

Xmedia Server

Digital Asset Management System

Configuration Guide

M841-9900-491



www.miranda.com

Copyright & Trademark Notice

Copyright © 2014, Grass Valley, A Belden Brand. All rights reserved.

Grass Valley, A Belden Brand, Belden, Belden Sending All The Right Signals, and the Belden logo are trademarks or registered trademarks of Belden Inc. or its affiliated companies in the United States and other jurisdictions. Vertigo Suite, Vertigo XG and Xmedia Server are trademarks or registered trademarks of Grass Valley, A Belden Brand. Belden Inc., Grass Valley, A Belden Brand, and other parties may also have trademark rights in other terms used herein.

Terms and Conditions

Please read the following terms and conditions carefully. By using the Xmedia Server documentation, you agree to the following terms and conditions.

Grass Valley, A Belden Brand (“Grass Valley”) hereby grants permission and license to owners of the Vertigo Suite to use their product manuals for their own internal business use. Manuals for Grass Valley, A Belden Brand products may not be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose unless specifically authorized in writing by Grass Valley, A Belden Brand.

This manual may have been revised to reflect changes made to the product during its manufacturing life. Thus, different versions of a manual may exist for any given product. Care should be taken to ensure that one obtains the proper manual version for a specific product serial number.

Information in this document is subject to change without notice and does not represent a commitment on the part of Grass Valley, A Belden Brand.

Warranty Policies

Warranty information is available in the Support section of the Grass Valley, A Belden Brand Web site (www.miranda.com).

Document Identification

Title	Xmedia Server Configuration Guide
Part number	M841-9900-491
SW version	Vertigo Suite v.4.9 SP1

Revision History

After the original release date, this document may be updated with edits and then re-released. The following table tracks the versions of this document.

Revision date	Description
March 31, 2014	Original release
May 12, 2014	<ul style="list-style-type: none">Rebranded this document from Miranda Technologies Partnership to Grass Valley, A Belden Brand.Added multilingual and extensive safety and regulatory information.
May 15, 2014	<ul style="list-style-type: none">Updated the screen captures of the Xmedia Server Control Panel's Service Control tab to include the REST Interface setting.Added a section for the REST Interface setting on page 15-6.

Safety Compliance



This equipment complies with the requirements of CSA/UL/IEC/EN 60950-1, 2nd Ed. + AM1, Safety of information technology equipment.

The power cords supplied with this equipment meet the appropriate national standards for the country of destination.

[fr] **Conformité aux normes de sécurité**

Cet équipement est conforme aux exigences de CSA/UL/IEC/EN 60950-1, 2^e éd. + AM1, Sécurité du matériel informatique.

Les cordons d'alimentation fournis avec l'appareil répondent aux normes nationales appropriées du pays destinataire.

[es] **Conformidad en seguridad eléctrica**

Este equipo cumple con las exigencias de la CSA/UL/IEC/EN 60950-1, 2^a ed. + AM1, Seguridad de los equipos de tecnología de la información.

Los cables de alimentación incluidos con el equipo cumplen con las normas nacionales apropiadas para el país de destino.

[pt] **Conformidade de segurança elétrica**

Este equipamento está em conformidade com os requisitos da CSA/UL/IEC/EN 60950-1, 2^a ed. + AM1, Segurança de equipamento de tecnologia da informação.

Os cabos de alimentação fornecidos com este equipamento encontram as normas nacionais adequadas para o país de destino.

Safety of Laser Modules



This equipment incorporates modules containing Class 1 lasers. These modules are certified by the manufacturer to comply with:

- IEC/EN 60825-1 Safety of laser products
- IEC 60950-1 Safety of information technology equipment

[fr] **Sécurité laser**

L'appareil comprend des modules laser de classe 1. Ces modules sont certifiés conformes aux normes suivantes par le fabricant :

- IEC/EN 60825-1 Sécurité des appareils à laser
- IEC 60950-1 Sécurité du matériel informatique

[es] **Seguridad por los módulos laser**

Este equipo incorpora módulos láser de la Clase 1

Estos módulos están certificados por el fabricante para cumplir con:

- IEC/EN 60825-1 Seguridad de los productos láser
- IEC 60950-1 Seguridad de los equipos de tecnología de la información

[pt] **Segurança por módulo de laser**

Este equipamento incorpora módulos que contêm laser da classe 1. Estes módulos são certificados pelo fabricante em conformidade com:

- IEC/EN 60825-1 Segurança de equipamentos laser
 - IEC 60950-1 Segurança de equipamento de tecnologia da informação
-

Important Safeguards and Notices

This section provides important safety guidelines for operators and service personnel. Specific warnings and cautions appear throughout the manual where they apply. Please read and follow this important information, especially those instructions related to the risk of electric shock or injury to persons.

[fr] Mesures de sécurité et avis importants

La présente section fournit des consignes de sécurité importantes pour les opérateurs et le personnel de service. Des avertissements ou mises en garde spécifiques figurent dans le manuel, dans les sections où ils s'appliquent. Prenez le temps de bien lire les consignes et assurez-vous de les respecter, en particulier celles qui sont destinées à prévenir les décharges électriques ou les blessures.

[es] Medidas de seguridad y avisos importantes

Esta sección proporciona pautas de seguridad importantes para los operadores y el personal de servicio. Advertencias y precauciones específicas aparecen en el manual para su aplicación. Por favor, lea y siga esta importante información, especialmente aquellas instrucciones relacionadas con el riesgo de descarga eléctrica o lesiones a las personas.

[pt] Salvaguardas e avisos importantes

Esta seção fornece diretrizes de segurança importantes para os operadores e pessoal de serviço. Avisos e cuidados específicos estão listados no manual para sua aplicação. Por favor, leia e siga esta informação importante, especialmente aquelas instruções relacionadas ao risco de choque elétrico ou ferimentos.

Symbols and Their Meanings



The lightning flash with arrowhead symbol within an equilateral triangle alerts the user to the presence of dangerous voltages within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.



The exclamation point within an equilateral triangle alerts the user to the presence of important operating and maintenance/service instructions.



The earth ground symbol represents a protective grounding terminal. Such a terminal must be connected to earth ground prior to making any other connections to the equipment.



The fuse symbol indicates that the fuse referenced in the text must be replaced with one having the ratings indicated.



The presence of this symbol in or on Grass Valley, A Belden Brand equipment means that it has been designed, tested and certified as complying with applicable Canadian Standard Association (CSA) regulations and recommendations for USA/Canada.



The presence of this symbol in or on Grass Valley, A Belden Brand equipment means that it has been designed, tested and certified as complying with applicable Underwriters Laboratory (UL) regulations and recommendations for USA/Canada.



The presence of this symbol in or on Grass Valley, A Belden Brand equipment means that it has been designed, tested and certified as essentially complying with all applicable European Union (CE) directives.



The presence of this symbol in or on Grass Valley, A Belden Brand product means that it complies with safety of laser product applicable standards.

Warnings



A warning indicates a possible hazard to personnel, which may cause injury or death. Observe the following general warnings when using or working on this equipment:

- Appropriately listed/certified mains supply power cords must be used for the connection of the equipment to the mains voltage at either 120 V AC or 240 V AC.
- This product relies on the building's installation for short-circuit (over-current) protection. Ensure that a fuse or circuit breaker for 120 V AC or 240 V AC is used on the phase conductors.
- Any instructions in this manual that require opening the equipment cover or enclosure are for use by qualified service personnel only.
- Heed all warnings on the unit and in the operating instructions.
- Do not use this equipment in or near water.
- This equipment is grounded through the grounding conductor of the power cords. To avoid electrical shock, plug the power cords into a properly wired receptacle before connecting the equipment inputs or outputs.
- Route power cords and other cables so they are not likely to be damaged.
- Disconnect power before cleaning the equipment. Do not use liquid or aerosol cleaners; use only a damp cloth.
- Dangerous voltages may exist at several points in this equipment. To avoid injury, do not touch exposed connections and components while power is on.
- Do not wear rings or wristwatches when troubleshooting high current circuits such as the power supplies.
- To avoid fire hazard, use only the specified fuses with the correct type number, voltage and current ratings as referenced in the appropriate locations in the service instructions or on the equipment. Always refer fuse replacements to qualified service personnel.
- To avoid explosion, do not operate this equipment in an explosive atmosphere.
- This product includes a backup battery. There is a danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.
- Have qualified service personnel perform safety checks after any service.

[fr] Avertissements

- Un cordon d'alimentation dûment homologué doit être utilisé pour connecter l'appareil à une tension de secteur de 120 V CA ou 240 V CA.
 - La protection de ce produit contre les courts-circuits (surintensités) dépend de l'installation électrique du bâtiment. Assurez-vous qu'un fusible ou un disjoncteur pour 120 V CA ou 240 V CA est utilisé sur les conducteurs de phase.
-

-
- Dans le présent manuel, toutes les instructions qui nécessitent d'ouvrir le couvercle de l'équipement sont destinées exclusivement au personnel technique qualifié.
 - Respectez tous les avertissements figurant sur l'appareil et dans les instructions d'utilisation.
 - Ne pas utiliser cet appareil dans l'eau ou à proximité d'un point d'eau.
 - Cet équipement est mis à la terre par le conducteur de mise à la terre des cordons d'alimentation. Pour éviter les chocs électriques, branchez les cordons d'alimentation sur une prise correctement câblée avant de brancher les entrées et sorties de l'équipement.
 - Acheminez les cordons d'alimentation et autres câbles de façon à ce qu'ils ne risquent pas d'être endommagés.
 - Coupez l'alimentation avant de nettoyer l'équipement. Ne pas utiliser de nettoyeurs liquides ou en aérosol. Utilisez uniquement un chiffon humide.
 - Des tensions dangereuses peuvent exister en plusieurs points dans cet équipement. Pour éviter toute blessure, ne touchez pas aux connexions ou aux composants exposés lorsque l'appareil est sous tension.
 - Avant de procéder à toute opération d'entretien ou de dépannage visant des circuits à courant élevé (e.g., les blocs d'alimentation), enlevez tous vos bijoux (notamment vos bagues et votre montre).
 - Pour éviter tout risque d'incendie, utilisez uniquement les fusibles du type et du calibre indiqués dans la documentation ou sur l'équipement. Confiez le remplacement de fusibles au personnel technique qualifié.
 - Ne pas utiliser cet appareil dans une atmosphère explosive.
 - L'appareil 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 directives du fabricant.
 - Après tout travail d'entretien ou de réparation, faites effectuer des contrôles de sécurité par le personnel technique qualifié.

[es] **Advertencias**

- Un cable de alimentación aprobado deberá ser utilizado para la conexión del equipo a la tensión de red de 120 V CA o 240 V CA.
 - Este producto depende de la instalación del edificio para la protección de cortocircuitos (sobre-corriente). Asegúrese que un fusible o un interruptor térmico de 120 V CA o 240 V CA se utiliza en los conductores de fase.
 - Todas las instrucciones de este manual que requieren abrir la tapa del equipo se llevará a cabo por personal técnico calificado.
 - Respete todas las advertencias en el equipo y las instrucciones de funcionamiento.
 - No utilice este producto en el agua o cerca de este.
-

-
- Este equipo está conectado a tierra a través del conductor de puesta a tierra de los cables de alimentación. Para evitar una descarga eléctrica, enchufe el cable de alimentación a un tomacorriente debidamente instalado antes de conectar las entradas y salidas del equipo.
 - Instale los cables de alimentación y otros cables de forma de evitar ser dañados.
 - Desconecte la alimentación antes de limpiar el equipo. No use limpiadores líquidos o aerosoles, utilizar un paño húmedo.
 - Pueden existir tensiones peligrosas en varios puntos de este equipo. Para evitar lesiones, no toque las conexiones y componentes expuestos cuando la unidad está con alimentación.
 - No use anillos o relojes al solucionar problemas de circuitos de alta corriente como fuentes de alimentación.
 - Para evitar el riesgo de incendios, utilice sólo el fusible indicado con el número de tipo correcto, el voltaje y la corriente que se hace referencia en los lugares apropiados en las instrucciones de los servicios o el equipo. Siempre consulte el reemplazo del fusible a personal calificado.
 - Para evitar explosiones, no utilice este equipo en una atmósfera explosiva.
 - Este producto incluye una batería de reserva. Existe el peligro de explosión si la batería se instala de forma incorrecta. Reemplace la batería únicamente con el mismo tipo o equivalente recomendada por el fabricante. Deshágase de las baterías usadas según las instrucciones del fabricante.
 - Deje al personal calificado realizar las verificaciones de seguridad después de un servicio.

[pt] **Advertências**

- Um cabo de alimentação aprovado deve ser utilizado para ligar o equipamento à tensão da rede de 120 V CA ou 240 V CA.
 - Este produto baseia-se na instalação do edifício para proteção por curto-circuito (sobrecarga de corrente). Certifique-se de que um fusível ou disjuntor para 120 V CA ou 240 V CA é utilizado nos condutores de fase.
 - Todas as instruções contidas neste manual, que exigem a abertura da tampa do equipamento será realizada por pessoal qualificado.
 - Preste atenção a todos os avisos no equipamento e instruções de operação.
 - Não use este produto em ou perto da água.
 - Este equipamento é aterrado através do condutor de aterramento do cabo de alimentação. Para evitar choque elétrico, conecte o cabo de alimentação a uma tomada devidamente instalada antes de ligar as entradas e saídas do dispositivo.
 - Instale os cabos de alimentação e os outros cabos de modo a evitar danos.
 - Desligue a alimentação antes de limpar o equipamento. Não use detergentes líquidos ou aerossóis, usar um pano úmido.
-

-
- Tensões perigosas podem existir em vários pontos deste equipamento. Para evitar ferimentos, não toque as conexões e componentes expostos quando o aparelho está ligado.
 - Não usar anéis ou relógios ao solucionar problemas de circuitos de alta tensão, tais como fontes de alimentação.
 - Para evitar o risco de incêndio, utilize apenas o número especificado de fusível de tipo correto de tensão e corrente a que se refere o manual de serviço adequado. Referem-se sempre trocar o fusível por pessoal qualificado.
 - Para evitar a explosão, não utilize este equipamento em uma atmosfera explosiva.
 - Este produto inclui uma bateria de backup. Existe o perigo de explosão se a bateria está instalada incorretamente. Substitua a bateria somente com o mesmo tipo ou equivalente recomendado pelo fabricante. Elimine as baterias usadas de acordo com as instruções do fabricante.
 - Deixe o pessoal qualificado executar verificações de segurança depois de um serviço.
-

Cautions



A caution indicates a possible hazard to equipment that could result in equipment damage. Observe the following cautions when operating or working on this equipment:

- This equipment is meant to be installed in a restricted access location.
- When installing this equipment, do not attach the power cord to building surfaces.
- 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. Refer all servicing to qualified service personnel. Servicing should be done in a static-free environment.
- This unit has more than one power supply cord. Disconnect both power supply cords before servicing to avoid electric shock.
- To prevent damage to equipment when replacing fuses, locate and correct the problem that caused the fuse to blow before re-applying power.
- Use only the specified replacement parts.
- Follow static precautions at all times when handling this equipment.
- Products that have no on/off switch, and use an external power supply must be installed in proximity to a main power outlet that is easily accessible.

[fr] Mises en garde

- L'appareil est conçu pour être installé dans un endroit à accès restreint.
 - Au moment d'installer l'équipement, ne fixez pas les cordons d'alimentation aux surfaces intérieures de l'édifice.
 - Pour réduire le risque de choc électrique, n'effectuez pas de réparations autres que celles qui sont décrites dans le présent manuel, sauf si vous êtes qualifié pour le faire. Confiez les réparations à un technicien qualifié. La maintenance doit se réaliser dans un milieu libre d'électricité statique.
 - L'appareil comporte plus d'un cordon d'alimentation. Afin de prévenir les chocs électriques, débrancher les deux cordons d'alimentation avant toute opération d'entretien.
 - Pour éviter d'endommager l'équipement lors du remplacement de fusibles, localisez la source de la panne et corrigez la situation avant de rétablir le courant.
 - Employez uniquement les pièces de rechange recommandées par le fabricant.
 - Veillez à toujours prendre les mesures de protection antistatique appropriées quand vous manipulez l'équipement.
 - Les produits qui n'ont pas d'interrupteur marche-arrêt et qui disposent d'une source d'alimentation externe doivent être installés à proximité d'une prise de courant facile d'accès.
-

[es] Precauciones

- Este equipo está destinado a ser instalado en un lugar de acceso restringido.
- Al instalar este equipo, no sujete el cable de alimentación a la superficie del edificio.
- No realice reparaciones que no se encuentren en las instrucciones de funcionamiento a menos que esté calificado para hacerlo. Confíe las reparaciones a personal técnico calificado. El mantenimiento debe realizarse en un ambiente libre de estática.
- Esta unidad incluye dos cables de alimentación. Desconecte ambas fuentes de alimentación antes de dar servicio, para reducir el riesgo de descarga eléctrica.
- Para evitar daños en el equipo al sustituir los fusibles, primero localizar y corregir el problema que causó que el fusible se funda antes de aplicar la alimentación de nuevo.
- Utilice únicamente repuestos específicos.
- Siga las precauciones DES en todo momento al manipular este equipo.
- Los productos que no tienen interruptor de encendido/apagado, y utilizan una fuente de alimentación externa deben instalarse cerca de una toma de corriente de fácil acceso.

[pt] Precauções

- Este material destina-se a ser instalado em um acesso restrito.
 - Quando instalar o equipamento, não fixar o cabo de alimentação em superfícies do edifício.
 - Não faça reparações que não estão no manual de instruções, a menos que você estiver qualificado. Solicite a assistência de pessoal qualificado. A manutenção deve ser realizada em um ambiente livre de estática.
 - Esta unidade inclui dois cabos de alimentação. Desligue ambas as fontes de alimentação antes de manutenção para reduzir o risco de choque elétrico.
 - Para evitar danos ao equipamento ao substituir fusíveis, primeiro localizar e corrigir o problema que causou o fusível fundir antes de aplicar energia novamente.
 - Use unicamente partes específicas.
 - Siga as precauções DES em todos os momentos ao manusear este equipamento.
 - Os produtos que não têm um interruptor de ligar/desligar, e usam uma fonte de alimentação externa devem ser instalados perto de uma tomada elétrica de fácil acesso.
-

Electrostatic Discharge (ESD) Protection



Electrostatic discharge occurs when electronic components are improperly handled and can result in intermittent failure or complete damage adversely affecting an electrical circuit. When you remove and replace any card from a frame always follow ESD-prevention procedures:

- Ensure that the frame is electrically connected to earth ground through the power cord or any other means if available.
- Wear an ESD wrist strap ensuring that it makes good skin contact. Connect the grounding clip to an *unpainted surface* of the chassis frame to safely ground unwanted ESD voltages. If no wrist strap is available, ground yourself by touching the *unpainted* metal part of the chassis.
- For safety, periodically check the resistance value of the antistatic strap, which should be between 1 and 10 megohms.
- When temporarily storing a card make sure it is placed in an ESD bag.
- Cards in an earth grounded metal frame or casing do not require any special ESD protection.

[fr] Protection contre les décharges électrostatiques (DES)

Une décharge électrostatique peut se produire lorsque des composants électroniques ne sont pas manipulés de manière adéquate, ce qui peut entraîner des défaillances intermittentes ou endommager irrémédiablement un circuit électrique. Au moment de remplacer une carte dans un châssis, prenez toujours les mesures de protection antistatique appropriées :

- Assurez-vous que le châssis est relié électriquement à la terre par le cordon d'alimentation ou tout autre moyen disponible.
 - Portez un bracelet antistatique et assurez-vous qu'il est bien en contact avec la peau. Connectez la pince de masse à une *surface non peinte* du châssis pour détourner à la terre toute tension électrostatique indésirable. En l'absence de bracelet antistatique, déchargez l'électricité statique de votre corps en touchant une surface métallique *non peinte* du châssis.
 - Pour plus de sécurité, vérifiez périodiquement la valeur de résistance du bracelet antistatique. Elle doit se situer entre 1 et 10 mégohms.
 - Si vous devez mettre une carte de côté, assurez-vous de la ranger dans un sac protecteur antistatique.
 - Les cartes qui sont reliées à un châssis ou boîtier métallique mis à la terre ne nécessitent pas de protection antistatique spéciale.
-

[es] **Protección contra descargas electrostáticas (DES)**

La descarga electrostática se produce cuando los componentes electrónicos se manipulan de forma incorrecta pudiendo causar una falla intermitente o total afectando un circuito eléctrico. Al quitar y reemplazar una tarjeta de un chasis siempre siga los procedimientos para prevenir la DES:

- Asegúrese de que el chasis está conectado eléctricamente a tierra a través del cable de alimentación o cualquier otro medio si está disponible.
- Use una pulsera de DES asegurando que tiene buen contacto con la piel. Conecte la pinza de puesta a tierra a una *superficie sin pintar* del chasis para desviar a tierra cualquier voltaje de DES indeseable. Si ninguna pulsera está disponible, conéctese a tierra tocando la parte metálica *sin pintar* del chasis.
- Para su seguridad, verifique periódicamente el valor de la resistencia de la pulsera antiestática, que debe estar entre 1 y 10 megaohmios.
- Al guardar temporalmente una tarjeta electrónica asegúrese que está colocado en una bolsa de DES.
- Las tarjetas que están conectadas a un chasis de o caja de metal a tierra, no requieren una protección especial para la DES.

[pt] **Proteção contra descargas eletrostáticas (DES)**

DES ocorre quando os componentes eletrônicos são manipulados de forma inadequada e pode causar falha intermitente ou completa afetando um circuito elétrico. Remover e substituir um cartão eletrônico do chassi siga sempre os procedimentos para evitar DES:

- Certifique-se de que o chassi é eletricamente aterrado através do cabo de alimentação ou qualquer outro meio, se disponível.
 - Utilize uma pulseira DES assegurando que você tenha um bom contato com a pele. Conecte o clipe à terra a uma *superfície não pintada* do chassi para desviar qualquer tensão indesejável de DES. Se nenhuma pulseira está disponível, faça o aterramento tocando a parte metálica *não pintada* do chassi.
 - Por segurança, verificar periodicamente o valor da resistência da pulseira antiestática, que deve ser entre 1 e 10 megohms.
 - Por temporariamente salvar um cartão eletrônico, certifique-se de que ele é colocado em um saco de DES.
 - As cartas que estão ligados a um chassis ou caixa de metal ligada à terra, não necessitam de proteção especial para o DES.
-

Cautions for LCD and TFT Displays



If the LCD or TFT glass is broken, handle glass fragments with care when disposing of them. If any fluid leaks out of a damaged glass cell, be careful not to get the liquid crystal fluid in your mouth or skin. If the liquid crystal touches your skin or clothes, wash it off immediately using soap and water. Never swallow the fluid. The toxicity is extremely low but caution should be exercised at all times.

[fr] **Précautions pour les écrans LCD et TFT**

Si l'écran LCD ou TFT est brisé, manipulez les fragments de verre avec précaution au moment de vous en débarrasser. veillez à ce que le cristal liquide n'entre pas en contact avec la peau ou la bouche. En cas de contact avec la peau ou les vêtements, laver immédiatement à l'eau savonneuse. Ne jamais ingérer le liquide. La toxicité est extrêmement faible, mais la prudence demeure de mise en tout temps.

[es] **Precauciones para las pantallas LCD y TFT**

Si la pantalla LCD o TFT se rompe, retire con cuidado los fragmentos de vidrio cuando se deshaga de ellos. Si hay una fuga de líquido de una celda de vidrio dañado, tenga cuidado que el cristal líquido no entre en contacto con su boca o la piel. Si el cristal líquido toca su piel o su ropa, lávelos inmediatamente con agua y jabón. No ingiera nunca el líquido. La toxicidad es muy baja, pero se debe tener precaución en todo momento.

[pt] **Precauções para os LCD e TFT**

Se o ecrã LCD ou TFT está quebrado, retire cuidadosamente os fragmentos de vidro ao descartar deles. Se o líquido está vazando de uma célula de vidro danificado tenha cuidado para não tirar o fluido de cristal líquido em sua boca ou pele. Se o cristal líquido toca sua pele ou roupa, lave imediatamente com água e sabão. Nunca engula o líquido. A toxicidade é muito baixa, mas o cuidado deve ser exercido em todos os momentos.

Electromagnetic Compatibility



This equipment has been tested for verification of compliance with FCC Part 15, Subpart B requirements for class A digital devices.

NOTE

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.



This equipment has been tested and found to comply with the requirements of the EMC directive 2004/108/EC:

- EN 55022 Class A Radiated emissions
 - EN 55022 Class A Conducted emissions
 - EN 61000 -3-2 Harmonic current emission limits
 - EN 61000 -3-3 Voltage fluctuation and flicker limitations
 - EN 61000 -4-2 Electrostatic discharge immunity
 - EN 61000 -4-3 Radiated EMF immunity-RF
 - EN 61000 -4-4 Electrical fast transient immunity
 - EN 61000 -4-5 Surge immunity
 - EN 61000 -4-8 Power frequency magnetic field
 - EN 61000 -4-11 Voltage dips, short interruption and voltage variation immunity
-

TABLE OF CONTENTS

Introduction	1-1
About the Xmedia Server	1-2
Xmedia Server's standard and option features.....	1-3
Work Order Management Option.....	1-3
Xplorer - Media Asset Management application	1-4
XMS hardware overview	2-1
Front panel components, LEDs and buttons	2-2
Back panel components and connectors.....	2-4
Mounting the Xmedia Server chassis in a rack.....	2-5
XMS network integration and service applications	3-1
Xmedia Server virus protection guidelines	3-2
Network Setup and Configuration	3-2
Standard Anti-Virus Protection	3-3
Institution of Policies	3-3
Xmedia Server network ports	3-4
VertigoXmedia Data Server service.....	3-5
Setting the Data Server's connection parameters	3-7
Logging Data Server events	3-9
Controlling the Data Server service	3-11
File Ingest Server and Transcode Server.....	3-13
Xmedia Server Control Panel - XmediaServer Properties Window	3-14
Xmedia Server Control Panel's settings pages.....	3-16
The XMS's general configuration settings	4-1
Viewing the Xmedia Server's product information	4-2
Configuring the XMS's network connection and directories	4-3
Configuring the Authorization Manager	4-4
Verifying the XMS's database settings	5-1
Verifying the SQL Server database settings.....	5-2
Making a backup of the SQL Server database	5-4
Replication of the XMS Server's database	6-1
Conditions that trigger a failover	6-2
MOS Enabled Replication	6-3
Replication settings on the Xmedia Server Control Panel.....	6-4
Setting up and enabling Xmedia Server replication.....	6-6
Server replication requirements.....	6-7
Specifying the Replication settings on the primary server	6-13
Specifying the Replication settings on the secondary server.....	6-19
Make a backup of the primary server's database	6-20
Setting the Control Data Server option	6-20
Specifying the server settings on client applications.....	6-21
Verifying proper functioning of the servers and replication	6-23

MOS Server configuration and monitoring	7-1
Configuring the Xmedia Server's MOS settings	7-2
Instructions for configuring the Xmedia Server as a MOS server	7-3
Editing the Newsroom Control System's properties	7-6
Deleting the Newsroom Control System	7-7
Logging MOS Server activities	7-8
Specifying MOS logging options	7-8
Viewing the MOS log file	7-9
Monitoring inbound/outbound MOS messages	7-10
Mapping MOS channels	7-11
Adding a MOS Channel Association	7-12
Editing a MOS Channel Association	7-14
Deleting a MOS Channel Association	7-15
Using MOS Redirection to transfer media between Xmedia Servers	7-16
Prerequisites for using MOS Redirection	7-16
Overview of the MOS Redirection workflow	7-16
Limitations when using MOS Redirection with Xmedia Servers	7-17
Logging MOS Redirection events	7-19
License management	8-1
An overview of Vertigo Suite licenses	8-2
Vertigo Suite application and device licenses	8-3
Types of Vertigo Suite licenses	8-4
The vxls.bin license file	8-5
Xmedia Server Control Panel Licensing page versus License Manager	8-6
Licensing in a server replication environment	8-7
Orientation to Xmedia Server Control Panel's Licensing page	8-8
Licences view - License Summary tab	8-9
Licences view - License Detail tab	8-10
Soft Keys view	8-12
Viewing the existing device and application licenses	8-14
Viewing the details of a particular license	8-15
Resolving license errors and adding licenses to the Xmedia Server	8-16
Verifying the application's or device's server settings	8-17
Verifying the License Summary and License Details	8-20
Acquiring and adding licenses to the Xmedia Server	8-21
Deallocating a fixed license	8-22
Logging Xmedia Server events	9-1
Work Order workflow configuration	10-1
Xmedia Server Control Panel's Workflow options	10-2
Workflow models	10-3
Workflow option: States	10-5
Adding a new state to the workflow	10-6
Editing a state's properties	10-7
Removing a state from the workflow	10-8

Workflow option: Permissions.....	10-9
Adding a new permission to the workflow.....	10-10
Editing a permission's properties.....	10-11
Removing a permission from the workflow.....	10-12
Workflow option: Transitions.....	10-13
Transition properties and permissions.....	10-14
Adding a new transition to the workflow.....	10-18
Editing a transition's properties and permissions.....	10-20
Deleting a transition from the workflow.....	10-21
Workflow option: Priorities.....	10-22
Adding a new priority to the workflow.....	10-23
Deleting an existing priority from the workflow.....	10-24
Workflow option: Roles.....	10-25
Adding a new role to the workflow.....	10-26
Editing an existing role's properties and permissions.....	10-28
Deleting a role from the workflow.....	10-29
Workflow option: Users.....	10-30
Add a new user to the workflow.....	10-31
Edit a user's workflow properties and/or roles.....	10-33
Deleting a user from the workflow.....	10-34
Setting up E-Notifications.....	10-35
Creating the email template files for E-Notifications.....	10-36
Setting the Notification Parameters.....	10-37
Creating an E-List for each state change notification.....	10-38
Editing a state change notification's E-List.....	10-40
Setting the XMS system parameters.....	11-1
Setting the Ingest Parameters.....	11-2
Setting the Expiration Parameters.....	11-3
Setting the System field rate.....	11-4
OxSox connection settings.....	12-1
The XMS automation parameters for scheduled-based publishing.....	13-1
XFTP settings.....	14-1
Controlling the XMS service.....	15-1
Verifying the XMS service's status.....	15-2
Stopping and starting the XMS Service.....	15-3
Manually starting and stopping the XMS Service.....	15-3
Automatically starting the XMS Service.....	15-4
Controlling the DataServer.....	15-5
Enabling the Xmedia Server REST Interface.....	15-6
Launching the Services Management Console.....	15-7
Displaying XMS runtime statistics.....	16-1
Propagating assets to other Xmedia Servers.....	17-1

Configuring Xmedia Servers for asset propagation	17-4
Using automatic propagation	17-6
Setting up propagable categories and recipient associations	17-7
Using manual propagation	17-9
Resolving Propagation Exceptions	17-10
Information Propagation Exceptions	17-11
Category Propagation Exceptions	17-11
Categorisation Propagation Exceptions	17-12
Removing propagated assets from a recipient server	17-13
Propagation and distributed work orders	17-14
Distributed work order concepts and behaviors	17-15
Setting up a hub and spoke server for distributed work orders	17-16
Using distributed work orders	17-20
Setting and monitoring the XMS publishing activities	18-1
Setting the Central XMS IP Override	18-2
The Insta-publish device setting on the Xmedia Server Control Panel	18-3
Insta-publishing from the EXMS to a Localhost device	18-4
Monitoring and managing publish requests in the queue	18-5
User rights management	19-1
Target audience and prerequisites for setting up URM	19-2
Overview of the Authorization Manager	19-3
Vertigo Suite Operations	19-6
Configuring the Policy Store in Active Directory	19-8
Open the Authorization Manager	19-10
Creating a new organizational unit and assigning a Policy Store	19-11
Granting the domain user administrative rights to the Organizational Unit	19-13
Stopping the XMS Service	19-14
Adding the domain user to the Xmedia Server's security credentials	19-15
Granting the domain user administrative rights to the Policy Store	19-18
Setting the Authorization Manager Configuration settings	19-20
Starting the XMS Service to populate the VertigoXmedia application	19-20
Configuring the Policy Store in an XML file	19-22
Opening the Authorization Manager	19-24
Configuring the Authorization Manager to use an XML file stored on a network share	19-25
Creating the VertigoXmedia Policy Store in the Authorization Manager	19-26
Obtaining a Windows user with full control of the shared directory	19-28
Stopping the XMS Service	19-29
Adding the new user to the Xmedia Server's security credentials	19-30
Changing the security credentials of the Policy Store	19-31
Setting the Authorization Manager Configuration settings	19-33
Starting the XMS Service to populate the VertigoXmedia application	19-34
Setting up your user rights management system	19-35
Establish your user rights management security criteria	19-36
Creating a new task definition	19-37

Creating and populating a new role definition.....	19-38
Creating a new role assignment	19-40
Associating Windows users and groups with a role assignment	19-41
Maintaining the Authorization Manager's elements	19-43
Editing role definitions.....	19-43
Editing task definitions	19-45
Adding and removing users from a role assignment.....	19-47
Restricting access to asset categories	19-49
Setting access permissions for an asset category.....	19-50
Granting additional users access to a restricted category	19-53
Removing users from a category's security	19-53
Removing all access restrictions from a category.....	19-54
Ingesting media files using the File Ingest Server	20-1
Installing the File Ingest Server and creating an ingest watch folder.....	20-3
Running the File Ingest Server and Transcode Server.....	20-4
Configuring an ingest server instance	20-5
Ingestor Settings properties.....	20-7
Editing an instance's properties	20-13
Deleting an instance	20-13
Reloading the instances in the File Ingest Server Control Panel.....	20-13
Ingesting files and monitoring the ingest's progress.....	20-14
File Ingest Server's logging	20-17

1 INTRODUCTION

The Xmedia Server (XMS) is the central graphical asset management server for Vertigo Suite channel branding and playout systems. The Xmedia Server allows all branding assets to be ingested once, centrally archived, and automatically moved to the desired graphics device using rule-based publishing.



Figure 1-1. Xmedia Server - a central graphical asset management server

The main purpose of this configuration guide is to provide practical reference and procedural information on how to use the Xmedia Server Control Panel application to configure the Xmedia Server.

The following sections of this chapter provide general information about the Xmedia Server and its optional features:

- [“About the Xmedia Server” on page 1-2](#)
- [“Xmedia Server’s standard and option features” on page 1-3](#)

The next couple of chapters provide specific information about the Xmedia Server’s hardware, software, and network integration. Further chapters provide instructions for how to configure the Xmedia Server using the Xmedia Server Control Panel.

About the Xmedia Server

The Xmedia Server (XMS) is the central graphical asset management server for Vertigo Suite channel branding and playout systems. Assets only need to be ingested once for them to be centrally archived on the Xmedia Server. These assets are then made available to all of the Vertigo Suite applications on the network, which allow you to create a wide range of graphics, including advanced, data-driven broadcast applications that link on-air graphics elements to live data feeds. The resulting graphic pages and their assets can then be automatically published to a range of graphics playout devices, including Imagestore, Intuition XG, and Vertigo XG devices.

The Xmedia Server offers benefits to larger broadcast systems that have multiple channels by sharing assets between channels without having to duplicate the assets. It also allows for a more dynamic handling of content and a more natural workflow because media creation, asset management, and asset distribution are conveniently linked by a common environment.

Besides its main use as a central asset repository and asset management/distribution system, the Xmedia Server integrates and supports the Vertigo Suite applications and other playout devices. The following list identifies other ways in which the Xmedia Server is used to support graphics creation and playout activities:

- **Asset propagation:** The Xmedia Server can be used in a hub and spoke distribution model in which assets can be created and propagated from a central hub to various spoke servers.
- **Server replication:** Two Xmedia Servers can be configured to offer full redundancy for near instant failover with no interruption in services, including on-air playout.
- **Newsroom integration:** The Xmedia Server can provide graphics assets to newsroom environments using the MOS protocol to integrate with the newsroom control system.
- **User rights management:** Using the Xmedia Server's user rights management system, system administrators and workflow managers can restrict access to some of the system's functionality and/or asset categories on a per-user basis.
- **License management:** The Xmedia Server stores and manages the software licenses that are required to operate each of the Vertigo Suite applications.
- **Work Order Workflow:** The Xmedia Server provides an optional work order workflow module that fully integrates into the Vertigo Suite. The work order workflow is used for requesting, completing, tracking and approving graphics work orders.

Xmedia Server's standard and option features

The Xmedia Server is a 2RU rackmount server with 2TB of RAID-1 storage and is factory configured to run **Windows Server 2003** as its operating system. Additional software applications and services that are factory installed include:

- **MICROSOFT SQL SERVER 2008:** The Xmedia Server uses a **Microsoft SQL Server database** to store asset details, categories, work order processing data, publish processing data, and other relational information and data. See [page 5-1](#) for more information.
- **XMEDIA SERVER CONTROL PANEL:** The Xmedia Server Control Panel is the user interface for configuring and controlling the Xmedia Server. See [page 3-14](#) for more information.
- **VERTIGOXMEDIA DATA SERVER:** The Data Server is a service application that manages data coming from various feeds, provides live updates of data values when requested and distributes the data out to the appropriate recipients. See [page 3-5](#) for more information.
- **File Ingest Server:** The File Ingest Server is a service responsible for automatically ingesting media into the Xmedia Server from a user-created ingest folder. The File Ingest Server is also responsible for issuing media conversion requests to the **Transcode Server**, which is the service responsible for transcoding media from one format to another. See [page 3-13](#) for more information.

In addition to the Xmedia Server unit, the following options are also offered to enhance the capabilities of the Xmedia Server:

- [“Work Order Management Option” on page 1-3](#)
- [“Xplorer - Media Asset Management application” on page 1-4](#)

Work Order Management Option

The Xmedia Server provides an optional work order workflow module (**VX-WOM**) that fully integrates into the Vertigo Suite. The work order workflow is used for requesting, completing, tracking and approving graphics work orders. See [“Work Order workflow configuration” on page 10-1](#) for more information on how to use the Xmedia Server Control Panel to create and configure the work order workflow module.

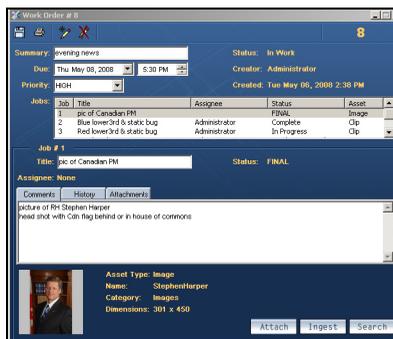


Figure 1-2. An integrated system for creating, completing, and tracking graphics work orders

Xplorer - Media Asset Management application

The Vertigo Suite features the **XPLORER** application (**VX-Xplorer**), which is a graphical content management system for viewing and managing the asset and file contents of the Xmedia Server and the devices to which the XMS has published assets. See the **XPLORER USER MANUAL** for more information.

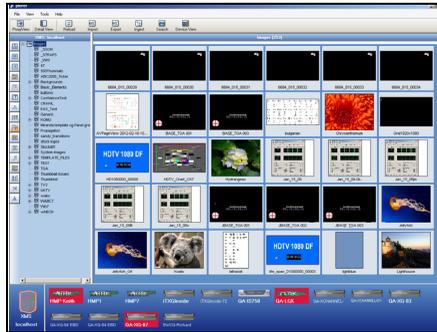


Figure 1-3. Xplorer - View and manage the media contents of the Xmedia Server

2 XMS HARDWARE OVERVIEW

Physically, the Xmedia Server is a 2RU rackmount server that incorporates redundant fans, power, and ethernet ports, with 2 TB of RAID-1 storage. The Xmedia Server features easy frontal access to the storage drives, and a control panel featuring LEDs and buttons for system monitoring and operation. The rear panel also provides convenient access to two power supply modules, seven PCI expansion slots (video, audio, and graphics cards), and various I/O ports (USB, COM1, VGA, Ethernet...etc).

The following sections provide additional details regarding the Xmedia Server’s hardware:

- [“Front panel components, LEDs and buttons” on page 2-2](#)
- [“Back panel components and connectors” on page 2-4](#)
- [“Mounting the Xmedia Server chassis in a rack” on page 2-5](#)

CAUTION

Xmedia Server devices should only be installed by trained personnel in a restricted access locations only. All health and safety regulations and precautions must be observed.

Chassis	FORM: 2U rackmount chassis HEIGHT: 3.5” (89mm) WIDTH: 17.2” (437mm) DEPTH: 25.5” (648mm)
Power consumption	700W (1 + 1) Redundant AC-DC power supply. Maximum draw is a total of 700W. Note that the device’s electrical ratings are located on the plug-in power supply modules.
Temperature	Ambient temperature: 35°C Note: This shall be the maximum internal temperature within the rack in which the Xmedia Server unit is installed.

WARNING

To reduce the risk of electric shock, disconnect all power sources before servicing Xmedia Server devices.

Front panel components, LEDs and buttons

Figure 2-1 demonstrates that the Xmedia Server's front panel provides easy access to the SATA drives, a floppy drive, DVD-ROM, a front port panel (USB & serial) and a control panel featuring LEDs and buttons for system monitoring and operation.

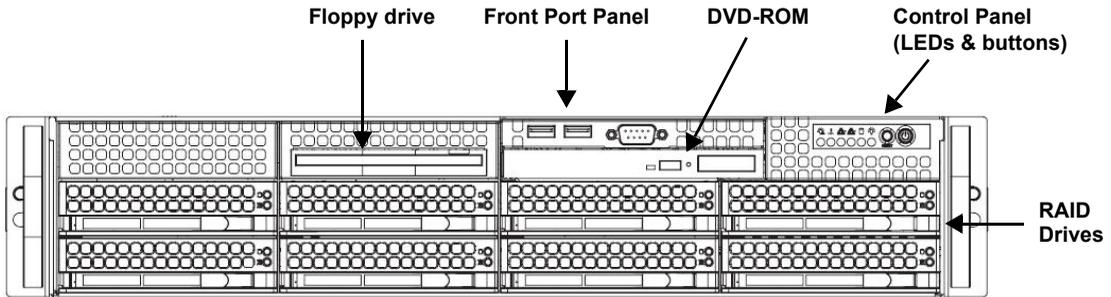


Figure 2-1. The Xmedia Server's front panel components

Figure 2-2 demonstrates that the control panel located on the front of the Xmedia Server chassis has six LEDs and two buttons. The table on page 2-3 describes the function of each LED and button, as well any corrective action you may need to take.

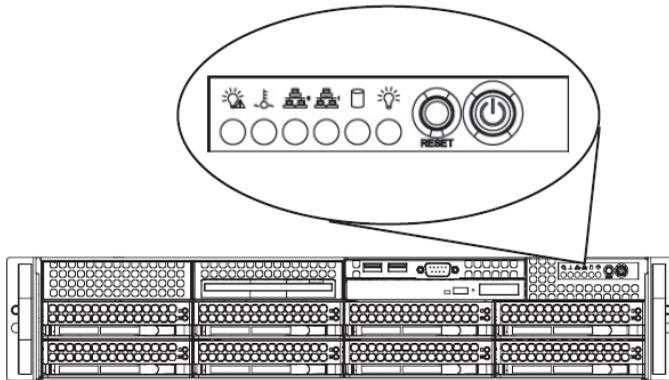


Figure 2-2. Xmedia Server chassis control panel LEDs and buttons

<p>POWER FAIL</p> 	<p>Indicates a power supply module has failed. This should be accompanied by an audible alarm. A backup power supply module will take the load and keep the system running, but the failed module will need to be replaced. This LED should be off when the system is operating normally.</p>
<p>OVERHEAT / FAN FAIL</p> 	<p>When this flashes, it indicates a fan failure. When it is constantly illuminated (solid on), it indicates an overheat condition, which may be caused by cables obstructing the airflow in the system or the ambient room temperature being too warm. Check the routing of cables and make sure that all fans are present and operating normally. You should also check to make sure that the chassis covers are installed properly. Finally, verify that the heatsinks are installed properly. This LED will remain flashing or on as long as the above mentioned conditions exist.</p>
<p>NIC2</p> 	<p>A flashing NIC2 LED indicates network activity on LAN2.</p>
<p>NIC1</p> 	<p>A flashing NIC1 LED indicates network activity on LAN2.</p>
<p>HDD</p> 	<p>Indicates IDE channel activity.</p>
<p>POWER (LED)</p> 	<p>Indicates that power is being supplied to the system's power supply units. This LED should normally be illuminated when the system is in operation.</p>
<p>RESET (BUTTON)</p> 	<p>The Reset button reboots the system.</p>
<p>POWER (BUTTON)</p> 	<p>This is the main power button, which is used to apply or turn off the main system power. Turning off this button removes the main power, but keeps standby power supplied to the system.</p>

Back panel components and connectors

Figure 2-3 demonstrates that the rear panel of the Xmedia Server provides convenient access to two power supply modules, seven PCI expansion slots (video, audio, and graphics cards), and various I/O port connectors (USB, COM1, VGA, Ethernet...etc). When using the Xmedia Server in a replication setup, you will insert the license dongle in one of the USB ports (see [page 6-8](#)).

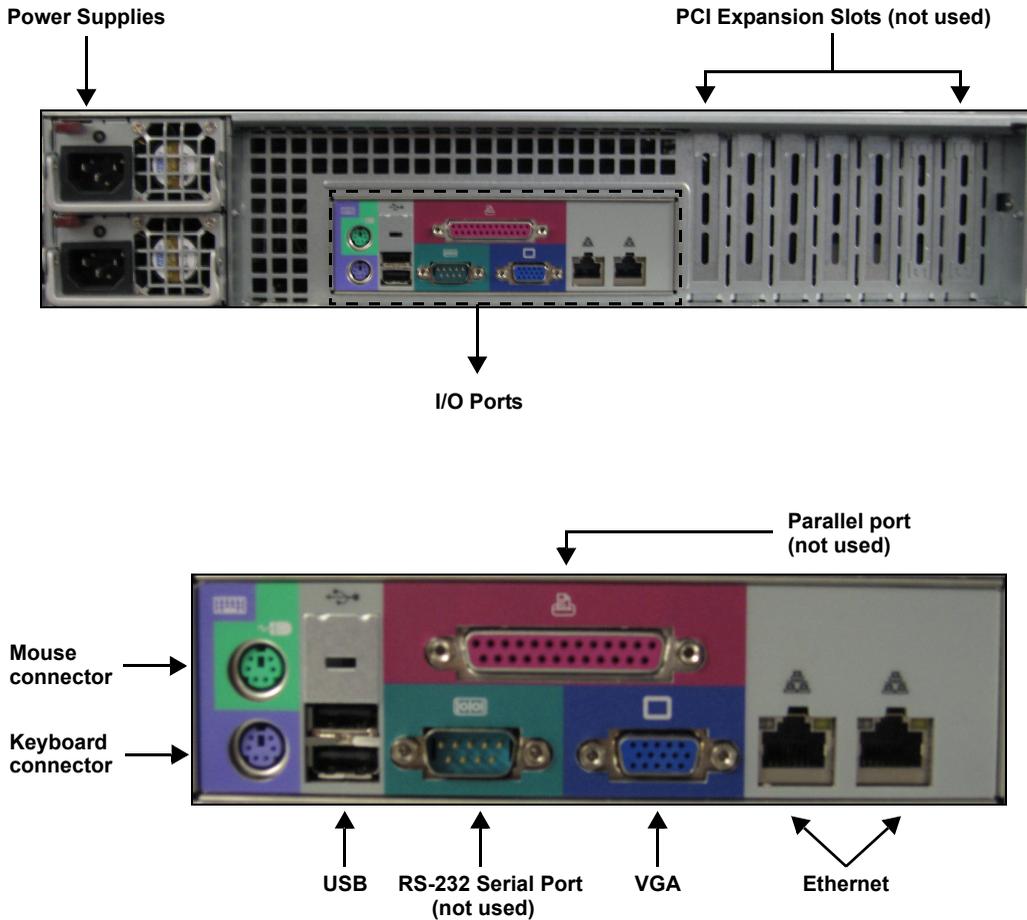


Figure 2-3. The Xmedia Server's rear panel components and connectors

☑ NOTE

The device's electrical ratings are located on the plug-in power supply modules.

Mounting the Xmedia Server chassis in a rack

Included in the shipping package is a rack mounting kit, which contains the rails, screws and washers required to mount the Xmedia Server chassis into an equipment rack.

Note that the rails are designed to fit in racks with a depth of 26" to 33.5". Due to the heavy weigh of the unit, the rack in which the Xmedia Server unit will be installed should be anchored to the building's structure.

CAUTION

Xmedia Server devices are intended to be installed in a restricted access location by qualified personnel. All health and safety regulations and precautions must be observed.

Included in the shipping package are a pair of rail assemblies. Each rail assembly consists of two sections: an inner fixed chassis rail that secures directly to the server chassis and an outer fixed rack rail that secures directly to the rack itself.

Figure 2-4 demonstrates that the inner rail assemblies are composed of two sections: inner rails and inner rail extensions. The inner rails are pre-attached to the chassis, while the inner rail extensions must be installed manually to the chassis.

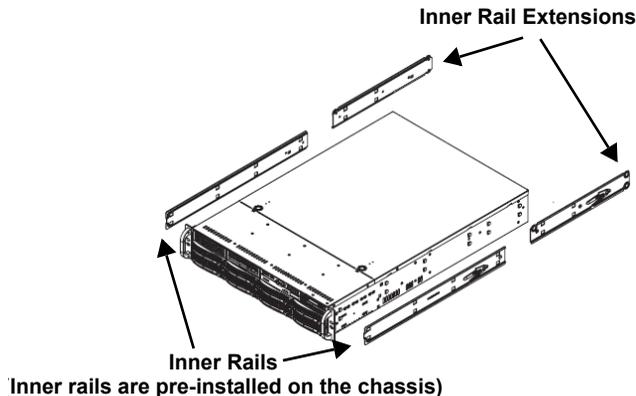


Figure 2-4. The Enterprise Server's inner rail assemblies

Once the inner rails are attached to the chassis, you must assemble and install the outer rails to the rack. Once both the inner and outer rail assemblies are properly installed, you can mount the Enterprise Server's chassis into the rack by sliding the inner rails into the outer rails.

Both chassis rails have a locking tab, which serves to lock the server in place when installed and pushed fully in the rack, as well as preventing the server from coming completely out when it is fully extended from the rack.

To install chassis rails and mount the Xmedia Server's chassis into an equipment rack:

1. Remove the Xmedia Server's faceplate by pulling the faceplate's handles away from the chassis.
2. Install the inner rail extensions to the server's chassis.
 - a. Place the inner rail extensions on the side of the chassis aligning the hooks of the chassis with the rail extension holes. Be sure that the extension faces "outward" just like the pre-attached inner rail.
 - b. Slide the extension toward the front of the chassis.
 - c. Secure the chassis with two screws as shown in figure [2-5](#).
 - d. Repeat steps 2A - 2C for the other inner rail extension.

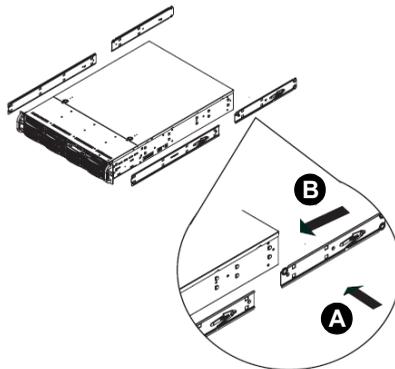


Figure 2-5. Installing the inner rail extensions

3. Install the outer rails to the rack (figure [2-6](#)).
 - a. Attach the shorter outer bracket to the outside of the longer rail. You must align the pins with the slides. Both bracket ends must face the same direction.
 - b. Adjust the short and long brackets to the proper distance so that the rail fits snugly with the rack.
 - c. Secure the longer bracket to the front of the outer rail with two screws.
 - d. Secure the shorter outer bracket to the rear side of the outer rail with three screws.
 - e. Repeat steps 3A - 3D for the remaining outer rail.

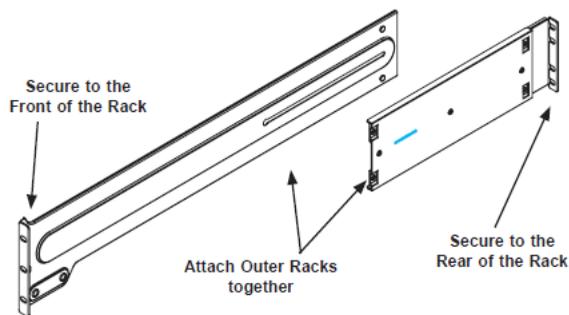


Figure 2-6. Installing the outer chassis rails to the equipment rack

4. Mount the Xmedia Server chassis into the rack (figure 2-7).
 - a. Align the inner rails on the chassis with the front of the outer rails on the rack.
 - b. Slide the inner rails into the outer rails, keeping the pressure even on both sides (it may be necessary to depress the locking tabs when inserting). When the server has been pushed completely into the rack, you should hear the locking tabs click into the locked position.

The chassis may not slide into the rack smoothly or easily when installed for the first time. Adjustments to the slide assemblies might be necessary to achieve a smooth insertion.
 - c. (Optional) Insert and tighten the thumbscrews that hold the front of the chassis to the rack.

CAUTION

Due to the heavy weight of the Xmedia Server, ensure that the rack is securely anchored onto a unmovable surface or structure before installing the chassis into the rack.

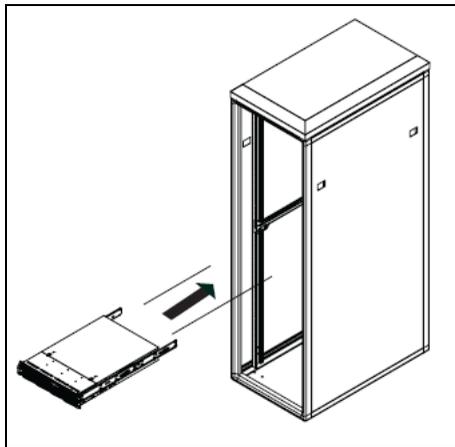


Figure 2-7. Mounting the Enterprise Server's chassis into a rack

CAUTION



Slide/rail mounted equipment is not to be used as a shelf or a workspace.

NOTE

To completely remove the chassis from the rack, you must release the locking tabs on both sides of the chassis.

5. Re-attach the faceplate by aligning and pushing the faceplate towards the Xmedia Server's chassis.

3 XMS NETWORK INTEGRATION AND SERVICE APPLICATIONS

It is recommended that the Xmedia Server be installed on a dedicated LAN, using the existing security infrastructure. A qualified system administrator should verify that the setup follows the organization's security standards. Specific recommendations regarding proper virus strategies, that won't compromise performance are provided in this chapter.

As the centralized server for the Vertigo Suite of products, you can connect to the Xmedia Server from any client PC on the network. All of connections used by the Vertigo Suite applications are over TCP and UDP.

The following sections provide guidelines for integrating the Xmedia Server into your network and an overview of the Data Server service, File Ingest Server and the Xmedia Server Control Panel interface:

- [“Xmedia Server virus protection guidelines” on page 3-2](#)
- [“Xmedia Server network ports” on page 3-4](#)
- [“VertigoXmedia Data Server service” on page 3-5](#)
- [“File Ingest Server and Transcode Server” on page 3-13](#)
- [“Xmedia Server Control Panel - XmediaServer Properties Window” on page 3-14](#)

Xmedia Server virus protection guidelines

Proper network setup and anti-virus software are key components of any virus protection strategy. As such, we highly recommend that you adhere to specific rules outlined in this section to avoid adversely affecting your production equipment's on-air performance. Our virus protection strategy, therefore relies on anti-virus software protection combined with the following:

- [Network Setup and Configuration](#) – A best case scenario for configuring your network for maximum protection against infection.
- [Standard Anti-Virus Protection](#) – Standard anti-virus practices for machines and applications not directly used for putting material on-air.
- [Institution of Policies](#) – Policies that all users must follow in order to avoid introducing infected files into the system.

Network Setup and Configuration

Ideally, the Xmedia Server and other non-critical components should be running anti-virus software, while the Vertigo XGs reside on a separate network. In such a case, the Vertigo XGs would not be running anti-virus software, leaving them potentially vulnerable. Therefore, provide proper protection and minimizing potential performance issues, it is recommended that restricted access be available by means of switch (see figure 3-1). It is also recommended that all other Xmedia equipment would be kept on a separate network isolated from other machines in the facility.

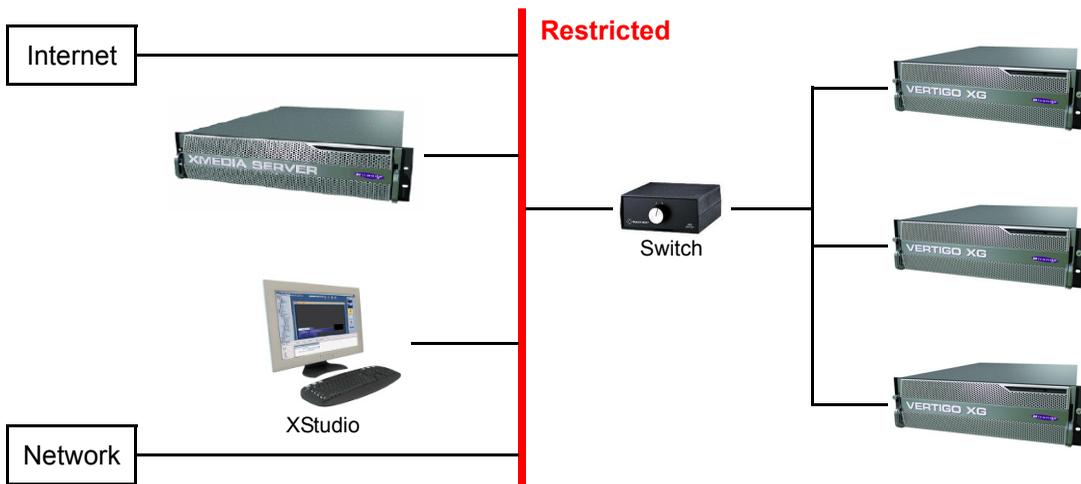


Figure 3-1. Recommended network configuration to provide virus protection

Standard Anti-Virus Protection

While critical for the on-air production process, many of the Vertigo Suite products do not put material directly on air. We therefore recommend that these products be configured with the same high level of anti-virus protection used for other machines on the broadcaster's network.

The following Vertigo Suite products should be configured with the highest level of anti-virus protection:

- Xmedia Server
- Data Server
- Xstudio
- Xbuilder

Institution of Policies

While the guidelines outlined in the previous sections are critical to your broadcast network's protection from infection, end users must accept some responsibility. We therefore recommend that your IT department enforce the following policies:

- Any machine that will be attached to the same network as the Xmedia Server must undergo a complete system scan.
- Any floppy, zip or other external media to be copied to or run on the Xmedia Server must undergo a complete scan.
- Material to be used in 24/7 operation should not be copied to the Xmedia Server. Instead, it should be transferred only during maintenance periods.
- Do not download Internet files directly onto the Xmedia Server.

Xmedia Server network ports

Users can connect to the Xmedia Server from any client PC on their network. All of connections used by the Vertigo Suite applications are over TCP and UDP, using the configurable range of ports listed below:

Description	Port #	Protocol
Client application connection (Primary connection)	14050	TCP
Client application connection (Back channel)	14051	TCP
Publish connection (Back channel)	14052	TCP
DataServer primary connection	10460	TCP
XPublish Agent publishing port	15000	TCP
MOS low port	10540	TCP
MOS high port	10541	TCP
Discovery port	15098	UDP
Discovery port	15099	UDP
Device connections (client apps to device)	4000	TCP

VertigoXmedia Data Server service

The Data Server is a service that runs in the background on the Xmedia Server and is responsible for managing data coming from various feeds by providing live updates of data values when requested, and distributing the data to the appropriate recipients (figure 3-2).

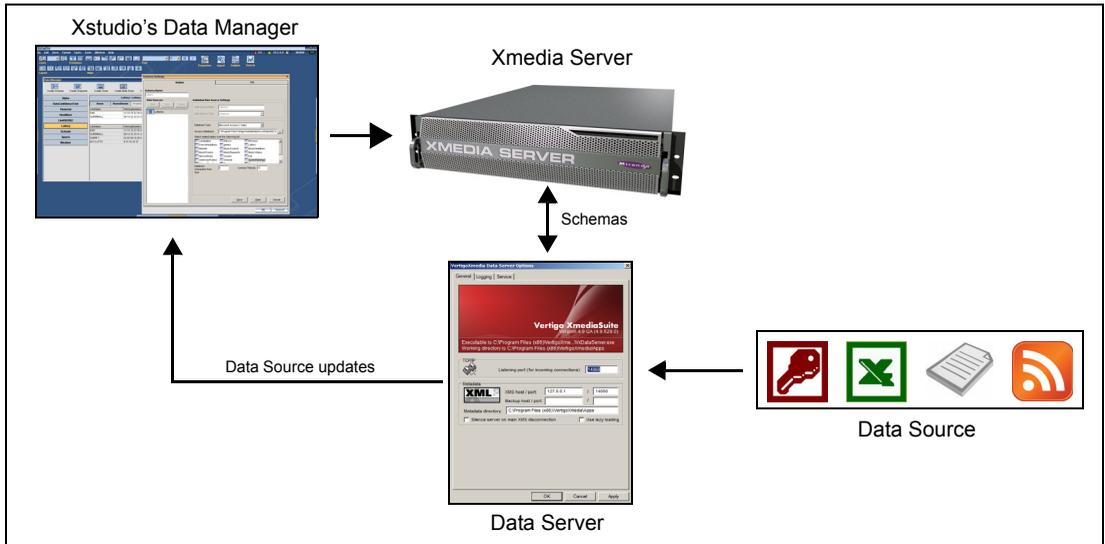


Figure 3-2. The Data Server manages and distributes data from various data sources

The **DATA SERVER CONTROL PANEL** (VertigoXmedia Data Server Option window) is the user interface that is used to configure and control the Data Server service (figure 3-3). You can open the Data Server Control Panel by selecting:

START > SETTINGS > CONTROL PANEL > VERTIGOXMEDIA DATA SERVER.



Figure 3-3. The Data Server Control Panel

The Data Server Control Panel features three (3) tabbed pages that contain parameters for configuring the connection, metadata, and logging options, as well as stopping and starting the Data Server service.

The upper portion of the Data Server Control Panel's **GENERAL** page identifies the Data Server's software version, the directory path where the Data Server's executable file is located, and the working directory path.



The following sections provide information and instructions for how to use the Data Server Control Panel to configure and manage the Data Server service.

- [“Setting the Data Server’s connection parameters” on page 3-7](#)
- [“Logging Data Server events” on page 3-9](#)
- [“Controlling the Data Server service” on page 3-11](#)

Setting the Data Server's connection parameters

The Data Server Control Panel's **GENERAL** page features parameters that allow the Data Server to connect and communicate with the Xmedia Server.

The **TCP/IP** section on the **GENERAL** page allows you to set the communication port number at which the Data Server listens for incoming data. Figure 3-4 demonstrates that the Data Server Control Panel's **LISTENING PORT** field must always be set to **14060**.

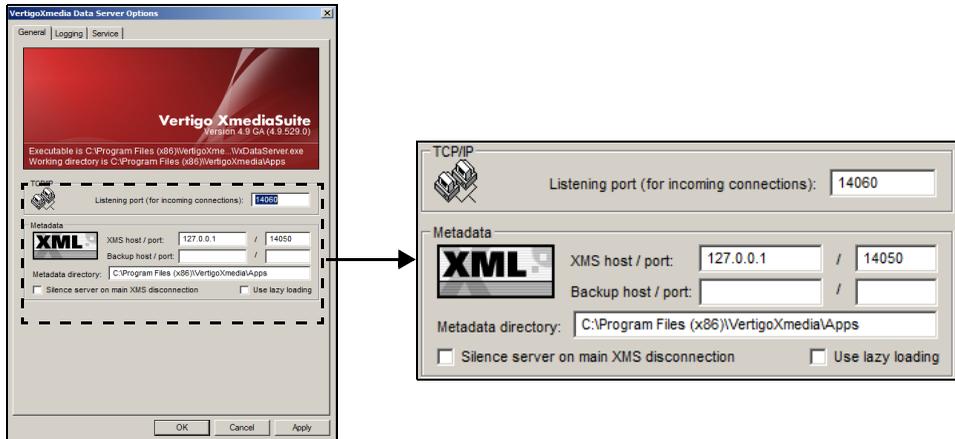


Figure 3-4. Setting the Data Server's communication port

The following table describes the parameters in the **METADATA** section on the **GENERAL** page, which determine the Data Server's settings for connecting and communicating with the Xmedia Server(s).

XMS HOST / PORT	<p>These settings are used to identify the primary Xmedia Server that the Data Server will connect to.</p> <ul style="list-style-type: none"> Specify the IP address or machine name of the Xmedia Server that hosts the XMS Service. Specify the communication port that allows a service to connect to an Xmedia Server. Typically, the port number is 14050.
BACKUP XMS HOST / PORT	<p>When operating within a server replication setup, these settings are used to identify the secondary Xmedia Server that the Data Server will connect to if the primary XMS server fails to respond.</p> <ul style="list-style-type: none"> Specify the IP address or machine name of the secondary Xmedia Server in the BACKUP HOST field. Specify the communication port of the secondary Xmedia Server in the BACKUP PORT field. Typically, the port number is 14050.

METADATA DIRECTORY	<p>Specify the directory path to the METADATA folder that contains all of the xml data that the data server needs to retrieve data. The folder is usually stored in C:\Program Files\VertigoXmedia\Apps\.</p> <p>This folder is primarily used when the data server can no longer connect to the XMS.</p>
SILENCE SERVER ON MAIN XMS CONNECTION	<p>This setting has been primarily replaced by the CONTROL THE DATASERVER setting on the Xmedia Server Control Panel's SERVICE CONTROL page (see page 15-5).</p> <p>When enabled, this setting causes the Data Server service to cease if the Xmedia Server connection is lost. In a replication setup, this condition forces a failover to the secondary Xmedia Server.</p>
USE LAZY LOADING	<p>When enabled, the Data Server does not parse the schemas until they are requested.</p>

Logging Data Server events

The Data Server Panel's **LOGGING** page (figure 3-5) allows you to set parameters to create a logging criteria that records the status of Data Server events. The resulting logging information is recorded and saved to a `DataServer*.log` file, which can be opened a basic text editor to determine whether the Data Server is being used correctly or help diagnose error conditions.

✓ NOTE

Be aware that logging may adversely affect the product's performance, especially on air performance. Therefore, we recommend enabling logging only when you are troubleshooting.

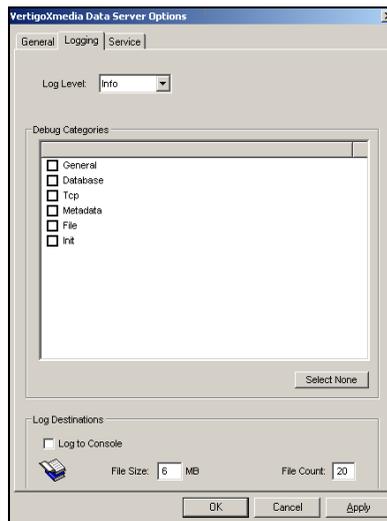


Figure 3-5. Data Server Panel's Logging page

The Data Server's **Logging Levels** and **Debug Categories** settings allow you to specify the type and categories of events that you want to be recorded in the Xmedia Server log files.

Log Level

This sets the default log level used by all logging categories except those that have been checked in the Debug Categories list. The choices are:

- **Error** - Only log errors and essential operations.
- **Warn** - Log unsuccessful operations that may indicate a problem (in addition to all messages logged at the Error level).
- **Info** - (Default) Log important events that occur during normal conditions (in addition to all messages logged at the Warn level).

It is recommended to set the **Log Level** to **Info** in order to provide enough information in the logs to diagnose common problems without affecting performance.

Debug Categories

Select the types of debug logging (categories) that you would like to record in the Data Server log file:

- **GENERAL** - General logging that does not fit under any other category.
- **DATABASE** - Database connections
- **TCP** - Network
- **METADATA** - Data source parsing
- **FILE** - File handling
- **INIT** - Startup and process initialization

The **SELECT NONE** button de-selects all of the Debug categories at once.

Log Destinations

All log files related to Vertigo Suite products are centrally archived in the Xmedia Server

- **LOG TO CONSOLE:** Currently not available for external use. The events are written to a console for Grass Valley personnel to use for testing and debugging tasks.
- **FILE SIZE** - Sets the maximum memory size for each log file created per run. The default value is 6 MB.
- **FILE COUNT** - Specifies the maximum number of DataServer*.log files that will be stored. A large enough number should be chosen to store over a day's worth of logs. This way if a problem happens the relevant log files will be available. Once the maximum number of files is reached, the oldest log file will be replaced by a new one. The default value is 20.

To access and view the contents of the most recent or archived DataServer*.log files:

1. Open Windows Explorer and navigate to the Vertigo Suite's log folder:
C:\Documents and Settings\All Users\Application Data\VertigoXmedia\Logs
2. Click on the **NAME** column's heading to sort the files.
3. Double click the DataServer*.log file that you want to display and it opens in a text editor (i.e. Notepad).

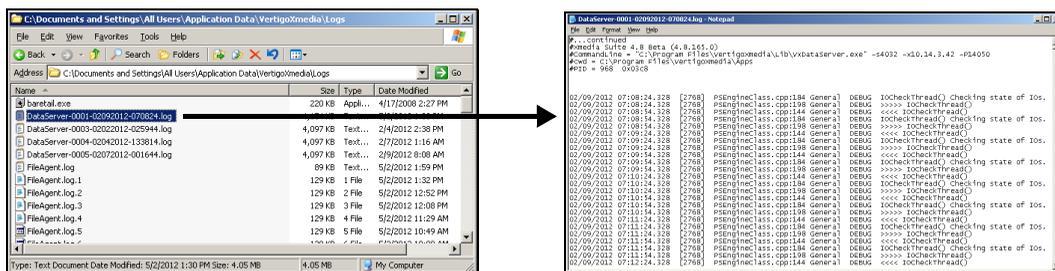


Figure 3-6. Accessing the Data Server log files

Controlling the Data Server service

By default, the Data Server service is set to automatically start when its host machine (i.e. Xmedia Server) is started. You can then use the controls on the Data Server Panel's **SERVICE** page to stop and start the service (figure 3-7). The service's current state (started or stopped) is always reported on this page as well.

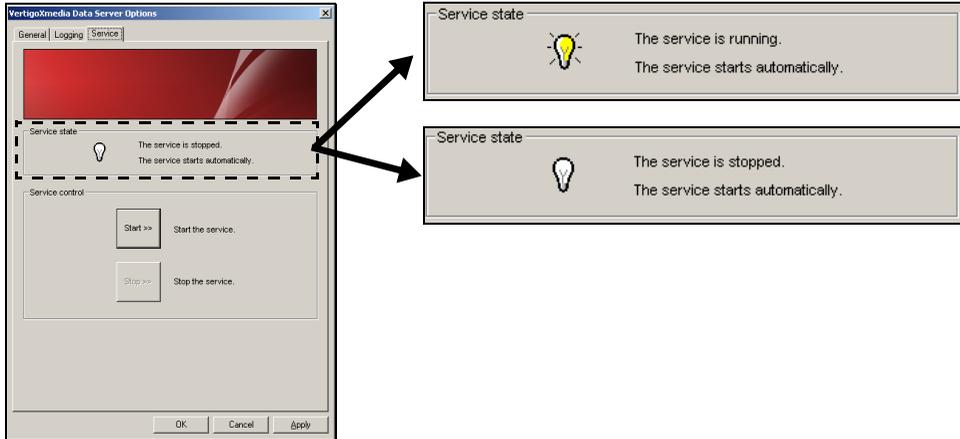


Figure 3-7. Manual controls for starting and stopping the Data Server service

In a replication environment, we recommend that authority to start and stop the Data Server service be given to the Xmedia Server by enabling the **CONTROL THE DATASERVER** setting on the Xmedia Server Control Panel (figure 3-8). The **CONTROL THE DATASERVER** setting ties the control of the Data Server service to the starting and stopping of the XMS service. Enabling this setting ensures the Data Server remains paired with the Xmedia Server at all times in the replication environment (see [page 15-5](#) for more information).

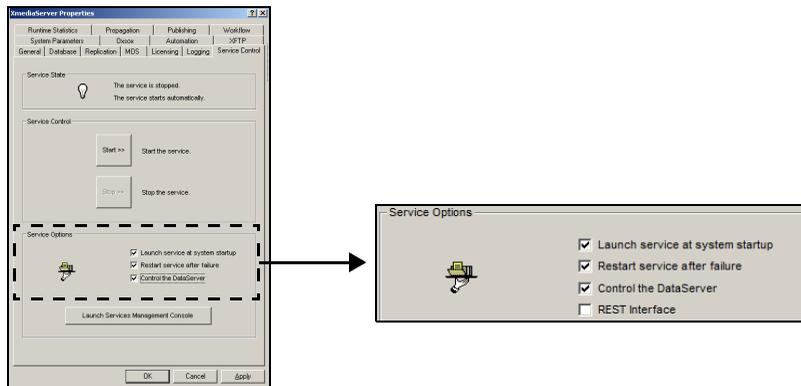
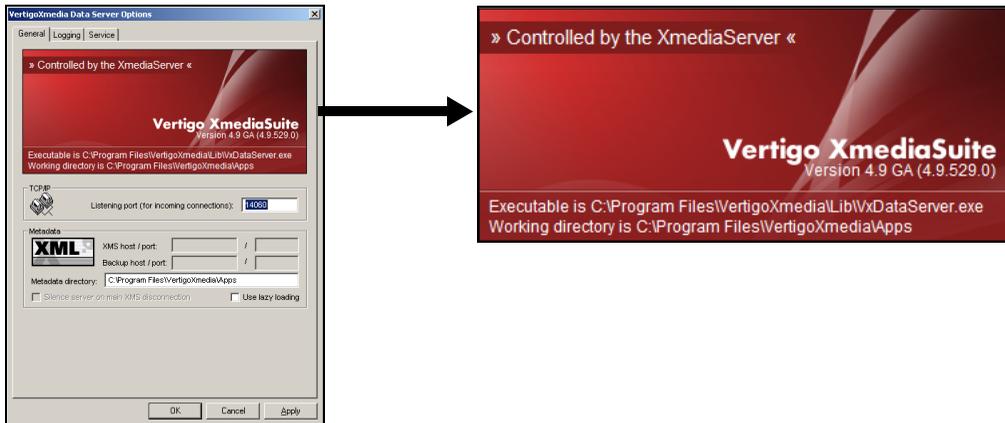


Figure 3-8. Configure the Xmedia Server Control Panel to control the Data Server service

The figures below demonstrate that once the **CONTROL THE DATASERVER** setting is enabled, the following changes are applied to the Data Server panel's **GENERAL** and **SERVICE** pages:

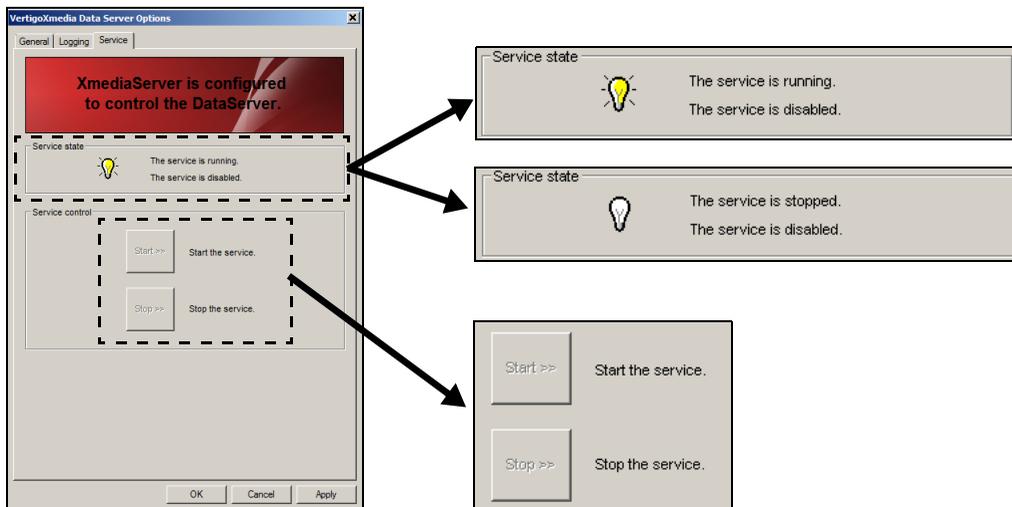
General Page

- The upper portion of the **General** page's software identification banner reads: **CONTROLLED BY THE XMEDIA SERVER.**



Service Page

- The manual start and stop controls become disabled
- The upper panel displays the following message: **XMEDIA SERVER IS CONFIGURED TO CONTROL THE DATASERVER**
- The **SERVICE STATE** message reports that the service is **DISABLED**, rather than **START AUTOMATICALLY**



File Ingest Server and Transcode Server

The Vertigo File Ingest Server is a service responsible for automatically ingesting media into the Xmedia Server from a user-created ingest folder. The File Ingest Server is also responsible for issuing media conversion requests to the Transcode Server, which is the service responsible for transcoding media from one format to another.

File Ingest Server can be configured to watch one or more folders by defining one or more *instances* of the ingest service in the configuration file. Each instance defines the set of rules that are mapped to each ingest folder being watched.

Information and instructions for using the File Ingest Server and Transcode Server are provided in [“Ingesting media files using the File Ingest Server” on page 20-1](#).

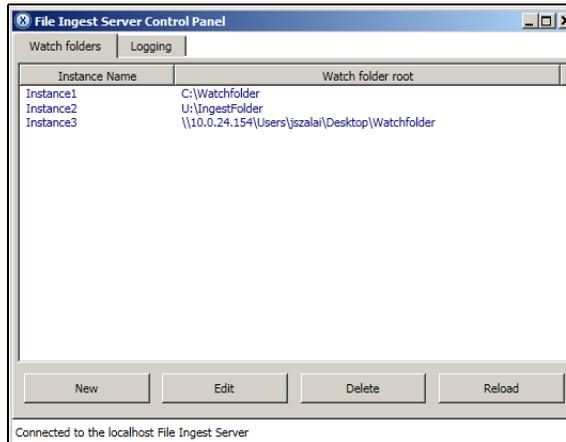


Figure 3-9. File Ingest Server Control Panel

Xmedia Server Control Panel - XmediaServer Properties Window

The user interface for configuring and controlling the Xmedia Server is the **XMEDIA SERVER CONTROL PANEL** (figure 3-10). The Xmedia Server Control Panel features fifteen (15) tabbed pages that contain parameters and settings related to the configuration and functioning of the Xmedia Server.



Figure 3-10. The Xmedia Server Control Panel

✓ NOTE

Although the title bar of this window displays **XMEDIA SERVER PROPERTIES**, it is most commonly referred to as the **XMEDIA SERVER CONTROL PANEL**.

Once the Xmedia Server has been installed, you can open the Xmedia Server Control Panel window by selecting: **START > SETTINGS > CONTROL PANEL > VERTIGOXMEDIA XMEDIA SERVER**.

Behind the Xmedia Server Control Panel's user interface runs the **XMS SERVICE** application. The XMS service's main responsibilities are to manage the Xmedia Server's interaction with the Vertigo Suite applications and to define the configuration settings for different Xmedia system setups and uses.

In most cases, the XMS Service is set to automatically launch when the Xmedia Server is started and it runs in the background, regardless of whether or not any applications from the Vertigo Suite have been opened. If the XMS service fails to start, the Xmedia Server Control Panel's **SERVICE CONTROL** page allows you to verify the status of the XMS Service (figure 3-11) and restart the service if necessary. See ["Controlling the XMS service" on page 15-1](#) for more information.

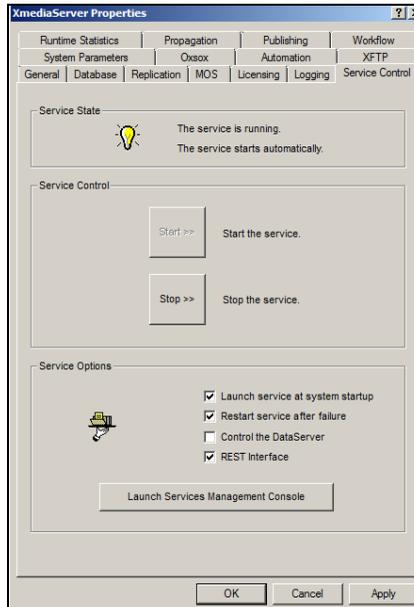


Figure 3-11. The Service Control page displays the state of the XMS Service

Xmedia Server Control Panel's settings pages

The following table describes the Xmedia Server Control Panel's fifteen (15) tabbed pages that contain the parameters and settings that are used to configure the Xmedia Server to interact with the Vertigo Suite applications and offer extended functionality.

Xmedia Server Control Panel Tab	Description
GENERAL	<p>The GENERAL tab displays the Xmedia Server Control Panel's product information, as well as parameters for configuring the XMS's communication port and directories. This page also features the Authorization Manager Configuration settings, which are used for enabling user rights management.</p> <p>See "The XMS's general configuration settings" on page 4-1 for more information about setting the parameters on the GENERAL page.</p>
DATABASE	<p>The DATABASE tab allows you to select and configure the Xmedia Server's database settings, as well as how to take a backup of the SQL Server database.</p> <p>See "Verifying the XMS's database settings" on page 5-1 for more information about setting the parameters on the DATABASE page.</p>
REPLICATION	<p>The REPLICATION tab allows you to configure the current Xmedia Server to participate in a replication setup, which offers full redundancy for near instant failover with no interruption in services including on-air playout.</p> <p>See "Replication of the XMS Server's database" on page 6-1 for more information about setting the parameters on the REPLICATION page.</p>
MOS	<p>The MOS tab allows you to configure the Xmedia Server to integrate with a newsroom control system. The Xmedia Server can then provide graphics assets to newsroom environments using the MOS protocol.</p> <p>See "MOS Server configuration and monitoring" on page 7-1 for more information about setting the parameters on the MOS page.</p>
LICENSING	<p>The LICENSING tab allows you to view, add, and remove the software licenses that are required to operate each of the Vertigo Suite applications.</p> <p>See "License management" on page 8-1 for more information about setting the parameters on the LICENSING page.</p>
LOGGING	<p>The LOGGING tab allows you to set parameters for creating and viewing a log file that records the status of events while the Xmedia Server is operating.</p> <p>See "Logging Xmedia Server events" on page 9-1 for more information about setting the parameters on the LOGGING page.</p>

SERVICE CONTROL	<p>The SERVICE CONTROL tab displays the current state of the XMS Service. It also allows you to manually stop and start the XMS service, and set Service Options for automatically restarting the XMS Service, linking the XMS to the DataServer and/or enabling the REST Interface functionality.</p> <p>See “Controlling the XMS service” on page 15-1 for more information about setting the parameters on the SERVICE CONTROL page.</p>
RUNTIME STATISTICS	<p>The RUNTIME STATISTICS tab displays a real-time tally of the content of the Xmedia Server’s database.</p> <p>See “Displaying XMS runtime statistics” on page 16-1 for more information about setting the parameters on the RUNTIME STATISTICS page.</p>
PROPAGATION	<p>The PROPAGATION tab allows you to create a hub and spoke asset distribution model in which assets can be created and propagated from a central hub to various spoke servers.</p> <p>See “Propagating assets to other Xmedia Servers” on page 17-1 for more information about setting the parameters on the PROPAGATION page.</p>
PUBLISHING	<p>The PUBLISHING tab displays a real-time view of the status of media assets that are currently being published. This view allows you to easily clear/cancel some or all of the pending publish requests. This tab also allows you to enable the insta-publish device option.</p> <p>See “Setting and monitoring the XMS publishing activities” on page 18-1 for more information about setting the parameters on the PUBLISHING page.</p>
WORKFLOW	<p>The WORKFLOW tab allows you to create a work order workflow that is used for requesting, completing, tracking and approving graphics work orders.</p> <p>See “Work Order workflow configuration” on page 10-1 for more information about setting the parameters on the WORKFLOW page.</p>
SYSTEM PARAMETERS	<p>The SYSTEM PARAMETERS page allows you to set the rate at which media objects are ingesting into the Xmedia Server, at what time expired published and archived assets will be purged, and the system’s field rate.</p> <p>See “Setting the XMS system parameters” on page 11-1 for more information about setting the parameters on the SYSTEM PARAMETERS page.</p>
OxSOX	<p>The OxSox tab allows you to configure the Xmedia Server to communicate with the ImageStore Media Manager (IMM) or/and Xplorer applications, which both use the Oxsox protocol.</p> <p>See “OxSox connection settings” on page 12-1 for more information about setting the parameters on the OxSOX page.</p>

AUTOMATION	<p>The Xmedia Server Control Panel's AUTOMATION page configures the Xmedia Server to communicate with a specific automation system for the purposes of publishing to devices based on the automation system's schedule.</p> <p>See “The XMS automation parameters for scheduled-based publishing” on page 13-1 for more information about setting the parameters on the AUTOMATION page.</p> <p>*** Note ***</p> <p>Although the Automation page still exists on the Xmedia Serve Control Panel, the functionality of scheduled-based publishing has been deprecated.</p>
XFTP	<p>Although the XFTP page still exists on the Xmedia Serve Control Panel, the functionality of importing files using a FTP server running locally on the Xmedia Server been deprecated.</p>

4 THE XMS'S GENERAL CONFIGURATION SETTINGS

The **GENERAL** page on the Xmedia Server Control Panel (figure 4-1) allows you to view and set some of the Xmedia Server's basic configuration and connection settings. The **GENERAL** page is divided into three (3) thematic areas and each is described in the following sections:

- [“Viewing the Xmedia Server’s product information” on page 4-2](#)
- [“Configuring the XMS’s network connection and directories” on page 4-3](#)
- [“Configuring the Authorization Manager” on page 4-4](#)



Figure 4-1. The General tab on the Xmedia Server Control Panel

Viewing the Xmedia Server's product information

The Xmedia Server Control Panel's **GENERAL** page provides a quick view of the Xmedia Server's product information (figure 4-2). This page displays the following three (3) pieces of information regarding the Xmedia Server:

- **Version:** Identifies the version and build number of the Vertigo Suite that is currently installed and running on the Xmedia Server.
- **Executable is:** Identifies the full directory path of where the Xmedia Server executable file is located.
- **Working directory:** Identifies the full directory path of the VertigoXmedia Apps folder that contains the Vertigo Suite's .ini files, license files, some log files, and some MOS-related XML files.

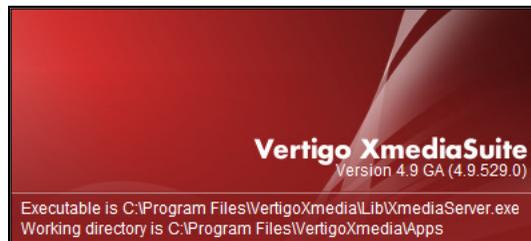


Figure 4-2. Xmedia Server product information on the Xmedia Server Control Panel's General page

Configuring the XMS's network connection and directories

The Xmedia Server Control Panel's **GENERAL** page (figure 4-2) features two sections that allow you to specify and view the Xmedia Server's communication port and the full directory paths where the XMS stores or retrieves information from. The following table provides more details about each field in these sections:

TCP/IP Configuration	Listen for incoming connections on port: The port number at which the Xmedia Server (XMS) will listen. IP address is the local IP.
Directories Configuration	<p>Virtual database path: The full directory path to the Virtual Database (VDB). The Virtual Database is a directory structure that contains all the hard assets that the XMS stores.</p> <p>Working folder: Identifies the full directory path of the VertigoXmedia Apps folder that contains the Vertigo Suite's .ini files, license files, some log files, and some MOS-related XML files.</p> <p>Filter directory: The full path to of the directory that contains filters such a LEAD tools filters. Filters are used to convert data from one format to another.</p>

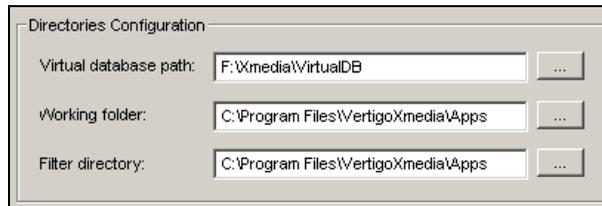


Figure 4-3. Xmedia Server connection and directories on the Xmedia Server Control Panel's General page

Configuring the Authorization Manager

The Vertigo Suite offers system administrators and workflow managers the possibility of restricting access to some of the functionality on a per-user basis using the Xmedia Server and the operations, tasks, and roles defined in Microsoft's Authorization Manager (see ["User rights management" on page 19-1](#) for more information).

Use of the Vertigo Suite's User Rights Management is completely optional and it can be configured, enabled, or disabled using the settings on the Xmedia Server Control Panel's **GENERAL** page (figure [4-4](#)).

Authorization Manager Configuration	<p>Enabled: If checked, it will ensure that next time the XMS runs, it will create a shared directory called AzMan in the working directory. Furthermore, it enables the authorization manager in the Xmedia Server.</p> <p>Policy store URL: Specifies the path of the policy store, which is a file that helps the AzMan coordinate user rights management. The file is stored in either the active directory or on disk as an XML file.</p> <p>Application name: The name of the object that contains rights for the user in the application.</p>
-------------------------------------	---

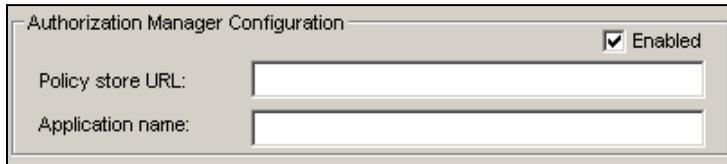


Figure 4-4. The Authorization Manager portion of the Xmedia Server Control Panel's General page

5 VERIFYING THE XMS'S DATABASE SETTINGS

The Xmedia Server uses a **Microsoft SQL Server database** to store asset details, categories, work order processing data, publish processing data, and other relational information and data.

The following sections describe how to use the Xmedia Server Control Panel's **DATABASE** page to verify the Xmedia Server's database settings, as well as how to take a backup of the SQL Server database:

- [“Verifying the SQL Server database settings” on page 5-2](#)
- [“Making a backup of the SQL Server database” on page 5-4](#)

NOTE

The Xmedia Server's database settings have been factory configured and/or commissioned by qualified Grass Valley professionals. Although this chapter instructs users on how to verify the Xmedia Server Control Panel's database settings, we strongly discourage users from making changes to database settings without the guidance of our Technical Support department (support@miranda.com).

Verifying the SQL Server database settings

The Vertigo Suite uses a Microsoft SQL Server database to store and manage asset details, categories, work order processing data, publish processing data, and other relational information and data. The following instructions describe how to verify the **MS SQL SERVER SETTINGS** on the Xmedia Server Control Panel's **Database** page (figure 5-1)

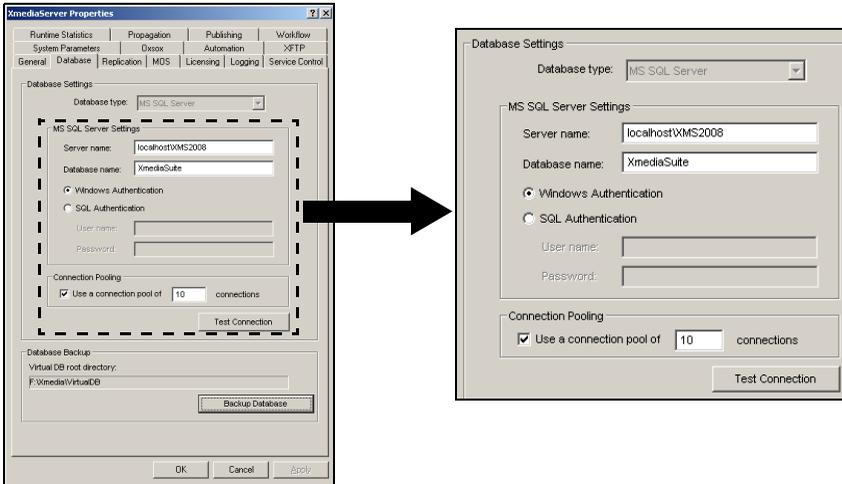


Figure 5-1. The MS SQL Server settings

To verify the MS SQL Server settings:

1. Select the **DATABASE** tab on the Xmedia Server Control Panel.
2. Verify that **MS SQL SERVER** is displayed in the **DATABASE TYPE** field.
3. Click the **TEST CONNECTION** button to verify the connection to the database.

The connection test validates the current **MS SQL SETTINGS** values. If the **TEST DATABASE CONNECTION** pop-up window reports a successful connection (figure 5-2), this indicates that all of the current settings are valid and you do not need to continue the verification procedure.

If the **TEST DATABASE CONNECTION** pop-up window reports a failed connection (figure 5-2), the current **MS SQL SERVER SETTINGS** are invalid and you must continue with this procedure to verify these settings.

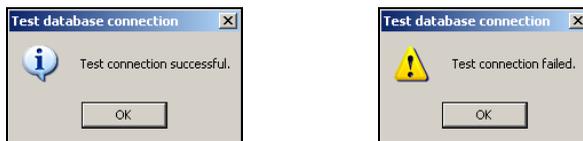


Figure 5-2. Testing the database connection is a quick way to verify the validity of the SQL Server settings

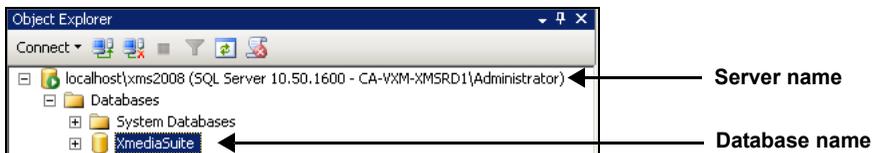
4. Verify that the **SERVER NAME** and the **DATABASE NAME** fields are accurate on the Xmedia Server Control Panel's **Database** settings page.

The server and database names can be obtained by opening the **SQL SERVER MANAGEMENT STUDIO**.

- a. Open the **SQL SERVER MANAGEMENT STUDIO** by selecting **START> PROGRAMS> MICROSOFT SQL SERVER 2008 R2>SQL SERVER MANAGEMENT STUDIO**.
- b. Click **CONNECT** in the **CONNECT TO SERVER** window.



- c. In the **Object Explorer** panel of the **Microsoft SQL Server Management Studio** window, expand the **DATABASES** folder to display the name of the database.



- d. Verify that the server name and database name match those specified on the Xmedia Server Control Panel's **Database** settings page.
5. Verify that the **USER NAME** and **PASSWORD** fields are accurate.
The **USER NAME** and **PASSWORD** provides a security measure to ensure that only the qualified user (i.e. the system administrator) has permission to connect, write, and read to the database.
By default these fields are both set to **sa**. Contact your system administrator if the **USER NAME** or **PASSWORD** appear to be different than the default.
 6. Verify that **CONNECTION POOLING** is enabled and set to **10**.
When this setting is enabled, the value specified establishes the number of connections in the connection pool. Having a connection pool helps the Xmedia Server service its clients in a timely fashion. When this setting is disabled, it will not use a connection pool to the database and it will have only a single connection.
 7. Click the **TEST CONNECTION** button to verify the validity of the settings and the connection to the database.
If the **TEST DATABASE CONNECTION** pop-up window again reports a failed connection, contact our Technical Support department for assistance (support@miranda.com).

Making a backup of the SQL Server database

The **DATABASE BACKUP** section of the Database page (figure 5-3) allows you to create or update a backup of the Xmedia Server's MS SQL Server database.

When the **BACKUP DATABASE** button is selected, the osql utility is executed and a backup file (**XmediaSuite.bak**) is created/updated and saved within the root folder of the server's Virtual Database (as indicated by the directory path in the **VIRTUAL DB ROOT DIRECTORY** field).

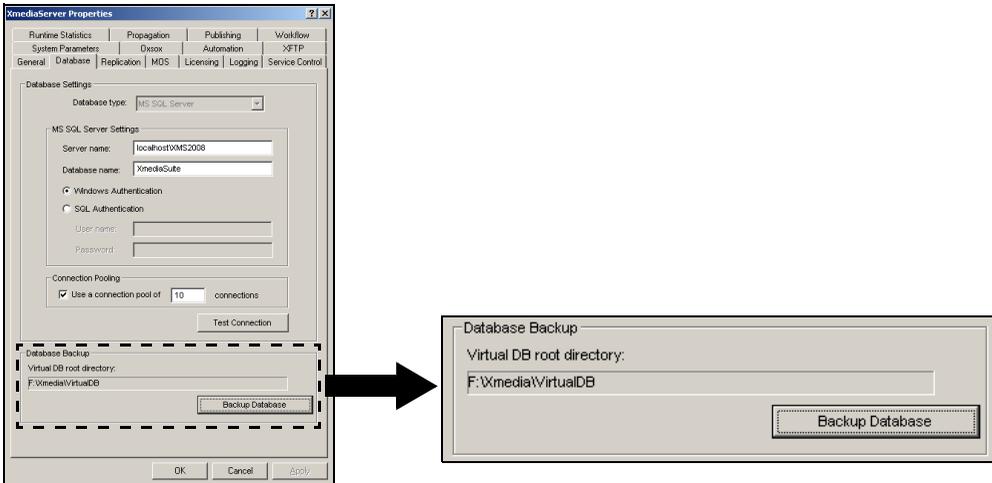


Figure 5-3. Create or update a backup of the Xmedia Server's MS SQL Database

6 REPLICATION OF THE XMS SERVER'S DATABASE

Replication enables full redundancy of an Xmedia Server that is available for near instant failover with no interruption in services including on-air playout.

The Xmedia Server implements a simple technique of replicating all events that change the database and/or virtual database (VDB). Two identically versioned Xmedia Servers (Primary and Secondary) communicate with each other to ensure database replicas by queuing all commands that alter the state of the database (and/or VDB) to disk. These commands are then sequentially executed on the secondary server as if it were a normal client with a few distinctions.

The primary server's connection to the secondary server is distinct in that the secondary server does not send normal replies to the primary server. Instead, it replies with simple acknowledgements. Most data altering commands consist of user-invoked changes such as Template saving, whereas other hidden changes, such as publish history and licensing changes such as soft-key ingestion, are also replicated.

At all times both servers are running and the secondary server is ready to take control when a failover condition arises at any time. Both servers contain identical licensing information and each has their own dongle with matching customer IDs. Each server is responsible for monitoring network conditions and each other's availability.

The following sections further describe the conditions and behavior of the Xmedia Servers replication. Instructions are also provided to guide you through the process of setting up and enabling server replication.

- [“Conditions that trigger a failover” on page 6-2](#)
- [“MOS Enabled Replication” on page 6-3](#)
- [“Replication settings on the Xmedia Server Control Panel” on page 6-4](#)
- [“Setting up and enabling Xmedia Server replication” on page 6-6](#)

Conditions that trigger a failover

The primary server makes an active TCP connection to the secondary on its main XMS port, which is typically 14050. When this connection is dropped, there are two perspectives from which to describe. Firstly, if the secondary server dropped the connection, then the primary server immediately attempts to reconnect and periodically tries on defined intervals (in seconds), while it remains running as usual. Secondly, if the primary server dropped the connection, the secondary server slips into a temporary wait state awaiting the primary server's reconnection for a period of time in seconds. If the primary server has not reconnected within the defined period, the secondary server assumes control and begins accepting connections from clients.

A failover occurs when one or more of the following conditions are met:

- The primary Xmedia Server service is stopped.
- The primary server loses network connectivity.
- The primary Xmedia Server service involuntarily crashes.
- The primary server tells the secondary server to takeover for otherwise unknown purposes, see the primary server's log file.
- The primary server loses its connection with the SQL server database.
- The primary server is powered off.

The secondary server assumes control by accepting connections from clients only when the primary server is inoperable. While the secondary server is accepting connections it queues the data changing events to disk, exactly like the primary server does when operating normally. While the secondary server is live, it periodically checks for primary server availability by attempting to connect to it.

Once the primary server is back online, the secondary server unloads the queue to the primary server, and when the queue is empty, the primary server resumes control and the secondary server resumes its role. The primary server is operable whenever it is running and the backlog queue from the secondary server is emptied.

MOS Enabled Replication

When MOS is enabled in the Xmedia Server Control Panel (see [page 7-1](#)), additional replication requirements must be met. The Newsroom Control System (NCS), which requires the Xmedia Server MOS presence, is configured to be aware of the Xmedia Server using a single IP address, which is often referred to as the Virtual IP address.

Figure 6-1 demonstrates that in MOS enabled environments the primary XMS adds the virtual IP address to the public network adapter. On failover, the primary server releases the virtual IP and the secondary server adds the IP address to its public network adapter. Since the two servers cannot concurrently support the same IP address, the Xmonitor service is responsible for removing the Virtual IP address from the public network adapter of the primary computer when the primary XMS tells it to, or when it suddenly stops or crashes. It functions the same way on the secondary server as well. Without the Xmonitor service, messages would appear on the network indicating an IP address conflict on the network.

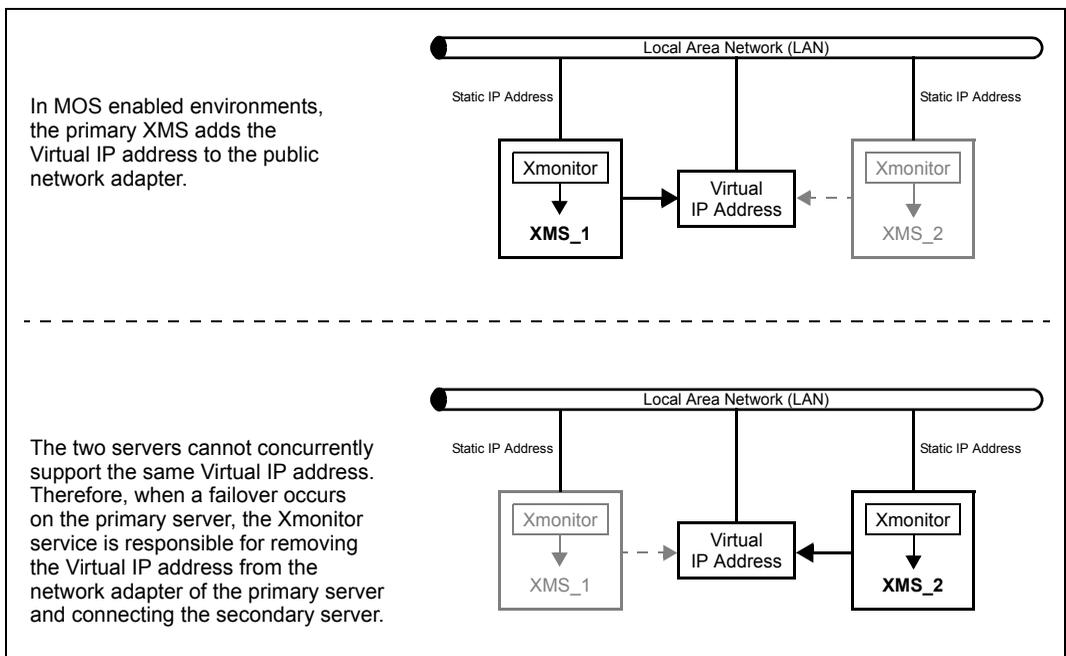


Figure 6-1. A Virtual IP Address must be available for replication when MOS is enabled

The `Xmonitor.exe` is part of the standard install, but it is not automatically configured to run as a permanent service. Therefore, as part of the replication setup you must manually install and start the Xmonitor service. See [“Verify and/or install the Vertigo Xmonitor service” on page 6-11](#) for instructions and further information regarding the Xmonitor service.

Replication settings on the Xmedia Server Control Panel

Replication is setup and enable using the Xmedia Server Control Panel's **REPLICATION** page on both the primary and secondary servers (figure 6-2). To open the Xmedia Server Control Panel, select **Start>Settings>Control Panel>VertigoXmedia XmediaServer** and then select the **REPLICATION** tab.

While the table below describes each of the settings on the **REPLICATION** page, instructions for using these settings to implement server replication are provided on [page 6-13](#).

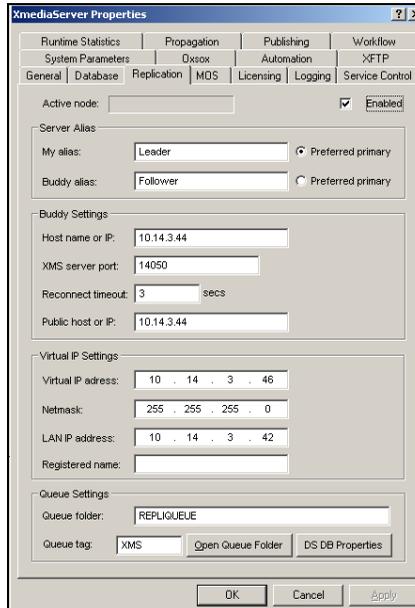


Figure 6-2. Replication settings on the Xmedia Server Control Panel

ENABLED	Selecting this check box enables the particular server for replication. Deselecting the check box disables replication. For replication to be activated between the primary and secondary servers, this setting must be active on each of the server's Xmedia Server Control Panels.
SERVER ALIAS	<p>MY ALIAS: Defines the name given to the primary server. We recommend naming it "Primary".</p> <p>BUDDY ALIAS: The name of the secondary server. We recommend naming it "Secondary".</p> <p>PREFERRED PRIMARY: Specifies the name of the chosen primary server.</p>

BUDDY SETTINGS	<p>HOST NAME OR IP: The name or IP address of the peer host. It is specifically the name as it is known to this server. It is typically the same as "PeerPublicHost". However, it can be different if you chose to use a private network between the two nodes. In this case, you would put the private network IP address of the peer.</p> <p>XMS SERVER PORT: The port that the peer XMS is listening on. This is typically, 14050.</p> <p>RECONNECT TIMEOUT: This is the period of time the secondary server waits for the primary server to reconnect before it switches itself to live mode. We recommend that this setting's value be set to 3.</p> <p>PUBLISH HOST OR IP: The hostname or IP address of the peer XMS server as it is known to the general network. This value is given to the clients so they know exactly where the peer XMS node is.</p>
VIRTUAL IP SETTINGS	<p>VIRTUAL IP ADDRESS: This is a third static IP address the two nodes of a replication setup toggle when live.</p> <p>NETMASK: This is typically 255.255.255.0</p> <p>LAN IP ADDRESS: The general IP address of the computer. The XMS monitors this IP address to detect network failure, and also binds the shared IP address to the adapter where this IP address is bound. Mandatory for MOS when using a shared IP address.</p> <p>REGISTERED NAME: If a shared IP address is added to the DNS of the network and given a name. You must put the exact fully qualified hostname bound to the shared IP address here. Otherwise, the XMS will not add the shared IP address to the public adapter.</p>
QUEUE SETTINGS	<p>QUEUE FOLDER: The full path of the folder where the XMS stores the queue of the replicated commands. If the drive letter is missing, it assumes that the folder is in the working folder of the XMS (see page 4-3). If the folder does not exist, the XMS creates it.</p> <p>QUEUE TAG: This is typically "XMS" and can be anything you choose. It is used as an identifier added to each filename in the queue folder. The queue tag does not have to match that of the peer's.</p> <p>OPEN QUEUE FOLDER: Opens an Explorer window to the Queue folder.</p> <p>DS DB PROPERTIES: This setting is for the DataServer on each node. If the DataServer is running centrally, which is recommended and usual practice, it should be provided with a default database. The default database is accessible in the Data Manager/Data Source dialog of Xstudio, where one chooses to use the default database rather than providing unique settings for the data source. The default database is unique per node, and is usually a separate database in the same SQL Server instance as the XmediaServer system database. This is how redundancy is created for DataServers. The Vertigo policy for populating the default databases is that the customer is fully responsible for providing data to each default database in the replication environment, and our system ensures that the DataServer instance stays paired with its relative XmediaServer instance.</p>

Setting up and enabling Xmedia Server replication

The procedure below identifies the high-level steps involved in setting up and enabling the replication service of the Xmedia Server's database. Subsequent sections (identified by the links within the procedure) provide step-by-step instructions for performing each step.

NOTE

It is recommended that you first read through the conceptual information contained on [page 6-1](#) before you proceed with the following procedure.

- 1. Verify that the two servers conform to the necessary replication requirements**
 - ["Verify the servers' dongles Machine IDs" on page 6-8](#)
 - ["Verify the registered licenses on both servers" on page 6-9](#)
 - ["Verify the SQL Server versions on both servers" on page 6-10](#)
 - ["Verify the XmediaServer software versions on both servers" on page 6-10](#)
 - ["Verify and/or install the Vertigo Xmonitor service" on page 6-11](#)
- 2. Specify the Replication settings on the primary server's Xmedia Server Control Panel**
 - ["Specify the Queue settings" on page 6-14](#)
 - ["Specify the Dataserver Database Connection settings" on page 6-15](#)
 - ["Specify the server's network settings in the Virtual IP Settings" on page 6-16](#)
 - ["Specify the Buddy settings" on page 6-17](#)
 - ["Specify the Server Alias settings" on page 6-18](#)
- 3. Specify the Replication settings on the secondary server's Xmedia Server Control Panel**
 - ["Specifying the Replication settings on the secondary server" on page 6-19](#)
- 4. Make a backup of the primary server's databases**
 - ["Make a backup of the primary server's database" on page 6-20](#)
- 5. Set the Control the Data Server option**
 - ["Setting the Control Data Server option" on page 6-20](#)
- 6. Specify the server settings on all client applications (i.e. Xstudio, Xplay, Xnews)**
 - ["Specifying the server settings on client applications" on page 6-21](#)
- 7. Verify proper functioning of the servers and replication**
 - ["Verifying proper functioning of the servers and replication" on page 6-23](#)

Server replication requirements

Before setting up or using Xmedia Server's replication, you should ensure that the servers respect the specific guidelines and requirements that are necessary to support replication. The following table briefly lists the mandatory requirements for Xmedia Server replication.

Licenses	A matching dongle on each machine is an absolute requirement and the servers' licenses must also be identical.
Database type	SQL Server is required.
Static IP Addresses	Acquire two mandatory static IP addresses from your IT department. These IP addresses are required to monitor network connectivity.
Virtual IP Address	Acquire an additional static IP address from your IT department. This IP address is only required for MOS Enabled environments.
Matching Software	Both servers (primary & secondary) must be using identical software versions (OS, SQL-Server, patch levels, MSXML, Vertigo Suite...etc.)
Xmonitor Service	The Xmonitor service must be installed on each server to maintain virtual IP address in a MOS Enabled environment.

Instructions for verifying that both servers conform to the replication requirements are provided in the following sections:

- [“Verify the servers' dongles Machine IDs” on page 6-8](#)
- [“Verify the registered licenses on both servers” on page 6-9](#)
- [“Verify the SQL Server versions on both servers” on page 6-10](#)
- [“Verify the XmediaServer software versions on both servers” on page 6-10](#)
- [“Verify and/or install the Vertigo Xmonitor service” on page 6-11](#)

Verify the servers' dongles Machine IDs

Each XMS server must have a dongle with a matching Machine ID (also known as Customer IDs). It is of paramount importance because when failed over, client applications must be able to connect without licensing issues.

To ensure that the two (2) dongles that are installed on the servers have identical Machine IDs:

1. On the primary server, open the Xmedia Server Control Panel.
2. Select the **LICENSING** tab (figure 6-3).
3. Select **SOFTKEYS** from the **LICENSE SERVER OPTIONS** drop-down list.
4. Take note of the Machine ID number.
5. Repeat steps 1 to 4 on the secondary server.
6. Confirm that the Machine IDs are an exact match. If they are not, contact one of our technical services representative.

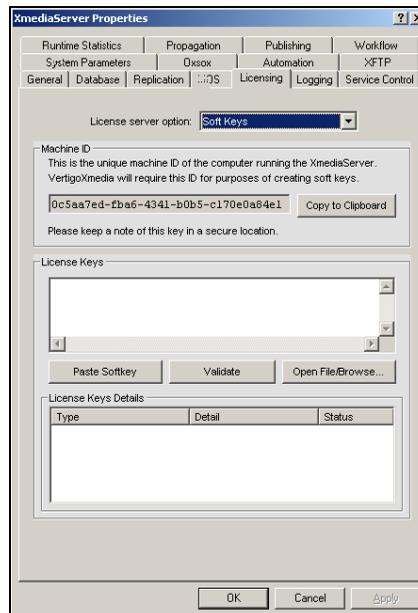


Figure 6-3. The dongle's Machine ID is displayed on the Xmedia Server Control Panel's Licensing page

Verify the registered licenses on both servers

Each XMS server must have exact duplicates of the `vxls.bin` license file. The XMS replicates soft-keys to maintain the licensing information at all times. Synchronizing scripts should take the `vxls.bin` file into account. Note that this verification must be done before replication is enabled, or while replication is disabled and there is no active primary server.

To ensure that the lists of registered licenses on the primary and secondary servers are identical:

1. On the primary server, open the Xmedia Server Control Panel.
2. Select the **REPLICATION** tab and ensure that Replication is disabled. Be sure that the **ENABLED** check box is cleared.
3. Select the **LICENSING** tab (figure 6-4).
4. Select **LICENSES** from the **LICENSE SERVER OPTIONS** drop-down list.
5. Take note of the licenses displayed on the **LICENSE SUMMARY** tab.
6. Repeat steps 1 to 4 on the secondary server.
7. Confirm that the licenses are an exact match. If they are not, choose the server that has the correct license list and copy its `vxsl.bin` file. Stop the XMS service on the server that is about to receive the license file, and then paste/replace the license file.

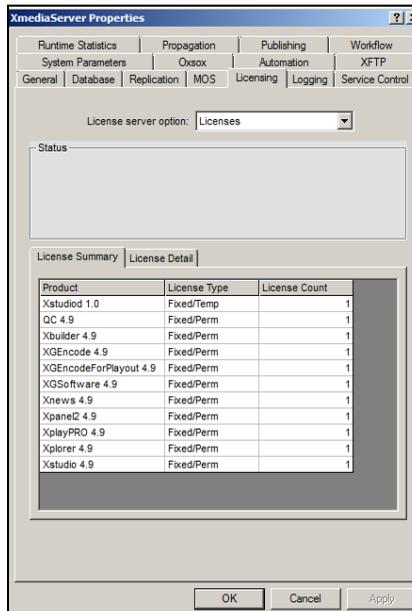


Figure 6-4. The server's licenses are displayed on the Xmedia Server Control Panel's Licensing page

Verify the SQL Server versions on both servers

Ensure that the SQL Server versions on the primary and secondary servers are identical by reading SQL-Server's program group label on the **Start** menu of both the primary and secondary server. Select **START>PROGRAMS>MICROSOFT SQL SERVER**. Figure 6-5 demonstrates that the version number is stated as part of the label.



Figure 6-5. The Start menu provides a quick reference to identify the SQL Server software version

Verify the XmediaServer software versions on both servers

Ensure that both the primary and secondary servers are running the same version of the VertigoXmedia XmediaServer software. Open the Xmedia Server Control Panel of each server and compare the software versions displayed on the **GENERAL** page (figure 6-6).

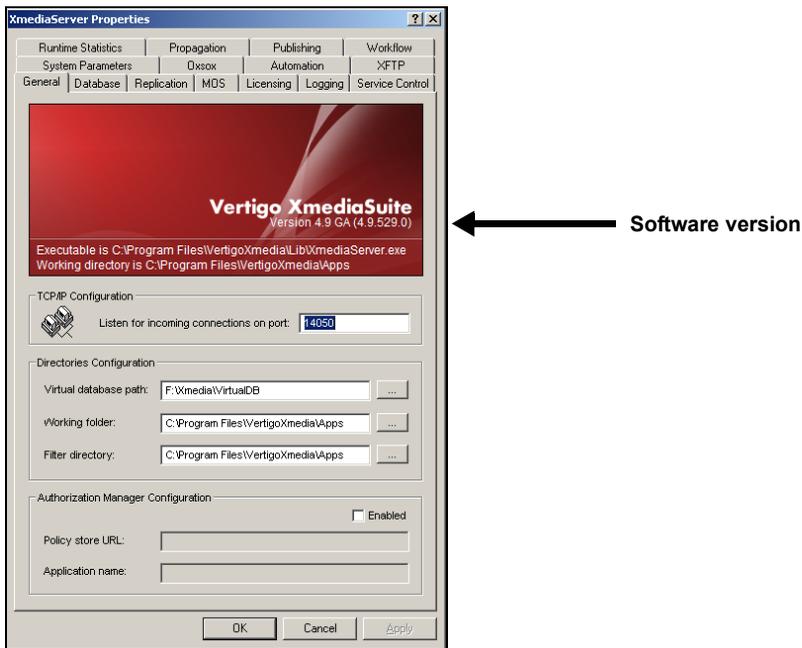


Figure 6-6. The version of the Vertigo Suite software is displayed on the General page

Verify and/or install the Vertigo Xmonitor service

In a newsroom environment, MOS enabled Xmedia servers require an additional IP address, referred to as the Virtual IP address. In a replication configuration, the two servers (primary and secondary) cannot concurrently support the Virtual IP address. Therefore, in the case of a primary server failover, the Xmonitor service is responsible for essentially transferring connectivity to the Virtual IP address from the primary to the secondary, and vice versa. See [“MOS Enabled Replication” on page 6-3](#) for more information.

The `Xmonitor.exe` is part of the standard install, but it is not automatically configured to run as a permanent service. Therefore, you must manually install and start the Xmonitor service *on both the primary and secondary servers*.

✓ NOTE

The installation and use of the Xmonitor service is only required for Xmedia Servers that are use in a newsroom environment where MOS is enabled. If this is not the case, then you do not need to proceed with this procedure.

To verify and/or install the Xmonitor service:

1. Verify if the Xmonitor service is already installed on the server.
 - a. Open the Xmedia Server Control Panel.
 - b. Select the **SERVICE CONTROL** tab.
 - c. Click the **LAUNCH SERVICES MANAGEMENT CONSOLE** button.
The **SERVICES CONSOLE** appears (figure [6-7](#)).

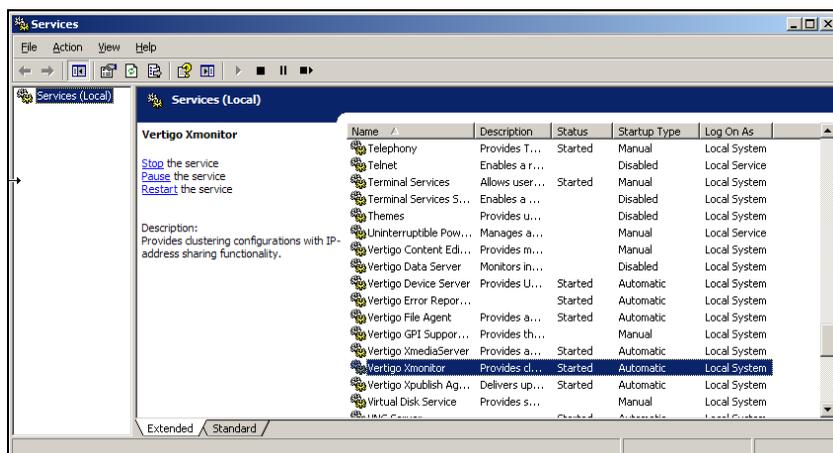


Figure 6-7. Microsoft's Services Console

- d. Navigate down the list of **SERVICES (LOCAL)**.
If the Vertigo Xmonitor service is already installed, it will be included in this list. Be sure that its **STATUS** is **STARTED**. If no status is displayed, continue to step 6 to start the service.
If the Vertigo Xmonitor service is not listed, then you must install the service.

2. Install the Xmonitor service.
 - a. Open the server's command prompt window (**START MENU > RUN** and type `cmd`, then press **ENTER**.)
 - b. At the prompt, type: `"%vxapps%"\.lib\xmonitor -i`
 - c. Press **ENTER**.

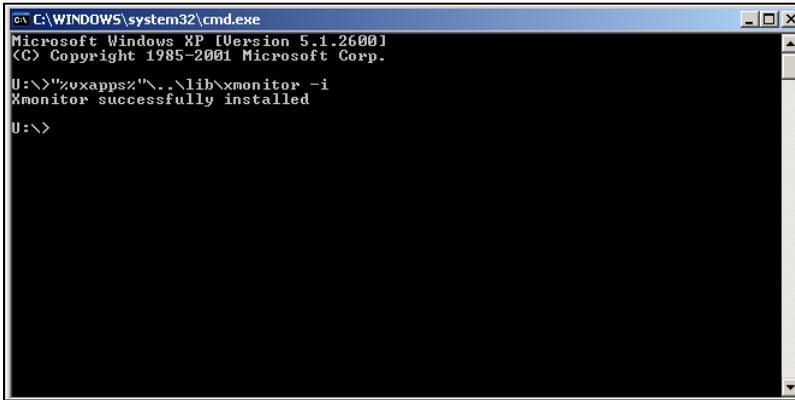


Figure 6-8. Launch the Vertigo Xmonitor installation from the command prompt

3. Start the Vertigo Xmonitor service.
 - a. Return to the Services Management Console and right-click the Vertigo Xmonitor listing.
 - b. Select the **Start** command from the context menu.

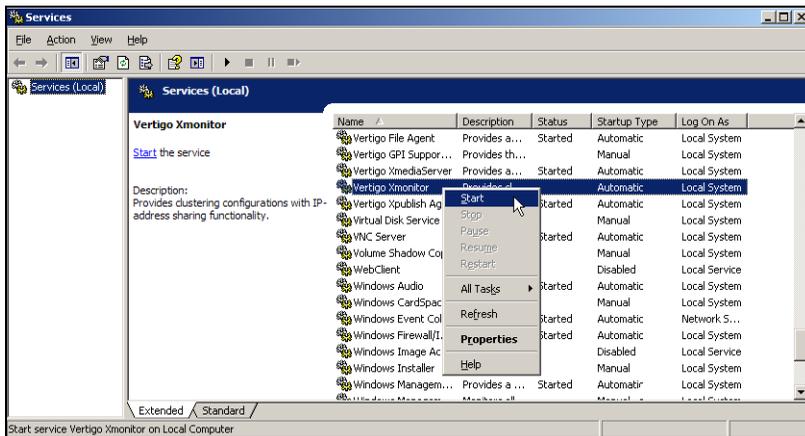


Figure 6-9. Start the Xmonitor service

4. Repeat the same procedure on the peer server (primary or secondary server).

Specifying the Replication settings on the primary server

The Xmedia Server Control Panel's **REPLICATION** page on the primary Xmedia Server contains all of the settings required to enable and configure the primary server for replication (figure [6-10](#)). The Xmedia Server Control Panel is opened by selecting:

Start>Settings>Control Panel>VertigoXmedia XmediaServer

Then, select the **REPLICATION** tab.

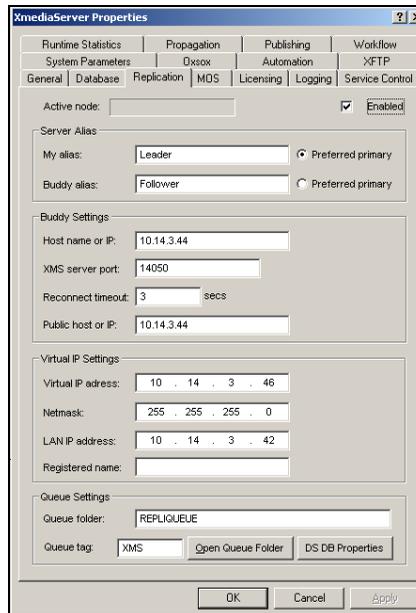


Figure 6-10. The Xmedia Server Control Panel's Replication page on the primary server

A quick-reference of each of the Replication page's fields and settings is available on [page 6-4](#). Meanwhile, the following topics provide instructions for specifying the necessary settings for server replication.

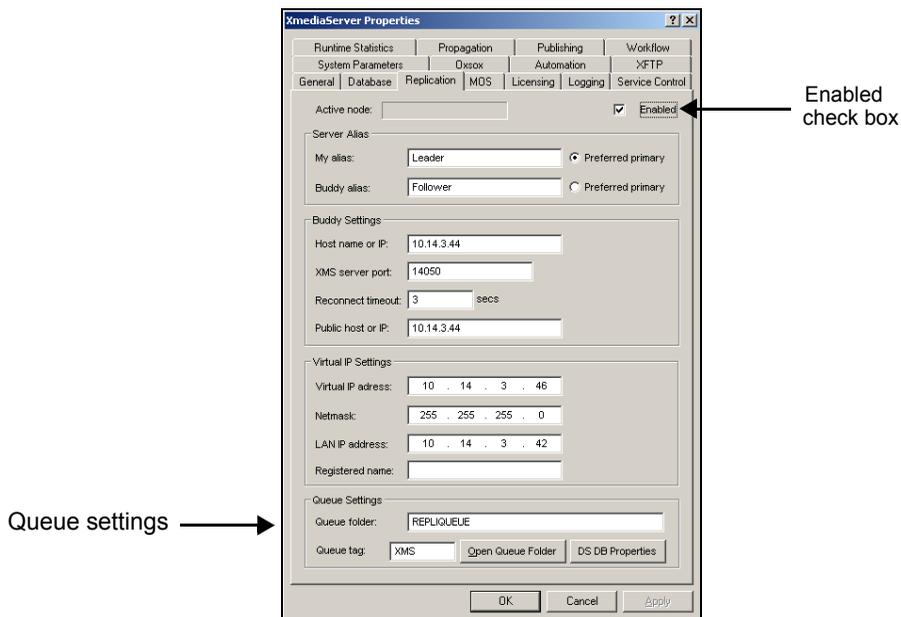
- [“Specify the Queue settings” on page 6-14](#)
- [“Specify the Dataserver Database Connection settings” on page 6-15](#)
- [“Specify the server's network settings in the Virtual IP Settings” on page 6-16](#)
- [“Specify the Buddy settings” on page 6-17](#)
- [“Specify the Server Alias settings” on page 6-18](#)

Specify the Queue settings

When a failover occurs on the primary server, the secondary server assumes control and queues the data changing events to disk in a queue folder, exactly like the primary server does when operating normally. Once the primary server is back online, the secondary server unloads the queue to the primary server, and when the queue is empty, the primary server resumes control and the secondary server resumes its role. The primary server is operable whenever it is running and the backlog queue from the secondary server is emptied.

In the **QUEUE SETTINGS** section of the Xmedia Server Control Panel's **REPLICATION** page, you must specify the full path (drive letter and the location) for the replication queue folder. Typically, the replication queue folder should be stored on the **F DRIVE**. If you do not specify a drive letter, the folder location defaults to the working folder specified on the Xmedia Server Control Panel's **GENERAL** page. Note that the folder is only created once the XMS service is restarted.

Also set the **QUEUE TAG**, which is an identifier added to each file name in the queue folder.



To set the Queue settings:

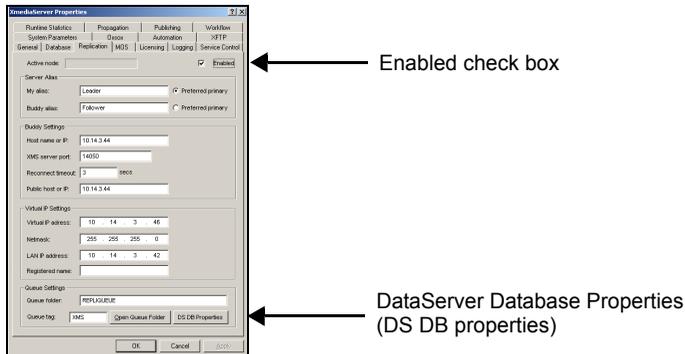
1. Open the Xmedia Server Control Panel and select the **REPLICATION** tab.
2. Select the **ENABLED** check box.
3. Type the full path for the folder's location (i.e. `f:\Repliqueue`) in the **QUEUE FOLDER** field.
4. Type an identifier in the **QUEUE TAG** field (i.e. `XMS`).
5. Click **APPLY**.

Specify the Dataserver Database Connection settings

Set the **DATASERVER DATABASE CONNECTION** settings. It is recommended to set the DataServer Database connection while the two servers are still fully independent of each other.

To set the DataServer Database connection settings:

1. Open the Xmedia Server Control Panel and select the **REPLICATION** tab.
2. Ensure that the **ENABLED** check box is selected.



3. Click the **DS DB PROPERTIES** button.
The **DATASERVER DATABASE CONNECTION SETTINGS** dialog box appears (figure [6-11](#)).



Figure 6-11. DataServer Database Connection Settings dialog box

4. Verify that the **Enable dataserver database connection SETTINGS** check box is selected.
5. Select **MS SQL SERVER** from the **DATABASE** type drop-down list.
6. Type **LOCALHOST** as the **SERVER NAME** field.
7. Type a user-defined database name (i.e. Datafeeds) in the **DATABASE NAME** field.
8. Enable the **WINDOWS AUTHENTICATION** option.
9. Type a user name and password in the appropriate fields.
Typically, we recommend using the same user name and password as specified on the Xmedia Server Control Panel's **DATABASE** tab.
10. Click **OK**.
11. Click **APPLY**.

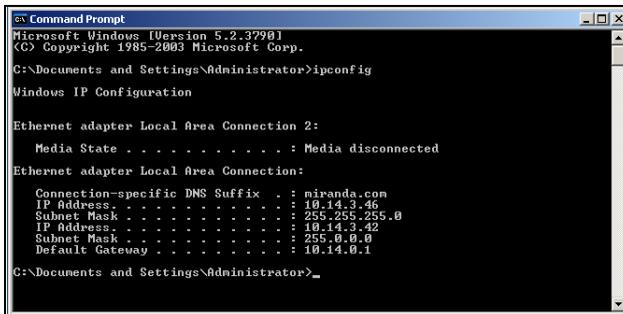
Specify the server's network settings in the Virtual IP Settings

The **VIRTUAL IP SETTINGS** section on the Xmedia Server Control Panel's Replication page identifies the server's IP address (LAN IP Address), as well as information required to support the Virtual IP address used in newsroom environments (Virtual IP Address, Netmask, and Registered name fields).

If you are configuring replication for a MOS enabled newsroom environment, then you must specify a value for all of the settings in this section (see the first procedure below). Otherwise, if your replication configuration does not require MOS, you only have to specify the server's IP Address in the **LAN IP ADDRESS** field (see the second procedure below).

To set the server's network settings for a MOS enabled newsroom environment:

1. Acquire an IP address that is not DHCP from your IT department. This IP address will be used as the Virtual IP address.
2. Open the command prompt and type: `ipconfig`



```

Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

    Media State . . . . . : Media disconnected

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : miranda.com
    IP Address . . . . . : 10.14.3.46
    Subnet Mask . . . . . : 255.255.255.0
    IP Address . . . . . : 10.14.3.42
    Subnet Mask . . . . . : 255.0.0.0
    Default Gateway . . . . . : 10.14.0.1

C:\Documents and Settings\Administrator>_

```

Figure 6-12. The server's IP Configuration values

3. Take note of the server's **IP ADDRESS** and **SUBNET MASK**.
4. Open the Xmedia Server Control Panel and select the **REPLICATION** tab.
5. Ensure that the **ENABLED** check box is selected.
6. Type the Virtual IP address in the **VIRTUAL IP ADDRESS** field.
7. Type the Subnet Mask value in the **NETMASK** field.
8. Type the server's static IP address in the **LAN IP ADDRESS** field.
9. If the Virtual IP address is registered in a Domain Name Server (DNS), then type the full qualified domain name in the **REGISTERED NAME** field (i.e. `replic1.miranda.com`).
10. Click **APPLY**.

To set the server's LAN IP address (non-MOS enabled configuration):

1. Open the command prompt and type: `ipconfig`
2. Take note of the server's **IP ADDRESS**.
3. Open the Xmedia Server Control Panel and select the **REPLICATION** tab.
4. Ensure that the **ENABLED** check box is selected.
5. Type the server's static IP address in the **LAN IP ADDRESS** field.
6. Click **APPLY**.

Specify the Buddy settings

When configuring the primary server for replication, the buddy server (also known as a peer or backup server) refers to the secondary Xmedia Server. When configuring the secondary server, the buddy server refers to the primary Xmedia Server.

Therefore, specifying the Buddy settings is relative to which server you are currently on.

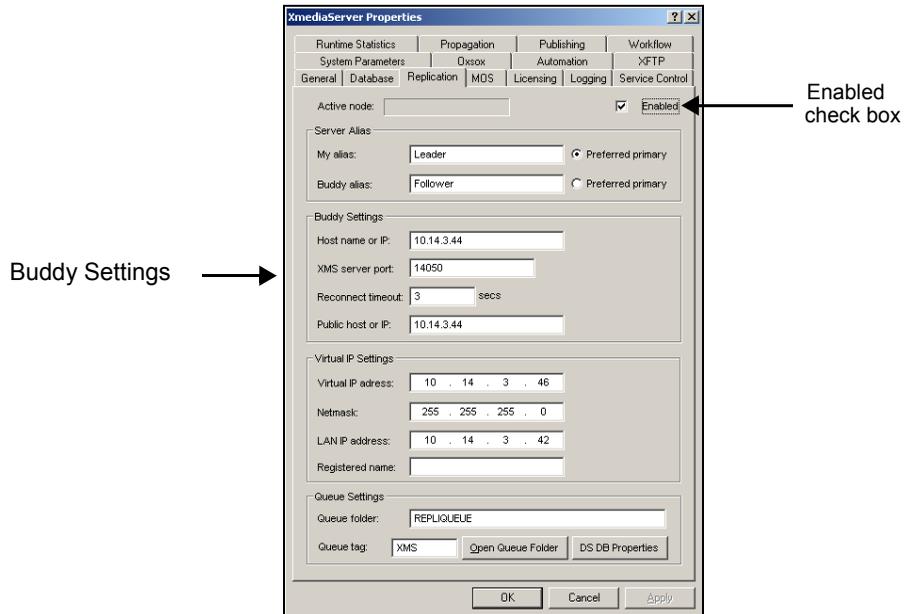


Figure 6-13. Identify the buddy server's IP address, communication port, and timeout settings

To specify the Buddy settings:

1. Take note of the buddy server's IP address by performing an IP Configuration on the buddy server.
 - a. On the buddy server, open the command prompt and type: `ipconfig`
 - b. Take note of the server's **IP ADDRESS**.
2. Go back to the server that you are configuring. Open the Xmedia Server Control Panel and select the **REPLICATION** tab.
3. Ensure that the **ENABLED** check box is selected.
4. In the **HOST NAME OR IP** field, type the buddy server's IP address (or hostname).
5. In the **XMS SERVER PORT** field, type the port number that the buddy server's communication port. Typically, this would be 14050.
6. Edit the **RECONNECT TIMEOUT** value from 0 to 3.
7. Leave the **PUBLIC HOST OR IP** field blank.
8. Click **APPLY**.

Specify the Server Alias settings

Like the Buddy Settings, the Server Alias settings are relative to which server is currently being configured. The **SERVER ALIAS** settings are used to designate whether the current server is the primary or the secondary server in the replication model.

Figure 6-14 demonstrates that if the current server is the primary server, you must provide it with an alias and then assign as the primary using the **PREFERRED PRIMARY** radio button. Next, you must identify the buddy server by also providing it a name. Then click **APPLY**.

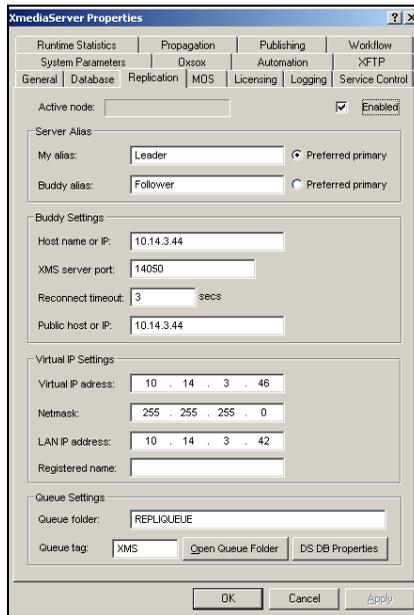
The same procedure must be performed on the secondary server's Xmedia Server Control Panel's **Replication** page, but the settings should be inverted (see figure 6-14).

Server Alias	My alias:	Buddy alias:	Preferred primary
Settings on the primary server	Primary	Secondary	<input checked="" type="radio"/>
Settings on the secondary server	Secondary	Primary	<input type="radio"/>

Figure 6-14. The Server Alias settings are relative to which server is being configured

Specifying the Replication settings on the secondary server

Once you have specify all of the replication settings on the primary servers Xmedia Server Control Panel's Replication page, you must also specify the complimentary replication settings on the secondary server's Xmedia Server Control Panel's Replication page.



Open the Xmedia Server Control Panel on the secondary server by selecting:

Start>Settings>Control Panel>VertigoXmedia XmediaServer

Then, select the **REPLICATION** tab.

The procedures for configuring the secondary server are identical to the ones described for the primary server. There are some settings and values that are relative to which server is being configured, however. This mainly applies to the **SERVER ALIAS** settings and the **BUDDY SETTINGS** sections and is thoroughly indicated in the instructions.

Therefore, complete each of the following procedures to configure the secondary server for replication:

- [“Specify the Queue settings” on page 6-14](#)
- [“Specify the Dataserver Database Connection settings” on page 6-15](#)
- [“Specify the server's network settings in the Virtual IP Settings” on page 6-16](#)
- [“Specify the Buddy settings” on page 6-17](#)
- [“Specify the Server Alias settings” on page 6-18](#)

Make a backup of the primary server's database

It is strongly recommended that you make a backup of the primary server's MS SQL Server database in case you experience any situations in the future that requires you to restore the server's database.

A convenient method for creating a backup of the server's database is to use **Backup Database** button on the primary server's XMS Control Panel's **Database** page ([page 5-4](#)). The backup file will be saved to the primary server's Virtual Database path.

Contact one of our Technical Support representatives for further information or assistance.

Setting the Control Data Server option

When replication is enabled, the **CONTROL THE DATASERVER** setting must be selected to ensure that the DataServer remains paired with the Xmedia Server at all times in a replication environment. An essential objective in the replication environment is to keep the server (which in reality has two components: the XMS and the Data Server) together.

To set the Control the DataServer setting on the primary replication server:

1. Open the Xmedia Server Control Panel's **SERVICE CONTROL** page.
2. Enable the **CONTROL THE DATASERVER** check box.
3. Select the **LAUNCH SERVICES MANAGEMENT CONSOLE** button.
The **SERVICES** window appears.
4. Navigate to the **VERTIGO DATA SERVER** service listed in the **SERVICES(LOCAL)** column.
5. Right-click on the **VERTIGO DATA SERVER** heading and select the **STOP** command ([figure 6-15](#)).

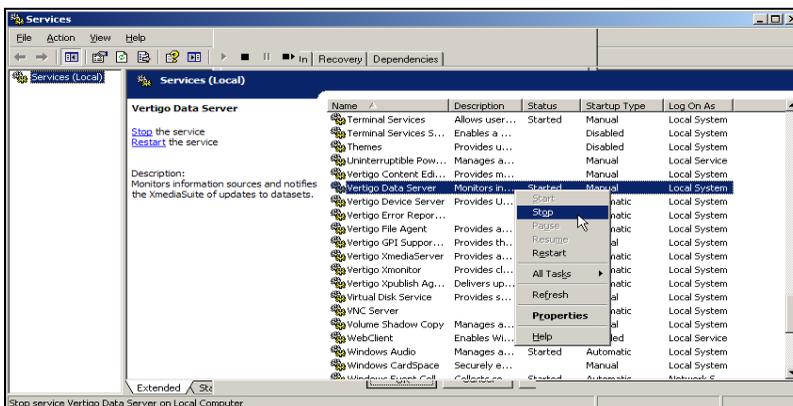


Figure 6-15. Stop the VXDataServer service

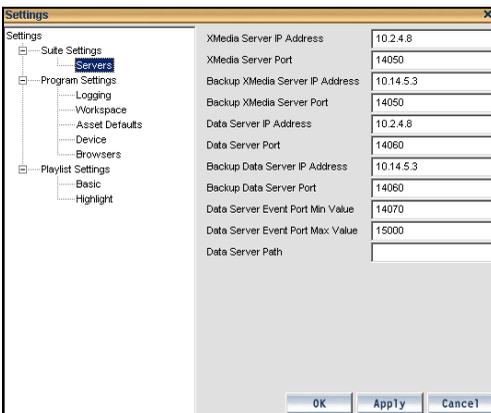
6. Return to the Xmedia Server Control Panel and click **APPLY**.

Specifying the server settings on client applications

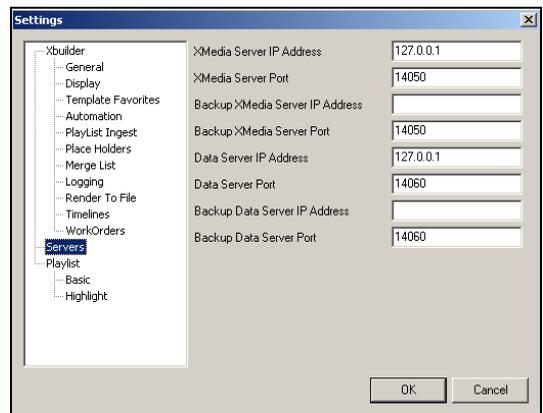
Vertigo Suite applications (Xstudio, Xbuilder, Xnews, and Xplay) that run on the client machines must be configured to connect and communicate with both the primary and the secondary Xmedia Servers. Therefore, you must open each of the client applications and specify the appropriate Server settings for the primary and the secondary Xmedia Servers (also referred to as the backup Xmedia Server).

To specify the server settings on a client application:

1. Open the **XMEDIA SERVER CONTROL PANEL** on the primary and secondary XMS servers and take note of the following information:
 - **GENERAL** page > **TCP/IP CONFIGURATION PORT** (typically, **14050**)
 - **REPLICATION** page > **VIRTUAL IP SETTINGS > LAN IP ADDRESS**
2. Open the **DATA SERVER PANEL** on the primary and secondary XMS servers (**START>SETTINGS>CONTROL PANEL>VERTIGOXMEDIA DATA SERVER**). Take note of the **TCP/IP>LISTENING PORT** value (typically, **14060**).
3. Launch an Vertigo Suite application by selecting **START>PROGRAMS>VERTIGO** and then one of the following applications:
 - **XSTUDIO**
 - **XBUILDER**
 - **XPLAY**
 - **XPLORER**
4. Select **TOOLS>SETTINGS** from the application's menu bar. The **SETTINGS** window appears.
5. Select the **SERVERS** heading from the tree structure to display the server settings (figure 6-16).



Xstudio Server Settings



Xbuilder Server Settings

Figure 6-16. Both the primary and secondary XMS servers must be specified in the Server settings

6. Specify the appropriate value in the following server setting fields:

XMEDIA SERVER IP ADDRESS	The IP address of the primary Xmedia Server, which should match the value in the LAN IP ADDRESS field on the primary server's Xmedia Server Control Panel.
XMEDIA SERVER PORT	The communications port of the primary Xmedia Server, which should match the value in the XMS SERVER PORT field on the primary server's Xmedia Server Control Panel. This is typically, 14050.
BACKUP XMEDIA SERVER IP ADDRESS	The IP address of the secondary Xmedia Server, which should match the value in the LAN IP ADDRESS field on the secondary server's Xmedia Server Control Panel.
BACKUP XMEDIA SERVER PORT	The communications port of the secondary Xmedia Server, which should match the value in the XMS SERVER PORT field on the secondary server's Xmedia Server Control Panel. This is typically, 14050.
DATA SERVER IP ADDRESS	The IP address of the primary Xmedia Server that is running the Data Server. Thus, this value should be identical to the value set for the XMEDIA SERVER IP ADDRESS listed above.
DATA SERVER PORT	The communications port of the primary Xmedia Server that is running the Data Server. Thus, this value should be identical to the value set for the XMEDIA SERVER PORT listed above.
BACKUP DATA SERVER IP ADDRESS	The IP address of the secondary Xmedia Server that is running the Data Server. Thus, this value should be identical to the value set for the BACKUP XMEDIA SERVER IP ADDRESS listed above.
BACKUP DATA SERVER PORT	The communications port of the secondary Xmedia Server that is running the Data Server. Thus, this value should be identical to the value set for the BACKUP XMEDIA SERVER PORT listed above.

7. Click either **OK** or **APPLY** on the **SETTINGS** window.
8. Repeat steps **3** to **6** for each of the remaining Vertigo Suite applications.

Verifying proper functioning of the servers and replication

When starting the Xmedia servers with replication enabled, it is recommended to first start the primary server followed by the secondary server. This ordering ensures that the primary server immediately becomes the live mode server. If the secondary server is started first, it will takeover live mode operation if the primary server does not start within the **RECONNECT TIMEOUT** value seconds. When the primary server finally does start up, it will force a failback operation.

Perform the following failover and failback tests to verify the proper functioning of the Xmedia Server replication:

	Type of test	Instructions
1	Failover	Disconnect the network cable to the primary server.
2	Failback	Reattach the network cable of the primary server.
3	Failover	Stop the primary Xmedia Server's XMS service control.
4	Failback	Start the primary Xmedia Server's XMS service control.
5	Failover	Terminate the primary Xmedia Server's service control using a kill utility like PsKill (or similar).
6	Failback	The service control manager should auto-start the primary XMS.
7	Failover	Repeat all failover tests while saving assets between tests and verify integrity.
8	Failover	Repeat all failover test while working a MOS enabled rundown and verify the playlist's integrity.

7 MOS SERVER CONFIGURATION AND MONITORING

The Xmedia Server Control Panel's **MOS Server settings** enable the Xmedia Server as a Media Object Server, which allows it to integrate into newsroom environments. As a MOS server, the Xmedia Server uses the MOS protocol to send metadata and pointer information about its MOS objects (i.e. graphics pages) to the Newsroom Control System (NCS). The NCS is responsible for managing all of the elements that contribute to the newscast's rundown. Also using the MOS Protocol, the NCS can request the transmission of the MOS objects from the MOS server for its rundowns. The Xmedia Server Control Panel's MOS Monitoring page allows you to monitor the inbound and outbound MOS messages between the Xmedia Server (MOS Server) and the Newsroom Computer System (NCS).

The following sections provide information and instructions for using the Xmedia Server Control Panel's MOS page to enable and use the Xmedia Server's MOS Server component for newsroom integration:

- [“Configuring the Xmedia Server's MOS settings” on page 7-2](#)
- [“Logging MOS Server activities” on page 7-8](#)
- [“Monitoring inbound/outbound MOS messages” on page 7-10](#)
- [“Mapping MOS channels” on page 7-11](#)
- [“Using MOS Redirection to transfer media between Xmedia Servers” on page 7-16](#)

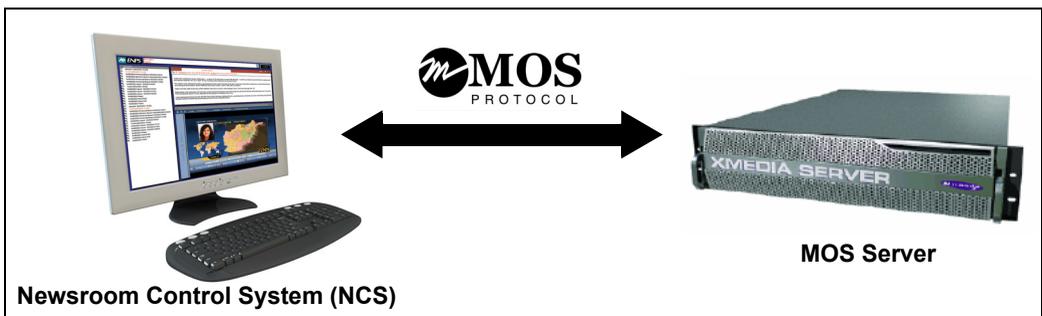


Figure 7-1. The Xmedia Server's MOS component allows it to integrate into newsroom environments

Configuring the Xmedia Server's MOS settings

Selecting the **MOS** tab on the Xmedia Server Control Panel displays the MOS component settings for the Xmedia Server. The MOS page has three (3) views, which are controlled using the **MOS OPTION** drop-down list at the top of the MOS page. Figure 7-2 shows that selecting the **CONFIGURATION** option from the **MOS OPTION** drop-down list displays the **GENERAL** and **NEWSROOM CONTROL SYSTEM (NCS)** settings, which are used to:

- Enable the Xmedia Server's MOS component and specify details about the Xmedia Server that allows it to become a MOS Server
- Identify the Newsroom Control System and configure its protocol options in preparation for communication with the MOS Server (i.e. Xmedia Server)

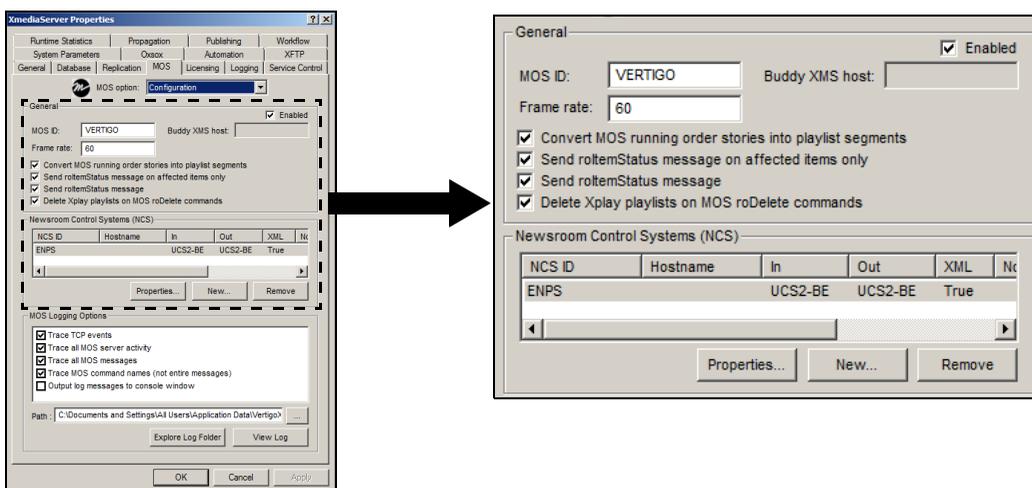


Figure 7-2. The Xmedia Server Control Panel's MOS configuration settings

The following sections provide instructions for enabling, configuring, and editing the settings that are responsible for establishing communication between the MOS server and the Newsroom Control System:

- [“Instructions for configuring the Xmedia Server as a MOS server” on page 7-3](#)
- [“Editing the Newsroom Control System's properties” on page 7-6](#)
- [“Deleting the Newsroom Control System” on page 7-7](#)

Instructions for configuring the Xmedia Server as a MOS server

To integrate the Xmedia Server (XMS) into a newsroom environment, the Xmedia Server must be configured as a MOS Server and then associated with a Newsroom Control System like ENPS or iNews. The following procedure provides you with detailed instructions for accomplishing these tasks.

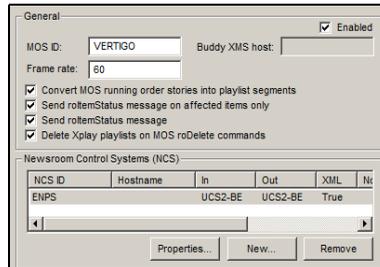


Figure 7-3. Xmedia Server Control Panel's MOS server configuration settings

To configure the Xmedia Server's MOS server component:

1. Open the Xmedia Server Control Panel and select **CONFIGURATION** from the **MOS OPTION** drop-down list.
2. Select the **ENABLED** check box to activate the MOS Server component.
3. Specify and/or verify the following options:
 - a. Type **VERTIGO** (all capital letters) in the **MOS ID** field.
All MOS messages to and from the Xmedia Server will be identified by this MOS ID.
 - b. If the Xmedia Server has been configured for a replication environment (see [page 6-1](#)), verify that the hostname or IP address of the buddy server is accurate in the **BUDDY XMS HOST** field.
 - c. Type **60** in the **FRAME RATE** field.
This field specifies the number of frames-per-second in the video format that is being used by the Xmedia Server. Valid values are 60 for NTSC, and 50 for PAL.
4. Enable or disable the check boxes for the following settings:
 - **CONVERT MOS RUNNING ORDER STORIES INTO PLAYLIST SEGMENTS**
When enabled, the MOS running order stories will be organized in the playlist within segments. When disabled, they are placed in the playlist as consecutive items in one list.
 - **SEND ROITEMSTATUS MESSAGE ON AFFECTED ITEMS ONLY**
When enabled, roItemStatus messages will be sent for each item affected by each running order operation processed by the MOS server. A running order operation is defined as an independent transaction enclosed in a MOS running order message.
 - **SEND ROITEMSTATUS MESSAGE**
When enabled (default), the roItemStatus message is sent to the MOS server with the status of the items in the rundown. When disabled, the roItemStatus message is suppressed and the status of items in the rundown are not reported.

- **DELETE XPLAY PLAYLISTS ON MOS roDELETE COMMANDS**
When enabled, the Xplay playlists that corresponds to the NCS's rundown will be automatically deleted when the rundown is deleted by the NCS client. When disabled, the Xplay playlists will not be deleted when the NCS's rundowns are deleted.
5. Identify the Newsroom Control System (NCS) that the Xmedia Server will communicate with by selecting the **NEW** button in the Newsroom Control System (NCS) section. The **NEWSROOM CONTROL SYSTEM (NCS)** dialog box appears.
 6. Specify the NCS settings for the ENPS or iNews server on the Newsroom Control System dialog box (figure 7-4).
 - a. Type the ID for the ENPS server or the iNews server in the **NCS ID** field. The ENPS's ID can be found at **ENPS>SYSTEM MAINTENANCE>SERVERS**.
 - b. Type ENPS or iNews server's host name or IP address in the **HOST** field. This value is often the same as the NCS ID.
 - c. In the **RUNDOWN CATEGORY** field, type the name of the Rundown subcategory where the rundowns will be stored by default.
 - d. Specify the **INBOUND ENCODING** and **OUTBOUND ENCODING** setting: Select **UCS2-BE** (2-byte Universal Character Set - Big-Endian format) from the drop-down lists for an ENPS server or iNews server configuration.
 - e. If using iNews, enable the **SUPPORTS XML VERSION TAG** option by selecting the check box. Enabling the MOS version tag, means the MOS server will ensure each MOS message sent to the NCS is headed with the <?xml ... /> tag. ENPS does not expect it, but iNews does.
 - f. Enable or disable the **NOTIFY NCS ON PAGE CREATION** option. Enabling **NOTIFY NCS ON PAGE CREATION** means that the MOS server will send `mosObj` messages to the NCS when graphics are created, modified or deleted in our system. As a result, you are able to see shared pages in the lists displayed on the NCS client user-interface.
 - g. Click **OK** to accept settings and close the **NEWSROOM CONTROL SYSTEM** dialog box.

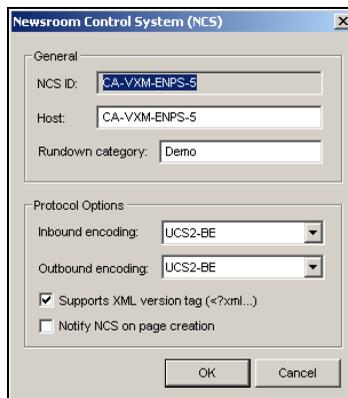


Figure 7-4. Newsroom Control System's properties

7. Click **APPLY**.

8. You must restart XMS Service before the new settings can properly take effect.
 - a. On the Xmedia Server Control Panel and select the **SERVICE CONTROL** tab (figure 7-5).
 - b. Click the **STOP SERVER** button and wait a couple of seconds.
 - c. Click the **START SERVER** button and verify that the **SERVICE STATE** reports: **"The service is running."**
 - d. Click **APPLY** and then return to the MOS configuration page by selecting the MOS tab at the top of the Xmedia Server Control Panel. Or, click **OK** to close the Xmedia Server Control Panel.

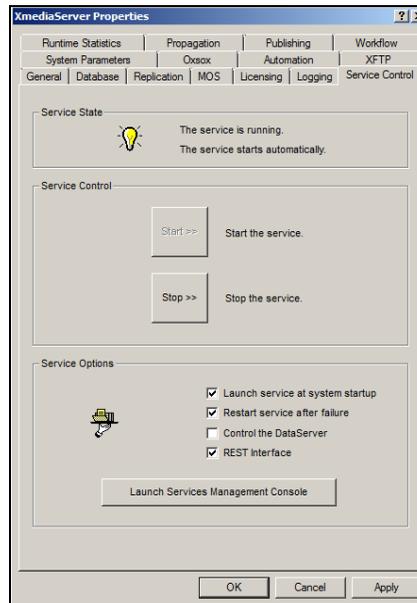


Figure 7-5. Stop and restart the XMS Service to apply the MOS server settings to the Xmedia Server

Editing the Newsroom Control System's properties

To edit the Newsroom Control System's properties:

1. Open the Xmedia Server Control Panel and select **CONFIGURATION** from the **MOS OPTION** drop-down list.
2. Verify that the **ENABLED** check box is selected.
3. In the **NEWSROOM CONTROL SYSTEM** table, select the Newsroom Control System that is to be edited.
4. Click the **PROPERTIES** button that is now enabled.

The **NEWSROOM CONTROL SYSTEM (NCS)** dialog box appears (figure 7-6) and displays the NCS's current settings.

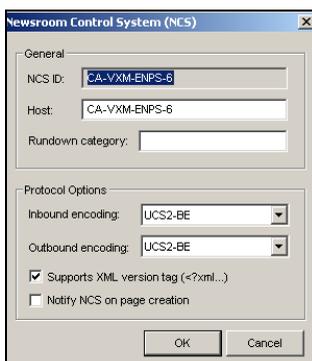


Figure 7-6. Newsroom Control System properties

5. Make the necessary edits to the setting values. See [page 7-4](#) for a description of each of the settings on the NCS properties dialog box.
6. Click **OK** to confirm the edits and close the dialog box.
The new settings immediately appear in the **NEWSROOM CONTROL SYSTEM** table.
7. Click **APPLY**.
8. You must restart XMS Service before the new settings can properly take effect.
 - a. On the Xmedia Server Control Panel and select the **SERVICE CONTROL** tab.
 - b. Click the **STOP SERVER** button and wait a couple of seconds.
 - c. Click the **START SERVER** button and verify that the **SERVICE STATE** reports: **"The service is running."**
 - d. Click **APPLY** and then return to the MOS configuration page by selecting the MOS tab at the top of the Xmedia Server Control Panel. Or, click **OK** to close the Xmedia Server Control Panel.

Deleting the Newsroom Control System

To delete the Newsroom Control System's properties:

1. Open the Xmedia Server Control Panel and select **CONFIGURATION** from the **MOS OPTION** drop-down list.
2. Verify that the **ENABLED** check box is selected.
3. Select the Newsroom Control System that is to be deleted from the **NEWSROOM CONTROL SYSTEM** table.
4. Click the **REMOVE** button that is now enabled.
The **REMOVE NCS** dialog box appears (figure 7-7).

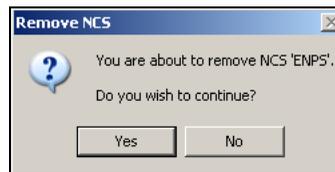


Figure 7-7. Select Yes to delete the Newsroom Control System from the MOS Server configuration

5. Select **YES** to confirm that you want to permanently delete the specified NCS.
The NCS is immediately removed from the **NEWSROOM CONTROL SYSTEM** table.

Logging MOS Server activities

Selecting the **CONFIGURATION** option from the **MOS OPTION** drop-down list displays the **MOS LOGGING OPTIONS** settings (figure 7-8). These settings allow you to set the MOS log file's criteria, as well as providing you access to locate and view the MOS log file.

The following sections provide instructions for setting the log file options and viewing the contents of the MOS log file:

- [“Specifying MOS logging options” on page 7-8](#)
- [“Viewing the MOS log file” on page 7-9](#)

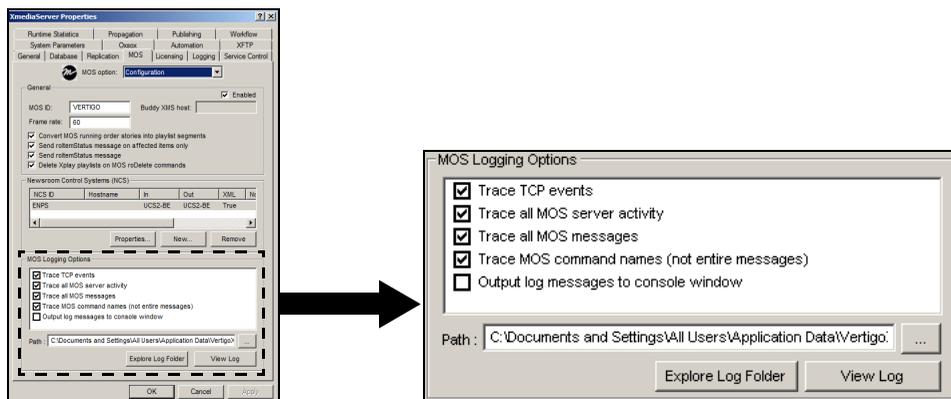


Figure 7-8. MOS Logging Options and log file access buttons

NOTE

Additional MOS logging can be enabled on the Xmedia Server's Logging tab, which records the MOS Redirection activities of the Xmedia Server. See [page 7-19](#) for more information.

Specifying MOS logging options

The Xmedia Server Control Panel's MOS Configuration page provides you with a set of **MOS LOGGING OPTIONS**, which determine the criteria for what type of information populates the MOS log file.

You can enable or disable the following MOS Logging options:

- **TRACE TCP EVENTS:** As the most verbose setting, it traces all activity related to network transmissions.
- **TRACE ALL MOS SERVER ACTIVITY:** Logs the MOS server engine messages.
- **TRACE ALL MOS MESSAGES:** Logs the content of the MOS messages.
- **TRACE MOS COMMAND NAMES:** Logs the MOS command names.
- **OUTPUT LOG MESSAGES TO CONSOLE WINDOW:** This is an advanced setting for debugging. It should be disabled at all times.

Viewing the MOS log file

During operation, the Xmedia Server's MOS activities are recorded in a log file. The logging criteria is determined by the settings specified in the **MOS LOGGING OPTIONS** (see [page 7-8](#)).

The contents of the log file are valuable for troubleshooting if for some reason the Xmedia Server's MOS server component is not behaving properly.

To view the MOS log file:

1. Open the Xmedia Server Control Panel's MOS page and select **CONFIGURATION** from the **MOS OPTION** drop-down list.
2. Verify that the **ENABLED** check box is selected.
3. Verify that the Path field displays the full directory path to the MOS log file, which is named `vxmos.log`.

If the log file path is not displayed, click the path field's **BROWSE** button and use the **BROWSE FOR COMPUTER** dialog box (figure 7-9) to navigate your way to the log file.

For example:

C:\Documents and Settings\All Users\Application Data\VertigoXmedia\Logs\vxmos.log



Figure 7-9. Browse for the MOS log file (`vxmos.log`)

4. There are two (2) ways of opening the MOS log file:
 - Click the **VIEW LOG** button, and the `vxmos.log` file opens immediately in a Notepad window.
- Or,
- Click the **EXPLORE LOG FOLDER** button. Windows Explorer opens to the **LOGS** folder that was specified in the **PATH** field (figure 7-10). Find and double-click the `vxmos.log` file. The `vxmos.log` file opens immediately in a Notepad window.

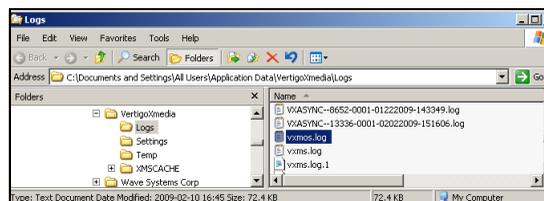


Figure 7-10. You can open the `vxmos.log` file from within the Windows Explorer window

Monitoring inbound/outbound MOS messages

Selecting **MONITOR** from the **MOS OPTION** drop-down list displays the MOS Monitor page (figure 7-11), which allows you to view the real-time inbound and outbound MOS messages that are being communicated between the Xmedia Server (MOS Server) and the Newsroom Control System (NCS).

The **INBOUND MOS MESSAGES** column displays messages that originate from the NCS. The messages communicate back to the MOS server any changes that were made to the NCS's running order (i.e. rundown). The MOS server can also initiate communication with the NCS and its messages are displayed in the **OUTBOUND MOS MESSAGES** section of the MOS Monitor page. Note that although these communications are in real-time, the originating system must wait for a response after sending each message.

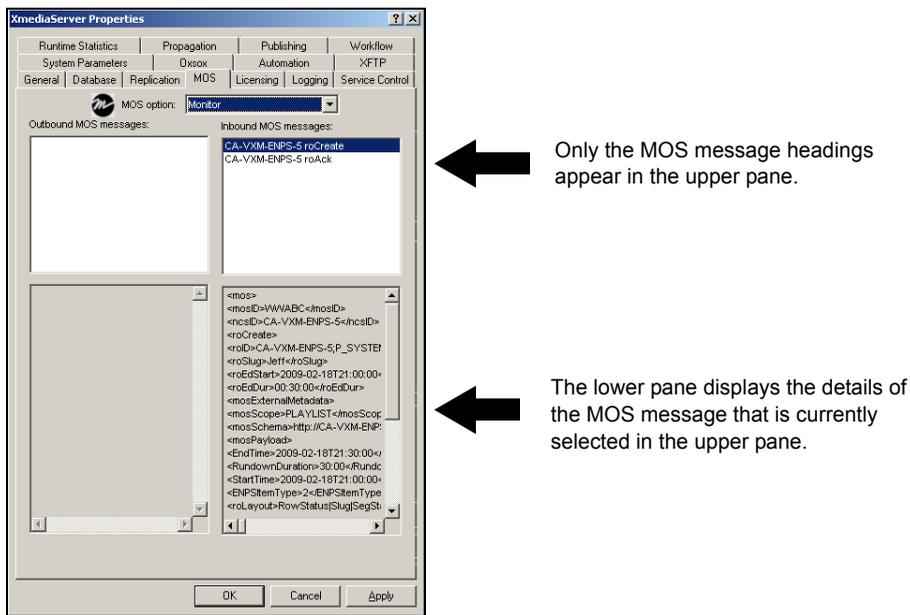


Figure 7-11. Monitor the inbound/outbound MOS messages between the MOS server and NCS

NOTE

We recommend that you familiarize yourself with the MOS Protocol's MOS messages by referring to the MOS message definitions at <http://www.mosprotocol.com/>.

Mapping MOS channels

The **MOS CHANNEL MAPPINGS** option on the Xmedia Server Control Panel's MOS page allows you to create associations between the Newsroom Control System's MOS channel name and the asset's publish location. These associations are used by the MOS Server to communicate to the NCS whether or not the story (template and all its linked assets) has been published to the appropriate location. If the story has not been published, the Xmedia Server triggers the necessary publish requests until the story in the rundown is published (i.e. published to all locations inferred by the MOS channel name).

A MOS channel map is created on the Xmedia Server Control Panel by adding a **MOS CHANNEL ASSOCIATION** for each of the MOS channel names listed in the NCS's rundown. The **MOS CHANNEL ASSOCIATION** links the MOS channel name with an **ASSET TYPE**, which determines where the assets will be published to. The following **ASSET TYPES** can be selected:

- **CHANNEL:** A channel is an object (asset) that is made up of a number of devices each associated to a publoc2 asset.
- **DEVICE2:** A Device2 is a logical representation of a Vertigo XG or another driver (i.e. Lyric, Deko, etc.) to which Xplay will send Cue/Take, Set text, and Set image commands.
- **PUBLOC2:** A Publoc2 is a logical representation of a location (i.e. hostname, drive, directory) to which clips, audio, scenes and other files are to be published.

You can also set a default channel mapping so that if no MOS channel name specified in the NCS application (e.g. an empty cell in the MOS Channel Name column), the assets will be published to the location specified in the **DEFAULT CHANNEL MAPPING** fields on the Xmedia Server Control Panel (figure 7-12).

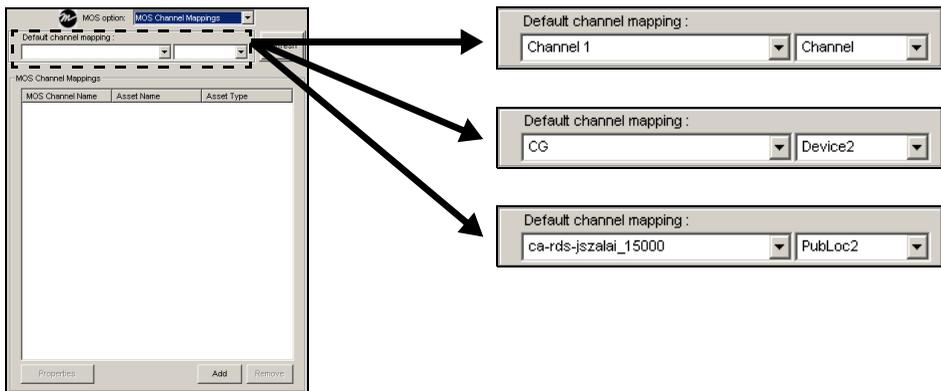


Figure 7-12. Default MOS channel mapping values

The following sections provides instructions for adding, editing, and deleting MOS Channel Associations:

- [“Adding a MOS Channel Association” on page 7-12](#)
- [“Editing a MOS Channel Association” on page 7-14](#)
- [“Deleting a MOS Channel Association” on page 7-15](#)

Adding a MOS Channel Association

A MOS channel map is created on the Xmedia Server Control Panel by adding a **MOS CHANNEL ASSOCIATION** for each of the MOS channel names listed in the NCS's rundown.

To map a MOS channel name to a publish location:

1. Open the Newsroom Control System (NCS) client application (i.e. ENPS or iNews) and open the rundown so that the MOS channel column is displayed. Take note of the MOS channel names.
2. Open the **XMEDIA SERVER CONTROL PANEL** and select **MOS CHANNEL MAPPINGS** from the **MOS OPTION** drop-down list (figure 7-13).

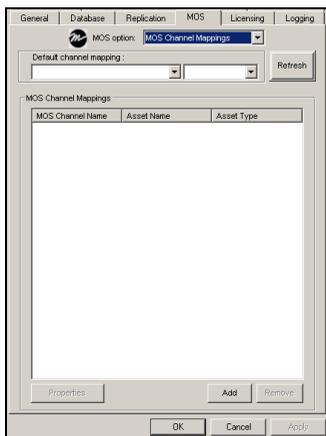


Figure 7-13. Select **MOS CHANNEL MAPPINGS** from the **MOS OPTION** drop-down list

3. Click **ADD**.
The **ADD A MOS CHANNEL ASSOCIATION** dialog box appears (figure 7-14).



Figure 7-14. The MOS Channel Association dialog box

4. Type the MOS channel name from the NCS in the **MOS CHANNEL** field.
5. Select either **CHANNEL**, **DEVICE2**, or **PUBLOC2** from the **ASSET TYPE** drop-down list.
6. Select the asset's name from the **ASSET NAME** drop-down list.

7. Click **ADD**.
The **ADD A MOS CHANNEL ASSOCIATION** dialog box closes and the MOS channel name's channel map is immediately displayed in the **MOS CHANNEL MAPPINGS** list.
8. Optional: Click **REFRESH** to refresh the MOS channel mappings list to verify if any other additions, deletions, or modifications of channels, devices and publoc2 assets have taken place.

Editing a MOS Channel Association

To edit an existing MOS Channel Association:

1. Open the **XMEDIA SERVER CONTROL PANEL** and select **MOS CHANNEL MAPPINGS** from the **MOS OPTION** drop-down list.
2. Select the MOS Channel Name of the MOS Channel association that is to be edited (figure 7-15).

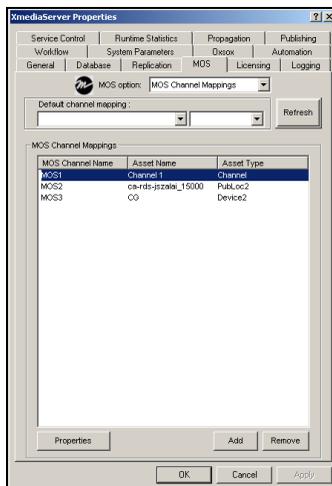


Figure 7-15. Select MOS channel association's MOS Channel Name

3. Click the **PROPERTIES** button, or double-click the MOS Channel association's name. The **EDIT MOS CHANNEL ASSOCIATION** dialog box appears (figure 7-16).



Figure 7-16. The MOS Channel Map's properties

4. Make the necessary edits to the **MOS CHANNEL**, **ASSET NAME**, and/or **ASSET TYPE** fields.
5. Click **SAVE** and the **EDIT MOS CHANNEL ASSOCIATION** dialog box closes. The edits made to the MOS channel association are immediately displayed in the MOS Channel Mappings list on the Xmedia Server Control Panel.

Deleting a MOS Channel Association

To delete an existing MOS Channel Association:

1. Open the **XMEDIA SERVER CONTROL PANEL** and select **MOS CHANNEL MAPPINGS** from the **MOS OPTION** drop-down list.
2. Select the MOS Channel Name of the MOS channel association that is to be deleted (figure [7-17](#)).

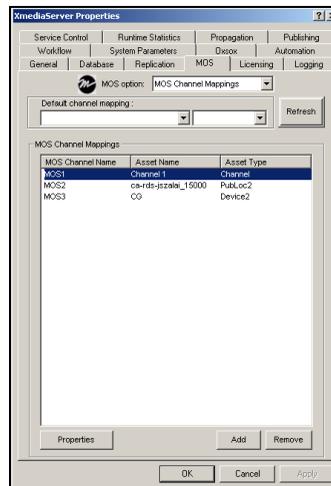


Figure 7-17. Select the MOS Channel Name of the MOS channel association

3. Click **REMOVE**.
The **CONFIRM DELETE** dialog box appears (figure [7-18](#)).

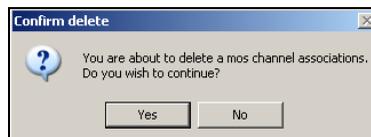


Figure 7-18. Select Yes to delete the select MOS channel association

4. Click **YES** to confirm your intention to delete the selected MOS channel association.
The MOS channel association is immediately removed from the MOS Channel Mappings list on the Xmedia Server Control Panel.

Using MOS Redirection to transfer media between Xmedia Servers

Using a MOS Protocol based technique called **MOS Redirection**, Xmedia Servers work with the ENPS Newsroom Computer System (NCS) to transfer stories and their associated media between Xmedia Servers within a single newsroom, or between multiple newsrooms and Xmedia Servers in different locations.

The following sections provide more information about how the Xmedia Server works with ENPS to transfer media between servers:

- [“Prerequisites for using MOS Redirection” on page 7-16](#)
- [“Overview of the MOS Redirection workflow” on page 7-16](#)
- [“Limitations when using MOS Redirection with Xmedia Servers” on page 7-17](#)
- [“Logging MOS Redirection events” on page 7-19](#)

Prerequisites for using MOS Redirection

It is a prerequisite that your ENPS Newsroom Computer System (NCS) be properly configured for MOS Redirection. We strongly recommend that you consult the **AP ENPS Integration Guide** for more information about MOS Redirection and instructions for setting up MOS Redirection within ENPS.

To use MOS Redirection with the Xmedia Servers, stories and their items must be created with Vertigo Suite’s Xnews v.4.9 or greater. The MOS items that are created in Xnews v.4.9 will contain the `objPath` MOS protocol field that allows the local Xmedia Server to resolve the IP of the remote Xmedia Server from which the underlying media of stories/items are obtained.

NOTE

At least one item in the story must have the `objPath` field for MOS Redirection to function properly. If a MOS item was created in a version previous to v.4.9, reopening an item in Xnews and saving the item inserts the required `objPath`.

Overview of the MOS Redirection workflow

When a story is dragged and dropped from foreign rundown to a local rundown inside ENPS, the Xmedia Server’s MOS Server recognizes this event by the fact that the MOS ID of the items do not match the Xmedia Server’s MOS ID. As a result, the redirection process is triggered.

During the MOS redirection of an item, the Xmedia Server only tries to fetch assets that do not already exist locally. Note that there is no checking to see if the asset on the remote server is newer than the local asset. If the asset is already on the local server, the Xmedia

Server does not attempt to fetch it from the remote Xmedia Server. When an item has been MOS redirected inside of ENPS, Xplay displays the **MOS REDIRECTION IN PROGRESS** message in the playlist's **Status** column and the Xmedia Server begins to receive items from the remote server.

Name	Status	Offset	Duration
PHDONE			
PH_F	Ready	00:10.00	00:00.00
PH_F	Ready	00:20.00	00:00.00
PH_T	Ready	00:30.00	00:00.00
PH_T	Mos Redirection In Progress	00:40.00	00:00.00

When all of the items have been received, the Xmedia Server requests that ENPS replace the `mos id`, `nsc id` and `objPath` of the item with the local Xmedia Server values. Once the NCS confirms that it has replaced these values, the MOS redirection is considered complete and the element will be validated like any other playlist element and the resulting status indicated.

Limitations when using MOS Redirection with Xmedia Servers

The following topics identify and discuss current limitations that users should be aware of before attempting to use MOS Redirection with Xmedia Servers:

- [“Placeholders are not permitted” on page 7-17](#)
- [“Category and/or asset conflicts are not resolved” on page 7-17](#)
- [“System templates are required for clip playout” on page 7-18](#)
- [“No attempts to repair damaged media” on page 7-18](#)

Placeholders are not permitted

Items with placeholders cannot be MOS redirected by the Xmedia Server. An attempt to MOS redirect an item with placeholders inside ENPS causes the item's Status in the playlist (Xplay) to display **“CAN'T MOS REDIRECT DUE TO PLACEHOLDERS”** and the media is not copied from the remote server. However, once the job is completed and the item contains no placeholders, the item may be MOS redirected.

Category and/or asset conflicts are not resolved

In the Xmedia Server, a category conflict is when two categories have the same name but different internal ids. For example, if the category “Headshots” was manually created on Xmedia Server 1 and also manually created on Xmedia Server 2, the categories will have the same name but different internal ids.

If an asset in category Headshots is redirected, a new category called **Headshots_Propag** is created on the local Xmedia Server and the redirected asset is put into this category. Redirection will succeed, but the item in question may not play out properly on air due to this category conflict.

The same type of conflict may occur if assets with the identical names but different internal ids exist in the same category on the remote and local Xmedia Server.

MOS Redirection users should be aware of this limitation and try to ensure category and asset names will not conflict with the remote server. See [“Resolving Propagation Exceptions” on page 17-10](#) for more information.

NOTE

In a hub & spoke model, assets and categories are propagated from the hub to the spoke. Therefore, the assets and categories on the hub and the spoke have the name same, but since the assets and categories were propagated (not created manually), they will have the same category id and asset id respectively and no conflict occurs.

System templates are required for clip playout

Although Xnews can be used to insert clips directly into a NCS item, proper playout of the clip on the XG device requires the use and proper configuration of **System Templates**. See [“Creating a clip template in Xstudio for clip playout” on page 4-6](#) in the Xnews User Manual for more information.

NOTE

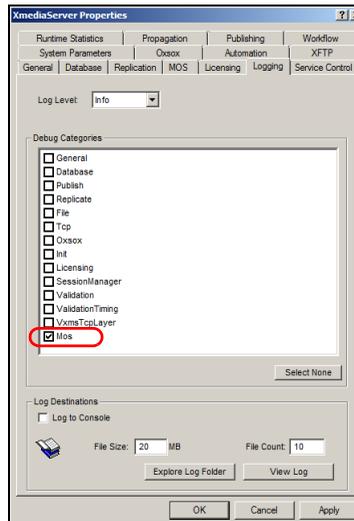
MOS Redirection will not copy, nor configure the system templates from the remote server. The system templates must be imported and pre-configured by the local Xmedia Server.

No attempts to repair damaged media

If an item is damaged and unplayable on the remote server due to media expiration, media re-categorization, or for any other reason; no attempts will be made to correct or fix problems when the item is redirected to the local server. If the item was unplayable on the remote server, it will remain unplayable when MOS redirected to the local server.

Logging MOS Redirection events

The Xmedia Server Control Panel's Logging page features the **MOS** Debug Category which records the MOS Redirection activities inside the Xmedia Server and saves them to the Xmedia Server's log text file (XmediaServer*.log).



This setting provides additional logging to the MOS logging activities already recorded in the vxmos.log file, which is enabled using the **MOS LOGGING OPTIONS** on the **MOS** tab.

8 LICENSE MANAGEMENT

The Xmedia Server stores and manages the licenses that are required to operate the Vertigo Suite applications and devices. As such, the Xmedia Server Control Panel's **Licensing** page provides you with an interface where you can:

- View the list of the existing application and device licenses stored on the Xmedia Server.
- View the details of a particular license, such as which computer or IP address is using the license, the license type, the allocation count...etc.
- Add new licenses to the Xmedia Server.
- Deallocate a fixed license from one client computer, so that it is free to be used by another computer.

The following sections describe how to use the Xmedia Server Control Panel's **Licensing** page to view and manage the licenses stored on the Xmedia Server:

- ["An overview of Vertigo Suite licenses" on page 8-2](#)
- ["Orientation to Xmedia Server Control Panel's Licensing page" on page 8-8](#)
- ["Viewing the existing device and application licenses" on page 8-14](#)
- ["Viewing the details of a particular license" on page 8-15](#)
- ["Resolving license errors and adding licenses to the Xmedia Server" on page 8-16](#)
- ["Deallocating a fixed license" on page 8-22](#)

An overview of Vertigo Suite licenses

All Vertigo Suite applications and devices require a valid license to operate. These licenses are added to and stored on the central Xmedia Server (or in some cases on the Intuition XG's EXMS). Factory configured XGs and Grass Valley commissioned Xmedia Servers will already have licenses installed according to the sales agreement.

The following sections provide further information about the Vertigo Suite licenses:

- [“Vertigo Suite application and device licenses” on page 8-3](#)
- [“Types of Vertigo Suite licenses” on page 8-4](#)
- [“The vxls.bin license file” on page 8-5](#)
- [“Xmedia Server Control Panel Licensing page versus License Manager” on page 8-6](#)
- [“Licensing in a server replication environment” on page 8-7](#)

Vertigo Suite application and device licenses

All Vertigo Suite applications and devices are required to have a valid license. Without a license the application or device will not be able to launch, or it will not operate to full functionality. All licenses must be purchased and they are distributed in the form of soft keys.

The following licenses are currently available for the Vertigo Suite applications:

- **QC 4.9**
- **XBUILDER 4.9**
- **XNEWS 4.9**
- **XPANEL2 4.9**
- **XPLAYPRO 4.9**
- **XPLORER 4.9**
- **XSTUDIO 4.9**
- **XSTUDIOD 1.0**

Vertigo Suite render and playout devices also require specific licenses to operate at full functionality, or to enable specific features. The following table identifies and describes the licenses that are available or related to the **XMEDIA SERVER**, **VERTIGO XG** and **VX PREVIEW** (Software CG) devices.

XGENCODE 4.9	The XG Encode license is required to use Xbuilder's Render to File feature, which renders and saves the playout of a template, page, and/or scene to a file in various clip formats. See the Xbuilder User Manual for more information.
XGENCODE FOR PLAYOUT 4.9	The XG Encode for Playout license is required to render pages and/or scenes to playout server compatible formats (XDCAM and IMX compatible MXF files). See the Xbuilder User Manual for more information.
XGSOFTWARE 4.9	The VX Preview (Software CG) requires a software application license to function properly. If the SoftwareCG does not have a valid application license, then the LiveWindow will show the message "Unlicensed Application" and the SoftwareCG will be internally disabled. It will only accept Dashboard connections at this point. See the Vertigo XG Configuration Guide for more information.

Types of Vertigo Suite licenses

A license's transference and lifespan are determined by its license type. The Xmedia Server supports four (4) different license types, which are reported in the **Type** column of the **License Summary** table on the Licensing page:

- **FIXED/PERM**
- **FIXED/TEMP**
- **FLOAT/PERM**
- **FLOAT/TEMP**

The following sections describe the difference between the license types and under which circumstances it would be more appropriate to choose one type rather than the other.

- [Fixed versus Floating license types](#)
- [Permanent versus Temporary license types](#)

Fixed versus Floating license types

Fixed licenses restrict the use of an application to one specific computer or device. Fixed licenses are recommended for a single-user or a devoted machine environment. The Xmedia Server allows you to deallocate (free up the license so that it can be used by another machine) up to four (4) times. The **DEALLOC COUNT** column on the **LICENSE DETAIL** tab keeps track of the amount of times the license has been deallocated. Deallocation of a fixed license is performed manually as described on [page 8-22](#). If you need to deallocate a fixed license more than four times, you must contact our Technical Support department to renew the license.

Floating licenses allow an application to be run on any computer/device that is connected to the Xmedia Server and which has the application's software installed on it. Therefore, floating licenses are recommended for sites that have multiple users, but do not need or want to purchase a license for each user. Floating license imply that multiple users share a fixed number of licenses since the number of computers permitted to run the application at the same time is limited to the number of floating licenses granted for the application. When a computer needs an application program, it sends a request to the Xmedia Server for a floating license. If a license is available, the Xmedia Server assigns the license to that computer. If no floating license is available, the request is rejected. Once the application is closed on a computer, the license is automatically deallocated back to the Xmedia Server, which is ready to reassign it to the next client.

Permanent versus Temporary license types

A permanent license type has no expiry date and it is valid for the lifetime of the software version indicated in the license's name. Temporary license types however, are associated with an expiry date upon which the validity of the license terminates and the application is no longer operational. A temporary license's expiry date is indicated in the **EXPIRATION** column on the **LICENSE DETAIL** tab. Contact our Technical Support department to extend or renew a temporary license.

The vxls.bin license file

The file that contains the required licensing information is named `vxls.bin` and it is stored on the Xmedia Server in the following directory location:

`C:\Program Files\VertigoXmedia\Apps`

You will also notice that the **Apps** folder (figure 8-1) also contains a series of ten similarly named files that use the following format:

- `4_9_vxls_1.bin`
- `4_9_vxls_2.bin`
- `4_9_vxls_3.bin`

These files are backups of the license file that get updated and archived every time the XMS service is restarted. In the case where the primary license file (`vxls.bin`) gets corrupted, then you can always revert to a functioning version of the license file.

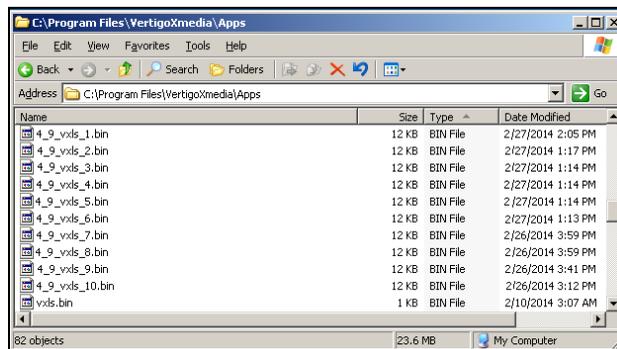


Figure 8-1. The license file (`vxls.bin`) and its backups are stored in the Apps folder on the XMS

The following instructions explain how to revert to a valid license file using a backup. The same procedure can be followed to install a license file sent by our Technical Support team.

1. Open the Xmedia Server Control Panel and select the **SERVICE CONTROL** tab.
 2. Select the **STOP** button to stop the XMS Service.
 3. Navigate to the Apps folder: `C:\Program Files\VertigoXmedia\Apps`
 4. Rename the old bin file (i.e. change `vxls.bin` to `vxls_old.bin`), or remove the file from the Apps folder.
 5. Rename the backup license file (i.e. `vxls_1.bin`) that you deem to be valid to `vxls.bin`.
- or,
- Add the new `vxls.bin` that was provided by the Technical Support team to the Apps folder.
6. Return to the Xmedia Server Control Panel's **SERVICE CONTROL** page and press the **Start** button to restart the XMS Service.

Xmedia Server Control Panel Licensing page versus License Manager

Although the Xmedia Server Control Panel's Licensing page is the main interface for viewing and managing the Vertigo Suite licenses, it is only accessible from the Xmedia Server. Vertigo Suite applications, like Xstudio, are installed on client computers and the Xmedia Server is likely only accessible to the IT technicians. As such, the Vertigo Suite applications (i.e. Xplorer, Xstudio, Xbuilder, and Xplay) are equipped with a **LICENSE MANAGER** (figure 8-2) that allows you to view and manage licensing from the application. The License Manager provides you with almost the exact same functionality as the Xmedia Server Control Panel Licensing's **SOFT KEYS** view, and all edits are immediately shared between the two once you select the **APPLY** button (see [page 8-12](#) and [page 8-21](#) for more information).

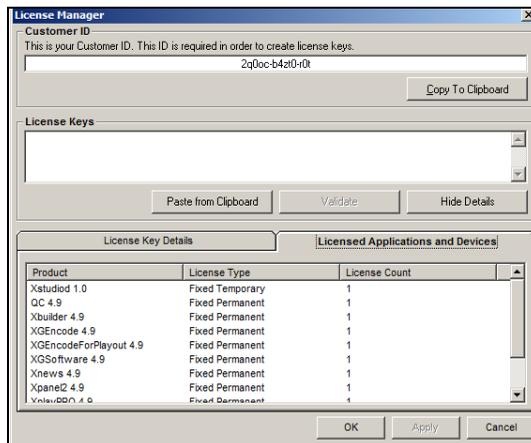


Figure 8-2. The License Manager allows you to view and manage licenses from within an application

There are two (2) ways to launch the License Manager:

- When a Vertigo Suite application is launched without a proper license, a license error appears and you can press the **ENTER LICENSE** button to launch the License Manager to remedy the problem.

Or,

- With the application open, you can select the **HELP>LICENSE** command from the application's menu bar.

NOTE

Further information and instructions for using the License Manager are provided in the user manual's for each of the Vertigo Suite applications and in the Release Notes for Vertigo Suite v.4.9.

Licensing in a server replication environment

In an Xmedia Server replication setup, the Vertigo Suite application and device licenses are also replicated from the primary server to the secondary server to ensure that both servers contain identical licensing information for a seamless transition in case of failover.

Since a critical part of the licensing mechanism is that machine ID matches exactly with the license, each Xmedia Server must have a dongle with matching Machine IDs. If the dongles do not have the same Machine IDs, then a licensing error will occur and client applications will not be able to connect to the secondary server when a failover occurs. See [“Replication of the XMS Server’s database” on page 6-1](#) for more information about these server replication services.

Orientation to Xmedia Server Control Panel's Licensing page

The Xmedia Server Control Panel's **Licensing** page provides you with an interface and settings for viewing and managing the licenses that are required to operate the Vertigo Suite applications and devices.

Selecting the **LICENSING** tab on the Xmedia Server Control Panel displays the Licensing page, which has two views: **LICENSES** and **SOFTKEYS**. You can switch between the two views by selecting from the **LICENSE SERVER OPTION** drop-down list at the top of the Licensing page (figure 8-3).

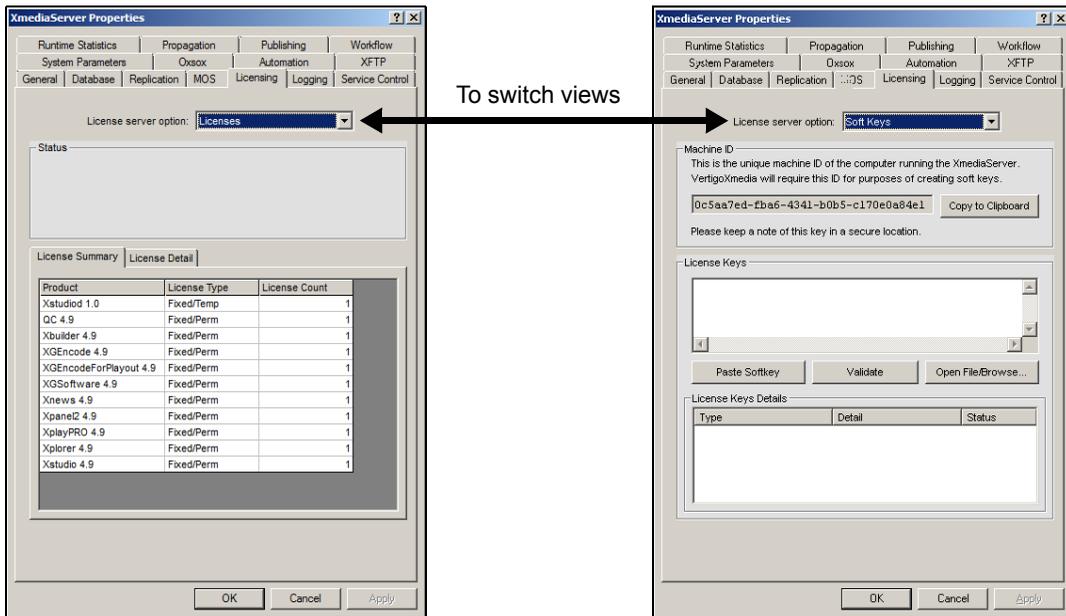


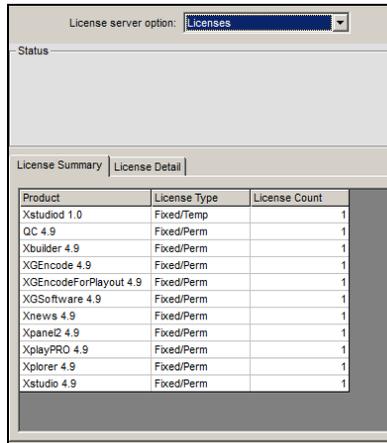
Figure 8-3. Switching between the Licensing page's Licenses and Softkeys views

The following sections provide a quick reference of the field and settings on each of the views on the Xmedia Server Control Panel's Licensing page, including a brief description of what the view allows you to accomplish.

- [“Licences view - License Summary tab” on page 8-9](#)
- [“Licenses view - License Detail tab” on page 8-10](#)
- [“Soft Keys view” on page 8-12](#)

Licences view - License Summary tab

Figure 8-4 demonstrates the License Summary table which lists all of the licenses that are currently installed on the Xmedia Server. Each row in the table represents a license category and provides the license's name, type, and the number of licenses installed (**PRODUCT**, **LICENSE TYPE**, and **LICENSE COUNT**). See [“Viewing the existing device and application licenses” on page 8-14](#) for more information.



Product	License Type	License Count
Xstudiod 1.0	Fixed/Temp	1
QC 4.9	Fixed/Perm	1
Xbuilder 4.9	Fixed/Perm	1
XGEncode 4.9	Fixed/Perm	1
XGEncodeForPlayout 4.9	Fixed/Perm	1
XGSoftware 4.9	Fixed/Perm	1
Xnews 4.9	Fixed/Perm	1
Xpane2 4.9	Fixed/Perm	1
XplayPRO 4.9	Fixed/Perm	1
Xplorer 4.9	Fixed/Perm	1
Xstudio 4.9	Fixed/Perm	1

Figure 8-4. The Licenses view with the License Summary tab selected

Licenses view - License Detail tab

Figure 8-4 and the following descriptions provide an overview of the **LICENSE DETAIL** table that is displayed when the License Detail tab is selected, or when a row in the License Summary table is double-clicked. The License Detail table is a one-row listing of properties related to the particular license that was last selected in the License Summary table. You can also deallocate and reallocate a license using this page. See [“Viewing the details of a particular license” on page 8-15](#) and [“Deallocating a fixed license” on page 8-22](#) for more information.

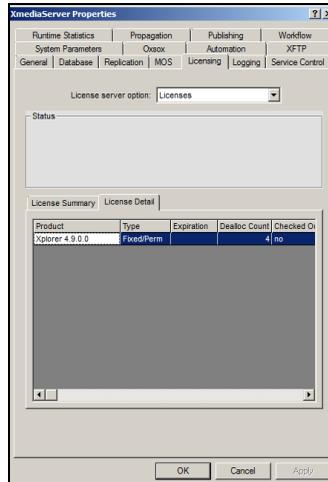


Figure 8-5. The License Detail table allows you to view properties related to the particular license

- **Product:** The name of the application or device license.
- **Type:** Categorizes the license by its transference (**FIXED** or **FLOAT**) and the lifespan of its validity (**PERMANENT** or **TEMPORARY**). See [“Types of Vertigo Suite licenses” on page 8-4](#) for more information.
- **Expiration:** If the license type is listed as **TEMPORARY**, then this field displays the date upon which the license will no longer be valid. If the license type is Permanent, then this field is blank. See [“Types of Vertigo Suite licenses” on page 8-4](#) for more information.
- **Dealloc Count:** The number of times that you can still deallocate a fixed license to another machine before losing this privilege. See [“Deallocating a fixed license” on page 8-22](#) for more information.
- **Checked Out:** Indicates whether or not a license is currently in use and allocated to a user. Conversely when a license is checked in, it means the user is no longer running the application associated with the license. If the license is a floating license and checked in, it is freely available for another user. Where a fixed license is always reserved for a particular computer and cannot be used by another computer even when it is checked in.

- **Computer:** The name of the machine that is currently using the floating license.
- **IP Address:** The IP address of the machine that is currently using the floating license.
- **Machine ID:** The Machine ID of the computer that is currently using the floating license.
- **Time stamp:** The time stamp is the time the license was last altered, either by a check-in or a check-out.

Soft Keys view

When **SOFT KEYS** is selected from the **LICENSE SERVER OPTION** drop-down list, the Xmedia Server Control Panel's Licensing page features fields and settings that allow you to add application and device licenses to the Xmedia Server. Figure 8-6 and the following descriptions provide an overview of each of the fields and settings. See [“Resolving license errors and adding licenses to the Xmedia Server” on page 8-16](#) for detailed instruction for using the Soft Keys page.

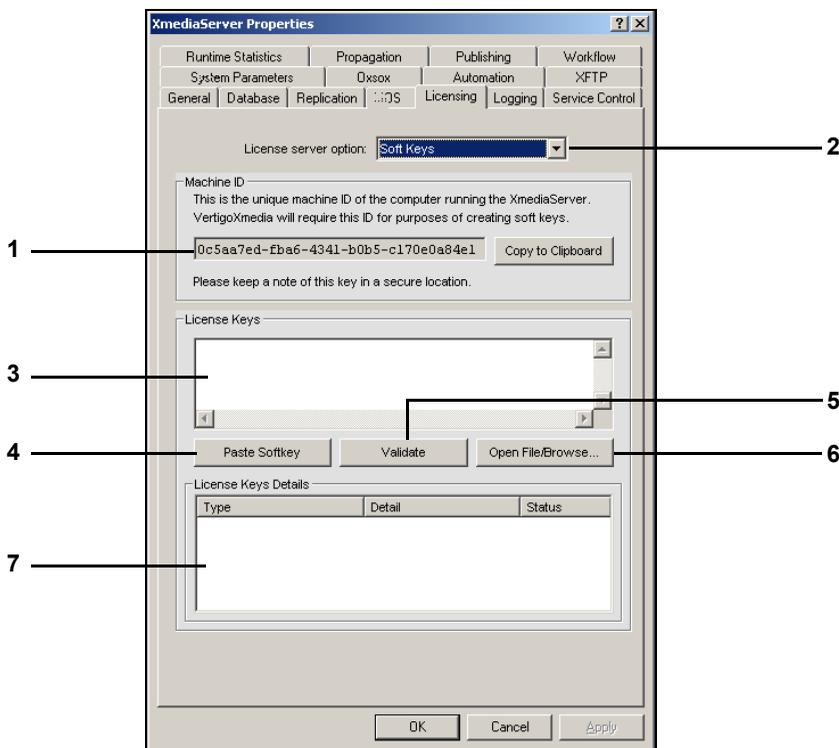


Figure 8-6. The Soft Keys page helps you to acquire and add new licenses to the Xmedia Server

1. **Machine ID:** This is a unique machine ID of the computer running the Xmedia Server. The Technical Support representative will require this ID for the purposes of creating the soft keys for license creation. Therefore, it is recommended that you take note of this ID and keep it in a secure location.
2. **Copy to Clipboard:** Since the Machine ID must be exact and error free when reported to our Technical Support team, this button allows you to copy the machine ID to your machine's clipboard. You can then paste it into an email and send it without worrying about errors.

3. **License Keys:** A license key is a long alpha-numeric code that our Technical Support team sends to you in response to a license request. The license key is used to add and engage licenses on the Xmedia Server.
4. **Paste Softkey:** Since the license keys are long alpha-numeric codes, it is recommended that you copy (**CTRL+C**) the license key(s) from the email onto your clipboard. Then you can press the **PASTE SOFTKEY** button to paste the license keys, (error free) into the **LICENSE KEYS** text box.
5. **Validate:** Once the license keys are pasted into the **LICENSE KEYS** text box, it is highly recommended that you press the **VALIDATE** button before applying the licenses. The **VALIDATE** button checks the validity of the license key, but does not apply the license. This check step helps to avoid unnecessary licensing errors.
6. **Open File/Browse:** Opens a window that allows you to browse your computer for the a license file containing a list of license soft keys. Selecting and opening the file using this window automatically populates the **LICENSE KEYS** text box with all of the soft keys contained in the file.
7. **License Key Details:** When the license keys are validated, you can preview the resulting licenses in the License Keys Details table.

Viewing the existing device and application licenses

The Xmedia Server Control Panel's Licensing page provides you with a complete inventory of the Vertigo Suite application and device licenses that are installed on the Xmedia Server. The list of licenses is often useful when troubleshooting licensing errors or to get a quick view of the system components.

To view the Xmedia Server's existing application and device licences:

- Open the Xmedia Server Control Panel and select the **LICENSING** tab.
The **LICENSE SUMMARY** table displays all of the licenses currently installed (figure 8-7).

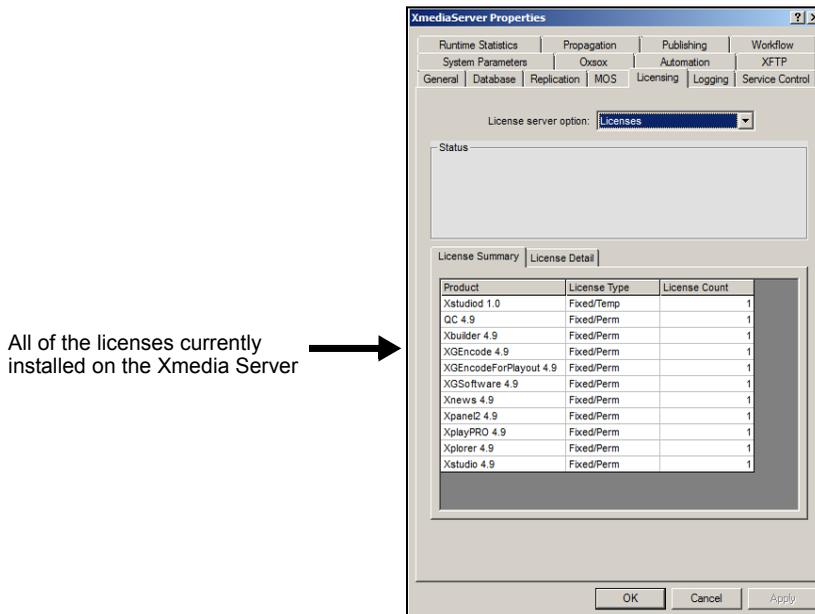


Figure 8-7. The License Summary table provides a list of the licenses installed on the Xmedia Server

If the Xmedia Server Control Panel's Licensing page does not display the License Summary table:

- Be sure that the **LICENSE SERVER OPTION** in the upper portion of the Licensing page is set to **LICENSES**.
- Be sure that the **LICENSE SUMMARY** tab is selected in the bottom portion of the Licensing page.

✓ NOTE

Contact your Grass Valley Sales representative if the License Summary table does not contain an expected license, or if you suspect an error in the type or number of licenses.

Viewing the details of a particular license

While the License Summary tab provides you with a high-level listing of the licenses installed on the Xmedia Server (see [page 8-7](#)), the License Detail tab displays a one-row listing of the properties related to the particular license that was last selected in the License Summary table. See [“Licenses view - License Detail tab” on page 8-10](#) for a list of the license details and a description of each property.

To view the details of a particular license:

1. Open the Xmedia Server Control Panel and select the **LICENSING** tab.
The **LICENSE SUMMARY** table displays all of the licenses currently installed on the Xmedia Server.
2. Select the license in the License Summary table that you want to view its properties.
3. Select the **LICENSE DETAIL** tab, or double-click the selected license in the License Summary table.
The Licensing page now displays the License Detail table with the selected license's details displayed in a single row (figure [8-8](#)).

The selected license's properties

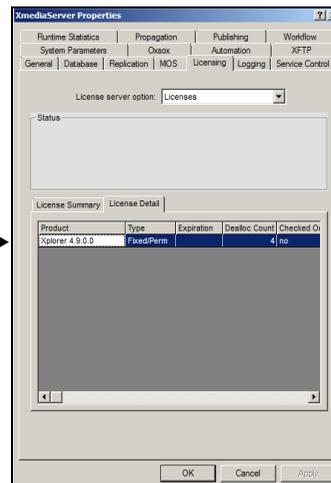


Figure 8-8. The license's properties are displayed in a single row on the License Detail tab's page

4. To view the various properties associated with the selected license, move the bottom scroll bar across the License Detail left-to-right.

✓ NOTE

These properties cannot be edited, except for deallocating a license (see [page 8-22](#)). Therefore, we recommend that you contact your Grass Valley Sales representative if the License Details does not contain the expected license settings.

Resolving license errors and adding licenses to the Xmedia Server

Your system's license requirements may have already been installed on the Xmedia Server when the system was factory configured or commissioned. Nevertheless, there are circumstance in which you may be required to resolve a license error that is preventing an application from opening, or features from being functional.

When an Vertigo Suite application does not find a valid license on start up, it produces a licensing error (figure 8-11), which prevents the application from launching until the error is resolved.

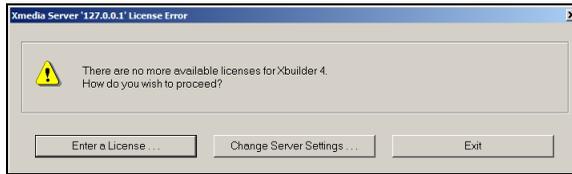


Figure 8-9. License error dialog box

Meanwhile, when devices like the Vertigo XG, Intuition XG, and VxPreview (Software CG) detect that the user is trying to operate a feature that is not licensed, it enables a watermark feature (figure 8-13) that disappears once a valid license is applied. Also, the title bar of the renderer's control panel states that there is no application license. See the **VERTIGO XG CONFIGURATION GUIDE** for more information about the watermark's behavior.

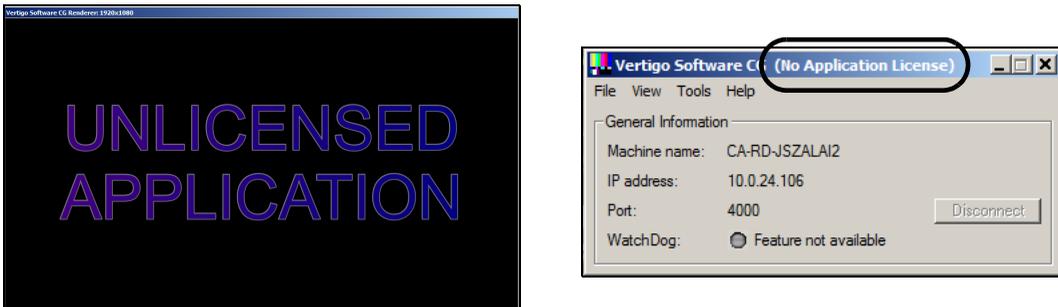


Figure 8-10. A watermark message appears if the Vertigo XG is not properly licensed

To investigate the cause and resolve an application's or device's license error, we recommend that you perform the procedures described in the following sections:

1. [“Verifying the application's or device's server settings” on page 8-17](#)
2. [“Verifying the License Summary and License Details” on page 8-20](#)
3. [“Acquiring and adding licenses to the Xmedia Server” on page 8-21](#)

Verifying the application's or device's server settings

The source of a license error may be as simple as incorrect server settings on the application or the device. The server settings specify the Xmedia Server's IP address and port, which allow the Xmedia Server to communicate licensing information to the applications and devices. For this reason, we recommend that you verify the server settings associated with the application or device before investigating the licenses themselves.

The following sections provide instructions for how to verify the server settings when a license error is raised for an application or a device:

- [“Verifying an application's server settings” on page 8-18](#)
- [“Verifying a device's server settings” on page 8-19](#)

Verifying an application's server settings

When an Vertigo Suite application does not find a valid license on start up, it produces a licensing error (figure 8-11). The source of the error may be as simple as incorrect server settings. These settings allow the Xmedia Server to communicate licensing information to the application. Therefore, we recommend that you verify the server settings associated with the application using the application's **SETTINGS** dialog box.



Figure 8-11. License error dialog box

NOTE

Additional information about application specific licensing is provided in each of the Vertigo Suite application's user manuals (i.e. Xstudio User Manual, Xbuilder User Manual...etc)

To verify that the application's server settings are properly set:

1. Select the **CHANGE SERVER SETTINGS** button on the **XMEDIA SERVER LICENSE ERROR** window (figure 8-11).

The application's **SETTINGS** dialog box appears (figure 8-12).

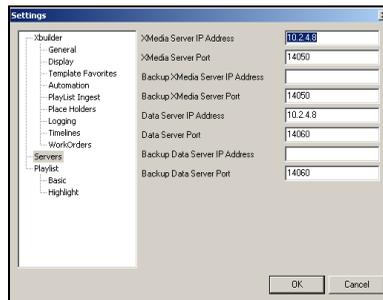


Figure 8-12. The application's Setting dialog box

2. Verify that all of the settings are correct, especially the Xmedia Server's IP address and port. If necessary, make the appropriate changes to the settings.
3. Click **OK** to close the **SETTINGS** dialog box.

If it was the server settings that were causing the license error, then the application will launch correctly now. However, if the **XMEDIA SERVER LICENSE ERROR** window immediately appears again, proceed to [page 8-21](#) and follow the instructions for acquiring and adding a valid application license to the Xmedia Server.

Verifying a device's server settings

When a device (Vertigo XG, Intuition XG, or Software CG) detects that the user is trying to use a feature that is not licensed, it displays a message on the device's panel and a watermark on the output (figure 8-13).

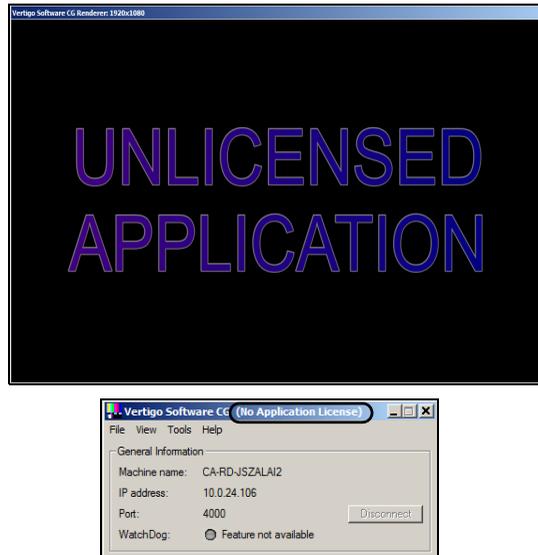


Figure 8-13. A watermark and message appears if the Vertigo XG is not properly licensed

The source of the license error may be as simple as incorrect server settings that allow the Xmedia Server to communicate licensing information to the device. Therefore, we recommend that you verify the server settings associated with the device using the device's panel and Dashboard.

To verify that the device's server settings are properly set:

1. Launch the XG Dashboard by selecting **TOOLS>LAUNCH DASHBOARD** from the device's panel.
2. Select the device from the Devices list in the upper portion of the Dashboard window.
3. Select the **DEVICE SETTINGS** tab.
4. Select the **LICENSING** page.
5. Verify the **XMS IP ADDRESS** and **XMS PORT** settings.

If the settings are incorrect, edit the settings and press the **APPLY CHANGES** button. Close the XG/CG window and then launch it again.

If the settings are correct but the licensing messages still appears, then verify the License Summary table and License Details on the Xmedia Server Control Panel's Licensing page (see [page 8-20](#)).

Verifying the License Summary and License Details

An application or a device might produce a licensing error if the required license has not been installed on the server, or if one or more of the license's properties has rendered it invalid. As such, we recommend that you verify the License Summary table to ensure that the appropriate license is indeed installed on the Xmedia Server. If so, then we also recommend that you verify the License Details to ensure that all of the license's properties are valid.

To verify that the appropriate license is installed and that its properties are valid:

1. On the Xmedia Server, open the **XMEDIA SERVER CONTROL PANEL** by selecting **VERTIGOXMEDIA XMEDIA SERVER** from within the Windows Control Panel.
2. Select the **LICENSING** tab.
3. Ensure that the **LICENSE SERVER OPTION** drop-down list is set to **LICENSES** and that the **LICENSE SUMMARY TAB** is selected.
4. Examine the contents of the License Summary table and verify if the required application or device license is listed (see [page 8-3](#) for a complete list of the available Vertigo Suite licenses).
 - If the required license is not listed in the **PRODUCT** column, or the license is listed but the value in the **LICENSE COUNT** column is **0**, then proceed to [page 8-21](#) and follow the instructions for acquiring and adding a license to the Xmedia Server.
 - If the required license is listed and the **LICENSE COUNT** value is greater than **0**, then proceed to the next step to verify the license details.
5. Select the license in the License Summary table.
6. Select the **LICENSE DETAIL** tab, or double-click the selected license in the License Summary table.

The Licensing page now displays the License Detail table with the selected license's details displayed in a single row (see figure [8-8 on page 8-15](#)).

7. Note the values in the **TYPE** column.
 - If the License type is **TEMPORARY**, then verify the expiry date in the Expiration column. If the license has expired, contact Grass Valley to renew the license.
 - If the License type is **FLOATING**, then another application/device might be using the license, thus making it unavailable. If this is the case, either change the application/device's server settings to get a license from another server, or free up a license by closing the application on another client computer and then try to launch the application again on the desired computer.
8. Use the scroll bar to move along the row in the License Detail, and note the values for the remaining properties.
 - If any of the values are incorrect, proceed to [page 8-21](#) and follow the instructions for acquiring and adding a license to the Xmedia Server.
 - If the values all appear to be correct, then contact our Technical Support team (support@miranda.com) for further investigation.

Acquiring and adding licenses to the Xmedia Server

When the cause of a license error is because a required license has not been installed, or because the license contains erroneous data, you will be required to acquire and apply a new license key to the Xmedia Server Control Panel's Licensing **SOFT KEYS** page.

To acquire and apply a valid license to the Xmedia Server:

1. Open the **XMEDIA SERVER CONTROL PANEL**, by selecting **VERTIGOXMEDIA XMEDIASERVER** from within the Windows Control Panel.
2. Select the **LICENSING** tab.
3. Select **SOFT KEYS** from the **LICENSE SERVER OPTION** field's drop-down list.
4. Press the **COPY TO CLIPBOARD** button in the **MACHINE ID** section to copy your machine's unique identification number.
5. Paste the **MACHINE ID NUMBER** into an email and send the email to our Technical Support department (support@miranda.com) and describe your need for valid licenses. Upon receipt of the email, a Grass Valley representative will verify the licensing agreement that you purchased and an email will be returned to you with the appropriate license code (soft key).
6. Copy and paste the license code from the email into the **LICENSE KEYS** text box on the Licensing tab.
7. Click **VALIDATE**.
8. Click **APPLY**.
9. Select **LICENSES** from the **LICENSE SERVER OPTION** field's drop-down list, and verify that the required licenses appear in the **LICENSE SUMMARY** table.
If the proper license is not listed, or if you require further licenses, please contact our Technical Support department (support@miranda.com).
10. To view the details of the license, select the license from the list and then select the **LICENSE DETAIL** tab.
11. Click **OK** to close the Xmedia Server Control Panel window.
12. Restart the device's panel or the application to verify that the licensing messages are no longer displayed.

Deallocating a fixed license

Fixed licenses are appropriate when a particular computer is dedicated to running the Vertigo Suite applications, or when a particular device is dedicated as the main playout machine. Licenses rarely need to be transferred or shared in these circumstances, but in case they do, the Xmedia Server allows you to manually deallocate a fixed license up to four (4) times. If you wish to deallocate a fixed license more than four times, you must contact our Technical Support department.

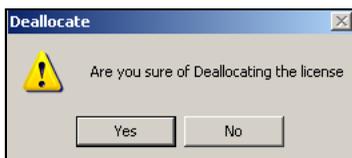
To deallocate a fixed license from one computer and reassign it to another:

1. Open the **XMEDIA SERVER CONTROL PANEL**, by selecting **VERTIGOXMEDIA XMEDIA SERVER** from within the Windows Control Panel.
2. Select the **LICENSING** tab.
3. Select **LICENSES** from the **LICENSE SERVER OPTION**'s drop-down list.
4. On the **LICENSE SUMMARY** tab, select the license that is to be deallocated.
5. Select the **LICENSE DETAIL** tab.
6. Verify that the **DEALLOC COUNT** column value is greater than **0**.
 - If the value is greater than 0, then you may proceed to deallocate the license.
 - If the value is 0, then you are not be permitted to deallocate the license and you must contact our Technical Support team (support@miranda.com) before you can proceed any further.
7. Move the License Detail tab's scroll bar to the right to display the **COMPUTER, IP ADDRESS, and MACHINE ID COLUMNS**.
8. Right-click on the license detail row and select the **DEALLOCATE** command.

Checked Out	Computer	IP Address	Machine ID	Time Stamp
no	cards-izsala	10.2.4.8	5LY8	06 11:18:37

Deallocate

9. Confirm your intention to deallocate the license by clicking **YES** when the **DEALLOCATE** dialog box appears.



The **DEALLOC COUNT** column value is reduced by one and the remaining columns will remain empty until an application or device is launched and requests this license from the Xmedia Server. At that point, the Xmedia Server will allocate the license to the machine or device hosting the application.

Dealloc Count	Checked Out	Computer	IP Address	Machine ID
3	no			

9 LOGGING XMEDIA SERVER EVENTS

The Xmedia Server Control Panel's **LOGGING** page (figure 9-1) allows you to set parameters to create a logging criteria that records the status of Xmedia Server events while the XMS Service is operating. The Xmedia Server events are recorded to a log text file (XmediaServer*.log), which allows you to determine whether the Xmedia Server is being used correctly and it helps you to diagnose error conditions. In fact, our Technical Support team will often ask its customers to send them the Xmedia Server's log file to help them troubleshoot any unexpected behavior that they may be experiencing with an Xmedia Server.



Figure 9-1. The Xmedia Server Control Panel's Logging page

✓ NOTE

Be aware that logging may adversely affect your product's performance, especially on air performance. Therefore, we recommend enabling logging only when you are troubleshooting.

The Xmedia Server's **Logging Levels** and **Debug Categories** settings allow you to specify the type and categories of events that you want to be recorded in the Xmedia Server log files.

LOG LEVEL

This sets the default log level used by all logging categories except those that have been checked in the Debug Categories list. The choices are:

- **Error** - Only log errors and essential operations.
- **Warn** - Log unsuccessful operations that may indicate a problem (in addition to all messages logged at the Error level).
- **Info** - (Default) Log important events that occur during normal conditions (in addition to all messages logged at the Warn level).

It is recommended to set the **Log Level** to **Info** in order to provide enough information in the logs to diagnose common problems without affecting performance.

Debug Categories

Select the types of debug logging (categories) that you would like to record in the Xmedia Server log file:

- **GENERAL** - General logging that does not fit under any other category.
- **DATABASE** - Database connections
- **PUBLISH** - Publishing subsystem
- **REPLICATE** - Replication subsystem
- **FILE** - File handling
- **TCP** - Network activities
- **OXSOX** - Oxsox protocol communication
- **INIT** - Startup and process initialization
- **LICENSING** - Vertigo Suite application licensing
- **SESSIONMANAGER** - All connections to the Xmedia Server
- **Validation** - Logging records how the validation status was obtained for each of the following events:
 - "verify playlist" elements in Xplay
 - the R3 oxtel command
 - MOS rundown validation
- **ValidationTiming** - Records in the logs how long the validation of an asset takes to execute, as well as detailing the duration of the different steps of the validation process. The **VALIDATIONTIMING** setting must be selected in conjunction with the **VALIDATION** setting.
- **VxmsTcpLayer** - Socket communication used by propagation and publishing is logged.
- **Mos** - Records MOS Redirection activity inside the Xmedia Server. This setting provides additional logging to the MOS logging activities already recorded in the vxmos.log file, which is enabled using the **MOS LOGGING OPTIONS** on the **MOS** tab (see [page 7-8](#)).

Log Destinations

The following settings allow you to manage and access the Xmedia Server log files on your system.



- **LOG TO CONSOLE:** Currently not available for external use. The events are written to a console for Grass Valley personnel to use for testing and debugging tasks.
- **FILE SIZE** - Sets the maximum memory size for each log file created per run. The default value is 20 MB.
- **FILE COUNT** - Specifies the maximum number of XmediaServer*.log files that will be stored. A large enough number should be chosen to store over a day's worth of logs. This way if a problem happens the relevant log files will be available. Once the maximum number of files is reached, the oldest log file will be replaced by a new one. The default value is 10.
- **EXPLORE LOG FOLDER** - Click this button to immediately open the folder that contains all of the Vertigo Suite's log files, including all of the existing Xmedia Server log files. This is a quick way to access previous log files as well as the current log file. The path to the Vertigo Suite's Log folder is:

C:\Documents and Settings\All Users\Application Data\VertigoXmedia\Logs

- **VIEW LOG** - Click this button to immediately open the current Xmedia Server log file in Notepad.

```
XmediaServer-0001-04292012-235339.log - Notepad
File Edit Format View Help
04/29/2012 23:53:39.889 [5636] FTPLClient.cpp:1533 General DEBUG FTP HEADER IN - 227 Entering Passive Mode
(10,14,8,1,73,54)
04/29/2012 23:53:39.889 [5636] FTPLClient.cpp:1623 General DEBUG FTP INFO - Trying 10.14.8.1...
04/29/2012 23:53:39.889 [5636] FTPLClient.cpp:1623 General DEBUG FTP INFO - connected
04/29/2012 23:53:39.889 [5636] FTPLClient.cpp:1623 General DEBUG FTP INFO - Connecting to 10.14.8.1
(10.14.8.1) port 18742
04/29/2012 23:53:39.889 [5636] FTPLClient.cpp:1589 General DEBUG FTP HEADER OUT - TYPE A
04/29/2012 23:53:39.889 [5636] FTPLClient.cpp:1533 General DEBUG FTP HEADER IN - 200 Type set to A.
04/29/2012 23:53:39.889 [5636] FTPLClient.cpp:1589 General DEBUG FTP HEADER OUT - NOOP
04/29/2012 23:53:39.889 [5636] FTPLClient.cpp:1533 General DEBUG FTP HEADER IN - 200 NOOP command
successful.
04/29/2012 23:53:39.889 [5636] FTPLClient.cpp:1623 General DEBUG FTP INFO - RETR response: 200
04/29/2012 23:53:39.889 [5636] FTPLClient.cpp:1623 General DEBUG FTP INFO - Remembering we are in dir ""
04/29/2012 23:53:39.889 [5636] FTPLClient.cpp:1623 General DEBUG FTP INFO - Connection #0 to host 10.14.8.1
left intact
04/29/2012 23:53:39.889 [5636] FTPLClient.cpp:278 General DEBUG FTPLClient::retrieveRequestInfo - Primary IP
address := 10.14.8.1
04/29/2012 23:53:39.889 [5636] FTPLClient.cpp:286 General DEBUG FTPLClient::retrieveRequestInfo - FTP entry
path := /media
04/29/2012 23:53:39.889 [5636] FTPLClient.cpp:294 General DEBUG FTPLClient::retrieveRequestInfo - Effective
url := ftp://10.14.8.1
04/29/2012 23:53:39.889 [5636] FTPLClient.cpp:299 General DEBUG FTPLClient::retrieveRequestInfo - Response
code := 200
04/29/2012 23:53:39.889 [5636] FTPLClient.cpp:303 General DEBUG FTPLClient::retrieveRequestInfo - Connection
error := 0
04/29/2012 23:53:39.889 [5636] FTPLClient.cpp:1589 General DEBUG FTP HEADER OUT - QUIT
04/29/2012 23:53:39.889 [5636] FTPLClient.cpp:1533 General DEBUG FTP HEADER IN - 221-You have transferred 0
bytes in 0 files.
04/29/2012 23:53:39.889 [4548] FTPLClient.cpp:1533 General DEBUG FTP HEADER IN - 230 User media logged in.
04/29/2012 23:53:39.889 [4548] FTPLClient.cpp:1589 General DEBUG FTP HEADER OUT - PWD
04/29/2012 23:53:39.889 [5636] FTPLClient.cpp:1533 General DEBUG FTP HEADER IN - 221-Total traffic for this
session was 436 bytes in 0 transfers.
```

10 WORK ORDER WORKFLOW CONFIGURATION

The Vertigo Suite provides a fully integrated module for requesting, completing, tracking and approving graphics work orders. The work order management system is based on a standardized workflow that is configured using the Xmedia Server Control Panel's **WORKFLOW** page.

Although the Xmedia Server provides a default workflow (see [page 10-3](#)), we recommend that you modify this workflow so that it represents the exact procedure by which work order requests are created, completed, and approved within your organization. The customization of the workflow is performed by adding, removing, and/or editing the **WORKFLOW OPTIONS** that appear on the Xmedia Server Control Panel's Workflow page.

Another feature of the Xmedia Server Control Panel's Workflow page is the **E-NOTIFICATION** workflow option, which allows the work order module to automatically send email alerts to users when a job's assignee is specified, or when a work order's has transitioned to a new state (see ["Setting up E-Notifications" on page 10-35](#) more information).

The following sections describe work order workflow models and how to use the Xmedia Server Control Panel's Workflow page to configure a workflow that best meets your organization's needs:

- ["Xmedia Server Control Panel's Workflow options" on page 10-2](#)
- ["Workflow models" on page 10-3](#)
- ["Workflow option: States" on page 10-5](#)
- ["Workflow option: Permissions" on page 10-9](#)
- ["Workflow option: Transitions" on page 10-13](#)
- ["Workflow option: Priorities" on page 10-22](#)
- ["Workflow option: Roles" on page 10-25](#)
- ["Workflow option: Users" on page 10-30](#)

NOTE

This document's coverage of work order management is limited to using Xmedia Server Control Panel to configure a work order workflow. Information and instructions regarding creating, completing, and approving work order requests are provided in the **XPLORER USER MANUAL** and the **XBUILDER USER MANUAL**.

Xmedia Server Control Panel's Workflow options

Selecting the **WORKFLOW** tab on the Xmedia Server Control Panel displays the **WORKFLOW** page. The **WORKFLOW** page is a multi-view interface that allows you to configure the **WORKFLOW OPTIONS** that are responsible for building the workflow that manages work order requests.

Selecting a Workflow option from the drop-down list changes the page's view to display the elements that belong to the option in the page's main pane (figure 10-1).

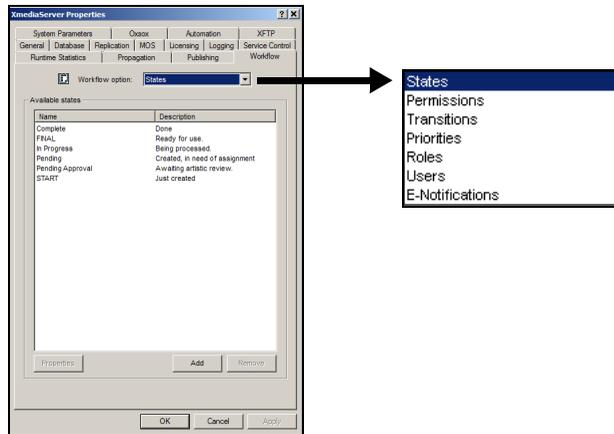


Figure 10-1. The Workflow option drop-down list controls the views of the Workflow page

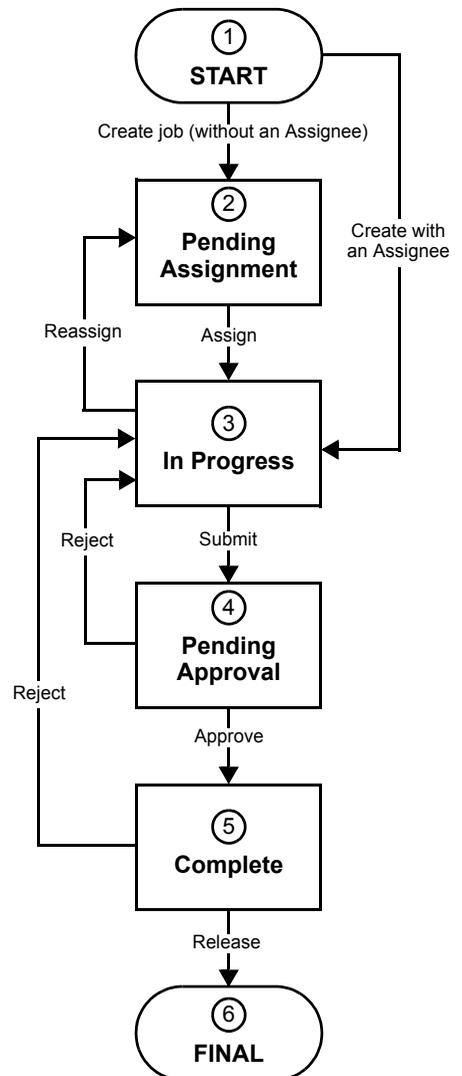
The following table briefly describes each of the workflow options, while the remaining sections of this chapter describe how to use the options to customize your work order workflow.

STATES	States are the milestones during a workflow that indicate the work order's current stage of completion.
TRANSITIONS	Transitions are the specific actions that are executed by users to advance the work order from one state to the next.
ROLES	Roles are groupings of permissions that allow users to perform the tasks applicable to their job function.
USERS	Each participant in the workflow has a user profile. Adding roles to a user's profile determines what functions the user is allowed to perform in the workflow process.
PERMISSIONS	Permissions grant users the authority to perform certain tasks or actions within the workflow, like create or approve a job.
PRIORITIES	Work orders can be assigned a priority classification to indicate the urgency of the request.
E-NOTIFICATION	E-notifications automatically send email alerts to users when a job's assignee is specified or when a work order's has transitioned to a new state.

Workflow models

The Xmedia Server Control Panel's **WORKFLOW** page contains a default workflow model that represents a realistic work order workflow. In some cases, the default workflow may only require minor adjustments (i.e. add new users, or edit roles or permissions) to meet your organization's work order needs. The following diagram and descriptions identify the states and transitions in the Xmedia Server's default work order workflow.

1. **START:** Work orders and jobs are requests made to the graphics department from a journalist or a producer for a new image or clip to be added to the system. A placeholder is set on the page(s) where the requested image or clip will eventually appear.
2. **Pending Assignment:** A journalist or producer can assign the job request immediately to a specific person when the job is created (step1), or the person responsible for workload assignment for the graphics department can assign the job to a specific graphic artist.
3. **In progress:** The graphic artist who is assigned the job, either creates or locates the requested image or clip and ingests it into the Xmedia Server. They then submit the job for approval. If for some reason a reassignment of the job is necessary, the job can be reassigned to another assignee.
4. **Pending Approval:** The job that is submitted by the graphic artist must be approved by the Art Director to ensure that it meets all of the standards and requirements. If the Art Director approves the job, then it is sent back to the journalist or producer to be sure that it meets their requirements. If the Art Director rejects the job, then the job is resubmitted to the graphic artist for editing.
5. **Complete:** The journalist or producer who originally created the job must provide the final approval before the job is considered complete. If the submitted job does not meet the requirements, then it is rejected and sent back to the graphic artist for editing.
6. **Final:** When the job is released by the journalist or producer who requested the job, the image or clip automatically replaces all of the placeholders on the pages that the job was linked to. The job is now final and cannot be edited.



Simplifying the workflow model

While the default workflow described on [page 10-3](#) represents a realistic work order workflow, it may be too complex for a small or informal organization and a simpler workflow may be required. In such a case, the default workflow's options can be edited to any degree to accommodate your organization's needs.

Figure [10-2](#) demonstrates that the Xmedia Server's **WORKFLOW OPTIONS** can be simplified to reflect work order workflow models that are as simple as a three-state (2 transitions) workflow.

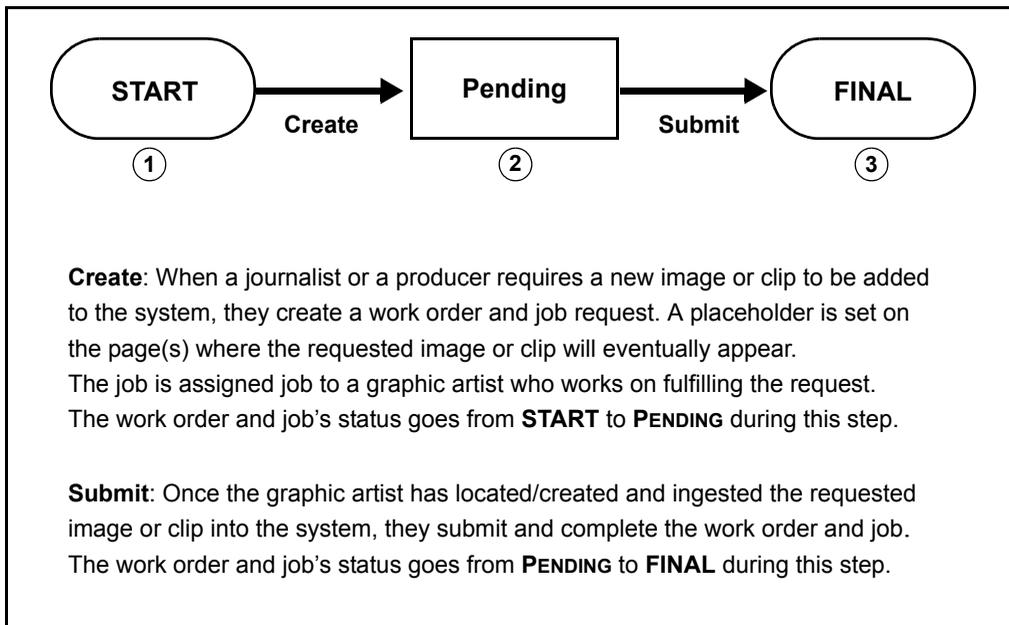


Figure 10-2. An example of a simplified work order workflow (3 states and 2 transitions)

Workflow option: States

The workflow that is responsible for creating and filling work orders is broken-down into various stages of completion called **STATES**. Each state is associated with **TRANSITIONS** (actions) that advance the work order to the next state (stage of completion).

When **STATES** is selected from the **WORKFLOW OPTION** drop-down list, the Workflow page displays the available states that have been defined for the current work order workflow.

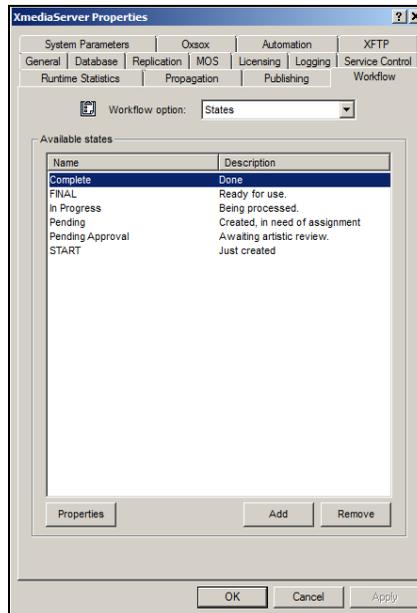


Figure 10-3. The States option displays a list of the current workflow's states

Figure [10-3](#) and the following list identifies the workflow states that are present in the Xmedia Server's default workflow. Further details are also available on [page 10-3](#).

- **START** - The work order/job is created.
- **PENDING** - The work order/job has been created, but has not yet been assigned to a user.
- **IN PROGRESS** - The work order/job is currently being worked on.
- **PENDING APPROVAL** - The work order/job has been submitted and is awaiting approval.
- **COMPLETE** - The work order/job has been approved and is about to be released.
- **FINAL** - The work order/job is ready to be used.

The following sections provide instructions for tasks for defining the workflow states, including how to add, remove and edit states:

- [“Adding a new state to the workflow” on page 10-6](#)
- [“Editing a state's properties” on page 10-7](#)
- [“Removing a state from the workflow” on page 10-8](#)

Adding a new state to the workflow

To add a new state to the workflow:

1. Open the Xmedia Server Control Panel and select **STATES** from the **WORKFLOW OPTION** drop-down list.
2. Click **ADD** in the lower-right corner of the Workflow page.
The **ADD A STATE** dialog box appears (figure [10-4](#)).

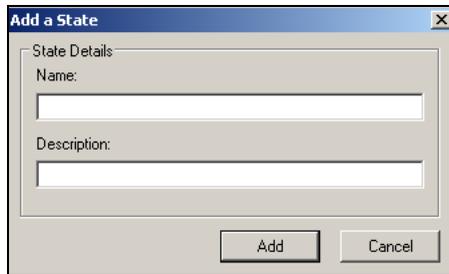


Figure 10-4. Add a state to the current workflow by assigning it a name and description

3. Type a name for the State in the **NAME** text box.
4. Type a brief description that identifies the purpose of the state in the **DESCRIPTION** text box.
5. Click **ADD**.
The state is immediately added to the **AVAILABLE STATES** list on the Workflow page, and it can now be used to define a transition in the workflow (see [page 10-13](#)).

Editing a state's properties

To view and edit the properties of a state that already exists in the workflow:

1. Open the Xmedia Server Control Panel and select **STATES** from the **WORKFLOW OPTION** drop-down list.
2. Select the state that is to be edited from the **AVAILABLE STATES** list.
3. Click **PROPERTIES** in the lower-left corner of the Workflow page, or double click on the state in the **AVAILABLE STATES** list.

The **EDIT STATE** dialog box appears (figure [10-5](#)).

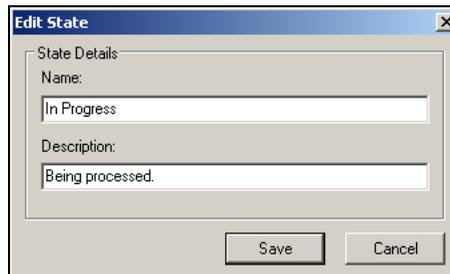


Figure 10-5. The state properties that can be edited are Name and Description

4. Edit the state's name and/or description by typing in the appropriate text boxes.
5. Click **SAVE** to apply the new properties to the state.

The edits to the state are immediately applied to the **AVAILABLE STATES** list on the Workflow page, as well as to any use of that state in the workflow's Transitions (see [page 10-13](#)).

Removing a state from the workflow

With the exception of the **START** and **FINAL** states which cannot be deleted, all other states can be deleted from the workflow.

As the instructions below describe, deleting a state involves clicking the **REMOVE** button in the lower-right corner of the Workflow page. Note that the **REMOVE** button is only enabled if the state that is selected is not currently being used by a transition. In other words, a state can only be deleted from the workflow if it is not actively assigned to a transition.

To remove and delete a state from the current workflow:

1. Open the Xmedia Server Control Panel and select **STATES** from the **WORKFLOW OPTION** drop-down list.
2. Select the state that is to be deleted from the **AVAILABLE STATES** list.
3. Click **REMOVE** in the lower-right corner of the Workflow page.
The **CONFIRM DELETE** dialog box appears (figure [10-6](#)).

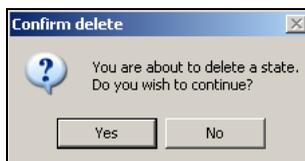


Figure 10-6. Select Yes to permanently delete the state from the workflow

4. Click **YES** to permanently delete the state from the current workflow.
The state is immediately removed from the Available States list on the Workflow page. As well, it is no longer available to be used to define a transition in the workflow (see [page 10-13](#)).

Workflow option: Permissions

Permissions grant the authority to perform specific tasks or actions within the workflow. Users are assigned roles, and the roles are associated with permissions that grant the user the authority to perform the tasks associated with the role.

When **PERMISSIONS** is selected from the **WORKFLOW OPTION** drop-down list, the Workflow page displays the available permissions that have been defined for the current work order workflow. Figure 10-7 and the following lists identifies the workflow permissions that are present in the Xmedia Server's default workflow.

- **ARTISTICAPPROVAL** - Grants permission to approve/reject a completed job
- **ASSIGN** - Grants permission to assign a pending job
- **COMPLETION** - Grants permission to indicate job completion
- **WOCREATION** - Grants permission to create a work order
- **WODELETION** - Grants permission to delete a work order
- **WOJOB CREATION** - Grants permission to create a work order job
- **WOJOB DELETION** - Grants permission to delete a work order job

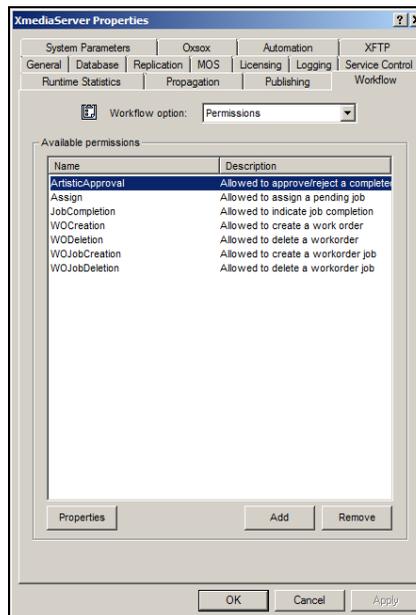


Figure 10-7. The Permissions option displays a list of the current workflow's permissions

The following sections provide instructions for tasks that help you to define the permissions for your workflow, including how to add, remove and edit permissions:

- [“Adding a new permission to the workflow” on page 10-10](#)
- [“Editing a permission’s properties” on page 10-11](#)
- [“Removing a permission from the workflow” on page 10-12](#)

Adding a new permission to the workflow

To add a new permission to the workflow:

1. Open the Xmedia Server Control Panel and select **PERMISSIONS** from the **WORKFLOW OPTION** drop-down list.
2. Click **ADD** in the lower-right corner of the Workflow page.
The **ADD A PERMISSION** dialog box appears (figure [10-8](#)).

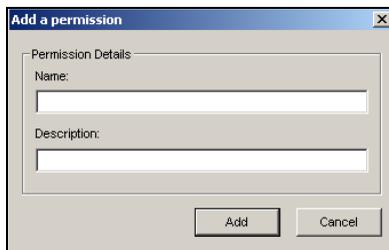


Figure 10-8. Add a permission to the current workflow by assigning it a name and description

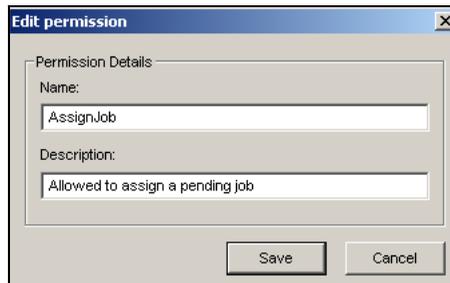
3. Type a name for the permission in the **NAME** text box.
4. Type a brief description that identifies the purpose of the permission in the **DESCRIPTION** text box.
5. Click **ADD**.
The permission is immediately added to the **AVAILABLE PERMISSIONS** list on the Workflow page, and it can now be used to define roles and transitions in the workflow (see [page 10-25](#) and [page 10-13](#)).

Editing a permission's properties

To view and edit the properties of a permission that already exists in the workflow:

1. Open the Xmedia Server Control Panel and select **PERMISSIONS** from the **WORKFLOW OPTION** drop-down list.
2. Select the permission that is to be edited from the **AVAILABLE PERMISSIONS** list.
3. Click **PROPERTIES** in the lower-left corner of the Workflow page, or double click on the permission in the **AVAILABLE PERMISSIONS** list.

The **EDIT PERMISSION** dialog box appears (figure [10-9](#)).



The screenshot shows a dialog box titled "Edit permission". Inside, there is a section labeled "Permission Details" which contains two text input fields. The first field is labeled "Name:" and contains the text "AssignJob". The second field is labeled "Description:" and contains the text "Allowed to assign a pending job". At the bottom of the dialog, there are two buttons: "Save" and "Cancel".

Figure 10-9. The permission's properties that can be edited are Name and Description

4. Edit the permission's name and/or description by typing in the appropriate text boxes.
5. Click **SAVE** to apply the new properties to the permission.
The edits to the permission are immediately applied to the **AVAILABLE PERMISSIONS** list on the Workflow page, as well as to any transitions or role definitions that use the permission (see [page 10-25](#) and [page 10-13](#)).

Removing a permission from the workflow

Note that the following system permissions cannot be deleted: WOCreation, WODEletion, WOJobCreation, WOJobDeletion. However, all other permissions can be deleted from the workflow if they are no longer desired.

Deleting a permission involves using the **REMOVE** button in the lower-right corner of the Workflow page. Note that the **REMOVE** button is only enabled if the permission that is selected is not currently assigned to a role or transition. In other words, a permission can only be deleted from the workflow if it is not actively assigned to a role or transition.

To remove and delete a permission from the current workflow:

1. Open the Xmedia Server Control Panel and select **PERMISSIONS** from the **WORKFLOW OPTION** drop-down list.
2. Select the permission that is to be deleted from the **AVAILABLE PERMISSIONS** list.
3. Click **REMOVE** in the lower-right corner of the Workflow page.
The **CONFIRM DELETE** dialog box appears (figure [10-10](#)).



Figure 10-10. Select Yes to permanently delete the permission from the workflow

4. Click **YES** to permanently delete the permission from the current workflow.
The permission is immediately removed from the **AVAILABLE PERMISSIONS** list on the Workflow page. As well, it is no longer available to be used to assigned to transitions or role definitions (see [page 10-25](#) and [page 10-13](#)).

Workflow option: Transitions

Transitions are the specific actions, like assign or approve, that are executed by users to advance the work order from one state to the next. Transitions are made available only to users who are assigned a specific role and permissions. They are created and configured in the **TRANSITIONS** workflow option section of the **XMEDIA SERVER CONTROL PANEL**.

Figure 10-11 and the following list identifies the transitions that belong to the Xmedia Server's default workflow.

- **APPROVE** - Advances the work order/job from **PENDING APPROVAL** to **COMPLETE**
- **ASSIGN** - Advances the work order/job from **PENDING** to **IN PROGRESS**
- **CREATE** - Automatic transition that advances the work order/job from **START** to **PENDING**
- **REASSIGN** - Reassigns a job to another qualified user during **IN PROGRESS**
- **REJECT** - Returns the work order/job from **COMPLETE** back to **IN PROGRESS**
- **REJECT** - Returns the work order/job from **PENDING APPROVAL** back to **IN PROGRESS**
- **RELEASE** - Advances the work order/job from **COMPLETE** to **FINAL**
- **SUBMIT** - Advances the work order/job from **IN PROGRESS** to **PENDING APPROVAL**

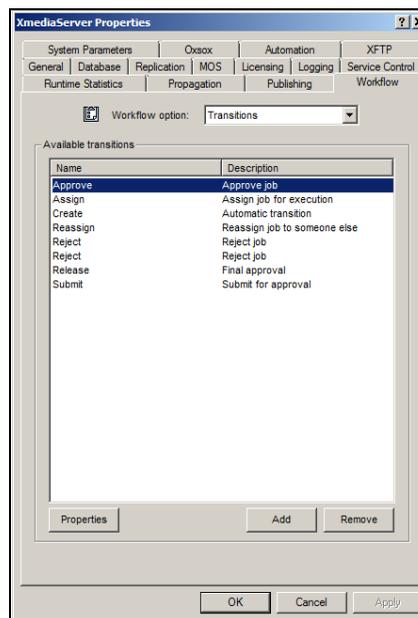


Figure 10-11. The default workflow's transitions

The following sections describe how to add and remove transitions from a workflow, as well as how to define the properties associated with a transition:

- [“Transition properties and permissions” on page 10-14](#)
- [“Adding a new transition to the workflow” on page 10-18](#)
- [“Editing a transition’s properties and permissions” on page 10-20](#)
- [“Deleting a transition from the workflow” on page 10-21](#)

Transition properties and permissions

A transition's properties are initially defined when the transition is created using the **NEW TRANSITION** dialog box (see [“Adding a new transition to the workflow” on page 10-18](#)). Once the transition has been created you can view or edit the transition's properties and permission assignment in the **TRANSITION PROPERTIES** dialog box (see [“Editing a transition's properties and permissions” on page 10-20](#)).

The **TRANSITION PROPERTIES** dialog box is accessed by:

- Double-clicking the transition's name in the **AVAILABLE TRANSITIONS** list

Or,

- Selecting the transition's name and then clicking the **PROPERTIES** button in the lower-left corner of the Workflow page's Transition view.

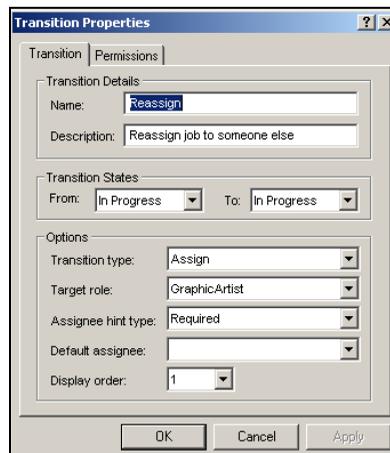


Figure 10-12. The Transition Properties dialog box

A transition is defined by the properties values set on the **TRANSITION** tab. These properties not only affect the transition's behavior, but they also determine the features and behavior of the Work Order window in the Vertigo Suite applications. Meanwhile, the **PERMISSIONS** tab allows you to add permissions to the transition to determine who can execute the transition.

The following sections provide more information about the settings and use of these two Transition Properties tabs:

- [“Transition tab settings” on page 10-15](#)
- [“Permissions tab” on page 10-17](#)

Transition tab settings

The following table describes each of the settings that are found on the **TRANSITION** tab of the **TRANSITION PROPERTIES** dialog box. These descriptions also explain the affect that the settings have on the appearance and behavior of the transition buttons that appear on the Work Order and jobs windows in the Vertigo Suite applications.

Name	The name of the transition. The name should clearly identify the function of the transition, like ASSIGN , APPROVE , or REJECT . The exact name is used to label the TRANSITION button on the Work Order and Jobs windows in the Vertigo Suite applications.
Description	A brief description of the function or purpose of the transition. For example, the description of the SUBMIT transition is SUBMIT FOR APPROVAL . This text is displayed when you hover your mouse's pointer over a TRANSITION button in the JOB window.
Transition States	<p>Specifies between which two states the transition can be executed. For example, in the default workflow the APPROVE transition can only be launched between the APPROVAL PENDING state (FROM) and the COMPLETE state (TO).</p> <p>The FROM setting also determines during which state the transition button will be displayed on the Work Order or Jobs windows in the application. For example, the APPROVE transition button will only be displayed when the job's state is APPROVAL PENDING. Note that the button is displayed, but it will only be enabled if the currently logged in user has the proper permissions for approving jobs, otherwise it is greyed out.</p> <p>Note: Each state can only be assigned to a maximum of three (3) transitions.</p>
Transition type	<p>The transition type settings determine the button format (icon) that will represent the transition at the top of the Work Order or Jobs windows in the application.</p> <p>Select one of the following predefined button formats and the button will consist of the given name and the icon associated with the TRANSITION TYPE setting:</p> <ul style="list-style-type: none"> • ACCEPT =  • ASSIGN =  • OTHER =  • REJECT =  • SUBMIT = 

Target role	Identifies the role that will be assigned to the job after the transition is executed. If the assignee is specified during the transition, the assignee must have this role to be able to proceed. See “Permissions tab” on page 10-17 for related information.
Assignee hint type	<p>This property provides you with the option to have a dialog box appear in the application’s Work Order or Jobs windows that allows you to specify which user the work order or job will be assigned to after the transition has been executed.</p> <ul style="list-style-type: none"> • CREATOR: The ASSIGNEE field already displays in the dialog box the name of the user who originally created the job. You can leave the assignee as is, or select another user’s name from the drop-down list. Note that only the name of the people that were assigned the same role as the one specified in the TARGET ROLE property appear in the list. • DEFAULT: Not implemented yet. No dialog box appears and the job continues immediately to the next state with the assignee specified as the user set in the DEFAULT ASSIGNEE property. • NOT REQUIRED: No dialog box appears and the job continues immediately to the next state without an assignee specified (i.e. NONE). • REQUIRED: A dialog box appears in the application, but the ASSIGNEE field is empty. You must select a user’s name from the drop-down list. Note that only the name of the people that were assigned the same role as the one specified in the TARGET ROLE property appear in the list. • SUBMITTER: A dialog box appears in the application and the ASSIGNEE field is already displays the name of the logged in user who is submitting the job. You can leave the ASSIGNEE as is, or select another user’s name from the drop-down list. Note that only the name of the people that were assigned the same role as the one specified in the TARGET ROLE property appear in the list.
Default assignee	Not implemented yet. Displays a list of users. If the ASSIGNEE HINT TYPE property is set to DEFAULT , then the user selected in this property will automatically be assigned the job when the transition is executed.
Display order	Determines the displayed order of the transition buttons at the top of the Work Order or Jobs windows. 1 positions the button as the first button (left) and 2 positions the button as the second button (right).

Permissions tab

The **PERMISSION** tab on the **TRANSITION PROPERTIES** dialog box displays the permissions that have been assigned to the transition (figure 10-13). The permissions ensure that only certain users are able to use the transition to move the work order or job from one state to another.



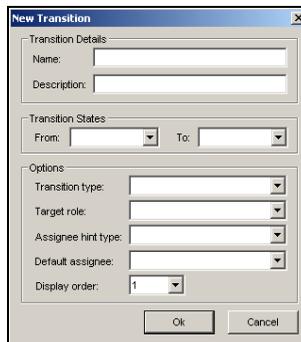
Figure 10-13. The Transition's permissions determine which users have access to the transaction

Before you can add permissions to the Transition, the permissions must be created and defined on the Workflow page's **PERMISSIONS** view (see [“Workflow option: Permissions” on page 10-9](#)). Once the necessary permissions have been created, you can add them to the Transition by following the directions on [page 10-19](#).

Adding a new transition to the workflow

To add a new transition to the workflow:

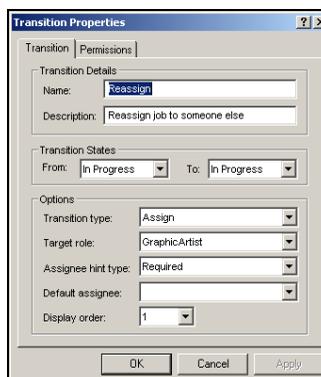
1. Open the Xmedia Server Control Panel and select **TRANSITIONS** from the **WORKFLOW OPTION** drop-down list.
2. Click **ADD** in the lower-right corner of the Workflow page.
The **NEW TRANSITION** dialog box appears (figure [10-14](#)).



The 'New Transition' dialog box is a standard Windows-style window with a title bar and a close button. It is divided into several sections: 'Transition Details' with 'Name' and 'Description' text boxes; 'Transition States' with 'From' and 'To' dropdown menus; and 'Options' with 'Transition type', 'Target role', 'Assignee hint type', 'Default assignee', and 'Display order' dropdown menus. At the bottom are 'Ok' and 'Cancel' buttons.

Figure 10-14. Specify the properties of a new transition in the New Transition dialog box

3. Define the transition by completing the new transition's properties. See [page 10-20](#) for a description of each of the transition property fields.
4. Click **ADD**.
The transition is immediately added to the **AVAILABLE TRANSITIONS** list on the Workflow page.
5. Double-click on the new transition's name in the **AVAILABLE TRANSITIONS** list.
The **TRANSITION PROPERTIES** dialog box appears (figure [10-15](#)).



The 'Transition Properties' dialog box has two tabs: 'Transition' and 'Permissions'. The 'Transition' tab is active, showing the same fields as Figure 10-14, but with pre-filled values: Name is 'Reassign', Description is 'Reassign job to someone else', From is 'In Progress', To is 'In Progress', Transition type is 'Assign', Target role is 'GraphicArtist', Assignee hint type is 'Required', and Display order is '1'. It includes 'Ok', 'Cancel', and 'Apply' buttons at the bottom.

Figure 10-15. The Permissions tab allows you to add permissions to the new transition

6. Select the **PERMISSIONS** tab and add permissions to the transition. These permissions ensure that only users that have been granted specific permissions are able to use the transition to move the work order or job from one state to the other.
7. Click **ADD**.
The **ADD PERMISSIONS TO TRANSITION** dialog box appears (figure [10-16](#)).

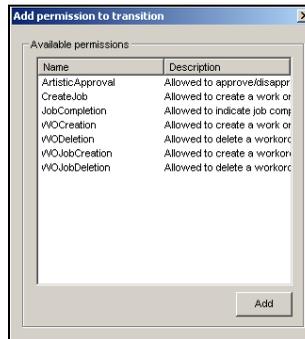


Figure 10-16. Select the permissions that are to be added to the transition

8. Select the permission(s) that will restrict the use of this transition to specific roles/users. To select multiple permissions, press the **SHIFT** key as you click on each item for consecutive selections, or press the **CTRL** key to select a grouping of non-consecutive permissions.
9. Click **ADD** and the selected permissions are added immediately to the transition's properties.
10. Click **OK**.

Editing a transition's properties and permissions

To edit an existing transition's properties and/or permissions:

1. Open the Xmedia Server Control Panel and select **TRANSITIONS** from the **WORKFLOW OPTION** drop-down list.
2. Select the transition that is to be edited from the **AVAILABLE TRANSITIONS** list.
3. Click **PROPERTIES** in the lower-left corner of the Workflow page, or double click on the transition in the **AVAILABLE TRANSITIONS** list.

The **TRANSITION PROPERTIES** dialog box appears (figure 10-17), which displays the transition's settings and permissions on the two tabs: **TRANSITION** and **PERMISSION**.

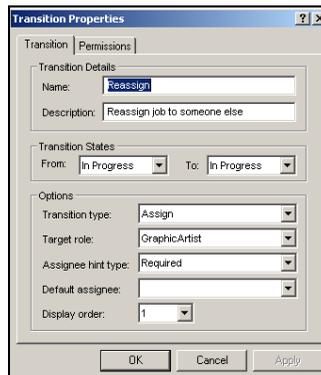


Figure 10-17. The Transition Properties dialog box

4. If necessary, edit the settings on the **TRANSITION** tab (see [“Transition tab settings” on page 10-15](#) for a description of each setting).
5. If any edits were made on the **TRANSITION** tab, click the **APPLY** button.
6. If necessary, add or remove permissions from the **PERMISSIONS** tab.
7. Click **OK** to apply the edits and close the **TRANSITION PROPERTIES** dialog box.

Deleting a transition from the workflow

Any transition can be deleted from the workflow, except those that use the **START** state. As described below, deleting a transition involves using the **REMOVE** button in the lower-right corner of the Workflow page.

To remove and delete a permission from the current workflow:

1. Open the Xmedia Server Control Panel and select **TRANSITIONS** from the **WORKFLOW OPTION** drop-down list.
2. Select the transition that is to be deleted from the **AVAILABLE TRANSITIONS** list.
3. Click **REMOVE** in the lower-right corner of the Workflow page.

The **CONFIRM DELETE** dialog box appears (figure [10-10](#)).

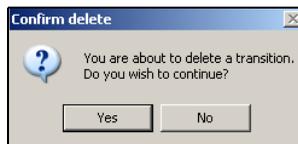


Figure 10-18. Select Yes to permanently delete the transition from the workflow

4. Click **YES** to permanently delete the transition from the current workflow. The transition is immediately removed from the **AVAILABLE TRANSITIONS** list on the Workflow page.

Workflow option: Priorities

Work orders can be assigned a priority classification to indicate the urgency of the request. In situations where several orders are pending completion, the work order's priority will suggest which should be completed immediately and which can wait.

Figure 10-19 identifies the priorities that are present in the Xmedia Server's default workflow. Although these default priorities suggest degrees of urgency, it is completely up to your organization to define the meaning and assignment of these priorities to work orders.

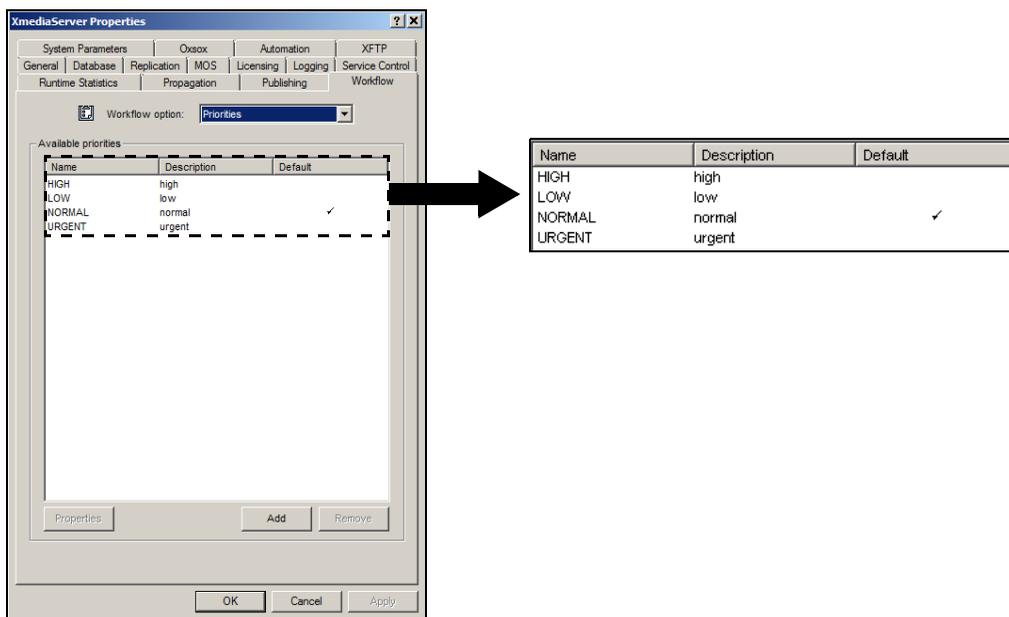


Figure 10-19. The default workflow's work order priorities

You can set a default priority for all new work order by clicking within the **DEFAULT** column of the priority that you want to become the default. This places a check-mark in the row to identify it as the default priority. A work order's priority can always be changed later in the application's Work Order window.

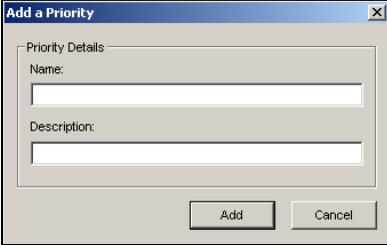
The following sections provide instructions for creating additional priorities or remove existing priority categories to meet your organization's needs:

- [“Adding a new priority to the workflow” on page 10-23](#)
- [“Deleting an existing priority from the workflow” on page 10-24](#)

Adding a new priority to the workflow

To add a new priority category to the existing workflow:

1. Open the Xmedia Server Control Panel and select **PRIORITIES** from the **WORKFLOW OPTION** drop-down list.
2. Click **ADD** in the lower-right corner of the Workflow page.
The **ADD A PRIORITY** dialog box appears (figure [10-20](#)).



The image shows a dialog box titled "Add a Priority". It has a standard Windows-style title bar with a close button (X). The main area is labeled "Priority Details" and contains two text input fields. The first field is labeled "Name:" and the second is labeled "Description:". At the bottom of the dialog, there are two buttons: "Add" and "Cancel".

Figure 10-20. Use the Add a Priority dialog box to define a new work order priority

3. Type a name for the priority in the **NAME** text box.
4. Type a brief description that identifies the purpose of the priority in the **DESCRIPTION** text box.
5. Click **ADD**.
The new priority is immediately added to the **AVAILABLE PRIORITIES** list. The new priority will also be available in the application's Work Order window's **PRIORITY** drop-down list.

Deleting an existing priority from the workflow

A priority cannot be deleted from the workflow if:

- the priority is the default priority (as indicated by the check mark in the **AVAILABLE PRIORITIES** list).
- the priority is currently being used by an existing work order

If either of these conditions is true, then the **REMOVE** button on the Workflow page's Priorities view is disabled (greyed out). However, if neither of the two conditions is true, then you can use the procedure below to delete the priority from the workflow.

To remove and delete a priority from the current workflow:

1. Open the Xmedia Server Control Panel and select **PRIORITIES** from the **WORKFLOW OPTION** drop-down list.
2. Select the priority that is to be deleted from the **AVAILABLE PRIORITIES** list.
3. Click **REMOVE** in the lower-right corner of the Workflow page.
The **CONFIRM DELETE** dialog box appears (figure [10-21](#)).

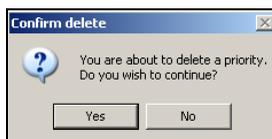


Figure 10-21. Select Yes to permanently delete the priority from the workflow

4. Click **YES** to permanently delete the priority from the current workflow.
The priority is immediately removed from the **AVAILABLE PRIORITIES** list on the Workflow page and it is no longer be available in the application's Work Order window's **PRIORITY** drop-down list.

Workflow option: Roles

There are some actions within the work order workflow, like approving a job, that you will want to restrict to a certain group of people. Rather than assigning individual permissions to each user, you can create groupings of permissions, called roles. Roles allow users to perform the tasks applicable to their job function.

For example, the two roles listed below contain permissions that are relevant to the job functions within a graphics department.

<u>Role: Graphic Artist</u> P1 - Create work order P2 - Ingest graphics	<u>Role: Art Supervisor</u> P1 - Assign staff P2 - Delete work order P3 - Approve work order P4 - Finalize work order
--	--

These roles can then be assigned to individual users who require specific permissions to perform their job functions (John and Jill). Note that roles also allow you to easily expand a user's permissions by assigning them additional roles (Jim), rather than additional permissions.

- John is a graphic artist who has been assigned the Graphic Artist role.
- Jim is a team leader who needs the permissions associated with both the Graphic Artist and Supervisor roles.
- Jill is the Art Director and she only needs the permissions associated with the Supervisor role.

The following sections provide instructions for creating new roles, removing existing roles, and editing an existing role's properties and permissions:

- [“Adding a new role to the workflow” on page 10-26](#)
- [“Editing an existing role's properties and permissions” on page 10-28](#)
- [“Deleting a role from the workflow” on page 10-29](#)

Adding a new role to the workflow

Prior to adding a new role to the workflow, we recommend that you verify that the required permissions have been added to the workflow. These permissions should grant users access to the components of the workflow that will allow them to perform their job function (see [“Workflow option: Permissions” on page 10-9](#)).

Since users can be assigned multiple roles, it may be unnecessary to add a new role to the workflow when editing an existing role might be sufficient. Therefore, we also recommend that you review the roles that already exist in the workflow before adding a new role.

To add a new role to the workflow:

1. Open the Xmedia Server Control Panel and select **ROLES** from the **WORKFLOW OPTION** drop-down list.
2. Click **ADD** in the lower-right corner of the Workflow page.
The **ADD A ROLE** dialog box appears (figure [10-22](#)).

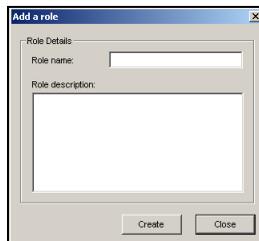


Figure 10-22. Provide a name and description for the new role

3. Type a name for the Role in the **ROLE NAME** text box. Note that roles are generally named after departments or staff positions within the organization that contribute or oversee the creation and completion of graphics requests (i.e. producer, graphic artists, art director...etc).
4. Type a brief description of the role in the **ROLE DESCRIPTION** text box.
5. Click **CREATE**.
The role is immediately added to the **AVAILABLE ROLES** list on the Workflow page.
6. Double-click on the new role's name in the **AVAILABLE ROLES** list.
The **ROLE PROPERTIES** dialog box appears (figure [10-23](#)).

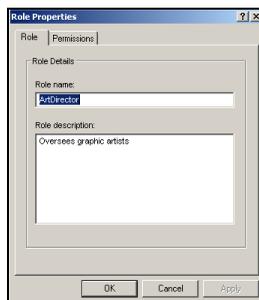


Figure 10-23. Add permissions assignment to the role using the Role Properties dialog box

7. Select the **PERMISSIONS** tab and add permissions to the role. Users with this role are granted these permissions, which allow them to perform their job functions within the workflow.
8. Click **ADD**.
The **ADD PERMISSIONS TO ROLE** dialog box appears (figure [10-24](#)).

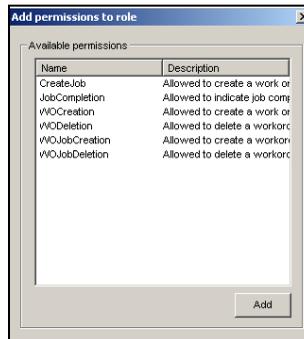


Figure 10-24. Select the permissions that are to be added to the role

9. Select the permission(s) that are to be added to the role. To select multiple permissions, press the **SHIFT** key as you click on each item for consecutive selections, or press the **CTRL** key to select a grouping of non-consecutive permissions.

NOTE

Users can be assigned one or more roles. Therefore, it is unnecessary to duplicate a specific set of permissions in one role if another role already contains the exact set of permissions.

10. Click **ADD** and the selected permissions are added immediately to the role's properties.
11. Click **OK**.

Editing an existing role's properties and permissions

To edit an existing role's properties and/or permissions:

1. Open the Xmedia Server Control Panel and select **ROLES** from the **WORKFLOW OPTION** drop-down list.
2. Select the role that is to be edited from the **AVAILABLE ROLES** list.
3. Click the **PROPERTIES** button in the lower-left corner of the Workflow page, or double click on the role in the **AVAILABLE ROLES** list.

The **ROLE PROPERTIES** dialog box appears (figure 10-25), which displays the role's settings and permissions on the two tabs: **ROLE** and **PERMISSIONS**.



Figure 10-25. The Role Properties dialog box

4. Optional: Edit the **ROLE NAME** and/or **ROLE DESCRIPTION** settings on the **ROLE** tab and then click **APPLY**.
5. Optional: Add additional permissions to the role.
 - a. Select the **PERMISSIONS** tab.
 - b. Click **ADD**.
The **ADD PERMISSIONS TO ROLE** dialog box appears
 - c. Select the permission(s) that are to be added to the role. To select multiple permissions, press the **SHIFT** key as you click on each item for consecutive selections, or press the **CTRL** key to select a grouping of non-consecutive permissions.
 - d. Click **ADD** and the selected permissions are added immediately to the role's properties.
6. Optional: Remove permissions from the role.
 - a. Select the permission(s) that are to be removed from the role. To select multiple permissions, press the **SHIFT** key as you click on each item for consecutive selections, or press the **CTRL** key to select a grouping of non-consecutive permissions.
 - b. Click **REMOVE**.
The permissions are removed immediately from the role's Permissions tab.
7. Click **OK** to apply the edits and close the **ROLE PROPERTIES** dialog box.

Deleting a role from the workflow

A role cannot be deleted from the workflow if the role is still assigned to a user or it is currently associated with a transition in the workflow. If either of these conditions is true, then the **REMOVE** button on the Workflow page's Roles view is disabled (greyed out). However, if neither of the two conditions is true, then you can use the procedure below to delete the priority from the workflow.

To remove and delete a role from the current workflow:

1. Open the Xmedia Server Control Panel and select **ROLES** from the Workflow option drop-down list.
2. Select the role that is to be deleted from the **AVAILABLE ROLES** list.
3. Click **REMOVE** in the lower-right corner of the Workflow page.
The **CONFIRM DELETE** dialog box appears (figure [10-26](#)).

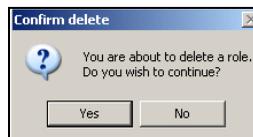


Figure 10-26. Select Yes to permanently delete the role from the workflow

4. Click **YES** to permanently delete the role from the current workflow.
The role is immediately removed from the **AVAILABLE ROLES** list on the Workflow page and it is no longer be available to be assigned to users or transitions.

Workflow option: Users

Only people with a registered user profile can participate in the work order workflow. User profiles consist of a user name and password. Each user is assigned a role (or many roles), which determines what functions the user is allowed to perform in the workflow process.

For example, figure [10-27](#) demonstrates the need for user profiles to be created to allow John, Jim, and Jill to participate in the work order workflow.

- John is a graphic artist whose user profile will be associated with the Graphic Artist role. The permissions associated with this role only grant John access to the workflow tasks and components that are relevant to his job functions.
- Jim is a team leader who needs the permissions associated with both the Graphic Artist and Supervisor roles. Therefore, both roles will be added to Jim's user profile.
- Jill is the Art Director and she only needs the permissions associated with the Supervisor role.

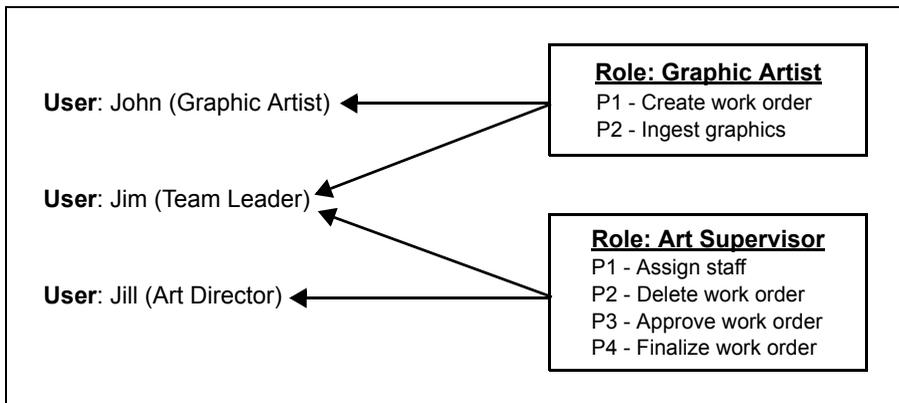


Figure 10-27. Assign roles to users so that they can perform their job functions within the workflow

The following sections provide instructions for creating new user profiles, removing existing users, and editing an existing user's properties and roles:

- ["Add a new user to the workflow" on page 10-31](#)
- ["Edit a user's workflow properties and/or roles" on page 10-33](#)
- ["Deleting a user from the workflow" on page 10-34](#)

Add a new user to the workflow

To add a new user to the workflow:

1. Open the Xmedia Server Control Panel and select **USERS** from the **WORKFLOW OPTION** drop-down list.
2. Click **ADD** in the lower-right corner of the Workflow page.
The **ADD A NEW USER** dialog box appears (figure 10-28).

Figure 10-28. Add a new user to the workflow by creating a user profile

3. Complete the **USER DETAILS** fields by typing a user name, full name, and email address for the new user.
4. Optional: Type and confirm a password for the user profile. The password adds an level of security to assure that the person using the user profile is authentic.
5. Click **CREATE**.
The User profile is immediately added to the **AVAILABLE USERS** list on the Workflow page.
6. Double-click on the new user's name in the **AVAILABLE USERS** list.
The **USER PROPERTIES** dialog box appears (figure 10-29), which features two tabs: **GENERAL** and **ROLES**. The **GENERAL** tab displays the **USER DETAILS** that you specified earlier.

Figure 10-29. The User Properties dialog box's General tab displays the User Details

7. Select the **ROLES** tab. The Roles tab displays the roles that have been assigned to the user.
8. Click **ADD**.

The **ADD ROLES TO USER** dialog box appears (figure 10-30).

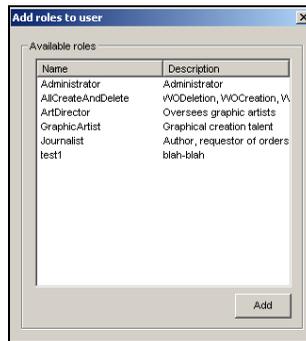


Figure 10-30. Select the roles that you want to add to the user's profile

9. Select the role(s) that are to be added to the user profile. To select multiple roles, press the **SHIFT** key as you click on each item for consecutive selections, or press the **CTRL** key to select a grouping of non-consecutive roles.
10. Click **ADD** and the selected roles are added immediately to the user's roles list.
11. Click **OK** and the **USER PROPERTIES** dialog box closes.

Edit a user's workflow properties and/or roles

To edit an existing user's properties and/or roles:

1. Open the Xmedia Server Control Panel and select **USERS** from the **WORKFLOW OPTION** drop-down list.
2. Select the user profile that is to be edited from the **AVAILABLE USERS** list.
3. Click **PROPERTIES** in the lower-left corner of the Workflow page, or double click on the user's login name in the **AVAILABLE USERS** list.

The **USER PROPERTIES** dialog box appears (figure 10-25), which displays the user's details and roles on the two tabs: **GENERAL** and **ROLES**.



Figure 10-31. The User Properties dialog box

4. Optional: Edit the **USER DETAILS** or change the password on the **GENERAL** tab and then click **APPLY**.
5. Optional: Add additional permissions to the role.
 - a. Select the **ROLES** tab.
 - b. Click **ADD**.
The **ADD ROLES TO USER** dialog box appears.
 - c. Select the role(s) that are to be added to the user profile. To select multiple roles, press the **SHIFT** key as you click on each item for consecutive selections, or press the **CTRL** key to select a grouping of non-consecutive roles.
 - d. Click **ADD** and the selected roles are added immediately to the user's role list.
6. Optional: Remove roles from the user profile.
 - a. Select the role(s) that are to be removed from the user profile's **ROLES** tab. To select multiple roles, press the **SHIFT** key as you click on each item for consecutive selections, or press the **CTRL** key to select a grouping of non-consecutive roles.
 - b. Click **REMOVE**.
The roles are removed immediately from the user's **ROLES** tab.
7. Click **OK** to apply the edits and close the **USER PROPERTIES** dialog box.

Deleting a user from the workflow

A user profile can only be deleted from the workflow if the user is not currently assigned to a job. As well, the workflow's **AVAILABLE USERS** list must always contain at least one user profile. The **REMOVE** button on the Workflow page's Users view is disabled (greyed out) when you are unable to delete a user because of the above two conditions.

To delete a user profile from the current workflow:

1. Open the Xmedia Server Control Panel and select **USERS** from the **WORKFLOW OPTION** drop-down list.
2. Select the user that is to be deleted from the **AVAILABLE USERS** list.
3. Click **REMOVE** in the lower-right corner of the Workflow page.
The **CONFIRM DELETE** dialog box appears (figure [10-32](#)).



Figure 10-32. Select Yes to permanently delete the user profile from the workflow

4. Click **YES** to permanently delete the user profile from the current workflow.

The user profile is immediately removed from the **AVAILABLE USERS** list on the Workflow page and it is no longer be available to be used in the **DEFAULT ASSIGNEE** field of the Transitions page.

Setting up E-Notifications

The Workflow page's **E-NOTIFICATIONS** workflow option (figure 10-33) allows you to configure the Xmedia Server to automatically send an email to alert specific workflow users when a job's assignee is specified, or when a work order's state has changed.

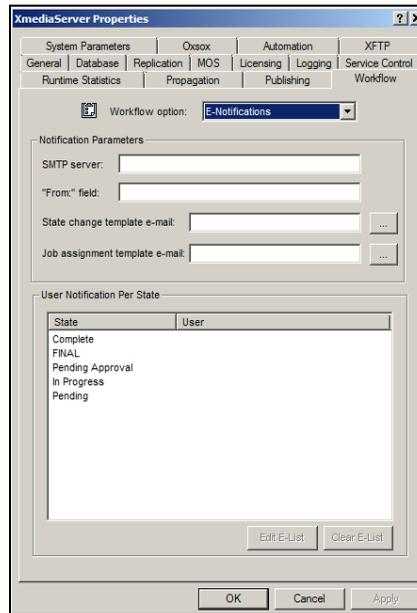


Figure 10-33. The Workflow page's E-Notifications workflow option

To configure the E-NOTIFICATIONS workflow option:

1. Create the email template files for the state change and/or job assignment notifications. See [“Setting the Notification Parameters” on page 10-37](#) for detailed instructions.
2. Set the **NOTIFICATION PARAMETERS** on the workflow's **E-NOTIFICATION** page. See [“Setting the Notification Parameters” on page 10-37](#) for detailed instructions.
3. Create an email recipient list to establish which workflow users will receive an email alert when a work order's state is changed. See [“Creating an E-List for each state change notification” on page 10-38](#) for detailed instructions.

✓ NOTE

Additional instructions for editing a state's email list (i.e. adding or removing users from the list) are provided in [“Editing a state change notification's E-List” on page 10-40](#).

Creating the email template files for E-Notifications

Prior to being able to use the e-notification system, you must first create the email template text files for the state change and job assignment notifications.

Using Notepad, you must create two (2) separate template text files and save them in a directory that is accessible to the Xmedia Server:

- StateEmailTpl.txt
- AssignEmailTpl.txt

The first line of each of the template files will be used to populate the email notification's subject line. The body of the assignment and state notification templates can use the following tokens, which are replaced by values when a transition is launched:

- %job_name
- %job_title
- %job_comments
- %wo_summary
- %wo_name
- %wo_due_dt
- %assignee_user_id
- %assignee_user_name
- %job_target_state_name

Example of a State Change Template (StateEmailTpl.txt)

```
State change!  
job_name           = %job_name  
job_title          = %job_title  
job_comments       = %job_comments  
wo_summary         = %wo_summary  
wo_name           = %wo_name  
wo_due_dt         = %wo_due_dt  
assignee_user_id   = %assignee_user_id  
assignee_user_name = %assignee_user_name  
job_target_state_name = %job_target_state_name
```

Example of a Job Assignment Template (AssignEmailTpl.txt)

```
Job Assignment!  
job_name           = %job_name  
job_title          = %job_title  
job_comments       = %job_comments  
wo_summary         = %wo_summary  
wo_name           = %wo_name  
wo_due_dt         = %wo_due_dt  
assignee_user_id   = %assignee_user_id  
assignee_user_name = %assignee_user_name  
job_target_state_name = %job_target_state_name
```

Setting the Notification Parameters

Once the assignment and state notification template text files have been created and saved, you must set the **NOTIFICATION PARAMETERS** (figure 10-34).

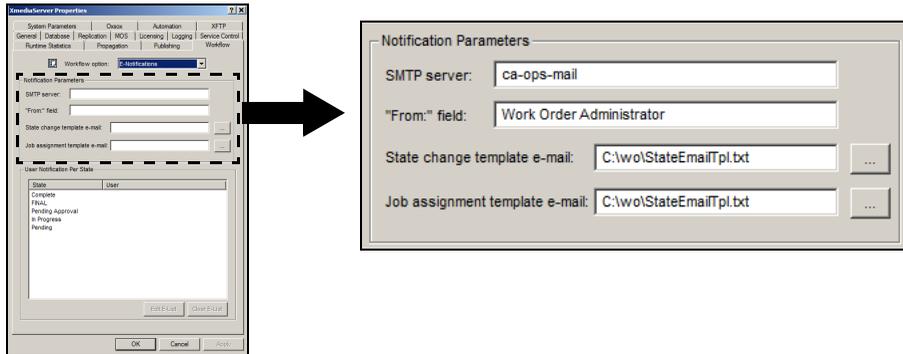


Figure 10-34. Set the Notification Parameters to configure the assignment and state E-Notifications

To set the NOTIFICATION PARAMETERS for the job assignment and state change notification:

1. In the **SMTP SERVER** field, type the hostname of the SMTP server (e.g. `ca-ops-mail`).
2. In the **"FROM:" FIELD**, type a string of text that identifies who the email notification is from. This text will appear in the **FROM** line on the notification email.
Note: The XMS Service must be restarted for the string to be applied to the emails.
3. In the **State change template e-mail** field:
 - Either type the exact directory path location of the state change template's text file.
 - Or,
 - Click the Browse button and browse for the state change template's text file.
4. In the **Job assignment template e-mail** field:
 - Either type the exact directory path location of the Job Assignment template's text file.
 - Or,
 - Click the Browse button and browse for the Job Assignment template's text file.
5. Click **APPLY** in the lower-right corner of the Xmedia Server Control Panel.

Creating an E-List for each state change notification

The **USER NOTIFICATION PER STATE** section of the **E-NOTIFICATION** workflow option page (figure 10-35) allows you to create an email recipient list (**E-LIST**) for each of the states in the workflow.

When a work order transitions to a new state, the users that are identified in the new state's E-List will receive an email alert concerning the state's transition.

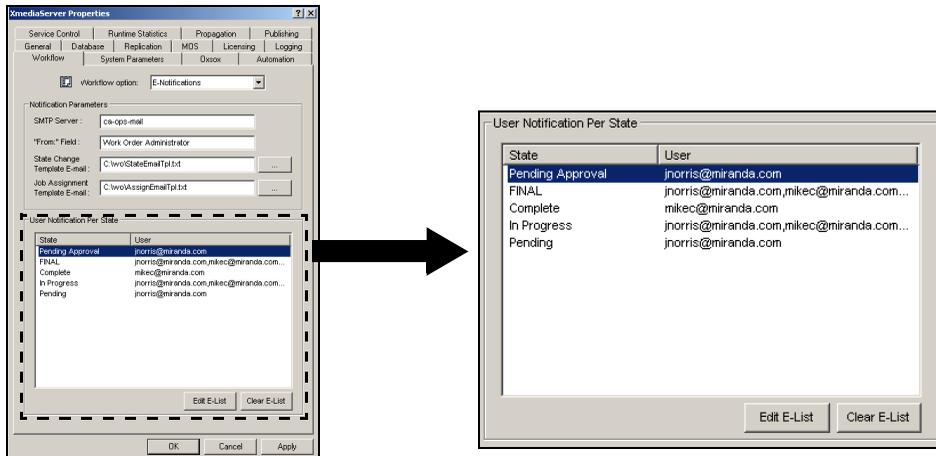


Figure 10-35. An E-List is created for each state in the workflow that lists the recipient users

NOTE

As a prerequisites to creating an E-Notification E-List, all user recipients that are to be added to the E-List must have a valid user profile in the workflow's Users workflow option, including a valid email address (see page 10-30). As well, all of the Notification Parameters must be properly set on the E-Notification page (see page 10-37).

To create an E-List for a state:

1. Double-click on a state in the **USER NOTIFICATION PER STATE** section of the E-Notification page.
The **STATE-EMAIL MAPPING** dialog box appears (figure 10-36).



Figure 10-36. The State-Email Mapping dialog box

2. Click the **MAIL LIST** button . The **LIST OF E-MAILS OF EXISTING USERS** dialog box appears (figure 10-37) and displays the email addresses of all of the users with workflow user profiles.

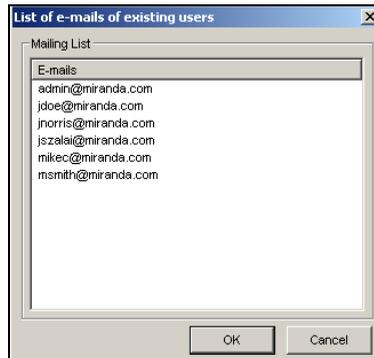


Figure 10-37. Create the E-List by selecting user email addresses

3. Select the email addresses that are to be added to state's e-notification. To select multiple email addresses, press the **SHIFT** key as you click on each item for consecutive selections, or press the **CTRL** key to select a grouping of non-consecutive addresses.
4. Click **OK** and the selected email addresses immediately populate the **To:** field in the **STATE-EMAIL MAPPING** dialog box.
5. Click **OK** and the selected email addresses are immediately displayed beside the state's name in the **USER NOTIFICATION PER STATE** section of the E-Notification page.



6. Repeat the above steps for each of the state's that require users to be notified of a work order's state change.

Editing a state change notification's E-List

The following sections provide instructions for adding or removing workflow users from a state's E-Notification email list (E-List):

- [“Adding additional users to the E-List” on page 10-40](#)
- [“Removing an individual user from the E-List” on page 10-41](#)
- [“Clearing all of the users from the E-List” on page 10-41](#)

Adding additional users to the E-List

To add additional users to a state's E-list:

1. Open the state's **STATE-EMAIL MAPPING** dialog box by either:
 - Double-clicking on a state in the **USER NOTIFICATION PER STATE** section of the E-Notification page.Or,
 - Selecting the state in the **USER NOTIFICATION PER STATE** section and then clicking the **EDIT E-LIST** button .
2. Click the **MAIL LIST** button . The **LIST OF E-MAILS OF EXISTING USERS** dialog box appears and displays the email addresses of all of the users with workflow user profiles.
3. Select the email addresses that are to be added to state's e-notification. To select multiple email addresses, press the **SHIFT** key as you click on each item for consecutive selections, or press the **CTRL** key to select a grouping of non-consecutive addresses.
4. Click **OK** and the selected email addresses immediately populate the **To:** field in the **STATE-EMAIL MAPPING** dialog box.
5. Click **OK** and the selected email addresses are immediately displayed beside the state's name in the **USER NOTIFICATION PER STATE** section of the E-Notification page.

Removing an individual user from the E-List

To remove an individual user from a state's E-list:

1. Open the state's **STATE-EMAIL MAPPING** dialog box by either:
 - Double-clicking on a state in the **USER NOTIFICATION PER STATE** section of the E-Notification page.
 Or,
 - Selecting the state in the **USER NOTIFICATION PER STATE** section and then clicking the **EDIT E-LIST** button .
2. Select the entire email address of the user that you would like to remove from the E-List, including the comma right before the first character in the address.



3. Press the **DELETE** key on your keyboard and the email address is removed.
4. Click **OK** on the **STATE-EMAIL MAPPING** dialog box to apply the edit and close the dialog box.

Clearing all of the users from the E-List

To remove all of the users from a state's E-list:

1. Select the state in the **USER NOTIFICATION PER STATE** section and click the **CLEAR E-LIST** button .

The **DELETING STATE MAILING LIST** dialog box appears (figure [10-38](#)).



Figure 10-38. Select Yes to immediately remove all of the users from the state's E-List

2. Click **YES** to immediately remove all of the current users from the state's E-List.

11 SETTING THE XMS SYSTEM PARAMETERS

The **SYSTEM PARAMETERS** page allows you to set the rate at which files are transferred (ingested) into the Xmedia Server, at what time expired published and archived assets will be purged from the target device and XMS storage respectively. You can also set the system's field rate on this page.

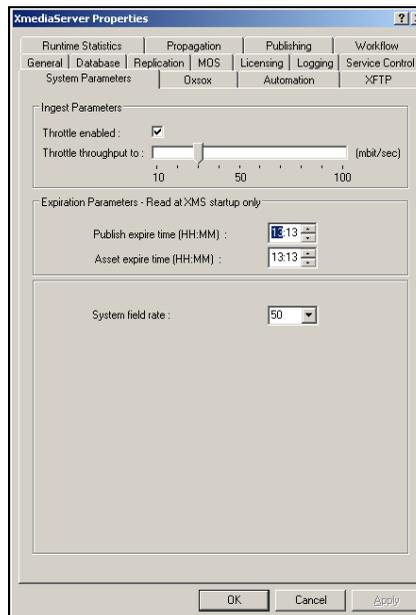


Figure 11-1. The System Parameters page

The following sections describe each of the settings on the Xmedia Server Control Panel's System Parameter page:

- [“Setting the Ingest Parameters” on page 11-2](#)
- [“Setting the Expiration Parameters” on page 11-3](#)
- [“Setting the System field rate” on page 11-4](#)

Setting the Ingest Parameters

The **INGEST PARAMETERS** on the **SYSTEM PARAMETERS** page allow you to control the rate at which any binary data is ingested into Xmedia Server during a file transfer. The use of these settings is optional and they are intended to be used in situations where the Xmedia Server is running with an Intuition XG. By lowering the ingest throttle throughput you may be able to avoid playout performance issues on the Intuition XG. The ingest throttle throughput is the rate at which binary data is ingested into the Xmedia Server. It is reported in units of megabits per second (mbits/sec).

Figure 11-2 demonstrates that you must select the **THROTTLE ENABLED** check box to activate this feature. You can then set the ingest throttle throughput by sliding the **THROTTLE THROUGHPUT TO** setting to a data rate within the range of 10 to 100 mbits/sec.

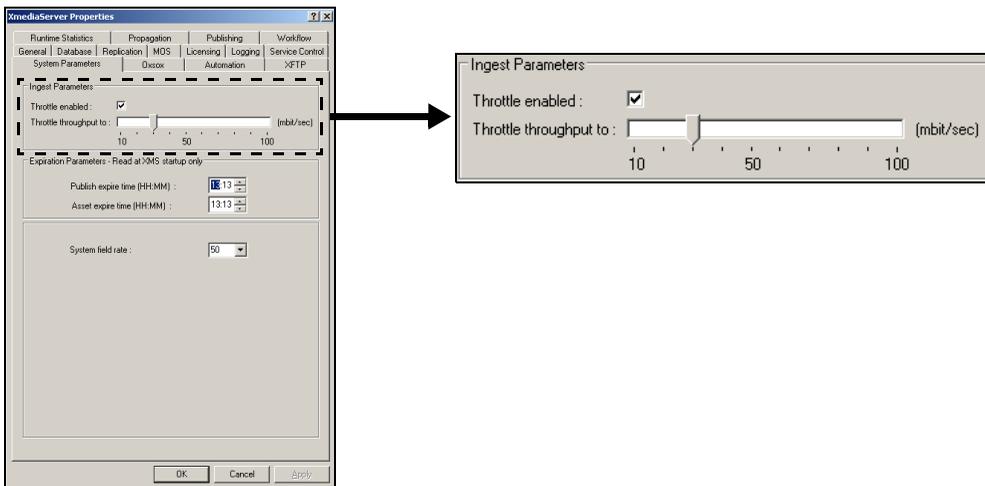


Figure 11-2. The System Parameters page's Ingest Parameters settings

Setting the Expiration Parameters

When an asset is ingested into the Xmedia Server, you have the option of setting the **EXPIRY DATE** and **PUBLISH LIFESPAN** fields in the Vertigo Suite application's **INGEST** window. These settings help to conserve storage space on the Xmedia Server and its associated playout devices by automatically deleting assets that are no longer needed.

- **EXPIRY DATE:** The date when the asset will be automatically deleted from the main Xmedia Server, secondary Xmedia Servers (hub & spoke model), as well as removing the asset from the devices that it was published to.
- **PUBLISH LIFESPAN:** This value is used by the Xmedia Server to determine how long after an asset has been published should it be removed from the playout device. The Publish Lifespan value is set in days, it has a one (1) day grace period.

Although both of these settings specify when the individual asset is to be removed from the Xmedia Server and devices, they do not specify the precise time of day when the Xmedia Server will execute the action of purging all of the expired assets.

The **EXPIRATION PARAMETERS** on the Xmedia Server Control Panel's **SYSTEM PARAMETERS** page (figure 11-3) allow you to set the precise **time** at which the Xmedia Server will execute the action of purging all expired assets. Note that these parameters are read at XMS startup only.

- **Publish expire time:** Specifies the precise time at which the Xmedia Server will purge assets that have been set to expire after they have been published. This expiry time value is set in hours and minutes (HH:MM) and the default value is 2:00 AM.
- **Asset expire time:** Specifies the precise time at which the Xmedia Server will purge expired assets that are stored in the Xmedia Server's database or on its associated devices. This expiry time value is set in hours and minutes (HH:MM) and the default value is 3:00 AM.

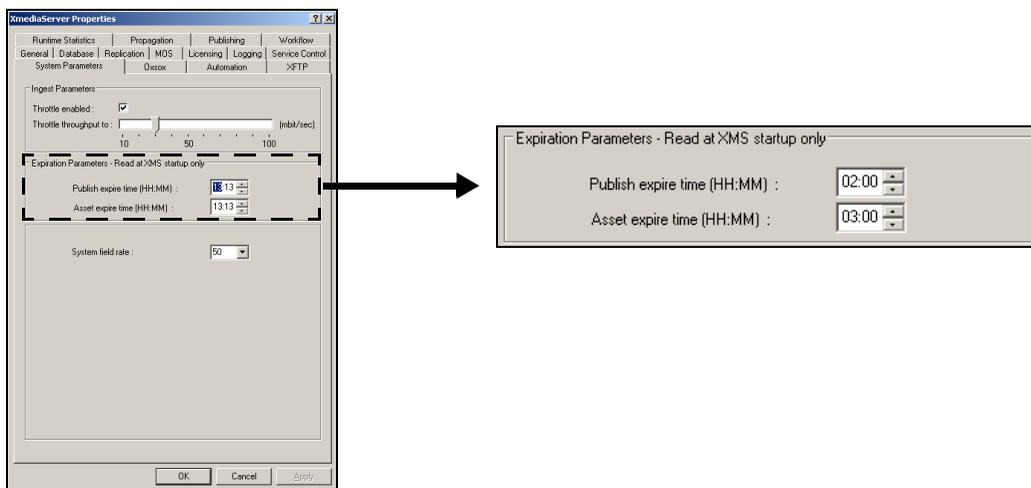


Figure 11-3. The Expiration Parameters on the Xmedia Server Control Panel's System Parameters page

Setting the System field rate

The **SYSTEM FIELD RATE** setting on the **SYSTEM PARAMETERS** page (figure 11-4) allows you to specify the frame rate at which scenes are intended to be played out. It also specifies what zone the playout is intended for. Select one of the following settings from the drop-down list:

- **50** Hertz for PAL
- **60** Hertz for NTSC

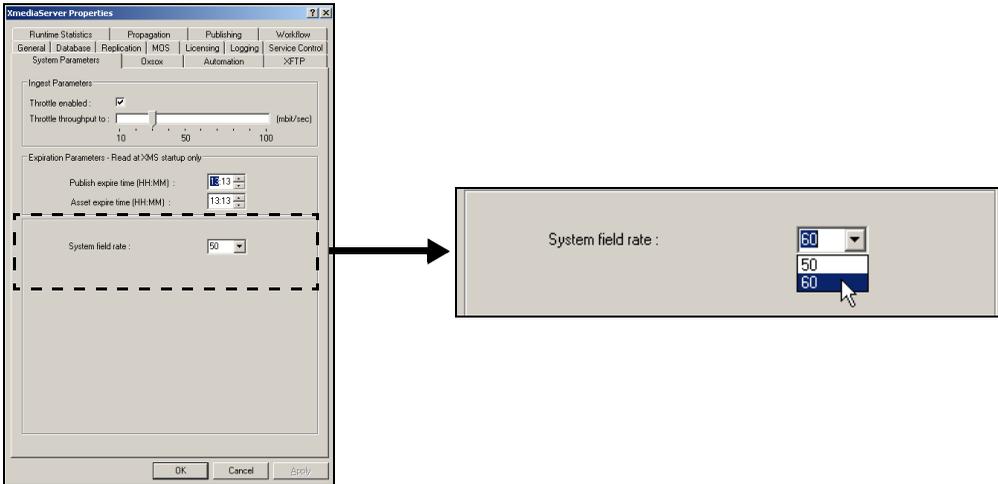


Figure 11-4. The System field rate setting

12 OxSox CONNECTION SETTINGS

Selecting the Xmedia Server Control Panel's **OxSox** tab allows you to configure the Xmedia Server to communicate with master control and automation systems using the Oxsox protocol. You can also set the logging options to record the OxSox activities to a log file.

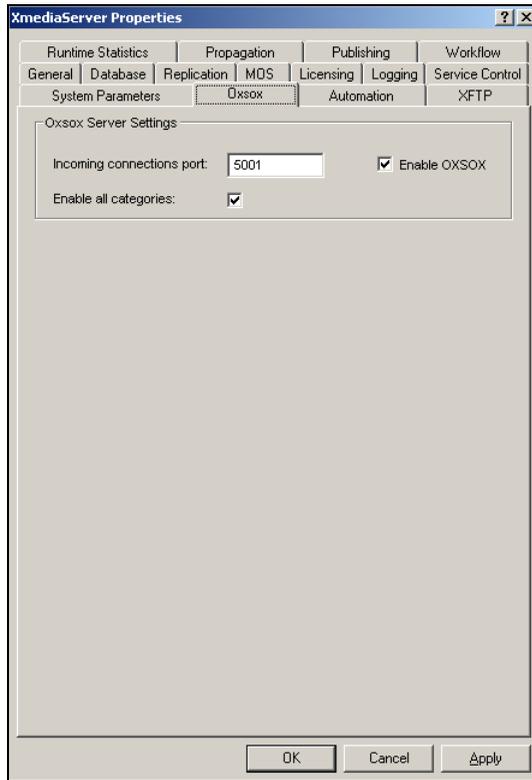


Figure 12-1. The Xmedia Server Control Panel's OxSox page

To activate the Xmedia Server's OxSox functionality:

1. Open the Xmedia Server Control Panel and select the **Oxsox** tab.
2. Select the **ENABLE OXSOX** check box.
3. Set the **INCOMING CONNECTION PORT** setting to **5001**.
This is the port that the Xmedia Server dedicates for communicating with the OxSox softwares.
4. Optional: Select the **ENABLE ALL CATEGORIES** check box.
Enabling all categories allows the Xmedia Server to reflect all of the assets in its database regardless of category as a flat list, thereby emulating the Intuition and ImageStore. When disabled, the XMS only reflects the assets stored in the asset type root categories.
5. Click **OK**.

13 THE XMS AUTOMATION PARAMETERS FOR SCHEDULED-BASED PUBLISHING

✓ NOTE

Although the Automation page still exists on the Xmedia Serve Control Panel, the functionality of scheduled-based publishing has been deprecated.

Schedule-based publishing allows media stored on the Xmedia Server (XMS) to be automatically published to and removed from playback devices based on schedules provided by automation systems.

You must use the Xmedia Server Control Panel's **AUTOMATION** page to configure the Xmedia Server to communicate with an automation system for the purposes of schedule-based publishing.

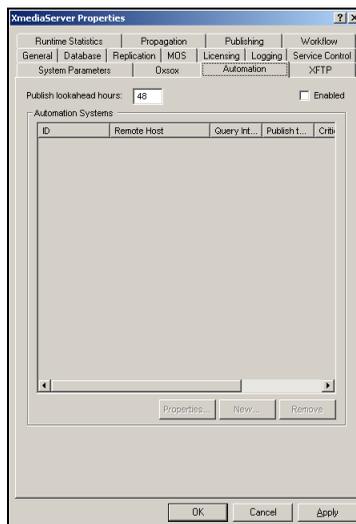


Figure 13-1. The Automation page

14 XFTP SETTINGS

NOTE

Although the **XFTP** page still exists on the Xmedia Serve Control Panel, the functionality of importing files using a FTP server running locally on the Xmedia Server has been deprecated.

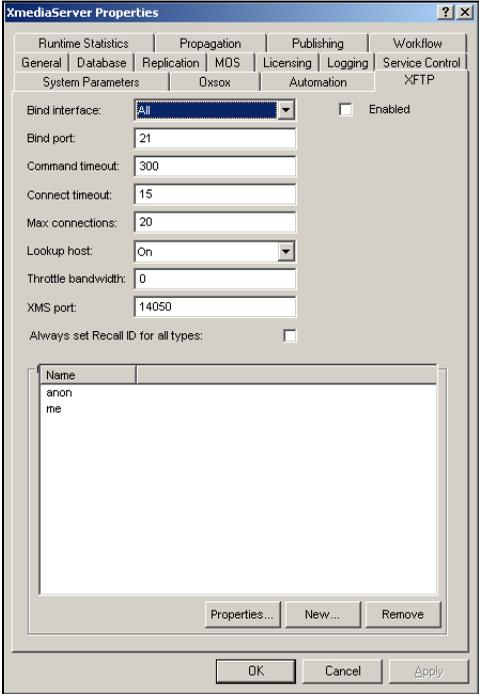


Figure 14-1. The Xmedia Server Control Panel's XFTP page

15 CONTROLLING THE XMS SERVICE

The Xmedia Server Control Panel is the user interface for the service application that controls the Xmedia Server. The service's main responsibilities are to manage the XMS's interaction with the Vertigo Suite applications and to define the configuration settings for different Xmedia system setups and uses.

In most cases, the XMS service is set to automatically launch and run in the background when the Xmedia Server is powered up. Once properly configured, you usually do not have to interact with the service or the Xmedia Server Control Panel unless you want to run diagnostic tests on the system or you want to change the configuration settings that affect the relationship between the XMS, Vertigo Suite applications, and/or Vertigo devices.

At times, the service needs to be stopped and restarted, either manually or as the result of a failure in the system. Therefore, the Xmedia Server Control Panel's **SERVICE CONTROL** page provides you with buttons and settings for stopping and restarting the XMS service.

The following sections describe how and when to use the settings on the Xmedia Server Control Panel's Service Control page:

- [“Verifying the XMS service’s status” on page 15-2](#)
- [“Stopping and starting the XMS Service” on page 15-3](#)
- [“Controlling the DataServer” on page 15-5](#)
- [“Launching the Services Management Console” on page 15-7](#)

Verifying the XMS service's status

You can quickly verify if the XMS service is running or stopped by checking the **SERVICE STATE** status displayed on the Xmedia Server Control Panel's **SERVICE CONTROL** page. Figure 15-1 and the following table identify the information on the Service Control page that allows you to quickly reference the status of the XMS Service.

Service is Running	<ul style="list-style-type: none"> Service State message: The service is running Light bulb indicator:  Service Control: STOP button is enabled
Service is Stopped	<ul style="list-style-type: none"> Service State message: The service is stopped Light bulb indicator:  Service Control: START button is enabled

The XMS service's status is displayed in the Service State and Service Control sections

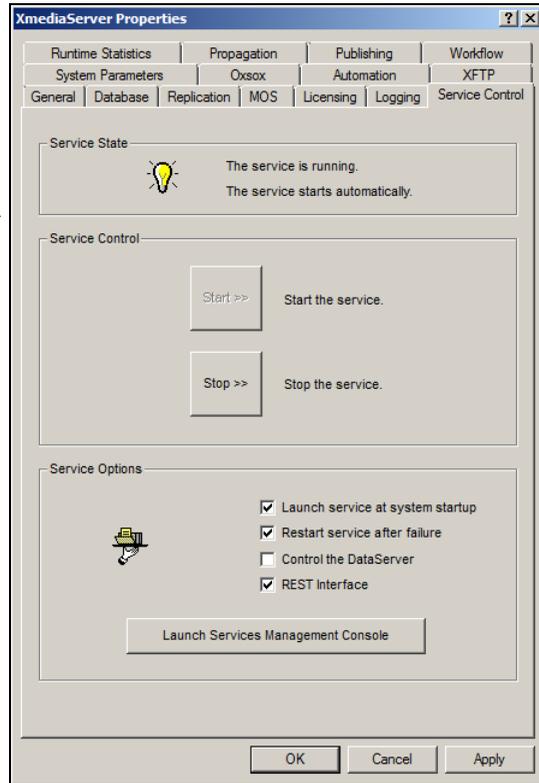


Figure 15-1. Verify the status of the XMS Service on the Service Control page

Stopping and starting the XMS Service

The **SERVICE CONTROL** page in the Xmedia Server Control Panel is equipped with buttons for manually stopping and starting the XMS service, as well as settings for automatically launching and restarting the service.

Some edits to the Xmedia Server Control Panel settings require that the XMS service be stopped and restarted manually before they can be applied to the Xmedia Server. Similarly, there are situations where the XMS service unexpectedly stops on its own and then needs to be restarted either automatically (if the settings are enabled) or manually.

The following sections describe how to stop and start the XMS service:

- [“Manually starting and stopping the XMS Service” on page 15-3](#)
- [“Automatically starting the XMS Service” on page 15-4](#)

Manually starting and stopping the XMS Service

While XMS Service’s **LAUNCH SERVICE AT SYSTEM STARTUP** parameter is usually enabled to allow the XMS service to be started automatically, there are situations where you will need to stop or start the service manually using the buttons on the Xmedia Server Control Panel’s Service Control page.

To manually stop the XMS service:

1. Open the Xmedia Server Control Panel and select the **SERVICE CONTROL** tab to display the Service Control page.
2. Press the **STOP** button in the Service Control section of the page (figure 15-2).
The Service State section displays the following message, **“THE SERVICE IS STOPPED”** and the light bulb is no longer illuminated.

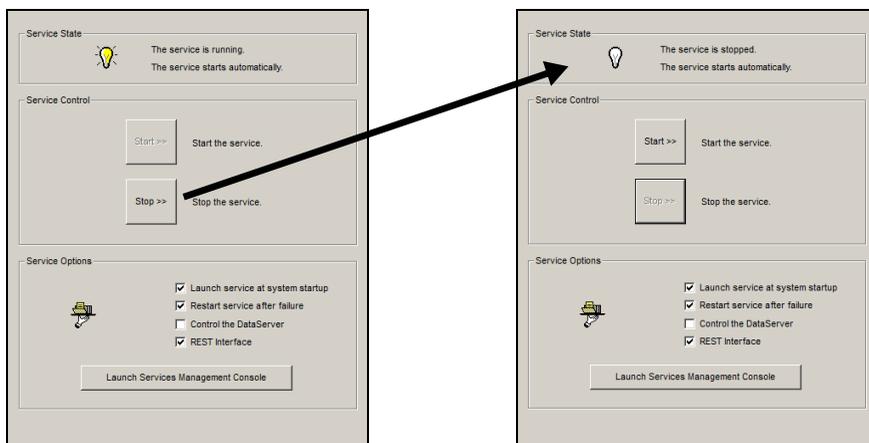


Figure 15-2. Use the **STOP** button to manually halt the operation of the XMS service

To manually start the XMS service:

1. Open the Xmedia Server Control Panel and select the **SERVICE CONTROL** tab to display the Service Control page.
2. Press the **START** button in the Service Control section of the page (figure 15-3).

The **XMEDIA SERVER SERVICE STATUS** window briefly appears and then the **SERVICE STATE** section displays the following message, “**THE SERVICE IS RUNNING**” and the light bulb becomes illuminated.

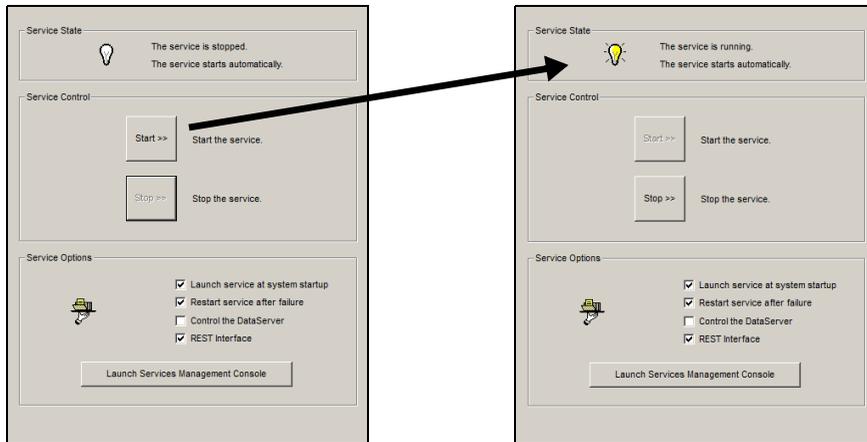


Figure 15-3. Use the **START** button to manually start the operation of the XMS service

Automatically starting the XMS Service

The Xmedia Server Control Panel provides you with two (2) settings to that enable the system to automatically start or restart the XMS service without user interaction.

When the **LAUNCH SERVICE AT SYSTEM STARTUP** setting is enabled on the **SERVICE CONTROL** page, the XMS service is automatically started each time the Xmedia Server is powered up. We recommend that this setting remain enabled to avoid having to manually start the service each time you start the Xmedia Server.

Similarly, when the **RESTART SERVICE AFTER FAILURE** setting is enabled on the **SERVICE CONTROL** page, the XMS service is automatically started when the service is accidentally stopped due to a failure with some other part of the system. We recommend that you enable this setting to avoid having to manually start the service each time another part of the system triggers a failure and stops the service.

Controlling the DataServer

The **CONTROL THE DATA SERVER** setting that appears among the **SERVICE OPTIONS** on the Xmedia Server Control Panel's Service control page (figure 15-4) must be enabled when the Xmedia Server is being configured for replication (see [page 6-1](#) for more information about replication).

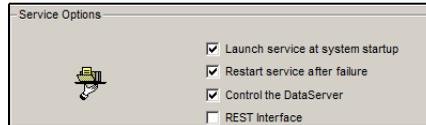


Figure 15-4. The Control the Data Server setting

NOTE

The Data Server manages data coming from various feeds, provides live updates of data values when requested and distributes the data out to the appropriate recipients.

Enabling the **CONTROL THE DATASERVER** setting ensures the Data Server remains paired with the Xmedia Server at all times in a replication environment. The objective in the replication environment is to keep the server's two components, the XMS and the Data Server, together. As a result of enabling this setting, the Xmedia Server becomes the master server to a Data Server and therefore is replicated as well.

Figure 15-5 demonstrates that once the **CONTROL THE DATA SERVER** setting is enabled, the following changes are applied to the Data Server Control Panel's **SERVICE** page:

- The manual start and stop controls are disabled
- The upper panel displays the following message: **XMEDIASERVER IS CONFIGURED TO CONTROL THE DATASERVER**
- The **SERVICE STATE** message reports that the service is **DISABLED**, rather than **START AUTOMATICALLY**

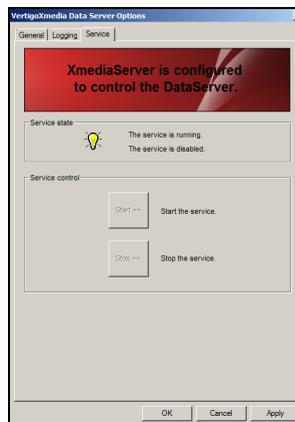


Figure 15-5. The Data Server Control Panel when the XMS is controlling the Data Server

Enabling the Xmedia Server REST Interface

Currently, the only function of the **REST INTERFACE** setting (figure [15-6](#)) is to enable the Xmedia Server to provide thumbnails of Pages and Clips that are displayed in the ENPS client application.

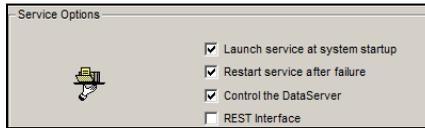


Figure 15-6. The REST Interface setting

Launching the Services Management Console

Selecting the **LAUNCH SERVICES MANAGEMENT CONSOLE** button from the **SERVICE OPTIONS** on the Xmedia Server Control Panel's Service control page opens the Windows Services Management Console (figure 15-7).

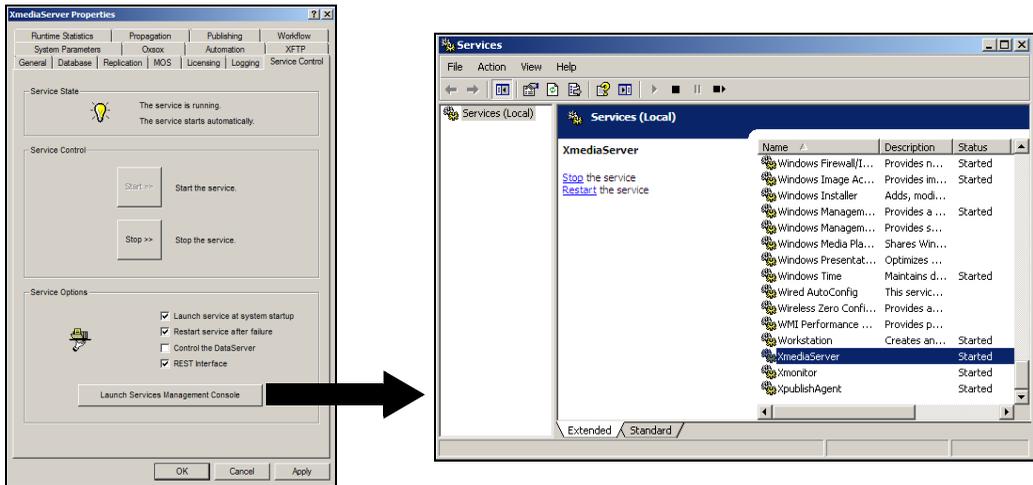


Figure 15-7. Access all of the system's services from the Microsoft Services Management Console

The Services Management Console is a Windows system administration interface that allows you to start, stop, and change configuration on services defined on the Xmedia Server. Listed among these services is the XMS Server. Double-clicking the XMS Server name in the list opens the **XMEDIA SERVER PROPERTIES** window, which provides a finer control over the service. Since the most common functionality (i.e. stopping and restarting the XMS service) is already provided on the Xmedia Server Control Panel's Service Control page, we discourage the use of this interface.

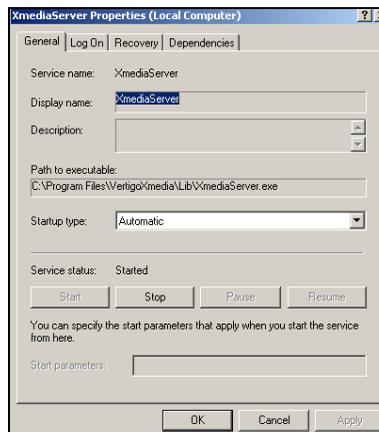


Figure 15-8. The XmediaServer Properties window is only for advanced users

16 DISPLAYING XMS RUNTIME STATISTICS

Selecting the **RUNTIME STATISTICS** tab on the Xmedia Server Control Panel displays a real-time tally of the Xmedia Server's session events and the asset content of its database. This information is useful when you have two Xmedia Servers in a replication setup ([page 6-1](#)). By comparing the Runtime Statistics counts of the various event categories, you can quickly determine if the databases on each machine are synchronized.

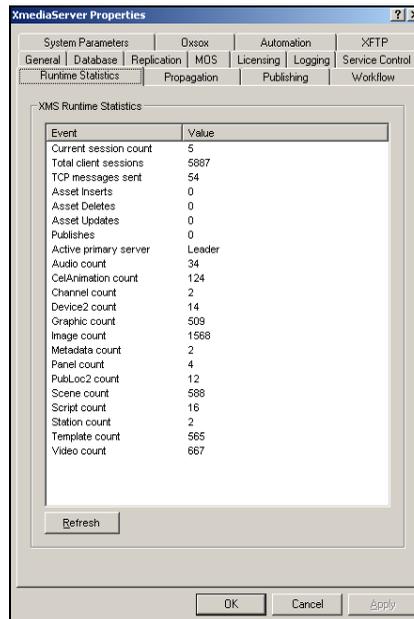


Figure 16-1. The Xmedia Server Control Panel's Runtime Statistics page

Clicking the **REFRESH** button (lower-left corner) executes a quick query for any changes to the server's events and updates the XMS Runtime Statistics list with the most current tallies.

The XMS Runtime Statistics list provides the latest tallies for the following event and asset categories:

CURRENT SESSION COUNT	The number of network connections to the server at the current moment. This event reports two (2) connections per application.
TOTAL CLIENT SESSIONS	The number of network connections the instance of this Xmedia Server has received.
TCP MESSAGES SENT	The number of back channel messages sent to all clients for the lifetime of this Xmedia Server session.
ASSET INSERTS	The number of assets that have been added to the Xmedia Server database since the beginning of the current XMS service session.
ASSET DELETES	The number of assets that have been deleted from the Xmedia Server database since the beginning of the current XMS service session.
ASSET UPDATES	The number of assets that have been edited and whose changes were saved to the Xmedia Server since the beginning of the current XMS service session.
PUBLISHES	The number of assets that have been published to devices since the beginning of the current XMS service session.
ACTIVE PRIMARY SERVER	Category heading that identifies that all of the remaining events in the XMS Runtime Statistics list are a tally of the assets belonging to the primary Xmedia Server.
AUDIO COUNT	The number of audio assets that are stored on the Xmedia Server.
BLOB COUNT	The number of generic assets that are stored on the Xmedia Server.
CEL ANIMATION COUNT	The number of cel animation assets that are stored on the Xmedia Server.
CHANNEL COUNT	MOS asset object type. A channel is an object that is made up of a number of devices each associated to a publoc2 asset.
DEVICE2 COUNT	MOS asset object type. A Device2 is a logical representation of a Vertigo XG or another driver (i.e. Lyric, Deko, etc.) to which Xplay will send Cue/Take, Set text, and Set image commands.
FONT COUNT	The number of font assets that are stored on the Xmedia Server.
GALLERY COUNT	The number of Xmedia objects that are stored on the Xmedia Server.
GRAPHIC COUNT	The number of pages that are stored on the Xmedia Server.
IMAGE COUNT	The number of image assets that are stored on the Xmedia Server.
METADATA COUNT	The number of data sources that are stored on the Xmedia Server.

PANEL COUNT	The number of panel assets that are stored on the Xmedia Server.
PLAYLIST COUNT	The number of playlist assets that are stored on the Xmedia Server.
PUBLOC2 COUNT	MOS asset object type. A Publoc2 is a logical representation of a location (i.e. hostname, drive, directory) to which clips, audio, scenes and other files are to be published.
RUNDOWN COUNT	The number of rundown assets that are stored on the Xmedia Server.
SCENE COUNT	The number of scene assets that are stored on the Xmedia Server.
SCRIPT COUNT	The number of script assets that are stored on the Xmedia Server.
SEGMENT COUNT	The number of segment assets that are stored on the Xmedia Server.
SHOW COUNT	This event has been deprecated and its value is always zero (0).
STATION COUNT	The number of station configuration assets that are stored on the Xmedia Server.
STRINGMAP COUNT	The number of lookup tables that are stored on the Xmedia Server.
TEMPLATE COUNT	The number of template assets that are stored on the Xmedia Server.
VIDEO COUNT	The number of video clip assets that are stored on the Xmedia Server.
WORKORDER COUNT	The number of work orders that are stored on the Xmedia Server.
WORKORDER_JOB COUNT	The number of work order jobs that are stored on the Xmedia Server.

17 PROPAGATING ASSETS TO OTHER XMEDIA SERVERS

Propagation is the act of accessing assets that are stored on one server and saving them onto another server. Guided by your asset distribution and sharing needs, Xmedia Servers can be configured for a simple unidirectional propagation between two servers, bidirectional propagation between two servers or a combination of both.

Figure 17-1 provides an example of a propagation configuration where assets can be copied from a propagation server (XMS 0) to one or more recipient servers by listing the recipient servers as propagation locations on the propagation server's Xmedia Server Control Panel.

Recipient servers can also be configured as propagation servers, which allows for bidirectional propagation. Again figure 17-1 demonstrates that the recipient server XMS 1 has listed the propagation server (XMS 0) as a propagation location on its Xmedia Server Control Panel. In such a configuration, when assets are propagated from the XMS 1 server to the XMS 0 server, the XMS 0 server may also propagate the assets to the other associated servers (XMS 2 & XMS 3). Internal mechanism prevent the XMS 0 server from propagating the assets back to the XMS 1 server (since they originally came from there).

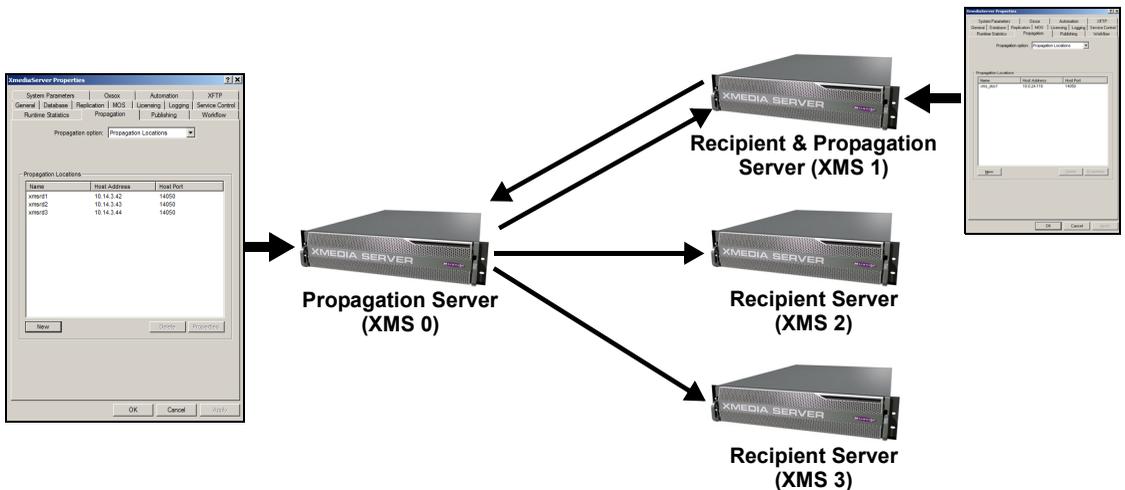


Figure 17-1. Propagating to and from various Xmedia Servers

Once propagation is configured on the propagation server's Xmedia Server Control Panel, there are two (2) methods for propagating assets to the recipient servers: **automatic propagation** and **manual propagation**.

Automatic propagation requires you designate propagable categories on the propagation server's Xmedia Server Control Panel. Once this is set up, certain events within the propagable category, like adding or editing an asset, will trigger the propagation server to automatically propagate the category's assets to the designated recipient servers.

Unlike automatic propagation, manual propagation does not require you to first set up propagable categories on the propagation server. In fact, manual propagation allows you to perform an immediate, on-demand propagation of any asset or category stored on the propagation server to a specific recipient server. However, **manual propagation can only be performed within the Vertigo Suite's Xplorer and Xstudio applications**. Unlike automatic propagation, manual propagation distributes the assets/category to the recipient server the one-time and does not update it until another manual propagation is triggered.

Whether you choose automatic or manual propagation, there are a few concepts and behaviors that you need to be aware of regarding the Xmedia Server propagation model:

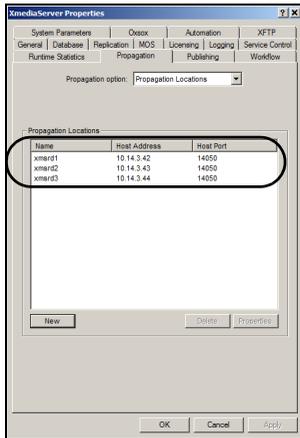
- When propagation is executed, a recipient category is created on the recipient server that is identical to the propagated category on the propagation server.
- The propagation of categories is recursive. Since categories on the propagation server can contain sub-categories, the entire contents of the parent category (i.e. sub-categories and assets) are propagated to the associated recipient servers.
- Child asset propagation is not supported. In other words, if a propagated asset contains assets that are bound to the propagated asset, only the principal asset is propagated, not the bound assets. For example, a template can be propagated to another server, but all its bound assets (i.e. the scene, images, video clips, lookup tables...etc.) will not be propagated along with the template. The template on the recipient server could potentially be incomplete. Therefore, it is very important that you correctly set up propagation to propagated all of the assets individually to avoid such a scenario.
- Deleting a propagable category on the propagation server also deletes the recipient category and its assets from the recipient server.
- The Xmedia Server's propagation model uses a mechanism called **PROPAGATION EXCEPTIONS** that allow assets and categories to be propagated to the recipient servers despite name clashes. This is accomplished by temporarily renaming the propagated asset or category and raising an exception on the recipient server, which prompts users on the recipient server to fix the problem by renaming, deleting, or moving one of its assets so that the propagated asset can use its name.
- When propagation is set up, work orders created on a recipient server are considered to be **distributed work orders** because they exist simultaneously on both the propagation server and a recipient server. To use distributed work orders, the servers must be set up in a hub and spoke configuration. See ["Propagation and distributed work orders" on page 17-14](#) for more information.

The following sections provide information and instructions for configuring and using the propagation to move assets and categories using from one Xmedia Server to others:

- [“Configuring Xmedia Servers for asset propagation” on page 17-4](#)
- [“Using automatic propagation” on page 17-6](#)
- [“Using manual propagation” on page 17-9](#)
- [“Resolving Propagation Exceptions” on page 17-10](#)
- [“Removing propagated assets from a recipient server” on page 17-13](#)
- [“Propagation and distributed work orders” on page 17-14](#)

Configuring Xmedia Servers for asset propagation

For an Xmedia Server to propagate assets to one or more recipient servers, the recipient servers' location must be defined in the **Propagation Locations** settings on the propagation server's Xmedia Server Control Panel (figure 17-2).



Propagation Server



Recipient Server

Figure 17-2. The Propagation Locations settings on a propagation server and recipient server

The following table provides examples of propagation configurations in which the Propagation Locations settings determine the relationship and direction of propagation. Note that recipient servers' Propagation Locations settings are not set unless the server is also intended to be used as a propagation server, as well as a recipient server.

Desired propagation configuration	XMS1 Propagation Locations setting(s)	XMS2 Propagation Locations setting(s)	XMS3 Propagation Locations setting(s)
Unidirectional propagation (XMS1 --> XMS2)	XMS2	----	----
Bidirectional propagation (XMS1 <--> XMS2)	XMS2	XMS1	----
Mixed (XMS1 <--> XMS2) (XMS1 --> XMS3)	XMS2 XMS3	XMS1	----

✓ NOTE

Before starting to configure the Xmedia Servers for propagation, please be sure that all servers involved can see each other on the network via their IP addresses. Also make sure that they can talk to each other via the standard XMS port (by default 14050) and the background port (14051).

Adding a recipient server's location on the propagation server:

1. Ensure that all servers involved can see each other on the network via their IP addresses. Also make sure that they can talk to each other via the standard XMS port (by default 14050) and the background port (14051).
2. Open the Xmedia Server Control Panel on the propagation server and select the **Propagation** tab.
3. In the **Propagation options** drop-down list, select **PROPAGATION LOCATIONS**.
4. Click the **NEW** button, which opens the **Add new node** window (figure [17-3](#)).

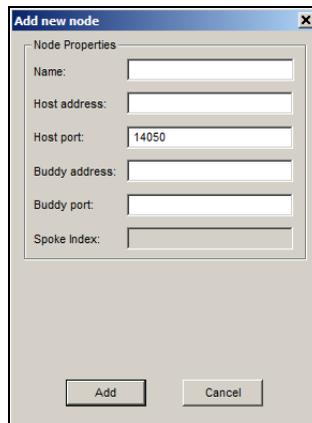


Figure 17-3. Add a new recipient server (node) to the propagation server's Propagation Locations table

5. Specify the name and IP address of the recipient server in the **NAME** and **HOST ADDRESS** fields.
6. Ensure that the **HOST PORT** field is set to the Xmedia Server's 14050 port (default).
7. Optional: If the recipient server has a backup server associated with it, specify the IP address and port of the backup server in the **BUDDY ADDRESS** and **BUDDY PORT** fields.
8. Click **ADD** to close the **Add new node** window. The recipient server is immediately added to the propagation server's Propagation Locations table.

✓ NOTE

Use the **EDIT** or **DELETE** buttons to edit the properties or delete a recipient server's propagation location from the propagation server's Propagation Locations table.

Using automatic propagation

Automatic propagation allows you setup in advance a propagation scheme in which specified categories on the propagation server are identified as “propagable” and associated to specified recipient servers. When an asset is added or the assets in the propagable categories are edited, then these assets are automatically propagated to the recipient servers without user intervention.

More specifically, automatic propagation is triggered when one of the following events occurs to or within in a propagable category on the propagation server:

- A new asset or propagable category is saved or ingested
- The contents of an existing asset or propagable category are edited
- The proxy/thumbnaill of an asset is edited
- An asset or propagable category is renamed, recategorized, or deleted
- The properties of an asset or propagable category are edited
- A proxy is deleted

Once the propagation and recipient servers are properly setup (see [page 17-4](#)), you must create propagable categories by associating categories on the propagation server with the recipient servers using the propagation server’s Xmedia Server Control Panel (figure [17-4](#)). Instructions for how to create propagable categories and recipient associations for automatic propagation are provided in [“Setting up propagable categories and recipient associations” on page 17-7](#).

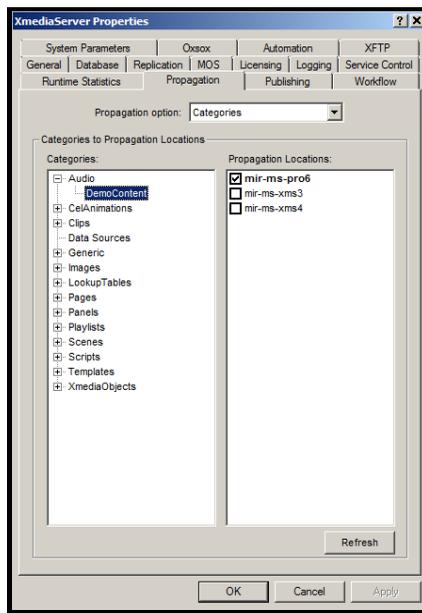


Figure 17-4. Create propagable categories on the propagation server’s Xmedia Server Control Panel

Setting up propagable categories and recipient associations

For an asset to be propagated by automatic propagation, it has to be placed in a propagable category on the propagation server. A category on a propagation server becomes propagable when it is associated with a recipient server on the Xmedia Server Control Panel's **PROPAGATION CATEGORIES** page. A category can be set to propagate its assets to a specific recipient server, a selection of recipient servers, to all of the recipient servers, or to none of the recipient servers.

A recommended propagation configuration is to have one common or global category, which propagates to all available recipient servers, and separate categories to propagate to individual recipient servers. For example, a network with three (3) stations might consider creating a **COMMON** category within the **IMAGES** root category that would be set to propagate to all three stations. Three (3) additional categories, one for each station, would also exist under the root category with each one propagating to one of the stations.

✓ NOTE

Before proceeding, we recommend that you consult [page 17-2](#) to learn more about the concepts and behaviors regarding the propagation of category assets.

To set categories on the propagation server to automatically propagate assets to the recipient servers:

1. Open the propagation server's Xmedia Server Control Panel and select the Propagation tab.
2. Select **CATEGORIES** from the **PROPAGATION OPTIONS** drop-down list.
3. Click on one of the asset categories displayed in the **CATEGORIES** column (left), which displays a list of asset categories that are stored on the propagation server. As a result, the **PROPAGATION LOCATIONS** column (right) is populated with the recipient servers that are associated with the propagation server (figure [17-5](#)).

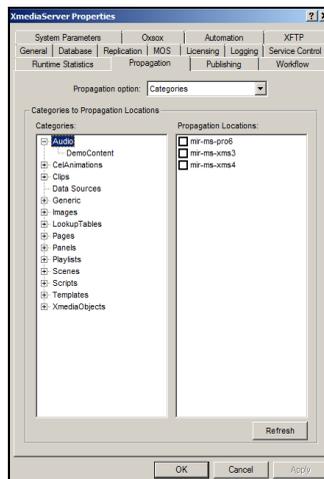


Figure 17-5. Categories to Propagation Locations

4. In the **CATEGORIES** column, expand and select the specific category that you wish to propagate.
5. In the **PROPAGATION LOCATIONS** column, select the check box for the recipient server(s) that you wish to propagate this category to (figure 17-6). You can choose to propagate to one, multiple, or no spokes.

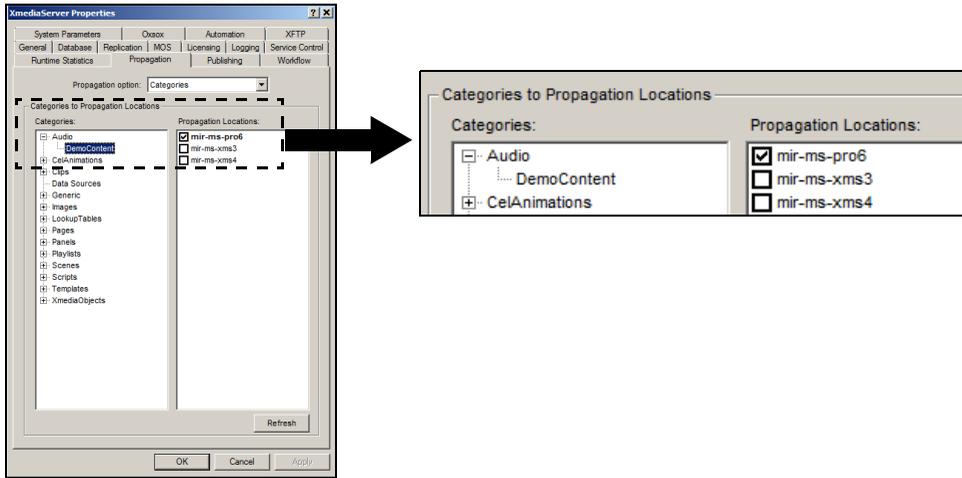


Figure 17-6. Creating propagable categories and associating them to recipient servers

6. Press **OK**.

Using manual propagation

Manual propagation allows you to perform an immediate, on-demand propagation of any category of assets stored on the propagation server to a specific recipient server. Unlike automatic propagation, manual propagation does not require you to first set up propagable categories on the propagation server. You simply use the **PROPAGATE TO** command in Xplorer or Xstudio to force the transfer of a category from the propagation server to a designated recipient server.

While automatic propagation performs an initial distribution and then maintains the recipient categories with the most up-to-date assets, manual propagation performs a one-time distribution of the category's assets to the recipient server and does not update it until another manual propagation is triggered.

✓ NOTE

Before proceeding, we recommend that you consult [page 17-2](#) to learn more about the concepts and behaviors regarding the propagation of category assets.

To perform a manual propagation of assets within a category:

1. Confirm that the propagation and recipient servers have been properly setup to allow for propagation (see [“Configuring Xmedia Servers for asset propagation” on page 17-4](#)).
2. Open one of the following Vertigo Suite applications: **XPLORER** or **XSTUDIO**
3. Ensure that Xplorer or Xstudio is connected to the propagation server (**Tools>Settings>XMS or Server**).
4. In the Asset Browser, right-click on the category that you want to propagate.
5. Select the **PROPAGATE TO** command, followed by the recipient server that will receive the recipient of the category's assets (figure [17-7](#)).

The **PUBLISH PROGRESS** window appears and displays the publication status of the assets that are being propagated to the recipient server.

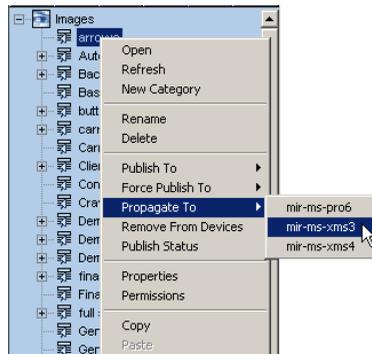


Figure 17-7. Use the Propagate To command to force a manual propagation

Resolving Propagation Exceptions

Propagation exceptions are alerts raised on a recipient server when a problem occurs during the propagation of assets. In most cases, these exceptions are triggered by a naming conflict between the propagable category or assets on the propagation server and the category on the recipient server.

In addition to alerting users of a problem, propagation exceptions allow assets and categories to be propagated to a recipient server, despite name clashes, by temporarily renaming the propagated asset or category. The exception produces a message which identifies what conditions need to be fixed for the exception to be cleared (figure 17-8). For example, the offending asset on the recipient server may need to be renamed, deleted, or moved so that the propagated asset can use its name and location. Once the user properly fixes the problem, they can clear the exception by pressing the **CLEAR** button.

Propagation exceptions always occur on a recipient server, never on the propagation server. The propagation server is merely notified that an exception occurred on one of its recipient servers. When an exception is raised, the **REFRESH LIST** button is highlighted on the recipient server's Xmedia Server Control Panel's Propagation Exceptions page. Click the **REFRESH LIST** button to update the Exception List with the most current exceptions.

The following sections describe each of the three (3) types of propagation exceptions, as well as providing instructions for how to resolve and clear these exceptions.

- [“Information Propagation Exceptions” on page 17-11](#)
- [“Category Propagation Exceptions” on page 17-11](#)
- [“Categorisation Propagation Exceptions” on page 17-12](#)

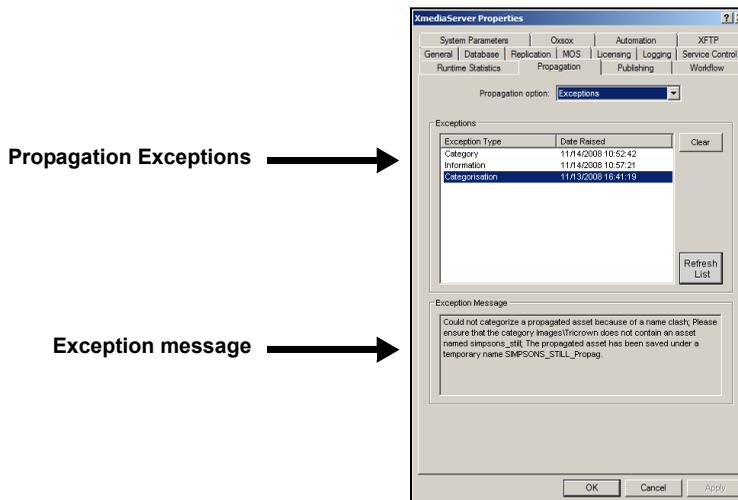


Figure 17-8. Propagations Exceptions alert users of problems that occurred during propagation

Information Propagation Exceptions

Information Propagation Exceptions identify that a problem has occurred during the propagation process, but the problem was resolved without any immediate user intervention required to proceed.

An Information Propagation Exception is raised when:

- a name clash between two categories (with the same category ID) prompts the automatic renaming and/or moving of a recipient server's category
- a propagated asset has been uncategorized by a non-propagation user session
- a propagated asset has been deleted by a user
- a propagated asset has been updated by a user session

Since Information propagation exceptions are resolved without any need for user intervention, they can easily be cleared from the Exception List using the **CLEAR** button.

Category Propagation Exceptions

Category Propagation Exceptions identify that a name clash has occurred between the propagated category on the propagation server and an existing category on the recipient server. In such a case, the categories would have different internal IDs, despite having the same name. As a result of the naming conflict, the existing category on the recipient server cannot be moved or renamed automatically, like it would have been for an Information Exception. The Category Exception still allows the category to be propagated, but the propagation category is given a temporary name on the recipient server until the name clash is resolved (figure 17-9). The propagated category is easily identifiable by its temporary name, which always ends with `_Propag`.



Figure 17-9. A category is added to the recipient server using a temporary name

The Category Propagation Exception's message suggests how to appropriately resolve the name clash. For example, **"TO CLEAR THE EXCEPTION, MAKE IT POSSIBLE FOR CATEGORY Image\Apples_Propag TO BE RENAMED TO Apples."**

Figure 17-10 demonstrates that any attempt to clear the exception will be rejected until the name conflict is resolved. Therefore to resolve the conflict, it is suggested that the category `Apples` be renamed, moved, or deleted, and then clear the Category Exception. Clearing the Category Exception triggers the system to automatically rename the `Apples_Propag` category to `Apples`.



Figure 17-10. The category name conflict must be resolved before the exception can be cleared

Categorisation Propagation Exceptions

Categorisation Propagation Exceptions are raised when a propagated asset fails to be categorized due to a name clash. Figure 17-11 demonstrates that in such a case, the propagated asset is temporarily renamed within the recipient server's category until the name conflict is resolved.

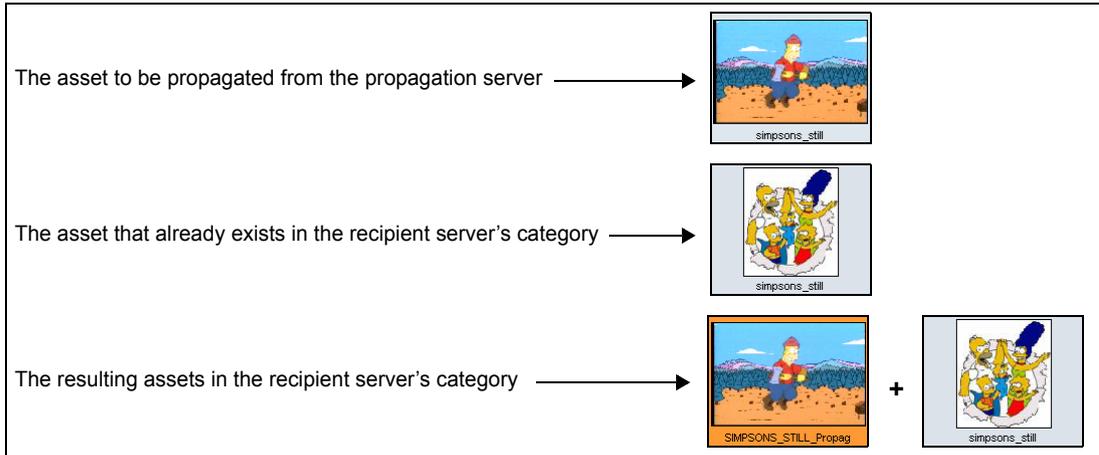


Figure 17-11. When a name conflict occurs the asset is propagated and temporarily renamed

The Categorisation Exception's message clarifies exactly what naming conflict occurred during propagation (figure 17-12). Attempting to clear the categorisation exception, without resolving the name conflict first, prompts an error message that indicates the necessary actions required before the exception can be cleared. The resolution often involves either renaming, deleting, or moving the asset that was already in the category. Once offending asset is removed/renamed, the exception can be cleared and the propagated asset is automatically renamed again.

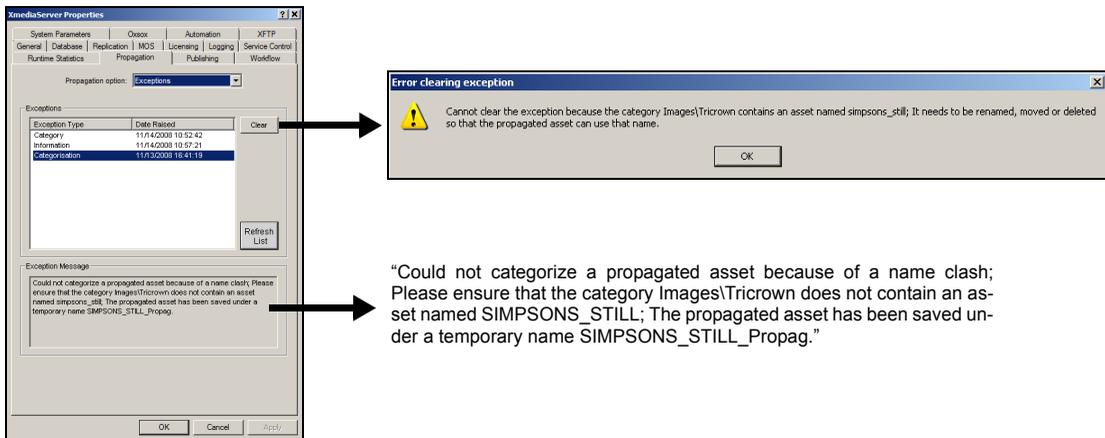


Figure 17-12. Resolve the name conflict by renaming, deleting, or moving the existing asset

Removing propagated assets from a recipient server

The propagation server is granted jurisdiction over managing the assets that are propagated onto the recipient servers. As such, the propagation server's administrator should be the one to determine which assets are present in the recipient server's categories.

Although the recipient server's applications (Xplorer and Xstudio) allow you to add, edit, and delete assets from categories configured as recipient categories, this practice is strongly discouraged. These actions may cause unintentional name conflicts, inconsistent versioning of assets, or render some assets (i.e. templates) incomplete by breaking links between assets.

Therefore, we strongly recommend that if you want to delete assets from a recipient server's category that you proceed by deleting the asset, or the asset category, from the propagation server rather than from the recipient server.

To remove an asset or an asset category from both the propagation and recipient servers:

1. Open either Xplorer or Xstudio:

`Start>Programs>VertigoXmedia>Xplorer`

Or,

`Start>Programs>VertigoXmedia>Xstudio`

2. Ensure that the application is connected to the Xmedia Server that is designated as the propagation server (**TOOLS>SETTINGS>XMS OR SERVERS**)
3. In the application's Asset Browser, navigate to the category that is to be deleted, or contains the asset(s) to be deleted.
4. Right-click on the asset or the category and select the **DELETE** command from the context menu.
The **CONFIRM DELETE** dialog box appears.
5. Click **YES** to confirm that you want to delete the asset or category.
6. The asset and/or its category is immediately deleted from the propagation server. If you chose to delete the category from the propagation server, the category will still exist on the recipient servers, but it is an empty category since all of the assets within it have been deleted.

Propagation and distributed work orders

Work orders are mechanisms within the Vertigo Suite for requesting the creation and addition of assets to the system (figure 17-13). Within a work order job, a placeholder can be created for an image or clip. A placeholder is an empty asset that serves as a temporary proxy for an image or clip that will be replaced later by completing the associated work order job (see [“Work Order workflow configuration” on page 10-1](#) for more information).

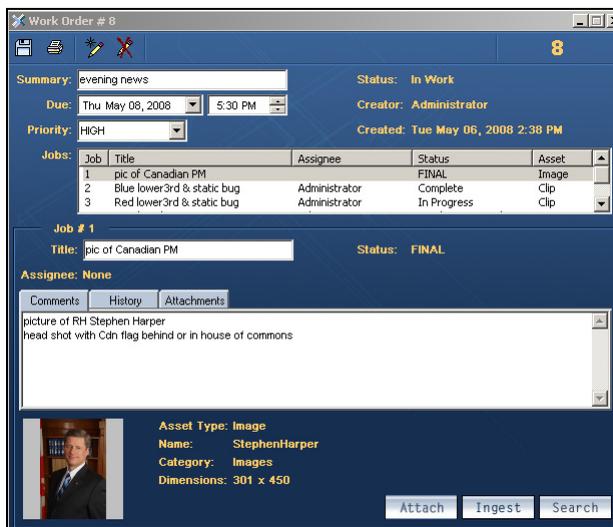


Figure 17-13. A work order is a mechanism for requesting and tracking the creation of required assets

A system that is *not* setup up for propagation, manages and stores its work orders only on the server on which it was created. When propagation is setup however, and the work order is created on a recipient server (spoke), a **distributed work order** is created and used so that the work order request exists simultaneously on both the propagation (hub) and recipient (spoke) servers allowing the hub server to fulfill the work order by propagating assets to the spoke.

The following sections provide information and instructions for setting up a hub and spoke propagation configuration for the sole purposes of using distributed work orders:

- [“Distributed work order concepts and behaviors” on page 17-15](#)
- [“Setting up a hub and spoke server for distributed work orders” on page 17-16](#)
- [“Using distributed work orders” on page 17-20](#)

Distributed work order concepts and behaviors

There are a few concepts and behaviors that you need to be aware of regarding the creation and use of distributed work orders in a hub and spoke propagation system:

- Even though distributed work orders will exist on that spoke and on the hub, they can only be created on a spoke server's Xplorer, Xbuilder, or Xnews applications.
- Work orders can be created on the hub, even if the hub server is setup for propagation. The spoke servers, however, will be unaware of these work orders. The work orders will be recognized as simple work orders (hub-only), not distributed work orders. As a result, the work order will *not* be prefixed by a spoke ID.
- Distributed work orders are always "pairwise" between a spoke and the hub. This means that work orders cannot be distributed between two spokes, or between two spokes and a hub.
- The work order workflow on both servers (hub and spoke) must be identical (see ["Setting up a hub and spoke server for distributed work orders" on page 17-16](#)).
- If a work order is created on the spoke, jobs cannot be added to the work order from the hub. The hub is only able to fulfil the distributed work order jobs, not create them.
- If a distributed work order's job undergoes a transition or is modified on a spoke, it will also transition or be modified on the hub, and vice versa.
- If an attachment is added to a distributed work order, it will be added on both servers.
- An asset that is ingested into a distributed work order on the hub will be propagated to the spoke's placeholder, once the work order is finalized.
- Placeholders are categorized on both the hub and spoke, unless the category does not already exist on the hub. In such a case, a placeholder is still categorized on the spoke, but it is *not* categorized on the hub. The placeholder category information on the hub would simply display **IMAGES** as the category.
- If a category on the hub is set to automatically propagate to the spoke associated with the distributed work order, editing the hub's category by ingesting and/or categorizing an asset, triggers a propagation to the spoke. This may result in the duplication of the asset in different categories on the spoke (one replacing the placeholder, another being the ingested asset). These assets will essentially be the same asset, only stored in two different categories. As a result, changes to one of these assets are reflected in the other. Therefore, it is advisable to ingest the asset into the same category as the placeholder.

Setting up a hub and spoke server for distributed work orders

Before using distributed work orders, the Xmedia Servers must be properly configured in a hub and spoke configuration by designating one Xmedia server as the hub server and at least one Xmedia Server as a spoke server. The following sections provide instructions for accomplishing this setup:

- [“Requirements for hub and spoke configuration” on page 17-16](#)
- [“Configuring an Xmedia Server to be a spoke propagation server” on page 17-16](#)
- [“Configuring an Xmedia Server as the hub propagation server” on page 17-17](#)

Requirements for hub and spoke configuration

Before starting to configure the Xmedia Servers for a hub and spoke propagation setup, please assure that the following requirements are met:

- Make sure all servers involved (hubs and spokes) can see each other on the network via their IP addresses. Also make sure that they can talk to each other via the standard XMS port (by default 14050) and the background port (14051).
- Avoid any potential asset conflicts by assuring that the databases on all servers involved are blank or empty prior to setting them up as a hub or spoke.

Configuring an Xmedia Server to be a spoke propagation server

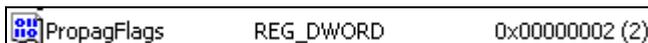
The Vertigo Suite’s hub and spoke propagation model allows hub server categories to propagate their assets to various Xmedia Servers that are designated as spoke propagation servers. To designate an XMS Server as a spoke propagation server, you must first create and set the propagation flag key in the XMS’s Registry.

To create and set the propagation flag key on a spoke server:

1. Launch the **REGISTRY EDITOR** on the Xmedia Server that is to be designated as a spoke server by typing `regedit` in the **RUN** prompt (Start>Run).
2. Navigate through the Registry Editor to the Xmedia Server’s parameter folder using the following path:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\XmediaServer\Parameters
```

3. Add a new **DWORD** value called `PropagFlags` by right-clicking in the Registry Editor’s right-panel and selecting the **NEW>DWORD VALUE** command and typing `PropagFlags` as its name.
4. Double-click the newly created `PropagFlags` registry key and the **EDIT DWORD VALUE** dialog box appears.
5. Set the **VALUE DATA** setting to **2** and then click **OK**.



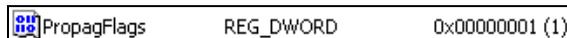
6. Open the **XMEDIA SERVER CONTROL PANEL** by selecting:
`Start>Settings>Control Panel>VertigoXmedia XmediaServer`
7. Select the **SERVICE CONTROL** tab and click the **STOP** button to stop the XMS Service.
8. Wait a couple of seconds and then click the **START** button to start the XMS Service.

Configuring an Xmedia Server as the hub propagation server

The Vertigo Suite's hub and spoke propagation model allows hub server categories to propagate their assets to various Xmedia Servers that are designated as spoke propagation servers. The instructions below describe how to designate an XMS Server as the hub propagation server by creating and setting the propagation flag key in the Xmedia Server's Registry. Then the spoke server(s) must be added to the hub server's Xmedia Server Control Panel **PROPAGATION LOCATION** page as a propagation node. We also recommend that before using distributed work orders that you override the spoke server's workflow and synchronize the user lists between the servers.

Create and set the propagation flag key on the hub server

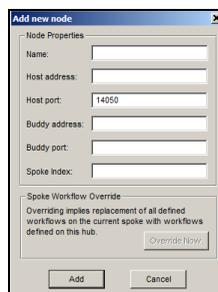
1. Launch the **REGISTRY EDITOR** on the Xmedia Server that is to be designated as the hub server by typing `regedit` in the **RUN** prompt (Start>Run).
 2. Navigate through the Registry Editor to the Xmedia Server's parameter folder using the following path:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\XmediaServer\Parameters`
 3. Add a new **DWORD** value called `PropagFlags` by right-clicking in the Registry Editor's right-panel and selecting the **NEW>DWORD VALUE** command and typing `PropagFlags` as its name.
 4. Double-click the newly created `PropagFlags` registry key and the **EDIT DWORD VALUE** dialog box appears.
 5. Set the **VALUE DATA** setting to `1` and then click **OK**.
- The resulting registry key should appear similar to the picture below.



6. On the Xmedia Server that is to be designated as the hub server, open the **XMEDIA SERVER CONTROL PANEL**.
7. Select the **SERVICE CONTROL** tab and click the **STOP** button to stop the XMS Service.
8. Wait a couple of seconds and then click the **START** button to start the XMS Service.

Add the spoke server as a propagation node on the hub server

1. Select the **PROPAGATION** tab on the Xmedia Server Control Panel.
2. In the **PROPAGATION OPTION** drop-down list, select **PROPAGATION LOCATIONS**.
3. Click the **NEW** button at the bottom of the **PROPAGATION LOCATIONS** section. The **ADD NEW NODE** window appears.

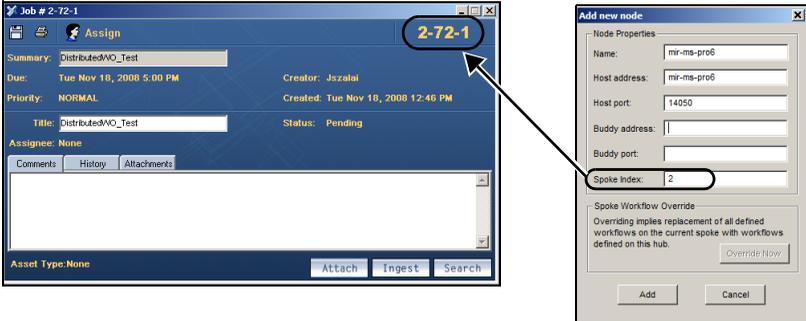


4. In the **NODE PROPERTIES** section, fill in the following text fields:

NAME	Enter an arbitrary name to identify the spoke. This does not need to be the hostname of the spoke server.
HOST ADDRESS	The IP address of the spoke server.
HOST PORT	The standard XMS port of the spoke server. By default it is set to 14050.
BUDDY PORT	(optional) The port used by the spoke's backup server if present.
BUDDY ADDRESS	(optional) The IP address of the spoke's replication backup server if present.
BUDDY PORT	(optional) The port used by the spoke's backup server if present.

SPOKE INDEX

Enter a unique integer for this spoke to allow the use of distributed work orders. The spoke-index number is used to uniquely identify the work order on both the spoke server and the hub server. For example, the job number **2-72-1** signifies: job 1 of work order 72 on spoke server index 2.



If the Spoke Index field is left empty, the work order would only be saved on the server where it was created and its job's identification number would only include the job and work order number.

5. Click **ADD** at the bottom to add this spoke server node (figure 17-14).

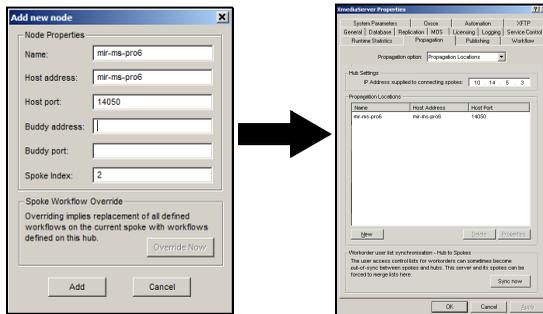


Figure 17-14. Adding a spoke server node to the hub server's Propagation Options page

Override the spoke server's workflow

For distributed work orders to function properly, the work order workflow must be identical on both the hub and spoke servers. While it is best for you to manually verify and ensure that the workflows are indeed identical, the spoke's **EDIT NODE** window on the hub server provides a **SPOKE WORKFLOW OVERRIDE** (figure 17-15). Clicking the **OVERRIDE NOW** button forces the hub's workflow onto the spoke server by overriding the spoke's existing workflow. This ensures that the workflow is identical on both servers.

The **SPOKE WORKFLOW OVERRIDE** button is disabled when the spoke server node is added (**ADD NEW NODE** window). To enable the **SPOKE WORKFLOW OVERRIDE** button and launch the command, complete the procedure for adding a new spoke node. Select the node from the **Propagation Locations** section of the Xmedia Server Control Panel's Propagation page. Click the **PROPERTIES** button to open the **Edit node** window. Click the **OVERRIDE NOW** button.

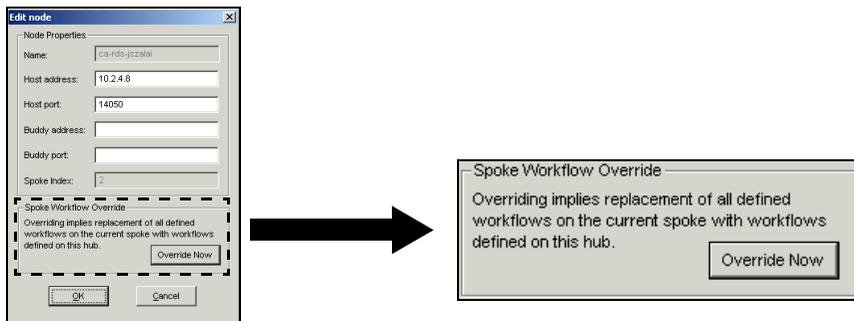


Figure 17-15. The Spoke Workflow Override ensures that the workflow is identical on both servers

Synchronize the work order user lists between the servers

Although the workflows might be identical on the hub and spoke servers, the user access lists associated to each of the workflows may be different over time as users are added, removed, or their permissions are edited. As such, a **SYNCH NOW** button is available to merge the user lists between the servers to ensure that the workflow's user lists are identical.

The hub server's **PROPAGATION LOCATIONS** page (figure 17-16) features a **SYNCH NOW** button in that merges the user list on the hub server with all of the spoke servers associated to the hub (Hub to Spokes).

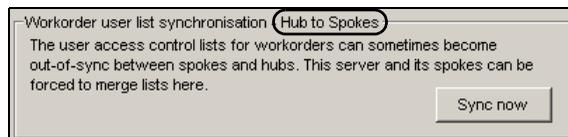


Figure 17-16. The hub server's Propagation Locations page features the Workorder Synch feature

Using distributed work orders

The following instructions describe how to generally create a distributed work order within a system configured for propagation.

1. Setup the hub and spoke servers for propagation as described on [page 17-16](#). Be sure to provide a unique number to the spoke-index property to identify the spoke server.
2. Use the **SPOKE WORKFLOW OVERRIDE** to ensure that the work order workflow on both servers (the hub and spoke) are identical (see [page 17-19](#)).
3. Optional: Use the **WORKORDER USER LIST SYNCHRONISATION** to ensure that the required user profiles are present in the hub and spoke's work order workflow (see [page 17-19](#)).
4. Using the **XBUILDER** application on the spoke server, open the template that the work order's job will apply to. Click the **CREATE NEW WORK ORDER** button  to create a new work order and job (figure [17-17](#)).

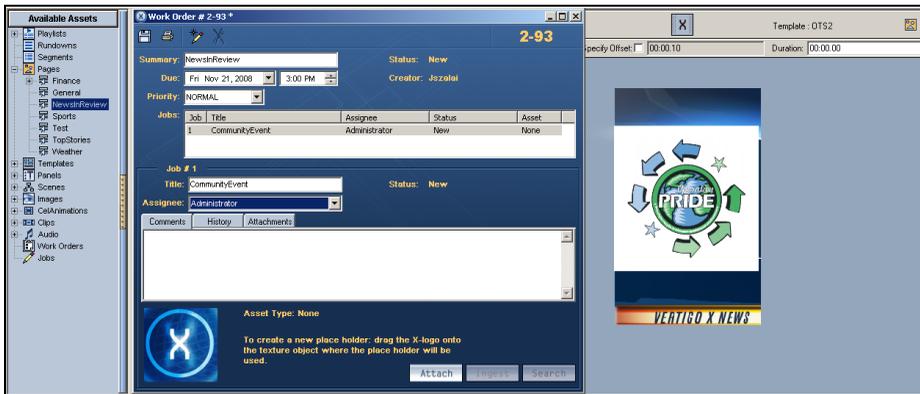
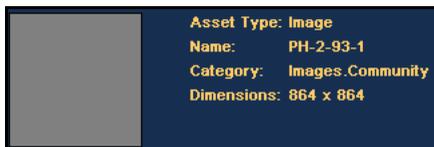


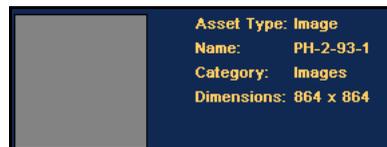
Figure 17-17. Create a work order and job, then create a placeholder

5. Create a placeholder on the spoke by dragging the x-logo icon from the work order onto the texture object on the template/page.

Placeholders are categorized on the hub and spoke. The placeholder is categorized on the spoke within the category retrieved from the **CATEGORY** property of the template's container from which the placeholder was created. If the placeholder's category already exists on the hub server, then it too is placed within this category on the hub. However, if the category does not already exist on the hub, then the placeholder information on the hub's work order lists **IMAGES** as the Category, and the placeholder is not categorized on the hub (figure [17-18](#)).



Spoke placeholder information



Hub placeholder information

Figure 17-18. Placeholder category defaults to Images when the category does not exist on the hub

6. Complete the work order and job fields, including the name of the work order, the name of the job, and the Assignee's name.
7. Save the work order.
The work order, job, and placeholders now exist on both the spoke and the hub server. They are easily identifiable by their spoke-indexed identification number (i.e. 2-93-1).
8. Open the work order or job on the hub server using **XPLORER**, **XBUILDER**, or **XNEWS**.
9. Use the **INGEST** button or the **SEARCH** button to fulfill the placeholder's image or clip request.
 - If you suspect that an asset that meets the job's criteria already exists on the system, use the **SEARCH** button to build a query and locate the asset. Once you have located the asset, selecting it links it to the job's placeholder on the both the hub and the spoke.
 - If the desired asset is not yet an asset on the hub, you must ingest the requested image/clip into the job's placeholder on the hub server. The category into which the asset will be ingested will be preselected if the category placeholder's category already exists on the hub server. If the category does not exist on the hub, then no category is preselected and you must categorize the ingested image to a category.

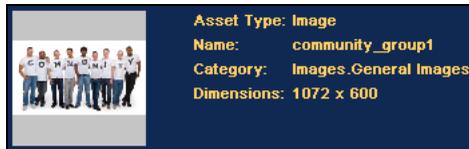


Figure 17-19. Placeholder information on the hub after being ingested

10. Save the job/work order and transition (i.e. submit) it back to the spoke.
The generic placeholders within the spoke and hub categories are updated to reflect the new image with a watermark status tag (figure [17-20](#)).

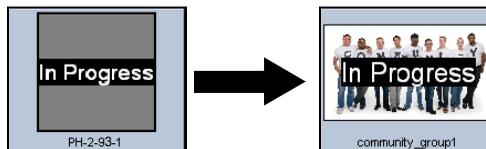


Figure 17-20. Placeholder is updated in the category

11. Open the work order/job on the spoke server and transition the job until it is finalized.
Finalizing the job replaces the placeholder in the spoke's category and on the template with the image/clip asset from the hub. As well, the placeholder on the hub is removed from its category.

✓ NOTE

In some cases, the placeholder asset from the hub is propagated to the spoke's placeholder category, as well as to another category. This results in the same asset being stored in two categories on the same spoke server. This is often the result of the placeholder asset being stored in a category other than the placeholder category on the hub, while the asset's category is also enabled for automatic propagation. Therefore, the system is executing a distributed work order finalization and an automatic propagation.

18 SETTING AND MONITORING THE XMS PUBLISHING ACTIVITIES

The Xmedia Server Control Panel's **PUBLISHING** page provides you with an interface for managing and monitoring the real-time status of items that are to be published from the Xmedia Server.

The following sections describe how to set and use the Publishing page's settings and Publish Requests monitoring system:

- [“Setting the Central XMS IP Override” on page 18-2](#)
- [“The Insta-publish device setting on the Xmedia Server Control Panel” on page 18-3](#)
- [“Monitoring and managing publish requests in the queue” on page 18-5](#)

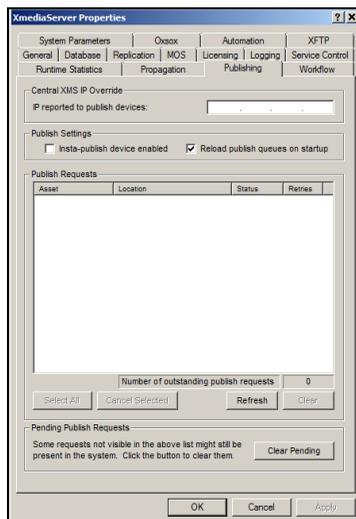


Figure 18-1. The Xmedia Server Control Panel's Publishing page

Setting the Central XMS IP Override

The Xmedia Server is often equipped with two network cards and with two IP addresses: a private IP address and a public IP address. The private IP address is only accessible from behind the firewall and it is the server main IP address for the Vertigo Suite. The public IP address is accessible from outside of the firewall and it is mainly used for propagating assets from a hub server to a spoke server (see [“Propagating assets to other Xmedia Servers”](#) on page 17-1).

When an Xmedia Server has two IP addresses, sometimes the public IP address gets picked and used rather than the private IP address. Since the public IP address is not accessible from the Embedded Xmedia Server (EXMS) running behind the firewall, communication is broken and serious publishing problems could ensue.

The **CENTRAL XMS IP OVERRIDE** section (figure 18-2) on the Publishing page aims to avoid IP confusion by definitively identifying the central Xmedia Server’s private IP address. Therefore, it is recommended that you type the private IP address of the central Xmedia Server in the **IP reported to publish devices** field.

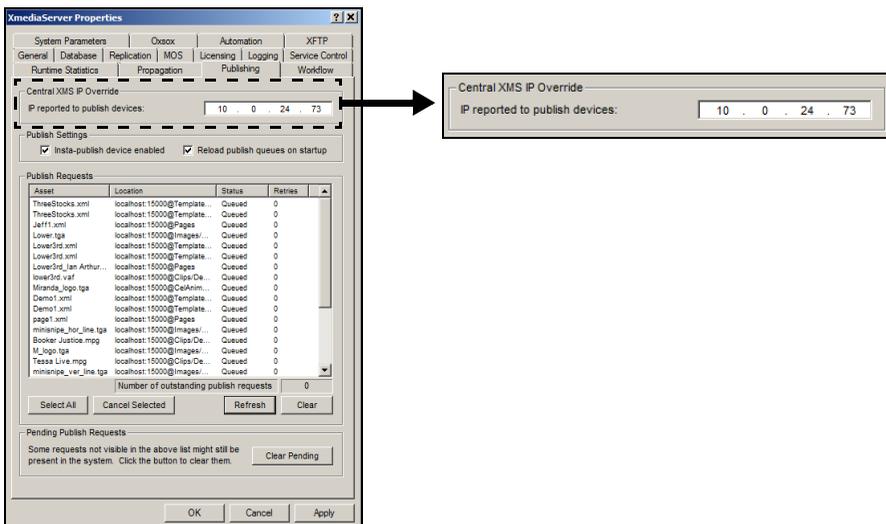


Figure 18-2. Definitively identify the private IP address of the central Xmedia Server

The Insta-publish device setting on the Xmedia Server Control Panel

Although the control panels for the Xmedia Server (Xmedia Server Control Panel) and the Embedded Xmedia Server (EXMS Control Panel) are two separate windows, many of their interface features are identical. An example of an identical feature is the **INSTA-PUBLISH DEVICE ENABLED** setting on the Publishing page (figure 18-3).

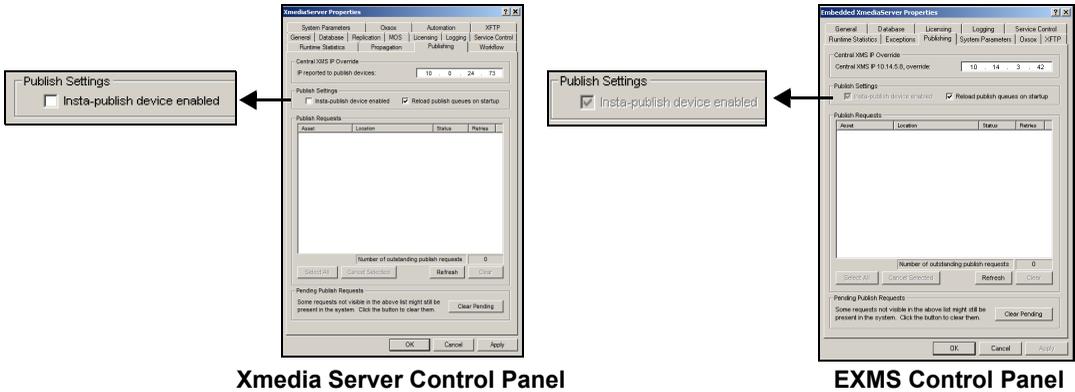


Figure 18-3. The XMS Control Panel and EXMS Control Panel both have the Insta-Publish device setting

Although the **INSTA-PUBLISH DEVICE** setting appears on the Xmedia Server Control Panel, it is not relevant to the Xmedia Server. Therefore, there is no impact on the Xmedia Server whether or not the **INSTA-PUBLISH DEVICE** setting is enabled or disabled. To be on the safe side, we recommend that the settings should always remain disabled on the Xmedia Server Control Panel.

✓ NOTE

The Insta-publish device setting's name on the Xmedia Server Control Panel may lead you to believe that you can instantly publish assets that are saved on the Xmedia Server to devices. While this particular feature does not accomplish this, the Xmedia Server does have access to an auto-publishing feature that achieves the same goal. Auto-publishing is set up in the Asset Browser of an Vertigo Suite application (i.e. Xplorer, Xstudio...etc). See "Automatically publishing assets to devices" in the **Xplorer User Manual** for more information.

Insta-publishing from the EXMS to a Localhost device

While this guide's main focus is on configuring the Xmedia Server, the following information applies only to configuring the Embedded Xmedia Server (EXMS) installed on Vertigo XG devices. A brief overview of the EXMS is provided in relation to the **INSTA-PUBLISH DEVICE ENABLED** setting.

The Embedded Xmedia Server (EXMS) allows users to continue working on the Vertigo Suite applications in the case of a network failure by replacing the application cache with an Xmedia Server (XMS service and database) situated on the same Vertigo XG device.

Figure 18-4 demonstrates that since the **INSTA-PUBLISH DEVICE ENABLED** setting on the EXMS Control Panel is always enabled, the EXMS is always ready to instantly publish all newly received assets locally to a device called **LOCALHOST**. The Localhost device is an Xpublish Agent device that publishes the EXMS assets (soft-links) to a folder on the same drive as its virtual database (VDB), so that the assets can be accessed by the XG.

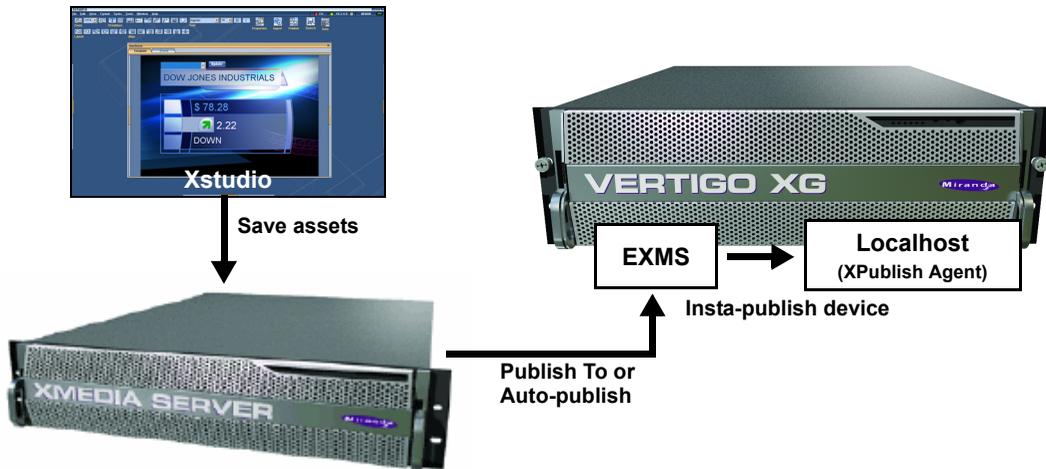


Figure 18-4. The Insta-publish setting publishes assets from the EXMS to a Localhost device

Monitoring and managing publish requests in the queue

The Publishing page's **PUBLISH REQUEST** list and its controls (figure 18-5) allow you to manage and monitor (in real-time) the items that are waiting to be published by the Xmedia Server.

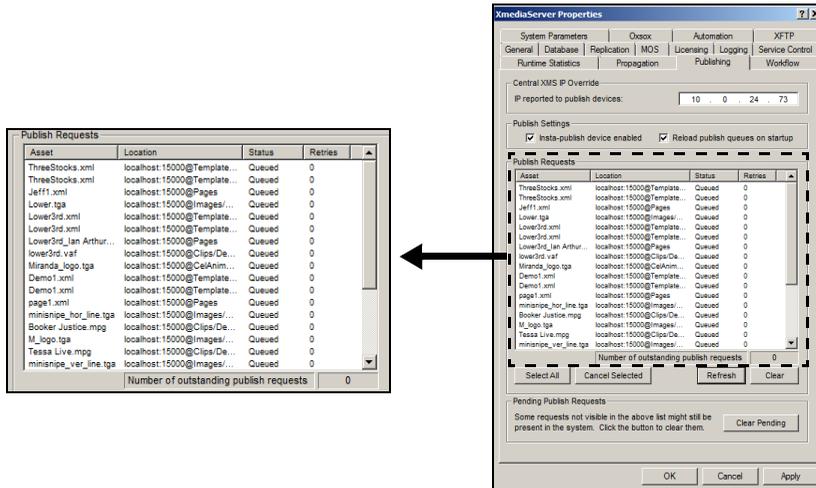


Figure 18-5. A real-time view of the Publish Requests that are in the Publish Queue

NOTE

Xplorer's **PUBLISH QUEUE MONITOR** and Xstudio's **PUBLISH PROGRESS** window offer a more comprehensive interface for monitoring the status of items that are to be published by the Xmedia Server.

The Publish Request list is automatically created when a publish request is launched by an Vertigo Suite application (i.e. Xplorer, Xstudio...etc.) and the items are waiting in the publish queue. Enabling the **RELOAD PUBLISH QUEUES ON STARTUP** setting on the Publishing page also allows the list to be populated with the current publish queue items when the XMS service is started.

Clicking the **REFRESH** button updates the list with the most current list of items in the queue. While the **NUMBER OF OUTSTANDING PUBLISH REQUESTS** field (lower portion of the pane) reports the exact number of publish requests that have not been serviced yet by the Xmedia Server. This field is updated every 5 seconds.

Each row in the Publish Request list identifies an asset that is waiting or has been published by the Xmedia Server. The following information is provided in each row:

Asset	Identifies the name of the asset.
Location	Identifies where or to which device or publish location the publish request has targeted.
Status	The status will always display Queued, which means that the asset is waiting in the queue to be published by the Xmedia Server.
Retries	The number of retries for this publish request after failure.

The following buttons, which are located below the Publish Request list, allow you to manage the Publish Request Queue by removing/cancelling some or all of the pending publish items:

Select All	Selects all of the publish requests currently displayed in the Publish Request list.
Cancel Selected	Used to cancel all of the XMS publish requests that have been selected in the list.
Refresh	Re-populates the list with the publish requests currently in the XMS.
Clear	Clears the list view without affecting the actual list of publish requests.
Clear Pending	Directly cancels and deletes any publish requests that are outstanding in the XMS.

19 USER RIGHTS MANAGEMENT

The Vertigo Suite offers system administrators and workflow managers the possibility of restricting access to some of the functionality on a per-user basis using User Rights Management (URM). **Access rights** are controlled using the Xmedia Server and the operations, tasks, and roles defined in Microsoft's Authorization Manager.

Access control is enforced through two different set of restrictions; category visibility and asset type security. The first set of restrictions determine, for any given category, which users are allowed to view the category and its contents via the Asset Browser. The second set of restrictions determine, system-wide, upon which asset types a user is granted read, write and delete access. In combining both sets of restriction, one can enforce access control on a category and asset-type basis.

A typical use of URM is to have a set of templates that are "in progress", and therefore visible only to graphics staff, but not to be used from Xnews or Xbuilder.

Use of the Vertigo Suite's URM is completely optional and it can be enabled or disabled using the Xmedia Server Control Panel's General page.

The following sections provide more details and instructions for configuring and using URM:

- ["Target audience and prerequisites for setting up URM" on page 19-2](#)
- ["Overview of the Authorization Manager" on page 19-3](#)
- ["Configuring the Policy Store in Active Directory" on page 19-8](#)
- ["Configuring the Policy Store in an XML file" on page 19-22](#)
- ["Setting up your user rights management system" on page 19-35](#)
- ["Maintaining the Authorization Manager's elements" on page 19-43](#)
- ["Restricting access to asset categories" on page 19-49](#)

Target audience and prerequisites for setting up URM

The Vertigo Suite's user rights management system is intended to be designed, set up, and used by system administrators and/or IT professionals, not the application users. As such, the target audience for this document is restricted to system administrators and IT personnel whose responsibilities grant them jurisdiction over system and network security. This document assumes that these professionals have a solid understanding and experience of Windows networking, including Windows Servers 2003, Active Directory, Windows users management, as well as the Microsoft Authorization Manager.

If information or guidance is required that goes beyond the scope of this document, we recommend that you first refer to Microsoft's user documentation to determine if the issues are Windows related. If the issues are determined to be specific to the Vertigo Suite's use of the Authorization Manager, please contact one of our Technical Support representatives (support@miranda.com).

Overview of the Authorization Manager

User rights management for Vertigo Suite applications is provided by Microsoft's Authorization Manager (often referred to as AzMan). The Authorization Manager allows for a role-based management system, which grants or restricts user access by mapping the user's login profiles to roles that are inspired by job functions.

Before using the Authorization Manager, system administrators must create and configure a Policy Store repository. The Policy Store contains the AzMan-related configuration and Vertigo Suite access restrictions. It is manipulated via a Microsoft Management Console snap-in. Through the snap-in's user interface, access to various components of the Vertigo Suite can be restricted (figure 19-1). For more information on Microsoft's AzMan, please refer to <http://technet.microsoft.com/en-us/library/cc732077.aspx>.

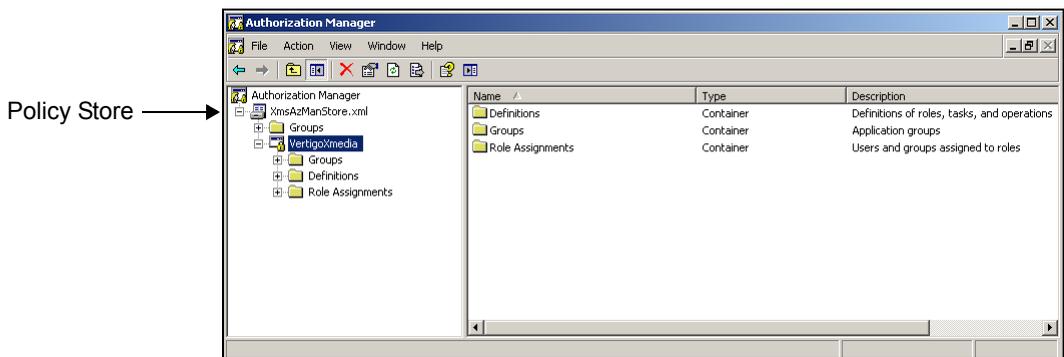


Figure 19-1. AzMan's MMC snap-in user interface used to manipulate the Policy Store

Prior to configuring the Policy Store, the type and location of the repository must be determined. The repository can be housed in two types of containers, as demonstrated in figure 19-2; an **XML FILE** or a node in an **ACTIVE DIRECTORY** installation of Windows 2003 functional level domain (see [“Configuring the Policy Store in Active Directory”](#) on page 19-8 and [“Configuring the Policy Store in an XML file”](#) on page 19-22 for more information).

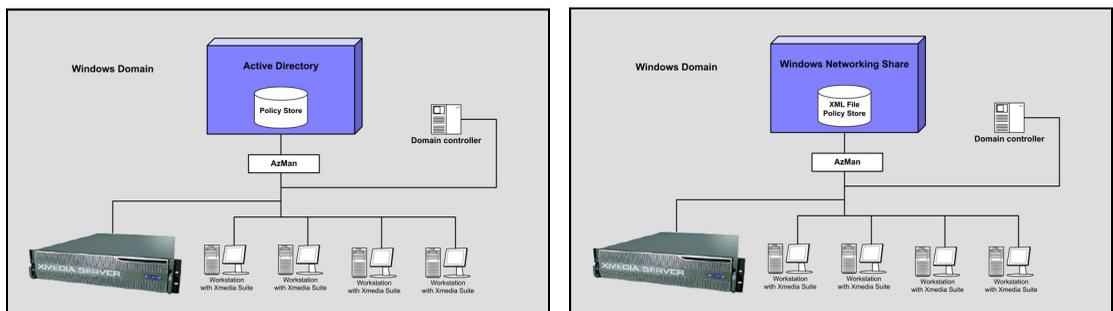


Figure 19-2. The Policy Store can be stored in Active Directory (left) or an XML file (right)

Once the Policy Store repository is created, it is populated with operations, task definitions, and role definitions, which can be assigned to Windows users and groups (figure 19-3). These are the basic building blocks of the Policy Store used by the Authorization Manager to grant or deny operations within the Vertigo Suite to your organization's users and groups.

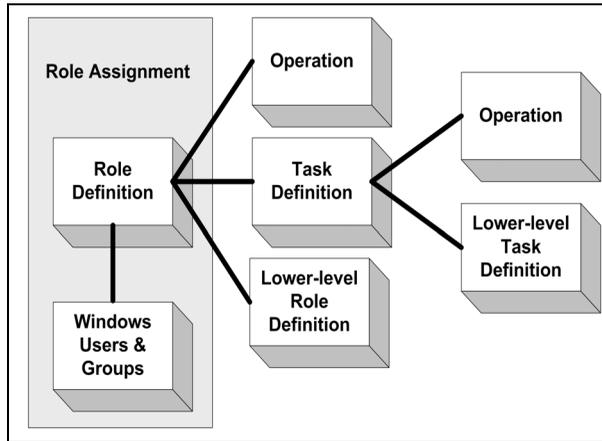


Figure 19-3. The relationship between the Policy Store elements

Figure 19-3 demonstrates the relationship between the Policy Store elements. An overview of each element is provided in the following sections:

- [“VertigoXmedia Application, operations, and task definitions” on page 19-4](#)
- [“Role definitions” on page 19-5](#)
- [“Role assignments” on page 19-5](#)
- [“Scopes” on page 19-5](#)

VertigoXmedia Application, operations, and task definitions

Operations correspond to the actions that can be undertaken in the Vertigo Suite applications, like saving or deleting an asset. The Vertigo Suite pre-defines a series of operations under the application name **VERTIGOXMEDIA** that it uses to restrict access to its various components based on the security policy defined in the Policy Store. In essence, an application is a scope or a grouping, and the VertigoXmedia application is the grouping that the Xmedia Server uses via the Authorization Manager to implement an access control list. See [“Vertigo Suite Operations” on page 19-6](#) for a list of the operation definitions included in the VertigoXmedia application.

Operation definitions are most commonly grouped into task definitions. For example, by grouping several operations together you can create a task definition that grants all of the permissions required to publish a scene. Note that task definitions can also support inheritance from other task definitions.

The following sections provide instructions for creating or editing task definitions:

- [“Creating a new task definition” on page 19-37](#)
- [“Editing task definitions” on page 19-45](#)

Role definitions

Since the authentication model is role-based, operations and task definitions are grouped together into Role Definitions. Role definitions are determined by the job functions in your organization's workflow and they essentially group together the permissions that are required for someone to perform the job function.

Figure 19-3 demonstrates that role definitions support inheritance from other role definitions. In other words, a role definition's permissions is the sum of all lower-level role permissions and its own.

The following sections provide instructions for creating or editing role definitions:

- [“Creating and populating a new role definition” on page 19-38](#)
- [“Editing role definitions” on page 19-43](#)

Role assignments

Figure 19-3 demonstrates that a role assignment associates a single role definition with the Windows users and groups that require the permissions encompassed within the role definition to perform their job functions.

The most common procedure that system administrators carry out in the user rights management models is to assign Windows users and groups to a role. The following sections provide instructions for creating or editing role assignments:

- [“Creating a new role assignment” on page 19-40](#)
- [“Adding and removing users from a role assignment” on page 19-47](#)

Scopes

Category access restrictions are catalogued using the Authorization Manager's concept of Scopes. Scopes appear as GUID-named folders under the VertigoXmedia application. They contain mappings between internal XmediaServer category identifiers (GUIDs) and the Windows users and groups that are allowed to see the category in the asset browser. They are created by the Xmedia Server and edited within the asset browser in Vertigo Suite applications. The scopes that are created in the Authorization Manager snap-in must not be modified or deleted manually. The presence of a category's identifier as a scope in the Authorization Manager means that the category has restrictions set. More information about Authorization Manager scopes is provided in [“Restricting access to asset categories” on page 19-49](#).

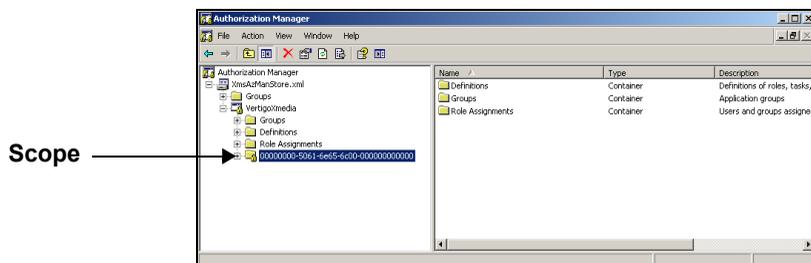


Figure 19-4. A scope is automatically added by the XMS when an asset category is restricted

Vertigo Suite Operations

The Vertigo Suite provides a set of pre-defined operations, which are used to implement a security model for the Vertigo Suite applications. Not granting a specific operation to a role is the equivalent of revoking the right to the operation. Instructions for installing these operations within the Policy Store are provided in [“Granting the domain user administrative rights to the Organizational Unit” on page 19-13.](#)

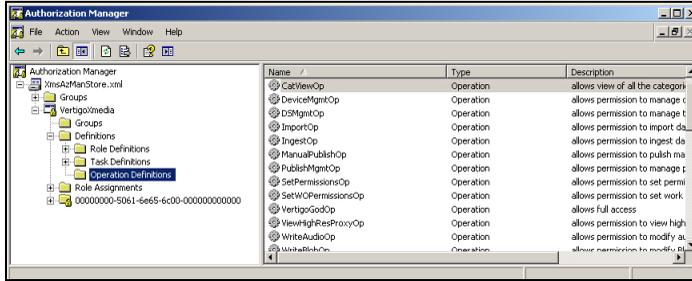


Figure 19-5. Pre-packaged VertigoXmedia operation definitions

Meanwhile, the following table lists the operations used by the Vertigo Suite:

CategoryMgmtOp	Grants permission to manage categories (deleting, renaming, etc.)
CatViewOp	Grants permission to view all of the categories
DeviceMgmtOp	Grants permission to manage devices (edit, delete, etc.)
DSMgmtOp	Grants permission to manage the data server
ImportOp	Grants permission to import assets into XMS
IngestOp	Grants permission to ingest assets into XMS
ManualPublishOp	Grants permission to publish assets manually
PublishMgmtOp	Grants permission to manage the publishing between categories and publish locations
SetPermissionsOp	Grants permission to set or disable user rights management permissions within the applications. Users with access to the Authorization Manager supersede this permission.
SetWOPermissionsOp	Grants permission to set or disable work order permissions within the applications
VertiGodOp	Supersedes all other permissions. In other words, allows full access without restrictions
ViewHighResProxyOp	Grants permission to modify view high resolution proxies. If not set, user can only view low-resolution proxies

WriteAudioOp	Grants permission to modify audio clip assets
WriteBlobOp	Grants permission to modify blobs
WriteCelAnimationOp	Grants permission to modify cel animation assets
WriteCustomObjectOp	Grants permission to modify custom objects
WriteExtraOp	Grants permission to modify extras
WriteFontOp	Grants permission to modify fonts
WriteGalleryOp	Grants permission to modify galleries
WriteGraphicOp	Grants permission to modify graphics
WriteImageOp	Grants permission to modify image assets
WriteLayoutOp	Grants permission to modify layout
WriteMetadataOp	Grants permission to modify metadata
WritePanelOp	Grants permission to modify panels
WritePlayListOp	Grants permission to modify playlists
WritePluginOp	Grants permission to modify plugins
WriteRunDownOp	Grants permission to modify rundowns
WriteSceneOp	Grants permission to modify scenes
WriteScriptOp	Grants permission to modify scripts
WriteSegmentOp	Grants permission to modify segments
WriteShowOp	Grants permission to modify shows
WriteStringMapOp	Grants permission to modify string map
WriteTaskOp	Grants permission to modify tasks
WriteTemplateOp	Grants permission to modify template assets
WriteVideoOp	Grants permission to modify video clip assets
WriteWorkOrderJobOp	Grants permission to modify work order jobs
WriteWorkOrderOp	Grants permission to modify work orders
XmsMgmtOp	Grants permission to manage the Xmedia Server using the Xmedia Server Control Panel
XPSMgmtOp	Grants permission to manage the Xpublish Agent

Configuring the Policy Store in Active Directory

Before using the Authorization Manager, system administrators must create and configure a Policy Store repository. The Policy Store contains the AzMan-related configuration and Vertigo Suite access restrictions. It is manipulated via a Microsoft Management Console snap-in. Through the snap-in's user interface, access to various components of the Vertigo Suite can be restricted.

Prior to configuring the Policy Store, the type and location of the repository must be determined. The repository can be housed in two types of containers; an **XML FILE** or a node in an **ACTIVE DIRECTORY** installation of Windows 2003 functional level domain.

The preferred repository is an Active Directory node, as it is best for multi-user environments. Nevertheless, certain situations might call for an XML repository (see [page 19-22](#)).

Choose the **ACTIVE DIRECTORY** type when:

- you are working within a Microsoft Windows 2003 network domain
- you want multiple users to access the policy store
- you want to restrict access to the policy store

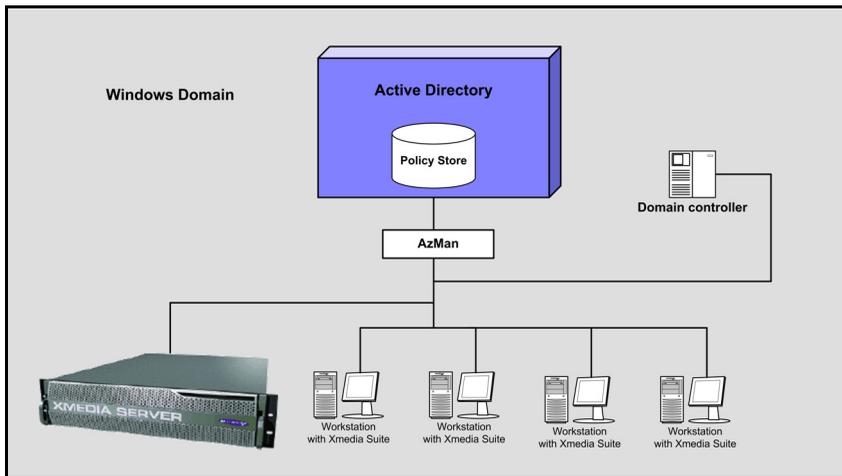


Figure 19-6. User rights management configuration with Policy Store in Active Directory

NOTE

Configuring the Policy Store in an Active Directory should only be attempted by system administrators and IT personnel whose responsibilities grant them jurisdiction over system and network security. These professionals must also possess a solid understanding and experience of Windows networking, including Windows Servers 2003, Active Directory, Windows users management, as well as the Microsoft Authorization Manager.

The procedure below identifies the high-level steps involved in creating and configuring the Authorization Manager's Policy Store in **Active Directory**. Subsequent sections (identified by the links within the procedure) provide step-by-step instructions for performing each step. Please also refer to Microsoft's documentation on user management and Active Directory Service for more information.

To configure the Authorization Manager's Policy Store in Active Directory:

Prerequisites:

The following are prerequisites for configuring the Authorization Manager's Policy Store in Active Directory. Please refer to Microsoft's documentation on user management and Active Directory Service more information.

- Create a new domain user, which will be used to grant the Xmedia Server access to the required domain resources.
- A new organizational unit named **VERTIGO** within the Active Directory to house the Policy Store.

1. Open the Microsoft Authorization Manager.
See ["Open the Authorization Manager" on page 19-10](#).
2. Assign a Policy Store within the organizational unit.
See ["Creating a new organizational unit and assigning a Policy Store" on page 19-11](#).
3. Grant the newly created domain user administrative rights to the Organizational Unit. See ["Granting the domain user administrative rights to the Organizational Unit" on page 19-13](#).
4. Open the Xmedia Server Control Panel and stop the XMS Service.
See ["Stopping the XMS Service" on page 19-14](#).
5. Change XMS service credentials to the domain user and add the domain user as an Administrator for the Xmedia Server.
See ["Adding the domain user to the Xmedia Server's security credentials" on page 19-15](#).
6. Add the domain user to the security credentials of the Policy Store. See ["Granting the domain user administrative rights to the Policy Store" on page 19-18](#).
7. Enable and set the Authorization Manager Configuration settings on the Xmedia Server Control Panel.
See ["Setting the Authorization Manager Configuration settings" on page 19-20](#).
8. Start the XMS Service in the Xmedia Server Control Panel and populate the VertigoXmedia application with the Vertigo Suite operations and roles.
See ["Starting the XMS Service to populate the VertigoXmedia application" on page 19-20](#).

NOTE

The instructions contained in this section are generic and intended to provide a very high-level information on how to create and configure the Authorization Manager's Policy Store in Active Directory. Therefore, you will likely need to modify these instructions to accommodate your specific network requirements or network configuration. Please refer to: <http://technet.microsoft.com/en-us/library/cc786774.aspx>

Open the Authorization Manager

Factory configured Xmedia Servers presently run Windows Server 2003, SP1 or later. Within Windows Server 2003, Microsoft provides the Authorization Manager snap-in. Therefore, the Authorization Manager is already installed and you can perform the instructions below to launch the AzMan snap-in.

To open the Authorization Manager snap-in:

- At the command prompt or in the Run box, type `azman.msc` and click **OK**.
Or,
- Select **START>SETTINGS>CONTROL PANEL>ADMINISTRATIVE TOOLS>AUTHORIZATION MANAGER**.

The **MICROSOFT MANAGEMENT CONSOLE** window appears, with the Authorization Manager snap-in active. The first time you open it, you'll see the message shown in (figure 19-7), which advises you that no authorization stores have been selected.



Figure 19-7. The Authorization Manager window the first time it is opened

If the Authorization Manager snap-in does not already exist on your system, you must manually add the Authorization Manager using the Microsoft Management Console. If you need further information, please refer to the Microsoft documentation:

<http://technet.microsoft.com/en-us/library/cc731573.aspx>.

Creating a new organizational unit and assigning a Policy Store

Before creating a policy store repository in Active Directory, it is recommended that you create a new Organizational Unit (OU) in the domain Program Data container within the domain-naming context (CN=Program Data residing directly in domain DC container). For information on how to create an organizational unit in an Active Directory environment, please refer the Microsoft Active Directory Service documentation.

Once the organizational unit is created, then you can create a store object in the new OU. Note that the user that will create the Policy Store in the OU must know the container name and have “Create Child Object Permission” in the container.

To assign a Policy Store within a new organizational unit:

1. Open the **AUTHORIZATION MANAGER CONSOLE** by selecting:
START>SETTINGS>CONTROL PANEL>ADMINISTRATIVE TOOLS>AUTHORIZATION MANAGER
2. Right-click on the root node (**AUTHORIZATION MANAGER**) and select the **OPTIONS** command. The **OPTIONS** dialog box appears.



Figure 19-8. The Options dialog box allows you to select the Authorization Manager mode

3. Select **DEVELOPER MODE** and click **OK**.
4. Open the Authorization Manager window (see [page 19-10](#)). Then, right-click the Authorization Manager node in the left column and select the **NEW AUTHORIZATION STORE** command.

The **NEW AUTHORIZATION STORE** dialog box appears (figure [19-9](#)).

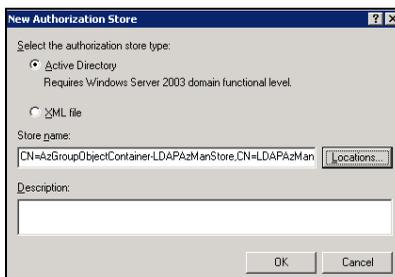


Figure 19-9. New Authorization Store

5. Enable the **ACTIVE DIRECTORY** setting (radio button).
6. Type in the **STORE NAME** field the policy store's LDAP name. For example:
`CN=LDAPAzMAnStore,OU=Vertigo,DC=<yourDomain>`
This specifies the Policy Store Name as Program Data.
7. Optional - Type a description of the new authorization store in the **DESCRIPTION** text box.
8. Click **OK**.
9. Return to the Authorization Manager Console by selecting:
START>SETTINGS>CONTROL PANEL>ADMINISTRATIVE TOOLS>AUTHORIZATION MANAGER
10. Right-click on the newly created Policy Store and select the **NEW APPLICATION** command.
11. Enter **VERTIGOXMEDIA** as the **APPLICATION NAME** and **VERTIGO SUITE POLICY STORE** as the **DESCRIPTION**.
12. Click **OK**.

Granting the domain user administrative rights to the Organizational Unit

Delegate administrative control of the organizational unit to the newly created domain user.

If you need further information, please refer to the Microsoft Active Directory documentation:
<http://technet.microsoft.com/en-us/library/cc778807.aspx>

To grant the domain user administrative rights to the Vertigo organizational unit:

1. Open the **AUTHORIZATION MANAGER CONSOLE** by selecting:
START>SETTINGS>CONTROL PANEL>ADMINISTRATIVE TOOLS>AUTHORIZATION MANAGER
2. Right-click on the **VERTIGO** organizational unit and select the **PROPERTIES** command.
 The **PROPERTIES** dialog box appears (figure [19-10](#)).

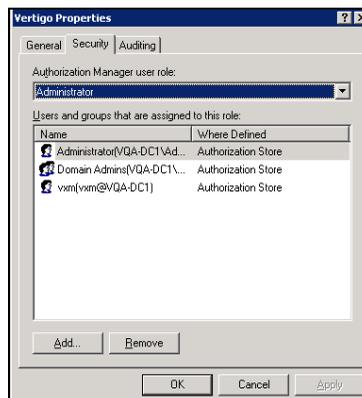


Figure 19-10. The Vertigo organization unit's Properties dialog box

3. Select **ADMINISTRATOR** from the **AUTHORIZATION MANAGER USER ROLE** drop-down list.
4. Click the **ADD** button and the **SELECT USERS, COMPUTERS, OR GROUPS** dialog box appears (figure [19-11](#)).

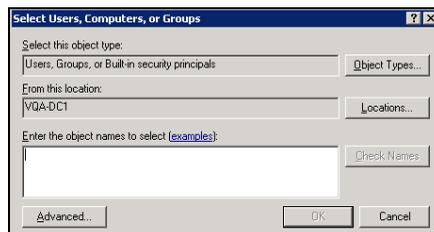


Figure 19-11. Specify the domain user's name to grant them administrative privileges

5. Type the Domain user's login name in the text box and click **OK**. The **SELECT USERS, COMPUTERS, OR GROUPS** dialog box closes and the user's name now appears in the **PROPERTIES** dialog box.
6. Click **OK**.

Stopping the XMS Service

The next few steps in the configuration procedure involve making and applying changes to the XMS Service settings. For these changes to take effect, you must first open the Xmedia Server Control Panel and stop the XMS Service. Later, these new settings will be applied to the Xmedia Server when it is restarted.

To open the Xmedia Server Control Panel and stop the XMS Service:

1. Open the **XMEDIA SERVER CONTROL PANEL** by selecting:
START>SETTINGS>CONTROL PANEL>VERTIGOXMEDIA XMEDIA SERVER
2. Select the **SERVICE CONTROL** tab on the **XMEDIA SERVER CONTROL PANEL** (figure [19-12](#)).

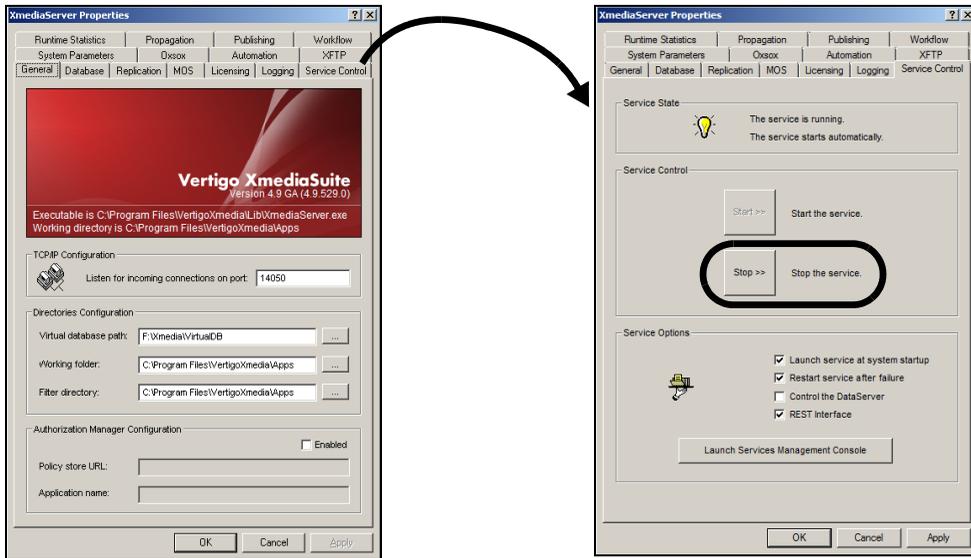


Figure 19-12. Accessing the XMS Service controls on the Xmedia Server Control Panel

3. Click the **STOP** button to stop the XMS Service.

Adding the domain user to the Xmedia Server's security credentials

A direct consequence of the use of user rights management is that the Xmedia Server and the VxDataServer services must run under a security context other than LocalSystemAccount. In fact, they both need to be running inside the security context of a domain user.

With the XMS Service now stopped, you can delegate administrative privileges to the domain user on the Xmedia Server machine.

To grant the domain user administrative privileges to the Xmedia Server:

1. Start and log into the Xmedia Server as an Administrator user.
2. Add the newly created domain user as an administrator to the XMS machine.
 - a. Right-click the **MY COMPUTER** icon on the Xmedia Server's desktop and select the **MANAGE** command.
The **COMPUTER MANAGEMENT** window appears (figure 19-13).

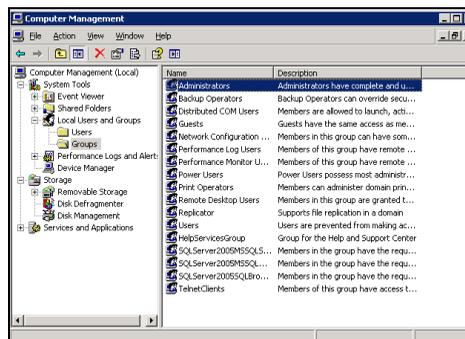


Figure 19-13. The Xmedia Server's Computer Management window

- b. Select **LOCAL USERS AND GROUPS>GROUPS>ADMINISTRATORS**.
The **ADMINISTRATORS PROPERTIES** dialog box appears (figure 19-14).

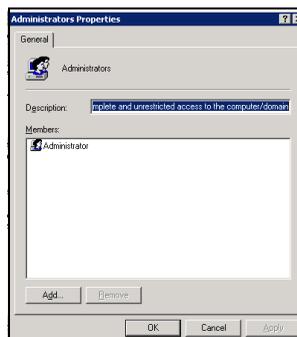


Figure 19-14. The Xmedia Server's Administrators Properties dialog box

- c. Press the **ADD** button.
The **SELECT USERS** dialog box appears (figure [19-15](#)).

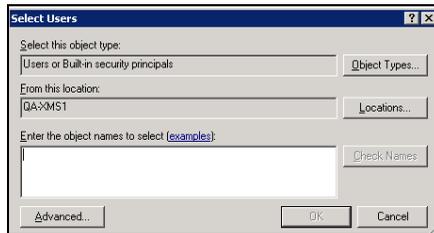


Figure 19-15. The Select Users dialog box

- d. Type the Domain user's login name in the text box and click **OK**.
The **SELECT USERS** dialog box closes and the user's name now appears in the **ADMINISTRATORS PROPERTIES** dialog box.
- e. Click **OK**.
3. Return to the Control Panel (**START>SETTINGS>CONTROL PANEL**) and open the Microsoft **SERVICES** console by selecting **ADMINISTRATIVE TOOLS>SERVICES**.
4. Navigate down the list of services to the **XMEDIA SERVER** service. Right-click on the Xmedia Server Service and select **PROPERTIES**. The **XMEDIA SERVER PROPERTIES** dialog box appears (figure [19-16](#)).

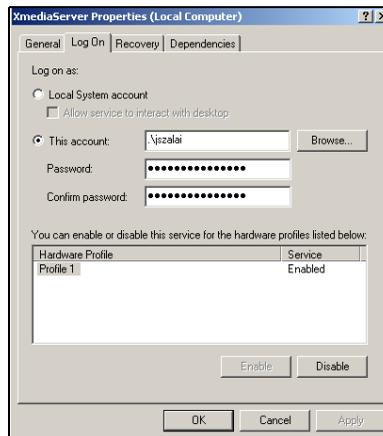


Figure 19-16. The XmediaServer Properties dialog box

5. Select the **LOG ON** tab and change the Log On as assignment from the local system account to the newly created domain account.
 - a. Press the **BROWSE** button. The **SELECT USER** dialog box appears (figure [19-17](#)).

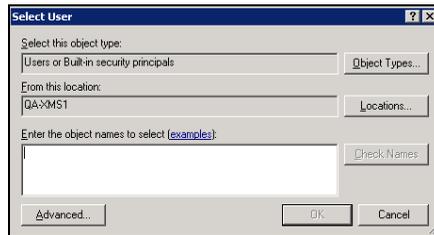


Figure 19-17. The Select User dialog box

- b. Type the domain user's name in the text box and press **OK**.
 - c. Press **OK** on the **XMEDIASERVER PROPERTIES** dialog box to close it.
 6. Close the **SERVICES** console and the **ADMINISTRATIVE TOOLS** windows.

Granting the domain user administrative rights to the Policy Store

Delegate administrative control of the Policy Store to the newly created domain user.

To edit the Policy Store's security credentials:

1. Open the Authorization Manager by selecting:
START MENU>PROGRAMS>ADMINISTRATIVE TOOLS>AUTHORIZATION MANAGER
2. Right-click on the **LDAPAZMANSTORE** policy store and select the **PROPERTIES** command (figure [19-18](#)).

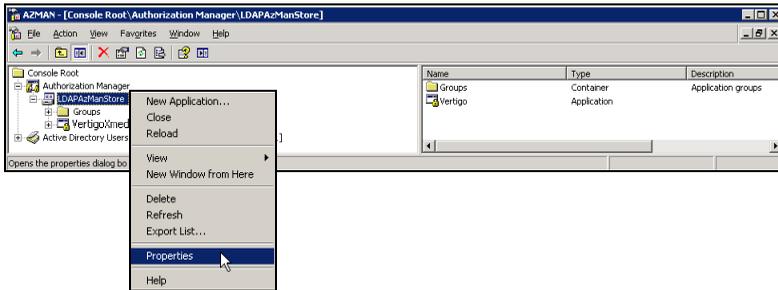


Figure 19-18. Open the Properties for the XmsAzManStore.xml policy store

3. Select the **SECURITY** tab on the policy store's **PROPERTIES** dialog box (figure [19-19](#)). If it is not already displayed, set the Authorization Manager user role field to Administrator.

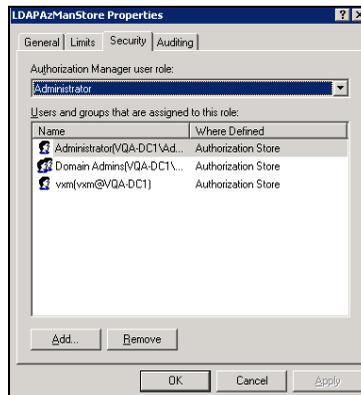


Figure 19-19. Select the Security tab on the policy store's Properties dialog box

- Click the **ADD** button and the **SELECT USERS, COMPUTERS, OR GROUPS** dialog box appears (figure [19-20](#)).

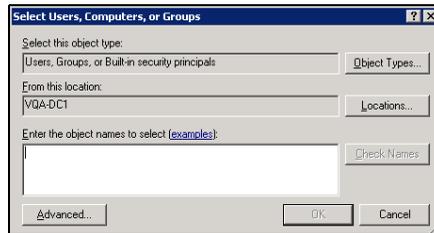


Figure 19-20. Specify the domain user's name to grant them administrative privileges

- Type the Domain user's login name in the text box and click **OK**. The **SELECT USERS, COMPUTERS, OR GROUPS** dialog box closes and the user's name now appears in the **PROPERTIES** dialog box.
- Click **OK**.

Setting the Authorization Manager Configuration settings

The Xmedia Server Control Panel's **AUTHORIZATION MANAGER CONFIGURATION** settings must be set to enable user rights management in the Vertigo Suite, providing the location of the policy store and the name of the application to be used.

To set the AUTHORIZATION MANAGER CONFIGURATION settings:

1. Open the **XMEDIA SERVER CONTROL PANEL** by selecting:
START>SETTINGS>CONTROL PANEL>VERTIGOXMEDIA XMEDIA SERVER



Figure 19-21. Authorization Manager Configuration settings on the Xmedia Server Control Panel

2. Select the **ENABLED** check box in the Authorization Manager Configuration section of the **GENERAL** page (figure 19-21).
3. Set the **POLICY STORE URL** field. Since the Store's repository is saved in the Active Directory, use a path in the following form to refer to the repository:
`msldap://CN=Program Data,OU={Unit Name},DC={Name of domain controller},DC=local`
4. Set the **APPLICATION NAME** field to the exact name given to the Application (i.e. VertigoXmedia).

Starting the XMS Service to populate the VertigoXmedia application

After having made changes to the Xmedia Server Control Panel settings, the XMS Service must be restarted for the changes to take effect. In restarting the XMS service, the Xmedia

Server will read the **AUTHORIZATION MANAGER CONFIGURATION** settings and populate the VertigoXmedia application (in the store repository) with the Vertigo Suite operations.

To start the XMS Service and populate the VertigoXmedia application:

1. With the Xmedia Server Control Panel open, select the **SERVICE CONTROL** tab on the Xmedia Server Control Panel.
2. Click the **START** button to restart the XMS Service and apply the new settings.
3. Click **OK** and the Xmedia Server Control Panel closes.
4. Open the Authorization Manager console by selecting:
START>SETTINGS>CONTROL PANEL>ADMINSTRATIVE TOOLS>AUTHORIZATION MANAGER
5. Expand **VERTIGOXMEDIA** and **DEFINITIONS** nodes.
6. Select the **OPERATION DEFINITION** node. The right-side panel should now be populated with VertigoXmedia operations (figure 19-22).

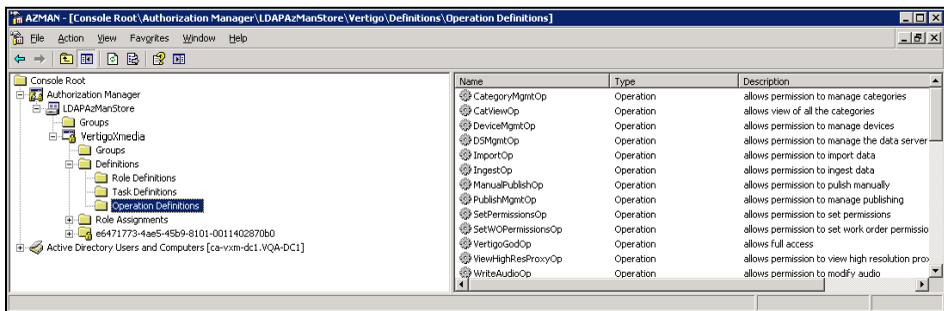


Figure 19-22. The operations that belong to AzMan's VertigoXmedia application

7. Select the **ROLE DEFINITION** node. The right-side panel should now be populated with VertigoXmedia role definitions (figure 19-23).

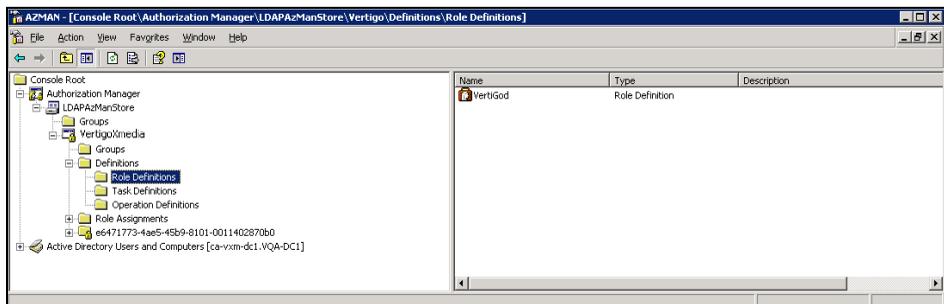


Figure 19-23. The role definitions that belong to AzMan's VertigoXmedia application

Configuring the Policy Store in an XML file

Before using the Authorization Manager, system administrators must create and configure a Policy Store repository. The Policy Store contains the AzMan-related configuration and Vertigo Suite access restrictions. It is manipulated via a Microsoft Management Console snap-in. Through the snap-in's user interface, access to various components of the Vertigo Suite can be restricted.

Prior to configuring the Policy Store, the type and location of the repository must be determined. The repository can be housed in two types of containers; an **XML FILE** or a node in an **ACTIVE DIRECTORY** installation of Windows 2003 functional level domain (see [page 19-8](#)).

The preferred repository is an Active Directory node, as it is best for multi-user environments. Nevertheless, you should choose the **XML FILE** type in situations where:

- your Microsoft network domain is not Windows 2003
- your domain administrator refuses to grant an external process access to an active directory node
- you have a computer with a network share that all other computers can read/write to
- you have a good understanding of Microsoft Windows networking permissions
- your network has a simple topology

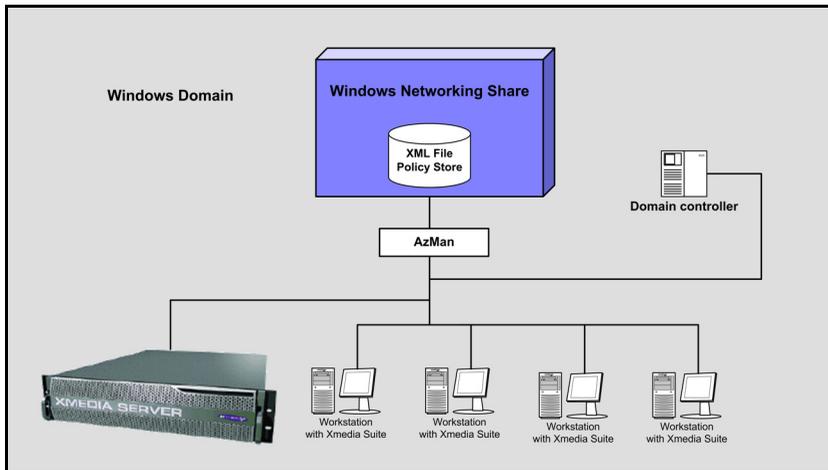


Figure 19-24. User rights management configuration with Policy Store in an XML file

☑ NOTE

Configuring the Policy Store in an XML file should only be attempted by system administrators and IT personnel whose responsibilities grant them jurisdiction over system and network security. These professionals must also possess a solid understanding and experience of Windows networking, including Windows Servers 2003, Active Directory, Windows users management, as well as the Microsoft Authorization Manager.

The procedure below identifies the high-level steps involved in creating and configuring the Authorization Manager's Policy Store in an **XML file**. Subsequent sections (identified by the links within the procedure) provide step-by-step instructions for performing each step.

To configure the Authorization Manager's Policy Store in an XML file:

1. Open the Microsoft Authorization Manager.
See ["Opening the Authorization Manager" on page 19-24.](#)
2. Configure the Authorization Manager to use an XML file on a network share. See ["Configuring the Authorization Manager to use an XML file stored on a network share" on page 19-25.](#)
3. Switch the snap-in to Developer mode and create the Policy Store.
See ["Creating the VertigoXmedia Policy Store in the Authorization Manager" on page 19-26.](#)
4. Obtain a Windows user with full control to the shared directory. See ["Obtaining a Windows user with full control of the shared directory" on page 19-28](#)
5. Open the Xmedia Server Control Panel and stop the XMS Service.
See ["Stopping the XMS Service" on page 19-29.](#)
6. Change the XMS Service credential to the new user and add the user as an Administrator on the Xmedia Server.
See ["Adding the new user to the Xmedia Server's security credentials" on page 19-30.](#)
7. Add the user to the security credentials of the Policy Store.
See ["Changing the security credentials of the Policy Store" on page 19-31.](#)
8. Enable and set the Authorization Manager Configuration settings on the Xmedia Server Control Panel.
See ["Setting the Authorization Manager Configuration settings" on page 19-33.](#)
9. Start the XMS Service in the Xmedia Server Control Panel and populate the Policy Store with the Vertigo Suite operations.
See ["Starting the XMS Service to populate the VertigoXmedia application" on page 19-34.](#)

Opening the Authorization Manager

Factory configured Xmedia Servers presently run Windows Server 2003, SP1 or later. Within Windows Server 2003, Microsoft provides the Authorization Manager snap-in. Therefore, the Authorization Manager is already installed and can follow the instructions below for launching the AzMan snap-in.

To open the Authorization Manager snap-in:

- Type `azman.msc` at the command prompt or **RUN** box and click **OK**.
Or,
- Select **START>SETTINGS>CONTROL PANEL>ADMINISTRATIVE TOOLS>AUTHORIZATION MANAGER**.

The **MICROSOFT MANAGEMENT CONSOLE** window appears, with the Authorization Manager snap-in active. The first time you open it, you'll see the message shown in (figure [19-25](#)), which advises you that no authorization stores have been selected.



Figure 19-25. The Authorization Manager window the first time it is opened

If the Authorization Manager snap-in does not already exist on your system, you must manually add the Authorization Manager using the Microsoft Management Console. If you need further information, please refer to the Microsoft documentation:

<http://technet.microsoft.com/en-us/library/cc731573.aspx>.

Configuring the Authorization Manager to use an XML file stored on a network share

Authorization Manager supports the storage of the Policy Store's repository in an .xml file that is stored on an Windows NT file system (NTFS) volume. The XML policy store should be stored on the Xmedia Server as a shared file.

If you select to store the Policy Store in an XML file, you'll need to designate its location in network-accessible folder structure by its path and specify particular permissions for that file.

To assign the Policy Store repository as an XML file:

1. Open the Authorization Manager snap-in window (see [page 19-24](#)). Then, right-click the Authorization Manager node in the left column and select the **NEW AUTHORIZATION STORE** command.

The **NEW AUTHORIZATION STORE** dialog box appears (figure [19-26](#)).

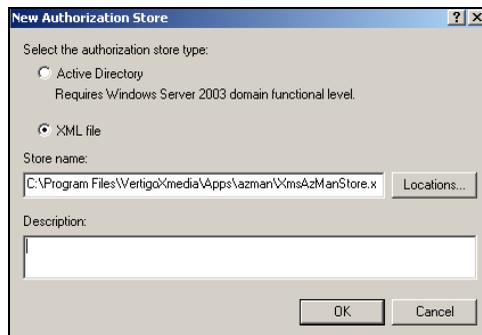


Figure 19-26. New Authorization Store dialog box

2. Specify the directory path and file name for the XML file in the **STORE NAME** field on the **NEW AUTHORIZATION STORE** dialog box (the XML repository must be stored in a network-accessible folder).

Type a path and file name that will be valid at run time.

We recommend using the following format: `\\<MachineName>\<NetworkShare>`

Alternatively, you can use the **LOCATIONS** button to navigate to the directory location, or you can create a new folder where you will store it.

3. Optional - Type a description of the new authorization store in the **DESCRIPTION** text box.
4. Click **OK**.

Creating the VertigoXmedia Policy Store in the Authorization Manager

The VertigoXmedia application is a container, which you must create, that stores all of the Vertigo Suite-related Authorization Manager elements. Once the application is created, the Xmedia Server will create the pre-defined set of operations offered by the suite in the application upon first start (after the Xmedia Server Control Panel has been properly configured).

A set of pre-determined operations and roles that grant users permission to view content or perform tasks related to the Vertigo Suite applications is initially stored on the Xmedia Server. These operations must be brought into the Authorization Manager's Policy Store repository by creating the **VERTIGOXMEDIA** application and then later importing them into the repository.

The following procedure provides instructions for creating a new application called **VERTIGOXMEDIA**.

To install the Vertigo Suite operations and roles:

1. Open the **AUTHORIZATION MANAGER CONSOLE** (figure 19-27) by selecting:
START>SETTINGS>CONTROL PANEL>ADMINSTRATIVE TOOLS>AUTHORIZATION MANAGER



Figure 19-27. The Authorization Manager

2. Right-click on the root node (**AUTHORIZATION MANAGER**) and select the **OPTIONS** command. The **OPTIONS** dialog box appears.



Figure 19-28. The Options dialog box allows you to select the Authorization Manager mode

3. Select **DEVELOPER MODE** and click **OK**.
4. Return to the Authorization Manager window. Right-click the Policy Store node (i.e. **XMSAZMANSTORE**) and select **NEW APPLICATION** command. The **NEW APPLICATION** dialog box appears (figure [19-29](#)).

Figure 19-29. The New Application dialog box

5. Enter **VertigoXmedia** as the **APPLICATION NAME** and **Vertigo Suite Policy store** as the **DESCRIPTION** field.
6. Click **OK**.
The VertigoXmedia application is added to the Authorization Manager's Policy Store (figure [19-30](#)).

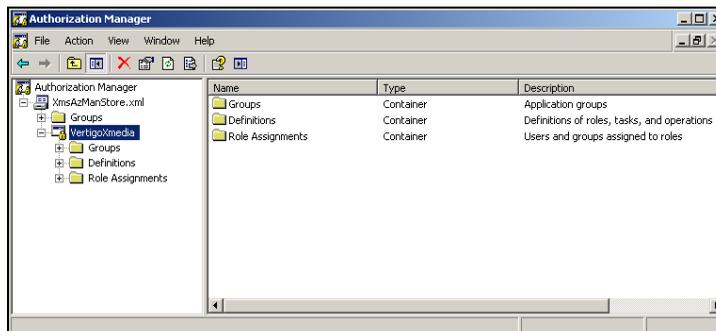


Figure 19-30. The VertigoXmedia application is added to the AzMan

Obtaining a Windows user with full control of the shared directory

For the Xmedia Server to manipulate the Policy Store, a Windows user must be created and be granted full control of the shared directory.

In a later step, the user credentials of the Xmedia Server will be set to this network user who has permission to access and change the XML Policy Store (see [page 19-30](#)).

NOTE

Every user that will access the Vertigo Suite must also have this permission because they will also be manipulating the Policy Store.

Stopping the XMS Service

The next few steps in the configuration procedure involve making and applying changes to the XMS Service settings. For these changes to take effect, you must first open the Xmedia Server Control Panel and stop the XMS Service. Later, these new settings will be applied to the Xmedia Server when it is restarted.

To open the Xmedia Server Control Panel and stop the XMS Service:

1. Open the **XMEDIA SERVER CONTROL PANEL** by selecting:
START>SETTINGS>CONTROL PANEL>VERTIGOXMEDIA XMEDIA SERVER
2. Select the **SERVICE CONTROL** tab on the **XMEDIA SERVER CONTROL PANEL** (figure [19-31](#)).

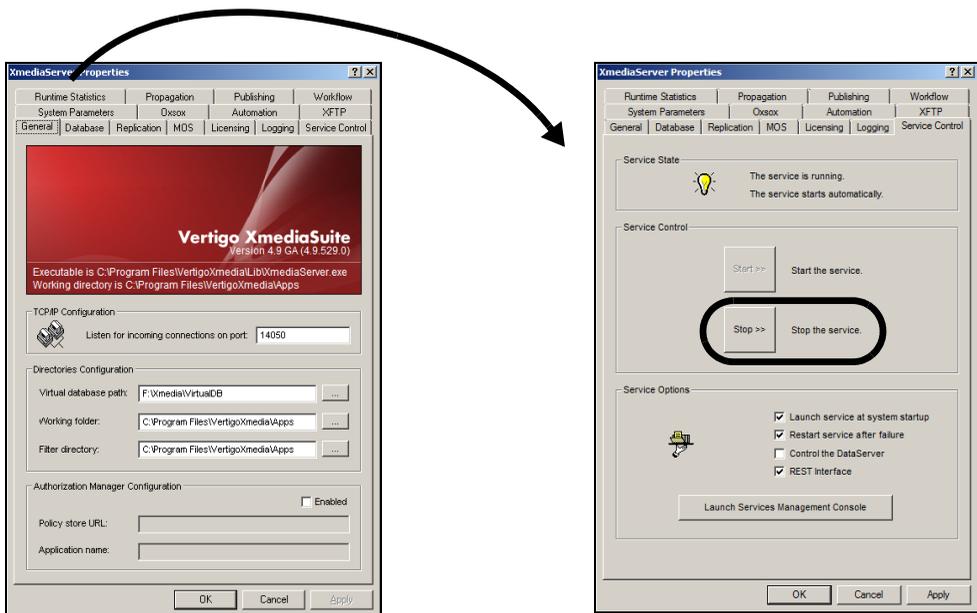


Figure 19-31. Accessing the XMS Service controls on the Xmedia Server Control Panel

3. Click the **STOP** button to stop the XMS Service.

Adding the new user to the Xmedia Server's security credentials

Earlier a new user was created. With the XMS Service now stopped, you must grant administrative rights (read/write) to the user on the Xmedia Server machine.

To grant the user administrative privileges to the Xmedia Server:

1. Start and log into the Xmedia Server as an Administrator user.
2. Add the newly created user as an administrator to the XMS machine.
3. Return to the Control Panel and open the Microsoft **SERVICES** console by selecting **ADMINISTRATIVE TOOLS>SERVICES**.
4. Navigate down the list of services to the **XMEDIA SERVER** service. Right-click on the Xmedia Server Service and select **PROPERTIES**. The **XMEDIA SERVER PROPERTIES** dialog box appears (figure [19-32](#)).

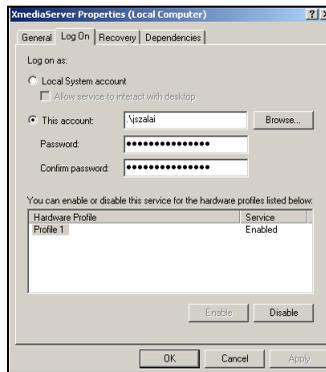


Figure 19-32. The XmediaServer Properties dialog box

5. Select the **LOG ON** tab and change the Log On as assignment from the local system account to the newly created domain account.
 - a. Press the **BROWSE** button. The **SELECT USER** dialog box appears (figure [19-33](#)).

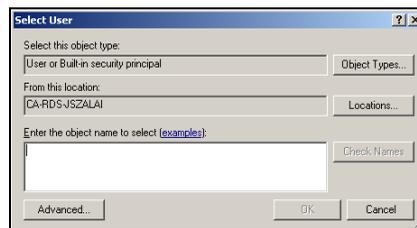


Figure 19-33. The Select User dialog box

- b. Type the domain user's name in the text box and press **OK**.
 - c. Press **OK** on the **XMEDIA SERVER PROPERTIES** dialog box to close it.
6. Close the **SERVICES** console and the **ADMINISTRATIVE TOOLS** windows.

Changing the security credentials of the Policy Store

Now that the new user has been granted administrative privileges, they must be added to the Policy Store's security credentials so that the Xmedia Server can add, delete, or modify the Policy Store (i.e. operations).

To edit the Policy Store's security credentials:

1. Open the Authorization Manager by selecting:
START MENU>PROGRAMS>ADMINISTRATIVE TOOLS>AUTHORIZATION MANAGER
2. Right-click on the **XMSAZMANSTORE.XML** policy store and select the **PROPERTIES** command (figure 19-34)

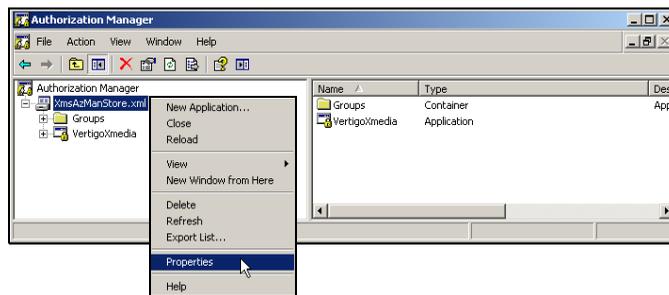


Figure 19-34. Open the Properties for the XmsAzManStore.xml policy store

3. Select the **SECURITY** tab on the policy store's **PROPERTIES** dialog box (figure 19-35). If it is not already displayed, set the Authorization Manager user role field to Administrator.

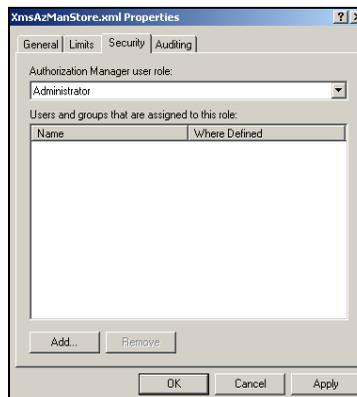


Figure 19-35. Select the Security tab on the policy store's Properties dialog box

4. Click the **ADD** button and the **SELECT USERS, COMPUTERS, OR GROUPS** dialog box appears (figure 19-36).

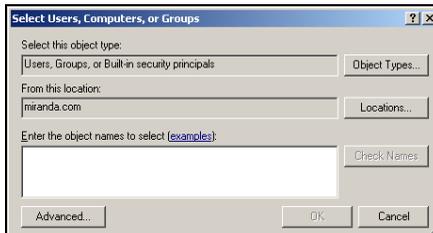


Figure 19-36. Specify the user's name to grant them administrative privileges

5. Type the user's login name in the text box and click **OK**. The **SELECT USERS, COMPUTERS, OR GROUPS** dialog box closes and the user's name now appears in the **PROPERTIES** dialog box.
6. Click **OK**.

Setting the Authorization Manager Configuration settings

The Xmedia Server Control Panel's **AUTHORIZATION MANAGER CONFIGURATION** settings must be set to enable user rights management in the Vertigo Suite, providing the location of the policy store and the name of the application to be used.

To set the AUTHORIZATION MANAGER CONFIGURATION settings:

1. Open the **XMEDIA SERVER CONTROL PANEL** by selecting:
START>SETTINGS>CONTROL PANEL>VERTIGOXMEDIA XMEDIA SERVER

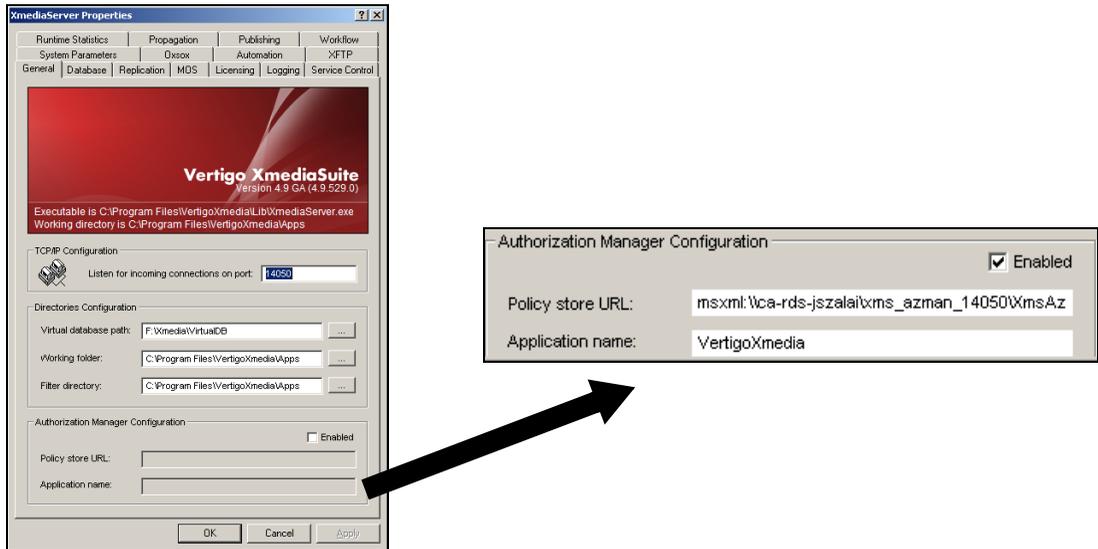


Figure 19-37. Authorization Manager Configuration settings on the Xmedia Server Control Panel

2. Select the **ENABLED** check box in the Authorization Manager Configuration section of the **GENERAL** page (figure 19-21).
3. Set the **POLICY STORE URL** field. Since the Store's repository is saved as an XML file, use the following form for the path setting: `msxml:\\{hostname}\\{path}\\{to}\\{file}`
4. Set the **APPLICATION NAME** field to the exact name given to the Application (i.e. VertigoXmedia).

Starting the XMS Service to populate the VertigoXmedia application

After having made changes to the Xmedia Server Control Panel settings, the XMS Service must be restarted for the changes to take effect. In restarting the XMS service, the Xmedia Server will read the **AUTHORIZATION MANAGER CONFIGURATION** settings and populate the VertigoXmedia application (in the store repository) with the Vertigo Suite operations.

To start the XMS Service and populate the VertigoXmedia application:

1. With the Xmedia Server Control Panel open, select the **SERVICE CONTROL** tab on the Xmedia Server Control Panel.
2. Click the **START** button to restart the XMS Service and apply the new settings.
3. Click **OK** and the Xmedia Server Control Panel closes.
4. Open the Authorization Manager console by selecting: **START>SETTINGS>CONTROL PANEL>ADMINSTRATIVE TOOLS>AUTHORIZATION MANAGER**
5. Expand **VERTIGOXMEDIA** and **DEFINITIONS** nodes.
6. Select the **OPERATION DEFINITION** node. The right-side panel should now be populated with Vertigo Xmedia operations (figure 19-22).

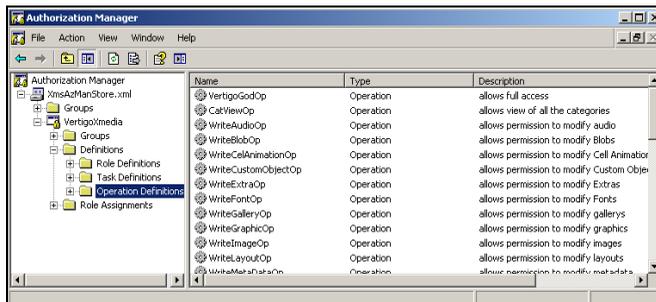


Figure 19-22. The operations that belong to AzMan's VertigoXmedia application

7. Select the **ROLE DEFINITION** node. The right-side panel should now be populated with Vertigo Xmedia role definitions (figure 19-23).

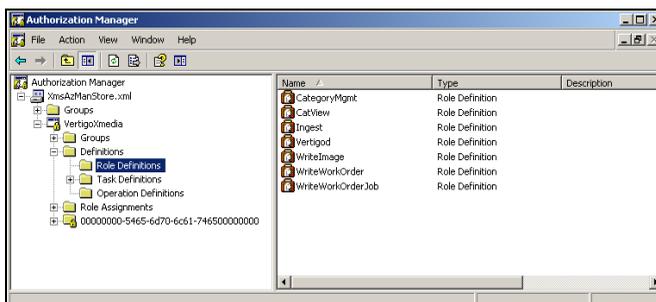


Figure 19-23. The role definitions that belong to AzMan's VertigoXmedia application

Setting up your user rights management system

Once the Policy Store repository has been created, the system administrator must populate it with role definitions, and role assignments that are appropriate for your organization's workflow and security policies.

The procedure below identifies the high-level steps involved in setting up your user rights management system in the Authorization Manager. Subsequent sections (identified by the links within the procedure) provide step-by-step instructions for performing each step.

NOTE

The VertigoXmedia application that was added to the Policy Store already contains all of the operation definitions that should be needed to operate the Vertigo Suite applications.

To set up the Authorization Manager's Policy Store for your user rights management model:

1. Establish your organization's user rights management model and policies to get a better idea of what tasks, and roles need to be created for the Policy Store.
See ["Establish your user rights management security criteria" on page 19-36](#).
2. Create task definitions that group together the VertigoXmedia application's operation definitions and/or lower-level task definitions into logical sets.
See ["Creating a new task definition" on page 19-37](#).
3. Create role definitions that group together task definitions, operation definitions, and/or lower-level role definitions that are based upon job functions in your organization's workflow.
See ["Creating and populating a new role definition" on page 19-38](#).
4. Create role assignments that allow you to map Windows users and/or groups with role definitions. See ["Creating a new role assignment" on page 19-40](#).
5. Assign users to the role assignments.
See ["Associating Windows users and groups with a role assignment" on page 19-41](#).

Establish your user rights management security criteria

An advantage of building the Vertigo Suite user rights management (URM) model around Microsoft's Authorization Manager technologies is the flexibility that it affords to system administrators to design and implement a security design that is appropriate to the organization's specific workflow and security needs. As such, each organization's URM system will contain tasks and roles that are unique to the way in which the organization is structured and operates. Nonetheless, there are a couple of relative constants that will be apparent in all Vertigo Suite URM models. More specifically, the original set of operation definitions and role definitions that are installed with the VertigoXmedia application are the foundation upon which system administrators will build their organization's security design (see ["VertigoXmedia Application, operations, and task definitions" on page 19-4](#) for more information).

Before you begin to set up your organization's URM system, we recommend that you consider and/or perform the following preliminary tasks:

1. Thoroughly familiarize yourself with the operations that are pre-packaged with the VertigoXmedia application.
2. Determine the organization's general security design and policies. For example, determine what content or actions will you want to restrict and from whom.
3. Based upon your organization's security design and policies, what roles and tasks will be required.

Once these design decisions are made, you can proceed with confidence that the URM system that you implement will effectively meets your organization's needs.

Creating a new task definition

A task definition is a grouping of operations and/or lower-level task definitions that are similar enough in nature or together they achieve a common goal. Task definitions provide the benefit of not having to repeatedly assign each operation individually to a role definition. Instead you can easily assign the single task definition.

To create a Task Definition:

1. Open Authorization Manager.
2. Navigate through the AzMan's policy store until you reach the Task Definitions folder (i.e. **XMSAZMANSTORE.XML>VERTIGOMEDIA>DEFINITIONS>TASK DEFINITIONS**)
3. Right-click the **TASK DEFINITION** folder and select the **NEW TASK DEFINITION** command. The **NEW TASK** dialog box appears (figure [19-40](#)).

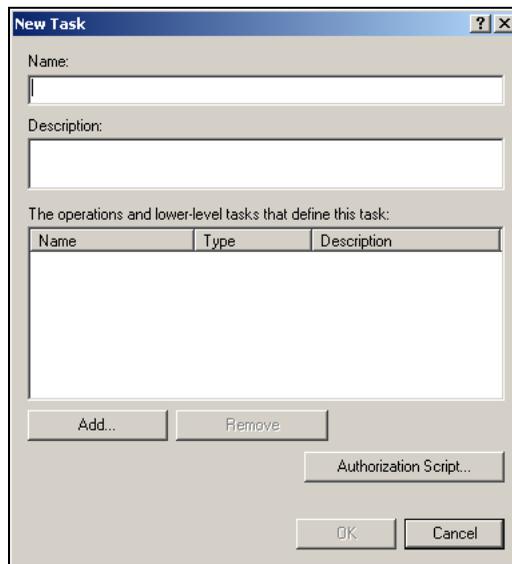


Figure 19-40. The New Task dialog box

4. Type the **NAME** and **DESCRIPTION** for the task.
5. Select the **ADD** button
6. Click **OK**.

Creating and populating a new role definition

Role definitions are normally based on a job function in your organization's workflow. The tasks and operations that are associated with the role provide the mechanism for granting permissions to access content or perform actions.

NOTE

If there are several authorization rules associated with a role definition (for example, it has several lower level roles and tasks), the authorization rules run synchronously. In Authorization Manager, the order has no effect on authorization.

To create a new role definition:

1. Open Authorization Manager.
2. Navigate through the AzMan's policy store until you reach the Role Definitions folder (i.e. **XMSAzMANSTORE.XML>VERTIGOMEDIA>DEFINTIONS>ROLE DEFINITIONS**)
3. Right-click the **ROLE DEFINITION** folder and select the **NEW ROLE DEFINITION** command. The **ROLE DEFINITION** dialog box appears (figure [19-41](#)).

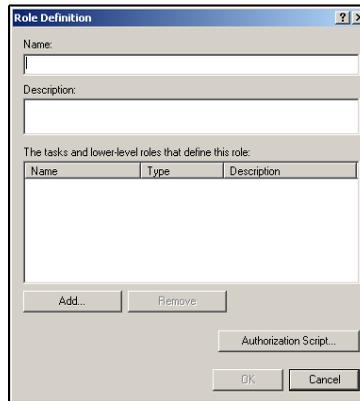


Figure 19-41. The Role Definition dialog box

4. Type the **NAME** and **DESCRIPTION** of the role. It is recommended that the name be indicative of a job function in your organization's workflow.
5. Click **OK**.

To assign tasks and/or operations to a role definition:

1. Open Authorization Manager.
2. Navigate through the AzMan's policy store until you reach the Role Definitions folder (i.e. **XMSAzMANSTORE.XML>VERTIGOMEDIA>DEFINTIONS>ROLE DEFINITIONS**)
3. Double-click the name of the role definition located in the right-side panel. The **DEFINITION PROPERTIES** dialog box appears.

4. Select the **DEFINITION** tab on the **DEFINITION PROPERTIES** dialog box (figure [19-42](#)).

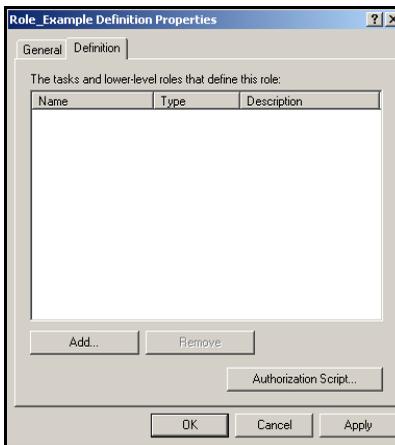


Figure 19-42. The Role Definition's properties dialog box

5. Click the **ADD** button and the **ADD DEFINITION** dialog box appears (figure [19-43](#)).

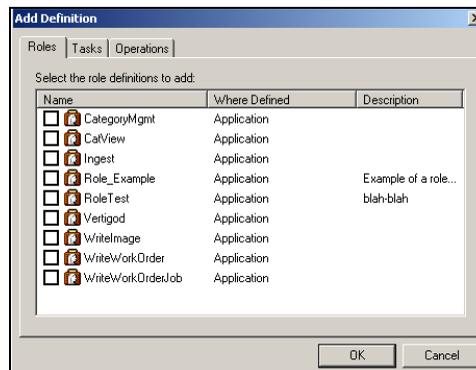


Figure 19-43. The Add Definition dialog box allows you to assign roles, tasks, and/or operations

6. Select the tabs on the **ADD DEFINITION** dialog box to display the roles, tasks, and operations that are available to be added to the role definition.
7. Enable the check box next to the roles, tasks, and operations that you want to add to the role.
8. Press **OK** and the **ADD DEFINITION** dialog box closes.
The **DEFINITION PROPERTIES** dialog box now lists the roles, tasks, and operation that were added to the role definition.
9. Press **OK** and the **DEFINITION PROPERTIES** dialog box closes.

Creating a new role assignment

A role assignment is a virtual container that is based on a single role definition. Once populated, the role assignment identifies the Windows users and/or groups that are authorized to perform the tasks and operations associated with the role definition.

To create a new role assignment:

1. Open Authorization Manager.
2. Navigate through the AzMan's policy store until you reach the Role Assignments folder (i.e. **XMSAzMANSTORE.XML>VERTIGOMEDIA>DEFINTIONS>ROLE ASSIGNMENTS**)
3. Right-click the **ROLE ASSIGNMENTS** folder and select the **ASSIGN ROLES** command. The **ADD ROLE** dialog box appears (figure 19-44).

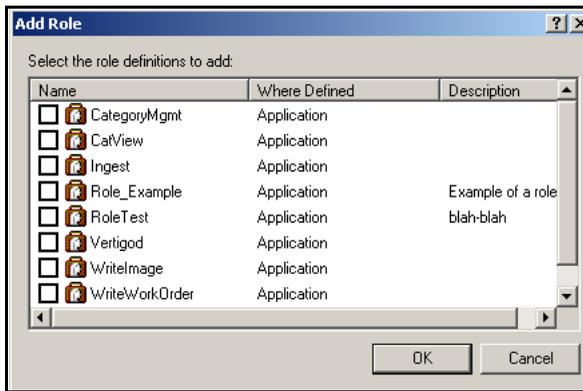


Figure 19-44. The Add Role dialog box

4. Select the role definitions that you want to make into role assignments by enabling the role definition's check box and press **OK**. The newly created role assignments are now displayed under the **ROLE ASSIGNMENTS** folder in the VertigoXmedia application.

Associating Windows users and groups with a role assignment

The most common procedure that system administrators carry out is the assignment of Windows users and groups to a role definition. Since the role definitions determine the permissions for accessing content or perform actions, a role assignment is responsible for designating which users are granted specific permissions.

To assign Windows users and/or groups to a role assignment:

1. Right-click a role assignment listed in the right-side panel of the Authorization Manager window and select the **ASSIGN WINDOWS USERS AND GROUPS** command.

The **SELECT USERS, COMPUTERS, OR GROUPS** dialog box appears (figure [19-45](#)).

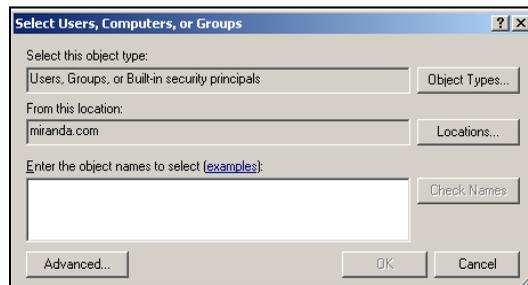


Figure 19-45. The Select Users, Computers, or Groups dialog box

2. The text box provides a space for you to type the object names that you want to find. You can search for multiple objects by separating each name with a semicolon.

Use one of the following syntax examples:

- DisplayName (example: FirstName LastName)
- ObjectName (example: Computer1)
- UserName (example: User1)
- ObjectName@DomainName (example: User1@Domain1)
- DomainName\ObjectName (example:Domain\User1)

3. Press the **CHECK NAMES** button.

- If only one match is found, then the name is immediately added to the text box. However, if multiple names match the search criteria, then the **MULTIPLE NAMES FOUND** dialog box appears (figure 19-46). Select the name of the user(s) that you want to add from the **MULTIPLE NAME FOUND** dialog box and press **OK**.

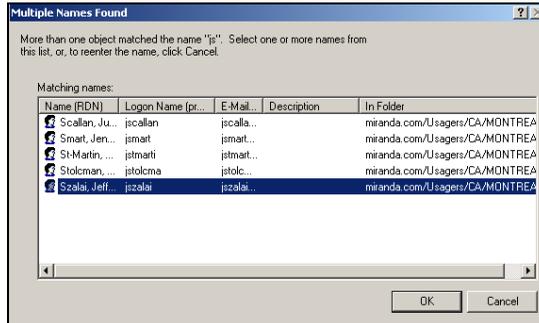


Figure 19-46. The Multiple Name Found dialog box

- The names are now listed in the **SELECT USERS, COMPUTERS, OR GROUPS** dialog box (figure 19-47).

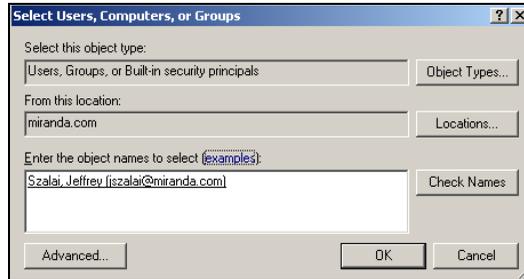


Figure 19-47. The Select Users, Computers, or Groups dialog box

- Press the **OK** button to close the **SELECT USERS, COMPUTERS, OR GROUPS** dialog box.

Maintaining the Authorization Manager's elements

Once your user rights management system for the Vertigo Suite products is properly configured, you may need to occasionally perform maintenance tasks like, editing the characteristics of role definitions, add tasks or operations to a role, or add additional users to a role assignment.

The following sections provide instructions for performing many of the tasks to maintain the user rights managements system:

- [“Editing role definitions” on page 19-43](#)
- [“Editing task definitions” on page 19-45](#)
- [“Adding and removing users from a role assignment” on page 19-47](#)

Editing role definitions

Once a role definition is created, you may need to edit some of the role's characteristics like its name or description. Or, you may need to add or remove tasks or operations from the role definition. The following sections provide you with instructions for performing editing tasks on existing role definitions.

- [“Editing the name or description of a role definition” on page 19-43](#)
- [“Adding additional tasks or operations to a role definition” on page 19-44](#)
- [“Remove tasks or operations from a role definition” on page 19-44](#)
- [“Deleting a role definition” on page 19-45](#)

Editing the name or description of a role definition

The following instructions guide you through the process of changing a role definition's name, as well as how to add/edit the description associated with the role definition.

To edit the name or description of a role definition:

1. Open Authorization Manager.
2. Navigate through the AzMan's policy store until you reach the Role Definitions folder (i.e. **XMSAZMANSTORE.XML>VERTIGOMEDIA>DEFINITIONS>ROLE DEFINITIONS**)
3. Double-click the **ROLE DEFINITION** that you want to edit.
The **DEFINITION PROPERTIES** dialog box appears.
4. Select the **GENERAL** tab and type in the **NAME** and/or **DESCRIPTION** text boxes to edit these settings.
5. Press the **OK** button to apply the changes and close the dialog box, or press the **APPLY** button to apply the changes and keep the dialog box open.

Adding additional tasks or operations to a role definition

The following instructions guide you through the process of adding additional tasks or operations to an existing role definition.

To add additional tasks and/or operations to a role definition:

1. Open Authorization Manager.
2. Navigate through the AzMan's policy store until you reach the Role Definitions folder (i.e. **XMSAZMANSTORE.XML>VERTIGOMEDIA>DEFINITIONS>ROLE DEFINITIONS**)
3. Double-click the **ROLE DEFINITION** that you want to edit.
The **DEFINITION PROPERTIES** dialog box appears.
4. Select the **DEFINITION** tab on the **DEFINITION PROPERTIES** dialog box. The tasks and operations that are currently associated with the role definition are displayed.
5. Click the **ADD** button and the **ADD DEFINITION** dialog box appears.
6. Select the tabs on the **ADD DEFINITION** dialog box to display the roles, tasks, and operations that are available to be added to the role definition.
7. Enable the check box next to the roles, tasks, and operations that you want to add to the role definition.
8. Press **OK** and the **ADD DEFINITION** dialog box closes.
The **DEFINITION PROPERTIES** dialog box now lists the roles, tasks, and operation that were added to the role definition.
9. Press **OK** and the **DEFINITION PROPERTIES** dialog box closes.

Remove tasks or operations from a role definition

The following instructions guide you through the process of removing unnecessary tasks or operations from an existing role definition.

To remove tasks and/or operations from a role definition:

1. Open Authorization Manager.
2. Navigate through the AzMan's policy store until you reach the Role Definitions folder (i.e. **XMSAZMANSTORE.XML>VERTIGOMEDIA>DEFINITIONS>ROLE DEFINITIONS**)
3. Double-click the **ROLE DEFINITION** that you want to edit.
The **DEFINITION PROPERTIES** dialog box appears.
4. Select the **DEFINITION** tab on the **DEFINITION PROPERTIES** dialog box. The tasks and operations that are currently associated with the role definition are displayed.
5. Select the task or operation that you want to remove. To select multiple tasks or operations, press the **SHIFT** key as you click on each item for consecutive selections, or press the **CTRL** key to select a grouping of non-consecutive files.
6. Click the **REMOVE** button and the selected tasks or operations are immediately removed.
7. Press **OK** and the **DEFINITION PROPERTIES** dialog box closes.

Deleting a role definition

The following instructions guide you through the process of removing an existing role definition from the Authorization Manager.

To delete a role definition from the AzMan's application:

1. Open Authorization Manager.
2. Navigate through the AzMan's policy store until you reach the Role Definitions folder (i.e. **XMSAZMANSTORE.XML>VERTIGOMEDIA>DEFINITIONS>ROLE DEFINITIONS**)
3. Right-click the **ROLE DEFINITION** that you want to delete and select the **DELETE** command.
4. A dialog box appears and asks you to confirm your intention to delete the role definition. Select **YES** to proceed in deleting the role definition, or **NO** to cancel the delete action.

Editing task definitions

Once a task definition is created, you may need to edit some of the task's characteristics like its name or description. Or, you may need to add or remove lower-level tasks or operations from the task definition. The following sections provide you with instructions for performing editing procedures on existing task definitions.

- ["Editing the name or description of a task definition" on page 19-45](#)
- ["Add tasks or operations to a task definition" on page 19-46](#)
- ["Remove operations or lower-level tasks from a task definition" on page 19-46](#)
- ["Deleting a task definition" on page 19-47](#)

Editing the name or description of a task definition

The following instructions guide you through the process of changing a task definition's name, as well as how to add/edit the description associated with the task definition.

To edit the name or description of a task definition:

1. Open Authorization Manager.
2. Navigate through the AzMan's policy store until you reach the Task Definitions folder (i.e. **XMSAZMANSTORE.XML>VERTIGOMEDIA>DEFINITIONS>TASK DEFINITIONS**)
3. Double-click the **TASK DEFINITION** that you want to edit.
The **DEFINITION PROPERTIES** dialog box appears.
4. Select the **GENERAL** tab and type in the **NAME** and/or **DESCRIPTION** text boxes to edit these settings.
5. Press the **OK** button to apply the changes and close the dialog box, or press the **APPLY** button to apply the changes and keep the dialog box open.

Add tasks or operations to a task definition

The following instructions guide you through the process of adding additional tasks or operations to an existing task definition.

To add additional tasks and/or operations to a task definition:

1. Open Authorization Manager.
2. Navigate through the AzMan's policy store until you reach the Task Definitions folder (i.e. **XMSAZMANSTORE.XML>VERTIGOMEDIA>DEFINITIONS>TASK DEFINITIONS**)
3. Double-click the **TASK DEFINITION** that you want to edit.
The **DEFINITION PROPERTIES** dialog box appears.
4. Select the **DEFINITION** tab on the **DEFINITION PROPERTIES** dialog box. The tasks and operations that are currently associated with the task definition are displayed.
5. Click the **ADD** button and the **ADD DEFINITION** dialog box appears.
6. Select the tabs on the **ADD DEFINITION** dialog box to display the tasks and operations that are available to be added to the task definition.
7. Enable the check box next to the tasks and operations that you want to add to the task definition.
8. Press **OK** and the **ADD DEFINITION** dialog box closes.
The **DEFINITION PROPERTIES** dialog box now lists the tasks and operation that were added to the task definition.
9. Press **OK** and the **DEFINITION PROPERTIES** dialog box closes.

Remove operations or lower-level tasks from a task definition

The following instructions guide you through the process of removing unnecessary tasks or operations from an existing task definition.

To remove tasks and/or operations from a task definition:

1. Open Authorization Manager.
2. Navigate through the AzMan's policy store until you reach the Task Definitions folder (i.e. **XMSAZMANSTORE.XML>VERTIGOMEDIA>DEFINITIONS>TASK DEFINITIONS**)
3. Double-click the **TASK DEFINITION** that you want to edit.
The **DEFINITION PROPERTIES** dialog box appears.
4. Select the **DEFINITION** tab on the **DEFINITION PROPERTIES** dialog box. The tasks and operations that are currently associated with the task definition are displayed.
5. Select the task or operation that you want to remove. To select multiple tasks or operations, press the **SHIFT** key as you click on each item for consecutive selections, or press the **CTRL** key to select a grouping of non-consecutive files.
6. Click the **REMOVE** button and the selected tasks or operations are immediately removed.
7. Press **OK** and the **DEFINITION PROPERTIES** dialog box closes.

Deleting a task definition

The following instructions guide you through the process of removing an existing task definition from the Authorization Manager.

To delete a task definition from the AzMan's application:

1. Open Authorization Manager.
2. Navigate through the AzMan's policy store until you reach the Task Definitions folder (i.e. **XMSAZMANSTORE.XML>VERTIGOMEDIA>DEFINITIONS>TASK DEFINITIONS**)
3. Right-click the **TASK DEFINITION** that you want to delete and select the **DELETE** command.
4. A dialog box appears and asks you to confirm your intention to delete the task definition. Select **YES** to proceed in deleting the task definition, or **NO** to cancel the delete action.

Adding and removing users from a role assignment

Even after you have set up your user rights management system, you may need to add or remove users from a role assignment. The following instructions guide you through the process of adding and removing an existing operation definition from the Authorization Manager.

To add additional users to a role assignment:

1. Open Authorization Manager.
2. Navigate through the AzMan's policy store until you reach the **ROLE ASSIGNMENTS** folder (i.e. **XMSAZMANSTORE.XML>VERTIGOMEDIA>DEFINITIONS>ROLE ASSIGNMENTS**)
3. Expand the Role Assignments folder to display the existing Role Assignments.
4. Right-click the specific Role Assignment that you want to add a user to and then select the **ASSIGN WINDOWS USERS AND GROUPS** command.

The **SELECT USERS, COMPUTERS, OR GROUPS** dialog box appears.

5. The text box provides a space for you to type the object names that you want to find. You can search for multiple objects by separating each name with a semicolon.

Use one of the following syntax examples:

- DisplayName (example: FirstName LastName)
 - ObjectName (example: Computer1)
 - UserName (example: User1)
 - ObjectName@DomainName (example: User1@Domain1)
 - DomainName\ObjectName (example:Domain\User1)
6. Press the **CHECK NAMES** button.
 7. If only one match is found, then the name is immediately added to the text box. However, if multiple names match the search criteria, then the **MULTIPLE NAMES FOUND** dialog box appears. Select the name of the user(s) that you want to add from the **MULTIPLE NAME FOUND** dialog box and press **OK**.
 8. The names are now listed in the **SELECT USERS, COMPUTERS, OR GROUPS** dialog box.
 9. Press the **OK** button to close the **SELECT USERS, COMPUTERS, OR GROUPS** dialog box.

To remove a user from a role assignment:

1. Open Authorization Manager.
2. Navigate through the AzMan's policy store until you reach the **ROLE ASSIGNMENTS** folder (i.e. **XMSAzMANSTORE.XML>VERTIGOMEDIA>DEFINITIONS>ROLE ASSIGNMENTS**)
3. Expand the Role Assignments folder to display the existing Role Assignments.
4. Select a specific Role Assignment and the users and groups associated with the role assignment are listed in the right-side panel.
5. Select the group or user to be remove and press the **DELETE** key on your keyboard. The group or user is immediately deleted from the role assignment.

Restricting access to asset categories

Normally, the Asset Browser in the various Vertigo Suite applications displays all of the available assets and asset categories. As such, all users have access to these asset categories. Configuring and enabling the user rights management system allows system administrators to restrict access of certain asset categories from specific users. Access can be restricted for either the root category level or a subcategory level, but not for individual assets.

Figure 19-48 demonstrates that the assignment of asset category permissions is performed within the Vertigo Suite applications' Asset Browser, while the resulting category permissions are stored as scopes within the Authorization Manager's Policy Store. Meanwhile, the Xmedia Server acts as an intermediary between the application's Asset Browser and the Authorization Manager and is responsible for creating and destroying scopes.

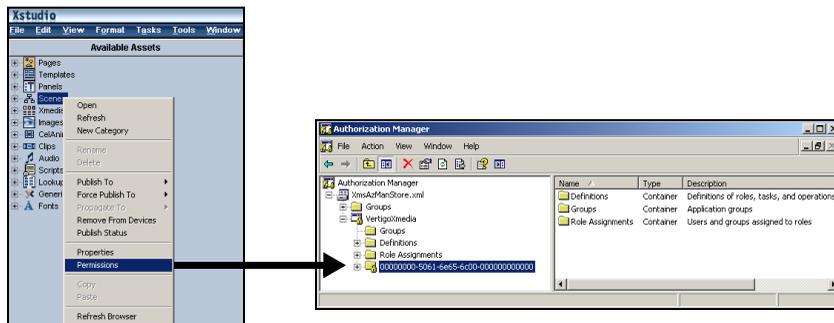


Figure 19-48. Category access permissions management components

Scopes provide a mapping between a given asset category and the users that are allowed to view the category. Therefore, a scope is created in the Authorization Manager for each of the asset categories whose permissions are set to allow access to only particular users. By the same token, asset categories that are universally (no permission restrictions) do not have a scope in the Authorization Manager.

The following sections provide instructions on how to restrict asset categories using the Asset Browser's permissions, as well as how to edit or remove the restrictions:

- [“Setting access permissions for an asset category” on page 19-50](#)
- [“Granting additional users access to a restricted category” on page 19-53](#)
- [“Removing users from a category’s security” on page 19-53](#)
- [“Removing all access restrictions from a category” on page 19-54](#)

Setting access permissions for an asset category

The following procedure describes how to set the Asset Browser's category permissions to restrict access of a selected asset category to only a select group of users.

To restrict access of asset category to only a select group of users:

1. With an Vertigo Suite application open (i.e. Xplorer, Xstudio, Xbuilder...etc.), right-click on the asset category from the Asset Browser that you want to restrict access to. Select the **PERMISSIONS** command from the context menu (figure 19-49).

The **CATEGORY SECURITY** dialog box appears and states that there are currently no viewing restrictions set for the selected category. It further explains that the action of adding a user or a group instantly hides the category from every user except those users or groups add to this permission.

✓ NOTE

If the **PERMISSIONS** command is disabled in the context menu, this indicates that either the Authorization Manager is not installed; or that the Xmedia Server does not have its Authorization Manager Configuration settings enabled or set properly; or the user does not have access to the Policy Store.

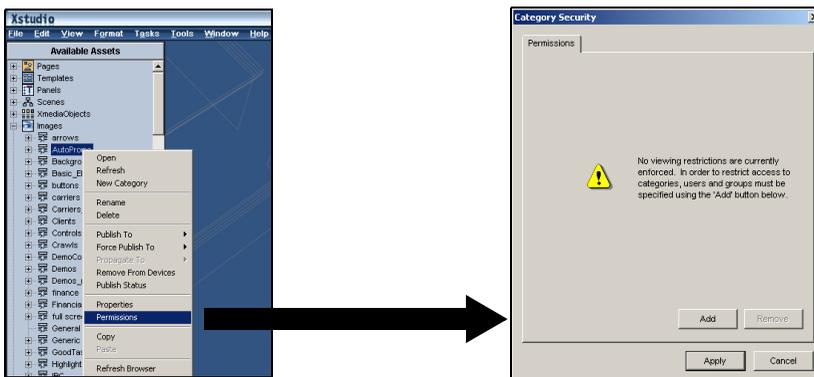


Figure 19-49. Select the Permissions command to restrict access to the selected asset category

2. Click the **ADD** button.

The **SELECT USERS OR GROUPS** dialog box appears (figure 19-50).

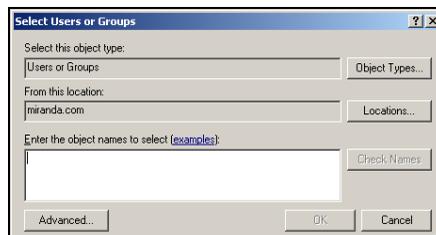


Figure 19-50. The Select Users or Groups dialog box

3. The text box provides a space for you to type the names of the user or group that you want to find.
4. Press the **CHECK NAMES** button.
5. If only one match is found, then the name is immediately added to the text box. However, if multiple names match the search criteria, then the **MULTIPLE NAMES FOUND** dialog box appears (figure 19-51). Select the name of the user(s) that you want to add from the **MULTIPLE NAME FOUND** dialog box and press **OK**.

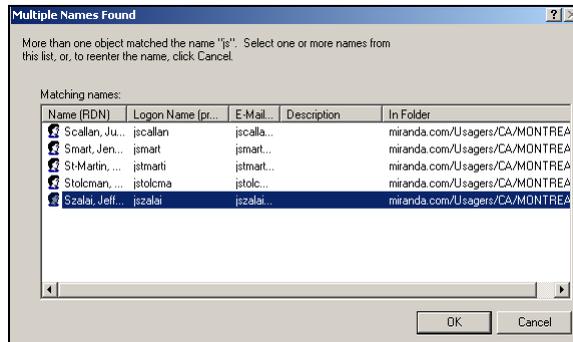


Figure 19-51. The Multiple Name Found dialog box

6. The names are now listed in the **SELECT USERS OR GROUPS** dialog box (figure 19-47).



Figure 19-52. The Select Users or Groups dialog box

- Click the **OK** button and the **SELECT USERS OR GROUP** dialog box closes. The **CATEGORY SECURITY** dialog box now lists the users and/or groups that have permission to view and interact with the assets in this category (figure 19-53).

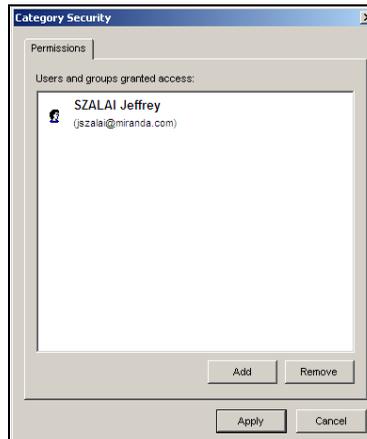


Figure 19-53. The Category Security dialog box lists the users and/or groups who have permission

Meanwhile, the Xmedia Server has created a scope and placed it as a folder in the Authorization Manager's Policy Store (figure 19-54).

NOTE

Under no circumstance should you edit or delete scopes in the Authorization Manager window. The remaining topics in this section describe how to edit or delete the category restrictions using the Asset Browser's permissions function.

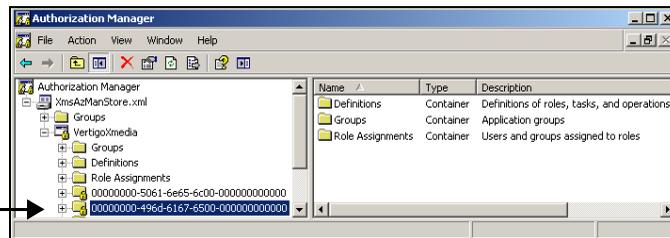


Figure 19-54. The XMS creates a create scope for each an asset category that is restricted

Granting additional users access to a restricted category

The following procedure describes how to grant additional users permission to access and interact with an asset category that is already restricted to specific users.

To add additional users to an asset category's access control permissions:

1. In the Asset Browser, right-click on the asset category and select the **PERMISSIONS** command from the context menu.
The **CATEGORY SECURITY** dialog box appears and displays the current users and/or groups that have permission to access the category.
2. Click the **ADD** button.
The **SELECT USERS OR GROUPS** dialog box appears.
3. The text box provides a space for you to type the names of the user or group that you want to find.
4. Press the **CHECK NAMES** button.
5. If only one match is found, then the name is immediately added to the text box. However, if multiple names match the search criteria, then the **MULTIPLE NAMES FOUND** dialog box appears. Select the name of the user(s) that you want to add from the **MULTIPLE NAME FOUND** dialog box and press **OK**.
6. The names are now listed in the **SELECT USERS OR GROUPS** dialog box.
7. Click the **OK** button and the **SELECT USERS OR GROUP** dialog box closes.
The **CATEGORY SECURITY** dialog box now lists the users and/or groups that have permission to view and interact with the assets in this category.

Removing users from a category's security

The following procedure describes how to remove users from a category's security and thereby restricting their access to the assets contained within the category.

To remove users from an asset category's security permissions:

1. In the Asset Browser, right-click on the asset category and select the **PERMISSIONS** command from the context menu.
The **CATEGORY SECURITY** dialog box appears and displays the current users and/or groups that have permission to access the category.
2. Select the user from the list of users/groups in the **CATEGORY SECURITY** dialog box. To select multiple users from the list, press the **SHIFT** key as you click on each name for consecutive selections, or press the **CTRL** key to select a grouping of non-consecutive names.
3. Click the **REMOVE** button and the user names are immediately removed from the **CATEGORY SECURITY** dialog box.
4. Click the **APPLY** button to apply the changes and close the **CATEGORY SECURITY** dialog box.

Removing all access restrictions from a category

The following procedure describes how to all remove users from a category's security and thereby removing all access restrictions from the category. As a result, the category will once again be accessible to all users.

To remove all access restrictions from an asset category rendering it accessible to all users:

1. In the Asset Browser, right-click on the asset category and select the **PERMISSIONS** command from the context menu.
The **CATEGORY SECURITY** dialog box appears and displays the current users and/or groups that have permission to access the category.
2. Select the all of the users/groups listed in the **CATEGORY SECURITY** dialog box by pressing the **SHIFT** key as you click on the first name listed and then the last name listed.
3. Click the **REMOVE** button. The user names are immediately removed and the **CATEGORY SECURITY** dialog box displays a message that states that there are currently no viewing restrictions set for the selected category.
4. Click the **APPLY** button to apply the changes and close the **CATEGORY SECURITY** dialog box. The asset category is now accessible to all users.

20 INGESTING MEDIA FILES USING THE FILE INGEST SERVER

The Vertigo File Ingest Server is an application that can be used to automatically ingest media into the Xmedia Server by simply placing the media files into a user-created ingest folder (watch folder). The File Ingest Server is also responsible for issuing media conversion requests to the Transcode Server, which is the service responsible for transcoding media from one format to another.

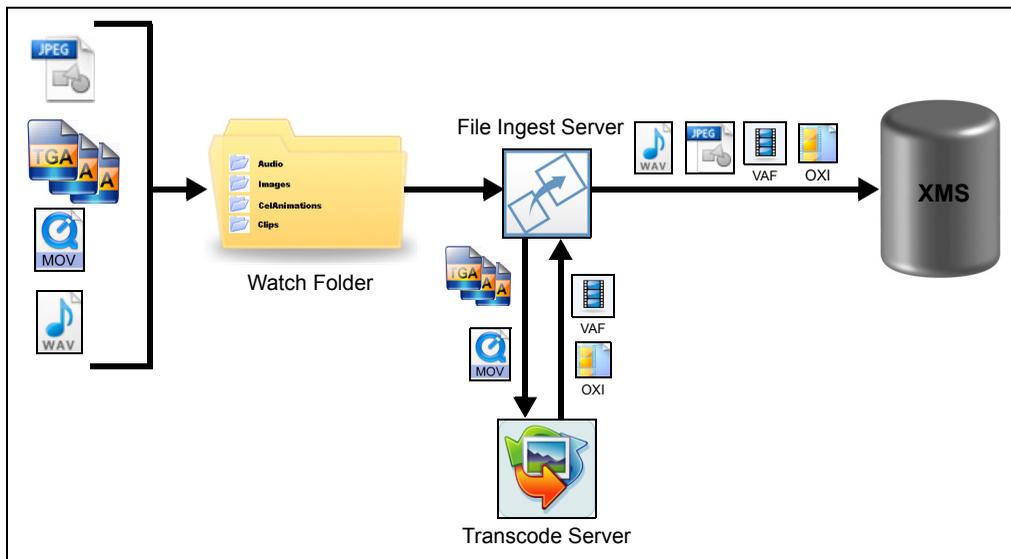


Figure 20-1. Media content is added to an ingest folder and then it is converted and/or ingested into the XMS

The File Ingest Server can be configured to watch one or more watch folders by defining *instances* of the ingest server in the **File Ingest Server Control Panel**. Each instance defines the set of rules that are mapped to its watch folder and determines how the files will be ingested, including if any file format conversion is necessary. Once an ingest is initiated by

placing files in the watch folder's subfolders, the progress of the files being ingested, the status of the ingest queues and ingest errors can be viewed using the **File Ingest Server Monitor**.

The following sections describe how to set up and use the File Ingest Server to ingest media into the Xmedia Server from a watch folder:

- [“Installing the File Ingest Server and creating an ingest watch folder” on page 20-3](#)
- [“Running the File Ingest Server and Transcode Server” on page 20-4](#)
- [“Configuring an ingest server instance” on page 20-5](#)
- [“Ingesting files and monitoring the ingest’s progress” on page 20-14](#)
- [“File Ingest Server’s logging” on page 20-17](#)

Installing the File Ingest Server and creating an ingest watch folder

In most cases, it is sufficient to run the File Ingest Server and Transcode Server locally on the Xmedia Server. However, if your organization's demand for ingest and transcoding is particularly high, we recommend installing and running the File Ingest Server and Transcode Server on a dedicated ingest server as to not burden the resources of the Xmedia Server.

Installing the File Ingest Server and Transcode Server:

Recent factory-configured Xmedia Servers will already have the File Ingest Server and Transcode Server installed as part of the Vertigo Suite software. However, when upgrading an existing Xmedia Server or configuring a dedicated ingest server, you must install the File Ingest Service and Transcode Server. Both of these applications are available as part of the Vertigo Suite installer's **Server Applications** (figure 20-2). See the **Vertigo Suite v.4.9 Release Notes** for complete installation information and procedures.

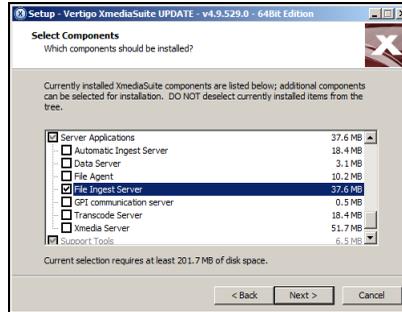


Figure 20-2. The Server Applications in the Vertigo Suite installer

Creating ingest watch folder(s):

Once the File Ingest Server and Transcode Server are properly installed, you must create a watch folder into which you will place the media files that are to be ingested into the Xmedia Server.

1. Add a new folder locally on the system that is hosting the File Ingest Server (`c:\Watchfolder`), on a remote file system on the same network (`\\10.14.4.51\Ingest`), or on a detachable network drive (`F:\IngestFolder`).
2. Right-click on the folder and select **Properties**. Select the **Security** tab and set the permissions to **FULL CONTROL**.

✓ NOTE

At this point the ingest watch folder is empty. However, when an instance of the file ingest server is configured to use this watch folder, subfolders for each applicable asset category (**IMAGES**, **CELANIMATIONS**, **CLIPS**, **IMAGES**) will automatically be added to this folder. See [“Configuring an ingest server instance” on page 20-5](#) for more information.

Running the File Ingest Server and Transcode Server

Both the File Ingest Server and the Transcode Server are applications that should start-up automatically and run in the background. When they are started, the File Ingest Server and Transcode Server icons both appear in the Windows notification area (figure 20-3).



Figure 20-3. Once started the File Ingest Server icon appears in the notification area

If the File Ingest Server icon is not displayed, you must launch the File Ingest Server by selecting **START>PROGRAMS>VERTIGO>FILE INGEST SERVER**. Once started, the icon will appear in the navigation area.

Trying to start the File Ingest Server when it is already running results in the DFIS already running error message (figure 20-4).

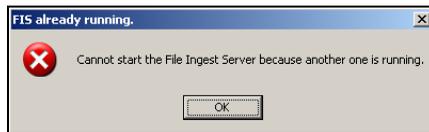


Figure 20-4. File Ingest Server is already running error message

If the Transcode Server has been stopped, its icon will no longer appear in the Windows navigation area. To restart the Transcode Server, navigate to **C:\PROGRAM FILES\VERTIGOXMEDIA\TRANSCODESERVER** and launch the **TranscodeServer.exe** file.

NOTE

To manually close either the File Ingest Server or the Transcode Server, right-click application's icon in the Windows Notification Area and select **EXIT**.

Configuring an ingest server instance

The File Ingest Server can be configured to watch one or more watch folders by defining *instances* of the ingest server in the **File Ingest Server Control Panel** (figure 20-5). Each instance defines the set of rules that are mapped to a watch folder and determines how the files will be ingested, including if any file format conversion is necessary.

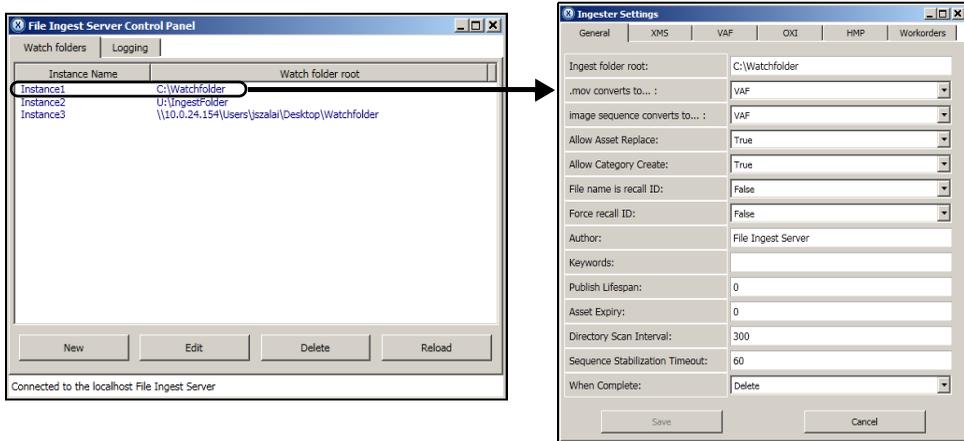


Figure 20-5. The File Ingest Server Control Panel and Ingester Settings window

To configure a new ingest server instance:

1. Open the **File Ingest Server Control Panel** by selecting:
START>PROGRAMS>VERTIGO>CONTROL PANELS>FILE INGEST SERVER CONTROL PANEL.

The File Ingest Server Control Panel appears, possibly with a few initial error messages:

- If the File Ingest Server is actively running, the lower message bar states: **CONNECTION TO THE LOCALHOST FILE INGEST SERVER**, and you may proceed. However, if the File Ingest Server is not actively running, the lower message bar turns red and states: **CONNECTION LOST TO THE LOCALHOST FILE INGEST SERVER**. In such a case, restart the File Ingest Service before proceeding (see [page 20-4](#)).
- The **Bad configuration file** error message (figure 20-6) may appear if an existing instance is not properly configured. For example, the File Ingest Control Panel initially contains only one default instance (*Instance1*) that has not yet been configured. In any case, click **OK** to proceed.



Figure 20-6. The default instance prompts a Bad configuration file error message

2. To create a new instance, click **NEW**.

The **Ingestor Settings** window appears and displays the instance's property settings on six (6) tabbed pages. Together these settings define the instance's behavior including identifying its target watch folder, Xmedia Server, as well as mapping the conversion and metadata definitions for the various file types.

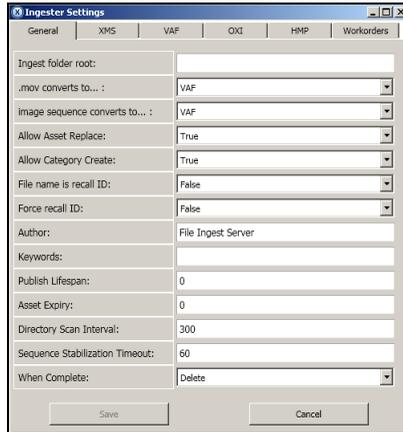


Figure 20-7. The Ingestor Settings window allows you to configure an ingest server instance

3. Define the instance by setting the appropriate properties in the Ingestor Settings window. In most cases, be sure to set the following properties:
 - [INGEST FOLDER ROOT](#)
 - [.MOV CONVERTS TO...](#)
 - [IMAGE SEQUENCE CONVERTS TO...](#)
 - [PRIMARY HOSTNAME](#)
 - [PRIMARY XMS PORT](#)

See "[Ingestor Settings properties](#)" on [page 20-7](#) for complete descriptions of each properties and setting on the Ingestor Settings window's pages.

4. Click **Save** to complete and apply the instance, which will now appear in the File Ingest Server Control Panel.

NOTE

When the configuration of a new instance is complete, subfolders for each applicable asset category (**IMAGES**, **CELANIMATIONS**, **CLIPS**, **IMAGES**) are automatically be added to the specified watch folder.

Ingester Settings properties

The following sections provide descriptions of each properties and setting on the Ingester Settings window's pages:

- [“General page - Ingester Settings” on page 20-7](#)
- [“XMS page - Ingester Settings” on page 20-9](#)
- [“VAF page - Ingester Settings” on page 20-10](#)
- [“OXI page - Ingester Settings” on page 20-11](#)
- [“HMP page - Ingester Settings” on page 20-12](#)
- [“Workorders page - Ingester Settings” on page 20-13](#)

General page - Ingester Settings

The table below describes each of the properties and settings on the **GENERAL** page of the Ingester Settings window. The purpose of the General page's properties is to identify the watch folder's exact location, the conversion behavior for MOV and image sequences, metadata settings, as well as the administrative rules for the ingest server.

INGEST FOLDER ROOT	The full (absolute) path to the root folder from which to ingest files. Note that the watch folder can be local on the system that is hosting the File Ingest Server (<code>c:\WatchFolder</code>), on a remote file system on the same network (<code>\\10.14.4.51\Ingest</code>), or on a detachable network drive (<code>F:\IngestFolder</code>).
.MOV CONVERTS TO...	Determines the target format when ingesting MOV files. Choose from: <ul style="list-style-type: none"> • As Is • VAF (default) • OXI • HMP • MXF • MOV WITH MXF ALTERNATE FORMAT
IMAGE SEQUENCE CONVERTS TO...	Determines the target format when ingesting image sequences. Choose from: <ul style="list-style-type: none"> • VAF (default) • OXI WITH EMBEDDED VAF • OXI WITH VAF ALTERNATE FORMAT • OXI • OXA • HMP

ALLOW ASSET REPLACE	Controls whether an asset can be replaced on the XMS (True - default). If set to False , the ingest fails.
ALLOW CATEGORY CREATE	When set to True , subcategories will be created in the Xmedia Server based on the directory subtree in the watch folder. For example, the subdirectory Images>Sports might not already exist on the target XMS. If you place an image file in this subdirectory in the watch folder, the subfolder will be created in the XMS upon ingest. If this setting is False , ingest will fail if the category does not exist.
FILENAME IS RECALL ID	When set to True , the Recall ID of assets being saved is added to the file name of the file being ingested. If this setting is set to False , then the Recall ID is not added to the file's name.
FORCE RECALL ID	When the FILENAME IS RECALL ID setting is True and the IF FORCE RECALL ID is also set to True , if the ingest server encounters a recall ID conflict prior to saving, the offending asset's recall ID will be cleared (i.e. set to empty) prior to ingestion. Note that clearing a recall ID of an asset with an all-numerical name is not possible. As a policy, such assets always have Recall ID equal to their all-numerical name. When the FILENAME IS RECALL ID setting is True and the IF FORCE RECALL ID is also set to False , if the ingest server encounters a recall ID conflict prior to saving, a RECALLIDCONFLICT error will be raised.
AUTHOR	Specifies the author property of assets ingested. By default, the author of assets ingested through the watch folder is set to FILE INGEST SERVER .
KEYWORDS	Allows you to specify a semi-colon (;) separated list of keywords to apply to ingested assets.
PUBLISH LIFESPAN	Controls the Publish Lifespan (the number of days the asset is kept on a device before being unpublished) assigned to ingested assets. The default value (0) disables the setting, meaning that assets are kept for an infinite amount of time.
ASSET EXPIRY	Controls the Asset Expiry (the number of days the asset is kept on the Xmedia Server before being deleted) assigned to ingested assets. The Asset Expiry setting supports three types of values: 0 means never expires; a positive value (i.e. 365) means that an expiry date of 365 days from the save date will be set; a fixed date (i.e. 2011-12-31), which must be in the following format: YYYY-MM-DD.

DIRECTORY SCAN INTERVAL	The File Ingest Server will scan the specified ingest folder at least every Directory Scan Interval seconds. The File Ingest Server will also subscribe to file system events in order to detect that something changed within the watch folder, but it will re-scan every Directory Scan Interval seconds if it hasn't seen any file system events in this time. This setting is useful in cases where an XMS connection was broken during a save. Such a file will be requeued at most after Directory Scan Interval seconds, even though no file system events occurred within the watch folder. The default value is set to 300 seconds.
SEQUENCE STABILIZATION TIMEOUT	Number of seconds to wait for image sequence files to have stabilized in the watch folder before considering that the sequence is complete. The default value is 60 seconds.
WHEN COMPLETE	Controls whether the ingested file is deleted or renamed (by appending <code>.complete</code> to its filename). The default value is DELETE .

XMS page - Ingestor Settings

The table below describes each of the properties and settings on the **XMS** page of the Ingestor Settings window. The purpose of the XMS page's properties is to identify the primary and optional secondary Xmedia Servers that will be the recipients of the files ingested from the watch folder.

PRIMARY HOSTNAME	The host name or IP Address of the primary Xmedia Server.
PRIMARY XMS PORT	The port of the primary Xmedia Server. The default value is 14050 .
BACKUP XMS HOSTNAME	The host name or IP address of the backup Xmedia Server.
BACKUP XMS PORT	The port of the backup Xmedia Server. The default value is 14050 .

VAF page - Ingestor Settings

The table below describes each of the properties and settings on the **VAF** page of the Ingestor Settings window. These settings apply when the **.MOV CONVERTS TO...** and/or **IMAGE SEQUENCE CONVERTS TO...** properties on the **General** page are set to **VAF**.

FORMAT	<ul style="list-style-type: none"> • When converting to VAF from an image sequence, the frame rate will be saved in the VAF metadata based on this setting. The resolution is not relevant. • When converting to VAF from MOV, the frame rate will be deduced from the MOV. The resolution is not relevant. <p>Choose from:</p> <ul style="list-style-type: none"> • PAL • NTSC (DEFAULT) • 720P 60 • 720P 60M • 720P 50 • 1080i 30 • 1080i 30M • 1080i 25
FRAMEREPEAT	<p>In cases where the audio and video tracks of the source material are not equal lengths, this setting determines the method video padding.</p> <p>Choose from:</p> <ul style="list-style-type: none"> • TRANSPARENT (default) • HOLD LAST FRAME • OUTPUT BLACK
OPTIMIZATION	<p>Determines if the VAF should be cropped to the smallest size. We recommend to always have this setting enabled.</p>
USEORIGINALSIZE	<p>Determines if the bounding box represents the original size of the content or the smallest cropped size.</p> <p>Enable this setting if you want the width and height of the video clip proxy to be equal to the width and height of the images from which it was created. When this setting is disabled, the video clip proxy will be cropped (by removing transparency) to the smallest size possible.</p>

OXI page - Ingester Settings

The table below describes each of the properties and settings on the **OXI** page of the Ingester Settings window. These settings apply when the **MOV CONVERTS TO...** and/or **IMAGE SEQUENCE CONVERTS TO...** properties on the **General** page are set to **OXI**.

FORMAT	<ul style="list-style-type: none"> When converting to OXI from an image sequence, the resolution and the frame rate will be saved in the OXI metadata based on the settings. When converting to OXI from MOV, the resolution will be saved in the OXI metadata based on the settings and the frame rate will be deducted from the MOV. <p>Choose from:</p> <ul style="list-style-type: none"> PAL NTSC (default) 720P 60 720P 60M 720P 50 1080i 30 1080i 30M 1080i 25
INTERLACED	<p>Determines if the encoded OXI file should be stored as fields (True) or frames (False).</p> <p>Note that this setting should be set to True when the FORMAT property is configured in interlaced mode (1080i 30, 1080i 30M, 1080i 25).</p>
PROXY FRAME	<p>Specifies the frame number within the OXI file that is to be designated as the proxy.</p> <p>Acceptable values are 0 to n, where n is the last frame number. 0 is the default.</p>
USEORIGINALSIZE	<p>Determines if the bounding box represents the original size of the content or the smallest cropped size.</p> <p>When set to True, the width and height of the cel animation proxy will be equal to the width and height of the images from which it was created. When set to False, the cel animation proxy will be cropped (by removing transparency) to the smallest size possible.</p>
REVERSE	<p>When set to True, the file will play in reverse order. When set to False, the file will play forward as normal.</p>
ASPECT	<p>Specifies the aspect ratio of the pixels. Choose from:</p> <ul style="list-style-type: none"> SQUARE PIXELS STANDARD TV (4:3) (default) WIDESCREEN (16:9)

KEY CLIPPED	When set to True , upon ingest each field will be clipped to a dynamically changing bounding box, eliminating transparent areas. When set to False , no clipping will be performed.
KEY CLIPPED LEVEL	Level of transparency to consider as transparent (between 0 and 1023). Anything at or below the specified value will be considered transparent for the purpose of creating a dynamically changing bounding box.

HMP page - Ingestor Settings

The table below describes each of the properties and settings on the **HMP** page of the Ingestor Settings window. These settings apply when the [.MOV CONVERTS TO...](#) and/or [IMAGE SEQUENCE CONVERTS TO...](#) properties on the **General** page are set to **HMP**, which converts the ingest file(s) into **.mxf** clip files for HMP devices.

FORMAT	<ul style="list-style-type: none"> When converting to HMP from an image sequence, the frame rate needed by the conversion will be based on this setting. The resolution is not relevant. When converting to HMP from MOV, the frame rate will be deduced from the MOV. The resolution is not relevant. <p>Choose from:</p> <ul style="list-style-type: none"> PAL NTSC (default) 720p 60 720p 60M 720p 50 1080i 30 1080i 30M 1080i 25
LOOP	When set to True , the clip's playout is looped according to the number in the LOOP COUNT property. When set to False , the clip only plays out once.
LOOP COUNT	Specifies the number of times the clip's playout will look when the LOOP property is set to True.
AUTO PLAY	Enables or disables autoplay.
ENDCLIPBEHAVIOUR	Determines the behavior of the clip when it reaches the end. Choose from: <ul style="list-style-type: none"> Output Black (default) Hold last frame Cue first frame
VIDEO FADE IN	Specifies the number of frames (duration) that it takes for the video to fade-in on initial playout.

VIDEO FADE OUT	Specifies the number of frames (duration) that it takes for the video to fade-out to the ending of playout.
VIDEO V JOINT	Specifies the number of frames (duration) that it takes for V-Joint.
VIDEO HOLD FIRST	Specifies the time (in number of frames) to hold on the first frame of data.
VIDEO HOLD LAST	Specifies the time (in number of frames) to hold on the last frame of data.

Workorders page - Ingestor Settings

The table below describes each of the properties and settings on the **WORKORDERS** page of the Ingestor Settings window. The purpose of the Workorders page's properties is to participate and contribute to the Xmedia Server's Work Order management system.

WORKORDER USER NAME	The user name to use to log into the Xmedia Server's Workorder subsystem.
ALLOW JOB TRANSITION	Set to True to enable work order processing. Set to False to disable (default).

Editing an instance's properties

To make can changes to the settings of existing instances:

1. Select the instance from the list of instance on the File Ingest Server Control Panel.
2. Click the **Edit** button.
The Ingestor Settings window appears with the instances current settings.
3. Make the necessary changes and then click **Save**.

Deleting an instance

To delete an existing instance:

1. Select the instance from the list of instance on the File Ingest Server Control Panel.
2. Click the **Delete** button.
The instance is immediately removed from the File Ingest Server Control Panel.

Reloading the instances in the File Ingest Server Control Panel

Changes to the status of the watch folders, Xmedia Server, or instance properties may have occurred while the File Ingest Server Control Panel has been open. Click the **Reload** button to ensure that all of the instances and their properties are accurate and up to date.

Ingesting files and monitoring the ingest's progress

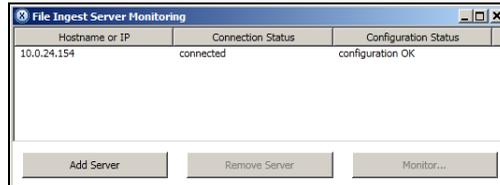
Once an instance of the File Ingest Server has been configured and associated with a watch folder, you may begin to ingest files into the Xmedia Server.

To perform and monitor the ingesting of files into the Xmedia Server:

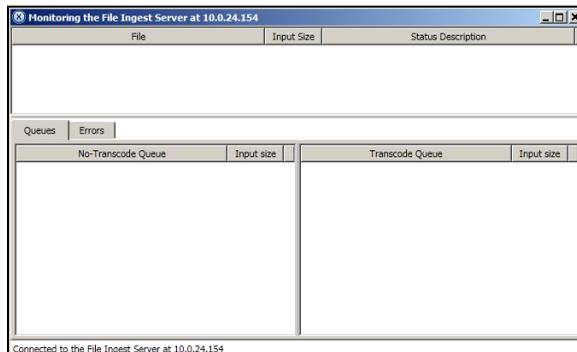
1. Optional - Ensure that the File Ingest Server and the Transcode Server are running by confirming that their icons are displayed in the Windows Navigation area ([page 20-4](#)).
2. In preparation for monitoring the progress of the ingest:
 - a. Select **START>PROGRAMS>VERTIGO>FILE INGEST SERVER MONITOR** to open the **File Ingest Server Monitor**.
 - b. If the server is not listed in the **File Ingest Server Monitoring** window, add the server that is hosting the File Ingest Server.
 - Click the **Add Server** button.
 - Type the server's hostname or IP address.
 - Click **OK**.



- c. Verify that the recipient server's **CONNECTION STATUS** is **connected** and the **CONFIGURATION STATUS** is **configuration OK**.



- d. Select the server row and click the **MONITOR** button to open the monitoring window.

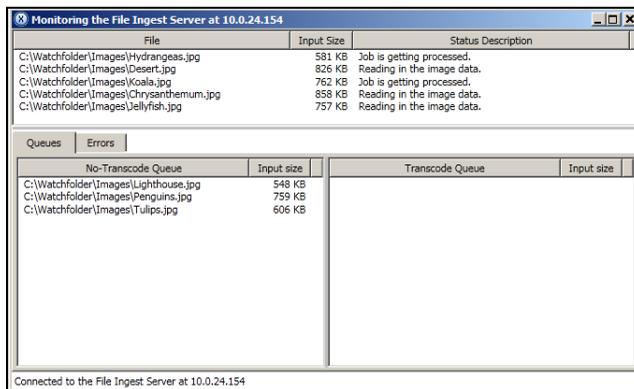


- Open the watch folder and add media files to the appropriate subfolders (**IMAGES**, **CELANIMATIONS**, **CLIPS**, **IMAGES**) based on the target/final asset type that will be ingested into the Xmedia Server, not the source file type (see note below).

NOTE

You will place the files in the subfolder that represents the final ingested asset type. For example, if you are ingesting a .MOV file and the instance is configured to convert f MOV to OXI, then the MOV must be placed in a **CELANIMATIONS** subdirectory, because the target asset will be a cel animation. Similarly, if the instance is configured to convert image sequences to VAF, then the image sequences must be placed in a **CLIPS** subdirectory because the resulting asset will be a video clip.

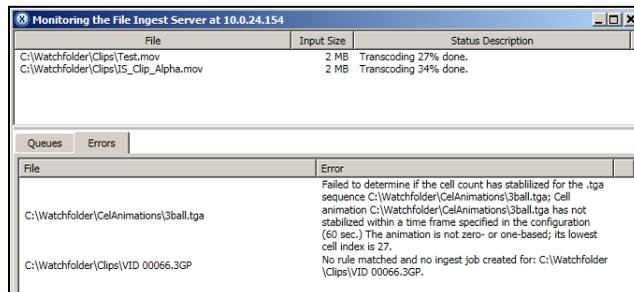
- Return to the server's **Monitoring** window. After a few seconds you will begin to see a listing of the files to be ingested, their file sizes and progress status in the upper pane.



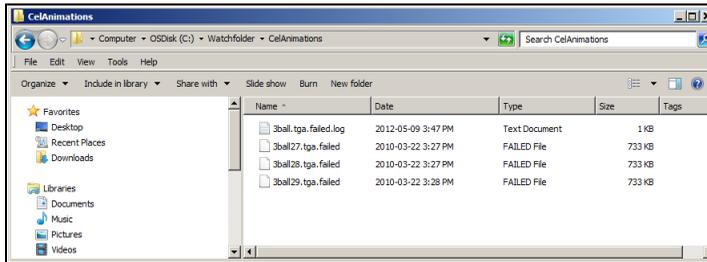
NOTE

When large amounts of files are submitted for transcoding and/or ingesting, they may be placed in an ingest or transcode queue. The **Queue** tab provides the queue status in two panes (**NO-TRANSCODE QUEUE & TRANSCODE QUEUE**).

- To verify if any errors occurred during the transcoding or ingest, click the **Errors** tab on the server's Monitoring window. The file is identified along with a description of the error.



- Once completely ingested, the file is automatically removed from or renamed in the ingest folder (depending upon the `when Complete` parameter's setting).
If a file failed to be ingested, it will remain in the watch folder, have `.failed` appended to its name and a log file specific to the failed file(s) will also be provided.



File Ingest Server's logging

The File Ingest Server Control Panel's **LOGGING** page (figure 20-8) allows you to set parameters to create a logging criteria. As ingest requests are processed, the operation status of the File Ingest Server and transcoding services are recorded to the `IngestServer.log` file, which is located in the following directory:

C:\Documents and Settings\All Users\Application Data\VertigoXmedia\Logs.

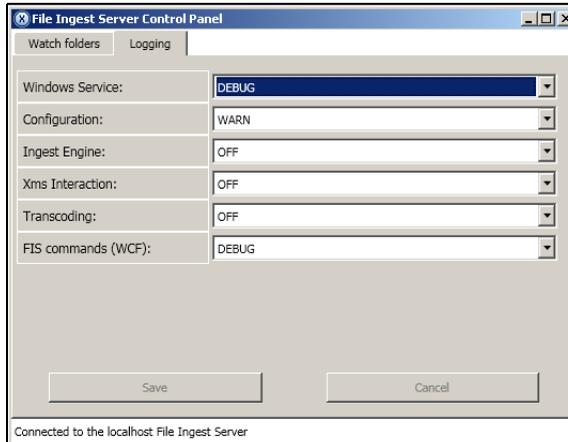


Figure 20-8. The File Ingest Server Control Panel's Logging page

The `IngestServer.log` file allows you to determine whether the File Ingest Server is being used correctly and it helps you to diagnose error conditions. In fact, our Technical Support team will often ask its customers to send them the File Ingest Server's log file to help them troubleshoot any unexpected behavior that they may be experiencing.

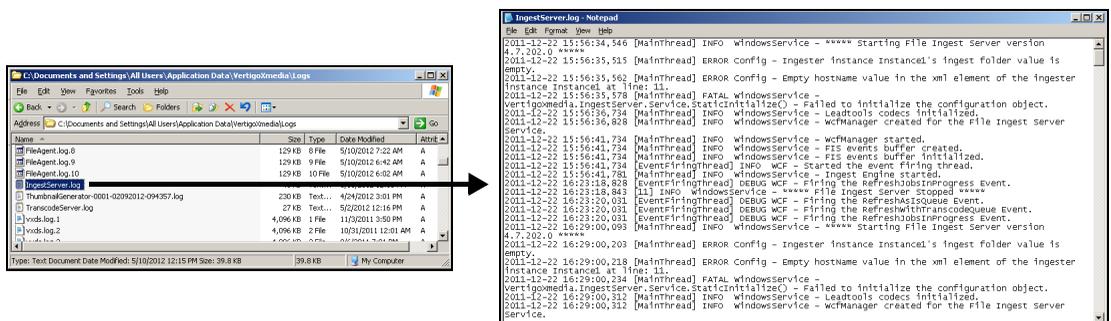


Figure 20-9. Accessing the IngestServer.log file