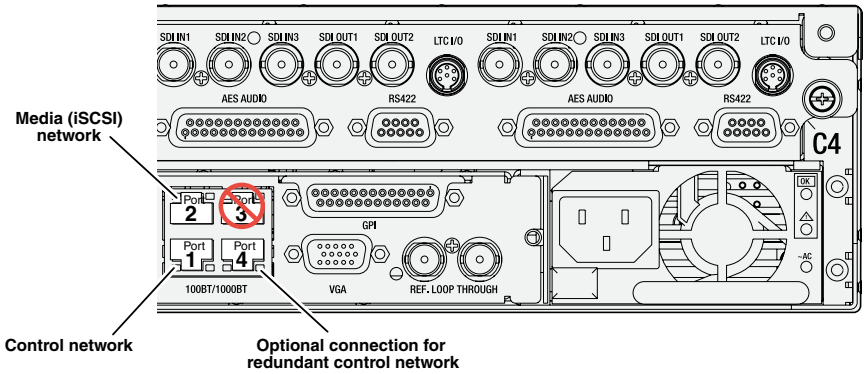
Connect network ports as appropriate for the K2 Summit/Solo system storage option as in the following illustrations. In these illustrations the first generation K2 Summit system is shown. Connections are identical on the K2 Summit 3G system.

Stand-alone storage K2 Summit/Solo network connections



On a K2 Solo Media Server, an internal storage K2 Summit system, or a direct-connect storage K2 Summit system, connect the control network to port 1, which is the first port of the control team. If you have a FTP/streaming network, connect that network to port 2. Port 3 is not used. In most cases port 4, which is the second port of the control team, is not used, although it is available to provide additional redundancy for the control network connection.

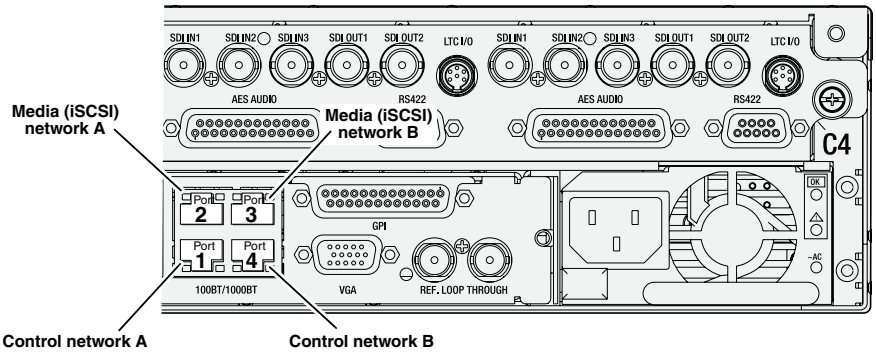
Basic shared storage (SAN) K2 Summit system network connections



On a non-redundant shared storage (SAN) K2 Summit system, connect the control network to port 1, which is the first port of the control team. Port 2 must be connected to the media (iSCSI) network. Port 3 is not used. Port 4, which is the second port of the control team, is not used except as follows: Port 4 may be used only if you extend your control network to provide the same redundancy as that of a redundant K2 SAN.

Refer to the *K2 SAN Installation and Service Manual* for more information.

Redundant shared storage (SAN) K2 Summit system network connections



On a redundant shared storage (SAN) K2 Summit system, you must connect both ports of the control team. Connect control network connection A to port 1 and control network connection B to port 4. You must also connect both media ports. Connect port 2 to the A media network and port 3 to the B media network. The media ports must not be teamed, as doing so interferes with failover functionality.

Refer to the *K2 SAN Installation and Service Manual* for more information.

Network configuration

This section contains instructions for configuring network connections.

About network functionality

K2 networks support the following:

- Remote control and configuration of the internal storage K2 system using AppCenter from a Control Point PC.
- Remote control of the internal storage K2 system using devices and applications software developed for the K2 system that use industry standard remote control protocols over Ethernet.
- Stream media transfers between K2 systems and other supported Grass Valley systems. Streaming transfers allow loading and playing a clip before the transfer is complete.
- Standard data network capability.
- General networking tasks such as file sharing and mapping network drives.

The procedures in this section guide you to relevant settings, but do not instruct you on the specific settings required for your network. It is assumed that you understand Ethernet networks in general and your particular network needs and that you can apply that understanding to make the required settings using standard Windows procedures. If you need help with these procedures, contact your network administrator.

Refer to the *K2 SAN Installation and Service Manual* for network configuration procedures for shared storage K2 clients.

About modifying or restoring network settings

Before configuring network settings, consider the following:

- Loopback adapter — When you receive a K2 Summit Production Client, a K2 Solo Media Server, or a K2 Media Client from the factory, it has a loopback adapter installed. The loopback adapter allows the media file system to continue operating if an Ethernet cable is disconnected. Do not modify the loopback adapter. If you need to restore the loopback adapter, refer to the Service Manual for your K2 product.

  The loopback IP address is 192.168.200.200. Keep that IP address reserved on your network. Do not assign it to any other device. If this causes conflicts with your existing network, consult your Grass Valley representative.
- Hostname changes — If you change the host name, remote AppCenter and other systems could have difficulty connecting. On a shared storage K2 client, Grass Valley strongly recommends that you do not change the host name or IP address unless following the documented procedure. For more information, refer to the *K2 SAN Installation and Service Manual*.
- Restoring factory default network settings — Several settings are configured at the factory and should never be modified. If you suspect settings have been changed, you should reimage the K2 system to restore settings. Refer to the Service Manual for your K2 product for recovery image and network configuration procedures.

Related Topics

Embedded Security modes and policies on page 183

Configure network settings for a stand-alone K2 systems

Stand-alone K2 systems with internal or direct-connect storage ship from the factory DHCP configured. If your control network has DHCP/DNS and you are satisfied to use the factory default host name (which is the serial number), then no local configuration of the control connection is required.

If the Windows network settings need to be configured, you must have Windows administrator security privileges on the K2 system.

1. Access the Windows desktop on the K2 system. You can do this locally with a connected keyboard, mouse, and monitor or remotely via the Windows Remote Desktop Connection.
2. Open the Network Connections Control Panel.
3. Continue with standard Windows procedures to configure the TCP/IP protocol properties. You can set up the network using DHCP, DNS, WINS, or other standard networking mechanisms.

   ***NOTE: On small networks or networks with certain security policies a DHCP server or domain name server (DNS) might not be available. In this case you can set up a static IP address and create a host file on each* K2 system.**

4. Configure the control connection on the K2 system as follows:
   a) Configure the network connection with the following name:

      Control Team

      The control team is GigE ports 1 (Control Connection #1) and 4 (Control Connection #2) on the rear panel.

      ⚠ ***CAUTION: Under no circumstances should you modify the loopback adapter. The loopback IP address is 192.168.200.200. Keep that IP address reserved on your network. Don't assign it to any other device. If this causes conflicts with your existing network, consult your Grass Valley representative.***

5. Configure the FTP/streaming connection (if needed) on the K2 system.

   This connection must have an IP address that is on a different subnet from the control connection. There are special name resolution requirements for the FTP/streaming network.

   Configure as follows:

   a) Configure the network connection with the following name:

      Media Connection #1

      This is GigE port 2 on the rear panel.

6. If prompted, shutdown and restart Windows.
7. If you are going to FTP/stream video between K2 systems, configure for streaming video between K2 systems; otherwise, the K2 system is ready for standard data networking tasks.

Related Topics

Embedded Security modes and policies on page 183

Streaming video between K2 systems

It is required that FTP/streaming traffic be on a separate subnet from control traffic and, in the case of a K2 SAN with shared storage K2 clients, separate from media (iSCSI) traffic. To reserve bandwidth and keep FTP/streaming traffic routed to dedicated ports, IP addresses for FTP/streaming ports must have double name resolution such that hostnames are appended with the "_he0" suffix. You can use host tables or another mechanism, such as DNS, to provide the name resolution. This directs the streaming traffic to the correct port.

In most K2 systems, network name resolution is provided by host tables, which are found in hosts files. The following procedure describes how to set up hosts tables to provide name resolution for both the control network and the FTP/streaming network. If you are using other mechanisms for name resolution, use the host table examples here to guide you. For shared storage K2 clients, also refer to the *K2 SAN Installation and Service Manual* for a discussion of host tables.

Setting up the K2 system for FTP/streaming transfer has the following network requirements:

- For stand-alone internal storage K2 systems, the K2 machine is the source/destination for FTP/streaming transfers. FTP/streaming traffic uses the FTP GigE port (Media Connection #1) on the K2 client.

- For K2 Summit Production Clients or K2 Media Clients with shared storage on a K2 SAN, a K2 Media Server is the source/destination for FTP/streaming transfers. FTP/streaming traffic uses the FTP GigE port on the K2 Media Server. No transfers go to/from the shared storage K2 client directly.
- Some kind of name resolution process must be followed. You have the following options:
  - Set up hosts files located on each networked device so that you reference host names through the hosts files.
  - Edit the DNS entries. See your network administrator.
- The host name of all peer K2 systems and Profile XP systems must be added to a Remote host registry using the K2 AppCenter Configuration Manager.
- To import to or export from a K2 system, both the source and destination must be in the same domain.

Set up hosts files

Set up a hosts file located in *C:\WINDOWS\system32\drivers\etc\hosts* on each K2 system. If you include the names and addresses of all the systems on the network, then you can copy this information to all the machines instead of entering it in the hosts file on each machine.

To provide the required name resolution for the FTP/streaming network, in the hosts file each system that is a transfer source/destination has its host name listed twice: once for the control network and once for the FTP/streaming network. The host name for the streaming network has the extension "_he0" after the name. The K2 systems use this information to keep the FTP/streaming traffic separate from the control traffic.

For FTP transfers to/from a K2 SAN, transfers go to/from K2 Media Servers that have the role of FTP server. No transfers go directly to/from the shared storage K2 clients that are on the K2 SAN. So in the hosts file, you must add the "he_0" extension to a K2 Media Server hostname and associate that hostname with the K2 Media Server's FTP/streaming network IP address.

1. Open Notepad or some other text editor. When you open the text editor you must right-click and select **Run as administrator**.
2. In the text editor, open the following file:

   C:\WINDOWS\system32\drivers\etc\hosts

3. Enter text in two lines for each K2 system that is a transfer source/destination.
   a) Type the IP address for the control network, then use the TAB key or Space bar to insert a few spaces.
   b) Type the machine name, such as `K2-Client`. This sets up the host file for resolving the machine name on the control network. The machine name must not have any spaces in it.
   c) On the next line, type the IP address for the FTP/streaming network, then use the TAB key or Space bar to insert a few spaces.
   d) Type the machine name followed by the characters "_he0". Be sure to use the zero character, not the letter 'o'. Refer to the following example:

```
00.16.42.10   K2-Client
00.0.0.10     K2-Client_he0
```

4. For systems that are not a transfer source/destination, the second line (for the FTP/streaming network) is not required.
5. If there are UIM systems on the FTP/streaming network, make sure you follow the UIM naming conventions. Refer to the *UIM Instruction Manual*.
6. Once you have added the host names for the all the systems on the networks for which the host file provides name resolution, save the file and exit the text editor.
7. Copy the hosts file onto all the other machines to save you editing it again.
8. Add host names to AppCenter to enable streaming.

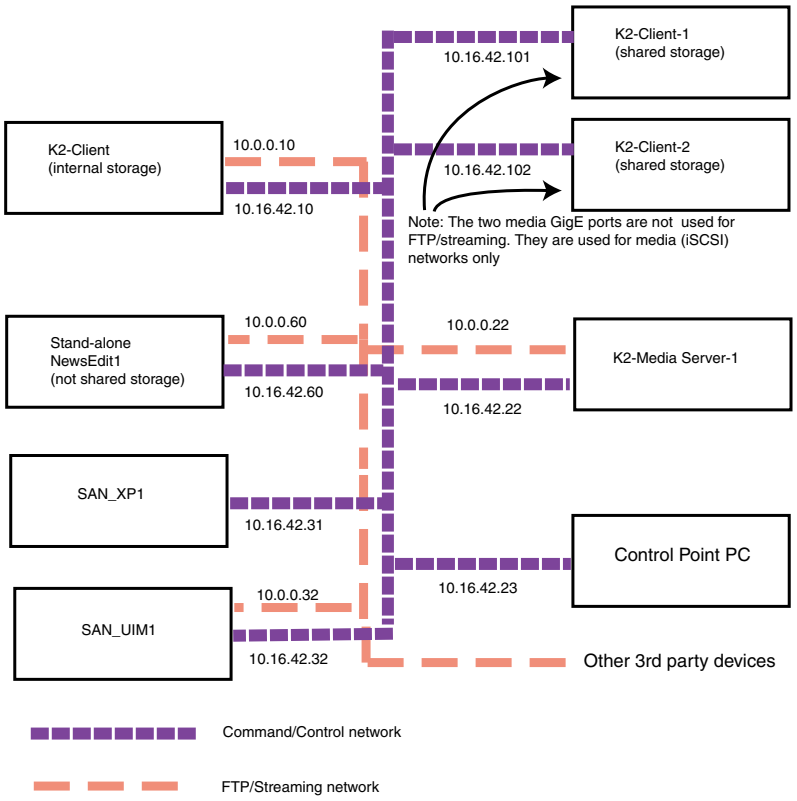
Related Topics

Embedded Security modes and policies on page 183

Add host names to AppCenter to enable streaming on page 70

Sample K2 client configuration and hosts file

The following diagram illustrates one possible configuration setup, including a K2 system with stand-alone storage, K2 clients with shared (SAN) storage, and other Grass Valley systems.



The following example shows the contents of a default Windows hosts file with new lines added that match the IP addresses and host names in the previous sample diagram.

All lines beginning with a # are comments and can be ignored or deleted.

```
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# For example:
# 102.54.94.97     rhino.acme.com # source server
# 38.25.63.10      x.acme.com   # x client host

127.0.0.1          localhost

10.16.42.10        K2-Client
10.0.0.10          K2-Client_he0

10.16.42.101       K2-Client-1
10.16.42.102       K2-Client-2

10.16.42.22        K2-MediaServer-1
10.0.0.22          K2-MediaServer-1_he0

10.16.42.23        ControlPointPC

10.16.42.60        NewsEdit1
10.0.0.60          NewsEdit1_he0

10.16.42.31        SAN_XP1
10.0.0.32          SAN_XP1_he0 SAN_UIM1_he0
10.16.42.32        SAN_UIM1
```

Add host names to AppCenter to enable streaming

In K2 AppCenter, you must add the host names of all peer K2 systems on the network that support streaming transfers. Adding host names is required to allow selection of networked K2 systems in the AppCenter user interface and to provide a successful network connection for streaming. The host names added appear in the “Import” and “Send to” dialog boxes.

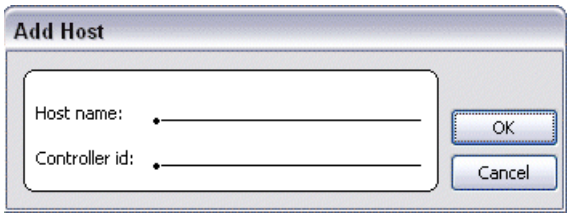
NOTE: By default, the K2 system host name is the same as the Windows operating system computer name.

1. Open AppCenter for the K2 client.
2. In the AppCenter toolbar, select **System**, then choose **Configuration**.
3. Select the **Remote** tab.

   The Remote Settings dialog box displays, showing any network host names that have been added.

4. Select **Add**, to open the Add Host dialog box, then do the following:
   a) Select the Host name field, then enter the computer name of a peer K2 system.

      Make sure to enter the exact computer name. Any differences will result in being unable to connect to the K2 system.



   b) If you are using VDCP remote protocol to perform video network transfers, use the following steps to add a unique Controller ID for each host. Otherwise, you can ignore this step and proceed to the next step.

      - Select controller id field.
      - Enter the controller ID of the K2 system, then select **OK**. Use a number between 1 and 255 that is not assigned to any other K2 system.

   c) Select **OK** in the Add Host dialog box.
5. Repeat the previous step for the remaining K2 systems.
6. In the Configuration dialog box, select **OK** to save settings.

Once the host names are added, the K2 system is ready for streaming operation. For information on transfer compatibility and supported formats, refer to K2 system specifications. For procedures on transferring media, refer to the *K2 AppCenter User Manual*.

NOTE: If you have trouble, try using the ping utility in the Windows command prompt using either the IP address or host name. Troubleshoot as needed. Also, refer to the Service Manual for your K2 system for troubleshooting procedures.

Related Topics

Specifications on page 215

Configuring Server 2008 for domain

This topic applies to Grass Valley servers with a base disk image created prior to mid-2011. Server disk images created after that time do not require this special configuration.

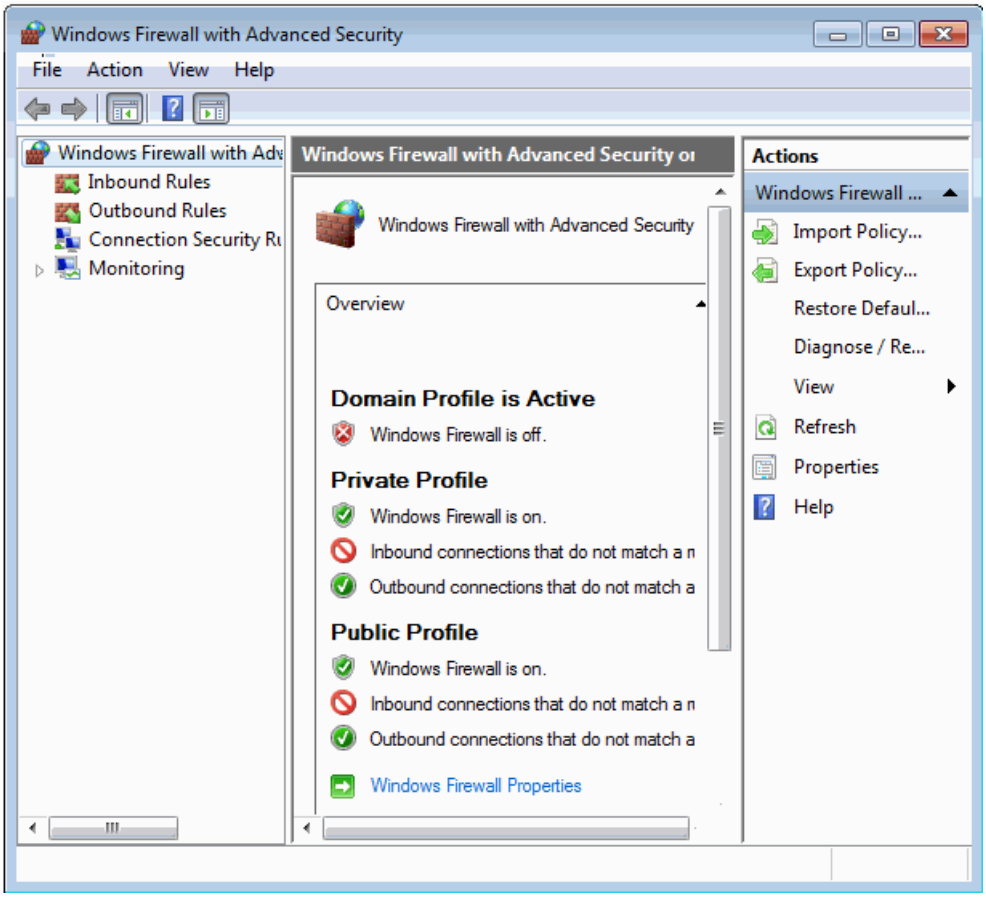
Systems with the Microsoft Windows Server 2008 R2 operating system require special configuration. A server must have its firewall disabled for proper K2 system operation. This includes the Windows firewall that has different profiles for workgroup, domain, etc. You must do the following steps to disable the firewall.

1. Log in to the server with Windows administrator privileges.

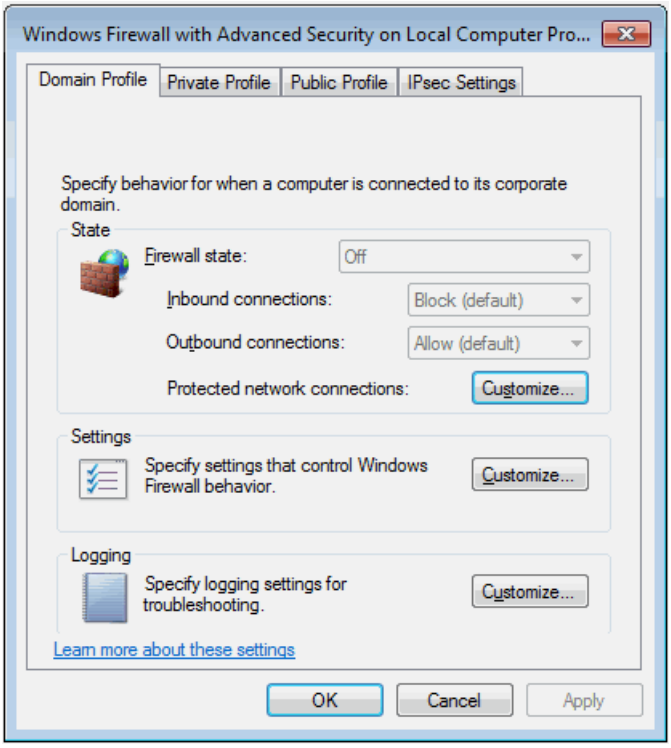
2. From the Windows desktop click **Start** and in the **Search programs and files** box type the following and then press **Enter**.

   `wf.msc`

   The Windows Firewall with Advanced Security window opens.



3. At the bottom of the Overview section, click **Windows Firewall Properties**.
   The Properties dialog box opens.



4. On the **Domain Profile** tab, set **Firewall state** to **Off**.
5. On the **Private Profile** tab, set **Firewall state** to **Off**.
6. On the **Public Profile** tab, set **Firewall state** to **Off**.
7. Click **OK** to save settings and close.

Using FTP for file transfer

This section contains topics about the K2 FTP interface.

About the K2 FTP interface

The K2 FTP interface has the following modes:

- Movie mode — FTP operations are performed on assets in the K2 media database. This is the mode on a K2 systems with a media database, such as online/production K2 SANs and stand-alone K2 Summit systems.
- File mode — FTP operations are performed on files. This is the mode on systems without a media database, such as Nearline K2 SANs.

The K2 FTP interface can run in the movie mode and the file mode simultaneously.

On online/production K2 SANs and stand-alone K2 Summit systems, FTP clients can log into the K2 FTP server using credentials for Windows user accounts that are registered on the K2 system. When such accounts are used, the K2 FTP server exposes "virtual" folders at the FTP root. A virtual folder exists for each video file format that is supported by the FTP server. Navigation to one of these virtual folders allows an FTP client to get or put clips in that file format.

In addition, the K2 FTP server supports reserved user login names that directly places the FTP client in a particular mode of operation. The login names and their modes are as follows:

movie	FTP gets/puts supported for K2 clips in the GXF file format; the clips root becomes the FTP root.
mxfmovie	FTP gets/puts supported for K2 clips in the MXF file format; the clips root becomes the FTP root
mpgmovie	FTP puts supported for MPEG program and transport streams; the clips root becomes the FTP root
video_fs	Pinnacle FTP emulation mode
k2vfs	All FTP operations supported on generic files on the K2 system's media file system; media file system root becomes the FTP root

You can use Internet Explorer to access the FTP interface to see an example.

The K2 FTP server runs on K2 Media Server that has the role of FTP server. While it also runs on the K2 Solo Media Server, stand-alone storage K2 Summit Production Clients and K2 Media Clients, it is important to understand that it does not run on shared storage K2 clients. When you FTP files to/from a K2 SAN, you use the FTP server on the K2 Media Server, not on the K2 client that accesses the shared storage on the K2 SAN.

If clips are created by record or streaming on a K2 file system such that media files have holes/gaps, i.e. unallocated disk blocks, in them, then that clip represents a corrupt movie that needs to be re-acquired. The K2 system handles corrupt movies of this type on a best-effort basis. There is no guarantee that all available media, especially media around the edges of the holes/gaps, is streamed.

You can also apply K2 security features to FTP access.

When using FTP in a shared storage environment, ensure that all FTP communication takes place on the FTP/streaming network, and not on the Control network.

Related Topics

FTP access by Internet Explorer on page 78
FTP and media access security on page 179
FTP and media access security on page 76
Importing via Pinnacle emulation K2 FTP on page 119

Limitations with complex media types

Depending on the system software versions of source and destination devices, it is possible that lists or programs made from lists that contain movies with mixed video compression types or mixed

audio types cannot stream to other devices, nor can they be exported to a file. Refer to release notes for the specific software versions for details.

MXF OP1A supports transfer of simple media types only, which are a subset of the K2 encode/decode/metadata capabilities. For example, MXF OP1A does not support the transfer of complex clips, such as a subclip that spans two media files. Do not attempt MXF OP1A transfers of complex clips.

Transferring between different types of systems

While GXF transfer of media with mixed format (such as an agile playlist) is supported between K2 systems, it might not be supported between a K2 system and a non-K2 system, depending on system software versions. Refer to the release notes for the software version.

You can also use remote control protocols to initiate transfers.

Related Topics

Remote control protocols on page 209
Specifications on page 215

Transfer mechanisms

You can move material between systems using the following mechanisms, each of which offers a different set of features:

- Manual mechanisms — These are the AppCenter transfer features. Refer to the K2 AppCenter User Manual for AppCenter instructions. When transferring between K2 systems you can browse and select files for transfer. When transferring between K2 systems and other types of systems, one or more of the following might be required, depending on software versions. Refer to release notes for the version information:
  - Specify the IP address, path, and file name to initiate a transfer.
  - Add the remote host in Configuration Manager before the transfer.
  - Enter machine names in compliance with UIM naming conventions.
- Automatic mechanisms, including the following:
  - K2 FTP interface — This interface supports transfers via third party FTP applications, such as automation systems. To demonstrate this, you can use Internet Explorer to transfer files between a PC and the FTP interface on a stand-alone K2 Summit Production Client or a K2 Media Server on the same network.
  - Remote control protocols — Industry standard remote control automation applications can initiate transfers. The protocol command must be sent to the K2 client. This applies to both stand-alone and shared storage K2 systems.

Related Topics

Remote control protocols on page 209
FTP access by automation on page 76

FTP access and configuration

For basic LAN access, the following Grass Valley products can connect as an FTP client to the K2 FTP server with no special configuration required:

- K2 Summit Production Client
- K2 Media Client
- K2 Solo Media Server
- UIM-connected Profile XP Media Platform

For WAN access, contact your Grass Valley representative for assistance.

If the FTP client is not one of these Grass Valley products, contact the product's supplier or your network system administrator for assistance with configuring TCP window scaling. Any computer that connects as an FTP client to the K2 FTP server must have TCP window scaling enabled. Refer to http://support.microsoft.com/kb/q224829/ for more information on this feature. Never set Tcp1323Opts without setting TcpWindowSize. Also, Windows NT 4.0 does not support TCP window scaling, but will still communicate with Grass Valley products in a LAN environment.

FTP access by automation

Using FTP, third parties can initiate transfers between two K2 systems or between a K2 system and another FTP server. Transfers of this type are known as "passive" FTP transfers, or "server to server" transfers.

If you are managing transfers with this scheme from a Windows operating system computer, you should disable the Windows firewall on that computer. Otherwise, FTP transfers can fail because the Windows firewall detects FTP commands and can switch the IP addresses in the commands.

NOTE: You should disable the Windows firewall on non-K2 systems issuing passive FTP transfer commands.

FTP and media access security

The following systems host the K2 FTP interface:

- A stand-alone K2 system.
- A K2 Media Server that takes the role of FTP server

The way in which the K2 FTP interface applies media access security is explained in this section.

The K2 FTP interface uses the credential information for the current FTP session logon and checks it against the access control list for a K2 bin. This is the access control list that you set up through the Organize Bins dialog box in AppCenter. Any media access related operations such as get, put, dir, rename and delete are checked against the FTP session's logon credentials to access the media. For example, if an FTP session is denied access to List Bin Contents for bin A, then the session can not initiate a dir operation on bin A to list the contents of the bin. Furthermore, the session can not transfer clips into bin A using the put operation.

For the purpose of compatibility FTP access conventions, accounts for user movie or user mxfmovie are provided on the K2 system. There is also a video_fs account for Mac/FCP access. These accounts

are automatically set up when you install K2 software version 3.2 or higher. Do not restrict access for these accounts. If your security policy requires restricting access to these accounts, contact Grass Valley Support.

On a K2 SAN, authentication takes place on the K2 Media Server. Setting up FTP security for specific local users and groups is not supported on a K2 SAN, with the exception of the local movie and mxfmovie accounts. However, you can set up FTP security for domain users and groups.

About FTP internationalization

The K2 FTP interface supports clip and bin names in non-English locales (international languages) as follows:

- Non-ASCII localized characters represented as UTF-8 characters.
- All FTP client/server commands are in ASCII.
- The named movie asset is Unicode 16-bit characters
- The K2 FTP client converts between Unicode and UTF-8 strings explicitly.

Also refer to “Internationalization” on page 210.

The Microsoft FTP client does not convert from a Unicode string to a UTF-8 string. Instead, it passes the Unicode string to the FTP server directly, which can cause errors. To avoid these errors, in the FTP command, every reference to the clip path must be in UTF-8.

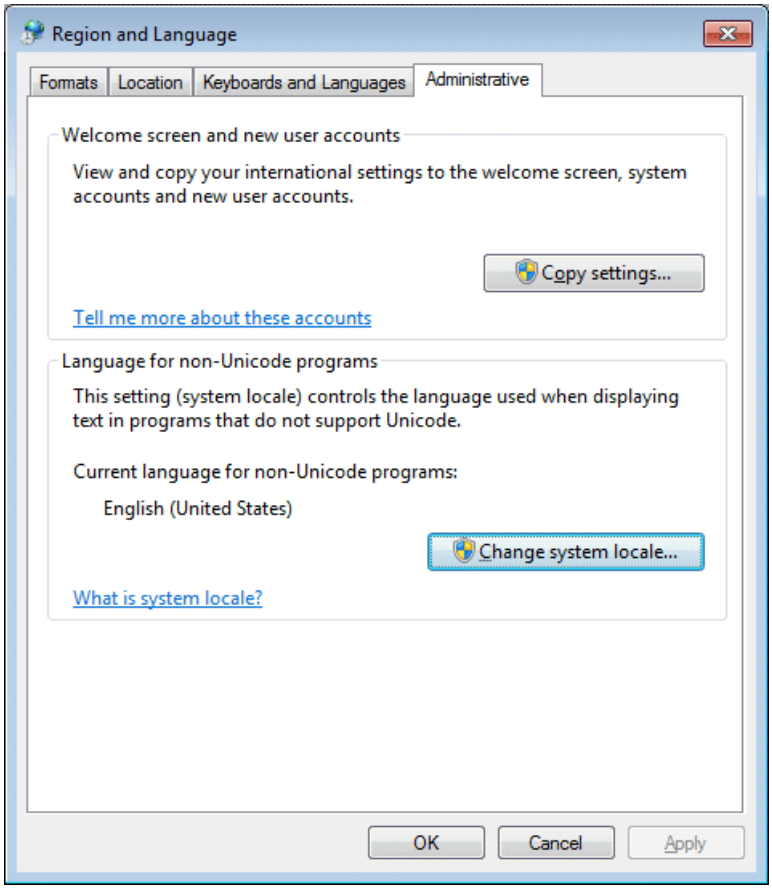
A specific language setting is required on the computer that hosts the K2 FTP interface. This requirement applies to a K2 Media Server, K2 Solo Media Server, and a stand-alone K2 client, as they all host the K2 FTP interface.

Related Topics

Internationalization on page 240

Setting the FTP language

1. Open the **Regional and Language** control panel.



2. On the **Administrative** tab make sure "Current language for non-Unicode programs" is set to **English (United States)**.
3. If you made a change click **Apply** and **OK**, and when prompted restart the computer to put the change into effect.

Related Topics

Embedded Security modes and policies on page 183

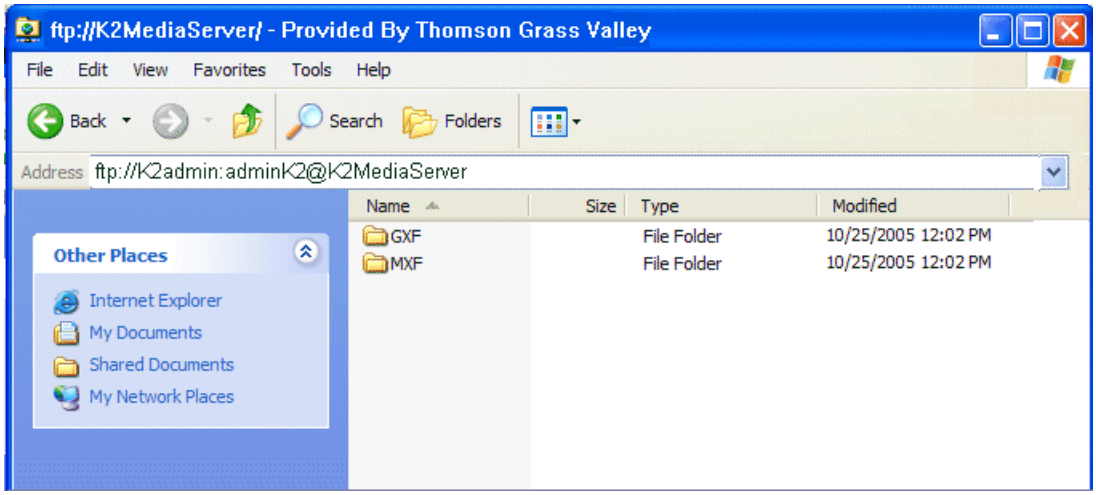
FTP access by Internet Explorer

You can use Internet Explorer to transfer files via FTP between a PC and the FTP interface on a stand-alone K2 system or a K2 Media Server, so long as both source and destination machines are on the same network.

While the K2 FTP interface supports local languages, some international characters are not displayed correctly in Internet Explorer. Use only English language characters with Internet Explorer.

To access FTP using Internet Explorer, use the following syntax in the Address field: `ftp://<username:password@hostname>`. The username/password can be any account set up on the machine hosting the FTP interface. The hostname can be the name of a stand-alone K2 client or it can be the name of a K2 Media Server. (You cannot make a FTP connection to a K2 client with shared storage or to a K2 Control Point PC.)

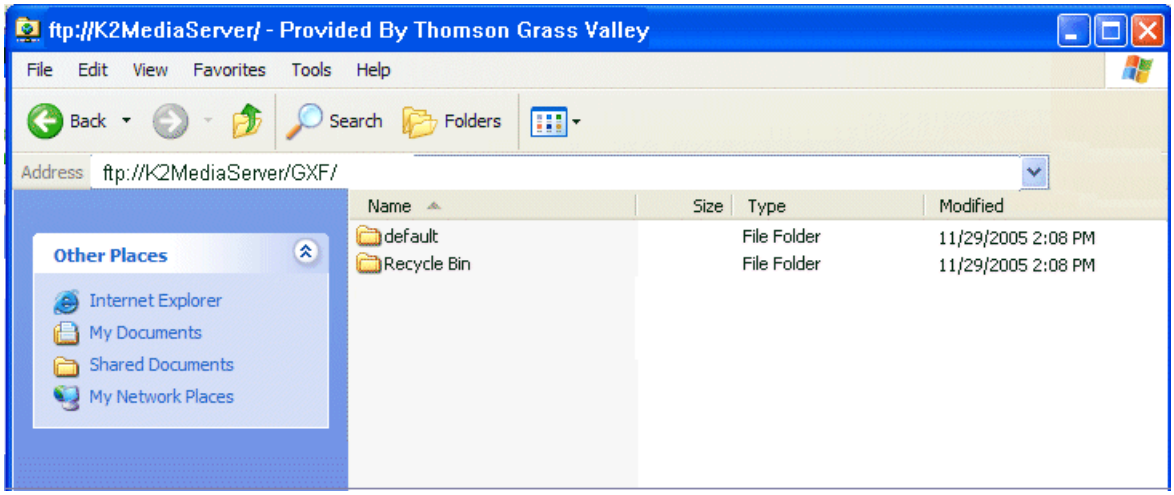
Once you have logged in, the two virtual directories are displayed.



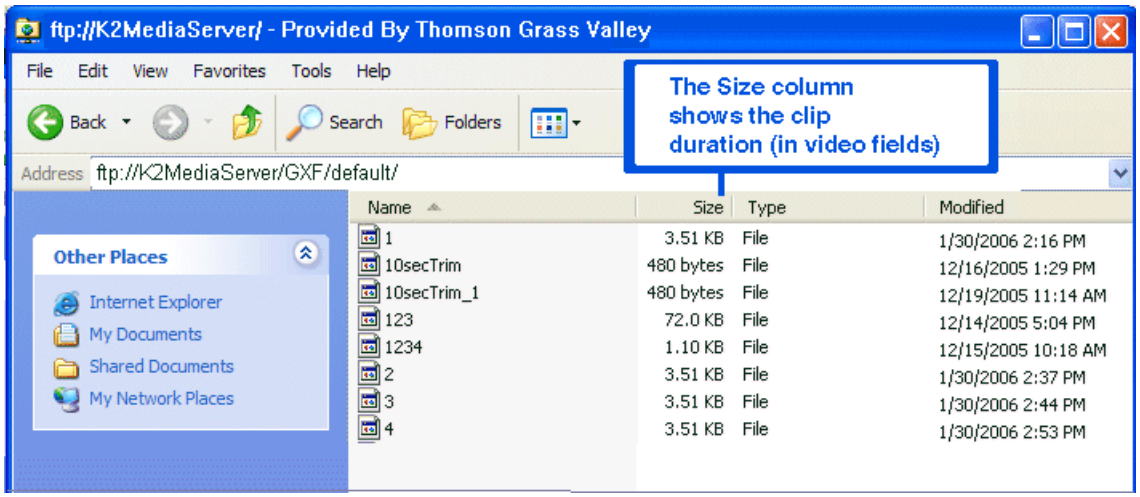
GXF — General Exchange Format (SMPTE 360M). This is the standard Grass Valley file interchange format. Refer to specifications later in this manual for media types supported.

MXF — Media Exchange Format (SMPTE 377M). Refer to specifications later in this manual for media types supported.

Inside the GXF and MXF folders you can see contents of the system.



The subfolders are organized in typical Windows fashion, with columns denoting the file's name, size, etc. The Size column refers to the clip duration (in video fields).



You can use Internet Explorer to drag a file from your stand-alone K2 system or K2 Media Server and drop it in a folder on your PC. You can also drag a file from your PC and drop it in the appropriate folder on your stand-alone K2 system or K2 Media Server.

Be careful not to mix files from the two types of file interchange formats. GXF files can only be transferred to the GXF folder, and MXF files can only be transferred to the MXF folder. If you try to drop a clip into the incorrect folder, the transfer fails. For example, `clip1.gxf` can be dropped into the `K2-MediaSVR/GXF/default/` folder, but not into the `K2-MediaSVR/MXF/default/ folder`.

Related Topics

FTP and media access security on page 76

FTP commands supported

The following table lists the FTP commands that the K2 FTP interface supports.

FTP command name	FTP command description	K2 FTP support
USER	User Name	Supported
PASS	Password	Supported
ACCT	Account	Not supported
CWD	Change working directory	Supported
CDUP	Change to parent directory	Supported
SMNT	Structure mount	Not supported
REIN	Reinitialize	Not supported
QUIT	Logout	Supported
PORT	Data port	Supported

FTP command name	FTP command description	K2 FTP support
PASV	Passive	Supported
TYPE	Representation type	Supported
STRU	File structure	Not supported
MODE	Transfer mode	Not supported
RETR	Retrieve	Supported
STOR	Store	Supported
STOU	Store unique	Not supported
APPE	Append (with create)	Not supported
ALLO	Allocate	Not supported
REST	Restart	Not supported
RNFR	Rename From	Supported
RNTO	Rename To	Supported
ABOR	Abort	Supported
DELE	Delete	Supported
RMD	Remove directory	Supported
MKD	Make directory	Supported
PWD	Print working directory	Supported
LIST	List	Supported. Reports size in number of video fields.
NLST	Name List	Supported
SITE	Site Parameters	Supported
SYST	System	Supported
SIZE	Size of file (clip)	Supported. Reports size in Bytes.
STAT	Status	Supported
HELP	Help	Supported
NOOP	No Operation	Supported

Using FTP on a K2 Nearline SAN

A K2 Nearline SAN is considered an “offline” system, as it has no media database and is not capable of direct playout of media. On this type of system the K2 FTP interface operates in file mode. Therefore, procedures that apply to “online” K2 SANs do not globally apply to the Nearline SAN. This includes procedures for streaming, import, export, and FTP.

The rules for transferring to/from a K2 Nearline SAN are as follows:

- Transfer files only. Streaming media, as in AppCenter's Import/Send to | Stream feature, is not supported.
- K2 media must be transferred to/from the Nearline system as a GXF or MXF file.
- Passive FTP mode is supported. You must use this mode for FTP transfers.
- In addition to FTP transfers, you can also map shared drives and use basic Windows networking to move files to/from a Nearline storage system.
- You should use the dedicated K2 FTP/streaming network.

Additional information about Nearline FTP is as follows:

- K2 FTP protocol supports clip and bin names in non-English locales (international languages) using UTF-8 character encoding. Refer to specifications for internationalization.
- The Nearline FTP interface operates in file mode so it does not have GXF and MXF folders to support format-specific functionality, as does the K2 FTP interface in movie mode for "online" K2 systems. This means the Nearline FTP interface treats all files, including GXF and MXF, as generic files with no particular consideration for any file format.

Using reference files

When you create a simple K2 clip on a K2 system, K2 software can create a corresponding reference file. The reference file is stored in a directory in the clip's folder on the V: drive. You can configure the software to create QuickTime reference files, MXF reference files, or no reference files. The following topics provide information about reference files on K2 systems.

About QuickTime reference files

The following formats are supported as QuickTime reference files:

- DV
- AVC-Intra
- XDCAM-EX
- XDCAM-HD
- XDCAM-HD 422
- IMX

The K2 clip must be a simple clip in order to create the reference file. With the QuickTime reference file you can open the K2 clip with QuickTime tools, such as Final Cut Pro, for playback and editing. For some formats the QuickTime tool does not provide default support, so you must configure the tool as necessary to support the format. The QuickTime tool must be run on another system. Running the QuickTime player or other QuickTime tools on the K2 system is not supported. You have options for connections, access, and software to support your workflow requirements.

About MXF reference files

For MXF reference files, the K2 clip can be any supported format simple clip. K2 software creates the MXF reference file when you create a new simple clip by recording, importing, or copying. K2

software does not create the MXF reference file when you create a playlist, a program with continuous-recorded material, or a clip with tracks having a duration less than the clip duration. The reference file is a MXF OP1b file with external essence. The reference file gives you options for connections, access, and software to support your workflow requirements.

Configuring reference file type on a standalone K2 Summit/Solo system

1. In AppCenter, click **File | System | Configuration**.
   Configuration Manager opens.
2. In Configuration Manager, click the **System** tab.
3. In Reference Files settings, for the **Reference file type** setting, select one of the following:
   - None — K2 software does not create reference files.
   - QuickTime — K2 software creates QuickTime reference files.
   - MXF — K2 software creates MXF reference files.
4. Click **OK** to apply the setting.
5. Restart the standalone K2 Summit/Solo system to put the change into effect.

Configuring reference file type on a K2 SAN system

1. In the K2Config application, for the K2 Media Server with role of file system server, access the File System Server Configuration page as follows:
   - On a SAN that is already configured, in the tree view click **File System Server**.
   - On a SAN that is not yet fully configured, work through the Configure K2 Server wizard until you reach the File System Server Configuration page.
2. On the File System Server Configuration page select one of the following:
   - No reference file — K2 software does not create reference files.
   - QuickTime reference file — K2 software creates QuickTime reference files.
   - MXF reference file — K2 software creates MXF reference files.
3. Click **Check** to apply the setting.
4. Manage the required K2 Media Server restart as follows:
   - On a SAN that is already configured, you must restart the K2 Media Server to put the change into effect. Follow the restart procedure appropriate for the basic or redundant K2 SAN.
   - On a SAN that is not yet fully configured, continue to work through the Configure K2 Server wizard. The restart at the end of the configuration process is sufficient.

If a redundant K2 SAN, you must configure similarly and restart both K2 Media Servers with role of file system server.

Quicktime and Final Cut Pro support

You can access K2 media as QuickTime for editing in Final Cut Pro, as explained in the following topics.

About connecting to K2 storage with Final Cut Pro

This topic describes the different ways you can access K2 media for editing with Final Cut Pro.

Connection types are as follows:

- Fibre Channel – This is a connection as a client to a Fibre Channel K2 SAN. The connection requires a K2 FCP Connect license and supporting software on the Macintosh system. The connection uses the K2 SAN's Fibre Channel network.
- iSCSI – This is a connection as a client to an iSCSI K2 SAN. The connection requires a K2 FCP Connect license and supporting software on the Macintosh system. The connection uses the K2 SAN's iSCSI Gigabit Ethernet network.
- CIFS – This is a basic CIFS connection. You can access files on K2 SAN storage or K2 stand-alone storage with this type of connection. The connection uses a basic Ethernet network.

Access methods are as follows:

- Edit-in-place – With this method you edit the K2 media in Final Cut Pro across the network while the media is still in place in K2 storage. You can do this over any connection type.
- File transfer – With this method you transfer (copy) the K2 media to the Macintosh system and then edit it in Final Cut Pro across the network while the media is still in place in K2 storage. You can do this over any connection type. You can initiate the transfer as file copy over Fibre Channel, file copy over iSCSI, file copy over CIFS, or via FTP.

With all access methods, after you are done editing the K2 media you export it back to K2 storage via a K2 HotBin.

Software components that support various workflows are as follows:

- K2 FCP Connect – This is a Grass Valley product that supports all connection types for optimal performance. It is a toolset that must be purchased, installed, licensed, and configured. It includes GV Connect, which is a Final Cut Pro plug-in. GV Connect supports edit-in-place and file transfer over Fibre Channel, iSCSI, or CIFS connections. It also includes GV Browse, which supports searching for QuickTime reference files on a MediaFrame server and transferring them to Final Cut Pro for editing.
- Flip4Mac – This is a Telestream product that supports FTP file transfer of K2 media to the Macintosh system. It is a Final Cut Pro plug-in.

Connections, access, and software apply to K2 storage and versions as follows:

K2 storage/version	Connection type	Access method	Software
K2 SAN and stand-alone K2 Media Client software version 3.3.2.1374 and higher	CIFS	File transfer	Flip4Mac recommended

K2 storage/version	Connection type	Access method	Software
Stand-alone K2 Media Client software version 3.3.2.1374 and higher, and stand-alone K2 Summit Production Client software version 7.2.7.1397 and higher	CIFS	All	K2 FCP Connect recommended
K2 SAN (K2 Media Client) software version 3.3 and higher, and K2 SAN (K2 Summit Production Client) software version 7.2.7.1397 and higher	All	All	K2 FCP Connect recommended for CIFS, required for iSCSI and Fibre Channel SAN.

For detailed instructions refer to documentation as follows:

- Fibre Channel, iSCSI, or CIFS connection with K2 FCP Connect – Refer to the K2 FCP Connect documentation set, which includes the following documents:
  - K2 FCP Connect Installation Manual
  - K2 FCP Connect Release Notes
  - GV Connect User Manual
  - GV Browse User Manual
- Basic CIFS connection without K2 FCP Connect – Refer to topics later in this manual.

Related Topics

About QuickTime reference files on page 82

Install and configure Macintosh Final Cut Pro systems on K2 storage

Read the following topics to get systems connected and media access operational.

Final Cut Pro CIFS mount to K2 storage quick start installation checklist

Use the following sequence of tasks to set up Final Cut Pro access to K2 storage via CIFS mount without a K2 FCP Connect license. This applies to the following K2 systems:

- K2 SAN and stand-alone K2 Media Client software version 3.2 and higher
- K2 SAN and stand-alone K2 Summit Production Client software version 7.1 and higher

This checklist assumes that the K2 system has been installed/commissioned and is fully operational.

On the K2 system

	Task	Instructions	Comment
☐	Configure hosts files on the K2 system	Add Macintosh systems to the K2 hosts file	Enter Macintosh IP address and name in hosts files.

	Task	Instructions	Comment
☐	Create a Macintosh user account. This is the account that the Macintosh system uses to log on to the K2 system.	Use standard Windows operating system procedures.	This is not necessary if the Macintosh system logs on with the default administrator account.
☐	Optional: Enable Access Control Lists, if desired.	Topic "Enable Access Control Lists on the K2 system"	This is optional. If you do this task, you must also configure Active Directory Domain on the Macintosh systems.
☐	Share V: drive as `default/gvfs_hostname`.	Use standard Windows operating system procedures. Set permissions to read only.	On a K2 SAN, create the share on the primary K2 Media Server. Do not create the share on a SAN connected K2 client.

On all Macintosh client computers

	Task	Instructions	Comment
☐	Install Final Cut Pro, if not already installed.	Final Cut Pro documentation	—
☐	Install Flip4Mac, if necessary for your workflow.	Flip4Mac documentation	This software is optional
☐	Cable network connections.	Connect the Macintosh system to the K2 system's control network.	Only the control network connection is necessary.
☐	Configure for control network, if not already done.	Topic "Configure Macintosh systems for control network"	—
☐	Optional: Configure Active Directory Domain	Topic "Configure Macintosh systems for Active Directory Domain"	This is optional. If you do this task, you must also enable Access Control Lists on the K2 system.
☐	Mount the K2 system's volume `default`.	Topic "Connecting via SAMBA/CIFS"	In the Name field, enter <K2_name>/<username>.

Final tasks

	Task	Instructions	Comment
☐	If used, verify Access Control Lists.	Topic "Verify Access Control Lists"	—
☐	If desired, configure HotBin on the K2 system to receive finished Final Cut Pro files.	Topics "Configure HotBin" and "About QuickTime import delay"	—

Enable Access Control Lists on the K2 system

Prerequisites for the K2 system are as follows:

- Current compatible versions of the Windows operating system and SNFS software.
- Standard C:, D:, E: and V: disk volumes.
- SNFS has been configured with Grass Valley's Storage Utility.
- The SNFS configuration file is located in the *D:\SNFS\config* directory.

If desired, you can enable Access Control Lists (ACLs). For SAN access enable ACLs on the K2 Media Server(s). For stand-alone K2 storage access enable ACLs on the stand-alone K2 system. If you do this task, you must also configure Active Directory Domain on the Macintosh systems.

1. If a redundant K2 SAN, take FSM K2 Media Servers out of service and manage redundancy as directed in documented procedures.
2. Navigate to *D:\SNFS\config* and open the SNFS configuration file in a text editor. The file is named either *default.cfg* or *gvfs_hostname.cfg* where hostname is the name of the K2 system—if a redundant SAN, the name of the primary FSM.
3. Confirm/enter/modify text lines as necessary to configure as follows:

```
WindowsSecurity Yes
EnforceACLs Yes
UnixIdFabricationOnWindows Yes
UnixDirectoryCreationModeOnWindows 0700
UnixFileCreationModeOnWindows 0600
UnixNobodyGidOnWindows 60001
UnixNobodyUidOnWindows 60001
```

   Avoid duplicate settings.

   NOTE: Once ACLs are enabled on the K2 system (WindowsSecurity set to Yes), they cannot be disabled.

4. Save the SNFS configuration file.
5. Restart the K2 system.
6. If a redundant K2 SAN, repeat these steps on the redundant FSM K2 Media Server.
7. After restart of K2 Media Server(s) is complete, restart all clients of the K2 SAN.

Configure Macintosh systems for control network

Depending on the version of your Macintosh operating system, the steps in this task can vary. Refer to your Macintosh documentation as necessary.

Configure each Macintosh system as follows:

1. Open System Preferences, Network settings.
2. Set Ethernet 1 to configure manually (static IP).
3. Configure IP address, subnet mask, and other settings as required for the control network.

Configure Macintosh systems for Domain

Depending on the version of your Macintosh operating system, the steps in this task can vary. Refer to your Macintosh documentation as necessary.

If desired, MAC OS X can be configured to use Active Directory (AD) resources such as users and groups. Once a computer is bound to an AD domain, users belonging to that domain may login to the Macintosh system at the main login prompt. If you do this task, you must also enable Access Control Lists on the K2 storage you access, either the K2 Media Server (FSM) for SAN access or the stand-alone K2 system.

1. Open System Preferences and click **Accounts**.
2. If the **Lock** icon is locked, unlock it by clicking it and entering the administrator name and password.
3. Click **Login Options**, then click **Join** or **Edit**. If you see an **Edit** button, your computer has at least one connection to a directory server.

4. Click the **Add (+)** button.
5. From the "Add a new directory of type" pop-up menu, choose **Active Directory**.
6. Fill in the Active Directory information for the domain administrator account.

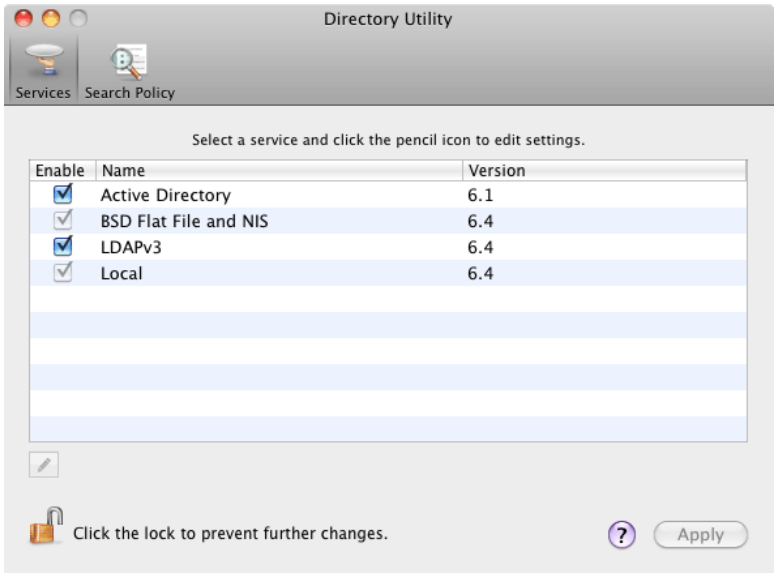
   The administrator account is only needed at the time of binding. Once the computer is bound to a domain, all users of the domain can be used to log in to the Macintosh system.

7. Click **OK**.

   The Macintosh computer goes through the binding process. If successful, the domain name is listed with the status message, "This server is responding normally".

8. Click **Open Directory Utility** or, if desired, click **Done** and open the **Directory Utility** from the `System/Library/Core Services` folder.

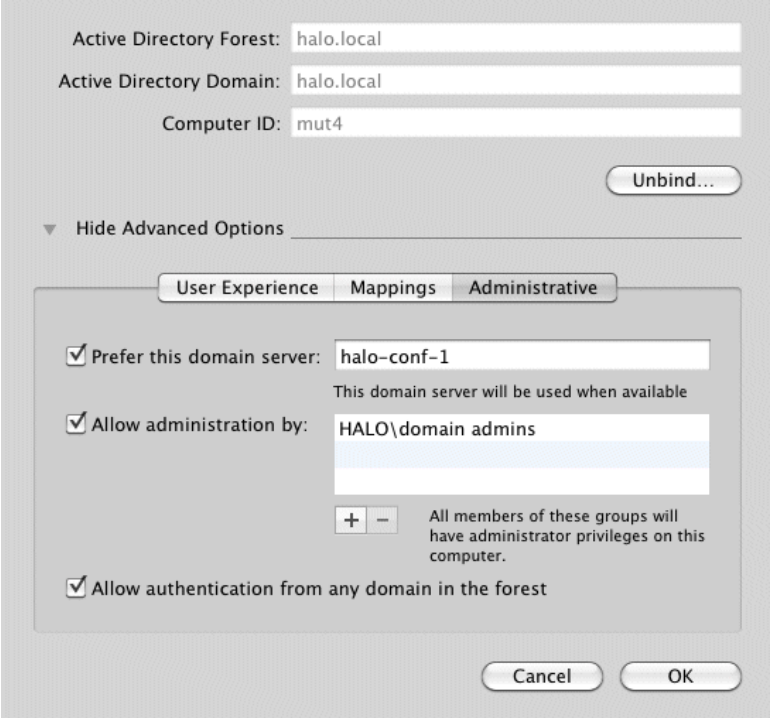
9. Click **Services**.



10. Verify that the Active Directory option is checked.

    If you need to change options, first double-click the Lock icon on the lower left hand corner and authenticate as administrator.

11. If desired, add AD accounts or groups as administrators of the Macintosh computer as follows:
    a) In the **Services** tab, double-click on the **Active Directory** name.
    b) Open the advanced options and click on the **Administrative** tab.



    c) Verify that the **Prefer this domain server** and **Allow administration by** check boxes are checked.
    d) Add any AD user or group of the domain to the list.

    You must type the user or group name, then a backslash, before the domain name.

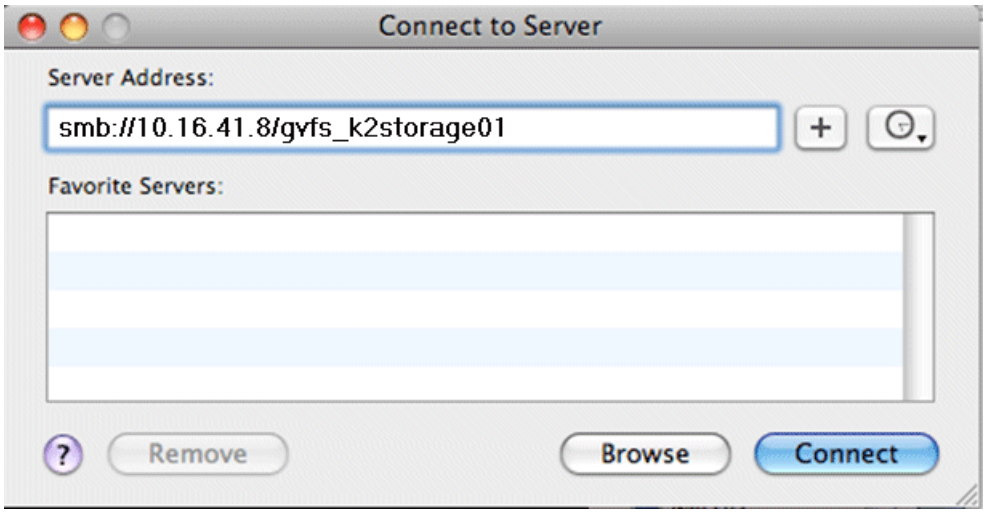
Connecting via SAMBA/CIFS

Depending on the version of your Macintosh operating system, the steps in this task can vary. Refer to your Macintosh documentation as necessary.

Use this method to connect to the SNFS volume via CIFS. Once the Macintosh computer has been bound to a domain it can then connect to any domain controlled, shared volume via SAMBA. If connecting via SAMBA, XSan software does not need to be installed or configured.

1. On the Macintosh computer open the Finder program and at the top menu click **Go | Connect to Server**.

   The Connect to Server dialog box opens.



2. In the Server Address field, type `smb://`, then type the IP or DNS name of the server to which you are connecting, slash, then type the volume name.

3. Click **Connect**.

   You are prompted to authenticate.

   In the **Name** field, make sure you enter the name of the K2 system (shown here as "yourdomain"), then a backslash, then the username.

The volume should be mounted in the /Volumes directory and viewable in the Finder program. Rights to files and folders are enforced based on the security profile of the user you authenticated with when connecting with SAMBA, not the user you are logged in as on the Macintosh computer.

Verify Access Control Lists on a Macintosh system

Verify the following before you begin:

- Two domain users
- A correctly configured K2 system

- At least one Macintosh system attached

If you are using Access Control Lists on Macintosh OS X and the Windows operating system, use this task to verify.

1. Test permissions on the K2 system as follows. For K2 SAN access, test permissions on the primary K2 Media Server FSM. For stand-alone K2 storage access, test permissions on the stand-alone K2 system.
   a) Create a new text file on the V: drive.
   b) Right-click on the text file and select **Properties**.
   c) Click the **Permissions** tab.
   d) Select **Everyone** and then for the **Write** permission select the **Deny** check box.
   e) Create a folder on the V: drive.
   f) Give full permissions to the first user (designated in this procedure as userA) on the domain.
   g) Give read only permissions to the second user (designated in this procedure as userB) on the domain.

2. On the Macintosh system, do the following:
   a) Login as userA.
   b) Right-click on the text file and select **Properties**.
   c) Open up **Terminal** and change directory to the volume.

      If the SNFS file system is named "default" type the following and press **Enter**:

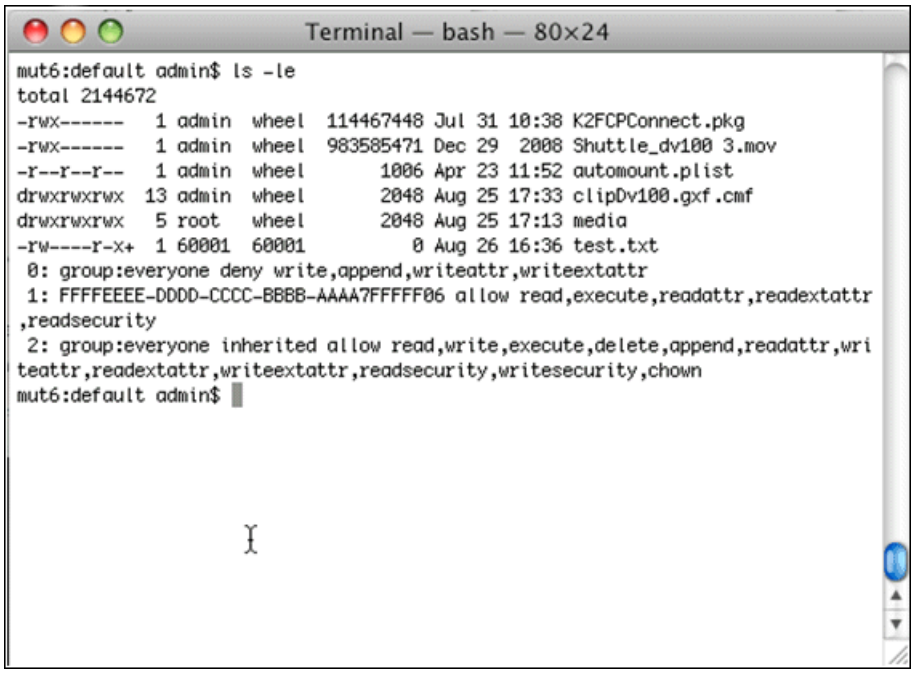
      ```
      cd /Volumes/default
      ```

      If the SNFS file system is named "gvfs_hostname" (where hostname is the name of the K2 system) type the following and press **Enter**:

      ```
      cd /Volumes/gvfs_hostname
      ```

   d) Type the following command:

      ```
      ls -le
      ```



   e) Verify that there is a "+" next the text file, plus a list of permissions below. If this is true then cross-platform ACLs are enabled.
   f) Open the Finder, go to the default volume and try to edit the text file. This should fail as the file should not be writeable.
   g) In the Finder, go to the folder you created earlier in this procedure and create a text file in the folder. This operation should be successful.
   h) Log out and then log back in as userB.
   i) In the Finder, go to the folder you created earlier in this procedure and try to create a text file in the folder. This operation should fail.

Configure HotBin

If a K2 SAN, the SNFS configuration file must have settings as follows:

- If Windows Security is No, GlobalSuperUser must be set to Yes.
- If Windows Security is Yes, no GlobalSuperUser setting is required.

Configure a HotBin on the K2 system to receive the finished media from Final Cut Pro.

1. In K2 AppCenter, create a bin with an appropriate name, such as "dstBin".
2. Configure `dstBin` as a HotBin.

   Refer to the *K2 System Guide* for instructions.
3. When you configure a HotBin, in the Capture Services Utility you can adjust QuickTime Import Delay. The recommended setting is 15 seconds. Refer to the next topic for more information.

About QuickTime import delay

When you copy a file into a K2 HotBin, the HotBin watches for the file to close and the copy operation to stop, which should indicate the file is complete, before it begins to import the file into K2 storage. However, Final Cut Pro repeatedly opens and closes any QuickTime file as it exports the file, so it is possible that the K2 HotBin can detect a file closed event and begin to import the file before Final Cut Pro is done. If this occurs, the K2 HotBin import for that file fails.

To avoid this problem, when you configure a K2 HotBin you can configure the QuickTime import delay setting. This setting allows you to adjust how long a QuickTime file must be idle (no data being written to the file) before the HotBin begins to import the file into K2 storage. The recommended default value is 15 seconds. If you have problems with failed imports and you suspect that Final Cut Pro is holding on to the file with pauses longer than 15 seconds, you should increase the QuickTime import delay time and re-try the import. The HotBin process constrains the QuickTime import delay range to between 10 and 60 seconds.

Using Final Cut Pro on a K2 storage

Read the following topics to use access and edit K2 media with Final Cut Pro.

Operation guidelines

Take the following into consideration as you use Final Cut Pro on K2 storage.

- Do not use the K2 AppCenter "Erase Unused Media" operation on clips that you are accessing on K2 storage.

Media access

1. From the Macintosh system on which you are running Final Cut Pro, access K2 media as follows:
   - If your access method is file transfer via Flip4Mac (FTP), in Final Cut Pro click **File | Import | Grass Valley...**.
   - If your access method is file transfer via direct file copy, open the Macintosh Finder.
   - If your access method is edit-in-place, in Final Cut Pro click **File | Open**.

2. Browse to the location of the media in your K2 bin structure.

   The QuickTime reference path/file is named according to the convention *\<bin name\>\<clip name\>\<clip name\>.mov*.

   If accessing media on a K2 version 7.x system, all the files associated with the clip are in the *\<bin name\>\<clip name\>* directory.

3. Do one of the following:

   - If your access method is file transfer via Flip4Mac (FTP), transfer the QuickTime reference file to the local Macintosh system, then open the file in Final Cut Pro and Save As to the location of your work in progress.
   - If your access method is file transfer via direct file copy, copy all the files associated with the clip to the local Macintosh system, then open the QuickTime reference file in Final Cut Pro and Save As to the location of your work in progress.
   - If your access method is edit-in-place, open the QuickTime reference file in Final Cut Pro.

4. Edit the file as desired.
5. When you have finished material that you have created in Final Cut Pro, export it to the K2 system.

Export to K2 storage

When exporting media to K2 storage, Final Cut Pro export options must be constrained so that the resulting media is playable on a K2. The exported media must match the frame rate of movies supported on the K2 system. This is especially important in XDCAM where there are 25, 29.97/30, 50 and 59.94/60 rates.

1. Create the Final Cut Pro clip with a single track of video.
2. Save the Final Cut Pro clip with a *.mov* extension.
3. Use the Final Cut Pro "Using QuickTime Conversion" method to export the Final Cut Pro clip as a stream movie to the K2 HotBin.

   Make sure the frame rate is supported on the K2 system.

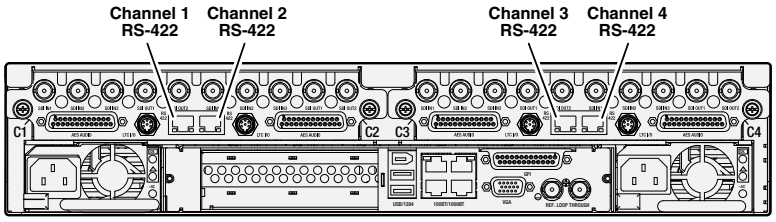
   For material originally recorded on a K2 system, supported frame rates are as follows:

   - If you are exporting 1080i material the frame rate must be "Current" or 60 (50 for PAL).
   - If you are exporting 720p material the frame rate must be "Current" or 60.
   - If you are exporting 720p material for 1080i conversions the frame rate must be 60 (50 for PAL).

The HotBin imports the clip into the K2 system as K2 media. As a by-product of the import, the K2 system creates a QuickTime reference file for the new K2 media.

Connecting RS-422 K2 Summit/Solo 3G system

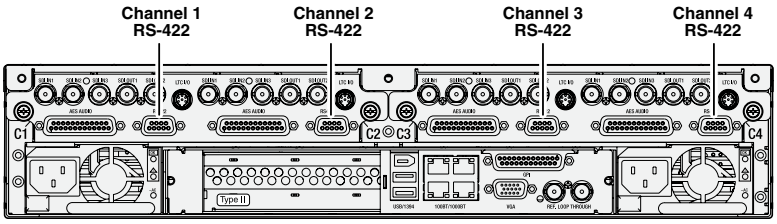
You can control the K2 system with remote control devices and software developed for the K2 system that use industry-standard serial protocols: AMP, BVW, and VDCP. Make RS-422 connections for protocol control as illustrated:



Refer to topics in "K2 AppCenter User Manual" to configure the K2 system for remote control.

Connecting RS-422 first generation Summit

You can control the K2 system with remote control devices and software developed for the K2 system that use industry-standard serial protocols: AMP, BVW, and VDCP. Make RS-422 connections for protocol control as illustrated:



Refer to the *K2 AppCenter User Manual* to configure the K2 system for remote control.

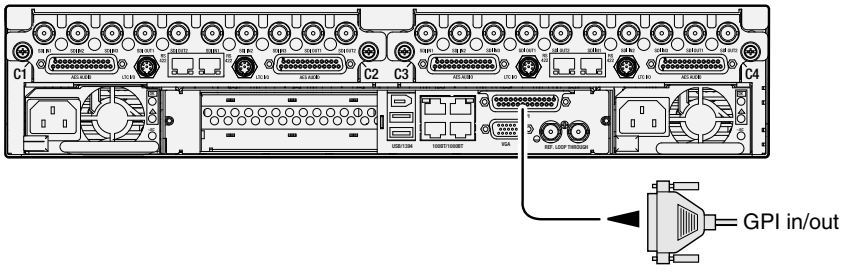
Related Topics

Remote control protocols on page 209

RS-422 protocol control connections on page 213

Connecting GPI

The K2 Summit/Solo system provides 12 GPI inputs, and 12 GPI outputs on a single DB-25 rear panel connector, as illustrated:



K2 Summit 3G system shown. Connection is identical on first generation K2 Summit/Solo system.

Refer to topics in "K2 AppCenter User Manual" for GPI configuration procedures.

Related Topics

GPI I/O specifications on page 223
GPI I/O connector pinouts on page 265

Chapter 4

Import/export services

This section contains the following topics:

Using the HotBin capture service

This section contains topics about the K2 HotBin Import capture service.

About the HotBin capture service

The functionality of the HotBin service is provided by the Grass Valley Import Service. The HotBin service provides a way to automate the import of files as clips into the K2 media file system and database. This is similar to what happens when you manually import files one at a time using K2 AppCenter import features, except with the HotBin service the files are automatically imported. The HotBin service can import any file or stream type that is supported as a K2 file-based import.

By default, the service does not start automatically. If you have never configured or used the service, it is set to startup type Manual. When you configure the 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.

There is no Grass Valley license required specifically for the HotBin service.

Before you can use the HotBin service, it must be configured through the K2 Capture Services utility. The HotBin service must be configured on the K2 system that receives the imported media. The K2 system that receives the imported media can be a K2 Solo Media Server, a stand-alone K2 Summit Production Client, a stand-alone K2 Media Client, or the K2 Media Server with the role of primary FTP server on a K2 SAN.

Once configured, the HotBin service monitors a watched folder (a HotBin). The watched folder is a specified source directory on a source PC. The watched folder can be on a stand-alone K2 system, a K2 Media Server, a Windows PC, or a Macintosh. When files are placed in the watched folder, the HotBin service imports them as a clip into the specified destination bin. The destination bin is on the K2 system that receives the imported media and is within that K2 system's media file system and database.

The HotBin service automatically creates sub-directories in the watched folder (source directory), described as follows:

- Success — After the HotBin service successfully imports the files in the source directory into the destination bin on the K2 system, it then moves those files into the Success directory.
- Fail — If the HotBin service can not successfully import the files in the source directory into the destination bin on the K2 system, it moves the failed files into the Fail directory.
- Archive — If there are files in the source directory when the Hot Bin service first starts up, it does not attempt to import those files into the K2 system. Instead, it moves those files into the Archive directory. This occurs when you first configure the Hot Bin service, if you manually stop/start the Hot Bin service, and when you upgrade K2 system software.

Related Topics

Specifications on page 215

Prerequisites for using the HotBin capture service

Before you can configure and use the P2 Import capture service, the following requirements must be satisfied:

- K2 system software must be at version 3.2.56 or higher.

Use topics in this section as appropriate to satisfy prerequisites.

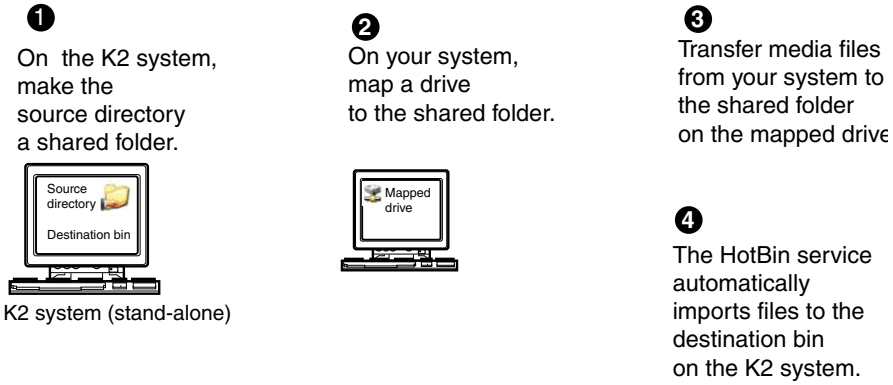
Considerations for using the HotBin capture service

When you are configuring and using the K2 HotBin capture service, bear in mind the following considerations:

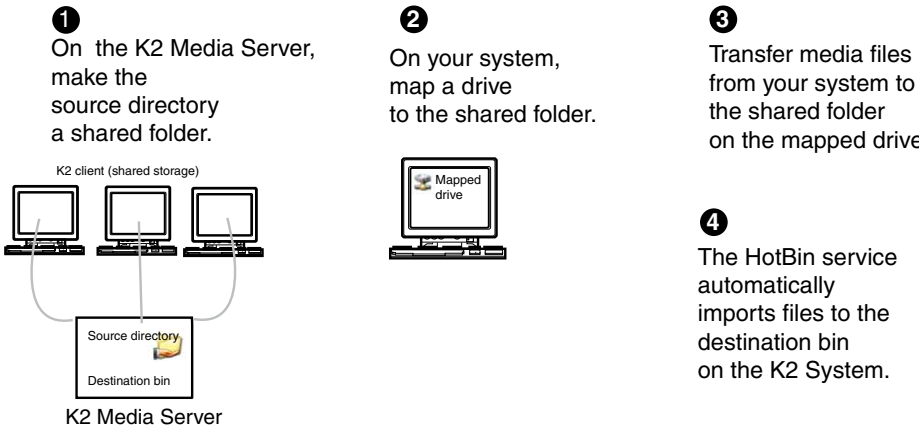
- You must be logged in with administrator privileges on the K2 system as well as having the appropriate security permissions to access the watched folder or bin.
- If you have multiple source folders (for import) or destination folders (for export) on external systems, use the same user account for all capture service access to all systems.
- If using the capture service on a K2 SAN, the K2 Capture Services utility and the import watched folder must be on a K2 Media Server that is also an FTP server. If your K2 SAN has multiple FTP servers, the utility and folder must be on the primary FTP server.
- It is recommended that you keep the source directory and destination bin located on the local V: drive, which is their default location.
- Do not configure the root of C:\ as the source directory or any other location with files that must be retained. When the HotBin service first starts up it removes files in the source directory.
- If you require that the source directory and destination bin be on different systems, system clocks must be synchronized. The Cleanup Frequency function depends on accurate system clocks.
- If you specify a destination bin name that does not yet exist, the K2 system creates it when files are transferred to it.
- Imports are serialized. For example, if you drop two clips into the watched folder for import, the capture service does not queue the second clip for import until the first clip is imported. This is different than the ordinary K2 transfer process.
- Capture service imports are serialized with other K2 transfers. For example, if fourteen items are already queued up from ordinary K2 transfers, and you drop content into the watched folder for import, the import triggered by the capture service becomes the fifteenth clip in the transfer queue.
- After the capture service imports media into K2 media storage successfully, the capture service immediately deletes the original media files from the watched folder. If the import fails, the original media files are retained in the watched folder for the number of days specified as the Cleanup Frequency.
- The “Cleanup Frequency” (purge) feature deletes files in the Success sub-directory and in the Fail sub-directory. It does not delete files in the Archive sub-directory.
- Files in the Success, Fail, and Archive sub-directories are “hidden” files in Windows Explorer. To see these files you must select Show Hidden Files in the Windows Explorer Folder Options dialog box.

Grass Valley recommends that you use the HotBin service as demonstrated in the following diagram.

Using the HotBin service with a standalone K2 system



Using the HotBin service with a K2 SAN



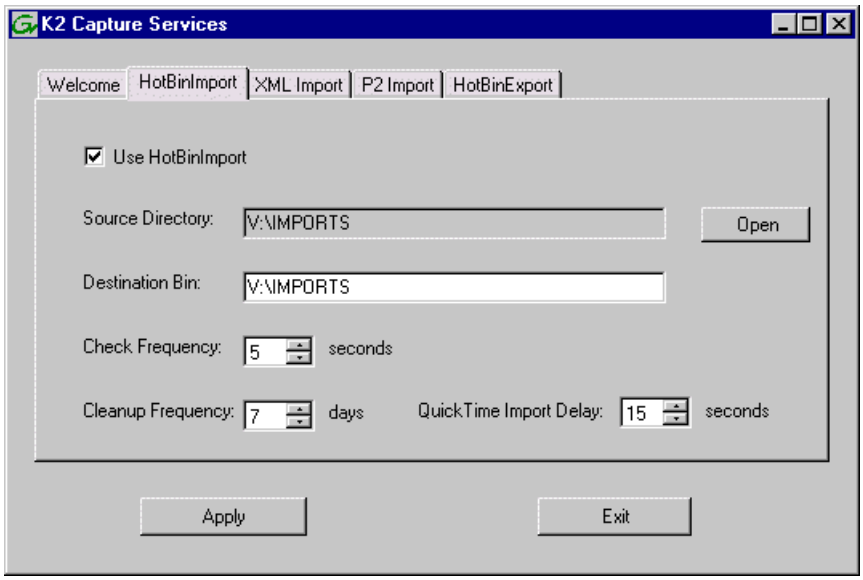
While not preferred, you can also use the HotBin service if the source directory is on another system. The following table lists the requirements for accessing a source directory located on various operating systems.

If your source directory is on:	...and the source directory is on a shared folder on a mapped drive, you need:
Another Windows system	• Administrator privileges for the K2 system • A user account with log-in service rights for your system
Macintosh operating system	• Privileges as listed above. • The identical user name and password on both systems. For example, if you have a Macintosh user named Jane, you would need to have a user named Jane on your Windows system with the same password. From the Windows Control Panel, select **Administrator Tools | Local Security Policy | User Rights Assignment | Log on as service** and click **Add New User**.

Configuring the HotBin Capture Service

NOTE: Once configured, the service deletes files in the watched folder or bin (source) that are older than the specified cleanup frequency.

1. From the **Start** menu, access the **Programs** menu and select **Grass Valley \| K2 Capture Services**. The K2 Capture Services utility dialog box is displayed.
2. Click the **HotBinImport** tab.



3. Select **Use HotBinImport**.

4. Enter the paths to the source directory and destination bin. If the source directory does not currently exist, it will automatically be created.

   NOTE: Do not configure the source directory to be a location with files that must be retained. When the HotBin service first starts up it removes files in the source directory.

5. For Check Frequency, it is recommended that you accept the default value. This value specifies how often you want the capture service to check the source directory for new files.
6. For the Cleanup Frequency, it is recommended that you accept the default value. This value specifies the maximum age of files in the source directory. The capture service deletes files that are older than this age.
7. If the source directory is not on the local K2 system, a User Account dialog box displays. Enter the user information that you use to access the source directory. If part of a domain, enter the domain name.
8. If necessary, configure QuickTime Import Delay.

   This setting adjusts how long a QuickTime file must be idle (no data being written to the file) before the HotBin begins to import the file into K2 storage. The recommended setting is 15 seconds.

9. When your capture service settings are complete, click **Apply**.

   If prompted, restart the K2 system.

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

Place files in the source directory to trigger the Hot Bin import processes.

HotBin capture service components

The following table describes the components that support K2 HotBin capture service functionality.

Name	Description
Grass Valley Import Service	This is the service that provides the functionality for a K2 capture service. It is the service that automatically creates the K2 clip from the media files in the watched folder (source directory) and puts the K2 clip in the K2 media storage (destination bin).
K2 Capture Services utility	Configures K2 capture services.
Source directory	This is the watched folder. It is a standard file system directory. When media files are placed in this directory, the capture service automatically creates a K2 clip in the K2 media storage. By default, the location of the source directory is `V:/IMPORTS`.
Check frequency	Determines how often (in seconds) the watched folder is checked for new files.
Cleanup frequency	Determines how long (in days) a file remains in the watched folder. A file with a file-creation date older than the specified number of days is deleted.

Name	Description
Destination bin	The clip bin in the K2 media storage that receives the K2 clip created by the capture service. The destination bin is in the K2 media database and appears in AppCenter as a media bin. By default, its location is `V:/IMPORTS`.

Using the XML Import capture service

This section contains topics about the K2 XML Import capture service.

About the XML Import capture service

The K2 XML Import capture service provides a way to have media automatically imported into a K2 system when it is pushed to the K2 system by a third party application. The XML Import capture service has a watched folder. The watched folder is a standard file system directory that can be recognized by the Windows operating system. You transfer the media to the directory using the third party application.

By default, the service does not start automatically. If you have never configured or used the service, it is set to startup type Manual. When you configure the 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.

After all the media files are finished being transferred to the watched folder, the third party application then transfers an XML file to the watched folder. This XML file defines the media files and specifies how they are to be assembled to create a K2 clip. When the XML file finishes transferring to the watched folder, the capture service goes into action and validates the XML file to make sure it has the proper structure. If the XML file is valid, the capture service then does the necessary processing to create the clip in the K2 media storage. The media is then available as a K2 clip, ready for playout.

The K2 XML Import capture service and its watched folder must be on a K2 system that hosts the K2 FTP interface, as follows:

- Stand-alone K2 system— When media files and the XML file are pushed to the watched folder, the capture service creates a K2 clip in the internal storage or direct-connect media storage of the K2 system. The watched folder must be on the K2 system's V: drive.
- Stand-alone K2 system— When media files and the XML file are pushed to the watched folder, the capture service creates a K2 clip in the internal storage or direct-connect media storage of the K2 system. The watched folder must be on the K2 system's V: drive.

Prerequisites for using the XML Import capture service

Before you can configure and use the XML Import capture service, the following requirements must be satisfied:

- K2 system software must be at a version that supports the XML Import capture service. Refer to *K2 Release Notes* for information on XML Import capture service version compatibility.

- The K2 XML Import capture service must be licensed on the stand-alone K2 system or K2 Media Server. This is a Grass Valley software license.
- The application that pushes the media files and XML file to the watched folder must provide valid files according to K2 XML Import capture service requirements. Developers of applications can contact Grass Valley Developer Support for more information

Use topics in this section as appropriate to satisfy prerequisites.

Considerations for using the XML import capture service

When you are configuring and using the K2 XML Import capture service, bear in mind the following considerations:

- You must be logged in with administrator privileges on the K2 system as well as having the appropriate security permissions to access the watched folder or bin.
- If using the capture service on a K2 SAN, the K2 Capture Services utility and the import watched folder must be on a K2 Media Server that is also an FTP server. If your K2 SAN has multiple FTP servers, the utility and folder must be on the primary FTP server.
- After the capture service imports media into K2 media storage successfully, the capture service immediately deletes the original media files from the watched folder. If the import fails, the original media files are retained in the watched folder for the number of days specified as the Cleanup Frequency.
- The transfer of the media files, then the XML file, must be 100% complete before the K2 XML Import capture service begins to create the clip in K2 media storage.

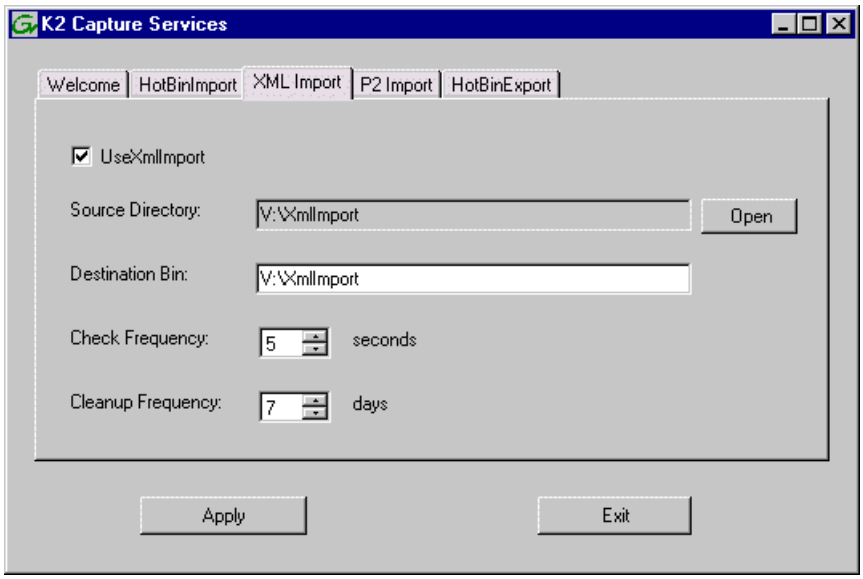
Configuring the XML Import Capture Service

NOTE: Once configured, the service deletes files in the watched folder or bin (source) that are older than the specified cleanup frequency.

1. From the **Start** menu, access the **Programs** menu and select **Grass Valley | K2 Capture Services**.

   The K2 Capture Services utility dialog box is displayed.

2. Click the **XML Import** tab.



3. Select **UseXMLImport**.

   If you have not yet licensed the XML Import capture service, a "…start the process of getting a license now?" message appears. Follow on-screen instructions to obtain a license. After licensing, restart the K2 Capture Services utility and continue with this procedure.

4. Enter the paths to the source directory and destination bin, which are defined as follows:

   - Source Directory — This is the watched folder. It is a standard file system directory. It must be on the K2 system's V: drive. When valid media is placed in this directory, the capture service automatically creates a K2 clip in the K2 media storage.
   - Destination Bin — The clip bin in the K2 media storage that receives the media processed by the capture service. The destination bin is in the K2 media database and it appears in AppCenter as a media bin. The bin must be on the K2 system's V: drive. If you specify a destination bin name that does not yet exist, the K2 system creates it when the K2 clip is created.

5. For Check Frequency, it is recommended that you accept the default value. This value specifies how often you want the capture service to check the source directory for new files.
6. For the Cleanup Frequency, it is recommended that you accept the default value. This value specifies the maximum age of files in the source directory. The capture service deletes files that are older than this age.
7. When your capture service settings are complete, click **Apply**.

   If prompted, restart the K2 system.

The service checks the source directory for any files that are beyond the specified cleanup age and deletes them from the directory.

Testing the XML Import Capture Service

1. Place media files into the watched folder.
2. On the K2 System, open Windows Explorer, browse to the watched folder and verify that files have completed the transfer. The transfer must be 100% complete before the capture service triggers the processes to create the K2 clip.
3. Place a valid XML file into the watched folder.
4. On the K2 System, open Windows Explorer, browse to the watched folder and verify that XML file has completed the transfer. The transfer must be 100% complete before the K2 XML Import capture service triggers the processes to create the K2 clip.
5. After the K2 clip is created, verify that the media appears in the destination bin.
6. Play to verify success.

XML Import capture service components

The following table describes the components that support K2 XML Import capture service functionality.

Name	Description
Grass Valley Import Service	This is the service that provides the functionality for a K2 capture service. It is the service that automatically creates the K2 clip from the media files in the watched folder (source directory) and puts the K2 clip in the K2 media storage (destination bin).
K2 Capture Services utility	Configures K2 capture services.
Source directory	This is the watched folder. It is a standard file system directory. When media files are placed in this directory, the capture service automatically creates a K2 clip in the K2 media storage. By default, the location of the source directory is `V:\XmlImport`.
Check frequency	Determines how often (in seconds) the watched folder is checked for new files.
Cleanup frequency	Determines how long (in days) a file remains in the watched folder. A file with a file-creation date older than the specified number of days is deleted.
Destination bin	The clip bin in the K2 media storage that receives the K2 clip created by the capture service. The destination bin is in the K2 media database and appears in AppCenter as a media bin. By default, its location is `V:\XmlImport`.

Using the P2 capture service

This section contains topics about the K2 P2 Import capture service.

About the P2 capture service

The K2 P2 Import capture service provides a way to have P2 media automatically imported into a K2 system. The P2 Import capture service has a watched folder. The watched folder is a standard file system directory that can be recognized by the Windows operating system. You transfer the media to the directory and it is imported into the K2 system.

By default, the service does not start automatically. If you have never configured or used the service, it is set to startup type Manual. When you configure the 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.

The watched folder receives the nested directories that define P2 media for one clip or multiple clips. After all the directories/files are finished being transferred to the watched folder, the capture service goes into action and validates the P2 media to make sure it has the proper structure. If the P2 file is valid, the capture service then does the necessary processing to create the clip in the K2 media storage. The media is then available as a K2 clip, ready for playout.

The K2 P2 Import capture service and its watched folder must be on a K2 system that hosts the K2 FTP interface, as follows:

- Stand-alone K2 system — When media files and the P2 file are pushed to the watched folder, the capture service creates a K2 clip in the internal storage or direct-connect media storage of the K2 system. The watched folder must be on the K2 system's V: drive.
- K2 Media Server with role of FTP server — When media files are pushed to the watched folder, the capture service creates a K2 clip in the shared media storage of the K2 SAN. The watched folder must be on the K2 Media Server's V: drive.

Prerequisites for using the P2 capture service

Before you can configure and use the P2 Import capture service, the following requirements must be satisfied:

- The K2 system must support AVC-Intra. This requires that the AVC-Intra codec card be installed.
- K2 system software must be at a version that supports the P2 Import capture service. Refer to *K2 Release Notes* for information on P2 Import capture service version compatibility.
- The K2 P2 Import capture service must be licensed on the stand-alone K2 system or K2 Media Server. This is a Grass Valley software license.
- The Panasonic storage device that is the source of the P2 media must be on a separate PC and all Panasonic drivers must exist on that PC.
- The directories/file transferred to the watched folder must be valid files according to P2 requirements.

Use topics in this section as appropriate to satisfy prerequisites.

Considerations for using the P2 capture service

When you are configuring and using the K2 P2 Import capture service, bear in mind the following considerations:

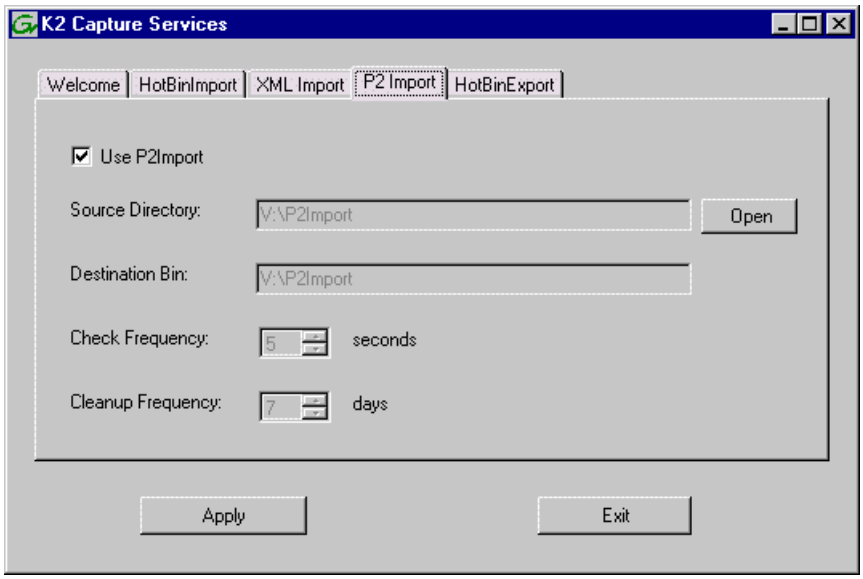
- You must be logged in with administrator privileges on the K2 system as well as having the appropriate security permissions to access the watched folder or bin.
- If you have multiple source folders (for import) or destination folders (for export) on external systems, use the same user account for all capture service access to all systems.
- If using the capture service on a K2 SAN, the K2 Capture Services utility and the import watched folder must be on a K2 Media Server that is also an FTP server. If your K2 SAN has multiple FTP servers, the utility and folder must be on the primary FTP server.
- You can share the K2 V: drive, so that the Panasonic storage device can access via CIFS.
- P2 content can be dragged/dropped onto the V: drive watch folder from a Panasonic storage device.
- After the capture service imports media into K2 media storage successfully, the capture service immediately deletes the original media files from the watched folder. If the import fails, the original media files are retained in the watched folder for the number of days specified as the Cleanup Frequency.
- The transfer of the directories/files must be 100% complete before the capture service begins to create the clip in K2 media storage.
- P2 content is imported as follows:
  - A simple clip with striped timecode is created.
  - Video (AVC-Intra and DV) track is imported and added to the clip
  - Audio tracks are imported and added to the clip
  - There is no P2 Import of metadata into the clip

Configuring the P2 Capture Service

NOTE: Once configured, the service deletes files in the watched folder or bin (source) that are older than the specified cleanup frequency.

1. From the **Start** menu, access the **Programs** menu and select **Grass Valley | K2 Capture Services**.
   The K2 Capture Services utility dialog box is displayed.

2. Click the **P2 Import** tab.



3. Select **Use P2Import**.

   If you have not yet licensed the P2 Import capture service, a "…start the process of getting a license now?" message appears. Follow on-screen instructions to obtain a license. After licensing, restart the K2 Capture Services utility and continue with this procedure.

4. Enter the paths to the source directory and destination bin, which are defined as follows:

   - Source Directory — This is the watched folder. It is a standard file system directory. It must be on the K2 system's V: drive. When valid media is placed in this directory, the capture service automatically creates a K2 clip in the K2 media storage.
   - Destination Bin — The clip bin in the K2 media storage that receives the media processed by the capture service. The destination bin is in the K2 media database and it appears in AppCenter as a media bin. The bin must be on the K2 system's V: drive. If you specify a destination bin name that does not yet exist, the K2 system creates it when the K2 clip is created.

5. For Check Frequency, it is recommended that you accept the default value. This value specifies how often you want the capture service to check the source directory for new files.
6. For the Cleanup Frequency, it is recommended that you accept the default value. This value specifies the maximum age of files in the source directory. The capture service deletes files that are older than this age.
7. When your capture service settings are complete, click **Apply**.

   If prompted, restart the K2 system.

The service checks the source directory for any files that are beyond the specified cleanup age and deletes them from the directory.

Testing the P2 Capture Service

1. Place P2 directories/files into the watched folder.
2. On the K2 System, open Windows Explorer, browse to the watched folder and verify that files have completed the transfer. The transfer must be 100% complete before the capture service triggers the processes to create the K2 clip.
3. After the K2 clip is created, verify that the media appears in the destination bin.
4. Play to verify success.

P2 capture service components

The following table describes the components that support K2 P2 Import capture service functionality.

Name	Description
Grass Valley Import Service	This is the service that provides the functionality for a K2 capture service. It is the service that automatically creates the K2 clip from the media files in the watched folder (source directory) and puts the K2 clip in the K2 media storage (destination bin).
K2 Capture Services utility	Configures K2 capture services.
Source directory	This is the watched folder. It is a standard file system directory. When media files are placed in this directory, the capture service automatically creates a K2 clip in the K2 media storage. By default, the location of the source directory is `V:\P2Import`.
Check frequency	Determines how often (in seconds) the watched folder is checked for new files.
Cleanup frequency	Determines how long (in days) a file remains in the watched folder. A file with a file-creation date older than the specified number of days is deleted.
Destination bin	The clip bin in the K2 media storage that receives the K2 clip created by the capture service. The destination bin is in the K2 media database and appears in AppCenter as a media bin. By default, its location is `V:\P2Import`.

Using the Export capture service

This section contains topics about the K2 Export capture service.

About the Export capture service

The Export capture service provides a way to have media automatically exported from a K2 system. The capture service has a watched bin. The watched bin is a K2 storage system bin. You place the media in the bin and it is exported from the K2 system.

By default, the service does not start automatically. If you have never configured or used the service, it is set to startup type Manual. When you configure the 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.

You configure the watched bin to export the K2 media as your desired clip format. After you place the K2 clip in the watched bin, the capture service goes into action and validates the media to make sure it has the proper structure for the desired file format. If it is valid, the capture service then does the necessary processing to export the clip to the destination folder.

The Export capture service and its watched bin must be on a K2 system that hosts the K2 FTP interface, as follows:

- Stand-alone K2 system — When you place a K2 clip in the watched bin, the capture service exports the clip from the internal storage or direct-connect media storage of the K2 system. The watched bin must be on the K2 system's V: drive.
- K2 Media Server with role of FTP server — When you place a K2 clip in the watched bin, the capture service exports the clip from the shared media storage of the K2 SAN. The watched bin must be on the K2 Media Server's V: drive.

Prerequisites for using the Export capture service

Before you can configure and use the Export capture service, the following requirements must be satisfied:

- The K2 system must support the clip format you plan to export. This could require specific hardware and/or licenses.
- K2 system software must be at a version that supports the Export capture service. Refer to *K2 Release Notes* for information on Export capture service version compatibility.
- The capture service must be licensed on the stand-alone K2 system or K2 Media Server. This is a Grass Valley software license.

Use topics in this section as appropriate to satisfy prerequisites.

Considerations and requirements for using the Export capture service

When you are configuring and using the Export capture service, do the following:

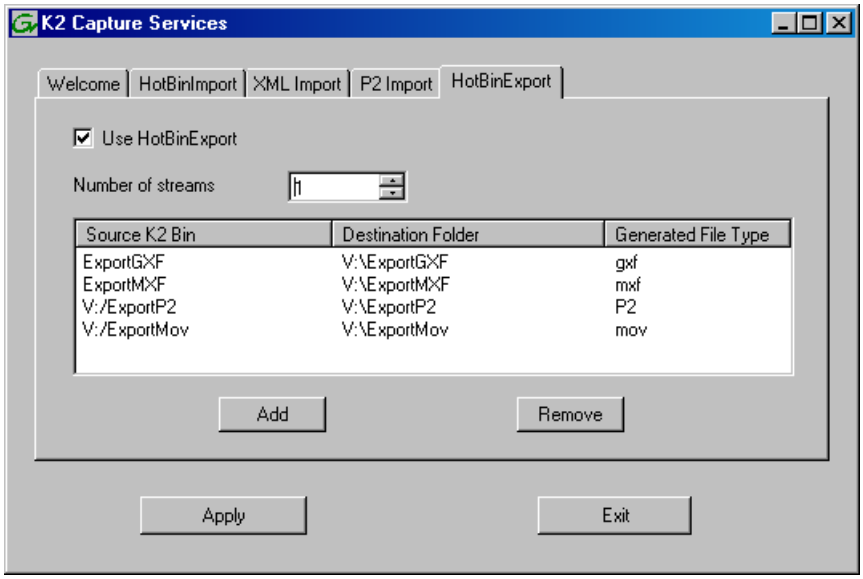
- You must be logged in with administrator privileges on the K2 system as well as having the appropriate security permissions to access the watched folder or bin.
- If the destination folder (for export) is on a remote machine, you must configure the "movie" user account as a local user account on that machine. The "movie" user account is not supported as a domain administrator account. Configure the account as follows:
  - Username: `movie`
  - Password: `M0vieK2M0vie`

  The password uses the number zero character, not the letter O character.

- If the destination folder (for export) is on a remote machine, the local K2 Summit system must be able to access the remote system with administrator level credentials. If on a domain, the account used to access the remote system must be a domain administrator account.
- If you have multiple source folders (for import) or destination folders (for export) on external systems, use the same user account for all capture service access to all systems.
- If using the export capture service on a K2 SAN, the K2 Capture Services utility must be on a K2 Media Server that is also an FTP server. If your K2 SAN has multiple FTP servers, the utility must be on the primary FTP server.

Configuring the Export Capture Service

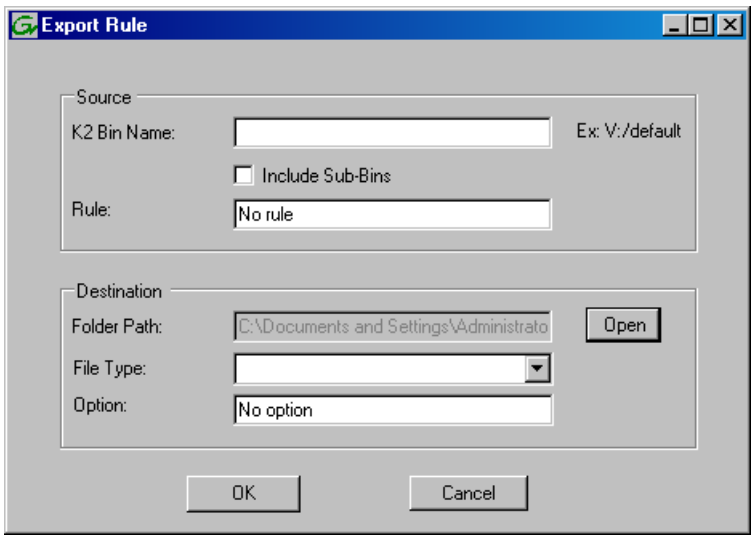
1. From the **Start** menu, access the **Programs** menu and select **Grass Valley | K2 Capture Services**.
   The K2 Capture Services utility dialog box is displayed.
2. Click the **HotBinExport** tab.



3. Select **Use HotBinExport**.
   If you have not yet licensed the HotBin Export capture service, a "…start the process of getting a license now?" message appears. Follow on-screen instructions to obtain a license. After licensing, restart the K2 Capture Services utility and continue with this procedure.
4. Select the number of streams.
   Exports run serially. If you select one stream, only one export can occur at a time. If you select multiple streams, multiple exports can occur at one time.

5. Click **Add**.

   The Export Rule dialog box opens.



6. Configure as follows:

   - Source K2 Bin Name — Required. This is the watched bin. The bin must be on the K2 system's V: drive. It must be in the K2 media database and appears in AppCenter as a media bin. When valid clips are placed in this bin, the HotBin Export capture service automatically exports the clips.
   - Include Sub-Bins — Optional. When selected, clips are exported if they are in a bin nested inside the Source K2 Bin.
   - Rule — Do not configure this field. Leave the default value as it is.
   - Destination Folder Path — Required. This is a standard file system directory. It receives the files/directories exported by the Export capture service. If you specify a destination folder that does not yet exist, the K2 system creates it when exporting. If the destination folder is not on the local K2 system, you are prompted to enter user account credentials to access the source directory. You must enter user account credentials that have administrator level privileges on the remote system. If part of a domain, the user account must be a domain administrator account. When you enter a domain account, you must enter the domain name.

     NOTE: You must use the same user account for all capture service access to all systems.
   - File Type — Required. Select the file format in which K2 clips are exported.
   - Option — Do not configure this field. Leave the default value as it is.

7. Click **OK** to save settings and close the Export Rule dialog box.
8. Repeat previous steps to add additional Export HotBins.

Testing the Export Capture Service

1. Place the clips to export into the watched bin.
2. Verify that the media appears in the destination.

3. Play to verify success.

Export capture service components

The following table describes the components that support Export capture service functionality.

Name	Description
Grass Valley Import Service	This is the service that provides the functionality for the capture service. It is the service that automatically exports K2 clips from the K2 media storage.
K2 Capture Services utility	Configures K2 capture services.
Source K2 bin	This is the watched bin. It is a bin in K2 media storage. When files are placed in this directory, the capture service automatically exports them from K2 media storage.
Destination folder	The folder that receives the files exported from the K2 media storage.

Licensing K2 capture service software

Licensing is required for K2 capture service software as follows:

- To use the XML Import capture service, you must obtain a XML Import capture service license from Grass Valley.
- To use the P2 Import capture service, you must obtain a P2 Import capture service license from Grass Valley.
- To use the Export capture service, you must obtain an Export capture service license from Grass Valley.

Licenses are requested through the K2 License Wizard and managed through the SabreTooth License Manager, which are installed with K2 system software.

1. To start the licensing process, open the K2 Capture Services utility and on the tab for your capture service, select the "Use…" checkbox.

   If you do not yet have a license, a "…start the process of getting a license now?" message appears.

2. Click **Yes** and **OK** to open the K2 License Wizard for the type of license. Refer to *K2 Release Notes* for procedures and information on obtaining and managing licenses.

PitchBlue workflow considerations

The K2 Summit system supports the H.264 format used in the PitchBlue workflow. However, you must consider the intended PitchBlue workflow when using this H.264 media, as it is not supported for general purpose use outside of the PitchBlue workflow.

The K2 Summit system ingests the PitchBlue material without any error correction. The material often has anomalies, such as a broken last frame, that the K2 Summit system accepts as-is. When PitchBlue plays out this material under VDCP automation control, it plays the known-good material only. PitchBlue determines where the anomalies exist and makes sure that they are not played out.

In this way PitchBlue avoids the errors that would otherwise occur if the material were used for general purpose playout without PitchBlue control.

Therefore, you must adhere to the complete PitchBlue workflow from ingest through playout for all PitchBlue material. Do not attempt to play out PitchBlue material except as part of the prescribed PitchBlue workflow. Playing out PitchBlue material in any other way can cause errors.

Pinnacle support

The K2 system can automatically convert Pinnacle material into K2 clips as part of a FTP transfer or a HotBin import, as described in the topics in this section.

Pinnacle material that can be converted

A Pinnacle clip is stored as a folder on a Pinnacle MediaStream server. The folder structure for its MPEG program/system stream based content is as follows:

```
<folder> clipname
  <file> header (contains Pinnacle clip metadata)
  <file> ft (Pinnacle version of "Frame Index Table")
  <file> info (File used to hold automation specific data. Not
  used by Pinnacle.)
  <file> std (The MPEG program or system stream -
  essence/media)
```

You have the following options for the Pinnacle material to convert:

- Convert only the media essence (the std file).
- Convert the metadata along with the media essence.

Pinnacle import mechanisms

You have the following options for import/transfer mechanisms:

- K2 HotBin import — This method converts only the media essence. It does not convert the Pinnacle clip metadata. You drop the Pinnacle clip's std file into a K2 HotBin. Then the K2 HotBin process imports, converts, and creates a K2 clip. The K2 clip is available for playout when the process is complete.
- K2 FTP import — This method converts only the media essence. It does not convert the Pinnacle clip metadata. Your third-party FTP client connects to the K2 FTP server as a normal K2 FTP session and puts the Pinnacle clip's std file.
- Pinnacle emulation K2 FTP import — This method converts the Pinnacle clip metadata along with the media essence. Your third-party automation vendor or FTP client connects to the K2 FTP server with the Pinnacle specific login, creates a new directory, and puts the Pinnacle clip files in the new directory. The K2 FTP server creates a corresponding K2 clip. The K2 clip is available for playout while the content is being transferred. The K2 clip contains timecode, mark in/out points, and other metadata as defined by the Pinnacle clip metadata.

Enabling Pinnacle import

Before you import your Pinnacle material, familiarize yourself with the configuration options in the following procedure.

1. To import Pinnacle material, create the following registry value:

```
HKEY_LOCAL_MACHINE\Software\Grass Valley Group\Streaming
REG_DWORD "ImportPinnacleStreams" = 1
```

   Without this registry value, the K2 system does not handle the import correctly.

2. Do one of the following:

   - If do not want to import captions and timecode from your Pinnacle material, skip the remainder of this procedure. No further configuration is necessary.
   - If you want to import captions and timecode from your Pinnacle material, continue with this procedure. Read each step carefully and proceed only if you are sure that your Pinnacle material is suitable.

3. To optionally import VITC from Pinnacle clips, proceed with this step as appropriate.

   - If you know that VITC was not recorded on your Pinnacle material in the Pinnacle-private uncompressed VBI data, skip to the next step. Do not create a registry value.
   - If you know that your Pinnacle material was recorded with VITC as Pinnacle-private uncompressed VBI lines and you want to preserve this timecode when you import the content into the K2 system, then create the following registry key:

```
HKEY_LOCAL_MACHINE\Software\Grass Valley Group\Streaming
REG_DWORD "ExtractPinnacleVitc" = 1
```

   This instructs the K2 system to extract and preserve the VITC.

4. To optionally import captions from Pinnacle clips, proceed with this step as appropriate.

   - If you know that captions were not recorded on your Pinnacle material in the Pinnacle-private uncompressed VBI data, skip the remainder of this procedure. Do not create a registry value.
   - If you know that your Pinnacle material was recorded with closed captions or teletext data as Pinnacle-private uncompressed VBI lines and you want to preserve the captions when you import the content into the K2 system, then create the following registry key:

```
HKEY_LOCAL_MACHINE\Software\Grass Valley Group\Streaming
REG_DWORD "ExtractPinnacleCaptions" = 1
```

   This instructs the K2 system to extract and preserve the captions.

When you are no longer using the K2 system to import Pinnacle material, you can delete all of the above registry values that you created to support the import.

Importing via K2 Hot Bin

1. If you have not already done so, configure a K2 HotBin.
2. Rename the Pinnacle clip's *std* file with your desired K2 clip name and a **.mpg* extension.

3. Drop the file in the K2 HotBin.

Importing via K2 FTP

1. With your third-party FTP client, connects to the K2 FTP server as a standard K2 FTP session.
2. Use the FTP `put` command to transfer the Pinnacle clip's *`std`* file with your desired K2 clip name.

   Use the following example as a guideline:

```
ftp mx-proto-b14
Connected to mx-proto-b14.
220 FTP Server (1, 0, 0, 1) ready.
User (mx-proto-b14:(none)): administrator
331 Password required for user administrator.
Password:
230 Logged in, and aspect successfully set to MOVIE, stream mode GXF.
ftp> bin
200 Type set to IMAGE.
ftp> put std /MPG/V:/default/646405_IMX30_ MXF_IPN
200 PORT command okay.
150 Opening MOVIE mode data connection for
/explodedFile/V:/default/646405_IMX30_ MXF_IPN.
226 Transfer complete.
ftp: 54547968 bytes sent in 14.05Seconds 3883.25Kbytes/sec.
ftp> quit
221 Goodbye.
```

Importing via Pinnacle emulation K2 FTP

1. With your third-party automation vendor or FTP client, connect to the K2 FTP server as follows:

   FTP username: video_fs

   FTP password: .video_fs

   The username and password are case sensitive.
2. Create a directory named for the Pinnacle clip.

3. Put the following Pinnacle clip files in the directory in the following order:

   header

   ft

   info (optional)

   std

   Use the following example as a guideline:

```
J:\>ftp mx-proto-b14
Connected to mx-proto-b14.
220 FTP Server (1, 0, 0, 1) ready.
User (mx-proto-b14:(none)): video_fs
331 Password required for user video_fs.
Password:
230 Logged in, and aspect successfully set to MOVIE, stream mode PIN.
ftp> bin
200 Type set to IMAGE.
ftp> mkdir pinnacle_clip
250 Command "XMKD pinnacle_clip" succeeded.
ftp> cd pinnacle_clip
250 Change of directory to explodedFile/V:/default/pinnacle_clip
successful, xfer mode PIN.
ftp> put header
200 PORT command okay.
150 Opening MOVIE mode data connection for header.
226 Transfer complete.
ftp: 132 bytes sent in 0.00Seconds 132000.00Kbytes/sec.
ftp> put ft
200 PORT command okay.
150 Opening MOVIE mode data connection for ft.
226 Transfer complete.
ftp: 393216 bytes sent in 0.11Seconds 3574.69Kbytes/sec.
ftp> put std
200 PORT command okay.
150 Opening MOVIE mode data connection for
/explodedFile/V:/default/pinnacle_clip.
226 Transfer complete.
ftp: 56097960 bytes sent in 16.25Seconds 3452.18Kbytes/sec.
ftp> quit
221 Goodbye.
```

Related Topics

About the K2 FTP interface on page 73

Specifications for Pinnacle support

- Pinnacle clips do not indicate timecode as drop-frame. The K2 import assumes non-drop-frame values.
- The time-code used in the header file and recorded into the MPEG Video GOP header starts out as 00:00:00:00 by default. If the option to extract VITC is not enabled, or no VITC is detected on import, timecode extracted from the MPEG Video GOP manifests as the timecode track for the imported K2 clip.

- Pinnacle servers preserve non-MPEG-1 (Musicam) audio as Pinnacle-private elementary streams within the program stream *std* file. Pinnacle clips allow up to 8 channels of audio. On import the K2 system detects the private stream audio packets when they are present and generates the appropriate K2 audio track(s).
- When importing Pinnacle content recorded as an MPEG1 system stream, any Pinnacle-private audio from MPEG2 program stream based clips is lost.
- The K2 system supports extraction of the following kinds of Pinnacle-private audio:
  - PCM-16, PCM-20 (PCM-20 is converted into PCM-24 on import)
  - DolbyE and AC-3
- If you enable the option via registry key, the K2 system examines specific VBI lines when it detects Pinnacle-private VBI lines, as follows:
  - Line 21 (default, can be overridden via registry) is examined for the presence of close captioning or SDP teletext. If detected, this is appropriately de-modulated into EIA-608 close caption or OP-47 subtitling packets and inserted as ancillary data packets into an ancillary data track on the imported clip.
  - Line 19-PAL and 14-NTSC (default, can be overridden via registry) is examined for the presence of VITC. If detected, this is appropriately de-modulated into SMPTE 12M compliant time-code values which is inserted as time-code values into the time-code track on the imported clip.
- The following applies to the Pinnacle emulation K2 FTP import:
  - All supported FTP commands, with the exception of those mentioned below, respond as they do for a conventional K2 FTP session. For instance, commands such as renames and deletes operate on K2 clips, directory listings reveal K2 clips and bins, and so on.
  - Navigation (`cd`) to K2 bins is allowed. By default, the *default* K2 bin is projected as the FTP root.
  - The `MKD/XMKD` command does not create a K2 bin for the argument specified, but merely retains the argument as the name of the K2 clip to be created based on following `STOR` commands.
  - The `CWD/XCWD` command does not allow navigation to a K2 bin. If the Pinnacle clip name used in a previous MKD command is used as an argument to `CWD`, the K2 FTP server does not internally navigate to that “bin”, but rather merely returns a success status.
  - The `STOR` command only honors `ft`, `std`, or `header` as arguments, or filenames with a *.mxf* extension. When the K2 FTP server receives data for the *std* file it creates a K2 clip with the name issued by a previous `MKD/XMKD` command.

Compressed VBI import

The K2 system can be set up to import Standard Definition (SD) Compressed VBI closed captioning. The feature can be useful for workflows that include SD clips from Profile XP and other video servers, or for facilities transitioning from SD to HD. If you are interested in this feature, contact Grass Valley Support to determine if it is appropriate for your system design. If appropriate, Grass Valley Support can provide you with the instructions to enable the feature.

About compressed VBI import processes

The K2 system extracts closed captioning by decoding the compressed video. The K2 system then inserts the extracted closed captioning as an SD ancillary data track into the K2 clip. These processes occur as the material is being transferred into the K2 system.

These processes take place on the K2 device performing the import. This can be a stand-alone or SAN K2 system. During these import processes the CPU consumption on the system performing the import is higher than with conventional imports. Take this into consideration when planning to use this feature.

Compressed VBI import specifications

The compressed VBI import is supported as follows:

- SD MPEG only.
- All forms of import are supported, such as FTP, automation protocols, AppCenter, Capture services, and InSync.
- GXF, MXF, MPEG, and MOV imports extract closed captioning from SD 720x512 video.
- D-10/IMX SD MPEG video is supported
- SD 525 line (NTSC) closed captioning is supported
- SD 625 line (PAL) teletext is not supported
- The first SD video track encountered is processed for compressed VBI. Multiple video tracks are not processed.
- If the incoming video contains compressed VBI lines but closed caption data is not present, the resultant K2 clip has an ancillary data track containing “blank” closed caption data. On playout, the blank closed caption data is inserted into the video, but no closed caption is displayed for the video.
- If an MPEG program/transport stream contains both ATSC Closed Captioning inserted into the MPEG picture user data and compressed VBI lines, the K2 system ignores the compressed VBI lines and processes for the ATSC Closed Captioning instead.
- The K2 system does not process the incoming video when the following occurs:
  - The video does not contain compressed VBI lines
  - The video already contains an ancillary data track
  - The video is High Definition (HD)
  - The video is a GXF complex movie, such as a program or a playlist.

Chapter 5

Managing Stand-alone Storage

This section contains the following topics:

About the internal storage system

A K2 Summit/Solo system with internal drives for media storage is a self-contained, stand-alone unit, with no external devices for storage, audio, or video connections required.

Related Topics

K2 Summit Transmission models on page 197

K2 Summit 3G internal storage system

The storage system on an internal storage first generation K2 Summit system includes the following:

mSATA — The mSATA SSD boot media on the front interconnect board serves as the system drive. The Windows operating system, applications, and other standard computer software components reside on the system drive.

RAID drives — There are slots for twelve 2.5 inch RAID drives, located behind the front bezel assembly in the front of the unit. These drives are for media storage. Twelve media drives are available. Media data is written or "striped" across media drives in a continuous fashion, which makes them a "stripe group". This media stripe group appears as the V: drive to the Windows operating system.

Disk controller board — The disk controller board provides the RAID functionality for the internal disks. It is mounted vertically in the front of the unit. K2 Summit 3G systems with direct-connect storage or shared SAN storage do not contain a disk controller board, as RAID disks are in the external RAID storage devices.

RAID 1 — Drives configured as RAID 1 provide redundancy. The two disks in a RAID 1 LUN are redundant partners. Any single disk in a LUN can fail and disk access can continue. When a disk fails, error messages in the AppCenter StatusPane inform you of the problem. You can then replace the failed disk. The data is rebuilt on the replacement disk and redundancy is restored.

RAID 0 — Media drives configured as RAID 0 offer no redundancy. If any single RAID 0 media drive fails, all data is lost on all media drives.

First generation K2 Summit internal storage system

The storage system on an internal storage first generation K2 Summit system includes the following:

Compact Flash — The Compact Flash boot media serves as the system drive. The Windows operating system, applications, and other standard computer software components reside on the system drive.

RAID drives — There are slots for eight 3.5 inch RAID drives, located behind the front bezel assembly in the front of the unit. These drives are for media storage. Eight media drives are available. RAID 0 is available as an option from the factory. Media data is written or "striped" across media drives in a continuous fashion, which makes them a "stripe group". This media stripe group appears as the V: drive to the Windows operating system.

Disk controller board — The disk controller board provides the RAID functionality for the internal disks. It is mounted horizontally in the front center of the unit. K2 Summit systems with direct-connect

storage or shared SAN storage do not contain a disk controller board, as RAID disks are in the external RAID storage devices.

RAID 1 — Drives configured as RAID 1 provide redundancy. The two disks in a RAID 1 LUN are redundant partners. Any single disk in a LUN can fail and disk access can continue. When a disk fails, error messages in the AppCenter StatusPane inform you of the problem. You can then replace the failed disk. The data is rebuilt on the replacement disk and redundancy is restored.

RAID 0 — Media drives configured as RAID 0 offer no redundancy. If any single RAID 0 media drive fails, all data is lost on all media drives.

K2 Solo Media Server internal storage system

The storage system on a K2 Solo Media Server includes the following:

Compact Flash — The Compact Flash boot media serves as the system drive. The Windows operating system, applications, and other standard computer software components reside on the system drive.

RAID drives — A K2 Solo Media Server contains 2 disk modules. Media data is written or "striped" across media drives in a continuous fashion, which makes them a "stripe group". This media stripe group appears as the V: drive to the Windows operating system. Disks are configured as RAID 0, so you cannot remove and replace a disk module while the K2 Solo Media Server is operational. If a disk fails, you lose all media.

Disk controller board — The disk controller board provides the RAID functionality for the internal disks.

RAID 0 — Media drives configured as RAID 0 offer no redundancy. If any single RAID 0 media drive fails, all data is lost on all media drives.

About the direct-connect storage system

A K2 Summit system that is directly connected to an external K2 RAID storage device for media storage is a self-contained, stand-alone unit.

The storage system on direct-connect storage K2 Summit system includes the following:

System Drive — Compact Flash (first generation Summit) or mSATA (Summit 3G) boot media serves as the system drive. The Windows operating system, applications, and other standard computer software components reside on the system drive.

Fibre Channel card — The direct-connect K2 Summit system has a direct Fibre Channel connection to external K2 RAID. The K2 Summit system must have the optional Fibre Channel card installed to support this connection.

There are no internal RAID drives or a disk controller board in a direct-connect storage K2 Summit system.

RAID 5 — Drives configured as RAID 5 provide redundancy. There are six disks in one RAID 5 LUN. A disk in a LUN can fail and disk access can continue. When a disk fails, error messages in the AppCenter StatusPane inform you of the problem. You can then replace the failed disk. The data is rebuilt on the replacement disk and redundancy is restored.

Using Storage Utility

This section contains topics about using Storage Utility for stand-alone internal storage.

About Storage Utility

You can use Storage Utility for general maintenance tasks on a stand-alone internal storage K2 system. Refer to the Service Manual for your K2 product for repair procedures, such as those required to replace a failed drive.

NOTE: Do not run Storage Utility on a shared storage (SAN) K2 client. For shared storage, run Storage Utility only via the K2 System Configuration application, as explained in the K2 SAN Installation and Service Manual.

The Storage Utility runs on either the local K2 system or from a Control Point PC. In both cases the Storage Utility's primary functionality is hosted by the K2 system. The Storage Utility uses the connection to the RAID disks for access and configuration.

A stand-alone K2 system runs in either an online mode or an offline mode. These modes are required for Storage Utility operations. Online/offline modes are as follows:

- Online mode — This is the stand-alone K2 system's normal operating mode. When the stand-alone K2 system is in the online mode and you open Storage Utility, you can stay in this mode while you view the devices, LUNs, and disks of the internal storage system, but you can not configure the storage system. However, some operations are available that do not configure the storage system, such as identify a drive (flash the drive LEDs), get controller logs, disable a drive, and force a drive to rebuild.
- Offline mode — In this mode the stand-alone K2 system channels are disconnected and all media access operations are disabled. You are prompted to put the stand-alone K2 system into offline mode when you select an operation that configures the storage system. When the stand-alone K2 system is in the offline mode you can configure the storage system and perform all Storage Utility operations. When you exit Storage Utility you can put the stand-alone K2 system back into online mode.

⚠ ***CAUTION: Use the Storage Utility only as directed by a documented procedure or by Grass Valley Support. If used improperly, the Storage Utility can render your K2 system inoperable or result in the loss of all your media.***

Related Topics

Storage Utility for standalone K2 Summit/Solo system on page 56

Opening Storage Utility

There are two ways to open Storage Utility for work on a stand-alone K2 system, as explained in the following sections.

Opening Storage Utility through AppCenter

Unless prevented by a system problem, you should always open Storage Utility through AppCenter. When you do this your AppCenter login permissions are passed to Storage Utility, so you do not have to log in to Storage Utility separately.

If you are running AppCenter on the local K2 system, as Storage Utility opens it connects to the storage system of that local K2 system. If you are running AppCenter on a control point PC, as Storage Utility opens it connects to the storage system of the K2 system that hosts the channel currently selected in AppCenter.

1. Open AppCenter, either on the local K2 system or on the control point PC and log in.

   Make sure you log in to AppCenter with appropriate privileges, as this log in 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 client 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.

Related Topics

About identifying disks on page 130

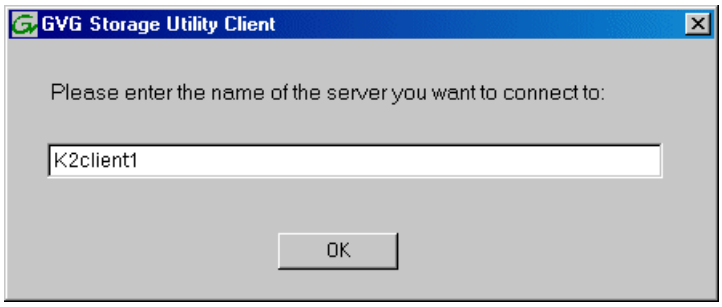
Opening Storage Utility Independently

Do not open Storage Utility independently unless there is a problem that prevents you from opening it through AppCenter.

1. Open the Storage Utility shortcut on the Windows desktop or from the Windows Start Menu at **Programs | Grass Valley | Storage Utility**.

   A dialog box opens in which you specify the machine to connect to with Storage Utility.

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

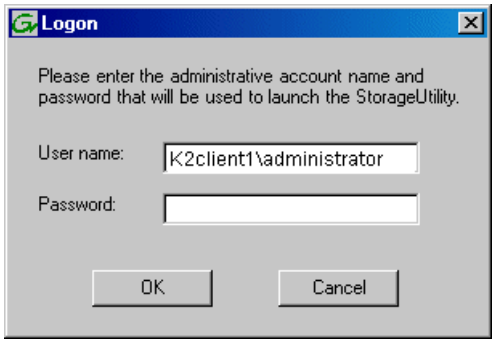


2. Enter the name or IP address of the K2 system for which you intend to use Storage Utility. If you are opening Storage Utility on a local K2 system, enter the name of that K2 system. Click **OK**.

   The Storage Utility logon dialog box opens.

3. Logon to Storage Utility. Make sure you log in with appropriate privileges. Administrator-level permission is necessary for most Storage Utility operations. For user name, you might need to enter the machine name as the domain to successfully log in.

   Storage Utility opens.

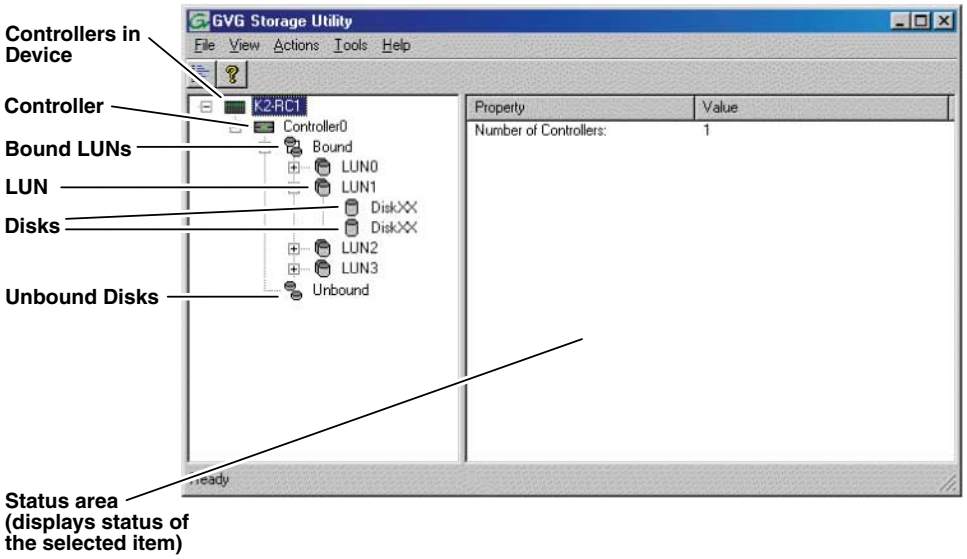


4. If you are connecting from a control point PC, you should verify that you are connected to the correct K2 system. To verify this, use the Identify feature to flash the disks.

Related Topics

About identifying disks on page 130

Overview of Storage Utility



The Storage Utility user interface includes a tree view in the left-hand pane, and a status information area displayed in the right-hand pane. The tree view displays the hardware that makes up the storage system connected. The context menus in the tree view are used to configure storage. The right-hand status pane displays information about the item selected in the tree view. The tree view hierarchy is as follows:

Controllers in Device — Provides a logical grouping of RAID Controllers by device.

Controller — Represents the RAID Controllers found. These are numbered in the order discovered. The controller icon represents both RAID Controller A and, if installed, RAID Controller B. To determine if an optional RAID Controller B is installed, select the Controller icon in the tree view, then examine the status pane for peer status.

Bound LUNs — Expanding the Bound node displays all bound LUNs.

LUN — Represents a bound LUN. Expanding the LUN node displays the disk modules that make up the LUN.

UnBound disks — Expanding the UnBound node, displays all unbound disk modules.

Disks — Represents the disk modules.

The Storage Utility detects disks available and lists them on the opening screen.

Refer to the following procedures to use Storage Utility for maintenance tasks

Checking storage subsystem status

Some limited status information for storage subsystems is displayed in the Storage Utility. This can be helpful when configuring storage.

You can view status information by selecting items in the tree view.

Item in tree view	Status information displayed
Controllers in Device	Number of Controllers
Controller	Microcode Version
Bound	Number of LUNs
LUN	Binding Type, such as RAID 1 State (online or offline)
Disk	Firmware Vendor State Product ID Capacity
Unbound	Number of disks

Checking controller microcode

As explained in the previous section, to check controller microcode, select the controller in the tree view and the microcode version is displayed.

About identifying disks

The Identify feature allows you to flash the disk LEDs so that you can physically locate a specific disk module or group of disk modules that make up a LUN. Always use the disk identify feature before removing and replacing a failed disk module. Accidentally removing the wrong disk module can destroy all data on the disk drives.

You can also use this feature to verify the K2 system to which you are currently connected.

Identifying internal disks

1. Open Storage Utility and in the tree view expand all nodes so that all disks are displayed.
2. On the K2 Summit system, remove the front bezel assembly. On the K2 Solo Media Server, disk LEDs are visible without removing the bezel.

   NOTE: Replace the bezel assembly within one minute to maintain system cooling.

3. The tables below illustrates the position of drives as numbered in the K2 Summit/Solo system chassis. Compare the drive number positions and the disk numbering displayed in Storage Utility to identify drive locations.

   K2 Summit 3G Production Client

Disk 0	Disk 1	Disk 2	Disk 3	Disk 4	Disk 5	Disk 6	Disk 7	Disk 8	Disk 9	Disk 10	Disk 11

   First generation K2 Summit Production Client

Disk 2		Disk 4		Disk 7
Disk 1		Disk 3		Disk 6
Disk 0				Disk 5

   K2 Solo Media Server

Disk 0
Disk 1

4. Position yourself so you can see the RAID drive LEDs.
5. Identify the disks in a LUN or identify a single disk, as follows:
   a) In the Storage Utility tree view, right-click a LUN or right-click a single disk, then select **Identify LUN** or **Identify Disk** in the context menu.

      A message box opens with a message that informs you that a disk or disks are blinking.

   b) View disks.

      The LEDs display an amber color flashing several times a second. This flashing pattern can stop automatically after a specific time interval, such as ten seconds.

   c) Verify the location of the disk or disks.

Get controller logs

1. In the tree view, select the controller.
2. Click **Actions | Get Controller Logs**.
3. A message informs you of the location of the logs.
4. Find the following files on the local K2 Summit/Solo system at *C:\logs*:

   tty.log

   ControllerEvents.log

Check disk mode pages

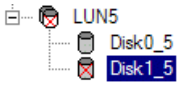
1. In the tree view, right-click the controller and select **Check DIsk Mode Pages**.
2. Messages report the results of the check. For each disk that has mode pages set incorrectly, click **Yes** when prompted "…restore the default mode page settings?".

Disabling a disk

1. In the tree view, right-click the disk and select **Advanced | Disable** and **OK** to confirm.

   A message "The drive is spinning down…Please wait" appears.

   If internal storage, the Service LED on the K2 system displays a flashing yellow pattern three time a second.
2. When the message "Operation succeeded…now safe to remove disk" appears, click **OK**.
3. The Storage Utility displays red Xs on tree view icons to represent a disk fault and a degraded LUN.



NOTE: On the K2 Media Client, remember that the LUN 0 (disks 0_0 and 0_1) is the system drive. Do not attempt disk operations on the system drive.

Forcing a disk to rebuild

With RAID 0 there is no RAID redundancy, so disks do not rebuild. With other RAID types, such as RAID 1, if media access (record/play) is underway, when you insert a media disk it automatically begins to rebuild. If there is no media access underway, to start the rebuild process either begin a media operation or use the following procedure:

1. In the tree view, identify the faulty disk . If the disk is not currently in the fault state, the Rebuild option is not available.
2. In the tree view, right-click the faulty disk and select **Rebuild**.
3. When the message "Succeeded to start rebuild…" appears, click **OK**.

   If internal storage, the Service LED on the K2 system displays a flashing pattern alternating yellow/green once a second.

Unbind LUN

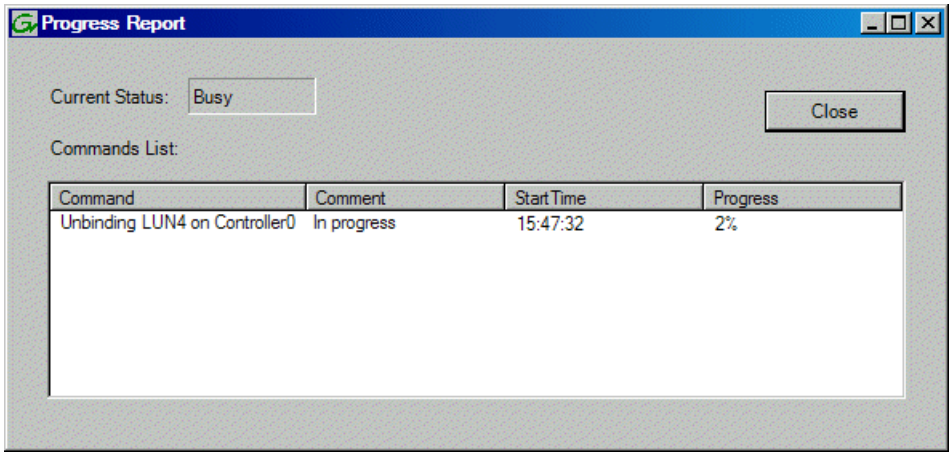
With internal storage, you can only unbind one LUN at a time. Also make sure the controller is not busy with other processes, such as rebuilding a disk. If the controller is busy, the unbind LUN operation fails.

⚠ ***CAUTION: Unbinding destroys all data stored on disk modules.***

Refer to topics about direct-connect external storage before using this procedure on direct-connect systems.

1. In the tree view, right-click the LUN and select **Unbind LUN**.
2. If online, messages appear "…offline mode now?" and "…continue?". Click **Yes** to put the system in offline mode.

   AppCenter channels go offline.
3. When warning messages appear "…destroy all existing media…" and "Are you sure?", click **OK** to continue.
4. The Progress Report opens and displays unbind progress.



5. When progress reports 100% complete, the LUN is unbound.
6. Restart the K2 system.

NOTE: On the K2 Media Client, remember that the LUN 0 (disks 0_0 and 0_1) is the system drive. Do not attempt disk operations on the system drive.

Related Topics

Direct Connect Storage on page 187

Bind Luns

When you bind a LUN, you select one or more unbound disks and create a new LUN. The Storage Utility places this new LUN at the bottom of the list and numbers it accordingly. However, with internal storage, disk numbers are enforced by the chassis slot in which the disk resides. Therefore, depending on the number and sequence of LUNs created, it is possible that the LUN numbers and the disk numbers do not match. When you create a new file system, this mismatched numbering does not hamper functionality. However, to make the internal storage K2 system easy to service, you should retain the correct numbering sequence. To do this you must unbind all media LUNs and then bind disks in sequence. On a K2 Media Client, do not unbind LUN0, which is the system drive.

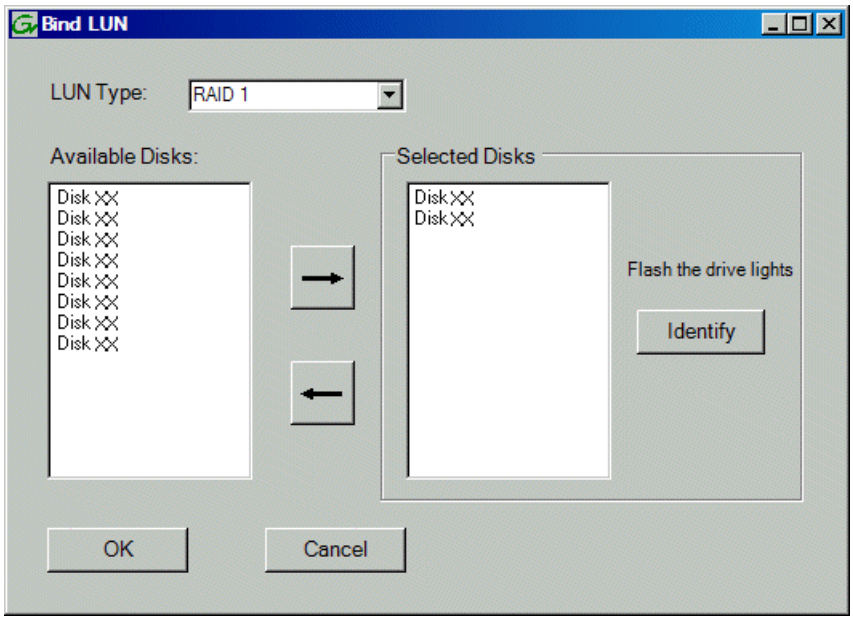
Refer to topics about direct-connect external storage before using this procedure on direct-connect systems.

1. In the tree view, right-click the **Unbound** node and select **Bind LUN**.

2. If online, messages appear "…offline mode now?" and "…continue?". Click **Yes** to put the system in offline mode.

   AppCenter channels go offline.

   The Bind LUN dialog box opens showing all unbound disks for the controller listed in the Available Disk list.



3. Make a selection in the LUN Type drop-down list and proceed as follows:

   - RAID 0 — For K2 Solo systems. Optional for internal storage first generation K2 Summit systems and K2 Summit 3G systems.

     In the Available Disks list, select one media disk, then click the arrow button to add it to the Selected Disks list. K2 Solo Media Server supports RAID 0 only.

   - RAID 1 — For internal storage first generation K2 Summit systems and K2 Summit 3G systems.

     In the Available Disks list, select two contiguous disks, then click the arrow button to add them to the Selected Disks list. (TIP: Use 'shift-click' or 'control-click' to select disks.)

   - RAID 5 — For direct-connect storage on K2 Summit systems.

     In the Available Disks list, select six contiguous disks, then click the arrow button to add them to the Selected Disks list. (TIP: Use 'shift-click' or 'control-click' to select disks.)

   NOTE: As an aid in identifying a disk module's physical location, select it in the Selected Disks list, then click Identify Disks. This causes the disk drive LED to flash.

4. Click OK to close the Bind LUN dialog box and begin the binding process.

   The Progress Report opens and displays binding progress.

5. Repeat the previous steps for remaining unbound disks. You do not need to wait until the first LUN is bound before you can start binding the next LUN. Multiple LUNs can be in the binding process all at the same time.

6. When progress reports 100% complete for all the LUNs that you are binding, proceed to the next step.
7. Restart the K2 system.
8. After binding one or more new LUNs, you must make a new file system.

Related Topics

Direct Connect Storage on page 187

Making a new media file system on a K2 Summit/Solo on page 136

Changing RAID type for internal storage

On an internal storage K2 Summit 3G system, you can change the internal media storage to be either RAID 1 or RAID 0, as follows:

- RAID 1 — Recommended for the "full" media drive option, which is eight drives on a first generation K2 Summit system. Not recommended for media drive options with fewer drives. With RAID 1, two media drives are configured as a mirrored pair to make one LUN. The capacity of each LUN is roughly equivalent to the capacity of one drive, so your total media storage capacity is approximately 50% of the sum total of all the drives. Since drives are mirrored in each LUN, your media is protected against drive failure. If a drive fails, the other drive in the LUN provides continued media access while you replace the failed drive.
- RAID 0 — Required on K2 Solo Media Server. With RAID 0 there is no mirroring, so your total media storage capacity is roughly equivalent to that of all drives combined. However, your media has no RAID protection against drive failure. If one media drive fails, the entire group of drives fails and you lose all your media.

Depending on your needs for capacity versus protection, you can change from one RAID type to another, as explained in the following procedure.

NOTE: This procedure loses all media.

1. If you need to retain media, transfer it to another K2 system or otherwise back it up.
2. Unbind all media LUNs.
3. Restart.
4. Bind media drives, as one of the following:
   - RAID 0 — Bind each media drive as a RAID 0 LUN.
   - RAID 1 — Bind the ten drives as five RAID 1 LUNs.
5. Restart.
6. Make a new file system.
7. If you backed up your media, you can now transfer it back.

Related Topics

Unbind LUN on page 132

Bind Luns on page 133

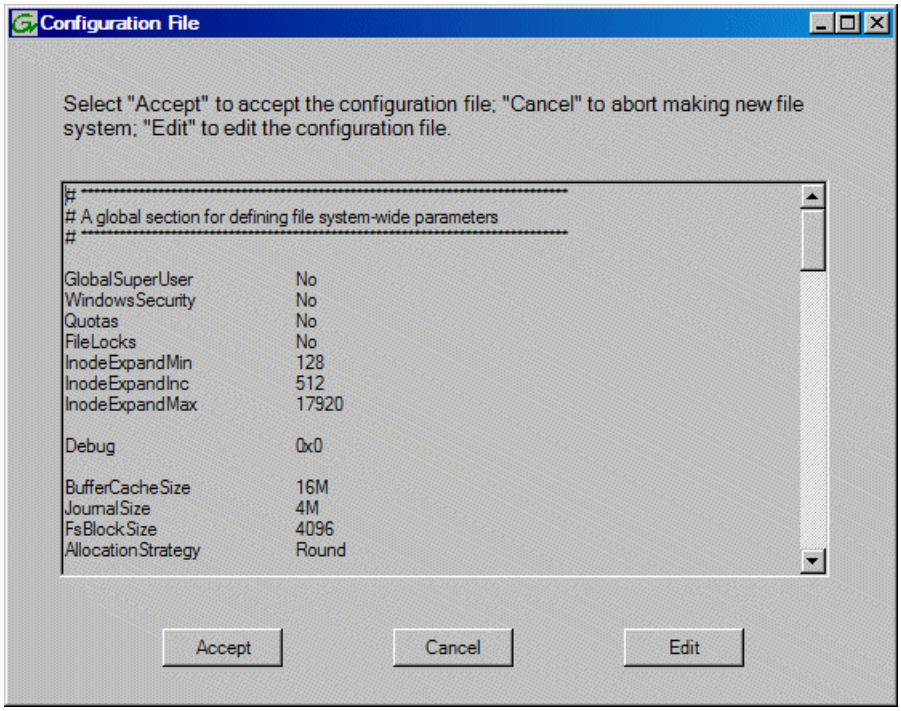
Making a new media file system on a K2 Summit/Solo on page 136

Making a new media file system on a K2 Summit/Solo

If your SNFS file system name is currently “default”, when you make a new file system the name changes to “gvfs_hostname”, where hostname is the name of the stand-alone K2 system. Also, Storage Utility creates unique disk labels, which is a requirement for compatibility with Dyno PA.

1. Click **Tools | Make New File System**.
2. If online, messages appear “…offline mode now?” and “…continue?”. Click **Yes** to put the system in offline mode.

   AppCenter channels go offline. The Configuration File window opens.



3. You can view media file system settings, but do not attempt to change them. Click **Accept**.

   A “Making new file system. Please wait” message box displays progress.
4. When a message “Succeeded to make the new file system. The server will be restarted now” appears, click **OK** to restart.
5. If you have Macintosh systems accessing the stand-alone K2 system, you should check that the SNFS file system volume is configured correctly on the Macintosh systems. Refer to K2 FCP Connect procedures in the K2 FCP Connect Installation Manual.

Checking the media file system

Prerequisites are as follows:

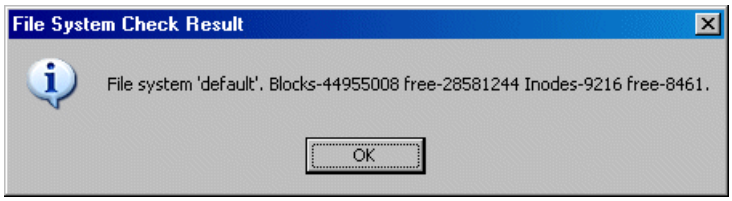
- Media operations must be stopped. You must put the standalone K2 System offline as part of this procedure.

This procedure checks the media file system but retains current media files.

1. In Storage Utility, click **Tools | Check File System**.
2. If online, messages appear "…offline mode now?" and "…continue?". Click **Yes** to put the system in offline mode.

   AppCenter channels go offline.
3. A message box appears "Checking media file system. Please wait". Observe progress.

   If problems are discovered they are reported. If the check process passes, when the process is complete a message appears to confirm success.



4. Click **OK** to dismiss the results.
5. Messages appear "…online mode now?" and "…continue?". Do one of the following:
   - Click **Yes** to put the system in online mode. This is the recommended option in most cases. For example, even if you plan to next clean unreferenced files and/or movies, that operation requires that the system be online, so you should put it online now. When you click Yes, AppCenter channels go online.
   - Click **No** to keep the system in offline mode. This is not recommended for most cases. Only do this when you are sure that subsequent operations require the system to be offlline.

Your file system has been checked.

Cleaning unreferenced files and movies

Prerequisites are as follows:

- The standalone K2 system must be online. If K2 AppCenter channels are in the offline state, the clean unreferenced files/movies operations fail.

These procedures allow you to keep the media database and the media files in sync. You can check the movies (clips) in the media database for the references to media files that should be currently

stored on the media disks. Likewise, you can check for media files that are not referenced by a movie in the media database. If you find any unreferenced files or movies, you can delete them.

Clean unreferenced files

1. In Storage Utility, click **Tools | Clean Unreferenced Files**.
2. A message box appears "…searching …Please wait". Observe progress.
3. A message box reports results. Respond as follows:
   - If no unreferenced files are found, click **OK** to dismiss the results.
   - If unreferenced files are discovered, you are prompted to delete them. Click **Yes** to delete the files or **No** to leave the files intact.

The process writes a log file to `C:\profile\logFS.txt`, which you can check for more information.

Clean unreferenced movies

1. In Storage Utility, click **Tools | Clean Unreferenced Movies**.
2. A message box appears "…searching …Please wait". Observe progress.
3. A message box reports results. Respond as follows:
   - If no unreferenced movies are found, click **OK** to dismiss the results.
   - If unreferenced movies are discovered, you are prompted to delete them. Click **Yes** to delete the movies or **No** to leave the movies intact.

The process writes log files to `C:\profile\cleanupDB.txt` and `C:\profile\MediaDB.txt`, which you can check for more information.

Downloading controller microcode

You might be instructed in K2 release notes to upgrade controller microcode. This allows you to take advantage of enhancements and benefit from improved performance and reliability.

To determine your current controller microcode version, select the controller in the Storage Utility tree view, then in the properties reported in the right-hand pane, note the controller microcode version. Use the following procedure if you need to download controller microcode.

1. Refer to *K2 Release Notes* to determine microcode types, versions, files, and any other special instructions regarding the particular controller microcode you are downloading.
2. In the Storage Utility, right-click the controller in the tree view, then select **Load Controller Microcode** in the context menu.
3. If online, messages appear "…offline mode now?" and "…continue?". Click **Yes** to put the system in offline mode.

   AppCenter channels go offline. The Open File dialog box opens.
4. In the Open File dialog box, browse to the desired microcode file, select the file.
5. Click **OK.**

   The Progress Report window appears showing the microcode download task and the percentage completion.
6. When finished, exit Storage Utility.

7. Put AppCenter channels back online.
8. Restart.

Downloading disk drive firmware

You might be instructed in K2 release notes to upgrade disk drive firmware. This allows you to take advantage of the disk drive enhancements and benefit from improved performance and reliability.

To determine your disk drive type and current firmware version, select a disk drive icon in the Storage Utility tree view, then note the drive properties reported in the right-hand pane. Use the following procedure if you need to download disk drive firmware.

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. Refer to *K2 Release Notes* to determine firmware types, versions, files, and any other special instructions regarding the particular disk drive firmware you are downloading.
2. In the Storage Utility, right-click a disk in the tree view, then select **Advanced | Download Disk Firmware** in the context menu.
3. If online, messages appear "…offline mode now?" and "…continue?". Click **Yes** to put the system in offline mode.

   AppCenter channels go offline. The Open File dialog box opens.
4. In the Open File dialog box, browse to the latest firmware file for your disks, select the file, and 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.
5. Repeat this procedure on each drive.
6. When finished, exit Storage Utility.
7. Put AppCenter channels back online.
8. Restart.

Placing the K2 system into online mode

If the stand-alone K2 system is in offline mode and you have completed your storage system configuration tasks, you have the following options to return the system to the online mode:

- Exit Storage Utility and bring channels online — If Storage Utility is closed, first open Storage Utility and then exit Storage Utility. When you exit Storage Utility you are prompted "…back to online mode?". Click **Yes**.

  After exiting Storage Utility, if AppCenter is open the channels remain offline. To bring channels online, if you are running AppCenter on a Control Point PC, select **System | Reconnect**. If you are running AppCenter on a local K2 system, close and reopen AppCenter.
- Restart the K2 system — Restarting automatically resets the system to online mode. When you log into AppCenter channels connect and come up online.

Chapter 6

Managing stand-alone K2 systems with SiteConfig

This section contains the following topics:

About managing stand-alone K2 clients with SiteConfig

The topics in this section apply to the following K2 client products:

- K2 Summit Production Client with internal storage
- K2 Summit Production Client with direct-connect storage

Work through the topics sequentially to get SiteConfig set up to remotely configure and manage one or more K2 clients. Then you can use SiteConfig for software upgrades and other management tasks.

SiteConfig and stand-alone K2 clients checklist

Use the following sequence of tasks as a guideline to set up SiteConfig and do your initial configuration for one or more stand-alone K2 clients. This checklist outlines the recommended workflow for a new system.

	Task	Comment
☐	Select a PC to use as the SiteConfig control point PC	Review system requirements and network access requirements about installing SiteConfig.
☐	Install SiteConfig on the control point PC	—
☐	Create a system description and add a custom site to the system description	If you already have a SiteConfig system description managing other devices in your facility, you can use that system description also for your stand-alone K2 clients, rather than creating a new system description.
☐	Add a control network to the site. You can also add a FTP/streaming network if desired	—
☐	Add a group for your K2 clients to the system description	—
☐	Add a placeholder K2 client to the system description for each of your actual K2 clients	—
☐	Configure the names of the placeholder K2 clients	—
☐	Configure the network interfaces of the placeholder K2 clients	Specify IP address ranges and other network details
☐	Discover your K2 clients	—
☐	Assign each discovered K2 client to its placeholder K2 client	—
☐	For each discovered and assigned K2 client, edit each network interface. Specify network settings and apply them to the K2 client.	On each K2 client, set the control network interface IP address first, then the FTP/streaming network interface, if present. Also set the hostname.

	Task	Comment
☐	Add a control point PC placeholder device to the system description	—
☐	Discover the control point PC and assign it to the placeholder control point PC	—
☐	If not already set correctly, set the hostname of discovered devices	Make sure the device name is correct, then make the hostname the same as the device name.
☐	Ping each K2 client and the control point PC to test network communication	—
☐	Generate host table information and distribute to hosts files on each K2 client and on the control point PC	Make sure you have completed network configuration of all network interfaces across all devices to ensure complete and valid host table information. You can use SiteConfig to copy hosts files to devices, or you can manage hosts files yourself.
☐	Create a deployment group	—
☐	Add stand-alone K2 clients to the deployment group	—

System requirements for SiteConfig host PC

The PC on which SiteConfig is installed must meet the following requirements:

Requirements	Comments
Operating system	Microsoft Windows (Must be a U.S. version): • XP Professional Service Pack 3 • Server 2003 • Vista Enterprise Service Pack 1 • Windows 7 • Server 2008 R2
RAM	Minimum 512 MB, 1 GB recommended
Graphics acceleration	Must have at least 128 MB memory
Processor	Pentium 4 or higher class, 2 GHz or greater
Hard disk space	400 MB
Microsoft .NET Framework	Version 4.0
Java JRE	1.3.1_12 and 1.4.2_05 or higher. Required for the HP Ethernet Switch configuration interface, which is used for K2 SANs.
XML	Microsoft XML 4 Service Pack 2 is required.

About installing SiteConfig

SiteConfig uses a protocol that involves sending Ethernet broadcast messages to discover and configure devices. To enable this protocol to work correctly, there must be unrestricted network access between the PC that hosts SiteConfig and the devices to be discovered.

This is achieved if control network interfaces are all connected to the same switch or to multiple switches interconnected with ISLs/trunks. If your site requires that other switches and/or routers be in the network path, you must make sure that no restrictions are in place that block SiteConfig protocols.

Also, do not install SiteConfig on a PC on which a drive from a managed device is mapped as an administrative share (C$). For example, if you have a PC set up to run anti-virus software and for this purpose you have network drives set up on the PC mapped to C$ shares on devices, then do not use that PC to host SiteConfig and manage those devices.

For a given system, there should be just one instance of SiteConfig managing the system.

Installing/upgrading SiteConfig

Prerequisites:

- The PC on which you are installing SiteConfg meets system requirements.
- The PC is connected to the LAN on which all the devices to be managed are connected.
- There are no routed paths to the devices to be managed.

1. Procure SiteConfig installation files from the Grass Valley website or via other distribution mechanisms.

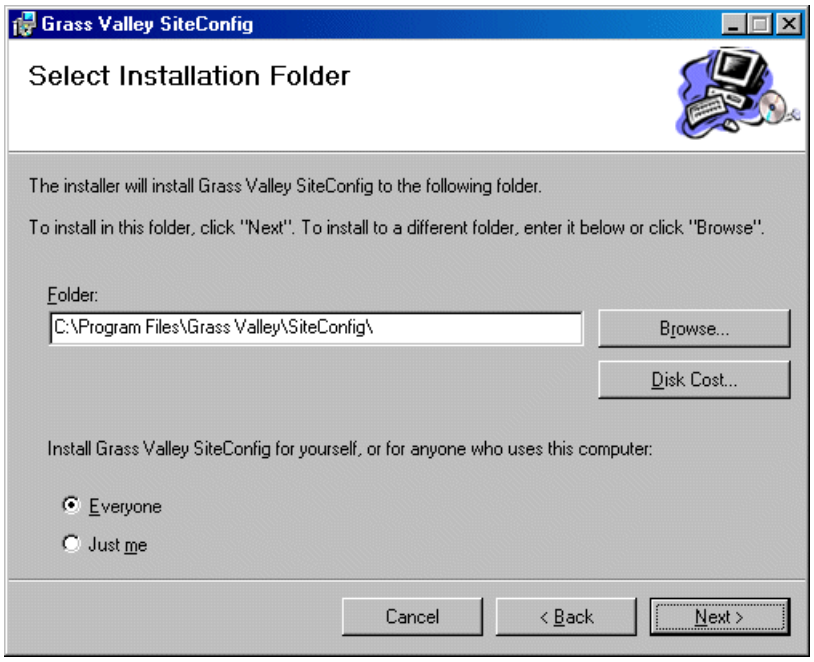
   The following directory and files are required to install SiteConfig:

   - *DotNetFx* directory
   - *ProductFrameUISetup.msi*
   - *setup.exe*

2. If you already have a version of SiteConfig installed, go to Windows **Add/Remove Programs** and uninstall it.
3. Double-click *setup.exe*.

   The installation wizard opens.

4. Work through the wizard pages, clicking **Next** and **Finish**.



   If the PC does not have the appropriate version of Microsoft .NET, the SiteConfig installation programs installs it.

5. Open the Windows operating system Services control panel on the PC and look for an entry called " ProductFrame Discovery Agent".

   The Discovery Agent must be installed on the SiteConfig PC so that the PC can be discovered by SiteConfig and added to the system description as a managed device. This is necessary to ensure name resolution in SiteConfig's hosts file.

   The Discovery Agent is also known as the Network Configuration Connect Kit. For example, in Windows Add/Remove Programs, it can be displayed as either Network Configuration Connect Kit or SiteConfig Discovery Agent.

6. Proceed as follows:

   - If the Discovery Agent is not installed, navigate to the SiteConfig install location's Discovery Agent Setup subdirectory and double-click the `DiscoveryAgentServiceSetup.msi` file. This launches the setup program and installs the Discovery Agent. Follow the setup wizard to complete installation. A restart is required after installation. Then continue with the next step in this procedure.
   - If the Discovery Agent is already installed, continue with the next step in this procedure.

7. If not already configured, configure the SiteConfig PC with a valid Ethernet IP address for the LAN using Windows Network Connections.
8. If you are not going to be using SiteConfig to manage system hosts files, put the system hosts file on the SiteConfig PC.

Creating a system description for stand-alone K2 clients

Do not do this task if:

- You already have or are developing a SiteConfig system description managing other devices in your facility and that system description has the correct networks and connectivity for your stand-alone K2 clients. In this case, skip ahead to the task in which you add a group to the system description for your stand-alone K2 clients.

Do this task if:

- You do not yet have a system description appropriate for managing your stand-alone K2 clients.

1. Open SiteConfig and proceed as follows:
   - If a dialog box opens that gives you the choice of creating or importing a system description, it means SiteConfig does not have access to a system description file. Click **Create**.
   - If the SiteConfig main window opens, click **File | New**.

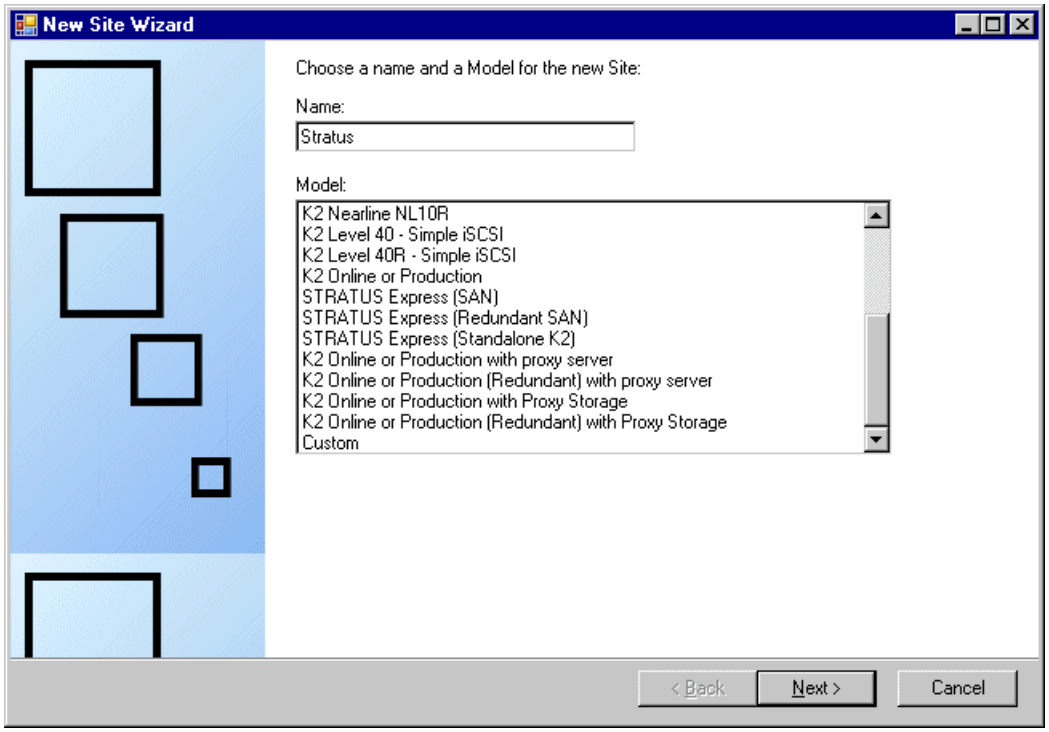
   The Create New System Description dialog box opens.
2. In the Create New System Description dialog box, enter the name of the file for the system description you are creating.

   It is recommended that you store the system description file in the default location, rather than browsing to store the file in a different location. SiteConfig always accesses the default location.
3. Click **OK**.

   A blank system description loads, which displays just the top-level System node in the tree view.

4. In the **Network Configuration | Devices** tree view, right-click the **System** node or a **Site** node and select **Add Site**.

   The New Site Wizard opens.



5. Enter a name for the site you are creating, considering the following:
   - Keep the site name short, as it becomes the root identifier that is the default prefix for device and network names.
   - Sites in the tree view are automatically sorted alphabetically.
6. Select **Custom** and click **Next**.
7. Click **Finish** to create the site.

The site is displayed in SiteConfig in the tree view with groups and device placeholders displayed under the site node. New networks are displayed in the tree view of networks in the Networks tab.

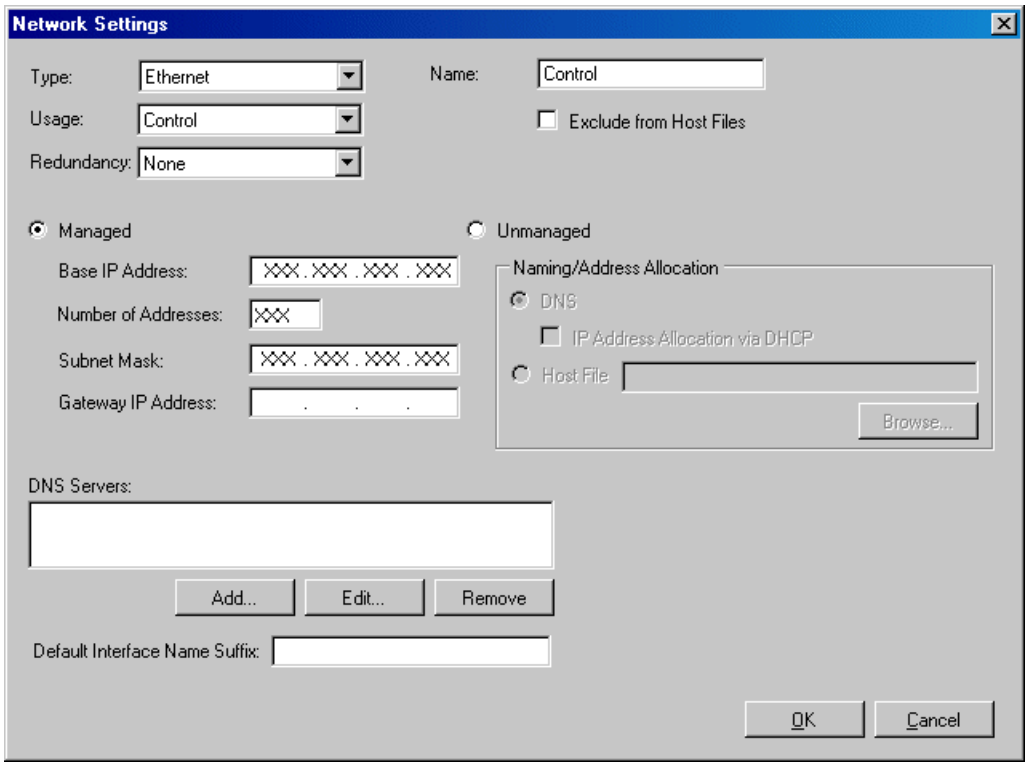
Creating the control network for stand-alone K2 clients

1. In the **Network Configuration | Networks** tree view, select a System node or a Site node.

2. Proceed as follows:

   - To add a network under the currently selected node, in the tree view right-click the node and select **Add Network**.

   The Network Settings dialog box opens.



3. Configure the settings for the network as follows:

Setting...	For control network
Type	*Ethernet* is required
Usage	*Control* is required
Redundancy	*None* is required. This is true even on a redundant K2 SAN. (Only the iSCSI network is redundant on a redundant K2 SAN.)
Name	*Control* is recommended
Exclude from Host Files	*Unselected* is required
Managed	*Selected* is required
Base IP Address	The first (lowest) IP address in the range of IP addresses managed by SiteConfig. Required.
Number of Addresses	The number of IP addresses in the range managed by SiteConfig. Required.
Subnet Mask	The network's subnet mask. Required.
Gateway IP Address	Additional network settings managed by SiteConfig. Allowed.
Unmanaged	*Unselected* is required. Related settings are disabled.
DNS Servers	Servers providing DNS for name resolution. Allowed.
Default Interface Name Suffix	Not allowed

4. Click **OK** to save settings and close.

Creating the FTP/streaming network for stand-alone K2 clients (optional)

If you transfer media to/from the stand-alone K2 client, create a FTP/streaming network.

1. In the **Network Configuration | Networks** tree view, select a System node or a Site node.
2. Proceed as follows:
   - To add a network under the currently selected node, in the tree view right-click the node and select **Add Network**.

   The Network Settings dialog box opens.

3. Configure the settings for the network as follows:

Setting...	For FTP/streaming network
Type	*Ethernet* is required
Usage	*FileTransfer* is required
Redundancy	*None* is required. This is true even on a redundant K2 SAN. (Only the iSCSI network is redundant on a redundant K2 SAN.)
Name	*Streaming* is recommended
Exclude from Host Files	*Unselected* is required
Managed	*Selected* is required
Base IP Address	The first (lowest) IP address in the range of IP addresses managed by SiteConfig. Required.
Number of Addresses	The number of IP addresses in the range managed by SiteConfig. Required.
Subnet Mask	The network's subnet mask. Required.
Gateway IP Address	Additional network settings managed by SiteConfig. Allowed.
Unmanaged	*Unselected* is required. Related settings are disabled.
DNS Servers	Servers providing DNS for name resolution. Allowed.
Default Interface Name Suffix	*_he0* is required

4. Click **OK** to save settings and close.

Adding a group

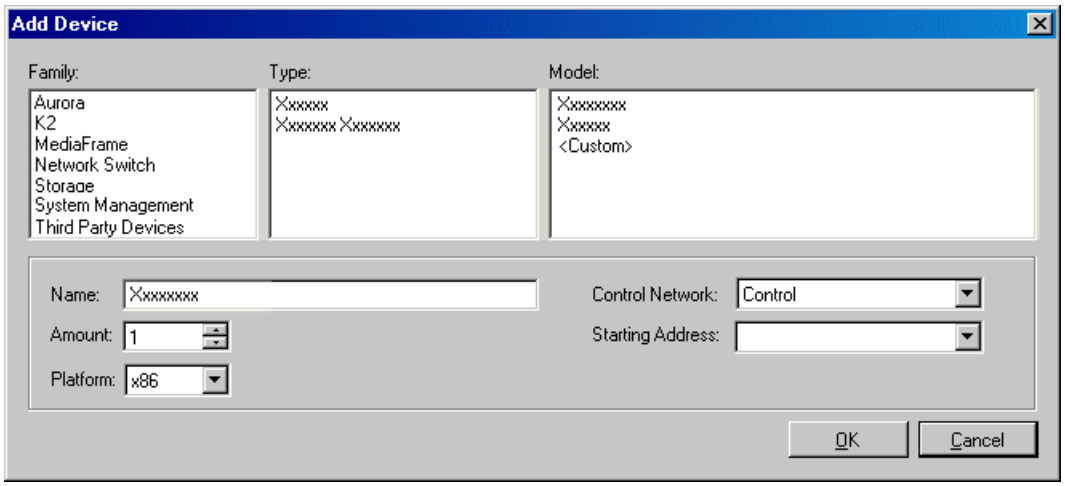
1. In the **Network Configuration | Networks** tree view, right-click a site node and select **Add Group**. The group appears in the tree view.
2. Right-click the group and select **Rename**.
3. Enter the desired name for the group.

Adding stand-alone K2 clients to the system description

Prerequisites for this task are as follows:

- The system description contains a group.

1. In the **Network Configuration | Devices** tree view, right-click a group and select **Add Device**.



2. Configure settings for the device you are adding as follows:
   - Family – Select **K2**.
   - Type – Select the appropriate type of K2 system.
   - Model – Select the model with the appropriate storage.
   - Name – This is the device name, as displayed in the SiteConfig device tree view and device list view. This name can be different than the host name (network name). You can accept the default name or enter a name of your choice. Devices in the tree view are sorted alphabetically.
   - Amount – You can add multiple devices, as currently defined by your settings in the Add Device dialog box. An enumerator is added to the name to create a unique name for each device added.
   - Control network– Select the control network.
   - Starting Address – Select from the list of available addresses on the selected control network. If adding multiple devices, this is the starting address, with addresses assigned sequentially to each device added.
3. Click **OK** to save settings and close.
4. Repeat these steps for each of your stand-alone K2 clients.

Modifying stand-alone K2 client unassigned (unmanaged) interfaces

Prerequisites for this task are as follows:

- The system description has a stand-alone K2 client that is a placeholder device.

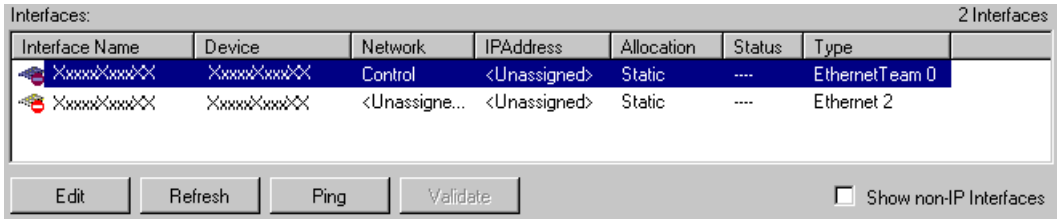
- The placeholder device has a one or more unmanaged network interfaces.

Use this task to modify unmanaged network interfaces on a standalone K2 client as follows:

- K2 Summit Production Client©

1. In the **Network Configuration | Devices** tree view, select a stand-alone K2 client placeholder device.

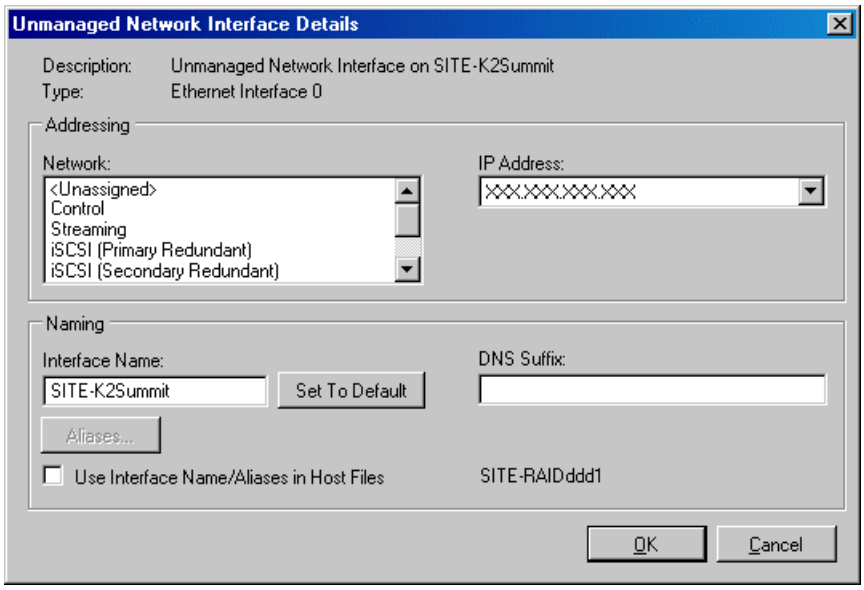
   The interfaces for that device are displayed in the interfaces list view.



   Edit the control network interface first.

2. In the interfaces list view, right-click an interface and select **Edit**.

   The Unmanaged Network Interface Details dialog box opens.



3. Configure the settings for the interface as follows:

Setting...	For control network interface
Network	*Control* is required
IP Address	The IP address for this interface on the network. Required.
Interface Name	The device host name. Required.
Set to Default	Not recommended. Sets the interface name to SiteConfig default convention, based on the root Site name and device-type.
...use Interface Name/Aliases in Host Files...	*Unselected* is required. Since not selected, the default behavior occurs, which is to use the device host name in the hosts file.
Aliases	Not allowed
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.

4. Click **OK** to save settings and close.
5. If you have a FTP/streaming network, repeat these steps but select the stand-alone K2 client's other network interface and configure settings as follows.

Setting...	For FTP/streaming network interface
Network	*Streaming* is required
IP Address	The IP address for this interface on the network. Required.
Interface Name	The device host name with the " _he0" suffix added is required. For example, if the host name is *K2prod01*, then *K2prod01_he0* is required here.
Set to Default	Not recommended. Sets the interface name to SiteConfig default convention, based on the root Site name and device-type.
...use Interface Name/Aliases in Host Files...	*Selected* is required
Aliases	Not allowed
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.

6. Click **OK** to save settings and close.
7. Repeat this procedure for each of your stand-alone K2 client placeholder devices.

Discovering devices with SiteConfig

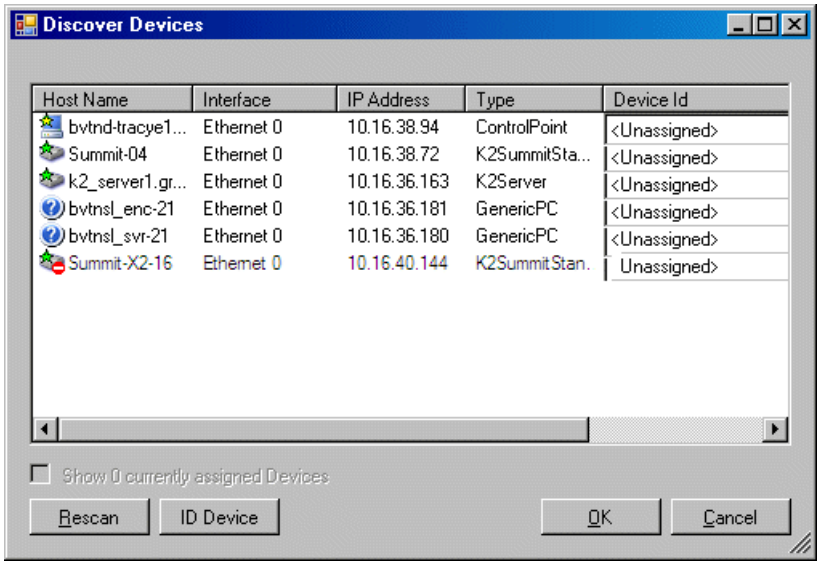
Prerequisites for this task are as follows:

- The Ethernet switch or switches that support the control network are configured and operational. If multiple switches, ISLs are connected and trunks configured.

- The PC that hosts SiteConfig is communicating on the control network.
- There are no routers between the PC that hosts SiteConfig and the devices to be discovered.
- Devices to be discovered are Windows operating system devices, with SiteConfig support installed.
- Devices are cabled for control network connections.
- If discovering a device with Microsoft Windows Server 2008 operating system, the device must have an IP address, either static or DHCP supplied.

1. Open SiteConfig.
2. In the toolbar, click the discover devices button. 

   The Discover Devices dialog box opens.



   A list of discovered devices is displayed.

3. Click **Rescan** to re-run the discovery mechanism. You can do this if a device that you want to discover has its network connection restored or otherwise becomes available. Additional devices discovered are added to the list.

Assigning discovered devices

Prerequisites for this task are as follows:

- Devices have been discovered by SiteConfig
- Discovered devices are not yet assigned to a device in the system description
- The system description has placeholder devices to which to assign the discovered devices.

1. If the Discovered Devices Dialog box is not already open, click the discover devices button  .

   The Discover Devices dialog box opens.

2. Identify discovered devices.
   - If a single device is discovered in multiple rows, it means the device has multiple network interfaces. Choose the interface that represents the device's currently connected control connection. This is typically Ethernet ... 0.
   - If necessary, select a device in the list and click **ID Device**. This triggers an action on the device, such as flashing an LED or ejecting a CD drive, to identify the device.
3. To also view previously discovered devices that have already been assigned to a device in the system description, select **Show … currently assigned devices**.

   The currently assigned devices are added to the list. Viewing both assigned and unassigned devices in this way can be helpful to verify the match between discovered devices and placeholder devices.
4. In the row for each discovered device, view items on the Device Id drop-down list to determine the match with placeholder devices, as follows:
   - If SiteConfig finds a match between the device-type discovered and the device-type of one or more placeholder devices, it displays those placeholder devices in the list.
   - If SiteConfig does not find a match between the device-type discovered and the device-type of a placeholder device, no placeholder device is displayed in the list.
5. In the row for a discovered device, click the Device Id drop-down list and select the placeholder device that corresponds to the discovered device.

   If there is no corresponding placeholder device currently in the system description, you can select **Add** to create a new placeholder device and then assign the discovered device to it.
6. When discovered devices have been assigned, click **OK** to save settings and close.
7. In the **Network Configuration | Devices** tree view, select each of the devices to which you assigned a discovered device.

Modifying stand-alone K2 client managed network interfaces

Prerequisites for this task are as follows:

- The physical device you are configuring has been discovered and is assigned to a device in the SiteConfig system description.
- SiteConfig has communication with the device.
- The device is defined in the system description with an appropriate network interface.

Use this task to modify managed network interfaces on stand-alone K2 client models as follows:

- K2 Summit Production Client

1. In the tree view select a K2 client, then in the Interfaces list view, identify interfaces as follows:
   - For a stand-alone K2 Summit Production Client, the control network interface is a team. Modify the control team interface first. The control team is comprised of two individual interfaces, one for Control Connection #1 and one for Control Connection # 2. If these individual interfaces are displayed, do not modify them.
   - A stand-alone K2 client's other interface is for FTP/streaming. If you have a FTP/streaming network, you can configure and use this interface if desired.

2. In the Interfaces list view determine the interface to configure, as follows:
   - Identify the interface with which SiteConfig is currently communicating, indicated by the green star overlay icon. This should be the control network interface.
   - Verify that the interface over which SiteConfig is currently communicating is in fact the interface defined for the control network in the system description. If this is not the case, you might have the control network cable connected to the wrong interface port. The control connection should always be the first port on the motherboard, except when you have a loopback connection.
   - Configure the control network interface first before configuring any of the other interfaces.
   - After you have successfully configured the control network interface, return to this step to configure each remaining interface.

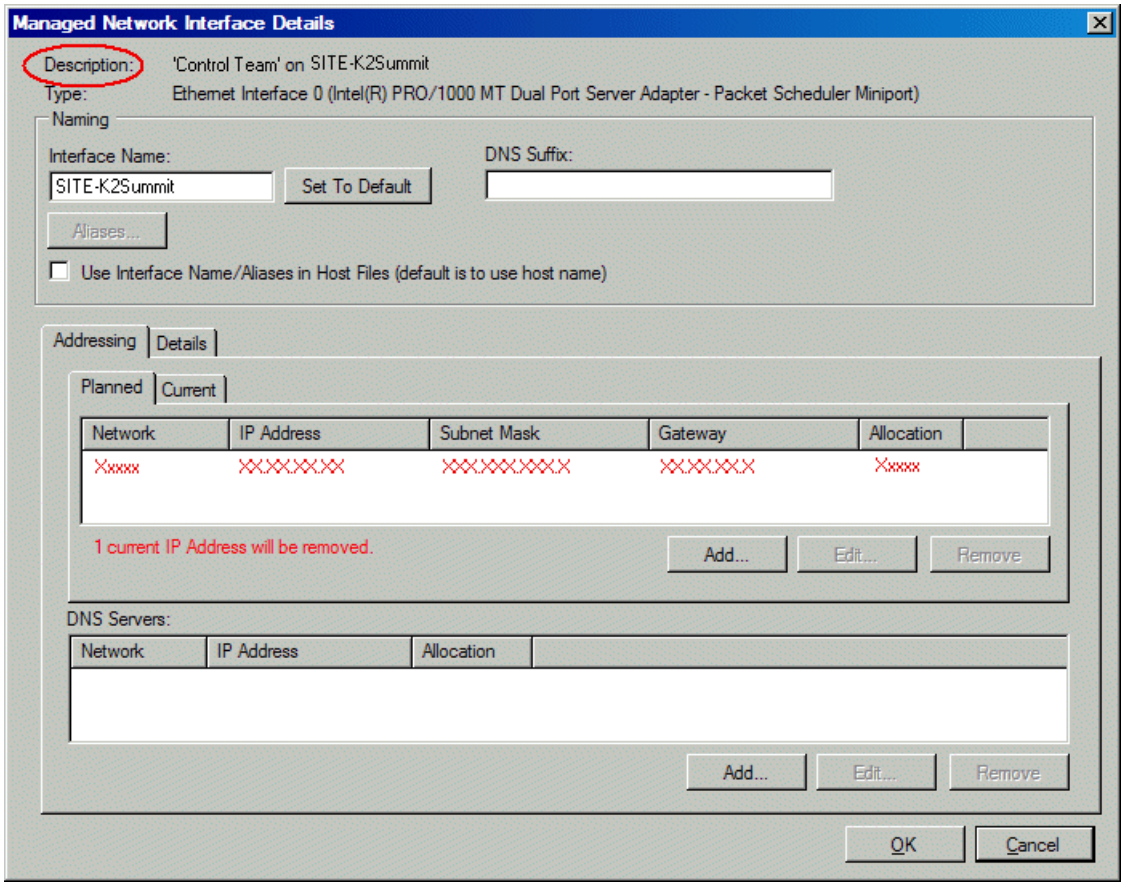
3. In the Interfaces list view, check the icon for the interface you are configuring.

   If the icon has a red stop sign overlay, it indicates that current settings and planned settings do not match or that there is some other problem. Hover over the icon to read a tooltip with information about the problem.

   NOTE: Make sure that the device is unlocked in SiteConfig before proceeding. For a K2 Summit Production Client with K2 software at a version lower than 9.0, this disables the write filter.

4. In the Interfaces list view, right-click the interface you are configuring and select **Edit**.

   The Managed Network Interface Details dialog box opens.



5. Identify the interface on the discovered device that you are configuring.

   - Identify Ethernet LAN adapters by their "Description" name. This is the Windows connection name. SiteConfig reads this name from the device and displays it at the top of this dialog box. This is the most accurate way to identify the network adapter on the discovered device that you are configuring.
   - For a K2 Summit Production Client, when you configure its first interface, make sure you are configuring the 'Control Team' interface.

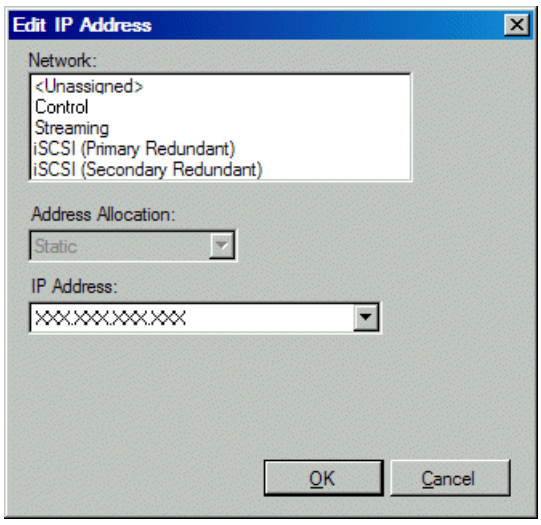
6. Configure naming settings as follows:

Setting...	For network interface Control Team
Interface Name	The device host name. Required.
Set To Default	Not recommended
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.
Aliases	Not allowed
Use Interface Name/Aliases in Host Files	*Unselected* is required. Since not selected, the default behavior occurs, which is to use the device host name in the hosts file.

7. Evaluate settings on the Planned tab and change if necessary.
   - Compare settings on the Planned tab with settings on the Current tab.
   - If you want to keep the current settings as reported in the Current tab, click **Remove** to remove the planned settings.
   - Do not specify multiple IP addresses for the same interface. Do not use the Add button.
   - Refer to SiteConfig Help Topics for information about planned and current IP configuration.

8. To modify planned settings, do the following:
   a) Select the network settings and click **Edit**.

      The Edit IP Address dialog box opens.



   b) Edit IP address settings as follows:

Setting...	For network interface Control Team
Network	*Control* is required
Address Allocation	*Static* is recommended.
IP Address	The IP address for this interface on the network. Required.

      The networks listed in the Edit IP Address dialog box are those currently defined in the system description, with available settings restricted according to the network definition. If you require settings that are not available, you can close dialog boxes and go to the **Network Configuration | Networks** tab to modify network settings, then return to the Edit IP Address dialog box to continue.

9. When you have verified that the planned settings are correct, click **OK**, then **Yes** to apply settings to the device and close.

   A Contacting Device message box reports progress.

10. After configuring control network settings, do the following
    a) If a message informs you of a possible loss of communication, click **OK**.

       This message is normal, since this is the network over which you are currently communicating.

    b) In the Device list view, observe the device icon and wait until the icon displays the green star overlay before proceeding.

       The icon might not display the green star overlay for several seconds as settings are reconfigured and communication is re-established.

    c) In the Interface list view, right-click the interface and select **Ping**.

       The Ping Host dialog box opens.

       If ping status reports success, the interface is communicating on the control network.

11. If you have a FTP/streaming network, repeat steps but select the stand-alone K2 client's other network interface. Open the Managed Network Interface Details dialog box and configure the interface for the FTP/streaming network.
12. Identify the interface on the discovered device that you are configuring.
    - On any stand-alone K2 client, for the FTP/streaming network, configure Media Connection #1.

13. Configure naming settings as follows:

Setting...	For network interface Media Connection #1
Interface Name	The device host name with the "_he0" suffix added is required.
Set To Default	Not recommended
DNS Suffix	Allowed, if applicable to the network. The DNS suffix is added to the interface name.
Aliases	Not allowed
Use Interface Name/Aliases in Host Files	*Selected* is required

14. As in steps earlier in this procedure, reconcile planned and current settings. If you must edit the IP address, make settings as follows:

Setting...	For network interface Media Connection#1
Network	*Streaming* is required
Address Allocation	*Static* is required.
IP Address	The IP address for this interface on the network. Required.

15. When you have verified that the planned settings are correct, click **OK**, then **Yes** to apply settings to the device and close.

    A Contacting Device message box reports progress.

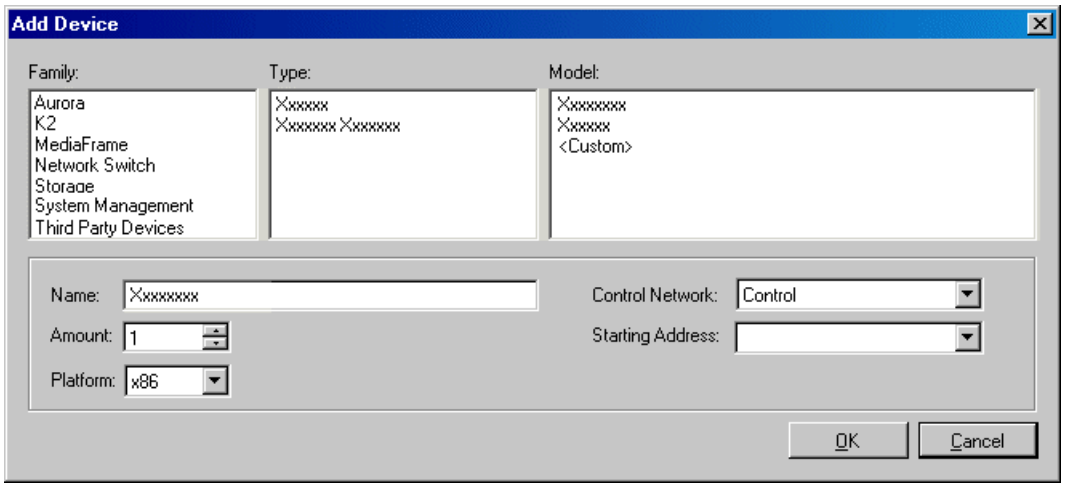
    NOTE: For a K2 Summit Production Client with K2 software at a version lower than 9.0, when configuration is complete, make sure you lock the device in SiteConfig. This enables the write filter.

Adding a control point PC placeholder device to the system description

Prerequisites for this task are as follows:

- The system description contains a group.

1. In the **Network Configuration | Devices** tree view, right-click a group and select **Add Device**.



   The Add Device dialog box opens.

2. Configure settings for the device you are adding as follows:
   - Family – Select **System Management**.
   - Type – Select **ControlPoint PC**.
   - Model – Select **Control Point PC**.
   - Name - This is the device name, as displayed in the SiteConfig device tree view and device list view. You must configure this name to be the same as the host name on the actual control point PC.
   - Amount – Leave this setting at **1**. Do not attempt to configure multiple control point PC simultaneously.
   - Control Network – Select the control network.
   - Starting Address – Select the IP address that is the address currently configured on the actual control point PC.

3. Click **OK** to save settings and close.

Verify that IP settings for the placeholder device's control network interface are identical to those on the actual control point PC before using SiteConfig to discover the control point PC on the control network.

Assigning the control point PC

Prerequisites for this task are as follows:

- The SiteConfig control point PC has the SiteConfig Discovery Agent installed. The Discovery Agent is also known as the Network Configuration Connect Kit. In Windows Add/Remove Programs, it can be displayed as either Network Configuration Connect Kit or SiteConfig Discovery Agent.
- The system description contains a control point PC placeholder device.
- The placeholder's control network interface is configured with the control network IP address that is currently on the actual control point PC.
- The device name of the control point PC placeholder is same as the host name of the actual control point PC.

In this procedure you discover the physical control point PC and assign it to the placeholder control point PC in the system description.

1. Open SiteConfig on the control point PC.
2. Discover devices and identify the control point PC discovered device.
3. Assign the discovered device to the control point PC placeholder.
4. In the **Network Configuration | Devices** tree view, select the control point PC.
5. In the Interfaces list view, right-click the control network interface and select **Edit**.

   The Managed Network Interface Details dialog box opens.
6. Evaluate IP settings as follows:

   - If only Current settings are displayed (the Planned tab is not displayed), it means the planned settings you configured on the placeholder device are identical to those on the actual control point PC If this is the case, no further configuration is required.
   - If both a Current tab and a Planned tab are displayed, it means the planned settings you configured on the placeholder device are not identical to those on the actual control point PC. If this is the case, do not apply planned settings. Doing so overwrites IP settings on the actual control point PC, which stops network communication. Instead, select the **Planned** tab and click **Remove**.

   NOTE: Do not click OK if planned settings (red text) are displayed.
7. When you are sure that only Current settings are displayed and that those are the current valid settings for the control point PC, click **Apply**, then **OK** to save settings and close.

Making the host name the same as the device name

1. Verify that the current device name, as displayed in the SiteConfig tree view, is the same as your desired host name.
2. In the **Network Configuration | Devices | Device** list view, right-click the device and select **Edit**.

   The Edit Device dialog box opens.

3. Identify the state of buttons as follows:
   - If the host name is different than the device name, the **Set to Device Name** button is enabled.
   - If the host name is the same as the device name, the **Set to Device Name** button is disabled.
4. If enabled, click **Set to Device Name**.
   This changes the host name to be the same as the device name.
5. Click **OK**.
6. When prompted, restart the device.

Pinging devices from the PC that hosts SiteConfig

Prerequisites:

- The devices you are pinging are in the SiteConfig system description.

You can send the ping command to one or more devices in the system description over the network to which the SiteConfig host PC is connected. Typically this is the control network.

1. In the **Network Configuration** | **Networks** tree view, select a network, site, or system node.
2. In the Devices list view, select one or more devices. Use Ctrl + Click or Shift + Click to select multiple devices.
3. Right-click the selected device or devices and select **Ping**.
   The Ping Devices dialog box opens and lists the selected device or devices.

The Ping Devices dialog box reports the progress and results of the ping command per device.

About hosts files and SiteConfig

SiteConfig uses the network information in the system description to define a hosts file and allows you to view the hosts file. SiteConfig can manage this hosts file on Windows operating system devices that are in the system description and that are part of a SiteConfig managed network.

When you have successfully assigned devices and applied planned network settings to interfaces, it is an indication that host table information, as currently captured in the system description, is valid and that you are ready to have SiteConfig assemble the host table information into a hosts file. Your options for placing this host table information on devices are as follows:

- If you do not want SiteConfig to manage your host table information, you can manage it yourself. This is typically the case if your facility has an existing hosts file that contains host table information for devices that are not in the SiteConfig system description. In this case, you can have SiteConfig generate a single hosts file that contains the host table information for the devices in the system description. You can then copy the desired host table information out of the SiteConfig hosts file and copy it into your facility hosts file. You must then distribute your facility hosts file to devices using your own mechanisms.
- If you want SiteConfig to manage all information in hosts files on devices, you can have SiteConfig copy its hosts file to devices. In so doing, SiteConfig overwrites the existing hosts files on devices. Therefore, this requires that all devices that have name resolution through the hosts file be configured accordingly in the SiteConfig system description.

If you choose to have SiteConfig write hosts files to devices, the process consumes system resource and network bandwidth. Therefore you should wait until you have verified the information for all devices/interfaces in the host file, rather than updating hosts files incrementally as you discover/assign devices.

SiteConfig does not automatically deploy hosts files to managed devices as you add or remove devices. If you add or remove devices from the system description, you must re-deploy the modified hosts file to all devices.

Generating host tables using SiteConfig

Prerequisites for this task are as follows:

- Planned control network settings are applied to control network interfaces and devices are communicating on the control network as defined in the system description.
- Interfaces for networks that require name resolution via the hosts file, such as the FTP/streaming network, have settings applied and are communicating.
- You have viewed host names, as currently defined in the system description, and determined that they are correct.
- The SiteConfig PC is added to the system description so that it is included in the host tables generated by SiteConfig.

When you add or modify devices or their IP addresses in the SiteConfig system description, you should update host tables on all devices that use them.

1. In the **Network Configuration | Networks** tree view, select a network, site, or system node.
2. Click **View Hosts file**.

   A Hosts File Contents window opens that displays the contents of the hosts file as currently defined in the system description.
3. Verify the information in the hosts file.

4. Do one of the following:
   - If you are managing host table information yourself, click **Save As** and save a copy of the hosts file to a location on the control point PC. Then open the copy of the hosts file, copy the desired host table information from it, and paste it into your facility hosts file as desired. Then you can use your own process to distribute the facility hosts file to devices. Remember to distribute to the control point PC so that SiteConfig and other management applications such as K2Config can resolve network host names.
   - If SiteConfig is managing hosts files, do the following:

   NOTE: Writing hosts files to multiple devices consumes system resource and network bandwidth. Therefore it is recommended that you wait and do this after the system is complete and fully implemented, rather than updating hosts files incrementally as you discover/assign devices.

   a) In the **Network Configuration | Devices | Devices** list view, right-click a device to which you intend to write the hosts file and select **View Current Host File**.

      A Host File Contents window opens that displays the contents of the hosts file that is currently on that actual device.

   b) Verify that there is no information that you want to retain in the device's current hosts file that is not also in the hosts file as currently defined in the system description. If you need to save the device's current hosts file, click **Save As** and save to a different location.

   c) In the **Network Configuration | Devices | Devices** list view, right-click a device or use Ctrl + Click to select multiple devices, and select **Update Host File**.

      The current hosts file is overwritten with the hosts file as defined in the system description.

Configuring deployment groups

Prerequisites for this procedure are as follows:

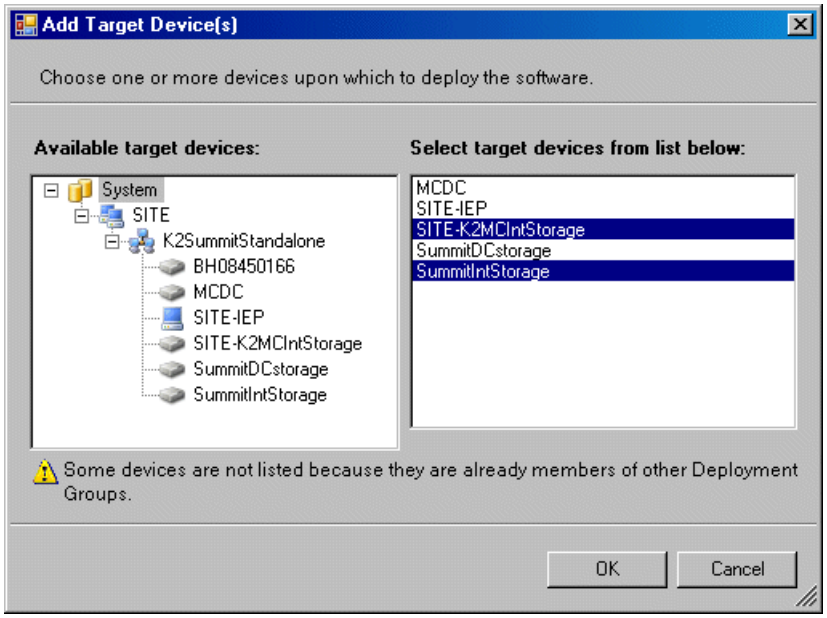
- The device is assigned in the SiteConfig system description and network connectivity is present.

1. In the **Software Deployment | Deployment Groups** tree view, right-click the top node and select **Add Deployment Group**.

   A deployment group appears in the tree view.

2. Right-click the deployment group, select **Rename**, and enter a name for the deployment group.

3. Right-click the deployment group and select **Add Target Device**.
   The Add Target Device(s) wizard opens.



4. In the Available Target Devices tree view, select the node that displays the devices that you are combining as a deployment group.
5. In the right-hand pane, select the devices that you are combining as a deployment group.
   To select multiple devices, you can drag through the devices, use Ctrl + Click, or use Shift + Click.
6. Click **OK**.

The devices appear in the Deployment Groups tree view under the deployment group. Before you perform a software deployment, you must check software on the devices that will be receiving new software. If you have already added packages to the group, on the Deployment Groups tab you will also see deployment tasks generated for every device with roles that match the package contents.

About deploying software for stand-alone K2 clients

You must control the sequence of software deployment tasks and device restarts as you upgrade software. The exact steps can vary from software version to version. Make sure you follow the documented task flow in the release notes for the version of software to which you are upgrading.

Chapter 7

Managing K2 system software

This section contains the following topics:

About K2 system software

Check *K2 Release Notes* for the latest information about software.

K2 system software components are as follows:

- K2 Client: Installed on K2 Summit/Solo system. Provides core functionality for all K2 Summit/Solo system models.
- K2 Server: Installed on K2 Media Servers. Provides core functionality for all K2 Media Servers in all roles.
- Control Point: Installed on Control Point PCs. Provides remote control and configuration of K2 Summit/Solo systems (both internal and external storage) as well as the K2 SAN.
- Media File System (SNFS): Installed on K2 Media Servers, stand-alone K2 Summit/Solo systems, and shared storage (SAN) K2 Summit/Solo system. Provides a dedicated file system for access to media data. Install only as instructed by release notes.

In addition, the following software is installed in special cases:

- Multi-Path I/O software — You must install this software on K2 Summit systems that are part of a redundant K2 SAN and on K2 Summit systems with direct-connect storage.

On a K2 SAN system, Grass Valley requires that you use SiteConfig to install K2 system software. On a standalone K2 Summit/Solo system Grass Valley recommends SiteConfig but allows manual installation as well. You can access software on your K2 Summit/Solo system's USB Recovery Flash Drive and via download from the Grass Valley website. On the USB Recovery Flash Drive, find SiteConfig `*.cab` files in the `ProductFrame` directory and find manual installation files in the `release` directory.

Software components installed

Each of the K2 installation packages installs software components that provide the functionality for various applications and system tools. The components installed are as follows:

Software	Components installed	Comments
K2 Client	Core system software	Provides the primary media functionality.
	AppCenter user interface	Allows you to operate AppCenter on the local machine.
	AppServer	Provides AppCenter functionality. It is accessed by both the remote AppCenter (on a Control Point PC) and the local AppCenter user interface.
	Storage Utility	Configures the media storage on internal storage K2 clients only. Do not run Storage Utility on shared storage K2 clients.
	K2 System Configuration	Installed only on shared storage models. Provides to the remotely connected K2 System Configuration application the ability to configure the local machine. You cannot run the K2 System Configuration user interface on the local K2 client.

Software	Components installed	Comments
	Multi-Path I/O	Installation files copied to K2 client but software not installed.
K2 Server	Core system software	Provides the primary media functionality.
	Storage Utility	Provides functionality for the remotely connected Storage Utility that runs on the Control Point PC. You should not run Storage Utility locally on the K2 Media Server.
	K2 System Configuration	Provides to the remotely connected K2 System Configuration application the ability to configure the local machine. You cannot run the K2 System Configuration user interface on the local K2 Media Server.
Control Point	AppCenter user interface	Connects to K2 clients for control and configuration of channels.
	K2 System Configuration user interface	Connects to K2 clients, K2 Media Servers, RAID storage, and Gigabit switches for configuration of the K2 SAN.
	Storage Utility	Connects to the K2 Media Server, and through the K2 Media Server to the RAID storage, for configuration of the media file system, media database, and RAID storage.

Installing Control Point software

If you are using the Grass Valley Control Point PC, it comes from the factory with software installed, so you should not need to install software.

If you intend to use a PC that you own as a Control Point PC, make sure that you choose a PC that meets system requirements for supporting Control Point software. Then install software and configure as follows:

1. Set up Windows user accounts according to your site's security policies. Refer to related topics in "K2 Release Notes" for the list of accounts and passwords.
2. Install the following software, as it is required to support K2 Control Point software:
   - MSXML 4.0
   - .NET Framework 1.1

   You can find this software on your K2 Summit/Solo system's USB Recovery Flash Drive.
3. Install K2 Control Point PC software, as referenced earlier in this chapter.

4. It is recommended that you install the following software, so that you can accomplish a broad range of operational and administrative tasks from the control point PC:
   - Java Real Time Environment Update 7 or higher. Required for the HP Ethernet Switch configuration interface, which is used for K2 SANs (shared storage).
   - QuickTime 7, for local viewing of exported media. You can find this on your K2 Summit/Solo system's USB Recovery Flash Drive.
   - Adobe Acrobat Reader, for reading documentation from the K2 Documentation Set.
5. Install SiteConfig. It is recommended that you use SiteConfig to manage stand-alone K2 Summit/Solo systems. It is required that you use SiteConfig to manage K2 SANs.
6. Install SNMP manager software.
7. Create a backup image.

Related Topics

Control Point PC system requirements on page 255

Installing K2 software

Except as noted in the preceding sections, when you receive your K2 Summit/Solo system, you do not need to install software. The system has software pre-installed at the factory.

If you are upgrading software on a K2 Summit/Solo system, refer to related topics in "K2 Release Notes" for that version of software for specific upgrade procedures. If you are upgrading a K2 SAN, you must use SiteConfig with the proper sequence and upgrade all K2 Media Servers and K2 Summit systems to the same software version. Upgrade K2 Media Servers first, then K2 Summit systems. Refer to related topics in "K2 Release Notes" for the complete explanation of the rules that apply to upgrading software on the K2 SAN.

Before upgrading K2 software, you should make a recovery image.

Pre-installed software

Software is pre-installed on K2 products when you receive them from the factory. Refer to related topics in "K2 Release Notes" for version updates.

Backup and recovery strategies

Find information on creating images, restoring from images, and other backup and recovery information as follows:

For this device…	Find information in this documentation:
K2 Summit system	K2 Summit Service Manual
K2 Media Client	K2 Media Client Service Manual
K2 Solo Media Server	K2 Solo Media Server Service Manual
K2 Media Server	K2 SAN Installation and Service Manual

For this device…	Find information in this documentation:
Control Point PC	Use procedures from a K2 Summit Service Manual

Chapter 8

Administering and maintaining the K2 system

This section contains the following topics:

Licensing

Grass Valley continues to develop the K2 product family to better meet the needs of a wide range of customer requirements. As these developments become available, you can add the specific functionality you need with Grass Valley software licenses. Detailed procedures for installing licenses come with option kits or are included in release notes for K2 products. Contact your Grass Valley representative to learn more about the licensing structure and for purchasing information.

Software version licenses

At major software releases, significant new features are added. If you are licensed for the software release, you can upgrade your software and receive the benefits of the new features.

Licensable options

Optional applications, bundles of advanced features, and enhanced functionality are available as licensable options for K2 products. Refer to the *K2 Release Notes* for a list of options, and contact your Grass Valley representative to learn more about options.

Configuring K2 security

The section contains topics about K2 security.

Overview of K2 security features

K2 security features reference Windows operating system user accounts and groups on the local K2 system to determine permission levels. Depending on the account used to log on to the Windows operating system, to log on to K2 applications, or to otherwise authenticate system access, permission is granted for various levels of operational and media access.

K2 systems offer security features as follows:

- Windows operating system — Depending on the current Windows logon, permission is granted to make security and user account settings in the Windows operating system.
- K2 applications — Depending on the user account used to log on to the application, permission is granted to control and configure the application. These K2 applications include AppCenter, Storage Utility, and the K2 System Configuration application.

- Media access — There are three types of media access security, as follows:
  - Media access in AppCenter — You can set user permissions on the K2 bins that store your media. Then, depending on the current AppCenter logon, permission is granted for AppCenter operations on the media in the bins.
  - Media access via FTP — The user permissions set on K2 bins in AppCenter also determine access via FTP. Depending on the FTP session logon, permission is granted for FTP commands accessing the media in the bins.
  - Media access via protocols — The permissions set on K2 bins in AppCenter also determine access for channels controlled by protocols. Depending on the channel accessing the media, permission is granted for operations on the media in the bins.

- Channel access security — You can set user permissions for each channel. Then, depending on the current AppCenter logon or protocol operating a channel, permission is granted or denied to operate the channel.

Related Topics

Passwords and security on Grass Valley systems on page 177
AppCenter operations and media access security on page 179
FTP and media access security on page 179
Protocol control of channels and media access security on page 180
About channel access security on page 180

Example: Setting up user access to bins

In this example User A requires a private bin in which only they can see media or have any access to media. User B requires a bin that provides media to other users, but prevents other users from modifying the media. To set up security features to meet these requirements, do the following:

Task	Documentation
Log on to the local K2 system with Windows administrator permissions.	*Passwords and security on Grass Valley systems* on page 177
Configure a “userA” account and a “userB” account on the local K2 client.	Use standard Windows procedures
Log on to AppCenter with GV administrator permissions.	*Passwords and security on Grass Valley systems* on page 177
Create a “userA_private” bin and a “userB_share” bin on the local K2 system.	*K2 AppCenter User Manual*
For bin “userA_private” configure an access control list with permissions as follows: • Create a group and add all users except user A to the group. For this group, set permissions to: Deny Full Control • userA: Allow Full Control	*Configuring media access security for K2 bins* on page 177

Task	Documentation
For bin “userB_share” configure an access control list with permissions as follows: • Create a group and add all users except user B to the group. For this group, set permissions to: Allow List Bin Contents, Allow Read, Deny Write, Deny Delete • userA: Allow Full Control	*Configuring media access security for K2 bins* on page 177
Log on to AppCenter as userA. Test userA access to bins. Log off.	—
Log on to AppCenter as userB. Test userB access to bins. Log off.	—

Example: Setting up user access to channels

In this example User A requires exclusive access to channels 1 and 2 and User B requires exclusive access to channels 3 and 4. To set up security features to meet these requirements, do the following:

Task	Documentation
Log on to the local K2 system with Windows administrator permissions.	*Passwords and security on Grass Valley systems* on page 177
Configure a “userA” account and a “userB” account on the local K2 client.	Use standard Windows procedures
Log on to AppCenter with GV administrator permissions.	*Passwords and security on Grass Valley systems* on page 177
For channels 1 and 2, configure access control lists with permissions as follows: • Create a group and add all users except user A to the group. For this group, set permissions to: Deny • userA: Allow	*About channel access security* on page 180
For channels 3 and 4, configure access control lists with permissions as follows: • Create a group and add all users except user B to the group. For this group, set permissions to: Deny • userB: Allow	*About channel access security* on page 180
Log on to AppCenter as userA. Test userA access to channels. Log off.	—
Log on to AppCenter as userB. Test userB access to channels. Log off.	—

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.

Configuring media access security for K2 bins

The permissions you set on a K2 bin restricts access to the media in the bin via AppCenter operations, via FTP, and via protocol control of channels.

You can set permissions on a K2 bin as follows:

- Write — Allow access to rename or delete any of the clips located in the bin.
- Delete — Allow access to delete any of the clips located in the bin.
- Read — Allow access to the clips located in a bin, but deny the ability to modify the clips.
- List Bin Contents — Allow or deny access to explore the contents of the bin. This permission also controls access to transfer clips in/out of the bin and to perform search operations on the bin.

- Full Control — Allow or deny all of the above permissions plus the ability to modify the permissions on a bin.

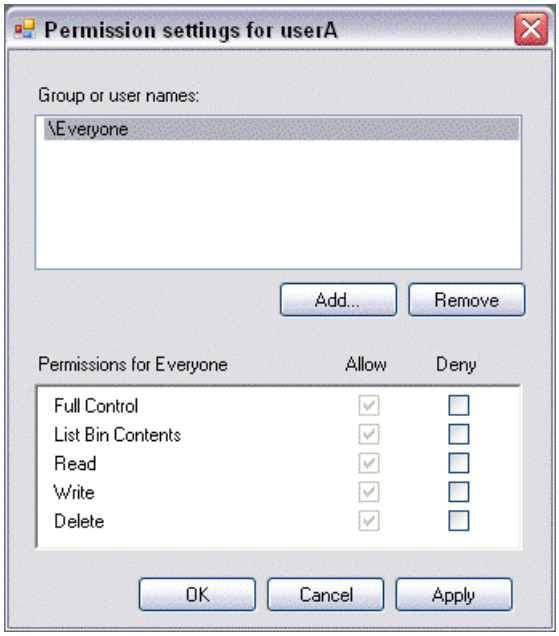
As you configure permissions, take the following into account:

- In case of conflicts, the Deny permission always overrides the Allow permission.
- Do not restrict access for the *movie*, *mxfmovie*, and *video_fs* accounts. These accounts are used for access by applications and modifying permissions can cause applications and transfers to fail. If your security policy requires restricting access to these accounts, contact Grass Valley Support.
- By default, the "Everyone" group is set to Full Control, with all permissions allowed. When you create a new bin it has these default permissions applied automatically.
- Avoid using the "Everyone" group to restrict permissions. Doing so causes some or all operations to fail, regardless of the account currently logged on.
- The "system" user account must retain access to bins and files.
- Never deny any permissions to the user NT AUTHORITY\System.
- The user account that originally created a bin always retains the ability to modify permissions on that bin.

If you need to restrict access to a K2 bin that you have created, set up a media access control list on the bin, as instructed in the following procedure.

1. Make sure you are logged on to Windows and AppCenter with administrator privileges.
2. Create user accounts and bins as necessary to support your permission policies.
3. In the Clips pane, select the Current Bin drop-down list, then select **Organize Bins**. The Organize Bins dialog box opens.
4. Create a bin if necessary, or otherwise select the bin for which you are setting permissions and then click **Permission**. The Permission settings dialog box opens.

   NOTE: You can not set permissions on the default bin or on the Recycle bin.



5. Add users and groups to the access control list and set permissions as follows:
   a) Click **Add**. The Select Users or Groups dialog box opens. This is the standard Windows operating system interface to users and groups, so you can use standard Windows procedures. In the "Enter the object names…" box, you can enter the users or groups for which you want to set permissions, then click **OK**.
   b) In the Permission settings dialog box, select a user or group and then set permissions as desired.
6. Click **Apply**, **OK**, and **Close** to save settings and close dialog boxes.

AppCenter operations and media access security

AppCenter uses the credential information for the current AppCenter logon and checks it against the access control list for a K2 bin. This is the access control list that you set up through the Organize Bins dialog box in AppCenter. In this way, AppCenter determines whether to allow or deny operations on media in a K2 bin.

Once permissions are granted based on the current logon account, those permissions remain in place until that account logs off of AppCenter.

FTP and media access security

The following systems host the K2 FTP interface:

- A stand-alone K2 system.
- A K2 Media Server that takes the role of FTP server

The way in which the K2 FTP interface applies media access security is explained in this section.

The K2 FTP interface uses the credential information for the current FTP session logon and checks it against the access control list for a K2 bin. This is the access control list that you set up through the Organize Bins dialog box in AppCenter. Any media access related operations such as `get`, `put`, `dir`, `rename` and `delete` are checked against the FTP session's logon credentials to access the media. For example, if an FTP session is denied access to List Bin Contents for bin A, then the session can not initiate a `dir` operation on bin A to list the contents of the bin. Furthermore, the session can not transfer clips into bin A using the `put` operation.

For the purpose of compatibility FTP access conventions, accounts for user `movie` or user `mxfmovie` are provided on the K2 system. There is also a `video_fs` account for Mac/FCP access. These accounts are automatically set up when you install K2 software version 3.2 or higher. Do not restrict access for these accounts. If your security policy requires restricting access to these accounts, contact Grass Valley Support.

On a K2 SAN, authentication takes place on the K2 Media Server. Setting up FTP security for specific local users and groups is not supported on a K2 SAN, with the exception of the local `movie` and `mxfmovie` accounts. However, you can set up FTP security for domain users and groups.

K2 SANs and media access security

This section applies to media access security, not FTP security. Refer to the preceding section for information about FTP security.

On a K2 SAN, the users and groups referenced by media access security features are the users and groups on the connected K2 clients, not the K2 Media Server. Use domain users and groups rather than local users and groups. Media access security is not supported with Workgroup network configuration on a K2 SAN.

Protocol control of channels and media access security

Protocol security restricts a channel in its access to the media in a bin, regardless of what user is currently logged on to AppCenter. This is different than the other types of media access security, in which the security restricts the user (as currently logged on to AppCenter) in their access to the media in a bin, regardless of what channel is being used.

Nevertheless, permissions for protocol channels are still derived from user accounts. In AppCenter's Configuration Manager, on the Security tab you can associate a user account with a channel of protocol control. Based on that association, when a protocol controls the channel, AppCenter checks the credential information for the associated user account against the access control list for a K2 bin. This is the access control list that you set up through the Organize Bins dialog box in AppCenter. In this way, AppCenter determines whether to allow or deny that channel's operations on the media in the bin.

By default, protocols have administrator privileges for media access. In addition, protocols are always allowed access to a channel.

Associating a protocol channel with a user account

1. Make sure you are logged on to Windows and AppCenter with administrator privileges.
2. Create user accounts and bins as necessary to support your permission policies.
3. Click **System | Configuration**. Configuration Manager opens.
4. Click a channel tab.
5. Click the **Security** tab.
6. Enter the username, the password, and (if applicable) the domain for the user account that you are associating with the channel.

   When this channel is under protocol control and it accesses media in a bin for which permissions have been set, AppCenter makes the channel's access to the media equivalent to this user's access to the media.
7. Click **OK** to save Configuration Manager settings and close Configuration Manager.
8. Restart AppCenter to put the change into effect.

About channel access security

Channel access security restricts the user (as currently logged on to AppCenter) in their use of an AppCenter channel, regardless of what bin or what media is involved. This is different than media access security, in which the security restricts the user in their access to the media in a bin, regardless of what channel is being used.

You can set up an access control list for each channel through the channel's Permissions dialog box. AppCenter uses the credential information for the current AppCenter logon and checks it against

the access control list for a channel. In this way, AppCenter determines whether to allow or deny access to the channel's controls.

When you set up a channel access control list, you select the permissions for the channel as follows:

Allow — The user can operate the channel. All channel controls are enabled.

Deny — The user can not operate the channel. The controls are not displayed on the channel pane.

If neither Allow nor Deny are selected permissions are inherited from the user's parent group.

You configure these permissions to apply to users and groups. By default, all channels have their permission set to allow access to "Everyone". In case of conflicts arising from a user belonging to multiple groups, the Deny permission always overrides the Allow permission.

When you log on to AppCenter on a local K2 system, permissions for all local channels are based on the single user logged on. Therefore channel permissions are enforced for just one user at a time across all local channels. If you require that channel permissions be enforced simultaneously for different users each accessing their own channel or channels on a single K2 system, those users must log on via a remote AppCenter channel suite from a Control Point PC. The remote AppCenter channel suite allows each channel to be operated by a different user.

Once permissions are granted based on the current logon account, those permissions remain in place until that account logs off of AppCenter.

If you need to restrict access to an AppCenter channel, configure channel access security by setting up a channel access control list.

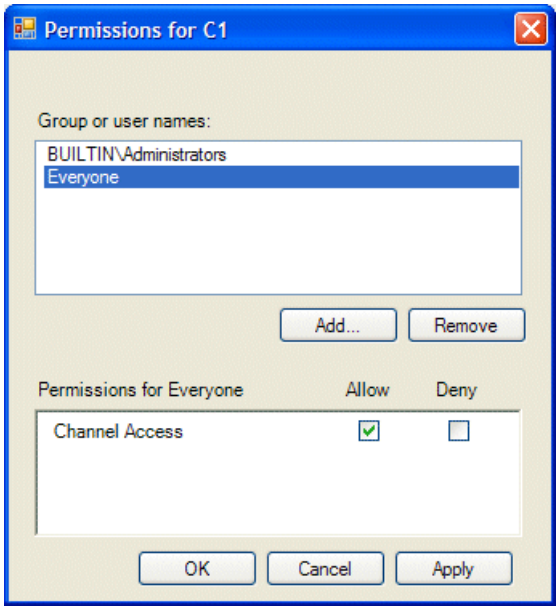
Setting up a channel access control list

1. Make sure you are logged on to Windows and AppCenter with administrator privileges.
2. Create user accounts and bins as necessary to support your permission policies.
3. Click **System | Configuration**. Configuration Manager opens.
4. Click a channel tab.
5. Click the **Security** tab.

   NOTE: Do not configure protocol user setup. This is for protocol media access security only and has nothing to do with channel access security.

6. Click **Permission**.

   The Permissions dialog box opens.



7. Add users and groups to the access control list and set permissions as follows:
   a) Click **Add**. The Select Users or Groups dialog box opens. This is the standard Windows operating system interface to users and groups, so you can use standard Windows procedures. In the "Enter the object names…" box, you can enter the users or groups for which you want to set permissions, then click **OK**.
   b) In the Permission settings dialog box, select a user or group and then set permissions as desired.

      Remember that by default, "Everyone" is set to Allow. You might need to change this in order to configure your permission policies.

   NOTE: You can not change permissions for the BUILTIN\Administrators account.

8. Click **Apply** and **OK** to save settings and close the Permissions dialog box.
9. Click **OK** to save Configuration Manager settings and close Configuration Manager.
10. Restart AppCenter to put the change into effect.

K2 and STRATUS security considerations

Access Control Lists (ACLs) specify individual user or group rights to specific system objects such as programs, processes, or files. K2 Summit systems enforce ACLs for security and permissions on K2 bins and channels. However, the STRATUS system does not enforce ACLs. Instead, the STRATUS system always accesses the K2 Summit system via the GVAdmin user, and the K2 Summit system is configured by default to allow full access to the GVAdmin user. This is an important consideration to allow the systems to operate together. Therefore you must not change the default configuration of security and permissions on your K2 Summit systems that are part of

your STRATUS system. This includes Windows operating system ACL settings and K2 AppCenter security/permission settings on bins and channels. Since the GVAdmin user is not a member of the Administrators group, changing these settings could prevent the STRATUS system from accessing the K2 Summit system.

Understanding virus and security policies

Read the topics in this section for a better understanding of your system.

Windows operating system update policy

Grass Valley recognizes that it is essential to deploy Microsoft security patches to Windows operating system products as quickly as possible. As Grass Valley systems are used to meet the mission-critical requirements of your environment, it is imperative that these systems be kept up to date in order to maintain the highest level of security available. To that end, Grass Valley recommends that for standard-edition Windows operating system products, you install all high priority updates provided by Microsoft. In the unlikely event that one of these updates causes ill effects to a Grass Valley system, you are urged to uninstall the update and contact Grass Valley customer service as soon as possible. Grass Valley will investigate the incompatibility and, if necessary, provide a software update or work-around to allow the system to properly function with the Microsoft update in question.

Note that this policy applies to "High Priority" updates only. There are countless updates not classified as "High Priority" that are made available by Microsoft. If you believe that one or more of these other updates must be applied, contact Grass Valley prior to installation. This policy also applies to standard-edition (not embedded) operating systems only. Do not attempt to update an embedded Windows operating system in any way except as directed by Grass Valley for the specific product.

You should exercise common sense when applying updates. Specifically, do not download or install an update while a Grass Valley product is being used for mission-critical purposes such as play to air.

Embedded Security modes and policies

The Embedded Security solution protects against viruses and other unauthorized programs on the following Grass Valley systems:

- K2 Summit/Solo system
- K2 Media Server
- GV STRATUS server
- K2 Dyno S Replay Controller

Embedded Security prevents any unauthorized programs from running on the system. It contains a whitelist of programs that are authorized to run. Whenever a program attempts to run, it is checked against the whitelist. If the program is not on the whitelist, Embedded Security blocks the program from running. SiteConfig, and any software deployed by SiteConfig, is on the whitelist, so you do not need to manage Embedded Security in any way when using SiteConfig to deploy software. All versions of SiteConfig are compatible with Embedded Security.

When installing software manually (without SiteConfig) it might be necessary to manage Embedded Security. When necessary, you can put Embedded Security in Update mode. This mode allows you to manually install software that is not on the whitelist. Do not confuse Update mode with the idea that Embedded Security is "disabled". When in Update mode, Embedded Security is still active. While in Update mode, Embedded Security keeps track of any software you run or install and adds it to the whitelist. When you are done installing software and any required restarts, you must take Embedded Security out of Update mode so that it can protect the system. For software that requires a restart after installation, such as K2 system software and SNFS media file system software, Embedded Security must remain in Update mode until after the restart is complete.

No system restarts are required for entering or leaving Update mode, and a restart does not change the Update mode status. If in Update mode before a restart, the system remains in Update mode after a restart. You use the Embedded Security Manager to enter and leave Update mode.

The following policies apply to the Embedded Security:

- Use Update mode only as instructed by Grass Valley product documentation or as directed by Grass Valley Support. Do not do any other operations with Embedded Security Manager, unless under the direct supervision of Grass Valley Support.
- Do not keep Embedded Security in Update mode long-term, as Embedded Security does extra processing while in Update mode and eventually problems arise when attempting to run software.
- Make sure that Embedded Security is not in Update mode when using SiteConfig to install software. Update mode interferes with SiteConfig's automatic management of Embedded Security and causes problems running the software installed.
- Leave Embedded Security enabled for normal operation of your Grass Valley system. Do not disable Embedded Security except as instructed by Grass Valley product documentation or as directed by Grass Valley Support. Enabling and disabling Embedded Security requires a restart.
- Do not install any programs or modify any operating system settings unless approved by Grass Valley. By design, Embedded Security prevents any programs from being installed or from running that are not present when you receive the system new from Grass Valley. These Grass Valley systems are not a general purpose Windows workstations. The applications and configuration have been specifically optimized on each system for its intended use as part of the Grass Valley system.
- While Embedded Security is the key anti-virus component on these systems, you should still follow the Grass Valley anti-virus scan policy and scan all the devices in your Grass Valley system to ensure viruses are not propagated between machines.

Embedded Security is part of the K2 Summit/Solo system generic disk image and the K2 Media Server generic disk image compatible with K2 software version 9.0 or higher. Both K2 Media Servers and GV STRATUS servers use the same generic disk image, so GV STRATUS servers inherit the Embedded Security solution. On K2 Summit/Solo systems, the Embedded Security solution introduced with K2 software version 9.0 replaces the write filter from previous versions.

Grass Valley anti-virus scan policy

Grass Valley systems are based on the Microsoft Windows operating system. It is important to defend this system against virus or Spyware attacks. However, you must use a strategy that allows you to scan Grass Valley systems without interrupting media access. Contact Grass Valley Support for to determine the strategy best suited to your environment.

Network and firewall policies

The following protection policies are recommended:

- Where possible, the K2 system should be run in a closed and protected environment without network access to the corporate IS environment or the outside world.
- If the K2 system must operate in a larger network, Grass Valley recommends that access be through a gateway or firewall to provide anti-virus protection. The firewall should allow incoming HTTP (TCP port 80) connections for client and configuration connections to the K2 system inside the private network.
- Access to the K2 system should be controlled in order to limit the likelihood of malicious or unintended introduction of viruses.

About tri-level sync

The K2 Summit/Solo system supports tri-level sync as a genlock reference source. The reference must be in an HD format and frame rate that is supported by the K2 Summit/Solo system, as follows:

- Reference Standard: NTSC (59.97Hz)
  - 1080i 29.97
  - 720p 59.94
- Reference Standard: PAL (50Hz)
  - 1080i 25
  - 720p 50

The K2 Summit/Solo system automatically detects, switches, and syncs to the reference. When you configure the reference standard for either NTSC (59.97Hz) or PAL (50Hz) in K2 AppCenter Configuration Manager, a restart is required to put the change into effect and the system starts with a SD reference format by default. It then attempts to detect a reference in a format and frame rate that is compatible with the current reference standard setting. When the K2 Summit/Solo system detects a reference in a supported format, it automatically switches to that format. This allows the system to switch between SD and HD tri-level formats with frame rates that are compatible with the reference standard setting. When the K2 Summit/Solo system locks to a new reference format, it saves the format and frame rate information, and upon restart it returns to the saved format and frame rate.

Do not use a progressive reference with an interlace output. For example, do not use 720p tri-level sync for interlace output formats (such as SD and 1080i). Output timing can be off by a field with this type of incompatibility.

The K2 Summit/Solo system treats the following conditions as a loss of reference:

- No reference is present
- A reference in an unsupported format is present
- A reference in a supported format is present but it has a frame rate that is not compatible with the current reference standard setting.

In these cases the K2 Summit/Solo system internal genlock flywheel provides a stable reference for the last reference set. The system reports this status in K2 AppCenter Configuration Manager Reference Standard by a black "Reference present" indicator.

Auto log on

If you set a K2 Media Client, a K2 Summit Production Client or a K2 Solo Media Server to automatically log on to the Windows operating system at startup, AppCenter honors this setting. This means that at startup AppCenter bypasses its log in dialog box and opens automatically. For more information about how to turn on automatic login in the Windows operating system, including security risks and procedures, refer to the related Microsoft knowledge base article.

Regional and language settings

On all K2 Summit Production Clients, K2 Media Clients, K2 Solo Media Servers and K2 Media Servers, in the Windows Control Panel “Region and Language”, there are special FTP internationalization requirements regarding the language for non-Unicode programs to support FTP transfers. Do not change these settings.

Related Topics

About FTP internationalization on page 77

Internationalization on page 240

Setting the FTP language on page 78

Checking RAM

You can determine the amount of Random Access Memory (RAM) on your K2 Summit/Solo system's CPU module.

1. Connect the the K2 Summit/Solo system's USB Recovery Flash Drive to the K2 Summit/Solo system.
2. On the USB Recovery Flash Drive, locate and double-click the following:

   `CPUList.exe`

   A System Inventory window opens and displays information about the manufacturer, model, and amount of RAM on the CPU module.
3. Press **Enter** to close the System Inventory window.

Related Topics

About memory requirements

Chapter 9

Direct Connect Storage

This section contains the following topics:

About the direct-connect Fibre Channel card

The direct-connect K2 Summit Production Client or K2 Media Client has a direct Fibre Channel connection to external K2 RAID. The K2 client must have the optional Fibre Channel card installed to support this connection. This gives the K2 client the large storage capacity of the external RAID, yet its media related functionality is that of a “stand-alone” K2 client, similar to a K2 client with internal storage.

A K2 Summit Production Client's optional Fiber Channel card is a 8 Gb/s ATTO Fibre Channel card.

Setting up direct-connect K2 G10v2 RAID storage

The topic applies to K2 G10v2 (M100) RAID storage with direct connection to a K2 Summit system system.

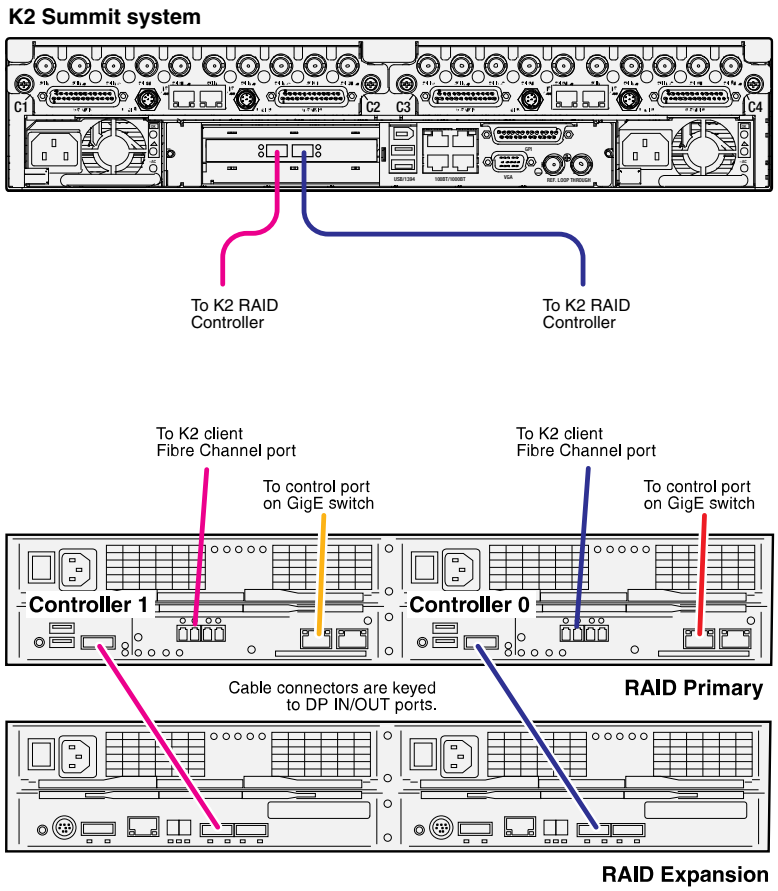
Prerequisites for the following procedure are as follows:

- For a 8 Gb/s Fibre Channel card on K2 Summit Production Client, RAID controllers must be configured for 8 Gb/s. This is the default configuration as shipped from Grass Valley.

The following procedure is intending for the initial installation of a factory-prepared direct-connect system that you have ordered new from Grass Valley. If you are repurposing equipment or otherwise putting together direct-connect storage with equipment that is not factory-prepared, refer to the Service Manual for your model of K2 client for the complete restore/recover procedure.

As you work through the following procedure, refer as necessary to the *K2 SAN Installation and Service Manual* "Installing" chapters for information about cabling and configuring K2 RAID.

1. Connect the K2 Summit system and RAID devices as shown in the following illustrations.



   Connect K2 Summit system Fibre Channel ports to RAID controllers. Connect Fibre Channel port 1 to RAID controller 0. If you have the redundant controller, connect Fibre Channel port 2 to RAID controller 1.

   Connect RAID controller Management ports to control ports on a K2 GigE switch. If you have redundant switches, connect controller 0 to switch A and controller 1 to switch B.

   NOTE: The control network connection is required to support basic functionality such as gathering logs and loading controller microcode, as well as SNMP monitoring.

   Connect RAID controller Disk Port to the Expansion chassis Disk Port In 1 ports.

2. Connect power cables and power up the RAID devices. Refer to "Powering on K2 RAID" later in this chapter.
3. Connect remaining cables to the K2 Summit system. Refer to the Quick Start Guide for the particular K2 Summit system model for cabling details.
4. Start up the K2 Summit system.

   The Windows initialization screen shows the progress bar but does not complete.

5. Power down the K2 Summit system.

6. Disconnect all Fibre Channel cables from the K2 Summit system.
7. Start up the K2 Summit system and log in to Windows.
8. Uninstall Multi-Path I/O (MPIO) software as instructed by the topic later in this section.
9. Log in to Windows.
10. Power down the K2 Summit system.
11. Reconnect one Fiber Channel cable.
12. Start up the K2 Summit system and log on to Windows.
13. On the K2 Summit system, open Storage Utility.
14. In Storage Utility, do the following:
    a) Configure network and SNMP settings for controllers.
    b) Bind the disks in the external RAID. Bind as RAID 5 or RAID 6, as specified by your system design.
    c) When the binding process completes, proceed to the next step.
15. Restart the K2 Summit system and log in to Windows.
16. Reconnect the other Fiber Channel cable.
17. Install MPIO software as instructed by the topic later in this section.
18. In Storage Utility, make a new file system

    If you get a "…failed to remove the media database…" message, you can safely proceed.
19. Restart the K2 Summit system and log in to Windows.
20. Open AppCenter and manually remove all clips and bins except the default bin and the recycle bin.
21. Uninstall and then reinstall both SNFS software and K2 Client software. Use the sequence and detailed procedure in the *K2 Release Notes* for the version of K2 Client software currently on the K2 Summit system.
22. As you install K2 Client software, when you arrive at the Specify Target Type page, select **K2 with local storage**.
23. Restart the K2 Summit system.

The K2 Summit system is now ready for record/play operations.

NOTE: If you ever unbind LUNs, you must do the above procedure again, starting at step 5.

Setting up direct-connect K2 G10 RAID storage

The topic applies to K2 G10 (D4) RAID storage with direct connection to a K2 Summit system system.

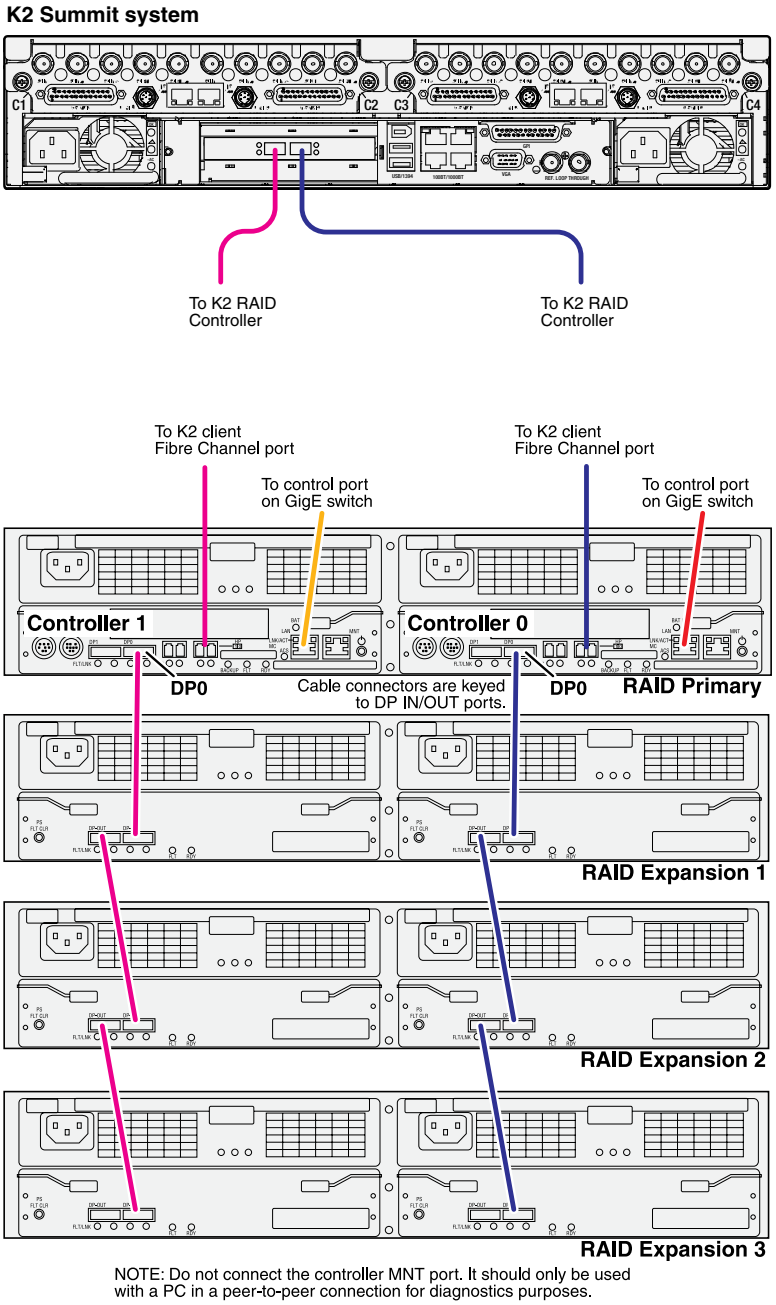
Prerequisites for the following procedure are as follows:

- For a 8 Gb/s Fibre Channel card on K2 Summit Production Client, RAID controllers must be configured for 8 Gb/s. This is the default configuration as shipped from Grass Valley.

The following procedure is intending for the initial installation of a factory-prepared direct-connect system that you have ordered new from Grass Valley. If you are repurposing equipment or otherwise putting together direct-connect storage with equipment that is not factory-prepared, refer to the Service Manual for your model of K2 client for the complete restore/recover procedure.

As you work through the following procedure, refer as necessary to the *K2 SAN Installation and Service Manual* “Installing” chapters for information about cabling and configuring K2 RAID.

1. Connect the K2 client and RAID devices as shown in the following illustrations.



Connect K2 client Fibre Channel ports to RAID controllers. Connect Fibre Channel port 1 to RAID controller 0. If you have the redundant controller, connect Fibre Channel port 2 to RAID controller 1.

Connect RAID controller LAN ports to control ports on a K2 GigE switch. If you have redundant switches, connect controller 0 to switch A and controller 1 to switch B.

Connect RAID controller DP0 ports to the first Expansion chassis DP-IN ports.

Connect remaining Expansion chassis using DP-OUT and DP-IN ports.

2. Connect power cables and power up the RAID devices. Refer to "Powering on K2 RAID" later in this chapter.
3. Connect remaining cables to the K2 client. Refer to the Quick Start Guide for the particular K2 client model for cabling details.
4. Start up the K2 client.

   The Windows initialization screen shows the progress bar but does not complete.
5. Power down the K2 client.
6. Disconnect all Fibre Channel cables from the K2 client.
7. Start up the K2 client and log in to Windows.
8. Uninstall Multi-Path I/O (MPIO) software as instructed by the topic later in this section.
9. Log in to Windows.
10. Power down the K2 client.
11. Reconnect Fiber Channel cables.
12. Start up the K2 client and log on to Windows.
13. On the K2 client, open Storage Utility.
14. In Storage Utility, do the following:
    a) Configure network and SNMP settings for controllers.
    b) Bind the disks in the external RAID. Bind as RAID 5 or RAID 6, as specified by your system design.
    c) When the binding process completes, proceed to the next step.
15. Restart the K2 client and log in to Windows.
16. Install MPIO software as instructed by the topic later in this section.
17. In Storage Utility, make a new file system

    If you get a "…failed to remove the media database…" message, you can safely proceed.
18. Restart the K2 client and log in to Windows.
19. Open AppCenter and manually remove all clips and bins except the default bin and the recycle bin.
20. Uninstall and then reinstall both SNFS software and K2 Client software. Use the sequence and detailed procedure in the *K2 Release Notes* for the version of K2 Client software currently on the K2 client.
21. As you install K2 Client software, when you arrive at the Specify Target Type page, select **K2 with local storage**.
22. Restart the K2 client.

The K2 client is now ready for record/play operations.

NOTE: If you ever unbind LUNs, you must do the above procedure again, starting at step 5.

Uninstalling Multi-Path I/O Software on a direct-connect K2 system

The following procedure applies to direct-connect K2 systems.

The files for the Multi-Path I/O software are copied on to the K2 system when the K2 software is installed.

1. Access the Windows desktop on the K2 system.

   You can do this locally with a connected keyboard, mouse, and monitor or remotely via the Windows Remote Desktop Connection.

2. Stop all media access. If AppCenter is open, close it.
3. Click **Start | Run**, type `cmd` and press **Enter**.

   The MS-DOS command prompt window opens.

4. From the command prompt, navigate to the *`C:\profile\mpio`* directory.
5. Type one of the following at the command prompt:

   - If uninstalling on a 32-bit system:

     ```
     gdsminstall.exe -u c:\profile\mpio gdsm.inf Root\GDSM
     ```

   - If uninstalling on a 64-bit system:

     ```
     gdsminstall64.exe -u
     ```

6. Press **Enter**.

   The software is uninstalled. The command prompt window reports progress.

7. Restart the K2 system.

Installing Multi-Path I/O Software on a direct-connect K2 system

Before doing this task, if a K2 Summit system with K2 software version lower than 9.0, make sure the write filter is disabled.

The following procedure is required for direct-connect K2 systems.

The files for the Multi-Path I/O software are copied on to the K2 system when the K2 software is installed.

1. Access the Windows desktop on the computer on which you are installing MPIO.

   You can do this locally with a connected keyboard, mouse, and monitor or remotely via the Windows Remote Desktop Connection.

2. Stop all media access. If AppCenter is open, close it.
3. Click **Start | Run**, type `cmd` and press **Enter**.

   The MS-DOS command prompt window opens.

4. From the command prompt, navigate to the *`C:\profile\mpio`* directory.
5. Type one of the following at the command prompt:

   - If installing on a 32-bit computer:

     ```
     gdsminstall.exe -i c:\profile\mpio gdsm.inf Root\GDSM
     ```

   - If installing on a 64-bit computer:

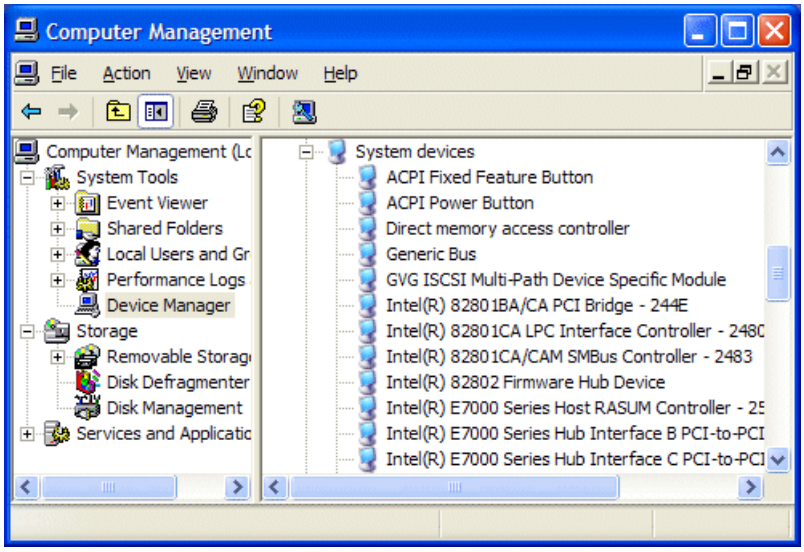
     ```
     gdsminstall64.exe -i
     ```

6. Press **Enter**.

   The software is installed. The command prompt window reports progress.

7. Restart the computer on which you installed MPIO.
8. After restart, to verify that the software is installed, on the Windows desktop right-click **My Computer** and select **Manage**.

   The Computer Management window opens.



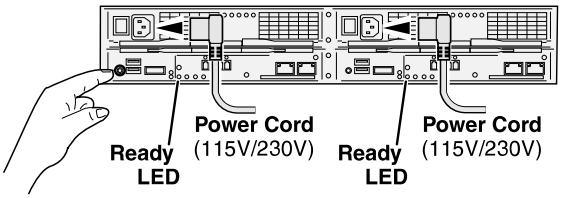
9. In the left pane select **Device Manager**.
10. In the right pane open the **System devices** node and verify that **GVG ISCSI Multi-Path Device Specific Module** is listed.

Powering on K2 G10v2 RAID

This topic applies to K2 G10v2 (M100) RAID.

1. Verify power and cabling.
2. Tap the power button on the controller, as shown.

   NOTE: Do not press and hold down the power button.



   If the RAID chassis has two controllers, you can tap the power button on either controller. You do not need to tap both power buttons.

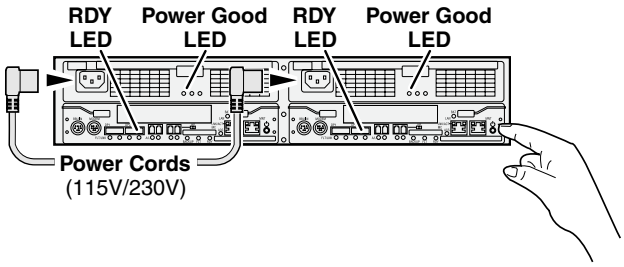
   Tapping the power button on a controller also powers on any connected Expansion chassis. There are no power buttons on Expansion chassis.

3. Wait while the primary RAID chassis performs self-test and initialization. This takes 6-8 minutes. While this is taking place, the Ready LED is illuminated with a steady on light.
4. Watch for the Ready LED to begin blinking at one second intervals. The LED might turn off and back on two times before starting the one second blink pattern. When the Ready LED is blinking at one second intervals, the self-test and initialization is complete and the chassis is ready for use.

Powering on K2 G10 RAID

This topic applies to K2 G10 (Condor) RAID.

1. Verify power and cabling.
2. Press and hold down the power button on the controller, as shown.



   If the RAID chassis has two controllers, you can press the power button on either controller. You do not need to press both power buttons.

   Pressing the power button on a controller also powers on any connected Expansion chassis. There are no power buttons on Expansion chassis.

3. Release the power button when the Power Good LED on the power supply is illuminated. This takes 1-3 seconds.
4. Wait while the primary RAID chassis performs self-test and initialization. This takes about four minutes. While this is taking place, the RDY LED is illuminated with a steady on light.
5. Watch for the RDY LED to begin blinking at one second intervals. The LED might turn off and back on two times before starting the one second blink pattern. When the RDY LED is blinking at one second intervals, the self-test and initialization is complete and the chassis is ready for use.

Chapter 10

K2 Summit Transmission models

This section contains the following topics:

K2 Summit Transmission models features

This chapter contains information that is unique to K2 Summit Transmission Client and Server models. Refer to other chapters for information that applies to all K2 Summit systems.

K2 Summit Transmission Client and Server models are optimized for playout, rather than record. Input/output configurations support the needs of playout applications. Higher efficiency MPEG-2 encoding reduces bandwidth and increases storage capacity. The result is that the K2 Summit Transmission Client and Server models are restricted to a subset of K2 Summit system bit rates, formats, and other features.

The following feature lists contain features that are unique to K2 Summit Transmission Client and Server models. Features that common to all K2 Summit models, both K2 Summit Production Client models and K2 Summit Transmission Client and Server models, are not listed here.

Features that all K2 Summit Transmission Client and Server models share are as follows:

- Records video bit rates up to 50Mbps, with 16 channels of audio at 24bits/sample.
- Supports MPEG-2 formats and DVCPRO formats at 50Mbps or less.
- Supports FTP bandwidth up to 30 MB/second.

The K2-XDT-4HD K2 Summit HD/SD Transmission Client has the following features:

- Two bi-directional and two playout only HD/SD channels.
- Channels are configurable as 1 x 3, 2 x 2 or 0 x 4.
- Shared storage via iSCSI connection on a K2 SAN.

The K2-XDT-4SD K2 Summit SD Transmission Client has the following features:

- Two bi-directional and two playout only SD channels.
- Channels are configurable as 1 x 3, 2 x 2 or 0 x 4.
- Shared storage via iSCSI connection on a K2 SAN.

The K2-XDT-2HD-IS K2 Summit HD/SD Transmission Server has the following features:

- One bi-directional and one playout only HD/SD channel.
- Channels are configurable as 1 x 1 or 0 x 2.
- Internal storage with twelve SAS media drives configured as RAID 1.

The K2-XDT-4HD-IS K2 Summit HD/SD Transmission Server has the following features:

- Two bi-directional and two playout only HD/SD channels.
- Channels are configurable as 1 x 3, 2 x 2 or 0 x 4.
- Internal storage with twelve SAS media drives configured as RAID 1.

The K2-XDT-4SD-IS K2 Summit SD Transmission Server has the following features:

- Two bi-directional and two playout only SD channels.
- Channels are configurable as 1 x 3, 2 x 2 or 0 x 4.
- Internal storage with twelve SAS media drives configured as RAID 1.

Related Topics

K2 Summit system features on page 31

K2 Summit Transmission models channel configurations

The details of the channel configurations available on K2 Summit Transmission Client and Server models are as follows:

1 x 3 channels

Channel	DV record	DV play	MPEG-2 record	MPEG-2 play
1	X	X	X	X
2		X		X
3		X		X
4		X		X

2 x 2 channels

Channel	DV record	DV play	MPEG-2 record	MPEG-2 play
1	X	X	X	X
2		X		X
3	X	X	X	X
4		X		X

0 x 4 channels

Channel	DV record	DV play	MPEG-2 record	MPEG-2 play
1		X		X
2		X		X
3		X		X
4		X		X

1 x 1 channels

Channel	DV record	DV play	MPEG-2 record	MPEG-2 play
1	X	X	X	X
2		X		X

0 x 2 channels

Channel	DV record	DV play	MPEG-2 record	MPEG-2 play
1		X		X
2		X		X

K2 Summit Transmission models requirements and restrictions

- MPEG-2 data rates above 50 Mbps not supported
- DVCPRO HD, AVC-Intra, H.264, Avid DNxHD formats not supported
- Transition effects not supported
- AppCenter Elite not supported.
- ChannelFlex Suite inputs and outputs are not supported.
- Mobile environment not supported. The standard K2 Summit system random vibration specifications do not apply to the K2 Summit Transmission Server models. Instead, random vibration specifications for K2 Summit Transmission Server (internal storage) models are as follows:

Characteristic	Specification
Random Vibration Operational	0.27 GRMS (5-500Hz)
Random Vibration Non-Operational	2.13 GRMS overall .015 g2/Hz (5-100Hz) .0075 g2/Hz (200-350Hz) .005256 g2/Hz (500 Hz)

Storage Utility procedures for K2 Summit Transmission Server models

Storage Utility detects drive type/capacity and allows only those operations that are correct for the drive type/capacity. If you need to bind the internal drives, RAID 1 is recommended. This is the default configuration as received from the Grass Valley factory. However, Storage Utility allows you to bind as RAID 0 if you so choose.

Related Topics

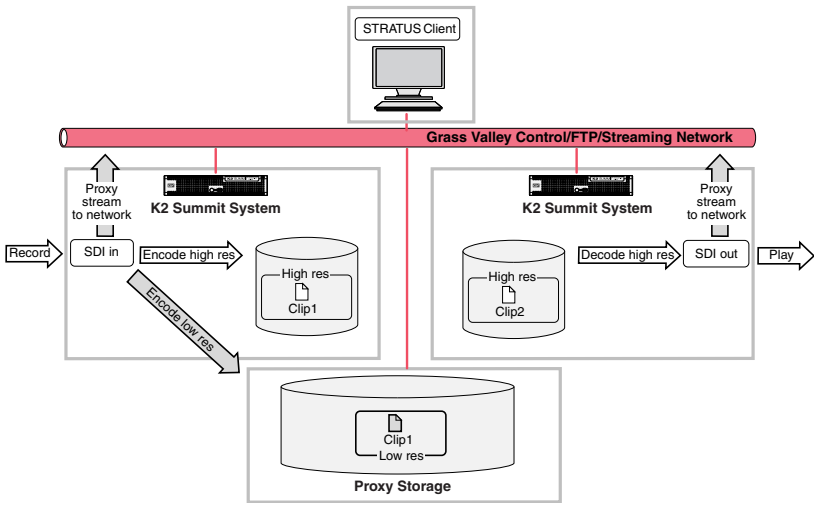
About Storage Utility on page 126

Chapter 11

Proxy/live streaming

This section contains the following topics:

Proxy and live streaming workflow overview



When licensed and configured, a K2 Summit system creates low-resolution representations of high-resolution media. Similar to PB/EE functionality, the K2 Summit System creates a live stream of low-resolution media at the SDI input and a live stream of low-resolution media at the SDI output, whether or not record/play operations are underway. These streams are multicast to the network and are available to applications on the network. When media is recorded, the K2 Summit system encodes a high resolution clip and a low resolution proxy clip. The system keeps these clips associated so any changes take effect simultaneously for both clips.

The GV STRATUS application accesses the low-resolution media over the network. When you monitor the K2 Summit system SDI inputs and outputs, the application displays the live stream. When you view an asset, the application displays the proxy representation of the asset. When you edit an asset, the K2 Summit system makes your changes on both the proxy and the high resolution asset.

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 or Type III CPU 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 — 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. Proxy files are not created.
- 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.

Related Topics

Proxy/live streaming technical details on page 207

Proxy/live streaming formats

The proxy files and streams created by a K2 Summit/Solo system conform to industry standards, as follows.

Video: MPEG-4 Part 2

Format	Frame Rate	Data Rate (Mbps)	Other
320x240p	29.97, 25	1.5 Mbps	GOP 1 second
384x288p	29.97, 25	1.5 Mbps	GOP 1 second
512x288p	29.97, 25	1.5 Mbps	GOP 1 second

Audio: MPEG-4 Part 3 AAC-LC, 64 kbps, 48 kHz

Proxy file: MPEG-4 Part 12 Fragmented MP4 Movie

Live streaming: SDP files and RTP/RTCP streams are compliant with the following RFCs:

- RFC 3350, RFC 4566, RFC 3016, RFC 3640, RFC 5484, MPEG-4 Part 8

Configuring proxy and live streaming settings

On the K2 Summit/Solo system, configure proxy and live streaming settings as in the following sections. For complete information about proxy and live streaming, refer to related topics in this document.

Enable proxy files

1. In AppCenter, click **File | System | Configuration**.
   Configuration Manager opens.
2. In Configuration Manager, click the **Channel** tab.
3. Select a channel.
4. In Proxy Setup settings, set **Record proxy files** to **Yes**.
5. Select the audio included in the proxy file as follows:
   - Select the first audio input pair to include in the proxy file.
   - Select the number of audio inputs to include in the proxy file.

   The K2 Summit system includes audio pairs beginning with the first pair selected and then each subsequent audio pair up to the selected number of audio inputs.
6. If you want to the K2 Summit system to automatically detect scene changes and include them in the proxy file, do the following:
   - Set **Detect scenes** to **Yes**.
   - Select a minimum scene length. This is the length of time the K2 Summit/Solo system waits after detecting a scene change to begin attempting to detect the next scene change.
7. Select another channel and configure as desired.
8. Click **OK** to apply the settings.

Enable live streaming

1. In AppCenter, click **File | System | Configuration**.
   Configuration Manager opens.
2. In Configuration Manager, click the **Channel** tab.
3. Select a channel.
4. In Proxy Setup settings, set **Live network streaming** to **Yes**.
5. Select the audio input pair to include in the proxy stream.
6. Select another channel and configure as desired.
7. Click **OK** to apply the settings.

Configure live streaming multicast

This task describes using AppCenter to configure multicast settings. You can also use the K2Config application to configure multicast settings on SAN-attached K2 Summit systems. Refer to related topics in this document.

1. In AppCenter, click **File | System | Configuration**.

   Configuration Manager opens.

2. In Configuration Manager, click the **System** tab.

   These setting apply to all channels on the K2 Summit system.

3. In Proxy Setup settings, select the multicast IP base.

   The K2 Summit system applies channel-specific IP addresses from this base.

   Your choices are constrained to those specified by IANA for multicast.

4. Select the multicast port base.

   This is the first UDP port address for elementary streams.

5. Click **OK** to apply the settings.

Configure live streaming multicast using K2Config

Before doing this task, make sure that the SAN-attached K2 Summit systems are in a state as follows:

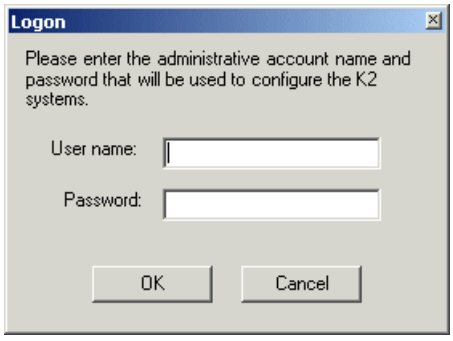
- Media access is stopped
- The K2 Summit system is not being used
- If a K2 Summit system with K2 software version lower than 9.0, the write filter is disabled

This task required a restart.

You can use the K2Config application to configure multicast settings on all the K2 Summit systems attached to a K2 SAN. Refer to related topics in this document for live streaming technical details.

1. On the PC that hosts K2Config, open the K2Config application.

   A login dialog box opens.

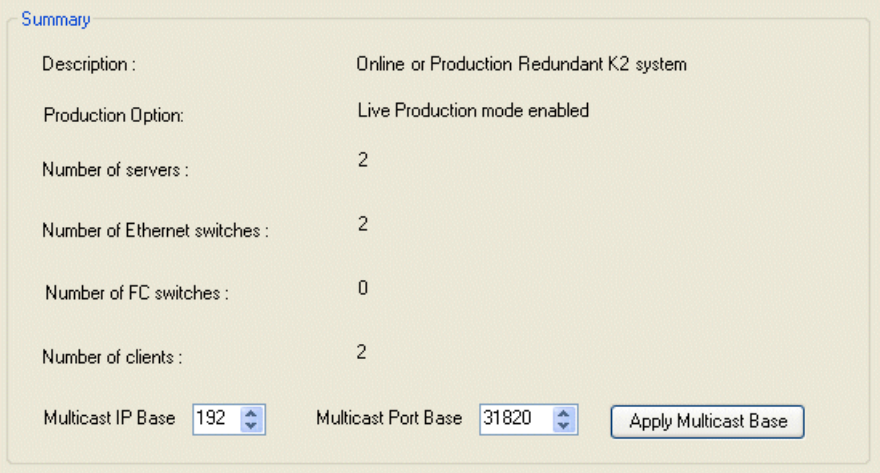


2. Log in to the K2Config application with the administrator account.

   The K2Config application opens.

3. If a K2 Summit system with K2 software version lower than 9.0, in the K2Config application tree view, select each K2 Summit system attached to the K2 SAN and verify that the **Write Filter Enabled** setting shows that the write filter is not enabled on the K2 Summit system.
4. In the K2Config application tree view, select the name of the K2 SAN, which is the top node of the storage system tree.

   The SAN summary information is displayed.



5. Select the multicast IP base.

   The K2 Summit system applies channel-specific IP addresses from this base.

   Your choices are constrained to those specified by IANA for multicast.
6. Select the multicast port base.

   This is the first UDP port address for elementary streams.
7. Click **Apply Multicast Base** to apply the settings.
8. When prompted, confirm your change and the restart of the K2 Summit systems.

The multicast settings are applied to all K2 Summit system attached to the K2 SAN.

Test proxy media generation

This test is valid for standalone K2 Summit systems. You can check the proxy media that the K2 Summit system generates. This can be helpful in troubleshooting situations where you need to verify that the proxy is available to other applications, such as the STRATUS application.

Use this procedure for test purposes only. Accessing proxy media as explained in this procedure is not supported for operational use.

1. Verify that in K2 AppCenter Configuration Manager, a K2 Summit system channel is enabled for live network streaming and for recording proxy files.
2. Verify that there is video available at the channel's SDI input.

3. Verify proxy live network streaming as follows:
   a) On the K2 Summit system, navigate to *V:\live streaming*.
   b) Identify the file that corresponds to the channel enabled for live network streaming.
      The file name is *hostname_Cx,sdp*, where *x* is the channel number.
   c) Double-click the file that corresponds to the channel enabled for live network streaming.
      QuickTime Player opens.
   d) View and verify the proxy video stream.
4. Verify recording proxy files as follows:
   a) Navigate to the proxy location.
      On a K2 Summit system that has not been configured to write proxy elsewhere, the location is *V:\proxy*. If configured by applications such as STRATUS to write proxy elsewhere, navigate to the configured location.
   b) While viewing the proxy location, start recording a new clip on the K2 Summit channel enabled for recording proxy files.
      The K2 Summit system creates a new folder at the proxy location. The folder is named with a long GUID.
   c) Stop the recording on the K2 Summit channel.
   d) In the new folder, double-click the *proxy.mp4* file.
      QuickTime Player opens.
   e) View and verify the proxy file.

Proxy/live streaming technical details

The K2 Summit system writes proxy files to the proxy location specified in the STRATUS Control Panel application. On the specified device the location is *V:\proxy*. For each clip recorded, the K2 system creates a directory and names it with the asset GUID, which is a long, unique string of characters. These directory names do not correspond to clip names or other human readable information. The directory contains the proxy files, which include the proxy video and audio files, as well as thumbnails files and a scene change file. The proxy video file is a fragmented MPEG-4 file. For test purposes, you can open the *proxy.mp4* file in a video player application that supports fragmented MPEG-4.

The K2 Summit system multicasts the low-resolution live stream using Real-time Transport Protocol, with UDP ports for the MPEG video with timecode and UDP ports for audio tracks, as defined by the Session Description Protocol (SDP). For each channel, the K2 system generates a **.sdp* file that contains the streaming media initialization parameters. The K2 system updates the file whenever you change the live streaming configuration. You can find these files on the K2 system at *V:\live streaming*. For test purposes, you can open a file in a text editor and read the IP addresses and ports assigned to the multicast session and other configuration information for the stream.

The K2 Summit system generates for each of its channels the specific live streaming network ports and IP addresses based on a port base and an IP address base. The port base is the first UDP port address for elementary streams. The IP address base is the first two octets in the IP address, as specified by the Internet Assigned Numbers Authority (IANA). By default, the port base is 31820

and the IP address base is 239.192.0.0. With these default bases, the range of network ports is UDP 31820 to 31827 , and the range of IP addresses is 239.192.x.x to 239.195.x.x. Grass Valley recommends that you use these default settings. However, if necessary for your site's network policies, you can also change the K2 system's default settings. You can configure the port base and the IP address base. Only IP addresses specified by IANA for multicast are allowed. Do not attempt to edit the `*.sdp` files, as the K2 system generates them automatically whenever the system is restarted. If you change the IP address of the K2 system, you must restart in order to update the IP address in the `*.sdp` file.

The K2 Summit system hosts a simple web server over which it delivers the live stream via HTTP. For test purposes, you can access the live stream by entering a URL of the following convention in a standard web browser:

`http://<httpservername>/live/<k2systemname>_<Cn>.sdp`

For example, to view the live stream from channel four on a K2 system named Summit01, the URL is `http://Summit01/live/Summit01_C4.sdp`. The http server name is the same as the name of the K2 system.

Related Topics

About proxy/live streaming on page 202

Appendix **A**

Remote control protocols

This section contains the following topics:

About remote control protocols

This section provides information for using remote control protocols to operate K2 Summit/Solo systems. It is intended for use by installers, system integrators, and other persons responsible for setting up automation systems at a customer site.

For information about configuring AppCenter to enable protocol control of a K2 channel, refer to topics in "K2 AppCenter User Manual".

Using AMP protocol to control K2 systems

Advanced Media Protocol (AMP) is an extension of the Odetics protocol.

AMP commands are available via Ethernet or RS-422 serial ports.

The automation setting for preroll should be at least 10 frames.

Preroll is 1 second for mixed compression format playout. Preroll is 10 frames for same compression format playout.

The AMP's socket interface uses IANA assigned port number 3811 for TCP.

In AppCenter, you must set a channel's options to enable protocol control of the channel. Subsequently, when the K2 Summit/Solo system starts up, the channel is immediately available for protocol control. Manual log on is not required.

For channels in gang mode, the protocol must connect to the lowest numbered channel in the gang. This is required to support jog/shuttle of ganged channels.

AMP Two-Head Player Model

The AMP protocol supports the use of a *two-head player model* in that two clips can be loaded for playout, as follows:

- Current clip — The AMP "preset id" is the active clip.
- Preview clip — The AMP "preview preset id" is the preview clip. The preview clip becomes the current clip and begins playing when the current clip completes. When controlling AMP in Auto mode, the "in preset" (and "out preset") command should be sent before the Preview in commands.

Related specifications are as follows:

- A 3D/Video+Key player channel does not support a two-head player model.

Controlling transfers with AMP

Remote control automation applications can initiate transfers via AMP. The AMP command must be sent to the K2 Summit/Solo system, not the K2 Media Server. This applies to both stand-alone and shared storage K2 systems.

If using AMP to initiate transfers between K2 systems and Profile XP systems, you must send the AMP command to the K2 system, not the Profile XP system. Transfers (both push and pull) are

successful if the K2 system hosts the command. Transfers fail if the Profile XP system hosts the command.

Transfers initiated by AMP between K2 systems and M-Series iVDRs are not supported.

AMP channel designations

When using AMP protocol with Ethernet and the K2 Summit/Solo system, the first port maps to the first channel, the second port maps to the second channel, and so on.

AMP internationalization

AMP supports UTF-8 2 and 3 byte characters. Unicode movie names pass through as opaque bits.

Using VDCP protocol to control K2 systems

Video Disk Control Protocol (VDCP) commands are available via RS-422 serial ports.

Preroll is 1 second for mixed compression format playout. Preroll is 10 frames for same compression format playout.

The K2 AppCenter Recorder application in protocol mode allows a default bin to be assigned to each record channel.

In AppCenter, you must set a channel's options to enable protocol control of the channel. Subsequently, when the K2 Summit/Solo system starts up, the channel is immediately available for protocol control. Manual log on is not required.

For channels in gang mode, the protocol must connect to the lowest numbered channel in the gang. This is required to support jog/shuttle of ganged channels.

Loop-play mode on the K2 Summit/Solo system is not supported under VDCP control.

The following categories of VDCP commands are not supported:

- Deferred (Timeline) Commands --these are the basic timeline commands but use the time specified by the PRESET STANDARD TIME
- Macro commands
- Archive Commands
- To control a given K2 channel, use only that channel's specific RS-422 rear panel connector. Send the VDCP "Open Port" and "Select Port" commands only to the RS-422 connector that is associated with the channel being controlled.

VDCP two-head player model

The VDCP protocol supports the use of a *two-head player model* in that two clips may be loaded for playout, as follows:

- Current clip — The VDCP "preset id" is the current clip.

- Preview clip — The VDCP "preview preset id" is considered the preview clip. When a play command is received, the preview clip becomes the active clip and begins playing after the preroll time has passed. If a play command has not been issued by the end of the clip, playout stops according to the VDCP end mode settings for that channel (last frame, black, first frame of preview clip).

Related specifications are as follows:

- A 3D/Video+Key player channel does not support a two-head player model.

Controlling transfers with VDCP

Remote control automation applications can initiate transfers via VDCP. The VDCP command must be sent to the K2 Summit/Solo system, not the K2 Media Server. This applies to both stand-alone and shared storage K2 Summit/Solo system.

If you are using VDCP to perform video network transfers, you must configure the K2 Summit/Solo system so that there is a unique Controller ID for each host.

If using VDCP to initiate transfers between K2 systems and Profile XP systems, you must send the VDCP command to the K2 system, not the Profile XP system. Transfers (both push and pull) are successful if the K2 system hosts the command. Transfers fail if the Profile XP system hosts the command.

Transfers initiated by VDCP between K2 systems and M-Series iVDRs are not supported.

VDCP internationalization

VDCP does not support UTF-8 or Unicode, so use ASCII only for clip names and bin names.

PitchBlue workflow considerations

The K2 Summit system supports the H.264 format used in the PitchBlue workflow. However, you must consider the intended PitchBlue workflow when using this H.264 media, as it is not supported for general purpose use outside of the PitchBlue workflow.

The K2 Summit system ingests the PitchBlue material without any error correction. The material often has anomalies, such as a broken last frame, that the K2 Summit system accepts as-is. When PitchBlue plays out this material under VDCP automation control, it plays the known-good material only. PitchBlue determines where the anomalies exist and makes sure that they are not played out. In this way PitchBlue avoids the errors that would otherwise occur if the material were used for general purpose playout without PitchBlue control.

Therefore, you must adhere to the complete PitchBlue workflow from ingest through playout for all PitchBlue material. Do not attempt to play out PitchBlue material except as part of the prescribed PitchBlue workflow. Playing out PitchBlue material in any other way can cause errors.

Using BVW protocol to control K2 systems

BVW commands are available via RS-422 serial ports.

A subset of BVW commands is supported through AppCenter in protocol mode.

Insert/Edit is not supported.

In AppCenter, you must set a channel's options to enable protocol control of the channel. Subsequently, when the K2 Summit/Solo system starts up, the channel is immediately available for protocol control. Manual log on is not required.

For channels in gang mode, the protocol must connect to the lowest numbered channel in the gang. This is required to support jog/shuttle of ganged channels.

To set in and out points with BVW protocol, load clips only from the working bin.

Special considerations for automation vendors

The following information is provided for your convenience as you set up your chosen automation product to control K2 systems. Consult your automation vendor for complete information.

Harris settings

The Harris automation product uses VDCP protocol.

The following settings are required for the Harris automation product:

Setting	Mixed compression format playout	Same compression format playout	Comments
Disk Prerolls	1 second	10 frames	—
Frames to send Play early (Preroll Play)	1 second	10 frames	These two settings should be the same as the Disk Prerolls setting. However, if there is extra fixed latency in your RS-422 communication path, you might need to adjust the settings differently.
Frames to send Record early (Preroll Record)	1 second	10 frames	
Disk Port Comm Timeout	60 frames	60 frames	This is the minimum required by K2. Do not use the Harris default value, which is 10.
Back To Back Rec	Unchecked	Unchecked	K2 does not support this feature.

RS-422 protocol control connections

You can control the K2 Summit/Solo system with remote control devices and software developed for the K2 system that use industry-standard serial protocols: AMP, BVW, and VDCP. (AMP

protocols can also use Ethernet connections.) You can connect one RS-422 cable to each channel. Each RS-422 connection controls the channel to which it is connected only. Connect the RS-422 cabling as required, then refer to topics in "K2 AppCenter User Manual" to configure the K2 system for remote control.

Specifications for the RS-422 connection are as follows:

- Data Terminal Equipment (DTE)
- 38.4K Baud
- 1 Start bit
- 8 Data bits
- 1 Parity bit
- 1 Stop bit

Security and protocol control

The K2 security features can be configured to restrict protocol control of channels.

Related Topics

Protocol control of channels and media access security on page 180

Appendix **B**

Specifications

This section contains the following topics:

K2 Summit transmission models specifications

Refer to the section about K2 Summit Transmission models for specifications unique to that system. If a specification is not unique to a K2 Summit Transmission model, then the general K2 Summit/Solo system specification found in this section applies.

Related Topics

K2 Summit Transmission models on page 197

AC power specification

Table 4: K2 Summit 3G AC power specification

Characteristic	Specification
Power supply	Dual, redundant
Mains Input Voltage	90 to 260V auto-range, 47-63Hz
Power consumption	450W typical (standalone) 390W typical (SAN client) Maximum AC current 8A @ 115VAC, 4A @ 230VAC

The specification is shown in the following table.

Table 5: First-generation K2 Summit AC power specification

Characteristic	Specification
Power supply	Dual, redundant
Mains Input Voltage	90 to 260V auto-range, 47-63Hz
Power consumption	350W typical (standalone) 300W typical (SAN-attached) Maximum AC current 7A @ 115VAC, 3.5A @ 230VAC

The specification is shown in the following table.

Table 6: First-generation K2 Solo and K2 Solo 3G Media Server AC power specification

Characteristic	Specification
Power supply	Single
Mains Input Voltage	100-240V, 50/60 Hz
Power consumption	180W typical Maximum AC current 4A @ 115VAC, 2A @ 230VAC

⚠ ***WARNING: Always use a grounded outlet to supply power to the system. Always use a power cable with a grounded plug, such as the one supplied with the system.***

Environmental specifications

The K2 Summit 3G system specification is shown in the following table:

Characteristic	Specification
Ambient Temperature Non-Operating	-40° to +60° C
Ambient Temperature Operating	10° to +40° C
Relative Humidity	Operating 20% to 80% from 10° to +40° C Non-Operating 10% to 85% from -30° to +55° C Do not operate with visible moisture on the circuit boards
Operating Altitude	To 10,000 feet IEC 950 compliant to 2000 meters
Storage Altitude	To 40,000 feet
Non-Operating Mechanical Shock	30G 11 ms trapezoid
Random Vibration Operational	0.27 GRMS (5-500Hz)
Random Vibration Non-Operational	2.38 GRMS overall .019 g2/Hz (5-100Hz) .009 g2/Hz (200-350Hz) .0065 g2/Hz (500 Hz)
Equipment Type	Information Technology
Equipment Class	Class 1
Installation Category	Category II Local level mains, appliances, portable equipment, etc.
Pollution Degree	Level 2 operating environment, indoor use only.

The first generation K2 Summit/Solo system specification is shown in the following table:

Characteristic	Specification
Ambient Temperature Non-Operating	-40° to +60° C
Ambient Temperature Operating	10° to +40° C

Characteristic	Specification
Relative Humidity	Operating 20% to 80% from 10° to +40° C Non-Operating 10% to 80% from -30° to +60° C Do not operate with visible moisture on the circuit boards
Operating Altitude	To 10,000 feet IEC 950 compliant to 2000 meters
Storage Altitude	To 40,000 feet
Non-Operating Mechanical Shock	30G 11 ms trapezoid
Random Vibration Operational	0.27 GRMS (5-500Hz)
Random Vibration Non-Operational	2.38 GRMS overall .0175 g2/Hz (5-100Hz) .009375 g2/Hz (200-350Hz) .00657 g2/Hz (500 Hz)
Equipment Type	Information Technology
Equipment Class	Class 1
Installation Category	Category II Local level mains, appliances, portable equipment, etc.
Pollution Degree	Level 2 operating environment, indoor use only.

Specifications vary for transmission products.

Related Topics

K2 Summit Transmission models requirements and restrictions on page 200

Mechanical specifications

The K2 Summit 3G Production Client specification is shown in the following table

Dimension	Measurement
Height	3.5 in (89mm)
Width	17.6 in (447 mm)
Depth [1]	24.3 in (617 mm) total 23.0 in (585 mm) rack depth
Weight:	55.0 lbs (25.0 kg) maximum

The first generation K2 Summit Production Client specification is shown in the following table

[1] Adjustable rack-mounting ears accommodate different rack depth limitations.

Dimension	Measurement
Height	3.5 in (89mm)
Width	17.6 in (447 mm)
Depth [2]	24.3 in (617 mm) total 23.0 in (585 mm) rack depth
Weight:	53.0 lbs (24.0 kg) maximum

The K2 Solo Media Server specification is shown in the following table

Dimension	Measurement
Height	3.5 in (89mm)
Width	8.25 in (210 mm)
Depth	17.7 in (446 mm)
Weight:	16.5 lbs (7.5 kg)

Electrical specifications

The following sections describe the electrical specifications:

Serial Digital Video (SDI)

The K2 Summit/Solo system specification is shown in the following table

Parameter	Specification
Video Standard	SD: 525 Line or 625 Line component HD: 720p or 1080i
Number of Inputs	1 per channel standard. 2 or 3 per channel when licensed for ChannelFlex Suite.
Number of Outputs	2 per channel
Data format	Conforms to SMPTE 259M (SD) and 292M (HD)
Number of bits	10bits
Embedded Audio Input	SD data format conforms to SMPTE 259M (48kHz, 20bits) HD data format conforms to SMPTE 299 48 kHz (locked to video) and 16- or 24- bit PCM Compatible with AC-3 and Dolby-E
Embedded Audio Output	Output data format is 48 kHz 24-bit User can disable embedded audio on SDI output

[2] Adjustable rack-mounting ears accommodate different rack depth limitations.

Parameter	Specification
Connector	BNC, 75 ohm, No loop-through
nominal Amplitude	800mV peak-to-peak terminated
DC Offset	0 +0.5V
Rise and Fall Times	SD: 400 - 1500ps; measured at the 20% and 80% amplitude points HD: less than 270ps
Jitter	less than 0.2UI peak-to-peak
Max Cable Length	SD 300 meters HD 125 meters
Return Loss	greater than or equal to 15db, 5Mhz to 1.485Ghz

Genlock Reference

The K2 Summit/Solo system specification is shown in the following table:

Characteristic	Description
Signal Type	NTSC/PAL Color Black Composite Analog
Connectors	2 BNC, 75 ohm passive loop through
Signal Amplitude Lock Range	Stays locked to +6 dB and -3 dB
Input Return Loss	Greater than or equal to 36 dB to 6MHz
Tri-level sync	Supported

System Timing

The K2 Summit/Solo system specification is shown in the following table. All delay values shown are relative to Black Reference.

Characteristic	Description
Encoder timing	Derived from the video input
Nominal Playback Output Delay	Adjustable (Default: Zero timed to reference genlock)
SD Output Delay Range (Independent for each play channel)	525 lines • Frames: 0 to +1 • Lines: 0 to +524 • Samples: 0 to +1715 clock samples

Characteristic	Description
	625 lines • Frames: 0 to +3 • Lines: 0 to +624 • Samples: 0 to +1727 clock samples
HD Output Delay Range (Independent for each play channel)	1080i at 29.97 FPS (SMPTE 274M-5) • Frames: 0 to +1 • Lines: 0 to +1124 • Pixels: 0 to +2199
	720p at 59.94 FPS (SMPTE 296M-2) • Frames: 0 to +1 • Lines: 0 to +749 • Pixels: 0 to +1649
	1080i at 25 FPS (SMPTE 274M-6) • Frames: 0 to +1 • Lines: 0 to +1124 • Pixels: 0 to +2639
	720p at 50 FPS (SMPTE 296M-3) • Frames: 0 to +1 • Lines: 0 to +749 • Pixels: 0 to +1979
Loop through/EE	The video, AES, and LTC inputs pass to the output connectors as loop through.

AES/EBU Digital Audio

The K2 Summit/Solo system specification is shown in the following table

Parameter	Specification
Standard	AES3
Audio Inputs	4 Channels per video input/output on DB-25. Supports 32 KHz to 96 KHz inputs, which are sample rate converted to 48 KHz, 16 bit, 20 bit, or 24 bit digital audio sources.

Parameter	Specification
Audio Outputs	4 Channels per video output. Audio mapping is direct and fixed. AES outputs are active at all times. Audio is output using a 48kHz clock derived from the video reference. Supports 16- or 24-bit media. On playout, audio is synchronized with video as it was recorded. Compatible with AC-3 and Dolby-E
Input Impedance	110 ohms, balanced
Audio time shift	Configurable relative to video for both record and playout.

LTC Input/Output

The K2 Summit/Solo system specification is shown in the following table

Parameter	Specification
Standard	SMPTE 12M Longitudinal Time Code, AC coupled, differential input
Number of Inputs	1 per video input - Shared 6 pin conn. with output
Number of Outputs	1 per video output
Input Impedance	1K ohm
Output Impedance	110 ohm
Minimum Input Voltage	0.1 V peak-to-peak, differential
Maximum Input Voltage	2.5 V peak-to-peak, differential
Nominal Output Voltage	2.0 V peak-to-peak differential.
LTC Reader	LTC reader will accept LTC at rates between 1/30 and 80 times the nominal rate in either forward or reverse directions.
LTC Transmitter	LTC transmitter outputs LTC at the nominal frame rate for the selected standard at 1x speed, forward direction only.

VITC Input/Output

The K2 Summit/Solo system specification is shown in the following table.

Parameter	Specification
VITC waveform	lines 10-20 NTSC (525 Line); lines 10-22 PAL (625 Line) VITC is decoded on each SDI input and inserted on each SDI output. VITC Reader configurable for a search window (specified by two lines) or set to manual mode (based on two specified lines). VITC Writer inserts VITC data on two selectable lines per field in the vertical interval. The two lines have the same data. VITC is not decoded off of the video reference input.

RS-422 specification K2 Summit 3G system

The RS-422 interface conforms to ANSI/SMPTE 207M-1997 standard (SMPTE 422).

The K2 Summit/Solo system specification is shown in the following table.

Characteristic	Description
Number of Inputs/Outputs	1 per channel
Connector type	Female RJ45

RS-422 specification first generation K2 Summit/Solo system

The RS-422 interface conforms to ANSI/SMPTE 207M-1997 standard (SMPTE 422).

The K2 Summit/Solo system specification is shown in the following table.

Characteristic	Description
Number of Inputs/Outputs	1 per channel
Connector type	Female DB9 pin

GPI I/O specifications

The K2 Summit/Solo system specification is shown in the following table.

Characteristic	Description
Number of Inputs/Outputs	12 inputs and 12 outputs.
Connector type	Female DB 25pin
GPI Input	TTL 0-0.8 V Low; 2.4-5 V High; 1 mA external current sink

Characteristic	Description
GPI Output	Max Sink Current: 100 mA; Max Voltage: 30 V Outputs are open drain drivers. Max. voltage when outputs are open = 45V Max. current when outputs are closed = 250mA Typical rise times approximately 625ns Typical fall times approximately 400ns

Operational specifications

This section contains specifications related to media operations.

Related Topics

Video codec description K2 Summit/Solo on page 224
Playout of multiple formats on page 227
Active Format Description (AFD) specifications on page 230
VBI/Ancillary/data track specifications on page 235
Internationalization on page 240
Limitations for creating and naming assets and bins on page 241
Video network performance on page 243
About file interchange mechanisms on K2 systems on page 243
Media file system performance on K2 systems on page 251
Transition effects formats and limitations on page 252
Protocols supported on page 253
Transfer compatibility with K2 Summit/Solo on page 253
Control Point PC system requirements on page 255

Video codec description K2 Summit/Solo

First generation K2 Summit Production Client, K2 Summit 3G Production Client, and K2 Solo Media Server specifications are shown in the following tables. Licenses and/or hardware options are required to enable the full range of specifications.

DV formats

Format	Sampling	Frame Rate	Data Rate	Other
DVCAM 720x480i 720x576i	4:1:1/4:2:0	29.97, 25	28.8 Mbps	Conforms to IEC 61834

Format	Sampling	Frame Rate	Data Rate	Other
DVCPRO25 720x480i 720x576i	4:1:1	29.97, 25	28.8 Mbps	Conforms to SMPTE 314M
DVCPRO50 720x487.5i 720x585i	4:2:2	29.97, 25	57.6 Mbps	Conforms to SMPTE 314M
DVCPRO HD 1280x1080i 1440x1080i	4:2:2	29.97, 25	100 Mbps	Conforms to SMPTE 370M
DVCPRO HD 960x720p	4:2:2	59.94, 50	100 Mbps	Conforms to SMPTE 370M

MPEG-2 formats

Format	Sampling	Frame Rate	Data Rate (Mbps)	Other
720x480i	4:2:0	29.97	2-15	I-frame and long GoP
720x480i	4:2:2	29.97	4-50	I-frame and long GoP
720x512i	4:2:2	29.97	4-50	I-frame and long GoP
720x576i	4:2:0	25	2-15	I-frame and long GoP
720x576i	4:2:2	25	4-50	I-frame and long GoP
720x608i	4:2:2	25	4-50	I-frame and long GoP
D10/IMX 720x512i	4:2:2	29.97	30, 40, 50 CBR	I-frame only
D10/IMX 720x608i	4:2:2	25	30, 40, 50 CBR	I-frame only
1920x1080i	4:2:0	29.97, 25	20-80	I-frame and long GoP[3]
1920x1080i	4:2:2	29.97, 25	20-100	I-frame and long GoP
XDCAM-HD 1440x1080i	4:2:0	29.97, 25	18 VBR, 25 CBR, 35 VBR	Long GoP
XDCAM-HD422 1920x1080i	4:2:2	29.97, 25	50 CBR	Long GoP

[3] Decode of lower bit rate is possible

Format	Sampling	Frame Rate	Data Rate (Mbps)	Other
XDCAM-HD422 1280x720p	4:2:2	59.94, 50	50 CBR	Long GoP
XDCAM-EX 1920x1080i	4:2:0	29.97, 25	35 VBR	Long GoP
XDCAM-EX 1280x720p	4:2:0	59.94, 50	25 CBR, 35 VBR	Long GoP

K2 systems record closed GoP structure. If an open GoP clip is imported, it is fully supported, including trimming the clip, playout of the clip, using the clip in playlists, and exporting the clip.

AVC-Intra formats

Format	Sampling	Frame Rate	Data Rate	Other
AVC-Intra 50 1440x1080i	4:2:0	29.97, 25	50 Mbps	Requires licenses or hardware for support on different K2 Summit/Solo system models.
AVC-Intra 50 960x720p	4:2:0	59.94, 50	50 Mbps	
AVC-Intra 100 1920 x 1080i	4:2:2	29.97, 25	100 Mbps	
AVC-Intra 100 1280 x 720p	4:2:2	59.94, 50	100 Mbps	

Related Topics

K2 Summit/Solo formats, models, licenses, and hardware support on page 33

AVCHD/H.264 formats

The following formats are for AVCHD and PitchBlue content. These are only supported for play output (decode) on AVCHD. A license is required. Record input (encode) is not supported.

Format	Sampling	Frame Rate	Data Rate	Other
720x480i	4:2:0	29.97	4-50	H.264-style open GoP. GoP length up to 30 frames. Up to 4 B-frames between anchor frames.
	4:2:2	29.97	4-50	
720x512i	4:2:2	29.97	4-50	
720x576i	4:2:0	25	4-50	
	4:2:2	25	4-50	
720x608i	4:2:2	25	4-50	

Format	Sampling	Frame Rate	Data Rate	Other
1920x1080i	4:2:0	29.97, 25	24 Mbps max.	
	4:2:2	29.97, 25	24 Mbps max.	
1440x1080i	4:2:0	29.97, 25	24 Mbps max.	
	4:2:2	29.97, 25	24 Mbps max.	
1280x720p	4:2:0	59.94, 50	24 Mbps max.	
	4:2:2	59.94, 50	24 Mbps max.	

Related Topics

K2 Summit/Solo formats, models, licenses, and hardware support on page 33

Proxy/live streaming formats

The proxy files and streams created by a K2 Summit/Solo system conform to industry standards, as follows.

Video: MPEG-4 Part 2

Format	Frame Rate	Data Rate (Mbps)	Other
320x240p	29.97, 25	1.5 Mbps	GOP 1 second
384x288p	29.97, 25	1.5 Mbps	GOP 1 second
512x288p	29.97, 25	1.5 Mbps	GOP 1 second

Audio: MPEG-4 Part 3 AAC-LC, 64 kbps, 48 kHz

Proxy file: MPEG-4 Part 12 Fragmented MP4 Movie

Live streaming: SDP files and RTP/RTCP streams are compliant with the following RFCs:

- RFC 3350, RFC 4566, RFC 3016, RFC 3640, RFC 5484, MPEG-4 Part 8

Playout of multiple formats

The K2 Summit/Solo system automatically handles material of various types and formats as specified in the following sections:

Playout on K2 Summit/Solo

For a given frame rate, you can play SD clips of any format back-to-back on the same timeline. Both 16:9 and 4:3 SD aspect ratio formats can be played on the same timeline. Refer to video codec description earlier in this section for a list of the supported formats.

On channels with the XDP (HD) license, for similar frame rates (25/50 fps or 29.97/59.95 fps), SD material transferred or recorded into the K2 Summit/Solo system along with its audio is up-converted when played on a HD output channel. Likewise, HD material is down-converted along with its audio when played on an SD output channel. HD and SD clips can be played back-to-back on the same timeline, and aspect ratio conversion is user configurable.

The K2 Summit/Solo system supports mixed clips with uncompressed and compressed (PCM, AC3, and Dolby) audio on the same timeline.

Related Topics

Aspect ratio conversions on HD K2 client on page 228

25/50 fps conversions on HD K2 Summit/Solo system models

The following specifications apply to K2 Summit/Solo system channels with the XDP (HD) license.

		Converted SD format	Converted HD format	Converted HD format
		625 at 25 fps	**1080i at 25 fps**	**720p at 50 fps**
Source SD format	**625 at 25 fps**	No conversion	Up-convert SD to HD	Up-convert SD to HD
Source HD format	**1080i at 25 fps**	Down-convert HD to SD	No conversion	Cross-convert from 1080i to 720p
	720p at 50 fps	Down-convert HD to SD	Cross-convert from 720p to 1080i	No conversion

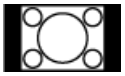
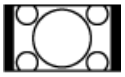
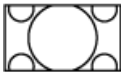
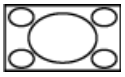
29.97/59.95 fps conversions on HD K2 Summit/Solo system models

The following specifications apply to K2 Summit/Solo system channels with the XDP (HD) license.

		Converted SD format	Converted HD format	Converted HD format
		525 at 29.97 fps	**1080i at 29.97 fps**	**720p at 59.94 fps**
Source SD format	**525 at 29.97 fps**	No conversion	Up-convert SD to HD	Up-convert SD to HD
Source HD format	**1080i at 29.97 fps**	Down-convert HD to SD	No conversion	Cross-convert HD to HD
	720p at 59.94 fps	Down-convert HD to SD	Convert HD to HD	No conversion

Aspect ratio conversions on HD K2 client

The following specifications apply to K2 Summit/Solo system channels with the XDP (HD) license.

Source aspect ratio	Source image	Conversion option	Conversion description	Converted aspect ratio	Converted image
4:3		Bar	The 4:3 aspect ratio is maintained, centered on the screen, with black bars filling the left and right portions of the 16:9 display.	16:9	
		Half Bar	The picture aspect ratio is maintained, but the image is slightly enlarged. The top and bottom of the image are slightly cropped, and thin black bars fill the left and right portions of the 16:9 display.	16:9	
		Crop	The picture aspect ratio is maintained, but the image is enlarged so that it horizontally fills the HD display. The top and bottom of the 4:3 SD image are cropped to fit in the 16:9 display.	16:9	
		Stretch	The picture aspect ratio is distorted. The image fills the screen vertically without cropping, and is stretched horizontally to fill the 16:9 display. This conversion up-converts Full Height Anamorphic (FHA) 16:9 SD material.	16:9	
16:9		Bar	The 16:9 aspect ratio is maintained, centered on the screen, with black bars filling the top and bottom portions of the 4:3 display.	4:3	
		Half Bar	The picture aspect ratio is maintained, but the image is slightly enlarged. The left and right sides the image are slightly cropped, and thin black bars fill the top and bottom portions of the 4:3 display.	4:3	
		Crop	The picture aspect ratio is maintained, but the image is enlarged so that it vertically fills the SD display. The left and right sides of the 16:9 HD image are cropped to fit in the 4:3 SD display	4:3	
		Stretch	The picture aspect ratio is distorted. The image fills the screen horizontally without cropping, and is stretched vertically to fill the 4:3 display. This conversion generates Full Height Anamorphic (FHA) 16:9 SD material.	4:3	

Active Format Description (AFD) specifications

NOTE: This topic applies to K2 Summit/Solo systems.

Active Format Description (AFD) settings automatically determine the proper aspect ratio to use for up- and down-conversions, based on the AFD information embedded in the clip metadata. If no AFD was set on the incoming SDI input, you can assign the AFD setting in K2 AppCenter. A related setting, aspect ratio conversion (ARC), makes settings in K2 AppCenter on a clip-by-clip basis or per channel basis but does not embed settings in clip metadata.

About Active Format Description

The AFD is defined during production. By inserting metadata about the aspect ratio into the vertical ancillary data, AFD can define the aspect ratio of the signal as it progresses through ingest, editing, up/down conversion and playout. If the aspect ratio is altered during processing, then the AFD passed on downstream might need to be modified to ensure the correct aspect ratio is obtained.

NOTE: If ARC leads to unsupported active video format (postage stamp), the new AFD code will be the 'undefined' value of 0000.

The playback Aspect Ratio Conversion (ARC) is prioritized according to the following table:

Playback aspect ratio conversion priority	
1	Clip property (ARC or AFD-based conversion rules)
2	Output channel (ARC configuration property)

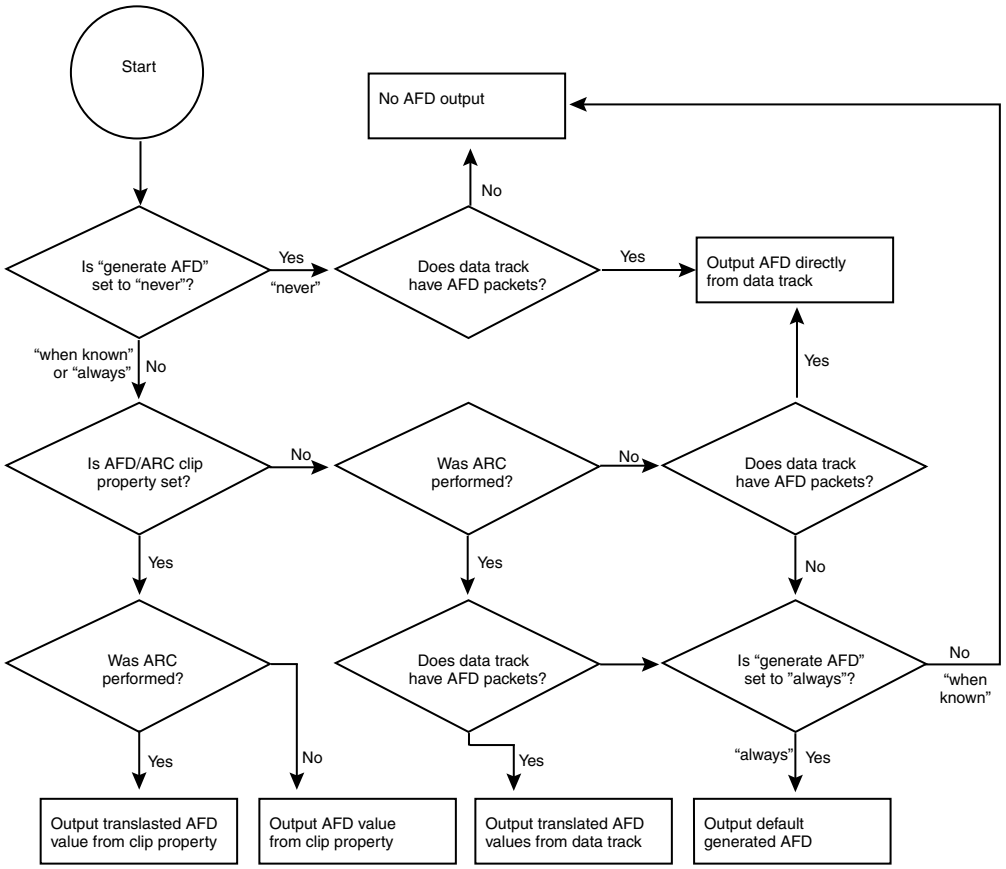
NOTE: Bar data is not supported on the K2 system.

Related Topics

AFD input/output settings

AFD output flowchart

The K2 Summit/Solo system determines AFD code values in output as illustrated by the following flowchart.



Storing AFD on K2 Summit/Solo systems

The K2 Summit/Solo system stores clip metadata in clip properties and uses this data throughout the workflow. You can modify the AFD setting in AppCenter.

You can store AFD in a data track. Grass Valley recommends selecting this for HD clips; if using SD, this is optional. This method takes more storage (it is approximately equal to four tracks of audio) but this method enables AFD and CC/Teletext support for HD.

Ingesting SDI

An SDI video signal stores AFD in the vertical ancillary data. The K2 Summit/Solo system processes the signal as follows:

- If present, the AFD setting from two seconds into the file is copied into the clip properties. This is the default K2 system behavior and occurs unless you set it to **No** in Configuration Manager.
- If selected, the ANC data is copied into the K2 data track.

Using AFD with file transfers

The following tables describe the AFD file priorities and the AFD behavior with GXF and MXF transfers.

File transfer AFD priority	
1	AFD from the MXF or GXF metadata is copied to the K2 clip properties.
2	If the MXF stream contains an ancillary data track with AFD ancillary data packets and Active Format Descriptor attribute of the Generic Picture Essence descriptor in the MXF header metadata is absent, then the AFD value for the K2 clip is derived from the AFD ancillary data packet located around 2 seconds into the material. That AFD value is then copied to the K2 clip properties.
3	If there is no AFD in the MXF, the GXF, or the data track, then no AFD is set.

GXF Export: (both AFD and ARC values inserted into XML of stream)	
Condition	**Description**
Exported to K2 system that does not support AFD	AFD setting is ignored, but setting is retained with clip ARC settings apply
Exported to K2 system that supports AFD	AFD overrides ARC settings

GXF Import	
Condition	**Description**
Imported from K2 system that does not support AFD	ARC converted to AFD
Imported from K2 system that supports AFD	AFD overrides ARC settings

MXF Export	
Condition	**Description**
AFD from clip property added to properties of the video in the header metadata	If clip property is not set, do not add property in stream
AFD from data track in stream's ancillary data	No change required

ARC is K2 specific and therefore not included in MXF transfers.

MXF Import	
Imported stream has AFD in the header metadata	AFD is stored in the clip property setting of the clip
Imported stream has AFD in the data track	AFD is stored in the clip property setting of the clip. (AFD is taken from the ancillary data two seconds from the beginning, or, if the clip is less than 2 seconds long, from the last valid AFD.)
Imported stream has no AFD	No AFD

ARC is K2 specific and therefore not included in MXF transfers.

Default generated AFD values

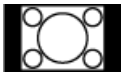
Default AFD values are generated when the three following conditions are met:

- The AFD output setting in the Configuration Manager is set to **Always**
- The clip does not have AFD in the data track, and
- The clip does not have AFD specified in its clip properties

Under these conditions, default AFD is generated and inserted, based on ARC performed and the source material format. Default generated AFD settings are described in the table below.

Default generated AFD values when up-converting to HD

Source image is presumed based on the conversion that has been selected.

Source aspect ratio	Presumed source image	Conversion option	Converted AFD and aspect ratio	Converted image
16:9 HD		No conversion	AFD = 1010 AR = 16:9 HD	
16:9 SD		Scale up Crop vertical	AFD = 1010 AR = 16:9 HD “crop”	
		Scale up	AFD = 1010 AR = 16:9 HD	
		Scale up Crop vertical Pillarbox	AFD = 1011 AR = 16:9 HD “half bars”	
4:3 SD		Scale up Pillarbox	AFD = 1011 AR = 16:9 HD “bars”	

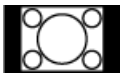
Default generated AFD values when down-converting to SD

Source image is presumed based on the conversion that has been selected.

Source aspect ratio	Presumed source image	Conversion option	Converted AFD and aspect ratio	Converted image
4:3 SD not widescreen		No conversion	AFD = 1001 AR = 4:3 SD	

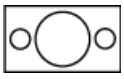
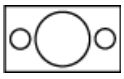
Source aspect ratio	Presumed source image	Conversion option	Converted AFD and aspect ratio	Converted image
16:9 SD widescreen		No conversion (only if ARC set to 'stretch')	AFD = 1010 AR = 16:9 SD	
16:9 HD		Scale down letterbox	AFD = 1010 AR = 4:3 SD "bars"	
		Scale down Crop horizontal	AFD = 1001 AR = 4:3 SD "crop"	
		Scale down	AFD = 1010 AR = 16:9 SD "stretch"	
		Scale down Crop horizontal Letterbox	AFD = 1011 AR = 4:3 SD "half bars"	

Supported conversions from SD to HD using AFD

Source AFD and aspect ratio	Source image	Conversion performed	Converted AFD and aspect ratio	Converted image
AFD = 1010 AR 4:3 SD		Scale up crop vertical	AFD = 1010 AR 16:9 HD	
AFD = 1000 or 1001 AR 4:3 SD		Scale up pillarbox	AFD = 1001 AR 16:9 HD	
AFD = 1010 AR 16:9 SD		Scale up	AFD = 1010[4] AR 16:9 HD	
AFD = 1011 AR = 4:3 SD		Scale up Crop vertical pillarbox	AFD = 1011 AR 16:9 HD	

[4] You can change the default converted value of AFD = 1010 to be AFD = 1001. This setting is in K2 AppCenter Configuration Manager play channel video settings.

Supported conversions from HD to SD using AFD

Source AFD and aspect ratio	Source image	Conversion performed	Converted AFD and aspect ratio	Converted image
AFD = 1000 or 1010 AR = 16:9		Scale down letterbox	AFD = 1010 AR = 4:3[5]	
AFD = 1001 AR = 16:9		Scale down crop horizontal	AFD = 1001 AR = 4:3	
AFD = 1010 AR = 16:9		Scale down	AFD = 1010 AR = 16:9[6]	
AFD = 1011 AR = 16:9		Scale down Crop horizontal letterbox	AFD = 1011 AR = 4:3	
AFD = 1111 AR = 16:9		Scale down crop horizontal	AFD = 1001 AR = 4:3	

VBI/Ancillary/data track specifications

This section contains topics about data carried in the media file.

VBI/Ancillary/data track definitions

Terms in this section are defined as follows:

Ancillary data	Ancillary data (ANC data) as specified in this section is primarily a means by which timecode, Closed Captioning, and Teletext information is embedded within the serial digital interface. Other Type 2 ancillary data packets are stored and played back without modification. Ancillary data is standardized by SMPTE 291M.
Closed Captioning (CC)	Line 21 NTSC Closed Captioning as defined in EIA-608 and used as a subset of EIA-708. EIA-708 has been updated and renamed to CEA-708. Includes other Line 21 services such as V-Chip.
Teletext (TT)	Teletext System B subtitles as defined ETSI EN 300 706 and other documents. The Australian standard for digital TV is Free TV Operational Practice OP-47. It has been ratified as SMPTE RDD 8.
Captioning	Denotes both NTSC Closed Captioning and Teletext subtitling.

[5] When play channel video settings Aspect Ratio is set to "Standard (4:3)"
[6] When play channel video settings Aspect Ratio is set to "Widescreen (16:9)"

Luma/Chroma VBI support on K2 Summit/Solo

Record and playout of VBI is supported for both Luma and Chroma. However, a given line of VBI data can be stored as either Luma or Chroma, but not both.

VBI data support on K2 Summit/Solo

The following table applies when in Configuration Manager, the Data Track settings are configured as:

- Record ancillary data: No

Or as:

- Record ancillary data: Yes
- Record Uncompressed VBI and captioning data to track: No

Use these Data Track settings to retain compatibility with legacy systems, such as the Profile XP Media Platform.

Video format	Compressed VBI	Uncompressed VBI	Captioning	Comments
DVCPRO25 525 line (NTSC)	Not supported	Not supported by DVCPRO25 format	CC supported, as native to DVCPRO25. VCHIP data supported.	—
DVCPRO25 625 line (PAL)	Not supported	Not supported by DVCPRO25 format	TT not supported as VBI data.	
DVCPRO50 525 line (NTSC)	Supported for playout	Not supported by DVCPRO50 format	CC supported, as native to DVCPRO50 (compressed VBI). VCHIP data supported.	—
DVCPRO50 625 line (PAL)	Supported for playout	Not supported by DVCPRO50 format	TT supported, as native to DVCPRO50 (compressed VBI).	—
DVCAM 525 line (NTSC)	Not supported	Not supported by DVCAM format	CC supported, as native to DVCAM.	—
DVCAM 625 line (PAL)	Not supported	Not supported by DVCAM format	TT not supported as VBI data.	—

Video format	Compressed VBI	Uncompressed VBI	Captioning	Comments
MPEG-2 525 line (NTSC)	Supported as 16 lines per field. Range: 7–22	Supported for record. Not supported for playout.	CC supported and always on. Not selectable.	—
MPEG-2 625 line (PAL)	Supported as 16 lines per field. Range: 7–22	Supported for record. Not supported for playout.	TT supported only as compressed or uncompressed VBI.	—
MPEG-D10 525 line (NTSC)	Supported	Not supported by D10 format.	CC supported, as native to D10.	—
MPEG-D10 625 line (PAL)	Supported	Not supported by D10 format.	TT supported, as native to D10.	—

Data track support on K2 Summit/Solo SD channels

The following table applies to SD channels when in Configuration Manager the Data Track settings are configured as follows:

- Record ancillary data: Yes
- Record Uncompressed VBI and captioning data to track: Yes

Video format	Data	Supported as follows:
525 line (NTSC)	Closed Captioning	Stored in EIA-708 packets. On playback, modulate to VBI line 21.
625 line (PAL)	Teletext	Stored in OP-47 packets. On playback, modulate to VBI line specified in OP-47 packet.
All supported SD formats	Uncompressed VBI	Selectable per line. Limited to 5 lines. The 5 line limit does not include any lines used for CC or TT. Can select either Luma or Chroma for each line, but not both.
	Ancillary timecode	Ancillary timecode is preserved only. No timecode track is constructed from ancillary timecode data. The timecode track is not inserted as ancillary timecode on playout.

Data track support on K2 Summit/Solo HD channels

On channels with the XDP (HD) license, the data track can contain ancillary data and other types of data. Luma ancillary data packets are stored. Chroma ancillary data packets are not supported.

Data	Supported as follows:
Ancillary timecode	For record, selectable to use VITC or LTC ancillary timecode as timecode source. For playout, selectable to insert recorded timecode track as ancillary data VITC or LTC timecode packets. If the recorded timecode track is inserted as VITC ancillary timecode and VITC ancillary timecode packets are already stored on the data track, then the recorded timecode track overrides the stored VITC ancillary timecode packets. If the recorded timecode track is inserted as LTC ancillary timecode and LTC ancillary timecode packets are already stored on the data track, then the recorded timecode track overrides the stored LTC ancillary timecode packets.
Vertical interval ancillary data packets	Extracted at input and stored on an ancillary data track. Upon playout, the data packets are inserted into the video stream on specified lines. Maximum 8 packets per field. CC and TT supported as native to format.

Captioning system support

An API is provided for access to captioning data, allowing Closed Captioning and Teletext systems to produce timecode correlated captions for an existing K2 clip.

About FCC requirements

Federal Communications Commission (FCC) rules incorporate sections of industry standards EIA-708 and EIA-608. The K2 Summit/Solo system complies with the rules for EIA-608 to DTV Closed Captioning (CC) transcoding. If SD material has EIA-608 CC present, the K2 Summit/Solo system can be configured so that when it up-converts the material the EIA-708 packet contains the EIA-608 data plus the DTV CC transcoded from EIA-608.

This applies to up-conversion only. HD material should already have compliant EIA-708 packets.

About privately defined data packets

In ancillary data, the K2 Summit/Solo system supports data defined by a private organization. This is data that is not defined and registered with SMPTE.

For example, if a facility puts privately defined data as special "triggers" in their stream for downstream devices, these triggers are preserved on record and transfer and played with field accuracy when needed. SMPTE standard data is supported as well as the privately defined data, for fully compliant, field accurate data track support.

Data bridging of VBI information on K2 Summit/Solo HD channels

On channels with the XDP (HD) license, data is bridged as follows:

Source format	Source data	Conversion ——>	Converted format	Converted data
SD 525 line	Closed-captioning (CC) on line 21 (EIA-608) can be stored as UserData[7] CC packets or UserData VBI Line21 (Uncompressed VBI Line21)	Up-convert	HD	Ancillary Closed Caption EIA-708-B packets
	EIA-708	Up-convert	HD	EIA-708
SD 625 line	Teletext (except as below)	No up-conversion to HD		
	5 lines of VBI Teletext in OP-47 packets	Up-convert	HD	OP-47 ancillary data packet in SD data track file. SD Teletext is in ancillary data location as specified in OP-47 packet.
SD 625 line 525 line	Ancillary data	Up-convert	HD	Moved to valid lines
HD	EIA-708 & 608 Ancillary data packets	Down-convert	SD	Closed-captioning on line 21 (EIA-608 standard).
HD	Teletext as OP-47 packets	Down-convert	SD	Output as VBI waveforms on lines specified in OP-47 packet or as specified by "Teletext Output Lines" data track settings in AppCenter Configuration Manager.
HD 1080i	Ancillary data	Cross-convert	HD 720p	Moved to valid lines.
HD 720p	Ancillary data	Cross-convert	HD 1080i	Moved to valid lines. Any data on lines 21-25 is moved to line 20 on 1080i output.

Line mapping of ancillary data packets on K2 Summit/Solo HD channels

On channels with the XDP (HD) license, you can use "Output OP-47 packet on line" data track settings in AppCenter Configuration Manager to specify that all OP-47 packets are output on the selected video line during playout.

Source format	Source data	Line mapping ——>	Playout format	Converted data
HD 1080i	OP-47 packets, as specified by DID and SID, on a line valid for 1080i	Maps to	HD 1080i (same as source)	OP-47 packets on a different line valid for 1080i.

[7] UserData CC packets always on. If CC exists, it is recorded and played back. MPEG UserData can be played out but not recorded.

Source format	Source data	Line mapping ——>	Playout format	Converted data
HD 720p	OP-47 packets, as specified by DID and SDID, on a line valid for 720p	Maps to	HD 720p (same as source)	OP-47 packets on a different line valid for 720p.

PitchBlue/H.264 ancillary data and timecode

The K2 Summit/Solo system extracts captioning and timecode information embedded in the video of H.264 material during ingest. The system plays this information during H.264 playout.

This functionality supports the PitchBlue workflow. However, the functionality applies to all H.264 material, not only PitchBlue material.

Internationalization

When you enable internationalization on a K2 Summit/Solo system, you can name your media assets in a local language. The K2 Summit/Solo system supports the local language name as specified in the following table.

System	Internationalization support
Keyboard input and display	• English • Chinese • Japanese • French • German • Spanish • Cyrillic (Russian) • Portuguese • Korean
Media database	• All external views of movie assets can be represented as wide-file names. • AppCenter runs in Unicode. • Only movie assets and searchable User Data keys are Unicode.
Media file system	• Support for Kanji and wide-character file and folder names. • File-folder representation of movie are internationalized, as well as the QuickTime reference file it contains. • Key names (V:\PDR) remain unchanged, but are Unicode. • Elementary streams remain as GUIDs, but are Unicode.
K2 Summit/Solo applications	• Movie assets are described in Unicode. • Application user interfaces are Unicode compliant.
Protocols	Refer to Appendix A, Remote control protocols.
FTP transfers	Refer to "FTP internationalization" in this document.

Names of media assets and bins must conform to the naming specifications for assets and bins.

Related Topics

Remote control protocols on page 209
About FTP internationalization on page 77

Limitations for creating and naming assets and bins

Media assets and bins must conform to the following specifications.

Characters not allowed in asset and bin names

Position	Character	Description
Anywhere in name	\	backward slash
	/	forward slash

Position	Character	Description
	:	colon
	*	asterisk
	?	question mark
	<	less than
	>	greater than
	%	percent sign
	|	pipe
	"	double quote
At beginning of name	~	tilde

Asset and bin name limitations

The maximum number of characters in an asset path name, including the bin name, is 259 characters. This includes separators such as "\" and parts of the path name that are not visible in AppCenter. The file system limits the number of bytes in a name as well as the number of characters. The values in this table apply to names in English and other languages referred to in ISO 8859-1. The full count of 259 characters might not be available with some other character sets.

	Asset name, bin name, and path			
Sections of an asset/path name	**The rest of the path name** (i.e. everything apart from the bin and asset names)	Bin name	Asset media directory and extension	Asset name and extension
Naming limitation	This part of the path name is not visible in AppCenter.	The bin name can be up to 227 characters (which would leave room for only a 1-character asset name)	This part of the path name is not visible in AppCenter. The directory name is the same as the asset name. 4 characters are reserved for the extension.	The extension is not visible in AppCenter. At least 25 characters are reserved for the asset name and extension, even if they are not all used.
Example	`\media`	`\mybin1\mybin2`	`\MyVideo.cmf`	`\MyVideo.xml`

The following examples show how a path name would appear in AppCenter and in the file system.

In AppCenter:

```
V:\mybin1\mybin2\MyVideo
```

In the file system:

```
V:\media\mybin1\mybin2\MyVideo.cmf\MyVideo.xml
```

Bin nesting limitations

The K2 media database supports nine levels of nested bins. This includes the top level (first) bin. Exceeding this specification results in a database error. When creating a bin do not create a bin at level ten or deeper.

For example:

- The following is supported:
  ```
  default\en\fr\es\de\it\be\dk\cn
  ```
- The following is not supported:
  ```
  default\en\fr\es\de\it\be\dk\cn\jp
  ```

Video network performance

K2 systems support streaming transfers to and from K2 Summit/Solo system, K2 Media Clients, K2 SANs, Profile XP Media Platforms, or any device that supports General Exchange Format (GXF) as described in SMPTE 360M.

Parameter	Specification	Comments
Transfer bandwidth per internal storage K2 Summit/Solo system	Up to 50 MBytes per second	—
Transfer bandwidth per K2-SVR-100	Up to 90Mbytes per second	Depending on system design
Transfer bandwidth per K2-SVR-NH10GE	Up to 600Mbytes per Second	Depending on system design
Maximum concurrent transfers per transfer engine	4 to 10, configurable on SAN	Additional transfers are queued.
Minimum delay from start of record to start of transfer	20 seconds	This applies to both 60Hz timing and 50Hz timing.
Minimum delay between start of transfer into destination and start of play on destination	20 seconds	—

About file interchange mechanisms on K2 systems

K2 Summit, Solo, and SAN systems can send and receive files as follows:

- File based import/export — This is based on a file that is visible from the operating system. For example, AppCenter import/export features are file based.
- HotBin import/export — This is file based import/export, with automated features that are triggered when a clip is placed in a bin. Some HotBin functionality requires licensing.
- FTP stream — This is file interchange via File Transfer Protocol (FTP).

GXF interchange specification

This specification applies to GXF file transfer, import, and export on K2 Summit, Solo, and SAN systems.

Streaming between online K2 systems supports complex movies and agile playlists of mixed format.

Formats are supported are as follows:

Supported formats		Notes
Video	DVCPRO25	—
	DVCPRO50	—
	DVCPRO HD	Super Slo-Mo requires software version 7.1. x or higher
	DVCAM	—
	MPEG-2	Includes all MPEG-2 formats (IMX, XDCAM, etc.) that can be stored on a K2 system
	AVC-Intra	—
	H.264	Playable on K2 Summit 3G system only. Can transfer to systems with K2 software version 8.x and higher.
	Audio	48 kHz —
16 bit, 24 bit		—
PCM, Dolby-E, AC-3		—
Data	VBI	—
	Ancillary	—

Interchange mechanisms are supported as follows:

Mechanism		Support
File based	Import	Yes
	Export	Yes
FTP stream	Import	Yes
	Export	Yes

MXF interchange specification

This specification applies to MXF file transfer, import, and export on K2 Summit, Solo, and SAN systems.

MXF supports simple clips with a single video track only. MXF does not support multiple video tracks, such as 3D/Video + Key or complex movies.

Formats are supported are as follows:

Supported formats		Notes
Video	DVCPRO25	—
	DVCPRO50	—
	DVCPRO HD	Super Slo-Mo requires software version 7.1. x or higher
	DVCAM	—
	D10	See MXF export behavior for eVTR style D10AES3.
	MPEG-2	Includes all MPEG-2 formats (IMX, XDCAM, etc.) that can be stored on a K2 system
	AVC-Intra	—
	Audio	48 kHz —
16 bit, 24 bit		—
PCM, Dolby-E, AC-3		—
Data	VBI	MXF supports either ancillary data packets or VBI lines in the data track but not both, so if ancillary data packets and VBI lines have been recorded into the K2 clip's data track, then the VBI lines will be dropped from the MXF data track on an MXF export.
	Ancillary	—

Interchange mechanisms are supported as follows:

Mechanism		Support
File based	Import	Yes
	Export	Yes
FTP stream	Import	Yes
	Export	Yes

With a special export option, you can export a completed continuous (loop) record clip as MXF or QuickTime, with the result being a flattened stream file. Recording must be complete before you export the clip, however you can make sub-clips while record is underway and export the sub-clips. For this feature, MPEG-2 long GoP is not supported.

MXF export behavior on K2 systems

Upon MXF export the K2 system checks clip structure for specifications as they apply to industry standard formats such as XDCAM and eVTR style D10AES3. If specifications match, the media is exported as the appropriate format.

The K2 system allows you to configure channels so that they no longer match the specifications for the industry-standard format. For example, you can add audio tracks to exceed the "# of Audio Tracks" specification for a D10AES3 channel. If you alter a clip in this way, on MXF export the K2 system exports the clip as MXF OP 1A but it is not the same eVTR style of MXF.

About MXF with DIDs and SDIDs

You can import and export MXF containing ANC packets and VBI lines as specified in SMPTE ST 436. The K2 system extracts the ANC packets or VBI lines to the K2 clip's data track.

AVI interchange specification

This specification applies to AVI file import on K2 Summit, Solo, and SAN systems.

AVI supports simple clips with a single video track only.

Formats are supported are as follows:

Supported formats		Notes
Video	DVCPRO25	Type-2 (non-interleaved) DV video only
	DVCPRO50	
	DVCPRO HD	
	DVCAM	
Audio	48 kHz	Audio tracks handled as stereo pairs
	16 bit, 24 bit PCM	
Data	None	—

Interchange mechanisms are supported as follows:

Mechanism		Support
File based	Import	Yes
	Export	No
FTP stream	Import	No
	Export	No

QuickTime interchange specification

This specification applies to QuickTime file transfer, import, and export on K2 Summit, Solo, and SAN systems.

QuickTime supports simple clips with a single video track only.

Formats are supported are as follows:

Supported formats		Notes	
Video	DVCPRO25	—	
	DVCPRO50	—	
	DVCPRO HD	Super Slo-Mo requires software version 7.1. x or higher	
	DVCAM	—	
	AVC-Intra	—	
	D10/IMX	—	
	XDCAM-HD	—	
	XDCAM-EX	—	
	XDCAM-HD422	—	
	H.264	Playable on K2 Summit 3G system only. Can transfer to systems with K2 software version 8.x and higher.	
	Audio	48 kHz	Audio tracks handled as stereo pairs on export
16 bit, 24 bit PCM			
Data	None	—	

Interchange mechanisms are supported as follows:

Mechanism		Support
File based	Import	Yes
	Export	Yes
FTP stream	Import	No
	Export	No

With a special export option, you can export a completed continuous (loop) record clip as MXF or QuickTime, with the result being a flattened stream file. Recording must be complete before you export the clip, however you can make sub-clips while record is underway and export the sub-clips. For this feature, MPEG-2 long GoP is not supported.

QuickTime video and key import specification

This specification applies to importing a QuickTime file with two video tracks for video and key playout. This is a licensed feature.

The imported file must be QuickTime 32 with alpha RLE 32-bit raster encoding, as produced by the Apple Animation Codec.

Supported video formats for import are as follows:

Format		Scan	Frame Rate
SD video	720 x 480	Interlaced	29.97
	720 x 512	Interlaced	29.97
	720 x 576	Interlaced	25
	720 x 608	Progressive	25
HD video	1920 x 1080	Interlaced	29.97, 25
	1280 x 720	Progressive	59.94, 50

Supported audio formats for import are as follows:

Format		
Audio tracks (if present)	48 kHz	Mono or stereo
	16 bit, 24 bit	
	PCM	

Interchange mechanisms are supported as follows:

Mechanism		Support
File based	Import	Yes
	Export	No
FTP stream	Import	No
	Export	No

When K2 software imports a file that meets the above requirements, it creates a K2 clip with two video tracks, in formats as follows:

Format			Frame Rate	Data Rate
SD video	D10/IMX	720 x 512	29.97	50 CBR
	D10/IMX	720 x 608	25	50 CBR
HD video	AVC-Intra 100	1920 x 1080	29.97, 25	100 Mbps
	AVC-Intra 100	1280 x 720	29.97, 25	100 Mbps

Audio tracks, if present are imported.

Timecode data is imported as K2 striped timecode. The first timecode value is the starting value and subsequent timecode is continuous.

The import process consumes system resource. Be aware of this if running other resource intensive processes during import.

QuickTime reference files

The following formats are supported as QuickTime reference files:

- DV
- AVC-Intra
- XDCAM-EX
- XDCAM-HD
- XDCAM-HD 422
- IMX

MPEG interchange specification

This specification applies to MPEG import on K2 Summit, Solo, and SAN systems.

Formats are supported are as follows:

Supported formats		Notes
Video	MPEG-2	Supports import of MPEG-2 program and transport streams. If the transport stream contains multiple programs, the first detected program in the transport stream is imported as a K2 clip.
	H.264	AVCHD /H.264 is K2 Summit 3G system only. Import only supported.
Audio	48kHz	—
	MPEG-1 (layer 1 & 2)	—
	SMPTE 302M AES3 LPCM	—
	AC-3	—
	AVCHD DVD VOB LPCM	AVCHD /H.264 is K2 Summit 3G system only. Import only supported.
	DVD/VOB AC-3	—
Data	ATSC a53 captions	—
	SMPTE RDD-11 ancillary data	—

Interchange mechanisms are supported as follows:

Mechanism		Support
File based	Import	Yes

Mechanism		Support
	Export	No
FTP stream	Import	Yes
	Export	No

P2 interchange specification

This specification applies to P2 file transfer, import, and export on K2 Summit, Solo, and SAN systems.

Formats are supported are as follows:

Supported formats		Notes
Video	AVC-Intra	Directory structure as specified by P2
	DVCPRO25	
	DVCPRO50	
	DVCPRO HD	
	DVCAM	
Audio	48 kHz	
	16 bit, 24 bit PCM	

Interchange mechanisms are supported as follows:

Mechanism		Support
File based	Import	Yes
	Export	Yes
FTP stream	Import	No
	Export	No

WAV audio interchange specification

This specification applies to WAV import on K2 Summit, Solo, and SAN systems.

Formats are supported are as follows:

Supported formats		Notes
Video	NA	—
Audio	48 kHz	Audio tracks handled as stereo pairs
	16 bit stereo PCM	
Data	NA	—

Interchange mechanisms are supported as follows:

Mechanism		Support
File based	Import	Yes
	Export	No
FTP stream	Import	No
	Export	No

Media file system performance on K2 systems

This section specifies media operations on K2 systems. On a K2 SAN, these specification are qualified at channel counts up to 48 channels. Performance on larger systems is not tested.

Record-to-play specifications

The following tables specify the minimum length of time supported between recording on one channel and cueing the same clip for playout on another channel. Live play mode is available only on a K2 Summit/Solo system with the AppCenter Pro license. On a K2 SAN, Live play mode is not supported with record-to-play on different K2 clients or on a K2 SAN with Live Production mode not enabled.

Standalone K2 Summit/Solo system

Formats	Live play	Normal play
DV	0.5 seconds	6.0 seconds
MPEG-2 I-frame, AVC-Intra	0.75 seconds	6.25 seconds
MPEG-2 long GoP, XDCAM	1.0 seconds	6.50 seconds

Live Play on K2 SAN with Live Production mode enabled

Formats	Record-to play on same K2 Summit System
DV	0.5 seconds
MPEG-2 I-frame, AVC-Intra	0.75 seconds
MPEG-2 long GoP, XDCAM	1.0 seconds

Normal play on K2 SAN with Live Production mode enabled

Formats	Record-to play on same K2 Summit System	Record-to play on different K2 Summit Systems
DV	6.0 seconds	8.0 seconds
MPEG-2 I-frame, AVC-Intra	6.25 seconds	8.25 seconds

Formats	Record-to play on same K2 Summit System	Record-to play on different K2 Summit Systems
MPEG-2 long GoP, XDCAM	6.50 seconds	8.50 seconds

Normal play on K2 SAN with Live Production mode not enabled

Formats	Record-to play on same K2 Summit System	Record-to play on different K2 Summit Systems
All formats	10 seconds	20 seconds

Other media file system specifications

Parameter	Stand-alone K2 Summit/Solo system	K2 SAN
Maximum number of clips[8]	20,000	50,000
Maximum length continuous record	24 hours	24 hours
Off-speed play range for audio scrub	-2x to +2x	-1.5x to +1.5x
Off-speed play range for insertion of MPEG user data and/or ancillary data on playout	0 to +1.2	0 to +1.2
Minimum duration between recordings	10 seconds	10 seconds

Transition effects formats and limitations

Transition (mix) effects are supported on K2 Summit/Solo system as follows.

Transition effects on first generation K2 Summit/Solo system

	DV	AVC-Intra	MPEG-2 I-frame	MPEG-2 long GoP
DV	Yes	No	No	No
AVC-Intra	No	Yes	No	No
MPEG-2 I-frame	No	No	Yes	No
MPEG-2 long GoP	No	No	No	No

When adding transitions to all events in a playlist for an on-the-fly (the **Go To** feature) pause or transition, limitations on the time for the length of the transition are as follows:

- 0.5 second or less on first generation K2 Summit/Solo system

[8] The maximum number of clips is based on clips with 16 or less audio tracks. Large quantities of clips with more than 16 audio tracks proportionally reduce the maximum number of clips.

Transition effects on K2 Summit 3G system

	DV	AVC-Intra	AVCHD/H.264	MPEG-2 I-frame	MPEG-2 long GoP
DV	Yes	No	No	No	No
AVC-Intra	No	Yes	Yes	No	No
AVCHD/H.264	No	Yes	Yes	No	No
MPEG-2 I-frame	No	No	No	Yes	No
MPEG-2 long GoP	No	No	No	No	Yes

When adding transitions to all events in a playlist for an on-the-fly (the **Go To** feature) pause or transition, limitations on the time for the length of the transition are as follows:

- 0.5 second or less on K2 Summit 3G systems

Protocols supported

AMP, VCDP, and BVW protocols are supported.

Related Topics

Remote control protocols on page 209

Transfer compatibility with K2 Summit/Solo

When transferring material between a K2 Summit/Solo and other Grass Valley products, you must consider the specifications of the different products. The following tables illustrate some of these considerations. In these tables, source material is assumed to have been recorded on the source device.

Transfer compatibility with K2 Media Client

Transfer	Material transferred	Compatibility
From K2 Summit/Solo to K2 Media Client	DVCPRO25, DVCPRO50	Playout supported.
	DVCPRO HD	Not supported
	MPEG	Supported
	AVC-intra	Not supported
	H.264	Not supported
	From K2 Media Client to K2 Summit/Solo	All types of material supported, according to the SD and/or HD capability.

Transfer compatibility with Profile XP Media Platform

Transfer	Material transferred	Compatibility
From K2 Summit/Solo to Profile XP Media Platform	DVCPRO25, DVCPRO50	Playout supported.
	DVCPRO HD	Not supported
	MPEG-2 HD 4:2:0 80 Mb or less MPEG-2 SD 4:2:2, XDCAM-HD422, XDCAM-EX	Supported. Can be played out.
	MPEG-2 720p MPEG-2 HD 4:2:2 XDCAM-HD HDV 1440x1080	Supported for storage only. Transfer is successful but playout not supported.
	AVC-intra	Not supported
	H.264	Not supported
	From Profile XP Media Platform to K2 Summit/Solo	All types of material supported, according to the SD and/or HD capability of the model.

Data compatibility between K2 Summit/Solo and PVS models

When material is transferred between a PVS Profile XP Media Platform and a K2 Summit/Solo system, data is supported as follows:

Transferring from PVS (source) to K2 Summit/Solo with HD license (destination)

Source format	Source data	SD playout data support on destination	HD playout data support on destination
DVCPRO25	Closed captioning	Yes	Yes
	Ancillary data	No	No
DVCPRO50	Closed captioning in compressed VBI	Yes	No
	Ancillary data	Yes	Yes
DVCPRO50	Compressed VBI	Yes	No
SD MPEG-2	Uncompressed VBI	Yes	Yes, with data bridging for CC only. Other VBI lines are discarded.
	Closed captioning	Yes	Yes. Ancillary data packets

Source format	Source data	SD playout data support on destination	HD playout data support on destination
	Compressed VBI	Yes	Yes, if enabled
	Ancillary data	Yes	Yes
HD MPEG-2	Ancillary data	Yes	Yes

Transferring from K2 Summit/Solo (source) to PVS (destination)

Source format	Source data	SD playout data support on destination	HD playout data support on destination
DVCPRO25, DVCPRO50	Any supported on K2 Summit/Solo	Yes	NA
DVCPRO HD	Any supported on K2 Summit/Solo	NA	NA
AVC-Intra	Any	NA — AVC-Intra not supported on PVS	
H.264	Any	NA — H.264 not supported on PVS	
SD MPEG-2	Any data recorded with Profile compatible setting[9].	All supported	Yes
	Uncompressed VBI and captioning on data track	Not supported. Do not attempt to transfer to PVS.	
	Compressed VBI	Yes	Yes, with data bridging for CC only. Other VBI lines are discarded.
	Uncompressed VBI	Yes	No, except for bridging of CC data, which requires Profile software v5.4.9.
HD MPEG-2	Ancillary data	Yes. CC bridging requires data-bridging SDI board.	Yes.

Control Point PC system requirements

If you are building your own Control Point PC, the machine you choose must meet the following requirements. These requirements assume that the PC is dedicated to its function as the host for Grass Valley product control and configuration applications. You should not run other applications on the PC that could interfere with system performance.

Control Point PC system requirements are as follows:

[9] When Record ancillary data = No or when Record Uncompressed VBI and captioning data to track = No

Requirements	Comments
Operating System	Microsoft Windows (Must be a U.S. version): • XP Professional Service Pack 3 • Server 2003 • Vista Enterprise Service Pack 1 • Windows 7 • Server 2008 R2
RAM	Minimum 512 MB, 1 GB recommended
Graphics acceleration	Must have at least 128 MB memory
Processor	Pentium 4 or higher class, 2 GHz or greater
Hard disk space	400 MB
Microsoft .NET Framework	Version 4.0
Sun Java 2 Runtime Environment	Version 1.5.0_11, Version 1.6.0 or higher. Required for the HP Ethernet Switch configuration interface, which is used for K2 SAN (shared storage).
XML	Microsoft XML 4 Service Pack 2 is required. You can install it from the `msxml4sp2` file on the K2 System Software CD.
Quicktime	Version 7 or higher
Acrobat Reader	Version 8 or higher

Find software at Internet locations such as the following:

- http://msdn.microsoft.com/en-us/netframework/default.aspx
- http://java.sun.com/javase/downloads/index.jsp
- http://www.microsoft.com/downloads/details.aspx?FamilyId=3144B72B-B4F2-46DA-B4B6-C5D7485F2B42&displaylang=en
- http://www.apple.com/quicktime/download/
- http://get.adobe.com/reader/

MIB specifications

This section specifies Management Information Base (MIB) information for monitoring K2 devices with the Simple Network Management Protocol (SNMP). The Grass Valley NetCentral product uses this protocol. This information is intended for SNMP developers. MIB files can be obtained from the Grass Valley Developers website.

In addition to the MIBs specified in this section, a K2 device might support other MIBs based on third party software/hardware. To determine whether other MIBs are supported by the operating system or independent hardware/software vendors, perform a “MIB walk” operation on the K2 device using conventional SNMP utilities and determine MIBs supported.

Related Topics

K2 client MIBs on page 257

K2 Media Server MIBs on page 258

K2 Appliance (Generic Windows computer based) MIBs on page 259

K2 client MIBs

Grass Valley MIBs

MIB	Description
gvg-reg.mi2 (GVG-REG)	Grass Valley SMI enterprise namespace
gvg-element.mi2 (GVG-ELEMENT-MIB)	Common object definitions for a Grass Valley device. • Generic device tracking information • SNMP trap target configuration • Generic IO/signal status information
gvg-prod.mi2 (GVG-PROD-REG)	Product sysObjectOID registrations for the Grass Valley devices
gvg-drs.mi2 (GVG-DRS-MIB)	Video disk recorder/server status information
gvg-tcm.mi2 (GVG-TCM-MIB)	Media transfer (import/export) statistical information
gvg-manclient.mi2 (GVG-MANCLIENT-MIB)	SAN client status information. Available only when the K2 client is connected to a SAN.

Other MIBs

MIB	Description
RFC1213-MIB.mib (RFC1213-MIB)	MIB-2 support as implemented by Microsoft for the Windows operating system.
hostmib.mib (HOST-RESOURCES-MIB)	Generic system information as implemented by Microsoft for the Windows operating system
lmmib2.mib (LanMgr-Mib-II-MIB)	Generic Windows networking, user account and service information as implemented by Microsoft for the Windows operating system
SUPERMICRO-SMI.my (SUPERMICRO-SMI)	Motherboard electromechanical sensor information (motherboard temperature hotspots, CPU fan, voltages, etc.)

MIB	Description
SUPERMICRO-HEALTH-MIB.my (SUPERMICRO-HEALTH-MIB)	
MEGARAID.mib (RAID-Adapter-MIB)	Internal RAID-1 SCSI drive and controller information

K2 Media Server MIBs

Grass Valley MIBs

MIB	Description
gvg-reg.mi2 (GVG-REG)	Grass Valley SMI enterprise namespace
gvg-element.mi2 (GVG-ELEMENT-MIB)	Common object definitions for a Grass Valley device. • Generic device tracking information • SNMP trap target configuration
gvg-prod.mi2 (GVG-PROD-REG)	Product sysObjectOID registrations for the Grass Valley devices
gvg-ssr.mi2 (GVG-SSR-MIB)	K2 Storage roles configured for the server by the K2 System Configuration application and their status information
gvg-sbs.mi2 (GVG-SBS-MIB)	K2 iSCSI Bridge and TOE (TCP Offload Engine) related status information. Available only if the K2 Media Server has the iSCSI Bridge role.
gvg-manfsm.mi2 (GVG-MANFSM-MIB)	Video File System and Clip Database (FSM) related status information. Available only if the K2 Media Server has role(s) of media file system server and/or database server.
gvg-tcm.mi2 (GVG-TCM-MIB)	Media transfer (import/export) statistical information. Available only if the K2 Media Server is configured to be a transfer/FTP/hotbins server.
gvg-manclient.mi2 (GVG-MANCLIENT-MIB)	SAN client status information. Available only when the K2 Media Server is a media system and/or database client. For example, if the K2 Media Server has the role of FTP server only, then it must be a media file system/database client to another K2 Media Server that is the media file system/database server.

Other MIBs

MIB	Description
RFC1213-MIB.mib (RFC1213-MIB)	MIB-2 support as implemented by Microsoft for the Windows operating system.
hostmib.mib (HOST-RESOURCES-MIB)	Generic system information as implemented by Microsoft for the Windows operating system
lmmib2.mib (LanMgr-Mib-II-MIB)	Generic Windows networking, user account and service information as implemented by Microsoft for the Windows operating system
mssql.mib (MSSQLSERVER-MIB)	Microsoft SQL Server information
10892.mib (MIB-Dell-10892)	Dell PowerEdge chassis related electro-mechanical status information
arymgr.mib (ArrayManager-MIB)	Dell RAID1 system disk (PERC) and controller information

K2 Appliance (Generic Windows computer based) MIBs

For details on the hardware/chassis running the K2 Appliance, check the chassis vendor's MIBs.

Grass Valley MIBs

MIB	Description
gvg-reg.mi2 (GVG-REG)	Grass Valley SMI enterprise namespace
gvg-element.mi2 (GVG-ELEMENT-MIB)	Common object definitions for a Grass Valley device. • Generic device tracking information • SNMP trap target configuration
gvg-prod.mi2 (GVG-PROD-REG)	Product sysObjectOID registrations for the Grass Valley devices
gvg-ssr.mi2 (GVG-SSR-MIB)	K2 Storage roles configured for the server by the K2 System Configuration application and their status information
gvg-tcm.mi2 (GVG-TCM-MIB)	Media transfer (import/export) statistical information. Available only if the K2 Media Server is configured to be a transfer/FTP/hotbins server.

MIB	Description
gvg-manclient.mi2 (GVG-MANCLIENT-MIB)	SAN client status information. Available only when the K2 appliance is a media system and/or database client.

Other MIBs

MIB	Description
RFC1213-MIB.mib (RFC1213-MIB)	MIB-2 support as implemented by Microsoft for the Windows operating system.
hostmib.mib (HOST-RESOURCES-MIB)	Generic system information as implemented by Microsoft for the Windows operating system
lmmib2.mib (LanMgr-Mib-II-MIB)	Generic Windows networking, user account and service information as implemented by Microsoft for the Windows operating system

Appendix **C**

Connector pinouts

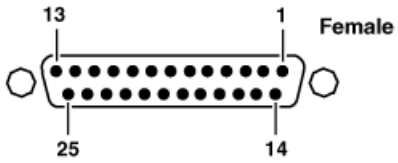
This section contains the following topics:

K2 Summit/Solo system connector pinouts

The following sections describe K2 Summit/Solo system rear panel connector pinouts.

AES Audio

Pinouts for each channel's AES Audio DB25 connector are as follows:



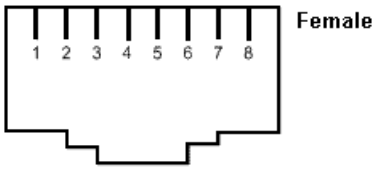
Pin #	Signal	Description
1	IN_P<0>	Channel Input 1&2 positive
2	IN_P<1>	Channel Input 3&4 positive
3	IN_P<2>	Channel Input 5&6 positive
4	IN_P<3>	Channel Input 7&8 positive
5	OUT_P<0>	Channel Output 1&2 positive
6	OUT_P<1>	Channel Output 3&4 positive
7	OUT_P<2>	Channel Output 5&6 positive
8	OUT_P<3>	Channel Output 7&8 positive
9	NO_C	NO_C
10	GND	GND
11	NO_C	NO_C
12	GND	GND
13	GND	GND
14	IN_N<0>	Channel Input 1&2 negative
15	IN_N<1>	Channel Input 3&4 negative
16	IN_N<2>	Channel Input 5&6 negative
17	IN_N<3>	Channel Input 7&8 negative
18	OUT_N<0>	Channel Output 1&2 negative
19	OUT_N<1>	Channel Output 3&4 negative
20	OUT_N<2>	Channel Output 5&6 negative
21	OUT_N<3>	Channel Output 7&8 negative
22-25	GND	GND

The optional audio cable has connections as follows:

RS-422 connector pinouts K2 Summit 3G

The K2 Summit 3G Production Client RS-422 interface conforms to ANSI/SMPTE 207M-1997 standard (SMPTE 422).

Pinouts for the individual RJ45 connectors are as follows:



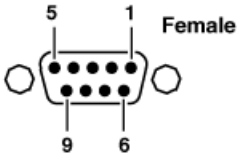
Pin #	Signal	Description
1	+TXD	Differential Transmit Data (high) (out TXB)
2	-TXD	Differential Transmit Data (low) (out TXA)
3	+RXD	Differential Receive Data (high) (in RXB)
4	GND	Signal Ground
5	GND	Signal Ground
6	-RXD	Differential Receive Data (low) (in RXA)
7	GND	Signal Ground
8	GND	Signal Ground

Balanced signals are placed on twisted wire pairs within a standard CAT5 or CAT3 cable.

RS-422 connector pinouts first generation K2 Summit/Solo system

The first generation K2 Summit/Solo system RS-422 interface conforms to ANSI/SMPTE 207M-1997 standard (SMPTE 422).

Pinouts for the individual DB9 connectors are as follows:

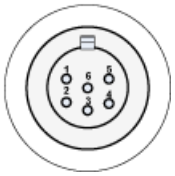


Pin #	Signal	Description
1	GND	Frame Ground
2	-TXD	Differential Transmit Data (low)
3	+RXD	Differential Receive Data (high)
4	GND	Transmit Signal Common
5	NC	Spare
6	GND	Receive Signal Common
7	+TXD	Differential Transmit Data (high)
8	-RXD	Differential Receive Data (low)
9	GND	Signal Ground

LTC connectors pinouts

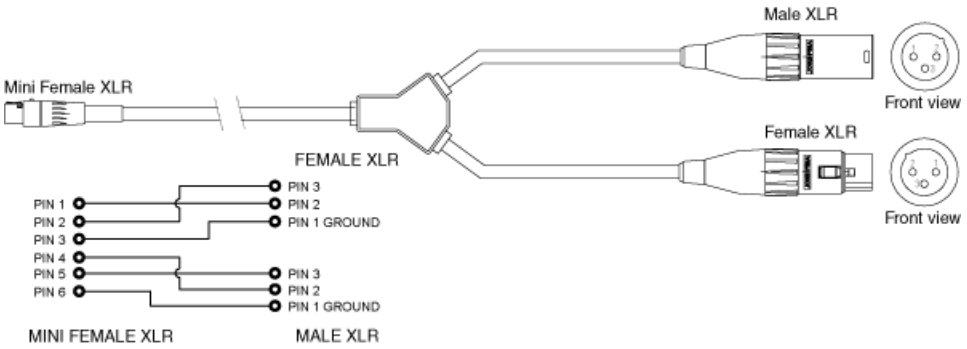
The K2 Summit/Solo system LTC panel connector provides balanced linear timecode input and output connections. The interface conforms to SMTPE 12M Linear Timecode.

On the K2 Summit/Solo system there is one 6 pin Switchcraft TRA6M Mini-XLR male connector for each channel. Pinouts are as follows:

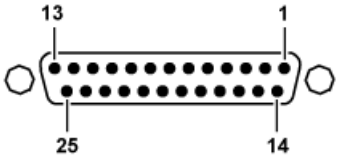


Pin #	Signal	Description
1	IN_P<0>	
2	IN_N<0>	
3	GND	Frame Ground
4	OUT_P<0>	
5	OUT_N<0>	
6	GND	Frame Ground

The mini-XLR to XLR LTC cable has connections as follows:



GPI I/O connector pinouts



Pin	Signal
1	Output 1
2	Output 2
3	Output 3
4	Output 4
5	Output 5
6	Output 6
7	Output 7
8	Output 8
9	Output 9
10	Output 10
11	Output 11
12	Output 12
13	Ground
14	Input 1
15	Input 2
16	Input 3

Pin	Signal
17	Input 4
18	Input 5
19	Input 6
20	Input 7
21	Input 8
22	Input 9
23	Input 10
24	Input 11
25	Input 12

K2 Media Server connector pinouts

The following sections describe K2 Media Server rear panel connector pinouts.

Redundant server heartbeat serial cable

Take care to use the proper serial cable to interconnect redundant K2 Media Servers that take the role of file system/database servers. This cable supports the heartbeat mechanism whereby the servers monitor each other's health. It is a 9 pin serial cable, but it is not a standard RS-232 null modem cable. The heartbeat cable is supplied with your system (Grass Valley part number 174-8137-00) and has a pin configuration as follows:

1 – 4

2 – 3

3 – 2

4 – 1&6

5 – 5

6 – 4

7 – 8

8 – 7

9 – No Connect

Appendix **D**

Rack mounting

This section contains the following topics:

Rack-mount considerations

When planning the placement of equipment in your equipment rack, bear in mind the following:

- Ensure adequate air flow around the chassis to provide sufficient cooling. Operating ambient temperature will affect the amount of air circulation required to keep the K2 system within its temperature limitations.
- Ensure that safety labels located on the top of the unit are visible after installation. This requires sufficient open space over the unit without cables or other devices impeding the view.
- If the system is installed with its ventilation intakes near another system's exhaust or in a closed or multi-unit rack assembly, the operating ambient temperature inside the chassis may be greater than the room's ambient temperature. Install the system in an environment compatible with this recommended maximum ambient temperature.
- Ensure that the power socket-outlet is installed near the equipment and is easily accessible.
- Ensure the rack is anchored to the floor so that it cannot tip over when the K2 system is extended out of the rack.
- Be sure to mount the K2 system in a way that ensures even weight distribution in the rack. Uneven mechanical loading can result in a hazardous condition. Secure all mounting bolts when installing the chassis to the rack.

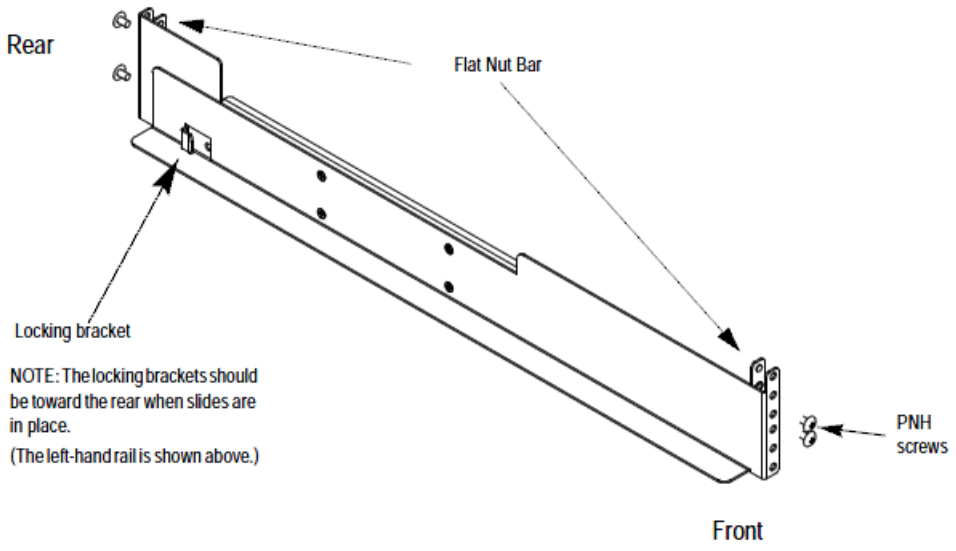
The following sections describe installing the K2 Summit Production Client step-by-step. For the K2 Solo Media Server, refer to *K2 Solo Media Server Accessories Installation Instructions* that you received with the rack kit.

Related Topics

Environmental specifications on page 217

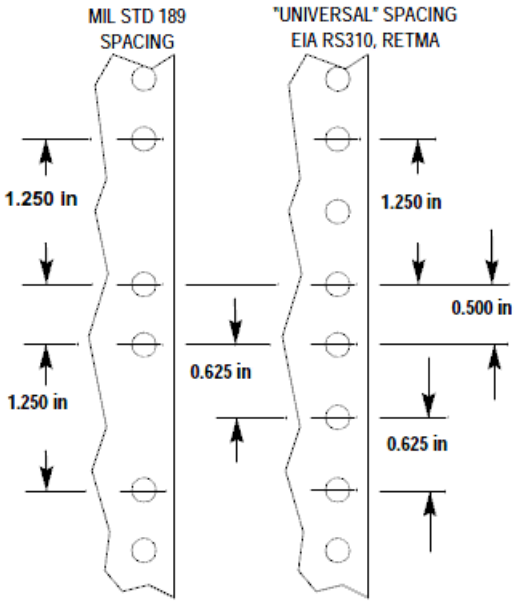
Rack mount hardware shipped with the K2 system

Your K2 system rack mount kit comes with rack mounting hardware as shown.

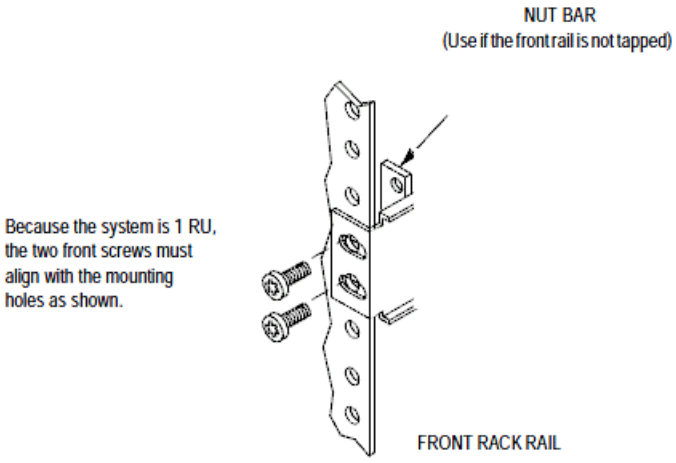


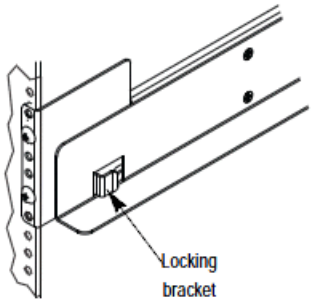
Mounting the Rack Slides

Choose the proper set of rail mounting holes on the rack. Notice that the hole spacing can vary with the rack type. When mounting the slides in racks with EIA spacing, make sure that the slides are attached to the 0.5-inch spaced holes.



Front and rear rack rail mounting hardware is provided with the rack mount kit. Mount the rails using the enclosed hardware. Make sure the stationary sections are horizontally aligned and are level, as well as parallel to each other.





REAR RACK RAIL (Nut bar not visible)

Installing the K2 system on the rack mount rails

1. Pull the slide-out track section to the fully extended position.

   ⚠ ***WARNING: To prevent injury, two people are required to lift the K2 system. It is too heavy for one person to install in the rack.***

   ⚠ ***WARNING: To prevent serious injury, ensure that the rack is anchored to the floor so that it cannot tip over when the K2 system is extended out of the rack.***

2. Push the chassis toward the rack until the chassis sections meet the locking bracket.
3. Verify the cabinet is pushed fully into the rack.
4. Insert and tighten the front panel retaining screws as shown in the previous diagram.

Making Rack Slide Adjustments

After installation, binding may occur if the slide tracks are not properly adjusted. To adjust the tracks:

1. Slide the chassis out approximately 10 inches.
2. Slightly loosen the mounting screws holding the tracks to the front of the rails and allow the tracks to seek an unbound position.
3. Tighten the mounting screws and check the tracks for smooth operation by sliding the chassis in and out of the rack several times.
4. Tighten the front panel retaining screws once the cabinet is in place within the rack to complete the installation.

Appendix **E**

Trademarks and Agreements

This section contains the following topics:

Trademarks

Grass Valley, GV 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. 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.

Index

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X