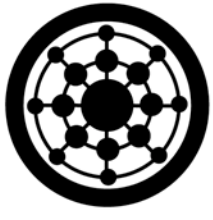
User's Guide



InfoChannel®
NETWORK MANAGER 3
ENTERPRISE EDITION

Software Release *6*

SCALA®
broadcast multimedia

www.scala.com

This manual was produced by Ross Hippely and Erik Mattsson.

IMPORTANT NOTICE FOR PURCHASERS OF UPGRADE OR EXTENSION VERSIONS. IF YOU HAVE PURCHASED AN UPGRADE LICENSE OR EXTENSION LICENSE TO SCALA SOFTWARE, YOU MUST READ AND AGREE TO BE BOUND BY SECTIONS 4(a) AND 4(b) OF THIS AGREEMENT.

END USER LICENSE AGREEMENT

This Software License Agreement ("Agreement") is entered into between Scala, Inc. ("Scala") and the users and/or purchasers of Scala software products (the "Licensee").

READ THIS LICENSE CAREFULLY. BY OPENING THE SCALA SOFTWARE PRODUCT PACKAGING AND/OR USING THE SCALA SOFTWARE, LICENSEE AGREES TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT.

If Licensee does not agree to the terms in this Agreement, Licensee must promptly cease using the Scala Software, uninstall and/or permanently delete the Scala Software, documentation (and any copies thereof) from the computer system(s) on which the Scala Software has been loaded or stored, and return the Scala Software, all media on which it is stored, all product packaging, and proof of payment to the Scala reseller pursuant to such reseller's return policy. If Licensee does not agree to the terms in this Agreement, and has acquired the Scala Software as part of a pre-configured computer system on which the Scala Software has been installed, Licensee must either promptly cease using the Scala Software, uninstall and/or permanently delete the Scala Software, documentation (and any copies thereof) from the computer system(s) on which the Scala Software has been preloaded, or return the pre-configured system pursuant to the system vendor's return policy.

In the mutual obligations described in this Agreement and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. LICENSE

Pursuant to the terms herein, Scala hereby grants Licensee a nonexclusive, nontransferable, non-sublicensable right and license to use the object code version of Scala's proprietary software, any software provided by third parties and incorporated into or delivered with the Scala product(s), and any graphical, textual, pictorial, audio or visual works or materials incorporated into or delivered with the Scala products (collectively referred to as "Scala Software"), along with any written documentation, including any Scala user guides, tutorials, reference manuals or other explanatory materials that accompany or are stored on or in the Software. This license will terminate immediately upon any termination of this Agreement.

2. TERM

This Agreement is effective as of the date at which Licensee opens the Scala Software product packaging, and will continue unless terminated as provided in Section 9.

3. SCOPE OF LICENSE AND USE

(a) **Internal Use**. Licensee may use the Scala Software and the documentation only for its own internal use on one, single-user computer. Licensee may not sublicense, lease, rent, sell or otherwise distribute the Scala Software. Licensee may not offer the use of the software to third parties as an application service provider, service bureau or remote-hosted service. Licensee may internally transfer the Scala Software to a different, single-user computer, provided that the Scala Software and any copies thereof are permanently uninstalled and/or deleted from the computer from which the Scala Software is transferred (a "Transferred Installation").

(i) **Limitations**. In connection with the development of content files using the Scala Software, Licensee may publish files for use or viewing via CD-ROM, web page or other file protocol, which publication shall involve the integration of Scala's iplay software, either within the content file or through download from the Scala Network. Use of the iplay software is limited solely to the review or display of the developed content file by Licensee through the single-user computer on which the Scala Software is loaded. Licensee expressly acknowledges and agrees that a separate, paid Scala Player end user license is required to display, perform or otherwise deliver content files created using Scala Software. Licensee shall not, directly or indirectly, distribute or cause to be distributed Scala Software content files in a manner calculated to circumvent the license limitation set forth in this Section 3(a)(i). Notwithstanding the foregoing, Licensee may distribute content files with integrated iplay software in connection with uses that are non-commercial, or limited to educational purposes for use in universities, primary or secondary schools.

(b) **Copies**. Licensee may not copy or otherwise reproduce the Scala Software or documentation except for one back-up copy of the Software for archival, testing or back-up purposes, provided that Licensee complies with the obligations of confidentiality set forth herein. Except as expressly permitted under applicable law, Licensee may not decompile, reverse engineer or disassemble the Scala Software in an attempt to derive or use the source code therefrom.

(c) **Third Party Software**. The Scala Software includes third party software ("Redistributable Code") that is licensed to Scala for redistribution with the Scala Software. The Redistributable Code is the property of Scala's licensors, and protected under United States and international copyright, trade secret or other proprietary rights laws, as well as international treaties. Licensee is hereby granted a limited, non-exclusive, non-sublicensable and nontransferable right and license to use and display the Redistributable Code solely in connection with the authorized operation and use of the Scala Software by Licensee and in conformance with the terms and conditions of this Agreement. Except as expressly permitted under applicable law, Licensee may not reproduce, redistribute, decompile, reverse engineer or disassemble the Redistributable Code, and may not disintegrate the Redistributable Code from the Scala Software.

4. LICENSE AND OTHER FEES

(a) **Upgrade Pricing**. Upgrade Edition pricing is only available to licensee's eligible previous versions of specified Scala Software Products as specified in this Section 4(a):

(i) IC Player 3: Upgrade pricing is only available to licensees of InfoChannel® IC100 Player for Microsoft Windows and InfoChannel®IC200 Player for Microsoft Windows products.

(ii) IC Network Manager 3: Upgrade pricing is only available to licensees of InfoChannel® IC100 Master for Microsoft Windows and InfoChannel® IC200 Master for Microsoft Windows products.

(iii) IC Designer 3: Upgrade pricing is only available to licensees of InfoChannel® Designer, InfoChannel® IC100 Master for Microsoft Windows and InfoChannel® IC200 Master for Microsoft Windows products.

(iv) If Licensee has acquired the Scala Software as an Upgrade Edition, Licensee must within sixty (60) days of installation of the Upgrade Edition of the Scala Software, return to Scala, at the address set forth below, the copy-protect dongle provided with the Eligible Previous Software along with the product warranty/registration card provided with the Scala Software. Failure to return the dongle to Scala as provided in this Section 4(a) shall void the licenses granted and any warranty provided hereunder. In the event that Licensee is found to have installed and/or used an Upgrade Edition in violation of the terms of this Section 4(a), such use shall be deemed a material breach hereof, and Licensee shall immediately either (i) pay the difference between the Upgrade Edition fee and the applicable non-upgrade fee for the Scala Software, or (ii) immediately cease all use of the Scala Software, and return the software in accordance with the provisions of Section 9(c) hereunder.

(v) Scala reserves the right to modify the list of eligible previous versions of the Scala Software and/or the Upgrade Editions associated with such eligible previous versions of the Scala Software. Stickers affixed to the Scala Software product packaging shall set forth the applicable Upgrade Edition restrictions. In the event of a conflict between this Agreement and a valid sticker affixed to the appropriate Scala Software packaging, the Upgrade Edition restrictions set forth in the product packaging sticker shall prevail (provided the stickers are affixed to the applicable and most recent version of the relevant Scala Software product).

(b) **Scala Plug In (EX)**. EX pricing is only available to licensees of a Scala Software product or Scala Software products with which such extension will be combined, integrated or otherwise used. In the event that Licensee is found to have installed and/or used an EX edition of the Scala Software in violation of the terms of this Section 4(b), such use shall be deemed a material breach hereof, and Licensee shall immediately either (i) acquire a license for the base Scala Software product(s) with which the EX is to be used, or (ii) immediately cease all use of the Scala Software, and return the software in accordance with the provisions of Section 9 hereunder.

(c) Any installation, customization or maintenance services by Scala will be provided under a separate agreement between the parties. Software updates are free of charge in the first year only. Any fees referred to in this or any separate agreement do not include any duties, taxes or handling fees. Whenever imposed, all duties, taxes and handling fees are payable by Licensee. Income or other taxes that are required to be paid or withheld by Licensee or Scala under the laws of jurisdictions other than the United States, in connection with the license and other fees paid by Licensee hereunder, are the sole obligation of Licensee and shall be exclusive of the license and other fees paid by Licensee.

(d) Other Scala Services and Information

(i) As a convenience to its Licensees, Scala provides certain services, materials and information related to the Scala Software to Licensees through Scala's Internet web site (the "Scala Network"). Scala expressly reserves the right to modify, terminate, limit, or alter the Scala Network, the contents thereof, any materials related thereto, or Licensee's access thereto, at any time without notice to Licensee.

(ii) Scala and Licensee expressly agree and acknowledge that:

(1) Any information posted by Licensee on or to the Scala Network, including without limitation information posted during the Scala Software registration procedure, is posted at Licensee's sole risk, and Licensee hereby fully and irrevocably waives any claim, cause of action or other allegation of liability assertable against Scala, its directors, officers or employees, associated with the disclosure of such information;

(2) Scala shall not sell, rent, distribute or otherwise disclose individually identifiable personal information provided to Scala through the Scala Network, or through the Scala Software registration process. Notwithstanding the foregoing, Scala may gather and disclose or distribute in its sole discretion statistics and other information concerning the Scala Software, Scala end user/licensees, the Scala Network, Scala's web sites, their use or any information provided by any users thereof, including without limitation software and configuration, provided that any such publication or distribution will be done only in aggregated form;

(3) Scala may use, grant, license or disclose any aggregated information gathered by or disclosed to Scala as provided above for commercial purposes;

(4) Licensee shall indemnify and hold harmless Scala, its officers, directors, employees, subsidiaries, suppliers and affiliates for any action taken or statement made by Licensee on or in connection with the Scala Network on or in connection with the Scala Network, including, without limitation, any claims of defamation or intellectual property infringement.

5. TITLE; CONFIDENTIALITY

(a) **Title**. Licensee acknowledges that the Scala Software, documentation and any and all upgrades, enhancements, modifications, additions or new releases of or to the Scala Software contain confidential information of, are trade secrets of, and are proprietary to Scala and its licensors and that title to such materials is and shall remain in Scala and its licensors, as the case may be. All applicable rights to patents, copyrights, trademarks and trade secrets in the Scala Software and other proprietary materials are and shall remain in Scala and its licensors. Licensee shall not assert any right, title or interest in the Scala Software or other materials provided to Licensee under this Agreement, except for the rights expressly granted to Licensee hereunder. Licensee shall not obscure or remove any copyright or other proprietary notice or legend contained on or included in the Scala Software and shall reproduce all such information on all copies made hereunder. Licensee shall not, directly or indirectly, disclose or distribute any technical information of Scala provided with or in the Scala Software without the prior written consent of Scala, which consent may be withheld at Scala's sole discretion.

6. WARRANTIES

(a) **Conformity to Specifications**. Scala warrants that the Scala Software will, for a period of ninety (90) days after the date of receipt of the Scala Software by Licensee, operate substantially in accordance with the documentation and specifications set forth in the written materials provided by Scala with the Scala Software. In the event that during this warranty period the Scala Software fails to operate in substantial conformity with the documentation and specifications, Licensee may return the Scala Software to Scala or the Scala Reseller from which the Scala Software was obtained in accordance with the Scala or Scala reseller return policy, as applicable.

(b) If the Scala Software is provided as a trial or evaluation version, the grant of the license to use the Software shall be on an "AS IS" basis and subject to the express limitations of the trial. Unless Licensee shall have entered into a written license agreement prior to the expiration or termination of the trial period, Licensee agrees to cease all use of the Scala Software and to return the Scala Software, or to destroy or permanently delete the Scala Software, Scala Software documentation and all copies thereof.

(c) **SOLE REMEDY**. SCALA AND ITS SUPPLIERS' AND LICENSORS' ENTIRE LIABILITY AND LICENSEE'S EXCLUSIVE REMEDY FOR THE FAILURE OF THE SCALA SOFTWARE TO CONFORM WITH ITS DOCUMENTATION AND SPECIFICATIONS SHALL BE, AT SCALA'S SOLE OPTION: A) RETURN OF THE PRICE PAID BY LICENSEE; OR B) REPAIR OR REPLACEMENT OF SCALA SOFTWARE WHICH IS RETURNED TO SCALA OR A SCALA RESELLER WITH A COPY OF THE INVOICE OR RECEIPT. THIS LIMITED WARRANTY IS VOID IF FAILURE OF THE SOFTWARE RESULTS FROM OR IS RELATED TO THE IMPROPER INSTALLATION OR OPERATION OF THE SCALA SOFTWARE BY OR ON BEHALF OF LICENSEE, THE FAILURE OF LICENSEE'S HARDWARE OR SOFTWARE SYSTEMS (OTHER THAN THE SCALA SOFTWARE) OR INCOMPATIBILITY OF SUCH SYSTEMS WITH THE SCALA SOFTWARE; THE ALTERATION, MODIFICATION OR UNAUTHORIZED INTEGRATION OF THE SCALA SOFTWARE BY OR ON BEHALF OF LICENSEE, OR FROM ACCIDENT, ABUSE, OR MISAPPLICATION. ANY REPLACEMENT SOFTWARE OR HARDWARE WILL BE WARRANTED FOR THE REMAINDER OF THE ORIGINAL WARRANTY AGREEMENT PERIOD (OR FOR THIRTY (30) DAYS, WHICHEVER IS LONGER). OUTSIDE OF THE UNITED STATES AND CANADA, NEITHER OF THESE REMEDIES NOR ANY PRODUCT SUPPORT SERVICES OFFERED BY SCALA ARE AVAILABLE WITHOUT PROOF OF PURCHASE FROM AN AUTHORIZED RESELLER.

7. LIMITATION OF LIABILITY

(a) THE SCALA NETWORK AND ANY INFORMATION PROVIDED THEREIN, WHETHER BY SCALA OR BY ANY THIRD PARTY IS PROVIDED ON AN "AS IS, WHERE IS, AS AVAILABLE" BASIS. SCALA DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF TITLE, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. LICENSEE FOR ITSELF, ITS SUCCESSORS AND ASSIGNS HEREBY DISCHARGES AND RELEASES SCALA, ITS DIRECTORS, OFFICERS, AND EMPLOYEES, FROM ANY LIABILITY FOR ANY INFORMATION PROVIDED IN CONNECTION WITH THE SCALA NETWORK, ANY RELIANCE BY LICENSEE ON SUCH INFORMATION, AND ANY INFORMATION OR MATERIALS POSTED BY THIRD PARTIES TO THE SCALA NETWORK, INCLUDING WITHOUT LIMITATION ANY CLAIMS OF DEFAMATION, INVASION OF PRIVACY, OR MISAPPROPRIATION OR VIOLATION OF ANY LICENSEE INTELLECTUAL PROPERTY RIGHTS.

(b) SCALA'S MAXIMUM LIABILITY TO LICENSEE HEREUNDER SHALL BE LIMITED TO THE AMOUNTS ACTUALLY PAID BY LICENSEE FOR THE SCALA SOFTWARE. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL SCALA OR ITS SUPPLIERS OR LICENSORS BE LIABLE FOR ANY INDIRECT OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SCALA SOFTWARE, EVEN IF SCALA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES/JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

(c) **U.S. Government Restricted Rights**. THE SOFTWARE, HARDWARE AND DOCUMENTATION PROVIDED WITH THIS PRODUCT BEAR RESTRICTED RIGHTS. USE, DUPLICATION, OR DISCLOSURE BY THE GOVERNMENT IS SUBJECT TO RESTRICTIONS AS SET FORTH IN SUBPARAGRAPH (c)(1)(ii) OF THE RIGHTS IN TECHNICAL DATA AND COMPUTER SOFTWARE CLAUSE AT DFARS 252.227-7013 OR SUBPARAGRAPHS (c)(1) AND (2) OF THE COMMERCIAL COMPUTER SOFTWARE RESTRICTED RIGHTS AT 48 CFR 52.277-19, AS APPLICABLE. MANUFACTURER IS SCALA, INC., 1 EAST UWCHLAN AVENUE, EXTON, PENNSYLVANIA 19341 USA.

8. INDEMNIFICATION

(a) **Scala's Obligation**. Subject to the Licensee indemnification set forth at Section 8(b) and the Limitations of Liability set forth in Section 7, Scala will defend, indemnify and hold Licensee harmless against any action brought against Licensee alleging that Licensee's use of the Scala Software as authorized hereunder infringes a United States copyright or patent. However, Scala will not be obligated to indemnify or hold Licensee harmless from any such action unless Licensee notifies Scala in writing of any claim within 10 days after it learns of such a claim, gives Scala sole control of the defense and settlement thereof and provides all reasonable assistance in connection therewith. If any Software is finally adjudged to infringe the intellectual property rights of a third party, or in Scala's opinion is likely to become the subject of an injunction, Scala shall, at its option and expense, either: (i) procure for Licensee the right to continue using the Software; (ii) modify or replace the Scala Software to make it noninfringing; or (iii) refund the fee paid, less reasonable depreciation, upon return of the Scala Software. Scala shall have no liability regarding any infringement claim arising out of: (w) use of the Scala Software in combination with non-Scala software, data or equipment if the infringement was caused by such use or combination; (x) any modification, alteration or derivation of the Scala Software made by or on behalf of Licensee; or (y) Licensee's use of third party software or works of authorship in conjunction with the Scala Software. THE FOREGOING STATES SCALA'S ENTIRE LIABILITY AND LICENSEE'S EXCLUSIVE REMEDY FOR INFRINGEMENT OR CLAIMS OF INFRINGEMENT OF ANY COPYRIGHT, PATENT AND OTHER PROPRIETARY RIGHTS BY THE SOFTWARE.

(b) **Licensee Obligation**. Except for the infringement claims set forth in Section 8(a), Licensee shall indemnify and hold Scala, its directors, officers, agents and employees harmless from any claims, demands, or causes of action whatsoever arising on account of Licensee's modification or enhancement of the Software. Licensee further agrees to indemnify and hold Scala, its directors, officers, agents and employees harmless from any claims, demands, or causes of action whatsoever arising from or related to the display, broadcast, reproduction, performance or other use or distribution of audio, visual, graphical and textual information developed by or on behalf of Licensee and not included in the Scala Software.

9. TERMINATION

(a) **By Licensee**. Licensee may terminate this Agreement at any time without notice to Scala. The license fee is not refundable and Scala will have no obligation to refund any amounts paid by Licensee under this Agreement upon its termination (except for any right of refund as set forth in Section 6). Licensee must cease any use of the Scala Software, and return to Scala or certify to Scala's reasonable satisfaction the destruction or permanent deletion of the Scala Software, and all copies thereof.

(b) **By Scala**. Scala may terminate this Agreement and all licenses granted hereunder upon thirty (30) days' prior written notice if Licensee fails to comply with any of the terms and conditions of this Agreement or any Schedule to this Agreement, and such noncompliance is not cured during within such thirty (30) day period.

(c) **Return of Software**. Upon any termination of this Agreement, Licensee shall return all copies of the Scala Software, in whatever format, together with the documentation and shall delete all copies of the Scala Software from its computer system(s). Licensee must promptly certify to Scala in writing that it has taken all such actions.

10. GENERAL

(a) **Audit Rights**. Scala shall have the right reasonably to audit the deployment and use of the Scala Software by Licensee, including without limitation Licensee's conformance with the provisions of Section 4(a) and 4(b) herein. Licensee agrees to cooperate with Scala's reasonable request for access to Licensee's computer systems to ensure Licensee's adherence with the license terms hereunder.

(b) **Purchase in Canada**. If Licensee acquired this software in Canada, Licensee agrees to the following: The parties hereto have expressly required that the present Agreement and any exhibits hereto be drawn up in the English language. / Les parties aux présentes ont expressément exigé que la présente convention et ses Annexes soient redigées en langue anglaise.

(c) **Notices**. Any notice required or permitted to be given by Licensee hereunder shall be in writing and shall be deemed to have been duly given (i) upon hand delivery, (ii) on the third day following delivery to the U.S. Postal Service as certified mail, return receipt requested and postage prepaid, or (iii) on the first day following delivery to a recognized overnight courier service, fee prepaid and return receipt or other confirmation of delivery requested. Any such notice shall be delivered or sent to Scala at the address as set forth below, or to such other address as Scala may designate from time to time.

SCALA, INC.
1 EAST UWCHLAN AVENUE
EXTON, PENNSYLVANIA 19341 USA

(d) **Governing Law**. This Agreement will be governed by and interpreted in accordance with the laws of the Commonwealth of Pennsylvania, without regard to its conflicts of law principles. In the event that any legal proceedings are commenced with respect to any matter arising under this Agreement, the parties specifically consent and agree that the courts of the Commonwealth of Pennsylvania and/or the Federal Courts located in the Commonwealth of Pennsylvania will have exclusive jurisdiction over each of the parties and over the subject matter of any such proceedings.

(e) **Restricted Rights**. Software acquired with United States Government funds or intended for use within or for any United States federal agency are provided with "Restricted Rights" as defined in DFARS 252.227-7013, Rights in Technical Data and Computer Software and FAR 52.227-14, Rights in Data-General, including Alternate III, as applicable. Scala must be notified in advance of any license grants to United States federal governmental entities. Licensee acknowledges that none of the Software is licensed for use in any nuclear, aviation, mass transit or medical application or in any other inherently dangerous applications.

(f) **Assignment**. Licensee may not assign this Agreement without the prior written consent of Scala. For all purposes under this Agreement, any merger, consolidation, spin-off, acquisition of or change-in-control involving Licensee will be deemed an assignment. Any attempted assignment by Licensee will be invalid.

(g) **Partial Invalidity**. If any provision of this Agreement is held invalid or unenforceable by competent authority, that provision will be construed so as to be limited or reduced to be enforceable to the maximum extent compatible with the law as it shall then appear. The total invalidity or unenforceability of any particular provision of this Agreement will not affect its other provisions and this Agreement will be construed in all respects as if the invalid or unenforceable provision were omitted.

(h) **Waiver**. No failure on the part of Scala to exercise, and no delay in exercising, any of Scala's rights hereunder will operate as a waiver thereof, nor will any single or partial exercise by a party of any right preclude any other or future exercise thereof or the exercise of any other right.

(i) **Entire Agreement**. This Agreement contains the entire understanding of the parties with respect to the transactions contemplated and supersedes any prior agreements or understandings among the parties with respect to the subject matter hereof.

(j) **Foreign Trade Restrictions**. The parties acknowledge that certain information, software technology, accompanying documentation and technical information may be subject to United States export control laws. Licensee shall not directly or indirectly export or re-export the Software in violation of the Export Administration Regulations ("EAR") of the U.S. Department of Commerce, and hereby expressly agrees to defend, hold harmless and indemnify Scala, its directors, officers, and employees, from any claim, suit or dispute alleging that Licensee has exported the Scala Software in violation of the EAR.

(k) **Construction**. The headings in this Agreement are for convenience only. They do not constitute a portion of this Agreement and shall not be used in any construction of it.

(l) **Third Party Beneficiary**. Licensee hereby agrees that the licensors of third party software shall be considered third party beneficiaries of this Agreement and shall be entitled to bring a direct action against Licensee in the event of breach of any applicable provisions of this Agreement, pursuant to the terms and conditions of this Agreement.

INFOCHANNEL 3

Technical Support Options

Scala is committed to providing our clients with excellence in support services. We understand that every customer's support requirements are different and have tailored our support options to accommodate a variety of requirements.

The following options pertain to all InfoChannel 3 products, including InfoChannel Designer 3, Network Manager 3, InfoChannel Player 3, InfoChannel Reporter 3, and all add-on EXes.

Scala Service Plan maintenance agreement - First Year

SUPPORT OPTION	DESCRIPTION	PRICE
Scala Service Plan maintenance agreement	• Covered for 1 Year from date of purchase • Unlimited access to Technical Support • Major and minor software upgrades • Priority response to phone and email • Electronic access to www.scala.com, and Web Discussion message boards	No charge

Scala Service Plan maintenance agreement - Renewal

SUPPORT OPTION	DESCRIPTION	PRICE
Standard	• Electronic access to www.scala.com, and Web Discussion message boards	No charge
Per Incident *	• Unlimited access to Technical Support	$99
Scala Service Plan maintenance agreement	• Covered for 1 Year • Unlimited access to Technical Support • Major and minor software upgrades • Priority response to phone and email • Prorate multiple InfoChannel products to one blanket Maintenance Agreement	Call for pricing

* "Incident" is defined as anything pertaining to a particular problem, question, or request. Any subsequent emails, phone calls, onsite actions pertaining to that incident will be covered under the agreement. Please have credit card information available at time of call.

Please contact your VAR for renewal information.

Scala Support USA: Hours: 8:00 am to 6:00 pm Eastern Standard Time
Phone 888 444-5867

Scala Support Europe: Hours: 9:00 to 17:00 Central European Time
Phone: +31 45 546 6690

Scala Training: Hours: 9:00 am to 6:00 pm Eastern Standard Time
Phone: 1-888-SCALA-96 (722-5296)

Scala VAR Support: Hours: 9:00 am to 6:00 pm Eastern Standard Time
Phone: 888-SCALA-25 (722-5225)

Software Maintenance Agreement

THIS SOFTWARE MAINTENANCE AGREEMENT is made between Scala, Inc. of 1 East Uwchlan Ave., Suite 300, Exton, PA 19341 ("SCALA") and the Customer. SCALA and Customer agree as follows:

1. Definitions

"Commencement Date" means the date referred to in Clause 3;

"Customer" means the end user of the SCALA Software.

"Initial Period" means the twelve (12) calendar months next ensuing after the Commencement Date;

"Related Persons" means and includes any related body corporate of SCALA (as defined in section 50 of the Corporations Law) or any director, secretary, officer or employee, agent or contractor of any of SCALA or its related bodies corporate.

"Software" means the SCALA software licensed to Customer pursuant to a license agreement.

"Software Updates" means bug fixes, documentation improvements and feature additions including all major and minor revisions.

"Software Support" means advice on operating the Software, advice on problems with the Software (given over the telephone or in writing and includes the provision of Software notes by SCALA).

"Software Maintenance" includes the provision of Software Support and Software Updates.

"Support Organization" means SCALA or, at SCALA's option, any person, firm or corporation designated by SCALA in writing at any time during the term hereof to supply Software Maintenance to Customer.

2. Services

Subject to the terms and conditions contained in this Agreement and Customer's payment of the applicable Software Maintenance fees, the Support Organization will provide Software Maintenance to Customer as further described hereunder.

3. Term

The Software Maintenance to be supplied under this Agreement will commence upon installation and delivery of the product and shall remain in force for the Initial Period. The parties may renew this Agreement for additional one (1) year periods (each, a "Renewal Term") upon mutually agreeable terms, provided that Customer indicates its desire to renew the Agreement at least thirty (30) days prior to the end of the Initial Period or a Renewal Term, as applicable.

4. Software Updates

A. Provided that Customer has paid for Software Maintenance, SCALA will deliver to Customer new releases of Software Updates on appropriate computer media or electronically, if and when they become available for general commercial release during the maintenance period for the modules purchased by and being supported for the Customer. A single copy of the Software Updates and pertinent documentation will be sent to the Customer for each affected Software product covered by this Agreement. Customer agrees that, unless otherwise agreed to in writing by SCALA and Customer, the installation and use of any Software Updates shall be governed by the underlying end user license agreement entered into by Customer and SCALA.

B. SCALA or a Support Organization may defer, postpone or withhold Software Maintenance pursuant to this Agreement in the event Customer unreasonably delays installation of any new Software release or upgrade delivered to Customer pursuant to the terms hereunder.

C. Customer acknowledges and agrees that Customer is solely responsible for the acquisition and maintenance of the computer hardware, firmware, telecommunications, and information technology systems necessary to use and operate the Software. The Software documentation includes information regarding recommended Customer hardware and software configurations for operation of the Software, and SCALA and/or the Support Organization may provide advice regarding appropriate operating system(s) configuration for use of the Software. NEITHER SCALA NOR ANY SUPPORT ORGANIZATION SHALL BE RESPONSIBLE FOR CORRECTING ERRORS OR MALFUNCTIONS OF THE SOFTWARE OR SOFTWARE UPGRADES RELATED TO OR ARISING AS A RESULT OF CUSTOMER'S FAILURE TO MAINTAIN COMPUTER SYSTEMS ADEQUATE TO OPERATE THE SOFTWARE, OR CUSTOMER'S USE OR OPERATION OF HARDWARE OR SOFTWARE SYSTEMS THAT ARE INCOMPATIBLE WITH OR DEGRADE THE PERFORMANCE OF THE SOFTWARE.

5. Software Support

A. The Support Organization will provide telephone and/or modem and/or facsimile and/or electronic mail support for problems associated with the routine use and operation of the software. This service is intended for users who have been trained in the Software and is not to be used as a substitute for basic training. The Scala Value Added Reseller ("VAR") shall be the Support Organization for first level Software Support. SCALA shall provide second-level support and shall also provide first-level Software Support in the event the VAR/Support Organization fails or refuses to provide first-level support. If the Software Support staff feels a customer is abusing the Software Support services, SCALA will notify the Customer in writing and suggest appropriate training, on-site assistance or other alternatives to meet the Customer's needs. SCALA reserves the right to qualify all customer sites before accepting an Agreement, and to refuse to provide Software Maintenance Services, or to adjust the fee based on the environment (hardware or operating systems) and/or age of the product(s) and current status of the product(s) respectively.

(i) The Support Organization will diligently investigate problems reported by the Customer. Subject to the exceptions set forth at Sections 4(C) and 6, if the Support Organization determines that the problem is the result of a reproducible error, defect, or malfunction in the supported Software, the Support Organization will make reasonable efforts to correct the problem. A Support Organization representative will provide Customer with a correction, a report/determination that further research is required, or confirmation that the system works per design specifications.

(a) If a reproducible error is not correctable, a Software performance report will be generated and sent to SCALA's engineering group. The correction for the error would be incorporated in the next release or software updates, if possible.

A. Customer is responsible for informing SCALA of the problem severity. Customer is encouraged to call the Support Organization for clarification or uncertainty as regards to Software. More severe problems will be given priority over general questions.

B. The Customer shall provide to the VAR or Support Organization the name and contact information of one (1) representative of Customer who, with SCALA's acknowledgement, shall have access to the Support Organization's telephone advice service. The representative may be changed from time to time by Agreement between the parties. The initial representative shall be as determined by Customer and communicated to the VAR or Support Organization during the Software registration process.

C. All services to be provided under this Agreement shall be provided Monday through Friday, excluding public holidays) between the hours of:

In the U.S.
9:00 a.m. to 6:00 p.m. EST

In Europe
9:00 to 17:00 CET

Service coverage required outside of these hours may be arranged by agreement with the Support Organization.

6. Services Not Covered

The following services are not covered by this Agreement:

A. Maintenance of facilities external to the Software; hardware support; questions regarding hardware installation, support or maintenance, telecommunications systems.

B. Repair or damage resulting from malfunction of electrical power or heating, ventilation and air conditioning; water damage; fire damage; theft; integration of the Software with non-compatible systems or software, misuse or improper use of the Software (including without limitation any use not specifically authorized in the Software license agreement, documentation or manuals); vandalism; civil commotion or war; or any combination thereof.

C. Support or Maintenance Services for altered or modified Software other than that altered or modified by SCALA and/or authorized agents of SCALA; or support versions of Software that have been superseded by a new release (provided that SCALA will continue to support superseded versions for a reasonable period, not to exceed forty-five (45) days, sufficient for Customer to implement the newest version).

D. Supervision of repairs on associated equipment.

7. Customer Responsibilities

A. The Customer must have a valid license to use the Software from SCALA and be in material compliance with the terms and conditions of such license.

B. The Customer must be current in its payment obligations under this Agreement.

C. The Customer shall notify the Support Organization of any Software problem together with complete information concerning the failure, as soon as possible after the problem has occurred.

(i) The Customer shall provide as accurate and complete a description as possible to the Support Representative. The customer shall assist in problem resolution by providing copies of reports and/or files deemed necessary by the Support Services group.

D. The Customer will provide the Support Organization with the following:

(i) Name of nominated personnel (and their location) who are competent to use the Software;

(ii) Access to the Software and computer(s) on which it resides;

(iii) Adequate working facilities (such as communication devices/modems);

(iv) Access to and use of all information reasonably necessary to service the Software;

(v) The Customer shall be responsible for security of its confidential, proprietary and classified information as well as for the maintenance of adequate backup procedures for files, as SCALA will not be responsible for loss of or altered files, data or programs;

(vi) The Customer agrees to provide a safe and secure installation environment which meets the specified requirements of the computer system(s) on which the Software is running, including without limitation environmental controls, electric supply, service clearances, cable runs and, in the event that the Support Organization agrees to send personnel to the Customer's premises, safety of the Customer's and the Support Organization's personnel; and,

(vii) The Customer agrees to limit use of the Software Maintenance Services that are the subject of this Agreement to occasions when the Software fails to work as set forth in the user manuals or occasions where the user manuals are unclear.

8. Service Charges

A. Annual Maintenance Services for the Initial Period shall be provided without charge to Customer. Thereafter, Customer may elect to renew Maintenance Services for additional annual periods at SCALA's then-current standard annual fee for Maintenance Services. Annual fees may be invoiced thirty (30) days prior to the expiration of the previous period.

B. On-site service shall be provided at the reasonable discretion of the Support Organization. If on-site service is designated by SCALA as required or customer requested of which the Software is located at a distance beyond fifty miles (50 miles) from the Support Organization's office, a travel charge may be assessed by the Support Organization upon notice to and approval of Customer.

9. Changes or Waivers to Software Maintenance Agreement

A. During the term of the Agreement no changes and/or waivers by either party of its rights shall be made to the term and conditions contained herein other than by variation agreed to by authorized representatives of both parties and set forth in a writing duly executed by the parties. The non-enforcement or waiver of any provision of this Agreement on any occasion shall not constitute a waiver of such provision on any other occasions unless expressly so agreed in writing. It is agreed that no use of trade or other regular practice or method of dealing between the parties hereto shall be used to modify, interpret, supplement, or alter in any manner the terms of the Agreement.

B. SCALA has the right to vary the charges made hereunder if the Customer wishes to extend the service hours beyond normal working hours referred to in Clause 5.

C. If both parties agree in writing, additional Software to be supported may be included on this Agreement at a later date. The initial maintenance fee for the cost of supporting the additional Software will be prorated from the new Commencement Date to the original Initial Period or Renewal Term end date. An addendum form (attached) will be used to convey the additional Software to be included under this Agreement. The addendum form will be referred to as the "Addendum Page".

10. Non-Payment

The Support Organization reserves the right to decline to provide Software Maintenance if any amounts invoiced by the Support Organization have not been paid by the Customer as set forth in the customers' approved credit terms.

11. Extraordinary Expenses

The Support Organization reserves the right to charge for unusual or excessive telephone, shipping, handling, media or user manual expenses in connection with the Software Support to be provided hereunder. In all cases, the Support Organization will notify the Customer of these costs in advance.

12. Assignment

Customer may not assign this Agreement to a third party without the prior written consent of SCALA, which consent may be withheld in SCALA'S sole discretion. SCALA may assign or delegate its rights and responsibilities hereunder to a third party Support Organization upon notice to Customer, and may freely assign its rights and obligations hereunder in connection with the merger, acquisition or sale of all or substantially all of the assets of SCALA.

13. Force Majeure

SCALA shall not be responsible or liable for failure to perform or observe, or for delay in performing or observing any obligation under this Agreement where such failure or delay arises from any cause beyond the control of SCALA or the Support Organization (as applicable), including, but not limited to, strikes, lockouts, industrial action, acts of God, insurrection, terrorism, or civil commotion, or any other cause beyond the reasonable control of SCALA or the Support Organization (as applicable).

14. Limited Warranty

SCALA shall perform its services hereunder in a workmanlike manner. In the event that it is established to SCALA's satisfaction that any Software Maintenance or other service carried out by SCALA or a third party Support Organization under this Agreement was defective, Customer's sole remedy shall be the re-performance of such services without cost to the Customer. Notwithstanding the functionality or performance of any addition or release of error corrections, enhancements, or new releases to the Software program(s) in connection with the Maintenance Services, SCALA's obligation to correct errors in such additional releases shall be limited to the maintenance terms of this Agreement. EXCEPT AS EXPRESSLY SET FORTH IN THIS PARAGRAPH, SCALA SHALL HAVE NO LIABILITY FOR THE SOFTWARE OR ANY SERVICES PROVIDED, INCLUDING ANY LIABILITY FOR NEGLIGENCE; SCALA MAKES AND CUSTOMER RECEIVES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, EXCEPT AS EXPLICITLY SET FORTH IN THIS AGREEMENT. SCALA SPECIFICALLY DISCLAIMS ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

15. Limitation of Liability

Laws from time to time in force in the jurisdiction where any services are to be performed hereunder may imply warranties or liabilities which cannot be excluded or which can only be excluded to a limited extent. In which case, SCALA hereby limits its liability to the extent permitted by law. If SCALA cannot exclude or limit any warranty implied by law, this Agreement shall be read and construed subject to such statutory provisions. SCALA'S MAXIMUM LIABILITY TO CUSTOMER HEREUNDER SHALL BE LIMITED TO THE AMOUNTS ACTUALLY PAID BY CUSTOMER FOR THE MAINTENANCE SERVICES. SUBJECT TO THIS CLAUSE UNDER NO CIRCUMSTANCES WILL SCALA OR ITS RELATED PERSONS BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, SPECIAL, PUNITIVE, OR INCIDENTAL DAMAGES, WHETHER FORESEEABLE OR UNFORESEEABLE, BASED ON CLAIMS OF CUSTOMER OR ITS CUSTOMERS, INCLUDING, BUT NOT LIMITED TO, CLAIMS FOR LOSS OF DATA, GOODWILL, PROFITS, USE OF MONEY OR USE OF THE SOFTWARE, INTERRUPTION IN USE OR AVAILABILITY OF DATA, STOPPAGE OF OTHER WORK OR IMPAIRMENT OF OTHER ASSETS, ARISING OUT OF BREACH OF EXPRESS OR IMPLIED WARRANTY, BREACH OF CONTRACT, MISREPRESENTATION, NEGLIGENCE, STRICT LIABILITY IN TORT OR OTHERWISE, EXCEPT ONLY IN THE CASE OF PERSONAL INJURY WHERE AND TO THE EXTENT THAT APPLICABLE LAW PROHIBITS EXCLUSION OF SUCH LIABILITY. IN NO EVENT WILL THE AGGREGATE LIABILITY WHICH SCALA AND ITS RELATED PERSONS MAY INCUR IN ANY ACTION OR PROCEEDING ARISING OUT OF PERFORMANCE OR NON PERFORMANCE OF THIS AGREEMENT EXCEED THE TOTAL AMOUNT ACTUALLY PAID TO SCALA BY CUSTOMER FOR THE SPECIFIC PRODUCT OR SERVICE THAT DIRECTLY CAUSED THE DAMAGE.

16. Applicable Law

This Agreement shall be governed and construed in accordance with the laws of the Commonwealth of Pennsylvania, without regard to its conflict of laws provisions.

17. Entire Agreement

This Agreement constitutes the entire agreement between the parties in respect of the Maintenance Services and supersede all proposals or prior agreements, whether oral or written, and all other communications between the parties relating to the subject matter hereof.

18. Notices

Any notice permitted or required under this Agreement shall be deemed given if in writing and personally served or sent by pre-paid registered or certified air mail, or by confirmed telex or facsimile, addressed (or as either Party may direct otherwise in writing) to the parties at the addresses provided during the Software registration process, marked for the attention of the Managing Director (in the event the Customer is a company).

Any notice given in accordance with this clause shall be deemed to be received by and served upon the other party on the date such airmail letter would in the ordinary course of post have reached such address or on the date such notice is served or left at the relevant address (as appropriate) and in the case of telex or facsimile shall be deemed to have been served on the day following the date of successful transmission.

19. Severability

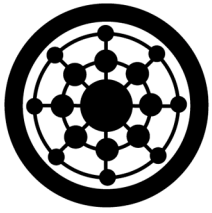
If any term, provision, covenant or condition of this Agreement is held by a court of competent jurisdiction to be invalid, void or unenforceable, it shall be severed herefrom and the remaining provisions of this Agreement will remain in full force and effect and will not be affected, impaired or invalidated.

Customer understands and agrees that the Software Maintenance Agreement fee is non-refundable.

Table of Contents

Introduction to InfoChannel Network Manager

1: Introduction to InfoChannel Network Manager



The next-generation multimedia networking tool from Scala® is called **InfoChannel® Network Manager 3 Enterprise Edition**. With Network Manager, you perform communication tasks to send scripts and multimedia content to InfoChannel Players.

Network Manager is a completely new piece of software designed to function with stability and long-term reliability as the prime goals. At the same time Network Manager is very simple and easy to use.

Communication scheme and network architecture

Network Manager is a separate application, not a part of the Scala authoring software. For optimum performance, a working InfoChannel installation would have Network Manager installed on its own dedicated server. It is possible, however, for Network Manager and Scala's multimedia script authoring application InfoChannel Designer 3 to coexist on the same machine.

In the InfoChannel Designer 3/Network Manager 3 world, scripts and content are *published* to the InfoChannel Network, meaning to a file server defined through Network Manager. Published files are then, in a separate step, transferred to Players using Network Manager.

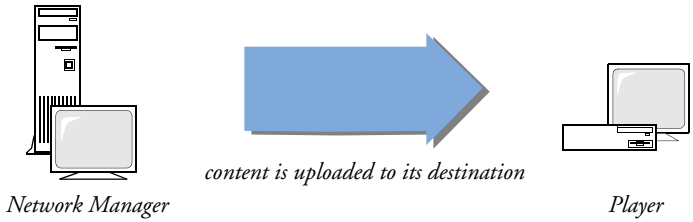
The communications scheme in InfoChannel Networks supports large numbers of Players well. When paired with Scala Broadcast Server 3 software, both point-to-point and broadcast technologies are supported, to cover installations ranging from small to global in scale.

In addition, because the InfoChannel Network approach decouples communication, storage, and authoring, you have greater flexibility in allocating resources for the different types of tasks and personnel involved.

Understanding the Network Manager approach

The efficiency of communication with Network Manager comes primarily from the indirect way content gets from the Network Manager

server to the Players. The way we usually talk about it, data is "sent to the Players" in a simple, linear movement of information from source to destination:

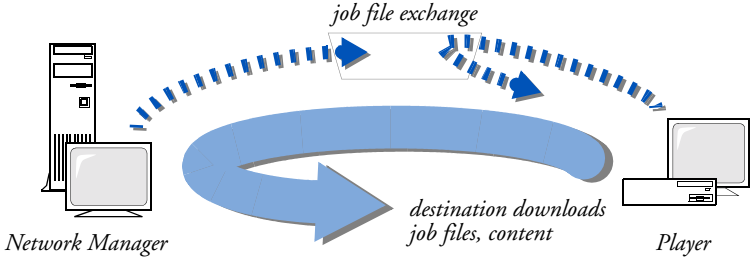


How we think of network data flow

This is how ScalaNet, the networking component in Scala's earlier generations of InfoChannel software, did work. However, although we continue to talk about it using similar terms, and the outward appearance is that it works this way, the actual operation of Network Manager in getting data from source to destination is quite different.

Network Manager does not typically send any content to Players. Instead, Network Manager simply tells the Players what needs to be done—then the Players do all the work.

When you work in Network Manager, you create a "job"—a set of tasks that Players need to perform. Network Manager generates a small "job file" that consists of just the instructions for these tasks, and puts the job file in an intermediate exchange location. Players regularly check the exchange location. When a job file is found they perform the tasks: for example, independently downloading content files specified in the job file.



Actual InfoChannel Network data flow

Although more complex, this indirect scheme is more efficient than simply sending the content directly to the Players.

The sequential, one-Player-at-a-time work that Network Manager needs to do ends with delivering the job files for pickup by the Players. The Players respond to their job files independently, at their own pace, and the Network Manager server can in turn respond to their requests for updated content files more or less simultaneously, in parallel.

The practical result is that solutions using the InfoChannel 3/Network Manager approach scale well to networks with many Players.

The underlying indirect data flow is important to understand only in the planning and configuration stages, or when things are not operating correctly. Diagnosing problems that can occur during configuration and transmission does require the attention of an administrator who understands the actual indirect scheme used in Network Manager.

Terminology

Note that most discussions in this documentation and the terminology within the Network Manager application still talk about communications taking place using the simple conceptual model: we say that Network Manager "sends content to" the Players. This is mainly a matter of convenience and common practice. In a properly set up and functioning installation, the underlying indirect method diagrammed above is invisible to those using it, and it appears that content is simply being sent from Network Manager to the Player.

Robustness and security features

Network Manager has been designed with the utmost in reliability and security in mind, for stable round-the-clock use in a wide range of real-world environments.

- Player health monitoring provides an overview of Player status, warning of Players that are beginning to show errors.

- All activity is logged to logfiles in Network Manager and on each individual Player.
- Players return log files on a daily basis, and log files can be retrieved at any time for up to the minute status history.
- Network Manager uses standard communications protocols (TCP/IP, FTP, UNC).
- Almost all operations automatically retry when communications attempts fail, so that temporary network difficulties do not bring the system to a halt. Retry timeouts are configurable.
- Communication is secured by using password-protected FTP or access-restricted accounts for local connections.
- Transmissions are encrypted and digitally signed to prevent unauthorized access.
- Transmissions use error checking.
- Multiple Network Manager user accounts, with configurable access privileges.
- Back channel allows retrieval of log files, content from Players.
- Players can be rebooted remotely, on schedule.
- Player software can be updated remotely.
- Separate playback and network processes on Players allow continuous playback even during content update.

About this guide

The *InfoChannel Network Manager 3 Enterprise Edition User's Guide* is designed to serve both first-time networked multimedia users and more advanced users in learning how to distribute multimedia productions with Network Manager. It contains a Troubleshooting section, Appendix, Glossary, and an Index.

Conventions

Below are some of the conventions used in this guide.

Convention	Usage
italic text	Aside from general emphasis, we use italics in the text to highlight option names, columns, and other text that appears as labels in the Network Manager menus. Use of italics also indicates terms that are defined in the Glossary.
bold text	Bold text is used for the names of Network Manager menus, wherever they need to be emphasized.
<angle brackets>	Text shown in angle brackets is not to be used literally, but rather indicates places where you must substitute the indicated information, such as a drive letter, share name, or file name. Don't type the angle brackets.

The Glossary and Index

Be sure to consult the Glossary when you come across unfamiliar terms, and the Index when you need to find specific information quickly.

Network Manager resources on the Web

Scala's Web site, `http://www.scala.com`, is an important resource for Network Manager customers, dealers, and VARs.

For answers to questions you can't find in the User's Guide, as well as downloads and additional information relevant to Network Manager users, the Scala Web site should be your first stop.

Pages you will find at the Scala Web site provide:

- General product information, press releases, contact data
- Technical support:
  - ❖ Registration
  - ❖ Tutorials
  - ❖ Troubleshooting FAQs
  - ❖ Problem report submission
  - ❖ Discussion groups
  - ❖ Recommended hardware configurations
- Downloads:
  - ❖ Software updates and demos
  - ❖ Additional documentation on EXes and ScalaScript
- VAR resources:
  - ❖ Sales and marketing information
  - ❖ Service packs
  - ❖ Technical support and training
- Customer case studies
- Third-party support links

Installation

2: Installation

If your InfoChannel Network installation does not consist of preconfigured machines with the software already installed, use the installation instructions in this chapter. It covers installing both Microsoft® Windows® operating system components and Scala InfoChannel 3 components.

Network Manager, InfoChannel Designer, and InfoChannel Player software have a set of built in defaults that allow you to set up a simple, working InfoChannel Network with a minimum of effort.

For these defaults to work correctly, you need to have performed your initial installation according to the instructions in this guide. These direct you to install all three software items—Network Manager, ICDesigner, and ICPlayer software—on the same physical machine.

Even though you will ultimately be installing the ICPlayer software on at least one separate machine, and possibly installing ICDesigner on still another machine, starting out this way is recommended. It will allow you to go through the setup process with a virtual guarantee that a working "starter" network will result.

Once you have gone through the process of setting up the default system and seeing it work, you will be in an ideal position to then expand and customize it into the InfoChannel Network you are planning.

Installation of Microsoft software

Scala InfoChannel Network Manager 3 Enterprise Edition requires Microsoft Windows 2000 or better. You should install Network Manager on a machine running Windows 2000 Professional or Windows 2000 Server (SP2 or higher).

Preliminary steps

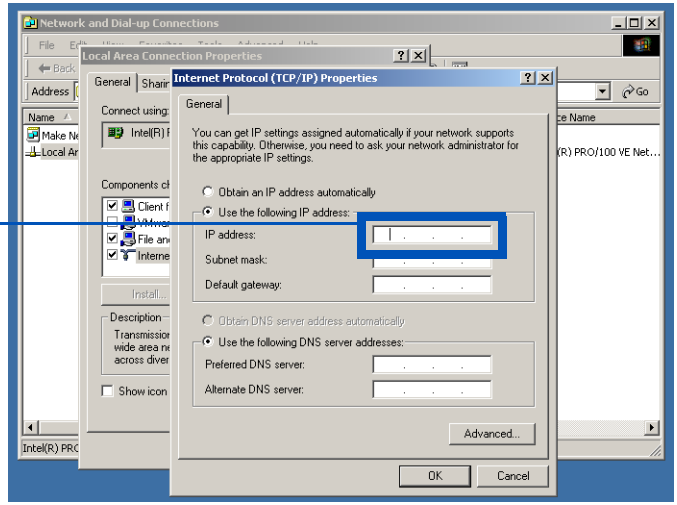
Although it is not strictly required, all instructions in this manual assume that you will dedicate a machine to Network Manager use. **We recommend a clean installation of Windows 2000 Professional or**

Windows 2000 Server on an NTFS 5 partition. (NTFS 5 enables permissions to be set on files and folders, which is an important capability for securing your installation.) So prepare an appropriate machine and create an NTFS 5 partition on it suitable for installation of the Windows operating system.

Windows Step 1: Install Windows 2000

1. Install Windows 2000 from the Microsoft Windows 2000 CD in its basic configuration. Refer to your Windows documentation for specific instructions.
2. After the installation is finished, you need to assign an IP address to the machine.
   a. Right-click on My Network Places and choose *Properties*.
   b. In the list, right-click on *Local Area Connection* and choose *Properties*.
   c. In the Local Area Connection Properties dialog, double-click *Internet Protocol (TCP/IP)*.
   d. In the resulting Properties dialog, enter the IP address for the machine in the *IP address:* box.

enter Network Manager machine's IP address



To ensure correct connectivity to the Network Manager server, the use of either "static" IP/DNS association or DDNS (DHCP-DNS "dynamic domain name server") assignments with long (99-year) leases is advised.

There are various other network-related settings here. Your system administrator will need to make sure all are set up appropriately for your particular network.

Windows Step 2: Install IIS

After the basic Windows 2000 installation, and before installing Network Manager, you need to add IIS (Internet Information Services) 5.0. This may require your Windows 2000 CD, so it's a good idea to keep it in the drive.

1. From the Start menu, choose *Settings* > *Control Panel*.
2. Choose *Add/Remove Programs*.
3. In the Add/Remove Programs dialog, click the *Add/Remove Windows Components* button on the left hand side of the dialog. This opens the Windows Components Wizard.
4. Using the Wizard, add the following items:
   - ❖ Internet Information Services (the HTTP service is required to run Network Manager; enable FTP only if you intend to use the IIS FTP server)
   - ❖ Management and Monitoring Tools
   - ❖ Networking Services
   - ❖ Script Debugger
5. To finish the installation, you need to reboot Windows.

Windows Step 3: Install service packs

After Windows has rebooted, you need to apply Windows 2000 Service Pack 2 or higher. SP 2 can be installed either using the Windows

Update shortcut available from the Start menu, or by downloading it directly from Microsoft:

http://www.microsoft.com/windows2000/downloads/servicepacks/sp2/default.asp

1. Apply the service pack.
2. Reboot Windows again.

Windows Step 4: Update Internet Explorer

After installing Windows 2000 and the service packs, it's time to update Internet Explorer to 5.5 Service Pack 2 or better.

Again, you can update IE either by using the Windows Update shortcut from the Start menu, or by downloading SP2 directly from Microsoft:

http://www.microsoft.com/windows/ie/downloads/recommended/ie55sp2/default.asp

1. Apply IE 5.5 Service Pack 2.
2. Reboot Windows again.

Windows Step 5: Apply security patches

After you have updated Internet Explorer 5.5 to SP2 or better, you need to apply the security patches. It is recommended that you obtain them using the Windows Update shortcut in your Start menu, as it lets you install most if not all the critical and recommended patches at once.

If you prefer to obtain the patches separately, go to the following sites:

Windows 2000 patch locations

http://www.microsoft.com/windows2000/downloads/critical/default.asp

http://www.microsoft.com/windows2000/downloads/security/default.asp

http://www.microsoft.com/windows2000/downloads/recommended/default.asp

Internet Explorer patch locations

http://www.microsoft.com/windows/ie/downloads/critical/default.asp

http://www.microsoft.com/windows/ie/downloads/recommended/default.asp

(Note that not all the downloads available at these locations will apply to the installed version of Windows 2000 or Internet Explorer.)

1. Install Windows 2000 security patches.
2. Install Internet Explorer security patches.
3. Reboot Windows again.

Windows Step 6: Install XML parser

Because Network Manager's communication with Players involves XML files, software to work with XML is required. After the security patches are applied, and the computer has rebooted, install the XML parser from Microsoft, MSXML version 3.0, SP 1 or better.

At the time of this writing, the XML parser could be obtained from this location:

http://msdn.microsoft.com/downloads/default.asp?url=/downloads/sample.asp?url=/MSDN-FILES/027/001/772/msdncompositedoc.xml

We suggest that you retain the installation file for the XML parser because InfoChannel Network Manager 3, InfoChannel Designer 3, and InfoChannel Player 3 all require it.

Windows Step 7: Review device driver certification

Scala strongly recommends that all InfoChannel-related systems be configured with the most current WHQL-certified device drivers. This is necessary for stability of the FTP server and Network Manager.

Security notes

In this time of rampant computer viruses, the installation of a virus scanner on every machine on your network is becoming a necessity rather than an option. Viruses can be spread to Web servers by exploiting security flaws in Windows 2000 and by other means. It is crucial to keep your Web server and all other machines in your installation up to date with:

- all security patches regarding Windows 2000
- virus scanning software

Patches, service packs, and installation order

Note that the *order* in which you perform installation steps is significant. Almost all security patches can be overwritten if you update something in the Windows 2000 installation. For example, suppose you took the following steps:

a. Installed Windows 2000 and IIS (without service packs) from CD-ROM.

b. Applied all security patches for Windows 2000 and IIS.

c. Applied Windows 2000 SP2.

If you followed these steps, you would *remove* the security patches applied in step (b).

Keep in mind that security patches tend to be released more often than service packs. Therefore it is not safe to assume that a given service pack contains all current patches—a patch may have been released after the most recent service pack.

So be careful when changing the Windows 2000 configuration, and diligent when applying security patches and virus scanner updates.

Installation of InfoChannel Network Manager 3

Make sure that the above steps have been completed before installing Network Manager. When they have been completed, you can then run the installer for Network Manager.

The installation process is extremely simple.

- It prompts you for an installation folder, which you may change from its default if desired.
- It asks whether you want to have the Network Manager Engine run automatically when Windows starts, which is recommended.
- It asks whether you want to install the Network Manager web at the root of the system's web server. This is recommended. If you prefer a different location, you are prompted for a folder name.
- It recommends the Internet Explorer updates and security patches discussed above, so if you followed those steps, you can ignore the installer's recommendation to use Windows Update.

Installation of InfoChannel Player 3 software

An InfoChannel Player machine requires the same installation of Windows 2000 and service packs as described for the Network Manager machine at the beginning of this chapter.

Once the installation of Microsoft software is complete on the Player machine, it is possible to install the InfoChannel Player 3 software. The InfoChannel Player 3 software is sold separately from Network Manager. You install it using the installer on the CD-ROM that comes in the InfoChannel Player 3 package.

The installation process for the InfoChannel Player 3 software is also extremely simple.

- The Player software installer prompts you for an installation folder, which you may change from its default if desired.

- It also asks whether you want to have the InfoChannel Player Engine run automatically when Windows starts, which is recommended if the machine you are installing to will be a dedicated Player machine.

When all software has been copied to the Player machine, the installer asks whether you want to configure the Player. If you leave the option on, the InfoChannel Player Configuration utility runs when you click *Finish.*

If you have not already configured Network Manager and defined Players there, however, you may wish to run the Player Configuration utility later. Completing the Player configuration requires knowing the Player's job folder location, which is generally determined during the Network Manager configuration process.

Configuring an InfoChannel Player is covered in chapter 8 of this guide. The same information is also contained in the *InfoChannel Player 3 Setup Guide* booklet included in each Player box.

You can re-run the Player Configuration utility at any time by choosing *InfoChannel Player 3* > *Configure InfoChannel Player 3* from the Player machine's Start menu.

Overview of InfoChannel Network Manager

3: Overview of InfoChannel Network Manager

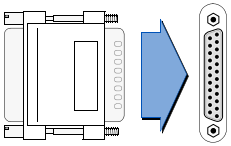
Scala InfoChannel Network Manager Enterprise Edition is an application that makes it possible for you to set up and maintain an InfoChannel Network of any size and complexity.

This chapter introduces the basic operation of the Network Manager user interface and offers guidance on choosing a network topology and layout that will be appropriate for your uses.

Starting Network Manager

Once the installation process is complete, you should log out of the Administrator account under which you installed the software, and log back in to Windows 2000 using the account under which you will be operating Network Manager.

If you have not inserted the Scala Key for Network Manager in the machine's parallel or USB port, do so. Without the Key inserted, Network Manager will not run.



Scala Key – Parallel port

Scala Key – USB port

Then you can start Network Manager. There are two steps to this: starting the Network Manager Engine, and starting the Network Manager application itself, which provides the user interface.

The Network Manager installer offers to automatically start the Engine when Windows boots, so it may already be running. If it is not, you can run it from the Start menu.

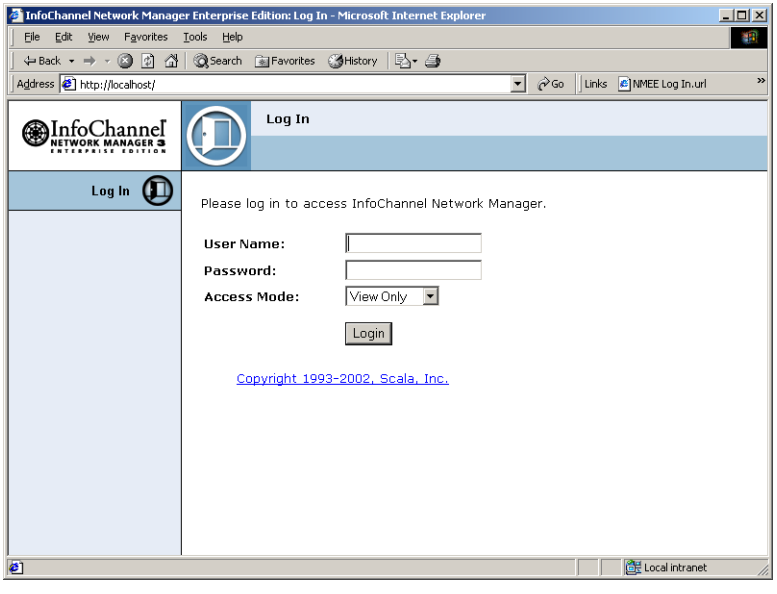
1. From the Start menu, choose *Programs > Scala InfoChannel Network Manager 3 Enterprise Edition> Start InfoChannel Network Manager 3 Enterprise Edition Engine*. The Network Manager

Engine runs continuously in the background, handling communications with the Players. It it thus generally left running at all times. (The Engine is not a Windows service; it must be run from a logged-in User account.)

When the Engine is running, you see its icon in the System Tray.

2. Start Network Manager itself by choosing *Programs* > *Scala InfoChannel Network Manager 3 Enterprise Edition* > *InfoChannel Network Manager 3 Enterprise Edition* from the Start menu. It provides your user interface for the Engine, allowing you to configure the program, define Players, create jobs, and so on.

Network Manager is now running. You see the **Log In** page.



Local login

The Network Manager Start menu shortcut is simply a Web link to the URL:

```
http://localhost
```

When you choose the shortcut, Internet Explorer starts if it is not already running. If it is running, the IE window is brought to the front. You can also enter the `http://localhost` URL in Internet Explorer manually. This URL, when entered on the local machine on which Network Manager is running, lets you log in to the system without the need to enter a username and password.

You therefore can leave the *User Name:* and *Password:* fields blank on this page when it has been opened using the `http://localhost` URL. Just click the *Log In* button to get to the Network Manager **Home** page.

> **CAUTION**
>
> Because using the "localhost" URL does not require a username and password, the local machine is a critical security point.
>
> In any working installation, the physical Network Manager server must be secured by other means, such as being installed in a locked or closely monitored location. A password-protected screen blanker with a short timeout is recommended.

Remote login

Anyone on a remote machine must run Internet Explorer 5.5 SP2 or better and in the *Address* field enter the Network Manager server machine's HTTP URL. This is the DNS name you entered in Windows Step 1 of the installation process (described on page 27), for example

```
http://netman.scala.com
```

or

```
http://192.168.0.10
```

Entering the Network Manager server machine's HTTP URL opens the Network Manager **Log In** page. There a valid username and password must be entered to get to the Network Manager **Home** page.

Logging out

Log out of Network Manager by clicking the *Log Out* option at the top of the control frame. You are logged out. You see the **Logged Out** page, which has a *Back to Log In* icon in its control frame.

Automatic logout

To help prevent unauthorized access, Network Manager can automatically log a user out if it detects no user activity. The default inactivity timeout is fifteen minutes. You can adjust this time on the **Edit System Settings** page.

There is no immediate evidence that automatic logout has taken place, but after it has, an attempt to manipulate any control on the visible page brings up the **Logged Out** page, with a message indicating that the user was logged out due to inactivity.

The Network Manager interface

When you log in to Network Manager, you see the program's **Home** page taking up most of the screen. The **Home** page contains introductory text, as well as links to Scala on the web. The link to www.scala.com is for our main public web site. The tutorial link takes you to a site dedicated specifically to helping you learn about Network Manager.

Scala strongly recommends using the Tutorial link to view the Network Manager tutorial. Valuable for first-time users and anyone else who needs a better understanding of Network Manager, the tutorial gives an overview of the program and a step-by-step guide to setting up a simple, working InfoChannel Network. This material is continually being updated and expanded with additional resources, so it is worth checking on a regular basis.

click for the Network Manager tutorial site

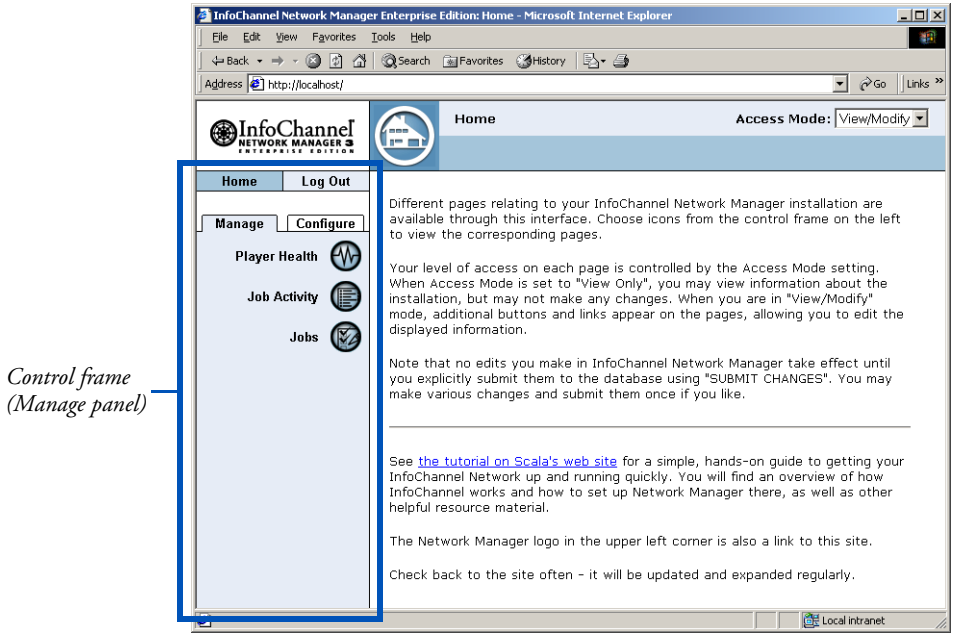
The Network Manager logo in the upper left corner of every page is also a link to the tutorial site, so you can get to it from any place in Network Manager.

How you work in Network Manager

In Network Manager, there are two general modes of work:

- Management: everyday monitoring and update of your Players
- Configuration: tasks required for initial setup and any subsequent changes in your InfoChannel Network

Accordingly, the control frame that runs along the left-hand side of the page has two tab panels, *Manage* and *Configure*. They organize the various functions available in Network Manager.



Control frame (Manage panel)

You first see the *Manage* panel. It has icons for the following pages:

- *Player Health* – displays the status of all the Players in your network, letting you view per-Player operational history and retrieve log files from problem Players (chapter 11)
- *Job Activity* – a continually updated listing of messages noting Network Manager activity (chapter 9)

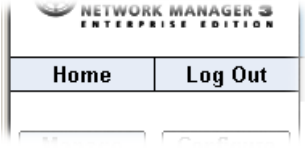
- *Jobs* – lists defined Network Manager jobs and lets you create, schedule, and run jobs (chapter 9)

Clicking the *Configure* tab displays a panel (see page 44 for an illustration) with icons for the following pages:

- *Players* – lists defined Players and lets you define new ones (chapter 7)
- *Publish Locations* – lists defined Publish Locations and lets you define new ones (chapter 6)
- *Broadcasting* – lists defined Broadcast Servers and lets you define new ones (chapter 12)
- *Accounts* – lists defined user accounts and lets you define new ones (chapter 5)
- *System Settings* – lists configuration settings and lets you adjust them (chapter 4)

A single click on any of these choices opens its page.

General remarks about working on these pages can be found in the remainder of this chapter. For more specific information on each subject, see the listed chapters.



The *Home* and *Log Out* options are always available at the top of the control frame.

Access levels in Network Manager

For an application that is accessible via the Internet, it is crucial for security reasons to be able to control who has access to the system. Network Manager has a multi-leveled access scheme, to offer security within a flexible framework.

Network Manager provides three access levels:

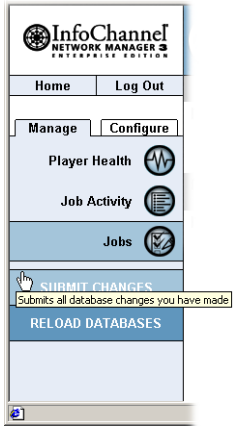
- Administrator – can view and modify any Network Manager database information
- Manager – can view and modify Network Manager database information other than configuration and accounts
- Observer – can only view information

An access level is part of a user account definition. Accounts and access levels are discussed more thoroughly in chapter 5.

Access locking and contacting other users

To prevent confusion and conflicting changes, only one person at a time can be logged in to Network Manager in its "View/Modify" editing mode. Other users can be logged in at the same time, but only in the "View Only" mode, which does not allow any changes to be made.

When someone is logged in to Network Manager in View/Modify mode, that person is said to be "locking" Network Manager—no one else can enter View/Modify mode and make changes. Any other users who log in are put in View Only mode, and cannot change the mode. They see the legend *Locked By:* in the upper right corner of the page, followed by the full name of the user who is currently editing the Network Manager databases.



The full name flashes, and is actually a link. Clicking on the flashing link opens a small dialog that allows a brief instant message requesting access to be sent to the locking user. The locking user can then either log out or switch to View Only mode, allowing the message sender to then switch to View/Modify mode and start working.

Submitting changes to the databases

At times you also see *SUBMIT CHANGES* and *RELOAD DATABASES* choices in the control frame. They appear whenever you have made any changes to information you see on Network Manager pages. Those changes are considered tentative until you choose *SUBMIT CHANGES*, which stores and activates them.

It is not necessary to submit your changes after each individual database change. You can continue to make other changes while the *SUBMIT CHANGES* choice is visible, and submit them all at once when you have finished.

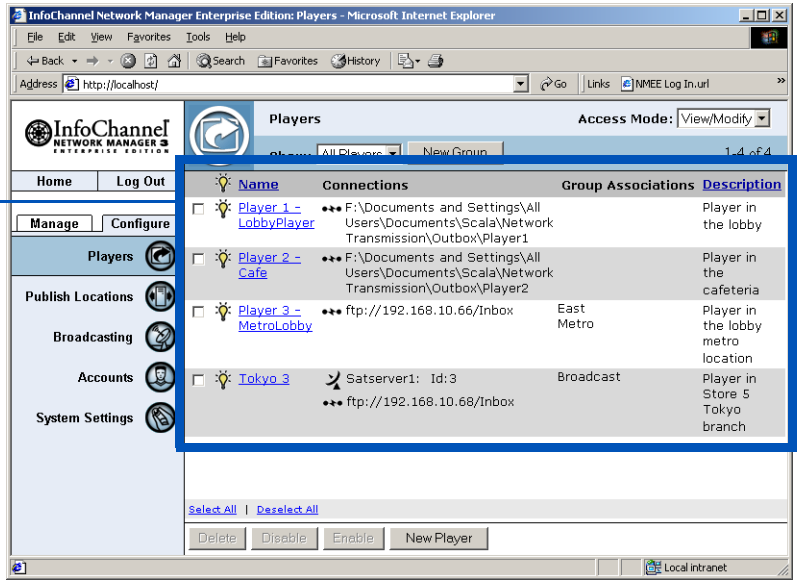
When you submit changes and click *Yes* in the confirmation dialog, the body of the page you are currently in clears, and the message "Working..." appears for several seconds, as the databases are updated. Then the current page is redisplayed.

If you have made changes and decide you don't want to keep them, you can choose *RELOAD DATABASES* to reset the displayed information to its last-submitted state. When you have used either of these two choices, they disappear until the next time any database information has been modified.

Working on Network Manager pages

The Network Manager **Jobs**, **Publish Locations**, **Players**, **Broadcast Servers**, **Player Health** and **Accounts** pages all list items defined in them in a similar table-like format. Each item—job, location, Player, log message or account—appears as a single row on its page, with columns that display information about the item. Alternate rows are

shaded, to help separate the rows. The rows can be sorted by different columns



four items in four columns

At the bottom of each page is a series of buttons for working with items, including *Delete*, *Disable*, *Enable*, and a *New* item button. Certain other controls appear in the page when there are too many items to view all at once.

Working on any of these pages, you use the same basic techniques for selection and editing.

Enabled and disabled items

Any items can be either enabled or disabled. The lightbulb icon to the right of the checkbox indicates an item's current state. A dark lightbulb indicates a disabled item.

Disabled items can still be seen, selected, and worked with just as when they are enabled. Disabling an item only affects what the Network Manager Engine does with it. A disabled job will not run automatically from a time-based or file change trigger. (It can still be run manually.) Disabled Publish Locations cannot have content or files

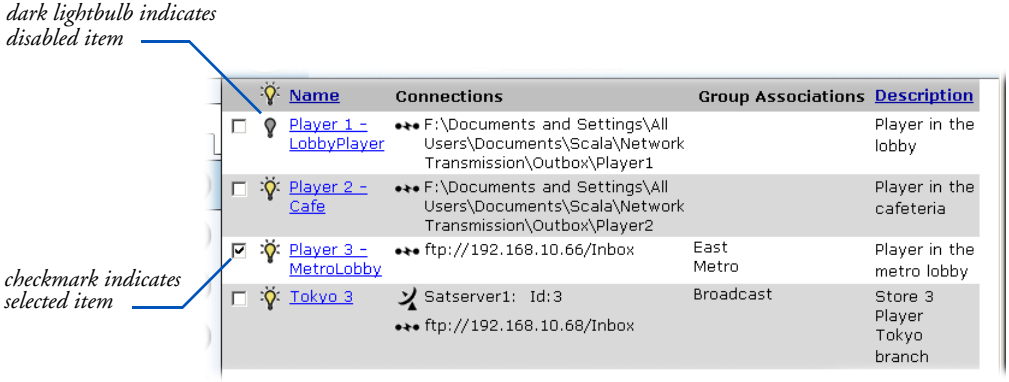
retrieved from them. Disabled Players are not addressed by jobs that reference them. Disabled accounts cannot be used to log in.

To disable an enabled item, select the checkbox next to its yellow lightbulb icon, then click *Disable*.

To enable a disabled item, select the checkbox next to its dark lightbulb icon, then click *Enable*.

Selecting items

To select an item you want to work with, click in the checkbox to the left of the item's name, so that it is marked with a check (✓).



To select all the items on the current page of the list, click the *Select All* link in the bottom left corner of the page.

To clear any selected checkboxes on the page, click the *Deselect All* link.

Editing items

The leftmost column is the *Name* column, and the name for each item is a link (blue, underlined). Clicking the name link opens an edit form for that item that allows you to modify its definition.

Make any changes necessary on the form, then click *OK* to return to the main page.

Whenever you have made a change on an edit form, you see the *SUBMIT CHANGES* and *RELOAD DATABASES* choices appear in the

control frame. The edits you made are visible on the page, but are still tentative. Click *SUBMIT CHANGES* to store your edits in the database. Or, if you have second thoughts about changes you made, click *RELOAD DATABASES* to clear the changes and return to the last stored database values.

In either case, the *SUBMIT CHANGES* and *RELOAD DATABASES* choices disappear from the control frame until the next time you make any edits.

Creating new items

Most of the pages have a button to allow to create a new item: *New Job*, *New Publish Location*, *New Broadcast Server*, *New Player* or *New Account*. Clicking a New button opens an empty form for you to fill in with the appropriate information.

Deleting items you no longer need

If you are sure you will not need an item again, you can delete it. Select it, then click the *Delete* button.

When you submit the change, the item is permanently removed from the database. Note that only the Network Manager database is affected by deletions. Deleting a Player or Publish Location definition has no effect on Player machines or Publish file servers.

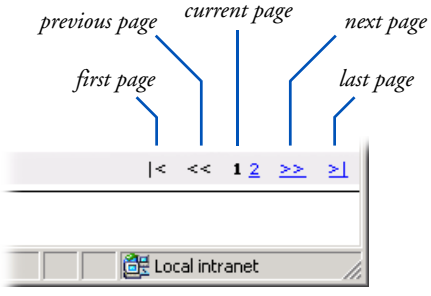
Viewing large amounts of data

When there are too many items to view at once, Network Manager presents items in paged format. A legend in the right-hand side of the page header shows the total number of items, and the range of items currently visible—for example, *11-20 of 27*.

When there are more items than can be seen at once, an *Items/Page* pop-up control appears next to the legend, allowing you to choose how many items should be displayed per page.

controls number of items shown per page

In the bottom right of the page, link-style controls let you page forward and backward through multi-page listings, or choose any arbitrary page to view.



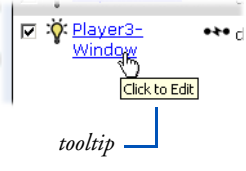
You can also enlarge the Network Manager window to let you see more information at a time. Occasionally it is necessary to make the window wider so you can see all parts of some forms without scrolling.

Sorting items

The listing of rows on most pages can be sorted based on the contents of any one of the columns.

Click any column heading that is displayed as a link to sort the items by that column.

Getting help on features of Network Manager



Virtually everything in Network Manager has a tooltip associated with it for quick help. Just hold the mouse pointer over almost any link, label, or button in Network Manager for a few seconds to see a brief description of what to do with that item.

Configuration steps

If this is the first time you have run Network Manager, there is a certain amount of configuration that needs to be done before you can

start doing useful work with the program. The most logical order of the configuration tasks is:

1. Configure Network Manager itself
2. Define Accounts
3. Define Publish Locations
4. Define Players
5. Configure Player machines
6. Define Jobs

Planning your InfoChannel Network

Before you can configure Network Manager and the Players it will be communicating with, you need to make certain decisions about the layout of your InfoChannel Network. The main topics you need to consider are:

- How these different parts of the Network will communicate with each other—via FTP or via direct folder access
- How the various functions required in an InfoChannel Network (ICDesigner authoring, Publish Location storage, Network Manager, Players) are to be allocated among physical machines
- Whether Players will contact Network Manager to poll for job instructions, or Network Manager will deliver job instructions directly to the Players
- If using a custom FTP link to communicate with Players, whether the FTP host is better located on Network Manager or remotely located

Direct FTP

With Release 6 and beyond of InfoChannel, Scala provides "Direct FTP", a way to dramatically simplify the most time-consuming InfoChannel Network setup task: linking Players to Network Manager.

Direct FTP is the preferred method of setting up an InfoChannel Network for point-to-point connections. The Direct FTP scheme takes advantage of FTP servers that are now built into the Network Manager and ICPlayer software. When you use Direct FTP, many of the decisions discussed in the remainder of this chapter, regarding topology, job folder location, etc., are taken care of automatically by the software. This reduces your labor and the associated chances for error. The only prerequisite for using Direct FTP is that Players must have static IP addresses.

Direct FTP cannot be used in every situation, however. For those cases in which it is not applicable, all the same Player connection options that InfoChannel has offered in the past are still available, as "Custom" connections.

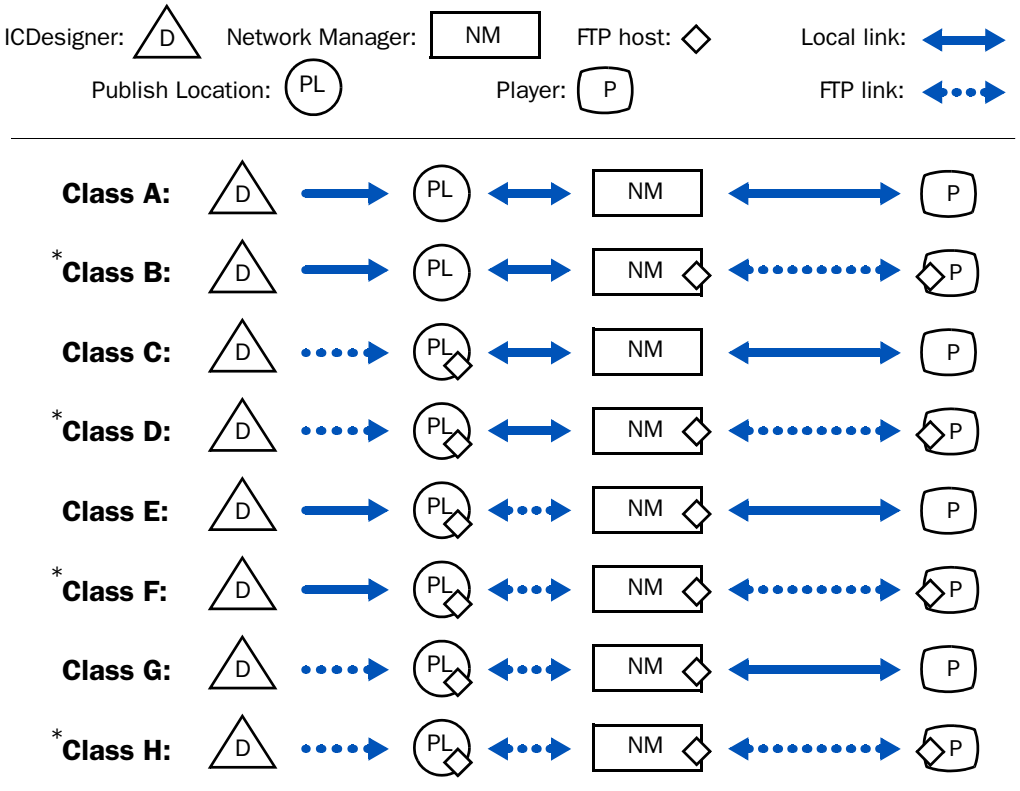
Having these choices gives you great flexibility in network architecture. It also gives you a large set of possible configurations, and thus many decisions to make. This section covers what you need to know to quickly narrow down the possibilities to just those that will apply to your InfoChannel Network.

InfoChannel Network topologies

The diagrams on the next page classify the possible combinations of connection types among the components of a simple, point-to-point InfoChannel Network. (Topologies that include broadcasting are discussed in chapter 12.) This produces a list of topologies that have been given arbitrary "Class" designations of A through L.

This classification is merely a way to illustrate the options involved in the topologies, and to provide convenient labels for discussing certain cases. All of these topologies when properly configured can work well, and function in essentially the same way. The most meaningful differences among them are how you set them up and how well they suit the physical needs/limitations of your planned installation.

To decide which topology is right for your InfoChannel Network, examine your needs and narrow down the list by eliminating what you don't need or can't use.



InfoChannel Network basic topologies

▶ **Recommendation: Ignore topologies that you don't need**

- ❖ If you do not need to use a remote FTP host for your Players, you can ignore the four networks in Classes I–L. (Note that these are just variations of Classes B, D, F, and H.)

  Conversely, if you *do* need to use remote FTP hosting, you do not have to consider Classes A–H. See "*Using a remote workspace*" on page 59 for information on when to use remote FTP hosting.

- ❖ If you cannot connect Network Manager to your Players through a local folder—that is, if the Players cannot be on a LAN with the Network Manager machine—you can ignore the Class A, C, E, and G networks.

  If you *can* connect to the Players through a LAN, you still might prefer Class B, D, F, and H networks if you can use Direct FTP, for its ease of setup.

At this point, it is likely that you have only four remaining options to consider.

▶ **Recommendation: Use Direct FTP and local connections wherever you can**

Communicating through either Direct FTP or local connections is simpler to configure than Custom FTP, and can be more secure as well. Avoid unnecessary configuration by using the topologies that minimize FTP links, such as Class A, B, and I.

Of these, Class B is the only one that lets you use Direct FTP and local connections exclusively, making that topology ideal.

Just these two steps may have allowed you to narrow the list to a single choice.

However, you still need to consider how the components of an InfoChannel Network—ICDesigner, Publish Locations, Network Manager, and Players—are distributed among physical machines.

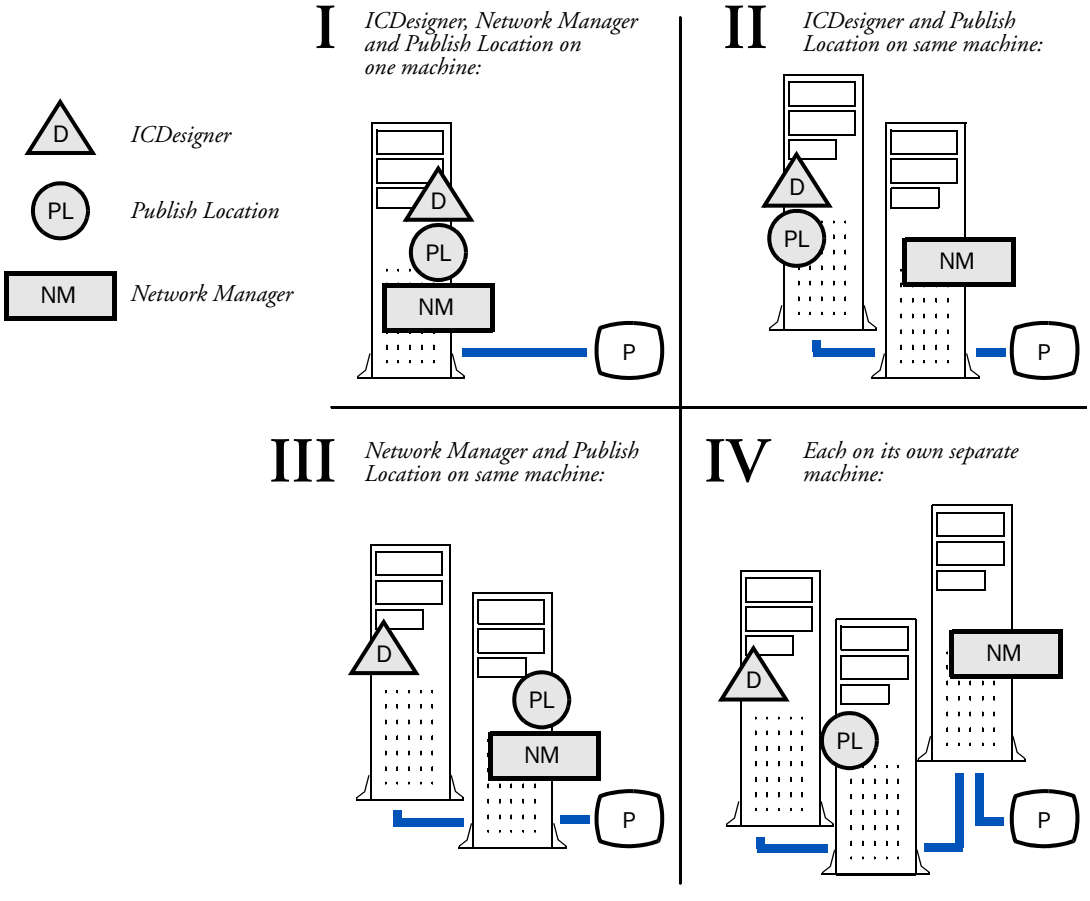
Your requirements in this next step (the "*Machine allocation*" section, below) may help you settle on a topology if you still have more than one choice. Or you may have to reconsider your topology choice.

InfoChannel Network machine allocation

Players are by definition separate machines dedicated to running InfoChannel Player software. The only allocation-related decision you might need to make with relation to Players is whether it would be practical for a given Player machine to drive more than one display device.

This leaves you to consider how ICDesigner, Network Manager and Publish Locations should be arranged. For simplicity assuming a single

ICDesigner installation, a single Publish Location, and a single Player, these are the possible arrangements:



InfoChannel Network machine allocation options

I – Putting ICDesigner, the Publish Location, and Network Manager all on the same machine is obviously the most economical approach, and the simplest to set up. However it is the least flexible, and the computational and disk I/O load placed on the machine by Network Manager and Publish Location operations would make ICDesigner response sluggish.

II – Keeping the Publish Location together with ICDesigner while dedicating a separate machine to Network Manager will allow for quick script publishing and improve certain aspects of network performance, but can still result in occasional sluggish authoring response.

III – Placing the Publish Location together with Network Manager while ICDesigner has its own machine is operationally efficient. It is also more practical when script authors will be working in ICDesigner frequently. It can call for copious hard drive space, as content may end up being stored in both the Publish Location and the Network Manager workspace.

IV – Dedicating separate machines for everything evenly distributes the processing and I/O loads. It is the most flexible approach, but also requires the greatest investment in hardware. Separating the Publish Location from Network Manager is actually less efficient than option III, because an extra communication step is added to the process.

▶ **Recommendation: Most networks should use Option III**

Any of these arrangements can work well. Which one you choose may be based largely on hardware availability and cost.

Generally speaking, option I is appropriate for very small networks, and option III is optimal for nearly all others. Options II and IV offer few advantages over option III, and should be considered only for networks that have some particular need for those configurations.

Job folder location

A factor to consider with Custom connections is the location of the Player job folders. Network Manager communicates with Players through an intermediate message exchange point, known as the *job folder*. Every Player has its own job folder, which it monitors continually for instruction messages ("jobs") from Network Manager.

The actual location of a Player's job folder can be either on the Network Manager machine or on the Player itself. When you use the Direct FTP scheme, Player job folders are on the Players, and their

creation and management is handled automatically. If you decide to use Direct FTP, you never need to concern yourself with them.

If you need to use a Custom scheme, however, you must decide where to locate the job folders.

These are the main factors to consider:

Job folders	Main advantage	Main disadvantage
on Network Manager	ease of setup and monitoring	heavy network traffic from constant Player polling
on Player	rapid Player response to jobs	labor-intensive setup for Custom schemes

Choosing one job folder location or the other does not change the way the InfoChannel Network itself operates. The data flow is exactly the same in either case, and the same functions are accomplished. The operational difference in only in what the Player has to do to monitor its job folder.

The practical differences between the two approaches, however, can have an effect on how you plan your network.

Job folders on Network Manager

When job folders are on Network Manager, the creation of new job folders for additional Players is easy because of their central location. Also, someone at the Network Manager machine can directly observe when job files appear in the job folder on delivery, and see them disappear as they are picked up by a polling Player. Thus verifying whether job file delivery to any Player on the network is working or not is simple.

However, to poll their job folders, Players must reach them across the network at a regular interval. This can result in heavy network traffic with larger numbers of Players. The polling traffic can also be expensive in situations, such as a dial-up installation, in which each access costs something.

A possible trade-off is to specify a long polling interval so that there is less traffic. This also lengthens the average time it takes for Players to respond to delivered jobs.

Job folders on the Player

When job folders are on the individual Players, each folder must be created and set up for accessibility to Network Manager separately, on each physical machine. If the Players are connected by FTP, this requires that each Player also be set up as an FTP server.

Once the Players are in their remote locations, the arrival and pickup of job files in the job folders cannot be observed directly from the Network Manager machine; that part of the InfoChannel communication chain must be verified by indirect means.

Nevertheless, the additional effort in initial setup can be worthwhile. When the job folders are on the Players, the only network traffic related to job delivery occurs when Network Manager actually delivers jobs—relatively infrequently, compared to how often Players would poll over the network to check for jobs.

Polling still does occur in this situation, but is internal to each Player. With no network overhead to consider, polling is fast and can be frequent while incurring no additional cost, so the polling interval is fixed internally at 10 seconds. This allows Players to respond to jobs almost the moment Network Manager sends them.

▶ **Recommendation: Use Direct FTP connections if possible**

Direct FTP locates job folders on the Players. With the FTP servers built in to both Network Manager and ICPlayer software, it is possible to create FTP connections to Players with minimal configuration overhead. Job folder creation—plus the related account creation and security modification tasks—are done automatically for Direct FTP connections.

Even for networks that could use local/shared connections for Player communication (Class A/C/E/G), using Direct FTP is simpler than Custom connections with Shared folders.

In networks that require FTP links but cannot use Direct FTP, however, the choice of job folder location is less clear-cut. The number of Players involved, and whether each polling connection through the FTP link incurs a separate telecommunication cost, are likely to be the deciding factors.

Using FTP

Any machine that will be on the receiving end of an FTP communication link must have FTP server software installed and configured on it. The machines must be connected via TCP/IP links, either directly or over the Internet.

Direct FTP connections

The InfoChannel software includes built-in FTP server software for both the Network Manager and the Player ends of a Direct FTP connection. Using Direct FTP connections automates almost all the configuration tasks associated with FTP communication.

Direct FTP does require static IP addresses for all Players that connect by that method.

Custom FTP connections

For customers who choose not to use Direct FTP, Custom connections are possible. Custom connections require you to manage the installation and configuration of the FTP server, but allow the use of any desired FTP server software.

The FTP service that comes as part of IIS in the Microsoft Windows 2000 and Windows XP operating systems can be used. Alternatively, other third-party FTP server products can also be used.

> ***Network Manager Note***
>
> Under Windows 2000 Professional, IIS allows a maximum of ten simultaneous connections of any kind to a machine.
>
> If you anticipate the possibility of more than ten communication attempts at the same time, you should consider installing Windows 2000 Server or above on that machine.

Managing the workspace

As part of Network Manager configuration for Custom connections, there are settings to be made for specifying the locations of the Network Manager Workspace folder and the Transmission Workspace folder. (The Workspace folders are managed automatically and invisibly for Direct FTP connections, which use the internal FTP server software and appropriate configuration defaults.)

The **Network Manager Workspace** folder is a place locally accessible to the Network Manager server, where Network Manager stores and manipulates all the files it deals with.

The **Transmission Workspace** folder is the place from which Players retrieve content and other files. It is also where Players send log files and any other data to be returned to Network Manager.

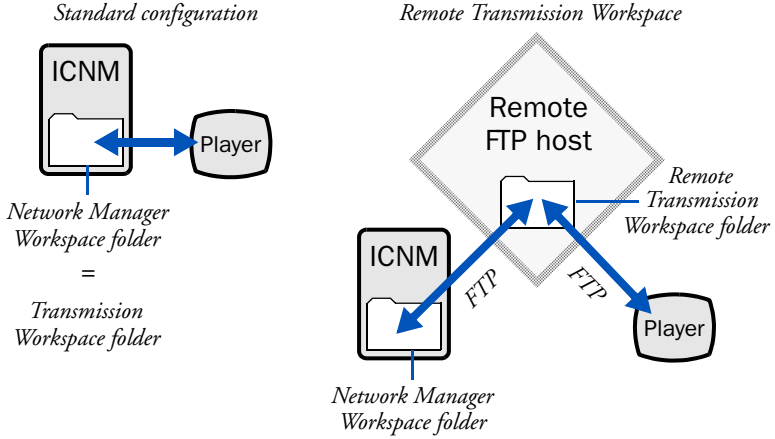
The recommended setup is with these two settings referring to the same location, a folder local to the Network Manager machine. However, it is not required that the two settings be the same. They can refer to different folders, even on different machines, and there are in fact certain situations in which this can be advantageous.

Using a remote workspace

In particular, the relative costs for telecommunication service, Internet storage, and FTP hosting in certain regions—notably in Europe—can make hosting your own FTP site prohibitively expensive. Or you may simply prefer not to have to deal with the other requirements of hosting an FTP site on the Network Manager machine, especially if you must support a large InfoChannel Network.

In such cases, it can be easier and/or more cost effective to use Custom connections and a remote FTP host—that is, a host not located on the Network Manager machine. This host could be a dedicated FTP server elsewhere on the Network Manager's LAN, or one located off-site, provided by a commercial FTP service provider.

To use a remote FTP host, the Transmission Workspace Location is configured to reside on the remote host.



Although the remote transmission folder arrangement can be worthwhile from a cost perspective, it has a significant downside: the "detour" that data must take on its way to the Players increases communication bandwidth requirements.

To use a remote Transmission folder, everything that is in the Workspace folder on the Network Manager machine—which includes all scripts and content going to or coming from all Players—must be

transferred between that Network Manager Workspace folder and the Transmission Workspace folder on the remote FTP site, an extra communication step that is unnecessary when the two folders are the same location. Moreover, the extra step introduces additional points of vulnerability to network security.

For these reasons, using a remote transmission folder/offsite FTP hosting is discouraged unless you find an overriding advantage to doing so.

More complex networks

The preceding diagrams of course illustrate only the most basic possible version of each topology, with one of each component for simplicity's sake. InfoChannel 3 has been designed to be easily expanded and readily adapted to the needs of diverse applications.

Almost any InfoChannel Network will have numerous Players. Multiple ICDesigner systems and Publish Locations in a single network are also supported. Moreover, in most areas you have the flexibility to use mixed topologies that allow you to create quite complex installations.

This manual cannot lay out all the possible combinations, but we can present guidelines for you to use in arriving at a definite layout for your InfoChannel Network concept.

- More units

  Once you understand how an InfoChannel Network functions and have succeeded in getting the simplest case of your preferred topology working, adding additional Players, ICDesigner systems, and Publish Locations should be very straightforward. It is primarily a matter of repeating steps that you have already taken.

  ❖ To add Players, you need to set up the Player in Network Manager and on the Player itself, so that both are linked to the job folder. When not using Direct FTP, you need to create a job folder for each Player.

  Any number of Players is supported, up to your license limit. With large numbers of Players, use Groups to organize them.

- ❖ To add Publish Locations, you need to define them in Network Manager, which simply means providing a network path to a folder that is accessible to both Network Manager and an ICDesigner machine.

  Any number of Publish Locations is supported. You can decide whether to locate them on the Network Manager machine or in other locations connected by FTP on an individual basis.

- ❖ To add ICDesigner machines, make it possible for them to access a Publish Location.

  Any number of ICDesigner stations is supported. Any ICDesigner station can publish to any Publish Locations that it can connect to.

- Mixed connections

  The preceding topology diagrams showed only one type of communication link between any two units. It is in fact possible to use mixed topologies, so that each unit can use the type of communication best suited to it.

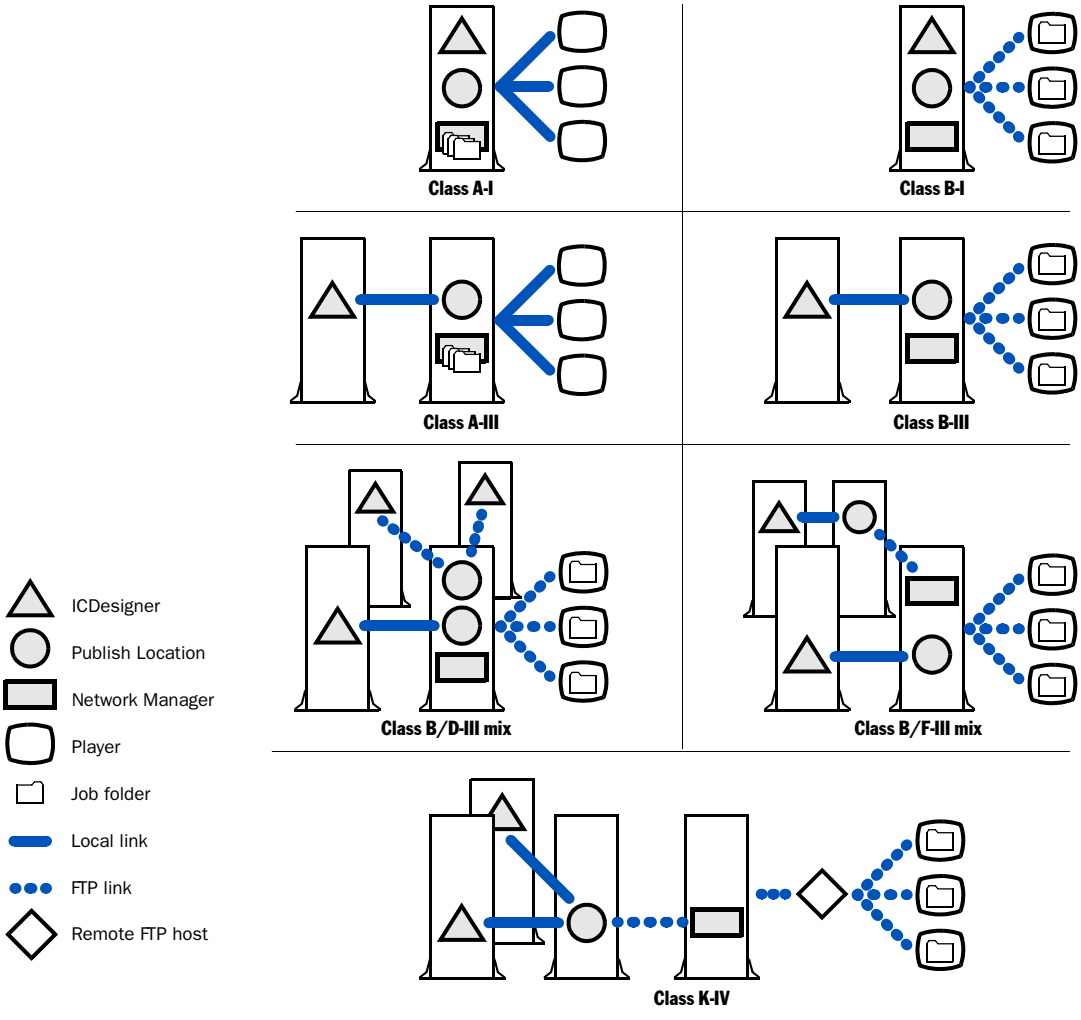
  For example, the default Publish Location set up on the Network Manager machine is a local folder, but you could add other Publish Locations in remote sites that connect using FTP. Similarly, ICDesigner systems that are near a Publish Location would probably publish to them via local connections, but could also publish to remote Publish Locations via FTP.

  In the case of Players, all Players must reach the Transmission Workspace (to send and receive content) using the same type of point-to-point connection. However, with Custom connections they may still have individual connection types to their job folders if necessary.

- Broadcast

  Players also have the option of using broadcast connections. Broadcasting is a special case, and can be used in addition to or

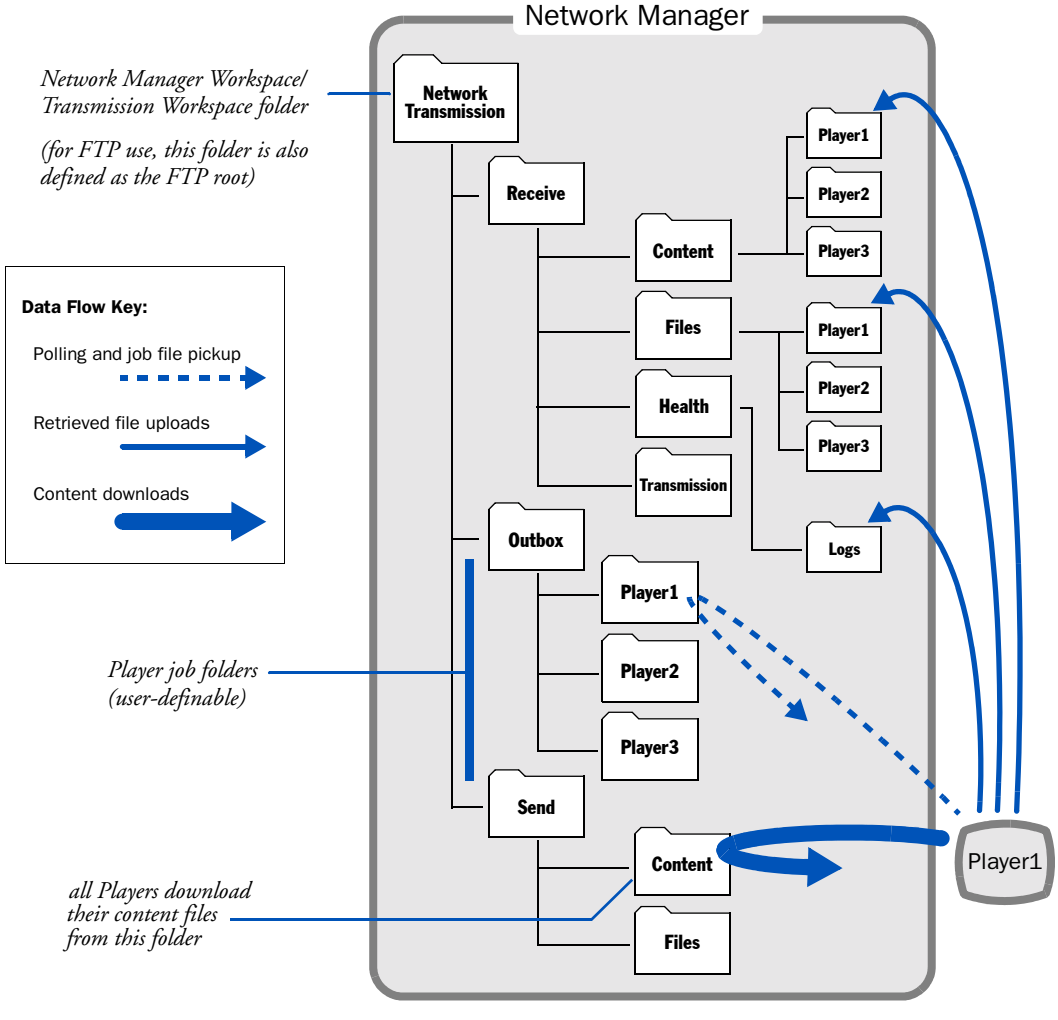
instead of point-to-point connection to Network Manager. Broadcasting is covered in detail in chapter 12 of this manual, and in the User's Guide for the InfoChannel Broadcast Server software, which is sold separately but required for broadcast use.



Some example InfoChannel Network layouts
(see page 49 and page 53 for class designations)

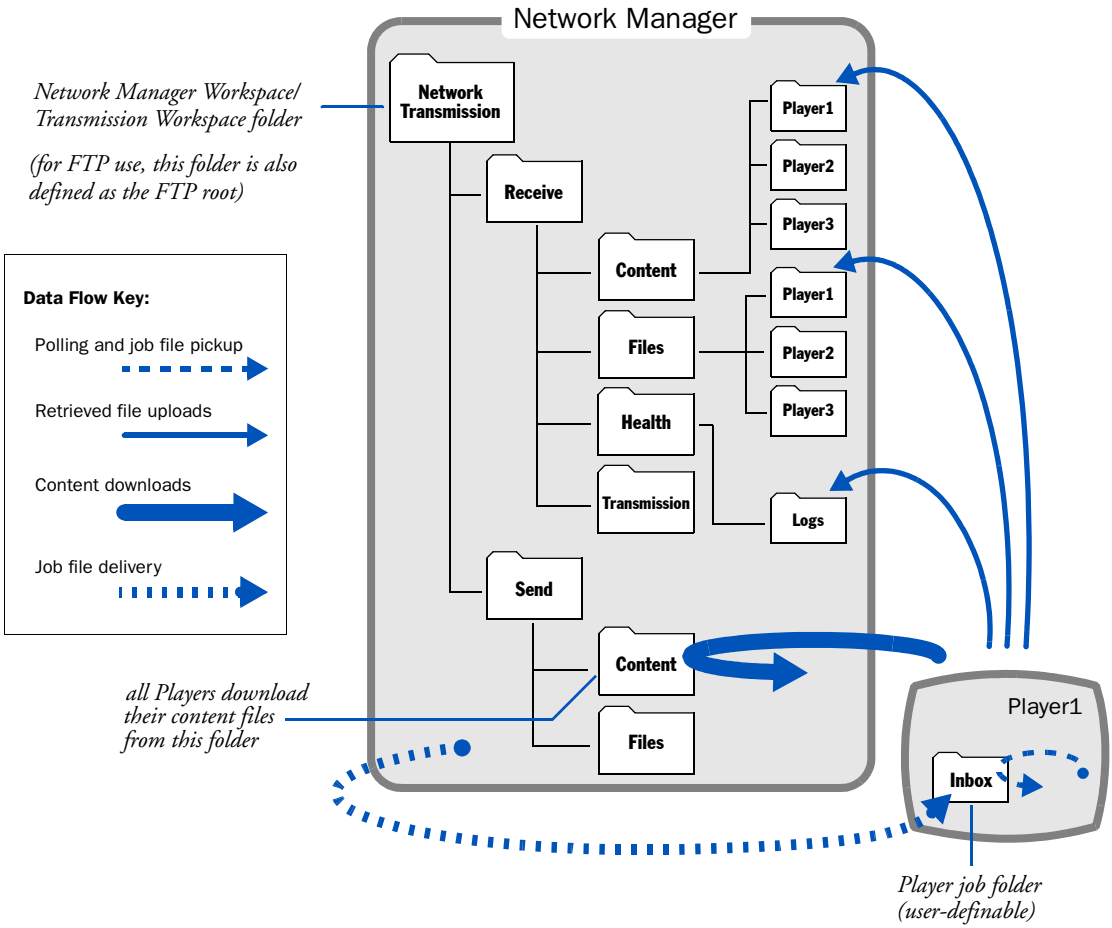
Mapping Network Manager

The following diagram illustrates the folder structure of the Network Manager machine on a typically configured three-Player InfoChannel Network and how a Player named "Player1" interacts with those folders.)



The diagram below illustrates the structure of an InfoChannel Network similar to the one diagrammed on the preceding page but configured with the Player job folders on the Player machines themselves. In this type of installation, Network Manager contacts the Players directly to deliver job files.

This is how an InfoChannel Network using Direct FTP is laid out.



The operation of such a network is really no different from one in which the job folders are on the Network Manager machine. A

Player's job folder is simply created in a place that is local to the Player, and the paths that define the Player are configured accordingly.

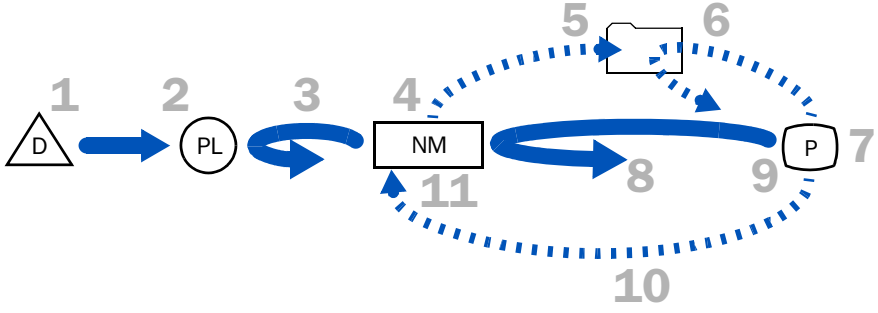
This architecture is extremely easy to set up with Direct FTP. Even when used with an installation based on third-party FTP servers, it can still be preferable for installations in which the network bandwidth and/or dial-up phone line charges incurred by Players polling remote job folders would make operation costs prohibitive.

When job folders are located on the Player, the polling is internal to the Player, so that source of communication traffic is eliminated. The Players' response to new jobs can also be faster: they can poll for job files much more often (every 10 seconds) since there is no bandwidth penalty.

Mapping the data flow

The following sequence of events for a *Send Content* job illustrates the typical communication flow among the various components of an InfoChannel Network:

1. Author publishes to InfoChannel Network from ICDesigner
2. Published script is deposited in Publish Location
3. Network Manager, monitoring Publish Location, copies published script to its workspace



4. A Network Manager *Send Content* job is run, creating a job file specifying the published script
5. Job file is placed in the job folder of Player named in the job
6. Player, polling its job folder, sees the job file and downloads it
7. Player reads the job file, determining required content and content location
8. Player connects with Network Manager, downloads the content from workspace
9. New content is seamlessly swapped in
10. Player generates log entries for the job, uploads them to Network Manager
11. Network Manager displays logged messages on its **Job Activity**, **Player Health** pages

For jobs other than *Send Content*, the fundamental communication operations in steps 4–11 are the same. Steps 8 and 9 would not be present in jobs that do not involve downloading.

Closing InfoChannel Network Manager

When Network Manager is running, you can close the interface portion of the application at any time if you do not need to work with it actively. The Network Manager Engine continues to run unless explicitly stopped, monitoring Publish Locations, running scheduled jobs and handling communication with Players.

Shutting down InfoChannel Network Manager

If you need to shut down Network Manager completely, it is a two-step process, like starting the program. Both Network Manager and the underlying network engine must be stopped.

To shut down the Network Manager application:

1. Exit Network Manager if it is running by clicking the close button in its window's upper right corner.

2. Right-click on the Network Manager icon in the System Tray. This produces a pop-up menu with just one choice, *Stop InfoChannel Network Manager Engine*. Choose this to shut down the network engine.

Any in-progress jobs are aborted by a shutdown.

Network Manager configuration

4: Network Manager configuration

Correct configuration is the key to a smoothly functioning InfoChannel Network.

Thorough planning of the layout and communication pathways of your InfoChannel Network is in turn the key to a smooth configuration process. It will help greatly if you have mapped out the system before you start to configure the Network Manager, Publish Location, and Player machines that make up your network.

Configuring InfoChannel Network Manager

Since InfoChannel Network Manager is Web-based, the machine running it needs to be configured as a Web server using Microsoft's Internet Information Services (IIS). If you are not familiar with configuring a Web server, then you may need the assistance of a Webmaster or IT manager/system administrator. The IIS Web server configuration is not inherently difficult, but it is time-consuming and requires attention to certain critical details.

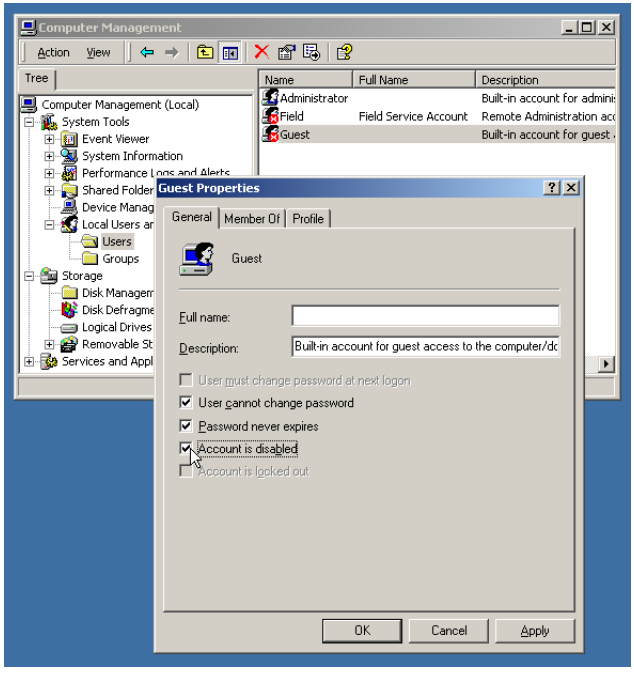
The Network Manager machine must have a static IP address.

Step 1: Disable Guest account

In order for the system to be secure, you need to disable the Guest user account. This is necessary to prevent ignorant or malicious users from gaining access to your FTP or Web server. (Later you will create a new user account that doesn't have Administrator privileges.)

1. From the Start menu, choose *Programs* > *Administrative Tools* > *Computer Management*.
2. On the left-hand side of the Computer Management dialog, expand the *Local users and Groups* tree.
3. Select the *Users* folder.
4. Select the Guest account in the right-hand pane.

5. Choose *Properties* from the *Action* menu.
6. In the Guest Properties dialog, turn on the *Account is disabled* option.



7. Click *OK*.

It is assumed that accounts and appropriate permissions have been set to allow Network Manager and Players to access each other.

Step 2: Delete unnecessary files

Some of the files left by the default IIS installation are unnecessary and could pose a security risk. They should be deleted.

1. Navigate via My Computer or Windows Explorer to the location of your Web site's root directory.
2. Delete the files located in the root directory.

3. Delete the Iissamples and Adminscripts folders in the Inetpub folder.

Step 3: Establish the Web Home Directory

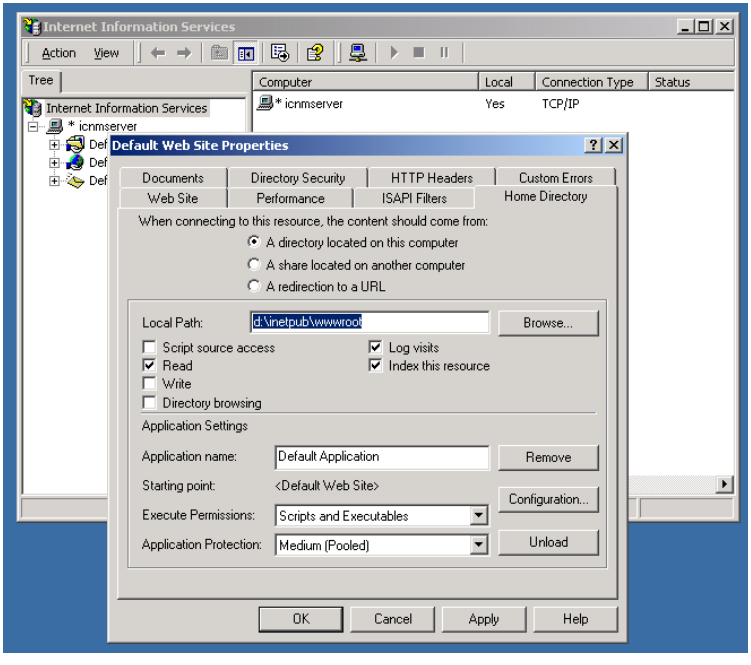
The default home directory for the Web is located at <*systemroot*>\InetPub\wwwroot, where <*systemroot*> is the letter of the drive where Windows is installed.

If you will retain the default, skip to "*Step 4: Configure transmission options*".

However, if for example you want to have the Web Home Directory on a drive different from the Windows drive, you need to change this:

1. From the Start menu, choose *Programs* > *Administrative Tools* > *Internet Services Manager*.
2. Expand the tree on the left-hand side of the Internet Information Services tool so that the *Default Web Site* tree is visible.
3. Right-click on *Default Web Site* and choose *Properties*. You should see the Default Web Site Properties dialog.

4. Select the *Home Directory* tab.



5. Change the path in *Local Path:* to your desired location.

The defaults on the remaining tabs do not need to be changed.

6. Click *OK*.

7. Close the Internet Information Services window.

Step 4: Configure transmission options

1. You need to know the Network Manager machine's static IP host address (or DNS name if you have DNS service on your network). You can retrieve the IP address with these steps:

    a. Open the Computer Management tool from *Start* > *Programs* > *Administrative Tools*.

    b. In Computer Management, open *System Tools* > *System Information* > *Components* > *Network* > *Adapter*.

c. Write down what is listed for *IP Address* in the dialog's right-hand pane.

d. Close Computer Management.

2. Enter the IP address within Network Manager, using these steps:

   a. Run InfoChannel Network Manager.

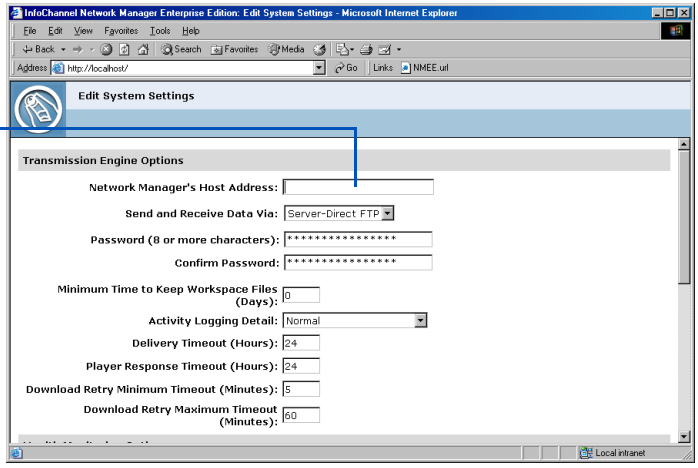
   b. Click the *Configure* tab to display the icons in that panel of the control frame.

   c. Click the *System Settings* icon.

   You see the **System Settings** page, which displays the current settings of its options.

   d. Click the *Edit Settings* button at the bottom of the page to open the following form:

enter Network Manager's IP address or DNS name



   e. Enter the IP address you got from Computer Management in step 1 into the *Network Manager's Host Address:* box.

3. Specify how Network Manager will communicate with Players.

   Scala InfoChannel has FTP server software that is built in to both Network Manager and ICPlayer. Configuration and administration of your InfoChannel Network is greatly simplified by using

this built in "Direct FTP" server software. Using Direct FTP requires that each Player have a static IP address.

Alternatively, if you need to use a particular third-party FTP server, or have other special requirements, you can opt for a custom approach.

- To use the built-in FTP servers, choose *Server-Direct FTP* from the *Send and Receive Data Via:* pop-up.

  The only option you need to set within Network Manager with respect to Server-Direct FTP connection to Players is a password. A randomized default password is provided, which if you leave it will work in your installation, however it is recommended that your choose your own password.

  This is the only place this password is entered. It is not necessary to know it to enter on individual Players.

  a. In the *Password:* box, enter a password that is at least eight characters long. Only asterisks appear.

     Passwords are case-sensitive.

  b. Re-enter the password in the *Confirm Password:* box.

- To use an external FTP server, or access other special configuration settings, choose *Custom* from the *Send and Receive Data Via:* pop-up.

  The other options you see when *Custom* has been selected involve a variety of additional factors related to more specialized InfoChannel Network configurations, and are discussed in the appendix, starting on page 247.

The remaining items in the *Transmission Engine Options* section of the form have default settings that work well for most systems and can be left as is for now.

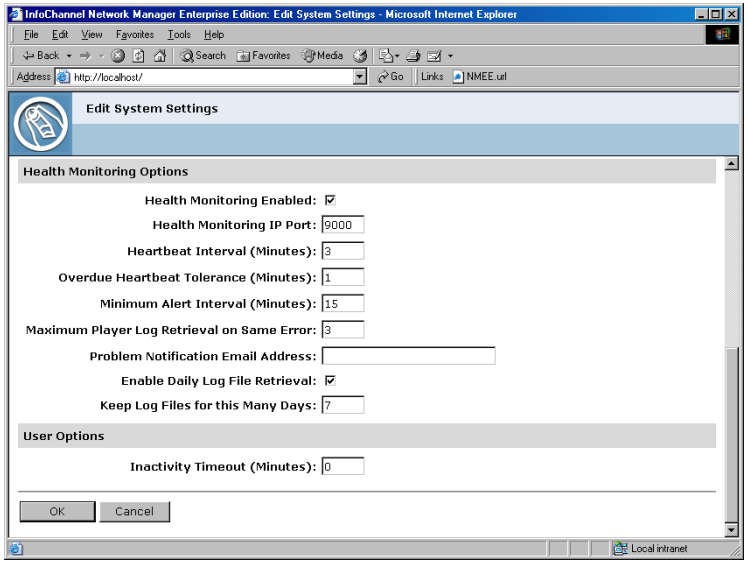
You should not need to adjust them unless and until you need to do some system "tuning".

Step 5: Configure Player Health Monitoring settings

Network Manager's Health Monitoring feature is not enabled by default; it requires certain machine-specific configuration steps before it can begin to operate.

Although using Health Monitoring is not required, it makes maintaining an InfoChannel Network much easier, so it is strongly recommended that you enable and configure it.

1. If it is not already on, turn on the *Health Monitoring Enabled:* option so that the other Health Monitoring options are visible.



2. The *Health Monitoring IP Port:* setting specifies the TCP/IP port at the Network Manager's Host Address through which Health Monitoring messages flow. Leave this setting at its default of 9000 unless you know that this port is being used by another application. Any open port number will do.

> ***Important***
>
> If your network is behind a firewall, the firewall must be configured to allow traffic on the port specified in *Health Monitoring IP Port:*, otherwise Health Monitoring will not function.

3. To receive automatic emails whenever a new problem occurs on a previously healthy network, enter an email address in *Problem Notification Email Address:*. Leaving this field blank disables the automatic email feature.

4. Make sure that *Enable Daily Log File Retrieval:* is turned on so that log files are automatically sent by each Player to Network Manager each night at around midnight.

5. The default setting for *Heartbeat Interval:* of three minutes can be used for general operation of most networks.

   However during initial InfoChannel Network setup, when you are trying to verify communication with your Players and see examples of Health Monitoring feedback, a shorter interval is useful. You might wish to set the interval to one minute so that you can get quicker feedback on configuration changes.

   Be sure to restore the interval setting for daily network operation once you have finished setting up the system.

The remaining items in the *Health Monitoring Options* section of the form have default settings that work well for most systems and can be left as is for now. You should not need to adjust them until and unless you need to do some system "tuning".

See page 182 in chapter 11 for more on Health Monitoring options.

6. Click *OK* to accept your changes on the **Edit System Settings** form.

7. Finally, click the *SUBMIT CHANGES* choice that appears in the control frame. This is what actually stores your changes in the database.

Step 6: Eliminate possible FTP port conflicts

If you intend to use InfoChannel's Direct FTP servers as well as use the FTP server provided by Microsoft's IIS, you need to eliminate a possible conflict with their FTP port numbers. Direct FTP requires exclusive use of TCP/IP port number 21. This is the default port number for the IIS FTP server.

You need to change the IIS FTP port number on any machines that will be using Direct FTP (Network Manager and Players):

1. Open IIS Manager.
2. Open the Properties sheet for the Default FTP Site.
3. On the *FTP Site* panel of the Properties sheet, change the *TCP Port:* setting to some value other than 21.
4. Click *OK*, and close IIS Manager.

If you do not require the IIS FTP server, it is recommended that you disable it on any machine that will use Direct FTP.

Step 7: Set up Publish Locations and Players

Before you can configure individual Player machines, you need to do further setup work within Network Manager to define Publish Locations and Players.

Defining Publish Locations is covered in chapter 6, starting on page 88.

Defining Players is covered in chapter 7, starting on page 96.

Defining accounts

5: Defining accounts

To be able to access InfoChannel Network Manager 3 over the Internet, or from any machine other than the local machine on which the Network Manager software is installed, login to a Network Manager user account is required.

As with any network system, you need to set up accounts that distribute access privileges appropriately, to prevent unauthorized or inadvertent alteration of critical information.

In Network Manager, an account definition consists of a username, a password, an email address, and an access level.

Note that there is no direct connection between Network Manager user accounts and Windows user accounts. They are independent. To prevent confusion, we recommend that you do not duplicate usernames and passwords between Network Manager and Windows user accounts.

Access levels

Network Manager provides three access levels:

- Administrator

  Someone with an Administrator account in Network Manager can view and modify any Network Manager database information. All Network Manager pages are available, and the access mode can be switched between *View/Modify* and *View Only* at any time.

- Manager

  Someone with a Manager account in Network Manager can view and modify most Network Manager information, but cannot edit or view configuration settings or accounts. The icons for the **System Settings** and **User Accounts** pages do not appear in the con-

trol frame for Managers. The access mode can be switched between *View/Modify* and *View Only* at any time.

- Observer

  Someone with an Observer account in Network Manager can only view information. The icons for the **System Settings** and **User Accounts** pages do not appear in the control frame for Observers. The *Access Mode:* control also does not appear. All pages are implicitly in *View Only* mode—there are no action buttons or links to editing pages.

Using the Access Mode control

The *Access Mode:* pop-up on **Log In** page and in the header bar of most other pages provides the choices *View/Modify* and *View Only*.

This control is necessary to allow several users to be logged in to Network Manager at once. Because only one user may edit information at a time, there must be a way for other logged in users to adjust their access levels so that only one can actually be able to edit the databases at a given moment.

The *Access Mode:* pop-up makes it possible for a Manager or Administrator who is working in Network Manager to relinquish control to another user who needs to edit the databases, by switching to *View Only* mode. In *View Only* mode, the *Delete*, *Enable*, *Disable*, and *New* item buttons disappear, and the links in the *Name* column that open an item's **Edit** form become plain text. All database information can still be viewed, but the only controls that remain are those that have no potential to affect the databases.

When the other user finishes editing and either logs out or switches to *View Only* mode, another user can switch to *View/Modify* mode.

While someone is using Network Manager in *View/Modify* mode, any other Manager or Administrator who logs in is automatically put in *View Only* mode, even if he or she specified *View/Modify* on the **Log In** page. The message *Locked By: <username>* appears in the page header to inform anyone else of the reason that edit access is currently denied.

Using the instant messaging feature

Network Manager provides an instant messaging feature to make it easier for users who are locked out to contact the locking user and request access.

To request access or send any other message to another logged-in Network Manager user:

1. Click the locking user's username shown after *Locked By:* to open an instant message window.
2. Type your message in the window.

   The prompts in the window identify your messages and the other user's responses by their full name. Any other Network Manager users who may be currently logged in or who log in while you are messaging are also identified.
3. Click *Send* to send your message.

   An instant message window opens on the other user's screen showing your message. You can message back and forth as long as you like.
4. When you are finished messaging, click *Exit Chat*.

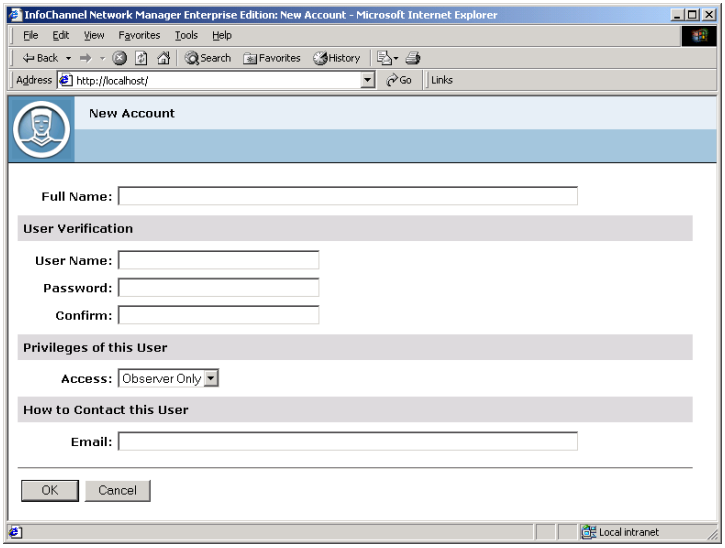
Creating an account

To create an account:

1. Click the *Accounts* icon in the control frame.

   You see the **User Accounts** page. Normally all user accounts that have been created for this system are listed here. Initially it is blank.

2. Click the *New Account* button. You see the **New Account** form:



3. Enter the indicated information in the form, which has the following fields:

   a. *Full Name:* – Enter the user's full name. The name you enter must be unique.

   b. *User Name:* – Enter the username that the person would enter on the **Login** page. The name you enter must be unique.

   c. *Password:* – Enter the password for this user.

   d. *Confirm:* – Enter the password again (to ensure you didn't type it wrong).

   e. *Access:* – Choose *Administrator*, *Manager*, or *Observer Only* from the pop-up to set the access level that this user will have when logging into Network Manager.

   f. *Email:* – Enter the email address for this user.

4. Click *OK* to close the form.

You see the **User Accounts** page again with the information you just entered listed. The *Name* column gives what you entered for Full Name as a link, which allows the editing of the user's account information.

The *Email* column gives the email address as a "mailto:" link. You might use it to send email to inform the account user that the account has been enabled or disabled.

Enter as many new accounts as you need. When you've finished, click *SUBMIT CHANGES* to store the new accounts in the database.

Editing an account

The names in the *Full Name* column of the **User Accounts** page are links that open the **Edit Account** form. This form is identical to the **New Account** form described in the preceding section.

To edit an account:

1. Click its *Full Name* link on the **User Accounts** page.

2. Make any changes necessary to the Account settings on the **Edit Account** form.
3. Click *OK*.
4. Click *SUBMIT CHANGES*.

Your changes are reflected in the listing.

Enabling and disabling accounts

Occasionally you may need to temporarily prevent accounts from being accessible. For example, you might have a Customer account with Observer access that allows a customer to keep track of how script updates are scheduled and executed. For security purposes, you would not want that account to be accessible at all times.

The *Disable* option achieves this without having to delete and then re-create the account when you later need it.

When you disable an account, its definition remains unchanged. It can later be re-enabled to allow access to the users that know its username and password.

To disable an enabled account:

1. Select it by clicking the checkbox next to its lightbulb icon.
2. Click the *Disable* button. You see its lightbulb darken.
3. Click *SUBMIT CHANGES*.

Login under the account username is no longer possible.

To enable a disabled account:

1. Select it by clicking the checkbox next to its darkened lightbulb icon.
2. Click the *Enable* button. You see its lightbulb light up.
3. Click *SUBMIT CHANGES*.

Users with the correct access information can once again log in to Network Manager using the account.

Deleting an account

If you are sure you will never need an existing account again, you can delete it.

To delete an account:

1. Select it by clicking the checkbox next to its lightbulb icon.
2. Click the *Delete* button. You see a confirmation dialog.
3. Click *OK* in the dialog.
4. Click *SUBMIT CHANGES*.

The account is deleted from the Network Manager databases and is no longer listed. No jobs or other Network Manager database contents created by the account user(s) are affected.

Defining Publish Locations

6: Defining Publish Locations

Publish Locations are definable central locations accessible to Network Manager. A Publish Location is really just a path to a directory/folder on a particular machine. Script content is published to Publish Locations from InfoChannel Designer 3 authoring stations. Network Manager in turn retrieves the content from Publish Locations and stores it locally, ready to be sent to Players under control of a job.

The path you provide in defining a Publish Location is where content (published scripts and their media files intended for transmission to Players) must be placed. Content is published directly to this location from ICDesigner during a Publish to InfoChannel Network operation. Network Manager refers to this path to retrieve content when you run Send Content/Send Files jobs.

The Publish Location machine

There is no special software installation to be done on a Publish Location. A Publish Location is simply a file server, and only needs to be a computer accessible through a network or FTP connection to the Network Manager machine. It does not even have to run Windows; a UNIX® file server would function just as well.

The only configuration steps necessary on the Publish Location server are possibly to create a folder, and then whatever is needed to enable access to it:

- For FTP access: running FTP server software and setup of an appropriate FTP user account and password

  See the section starting on page 223 of the appendix regarding FTP setup on the Network Manager machine for information on FTP server configuration.

- For Local/Shared Folder access: making sure the Publish Location folder is set to be Shared, and that accounts and permissions are set appropriately to allow Network Manager to access the folder

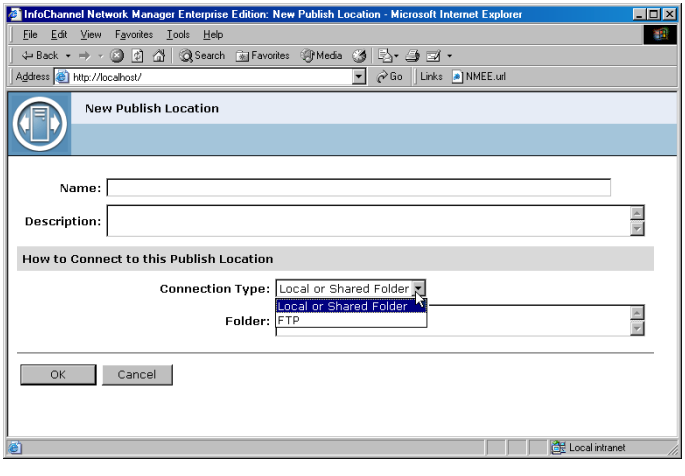
One or more Publish Locations might be located on the same physical machine as Network Manager itself. Using a Publish Location that is defined to be within the Network Manager Workspace (like the Default Publish Location that is automatically set up during installation) is in fact very advantageous, as it avoids an additional data transfer that would otherwise be necessary. However, Publish Locations can be located on any machines that are accessible to Network Manager.

The folder you define as the actual Publish destination can be anywhere, even the root of its own partition. Wherever it is, there needs to be plenty of empty space on the drive to hold all the published content that it will receive from ICDesigner stations.

Adding a Publish Location

To add a Publish Location:

1. In Network Manager, click the *Publish Locations* icon on the *Configure* panel of the control frame. You see the **Publish Locations** page. Normally all Publish Locations that have been created for this system are listed here. Initially it is blank.
2. Click the *New Publish Location* button. Enter the indicated information in the resulting form.



The **New Publish Location** form has the following fields:

a. *Name* – Enter a name for the Publish Location. It can be anything, as long as it is unique.

b. *Description:* – Enter a brief description for the Publish Location (optional).

c. *Connection Type:* – Choose the means by which you access the Publish Location from the Network Manager machine, either *FTP* or *Local or Shared Folder*.

3. Make settings specific to the connection type. Depending on which type you choose, a different set of options appears below in the form:

FTP

a. *URL:* – Enter the FTP location that this machine would use to get data from the Publish Location.

For example, `ftp://192.168.0.10/PubContent` or `ftp://PublishServer.com/PubContent`

b. *User Name:* – Enter the username to gain access to the FTP server.

c. *Password:* – Enter the password needed for the username. (Only asterisks appear.)

d. *Confirm Password:* – Enter the password again (to ensure you didn't type it wrong).

OR:

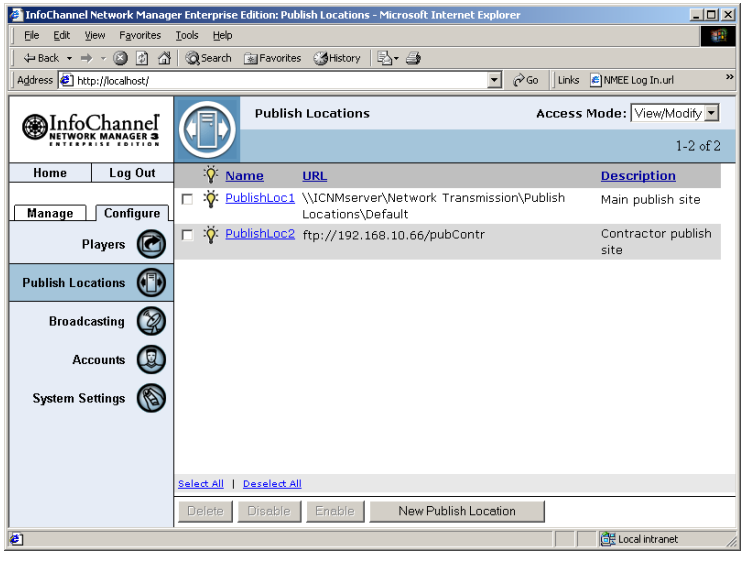
Local or Shared Folder

a. *Folder:* – Enter the path to the Publish Location from this machine, in either local drive-letter or UNC format. For example, if "F" is a share on "publishserver" the UNC path might be:

```
\\publishserver\f\pubcontent
```

4. Click the *OK* button to close the form.

The new Publish Location is listed on the **Publish Locations** page. Any number of Publish Locations can be defined; enter as many new ones as you need.



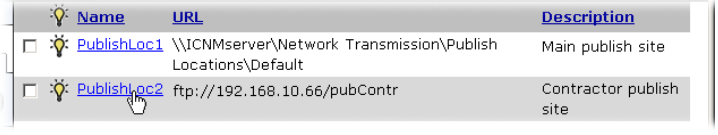
When you have finished, click *SUBMIT CHANGES* to store the new Publish Location(s) in the database.

Editing a Publish Location

The names in the *Name* column of the **Publish Locations** page are links that open the **Edit Publish Location** form. This form is identical to the **New Publish Location** form described in the preceding section.

To edit a Publish Location:

1. Click its *Name* link on the **Publish Locations** page.



2. Make any changes necessary to the Publish Location settings on the **Edit Publish Location** form.
3. Click *OK*.
4. Click *SUBMIT CHANGES*.

Your changes are reflected in the listing.

Enabling and disabling Publish Locations

Occasionally you may need to temporarily prevent Publish Locations from being accessible to jobs. For example, you might use one Publish Location for new, experimental scripts, and enable it only for testing purposes.

Doing so is possible without having to delete and then re-create the Publish Locations when you later need them by disabling them.

When you disable a Publish Location, its definition remains unchanged. It can still be selected in the creation and editing of jobs. However, when a job that uses a disabled Publish Location runs, content from that location is not actually sent.

To disable an enabled Publish Location:

1. Select it by clicking the checkbox next to its lightbulb icon.
2. Click the *Disable* button. You see its lightbulb darken.
3. Click *SUBMIT CHANGES*.

Content on the Publish Location will no longer be available to running jobs. The name of a disabled Publish Location shows up in red on the **Create Job/Edit Job** forms' *Source* pop-up.

To enable a disabled Publish Location:

1. Select it by clicking the checkbox next to its darkened lightbulb icon.
2. Click the *Enable* button. You see its lightbulb light up.
3. Click *SUBMIT CHANGES*.

Content on the Publish Location is again available to jobs.

Deleting a Publish Location

If you are sure you will never need an existing Publish Location again, you can delete it.

To delete a Publish Location:

1. Select it by clicking the checkbox next to its lightbulb icon.
2. Click the *Delete* button. You see a confirmation dialog.
3. Click *OK* in the dialog.
4. Click *SUBMIT CHANGES*.

The Publish Location is deleted from the Network Manager databases and no longer listed. Nothing on the Publish Location itself is affected.

Defining and working with Players

7: Defining and working with Players

Every Player in your installation needs to be defined within the InfoChannel Network Manager 3 database. A Player definition is a path to a unique folder associated with that Player. It may be local or remote. This folder is where Network Manager deposits job files that contain instructions for the Player. You also associate this folder with a Player when you configure the Player, as described in the next chapter.

The Player polls (looks in) this folder at regular intervals, checking for pending jobs. Player definitions let you refer to your Players by name when defining Network Manager jobs.

Creating a Player

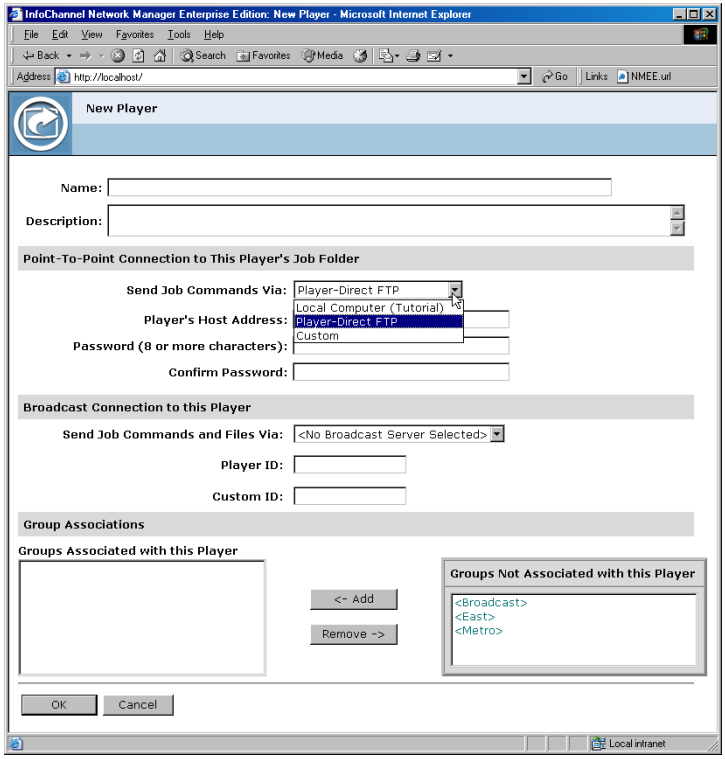
There are two basic steps to creating a Player:

- Defining the Player in Network Manager, covered in this chapter
- Setting up the individual Player machine in the InfoChannel Player Configuration utility, covered in the next chapter

Defining a Player in Network Manager

1. On the *Configure* control frame, click the *Players* icon. You see the **Players** page. Normally all Players that have been created for this system are listed here. Initially it is blank.

2. Click the *New Player* button. You see the **New Player** form:



3. Enter identifying information about the new Player in the following fields:

   a. *Name:* – Enter a name for the Player. It can be anything, as long as it is unique.

   b. *Description:* – Enter a description for the Player (optional).

4. Using the *Send Job Commands Via:* pop-up, choose how Network Manager gets to the Player's job folder:

   Local Computer (Tutorial) – This option is for use only with a Network Manager tutorial. It sets up Network Manager to access the Player software installed on the Network Manager machine itself, a default provided for testing and demonstration purposes.

Player-Direct FTP – This option is used for InfoChannel Networks that use "Direct FTP", the built-in FTP servers in the InfoChannel software.

When you choose *Player-Direct FTP*, you do not need to enter a site name or username—those are established automatically. All that is required are the Player's address and a password.

a. *Player's Host Address:* – Enter the IP number or DNS name that Network Manager should use to contact this Player.

b. *Password:* – Enter a password of at least eight characters. (Only asterisks appear.) This would be the password you give for the Player in Player Configuration, described on page 114.

c. *Confirm Password:* – Enter the password again for confirmation.

Custom – This option is used to expose the full configuration flexibility of InfoChannel Networking, necessary for special situations such as:

- Offsite FTP hosting is used
- The InfoChannel Network was set up under a previous release of the InfoChannel software, and changing over to Direct FTP is not desired
- Particular FTP server software must be used for customer-specific administrative reasons
- All Players are accessible locally over a LAN, so FTP access is not needed

The other options you see in this section when *Custom* has been selected involve a variety of additional factors related to more specialized InfoChannel Network configurations, and are discussed in the appendix.

Typically, you would choose *Player-Direct FTP*, which establishes the job folder on the Player.

4. If this Player is to have a broadcast connection, choose a Broadcast Server from the *Send Job Commands and Files Via:* pop-up in the *Broadcast Connection* section of the page.

   Please see chapter 12 for more detail on using broadcast connections.

5. If desired, associate the Player with one or more Groups.

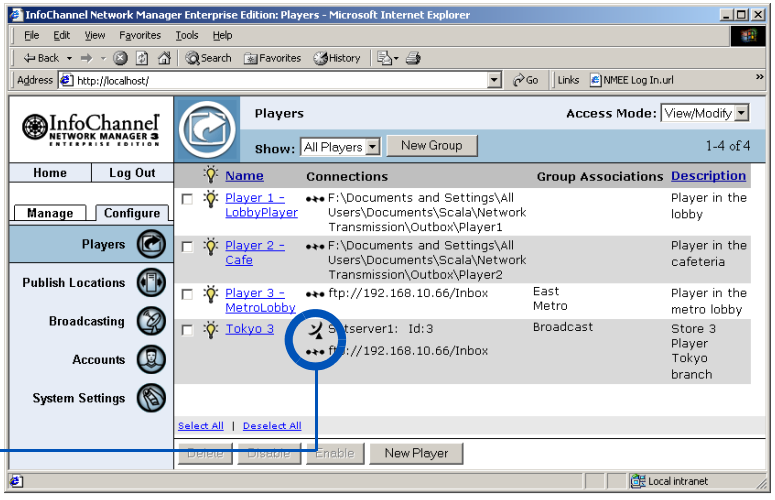
   In the *Groups Not Associated with this Player* list are the names of any Groups you have created. The names are enclosed in angle brackets (<>) and displayed in green. Click on as many as you wish to associate with this Player to select them, then click <- *Add*. The Groups you selected move to the left hand list.

   Associating a Player with a Group is optional. Group associations can be changed at any time.

   If you are creating your first Player, there are no Groups yet. You can associate Players with Groups either during the Group creation process, described in the section "*Using Groups*" on page 102, or during the Player creation process as described here.

6. Click the *OK* button to close the **New Player** form.

You see the Player you just created listed on the **Players** page with any other Players.



icons show Player connection types

Icons in the *Connections* column identify whether a Player has a point-to-point connection (), a broadcast connection (), or both.

Any number of Players can be defined, up to your license limit.

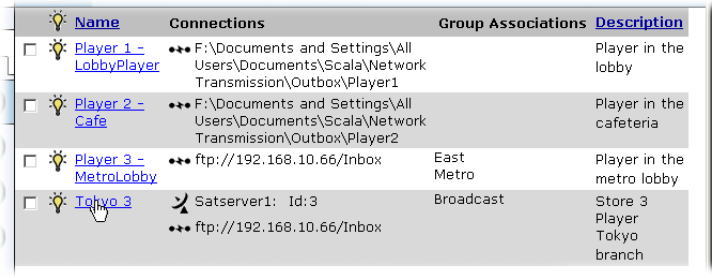
When you have finished, click *SUBMIT CHANGES* to store the new Player(s) in the database.

Editing a Player

The names in the *Name* column of the **Players** page are links that open the **Edit Player** form. This form is identical to the **New Player** form described in the preceding section.

To edit a Player:

1. Click its *Name* link on the **Players** page.



2. Make any changes necessary to the Player settings on the **Edit Player** form.
3. Click *OK*.
4. Click *SUBMIT CHANGES*.

Your changes are reflected in the listing.

Enabling and disabling Players

Occasionally you may need to temporarily prevent Players from being accessible to jobs. For example, you might use one Player for new, experimental scripts, and enable it only for testing purposes.

Doing so is possible without having to delete and then re-create the Players when you later need them by disabling them.

When you disable a Player, its definition remains unchanged. It can still be selected in the creation and editing of jobs. However, when a job that uses a disabled Player runs, no job file is placed in that Player's folder, so the Player is not affected.

To disable an enabled Player:

1. Select it by clicking the checkbox next to its lightbulb icon.
2. Click the *Disable* button. You see its lightbulb darken.
3. Click *SUBMIT CHANGES*.

The Player will no longer be affected by running jobs that include it as a target. The name of a disabled Player shows up in red in the Where section of the **Create Job/Edit Job** forms.

To enable a disabled Player:

1. Select it by clicking the checkbox next to its darkened lightbulb icon.
2. Click the *Enable* button. You see its lightbulb light up.
3. Click *SUBMIT CHANGES*.

The Player once again responds to jobs that target it.

Deleting a Player

If you are sure you will never need an existing Player again, you can delete it.

To delete a Player:

1. Select it by clicking the checkbox next to its lightbulb icon.
2. Click the *Delete* button. You see a confirmation dialog.
3. Click *OK* in the dialog.
4. Click *SUBMIT CHANGES*.

The Player is deleted from the Network Manager databases and no longer listed. Nothing on the Player machine itself is affected.

Using Groups

Groups in Network Manager are a way to make it easier to manage your Players, particularly in large installations.

Grouping your Players makes it easier to refer to many Players at once in a single job command. In installations that comprise hundreds, even thousands of Players, this allows a dramatic saving in effort for InfoChannel Network administrators when specifying jobs. Additionally, Groups give you a way to organize Players according to the factors that are meaningful to you.

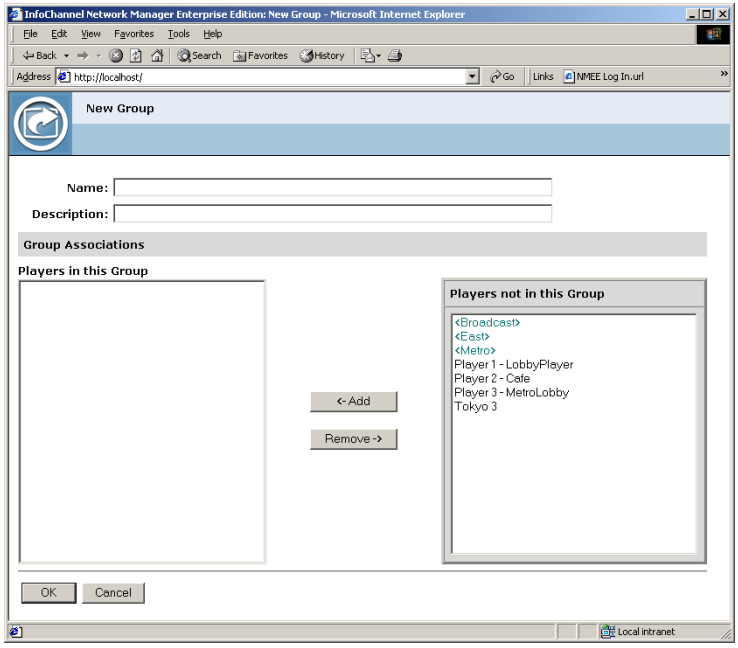
Players can be associated with Groups in any manner you choose. You might associate Players with Groups based on one or more of the following criteria:

- Players' installation site or geographic region
- Players' connection type (Direct FTP, Custom, broadcast)
- the nature or purpose of Players' content
- corporate division
- client

Players do not have to belong to a Group. They can belong to any number of Groups, and Groups themselves can be grouped.

To create a Group:

1. If you are not already on the **Players** page, click the *Players* icon.
2. Click the *New Group* button at the top of the page.
3. Enter the indicated information in the **New Group** form.



The form has the following fields:

a. *Name:* – Enter a name for the Group. It can be anything, as long as it is unique.

b. *Description:* – Enter a brief description for the Group (optional).

Associating Players with Groups

Under the heading *Players Associated with this Group*, on the right-hand side of the form is a list of the existing Players and Groups. To add Players (or Groups) to the new Group:

a. Select them in the *Players Not in this Group* list

b. Click the <-*Add* button. The selected item(s) are moved to the *Players in this Group* list. You can add as many Players or Groups to the new Group as you like.

4. Click the *OK* button to close the **New Group** form.

You see the Group you just created listed in the *Show:* pop-up list at the top of the **Players** page. Any listed Players that you added to the Group reflect this in their *Group Associations* column. The new Group is now available in the **New Player** and **Edit Player** forms as well.

Any number of Groups can be defined; enter as many new ones as you need.

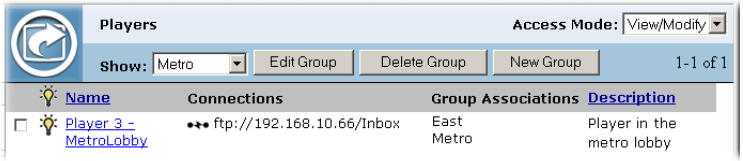
When you have finished, click *SUBMIT CHANGES* to store the new Group in the database.

Editing a Group

If you decide you need to change the name, description or associations of a Group:

1. Make sure you are on the **Players** page.
2. Select the Group name in the *Show:* pop-up.

   Just the Players and Groups in the selected Group are listed.



3. Click *Edit Group* to open the **Edit Group** form.

The form is the same as the **New Groups** form. Make any necessary changes.

4. Click the *OK* button to close the form.
5. Click *SUBMIT CHANGES*.

Deleting a Group

If you decide you need to delete a Group:

1. Make sure you are on the **Players** page.
2. Select the Group name in the *Show:* pop-up.

   Just the Players and Groups in the selected Group are listed.

3. Click *Delete Group*.

   You see a confirmation dialog.

4. Click the *OK* button to confirm the deletion.
5. Click *SUBMIT CHANGES*.

Deleting a Group only deletes the Group definition from the database, dissolving its associations. Any Players or Groups that were part of the deleted Group are unaffected.

Associating a Player definition with an actual Player

The Player definition in Network Manager is nothing more than a path to its job folder location. Whatever the connection type, associating this definition with a physical Player requires action at both ends of the connection.

- on Network Manager, entering identifiers in the Player definition:
  - *Player-Direct FTP* – an IP address and password
  - *Custom FTP* – a job folder URL, FTP username, and password
  - *Custom Local or Shared Folder* – a path to a shared job folder with appropriate account privileges

- on the Player, running the InfoChannel Player Configuration utility and entering matching identifiers:
  - *Player-Direct FTP* – a password
  - *Custom FTP* – a job folder URL, FTP username, and password
  - *Custom Local or Shared Folder* – a path to a shared job folder with appropriate account privileges

See page 112 in chapter 8 for details on this configuration task.

For Custom connections, it is vital that whoever performs the configuration on the Player machines knows the folder name that corresponds to each physical Player, so that folder names and Players can be correctly matched up.

See the section "*Creating Player job folders*" on page 216 in the appendix for details.

How content is stored on a Player

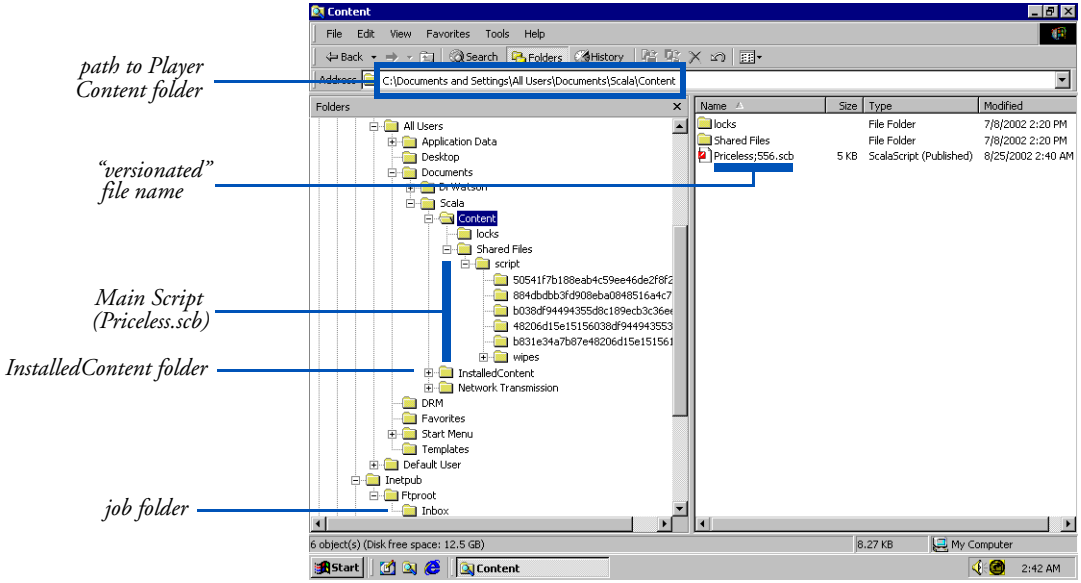
In normal operation it is not necessary to be concerned about what happens to content once it is sent to a Player. The InfoChannel Player software unpacks the transmitted file "package" and places it where it needs to be on the Player's hard drive automatically; the process is invisible from the Network Manager end.

However, because administrators must occasionally perform maintenance and diagnostic tasks on Players in the field, and because the filing scheme used for script content on Players is somewhat arcane, it can be valuable to understand how things are arranged.

The Content folder

All content files sent to a Player from Network Manager are stored in the Content folder, located in <*systemroot*>:\Documents and Settings\All Users\Documents\Scala, where <*systemroot*> is the system root drive letter, typically C.

This illustration shows the layout of files and folders within Content for a Player that has been sent a script named “Priceless”:



In the Content folder are additional folders and a file. The file is named for the script. However the name has been “versionated”, containing a semicolon (;) followed by a serial number:

<scriptname>;####.scb

In the preceding illustration, the versionated name for the “Priceless.scb” script is

`Priceless;556.scb`

The versionation serial number is generated and applied when the Player receives a content file, and is the means by which the Player distinguishes efficiently between updated versions of the same content during the update process. (At times you will also see the preceding version of a script, with a lower versionation serial number, still in the folder. This is normal.)

The "Priceless;556.scb" file is not the actual script file, but is a file that specifies the content required by the script. The actual script and content files for the script are inside the Shared Files folder.

Within the Shared Files folder are a folder named "Script" and the actual script data file, the name of which consists of a long alphanumeric string ending in "script.scb". This string is MD5 encoding, which is a way of uniquely tagging content items to ensure that newer content can be smoothly and reliably swapped for older content of the same base name.

The "Script" folder in turn contains a series of MD5-named folders, one for each content file in the script. The actual content files are in the folders, one file per folder.

If any linked content scripts are sent to the Player, they are placed in the Content folder, at the same level as the Shared Files folder. The filenames of linked content are also versionated.

The InstalledContent folder

Another folder in the same location as Content (visible in the illustration on the preceding page) is InstalledContent.

This folder can also hold script content files. The difference between this folder and Content is that InstalledContent is never used for content files that are sent through Network Manager jobs. It is used only for storage of files put on the Player by some other means—typically by being copied from a CD-ROM, DVD-ROM or other removable storage device.

There are various reasons that it might be more practical to put information onto a Player "manually" rather than by sending it with Network Manager:

- to eliminate the download time for very large amounts of data
- to avoid the network traffic for very large amounts of data
- the data is generated local to the Player, where physically going to the machine is easier than going through Network Manager

- the data is linked content that must be downloaded from some external source by an application other than Network Manager
- Network Manager is unavailable for some reason

Just putting such files into the Content folder would not work, however, for these reasons:

- the file naming and folder structure for everything within Content is cryptic and can only be generated by Scala software; the ICPlayer software requires this structure and could not find files that were simply copied there
- a Delete Unused Content job would not recognize files that were manually copied to the Content folder as valid, and would delete them regardless of whether they were in use

The ICPlayer software does not manage what is placed in InstalledContent in any manner. It only uses InstalledContent as a secondary place to look for content files called for by a script, if those files cannot be found within the Content folder.

Delete Unused Content jobs do not affect InstalledContent. If you use InstalledContent, you must remember to clean out old files yourself using Delete Files jobs, so that the Player's hard drive does not become filled with stale data.

InfoChannel Player configuration

8: InfoChannel Player configuration

On each Player machine in your InfoChannel network, the InfoChannel Player 3 software must be installed and configured.

The configuration on the Player end is complementary to the Network Manager Player definition, identifying the folder that the Player refers to for its job files. You make settings within the Player software governing how the Player physically accesses its folder on the Network Manager end, as well as playback-related settings.

Outside the Player software, in Windows, there are further configuration tasks to enable the Player and Network Manager to communicate securely and reliably.

Using the InfoChannel Player Configuration utility

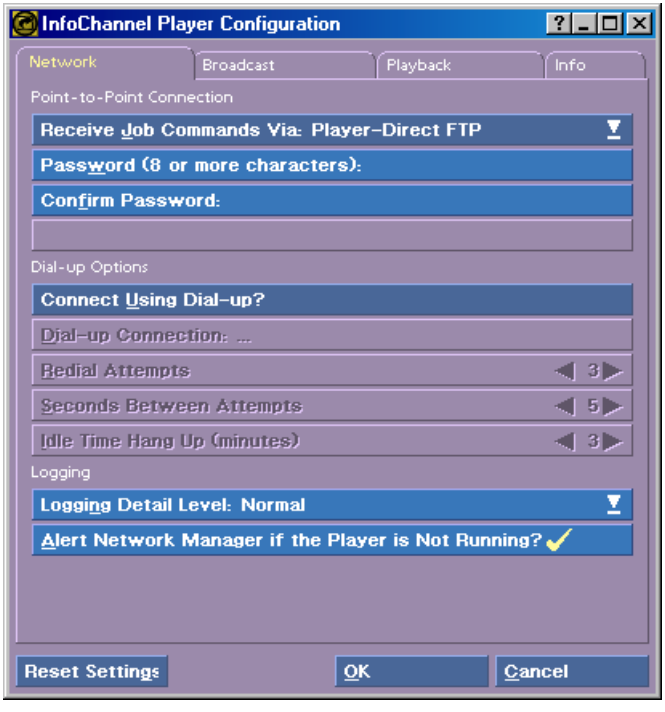
The InfoChannel Player Configuration utility is the tool you use to set up the InfoChannel Player software on a Player machine. Every Player in an InfoChannel Network must be individually configured using this utility.

Configuration of Player machines should be done after the definition of the Players in the Network Manager application.

This chapter discusses configuring Players for all types of connections: Direct FTP, Custom, and Broadcast.

For Players that communicate via a Custom connection, the factors to consider are more advanced. Settings for Custom connections in the *Point-to-Point Connection* and *Dial-up Options* sections of the utility are not covered here. The appendix to this manual, "*Setup of Custom connections*", discusses those aspects of Custom connections in detail. However, the other Player Configuration settings covered in this chapter are relevant to all Players and should be considered when setting up Custom connections.

Run the Player Configuration utility from the Start menu by choosing *Programs* > *Scala InfoChannel Player 3* > *Configure InfoChannel Player 3*. You see the InfoChannel Player Configuration dialog.



Network options

The *Network* panel of the dialog contains options related to how the Player Engine—the Player's networking and data-management background task—communicates with Network Manager.

The *Point-to-Point Connection* section is where you set up the Player's job folder location on the Player side.

Receive Job Commands Via

The *Receive Job Commands Via:* pop-up lets you specify the type of access the Player has to its job folder:

Local Computer (Tutorial) – This option is for use only with the Network Manager tutorial. It sets up the Player software that is installed on the Network Manager machine itself to access a local job folder, a simple default provided for testing and demonstration purposes.

Player-Direct FTP – This option is used for InfoChannel Networks that use "Direct FTP", the standard InfoChannel connection scheme that takes advantage of the built-in FTP servers in the InfoChannel software.

When you choose *Player-Direct FTP*, you do not need to enter a site name or username—those are established automatically. All that is required is a password.

1. *Password:* – Enter a password of at least eight characters. (Only asterisks appear.) This must match the password that you gave for Player-Direct FTP in the Network Manager Player definition, as described on page 98.
2. *Confirm Password:* – Enter the password again for confirmation.

Custom – This option is used for InfoChannel Networks that have special communications needs:

- You are using offsite FTP hosting
- You have an existing InfoChannel Network, and wish to retain its current communication setup
- You must use particular FTP server software for administrative reasons
- Players are accessed locally over a non-TCP/IP LAN, so using FTP is not possible

The other options you see when *Custom* has been selected involve a variety of additional factors related to more specialized InfoChannel Network configurations. They are discussed in the appendix.

The settings in the *Dial-up Options* section of this panel apply only to FTP connections. See the section on FTP dial-up connections starting on page 241 in the appendix for details.

The *Logging* section of the panel has options related to how the Player reports its activity back to Network Manager.

Changing the amount of log information

Players write messages describing their activities to daily log files. You can specify the level of detail you want included in the Player log files, depending on whether you want to make them easier to read through, or gather further information to help you troubleshoot a problem.

ICPlayer Note

When Direct FTP is in use, the Player logs include FTP operation messages.

Choose a level of detail from the *Activity Logging Detail* pop-up. The four choices, in increasing level of detail, are:

- Errors and Problems Only
- Low
- Normal
- Diagnostic

Keeping track of the Player's playback status

Because Players are generally assumed to be playing back scripts at all times, it is important to know if anything has happened to interrupt playback. The Player can be set to notice if its playback window has been closed and automatically send an alert to Network Manager when this happens. This precaution is designed to catch instances when someone accidentally closes the playback window without restoring it.

ICPlayer Note

Turning on this option does not automatically restore playback if it is interrupted. The best way to restart playback is for a Reboot command to be issued from Network Manager.

The *Alert Network Manager if the Player Is Not Running?* option is on (✓) by default. You can turn it off to avoid unnecessary alerts if a Player machine needs to be used for some purpose other than script playback.

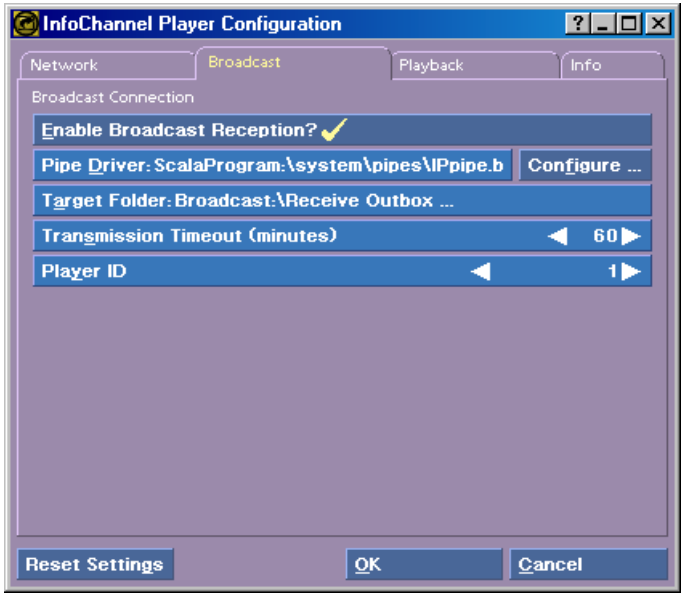
Typically the only reasons to turn this option off are if you intend to run only the Network Client and not the Player program, or you wish to allow people to use the machine for other purposes than as a Player

some of the time. Running only the Network Client can be used to set up a file server for a LAN-cluster of Players; it is also a way to update a Linked Content folder for a team of designers so that they have an up-to-date representation of files on the network that they can link to.

Broadcast options

The *Broadcast* panel contains options that apply to Players that receive transmissions through a connection to an InfoChannel Broadcast Server. The settings on this panel have no effect if the Player does not receive broadcast transmissions.

The initial basic configuration of a broadcast Player, as with any other Player, is done during installation of the ICPlayer software on the Player machine. Ideally, decisions about the type of connection(s) to be used by the Player should be done before installation, so that options can be set accordingly.



Enable Broadcast Reception?

Turn the *Enable Broadcast Reception?* option on (✓) if this Player is to have a broadcast connection to Network Manager.

Pipe Driver

The Player end must be configured for a particular pipe driver just as it must at the Broadcast Server end. The pipe driver configured on a Player must match the one specified on the Broadcast Server for transmissions to that Player.

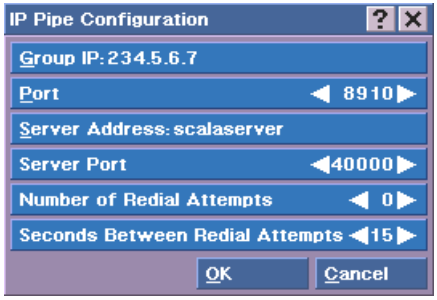
Click the *Pipe Driver:* button to open the File dialog, allowing you to choose a pipe driver .BOK file. The following pipe drivers are shipped with the current release of InfoChannel Player 3:

- IPpipe – IP multicast support
- HNSpipe – Hughes satellite network support
- Filepipe – a simple default pipe, useful only for testing purposes

Pipe drivers usually have their own configuration settings. When the chosen driver has configuration settings, the *Configure* button is enabled. Click this button to open a dialog where you can make settings for that pipe.

IP Pipe Configuration

Some options in the IP Pipe Configuration dialog duplicate ones that are found in the corresponding dialog seen on the Broadcast Server.



Group IP – The *Group IP:* setting is the multicast group IP address (in the standard four-part nnn.nnn.nnn.nnn form) used by broadcast applications. The valid range is 224.0.1.0 through 239.255.255.255 inclusive. The system administrator for your TCP/IP installation must supply the proper value.

> ***Broadcast Note***
>
> The *Group IP:*, *Port:*, and *Server Port:* settings for the Player available in this dialog must match those set on the Broadcast Server.

(The *Group IP:* default of 234.5.6.7 is suitable for testing purposes, but should be changed for actual use.)

The specification for Group IP is not Player-specific, but is common to the entire IP Multicast system. It is not related to Groups in Network Manager.

Port – Specifies the IP multicast port number that the Broadcast Server sends on, which the Players must therefore be configured to listen on.

Like the Group IP address, the *Port:* number setting must be supplied by your system administrator. The system may require a particular port number specific to your application, or you may be able to choose randomly. In any case, the port number must be unique within your system to avoid interfering with port numbers used by other applications.

The default of 8910 is suitable for testing purposes, and may be satisfactory for actual use.

Server Address – Specifies the host name or number of the Broadcast Server. This field is used only for confirmed IP multicasting. The number you enter here can be include an IP address, a phonebook entry, or both:

- If entering an IP address, the address should be entered in standard numerical IP address format (nnn.nnn.nnn.nnn).

  As an alternative you can enter a host name, assuming your network is set up to map the name to the IP number.

- If entering a Windows phonebook entry, the phonebook entry name must be entered within parentheses, as in *(MyPhoneBookEntry)*.

  RAS (Remote Access Service) must be installed on this system to use a dial-up connection, and a phonebook entry must be created using the RAS phonebook.

  You may use whatever name you like for a phonebook entry so long as the same name is entered here. The phonebook entry is also the place where you fill in the phone number to dial, a user name, a password, etc. The network interface IP address is obtained automatically after a connection is established with a remote access server.

- If entering a both a phonebook entry and an IP address, specify the IP address to be used by entering it after the phonebook entry, as in *(MyPhoneBookEntry) 192.168.0.1*.

  When an IP address is specified this way, the Player attempts to connect via RAS, but uses the specified IP address for communication with the Broadcast Server.

Server Port – Specifies the IP port number on which the Broadcast Server listens for incoming connections.

This field is used only for confirmed IP multicasting. You should not need to change this value unless the port number is being used by another application.

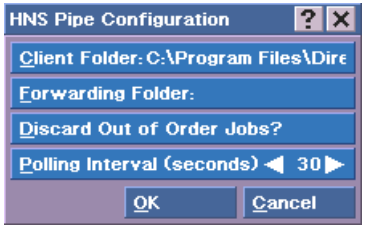
If you do change this value, the same change must be made on the Broadcast Server and all Players. You must also reset the Broadcast Server and Players before the new setting will take effect.

Number of Redial Attempts – Sets the number of times to automatically redial. This setting applies only for confirmed IP multicasting and only if this Player contacts the Broadcast Server via a dial-up (RAS) connection.

Seconds Between Redial Attempts – Sets the number of seconds the Player waits between redial attempts. This setting applies only for con-

firmed IP multicasting and only if this Player contacts the Broadcast Server via a dial-up (RAS) connection.

HNS Pipe Configuration
Four options are available in the HNS Pipe Configuration dialog.



Client Folder – This setting corresponds to the *Destination Client:* setting found in the HNS Options dialog on the Broadcast Server. It specifies the path to the folder on the Player where broadcast files are deposited by the HNS software when they are first received.

This folder is not the same as the Target Folder (see the section on page 121). Files received in the HNS Client Folder have yet to be "unpacked" by the Network Manager pipe driver software. Only after being processed through the pipe driver are the resulting files placed into the Target Folder. The default location for *Client Folder:* set up by the HNS VAR should not need to be changed.

Forwarding Folder – Lets you specify the UNC path to an optional folder where the Player can forward incoming package and envelope files.

This feature can be used to get broadcast transmissions to more than one Player on a network when only one Player has a receiver card.

To use this feature, the Players must be able to share files over a network shared drive or UNC path. If several Players need to share a transmission, you can set the Forwarding Folder separately on each to forward the transmission multiple times. The Player with the receiver card forwards to the second Player, the second forwards to the third, and so on.

Discard Out of Order Jobs? – When turned on (✓), this option prevents later content from being overwritten by earlier content.

The HNS broadcast transmission system does not guarantee that jobs are delivered to Players in the order the jobs were queued. This can result in jobs being delayed (possibly delivered hours later) and out of order.

The delivery system presumes that jobs will be spaced far enough apart (typically 24 hours) that the packages will be delivered in their queued order. For systems in which smaller content is being delivered more often, it is preferable that jobs that arrive out of order be discarded so that earlier jobs and content will not be received after later jobs.

With this option on, jobs and content that arrive out of order are discarded, preventing later content from being overwritten by earlier content. The negative consequence is that some jobs that are sent are never run.

This feature should be used only when all jobs are essentially the same, delivering all content with every job.

Polling Interval – This setting specifies the number of seconds the Player waits between each check for the arrival of new broadcast files in the Client Folder. The default of 30 seconds is not likely to need to be adjusted.

Target Folder

Target Folder: specifies the location of the folder on the Player into which files from the Broadcast Server are deposited after being processed by the selected pipe driver.

The default location is Broadcast:\Receive Outbox. To change the default, click this button to open the File dialog, where you can choose a different folder on the Player.

Transmission Timeout

Sometimes broadcast transmissions are interrupted. An interrupted transmission might be resumed, and ultimately completed, or if the connection is lost completely, the transmission might be aborted. When a transmission is aborted, the temporary files containing data

already transmitted are abandoned, and remain in the Target Folder on the Player.

To prevent an accumulation of abandoned transmission files from cluttering the Player's hard drive, the ICPlayer software regularly deletes transmission files that have shown no activity for a certain period of time. That period of time is specified by the *Transmission Timeout (minutes)* control.

Using the default of 60 minutes, incomplete transmission files that have not been updated in more than an hour are deleted, and the transmission is considered to have failed.

Adjustment of the timeout value used should rarely be necessary. If the setting is changed, it must take into account the length of typical transmission interruptions for the particular installation.

Too long a timeout might allow large amounts of abandoned files to accumulate, clogging the hard disk and blocking new transmissions. Too short a timeout can prevent transmissions from resuming after brief but recoverable service interruptions.

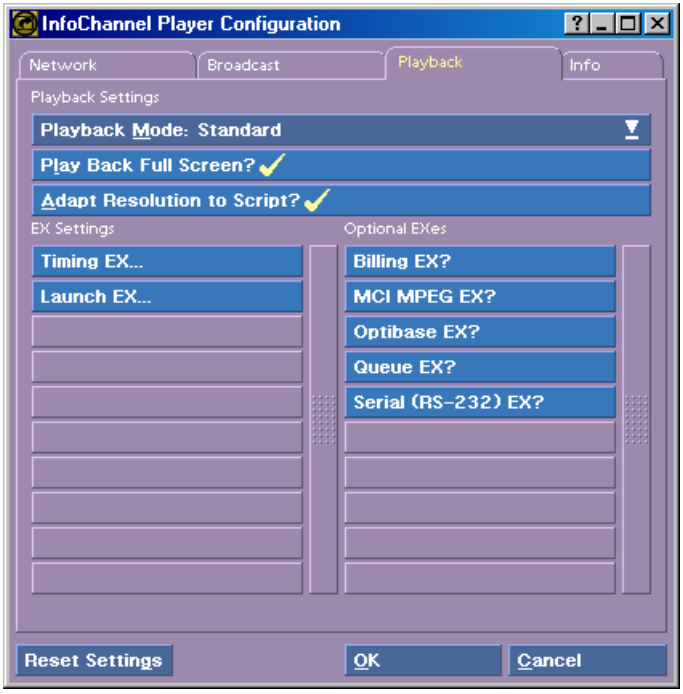
Player ID

Each Player requires a unique ID number to identify it so that transmissions can be properly targeted. The ID number is set with the *Player ID* control.

The Player ID must match what was defined in the corresponding *Player ID:* text box in the **New Player/Edit Player** form for this Player in Network Manager (see page 198 in chapter 12).

Playback options

The contents of the *Playback* panel mirror options available on the *Playback* and *EXes* panels of the Options dialog in InfoChannel Designer 3.



The *Playback* panel lets you decide how you want scripts to play back on your system. The primary questions are whether scripts should play back in a window or fill the screen, and what display mode is used for playback.

You can choose one of two ways to make these decisions on the *Playback Mode:* pop-up, by picking either *Standard* or *Custom*. The options below change depending on which mode you choose.

Playback Mode

Players normally use full screen playback.

▶ To ensure that scripts fill the screen:

1. Set *Playback Mode:* to *Standard*, if it is not already.
2. Make sure the *Play Back Full Screen?* option is on (✓).
3. To keep the display mode from changing from the standard Windows setting, make sure *Adapt Resolution to Script?* is off.

Using Standard mode does not let you choose a specific resolution for all your scripts to play back, or a particular color depth (number of colors) or monitor refresh rate.

It may be preferable to use Custom mode to make sure to specify a particular resolution, color depth, and refresh rate. This setting is implicitly full screen, and prevents display mode switching. It has the additional advantage of letting you choose a display mode that is independent of the normal Windows display mode.

▶ To choose an independent display mode for full screen script playback:

1. Set *Playback Mode:* to *Custom*.
2. Click the *Full Screen Display:* button to open a display mode dialog.
3. When switching to Custom mode, the dialog initially shows the current Windows display settings. Choose the size, color depth and refresh rate you prefer for script playback.

Windowed playback

Running the Player in a window is occasionally useful for testing purposes during setup and troubleshooting.

▶ To have the Player run in a window:

1. Set *Playback Mode:* to *Standard*.
2. Turn off *Play Back Full Screen?*.

EX options

The lower part of the *Playback* panel is devoted to EXes. EXes used by scripts must be enabled and configured just as they were on the systems from which they were authored in order to play back correctly.

When EXes that have configuration options are turned on in the *Optional EXes* column, buttons for them appear in the *EX Settings* column. Click a button in this column to display an Options dialog for that EX.

How to configure the Timing and Launch EXes, and remarks about the Scala EX system in general, can be found in chapter 15 of the InfoChannel Designer 3 "*Basic Authoring User's Guide*". Configuring the optional EXes that ship with InfoChannel Designer 3 is covered in chapter 7 of the InfoChannel Designer 3 "*Extended Authoring and Publishing User's Guide*". Separately-available EXes come with their own documentation.

Version information

You can view version information on the various software modules that make up the InfoChannel Player software by selecting the *Info* panel.

Resetting to defaults

You can reset the settings in the Player Configuration dialog to their defaults by clicking *Reset Settings*.

Storing your changes

When you have finished configuring this Player, click *OK* to save the changes and exit the utility.

Engine restart required

The changes you make do not actually take effect until the next time the InfoChannel Player Engine is restarted.

Miscellaneous Player issues

Virus scanning on Players

Although the use of virus scanning software is strongly recommended for security maintenance in an InfoChannel Network installation, Scala does *not* recommend that such software be installed on Players.

Testing by Scala has shown that even virus scanning products by the most reputable companies are a stability hazard on computers for which 24-hour, 7-day-a-week reliability is crucial.

The first line of defense in preventing virus infection of Players is simply not allowing them to become compromised:

- Players should remain dedicated systems, never used for email, Web surfing, or other high-risk activities
- Software other than Windows and InfoChannel Player software should be installed on a Player only if absolutely necessary, and should be scanned before installation
- The Network Manager workspace folder should be frequently virus-scanned, so that all files transmitted to Players are verified as clean

Scala does recommend that Player machines be scanned for viruses periodically. Ideally, the scan should be done from a virus scanner running on a remote machine with a network connection to the Player.

If remote scanning is not possible, virus checking software should be *temporarily* installed on the Player. After being used to perform a thorough scan, the virus software should then be uninstalled from the Player.

Player software and Windows services

You should be aware that the message dialog boxes that can be put up by certain standard Windows services can disrupt Player operation. For example, the Messenger service puts up dialogs for certain events.

When the Player is running a script in full-screen mode, as it normally is, it must be "switched out" to allow the dialog box to appear, interrupting normal playback.

The InfoChannel Player software attempts to intercept as many system dialogs as possible, but not every situation can be anticipated. A system administrator knowledgeable in Windows should disable services that may cause disruptive dialogs. For operation as a Player, many standard services are not necessary.

The following services, at a minimum, should be disabled on dedicated Player machines:

- Alerter service
- Indexing service
- Messenger service

If a problem service cannot be disabled, achieving non-interruptible playback requires finding a way to prevent the dialog boxes from having to appear.

Windows event log overflow

It is possible for a PC to freeze if its Windows event logs fill up and no further events can be recorded.

To prevent this from happening, the Windows System, Application, and Security logs on all Players should be set so that the oldest events are overwritten when the log becomes full:

1. Open the Event Viewer.
2. Right-click on the System log and choose *Properties*.
3. In the Properties sheet, make sure that *Overwrite events as needed* is selected.
4. Click *OK*.
5. Repeat steps 2–4 for the Application and Security logs.
6. Close Event Viewer.

Setting up jobs

9: Setting up jobs

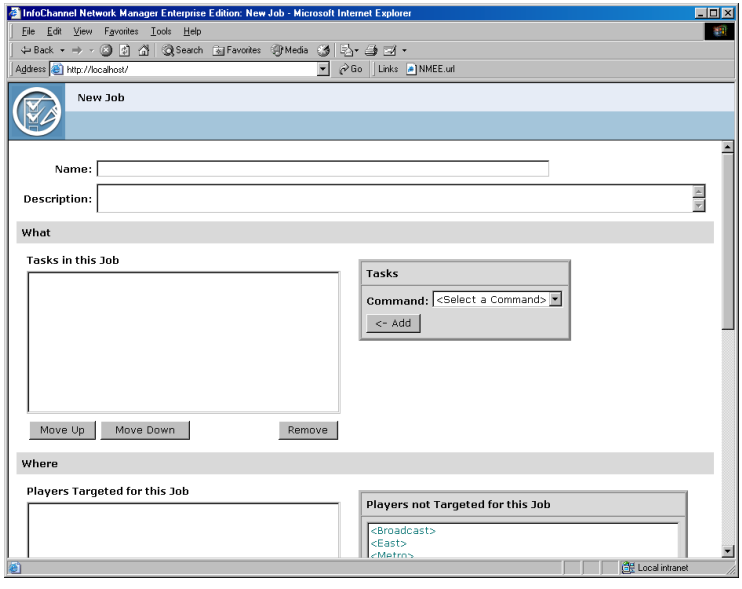
A *job* in InfoChannel Network Manager 3 is a definable action that the program takes regarding one or more Players. A job consists of one or more *tasks*. A task consists of one of the basic *commands*, usually with certain options, which specify the actual action to be taken. Jobs can be run by running them "manually", or triggering them automatically according to a regular schedule.

The most typical job is one that updates a Player's main script, by sending new content to the Player. Another example would be a job that sends a Player a new MPEG file of a radar weather map every hour. Or you could tell a set of Players to return a particular file to the Network Manager server. These are just a few examples of the many things that Network Manager can do.

Creating a job

1. Click the *Jobs* icon on the control frame. You see the **Jobs** page. Normally all jobs that have been created for this system are listed here. Initially it is blank.

2. Click the *New Job* button. You see the **New Job** form.



3. On this form, identify the job using the following fields:

   a. *Name:* – Enter a name for the job. It can be anything, as long as it is unique.

   b. *Description:* – Enter a brief description for the job (optional).

The **Jobs** page below is divided into three sections:

- *What* – specifies the action(s) that the job should perform
- *Where* – specifies the Player(s) affected by the job
- *When* – lets you optionally specify a means of triggering the job automatically

> **IMPORTANT**
>
> The scheduling capability for Network Manager jobs is separate and independent from the scheduling of script events in the ICDesigner **Schedule** menu. Job scheduling only determines when jobs run, and has no effect on when script elements play back.

4. Define the job's Task(s) under the *What* heading:

   a. Choose a command.

      This area of the page has a *Tasks* section with a *Command:* pop-up that lets you choose from a list of job commands.

      The *Command:* pop-up prompts you with <*Select a Command*>. When you first enter the **New Job** form, you see only the two most-used commands in the pop-up list, *Send Main Script* and *Send Content*, plus the choice <*More Commands*>.

      If you don't see the command you need, choose <*More Commands*>. The *Command:* pop-up then displays the full list of available job commands for you to choose from.

      See the section "*Job commands*" on page 137 for information on individual commands. Follow the steps described there for each command, after which you can resume this job setup procedure with the following step.

5. You can include more than one task in a job. If desired, return to step 4.

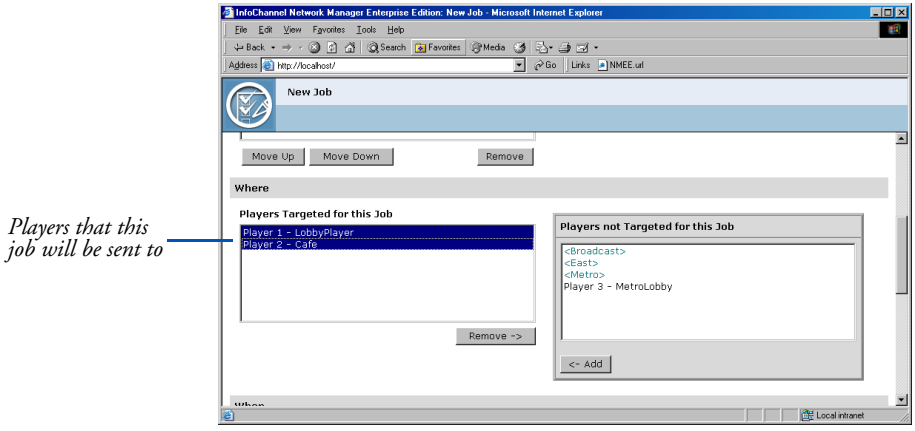
If you have more than one task in the *Tasks in this Job* list, you can change their order by selecting them and using the *Move Up* and *Move Down* buttons.

You can remove a task by selecting it and clicking the *Remove* button.

6. Select the Players this command should affect under the *Where* heading:

   a. The *Players not Targeted for this Job* list shows all available Players and Groups. Group names are green and enclosed in angle brackets (<>). Select Players and Groups to send the content to. You can select several at once.

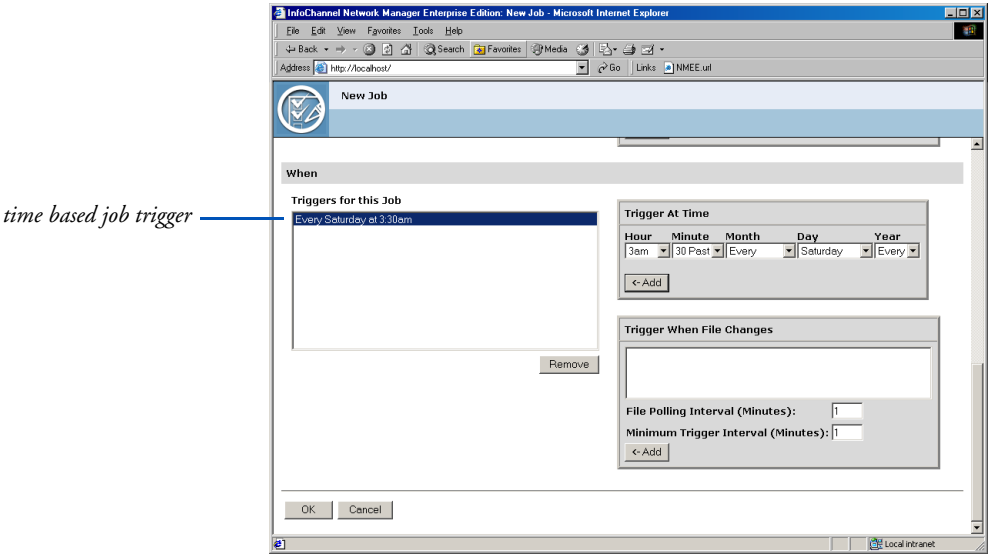
      (Players listed in red are currently disabled, and will not be affected by this job until they are re-enabled on the **Players** page.)



   b. Click the <- *Add* button. The Player(s) you selected are moved to the *Players Targeted for this Job* list.

      To remove Player names from the job, select them and click the *Remove* -> button. The selected items return to the *Players not Targeted for this Job* list.

7. Optionally, choose a way to trigger the execution of the job automatically under the *When* heading.



There are three ways to trigger a job:

- triggering manually
- scheduling a regular time
- detecting a change in a particular file

If you intend to trigger this job manually only, you can skip to step 8 on page 136, leaving the *Triggers for this Job* list empty. For details on manual triggering, see "*Running a job manually*" on page 150.

However, it can be very useful to have Network Manager automatically issue a job trigger event. Scheduling jobs this way increases the consistency and reliability of operations, especially in large installations. Plus it provides the flexibility of performing updates at any time of day or night, without a human needing to be present to trigger them.

You can create complex schedules by adding multiple triggers for each job, and can combine the time-based and file-based types of trigger.

Any job, scheduled or not, can still be manually triggered at any time.

To create a time-based trigger:

In the *Trigger At Time* section, you use the pop-ups for *Hour, Month*, *Day*, and *Year* essentially as "filters". Choosing anything from these controls limits the job trigger to occur only within the time span that they collectively specify. Choosing *Every* for any of these removes its limiting function.

The *Minute* pop-up does not have an *Every* choice. It specifies the number of minutes past the specified hour(s) that the job runs. It is not possible to specify, in a single trigger, an interval shorter than one hour. Multiple triggers, with different *Minute* values set, are required to do that.

For example, you could choose to trigger a job on the fifteenth of every month, and/or 5 minutes past 3 am every weekday in February 2003. To trigger a job every 15 minutes, you would need to add four triggers, with *Minute* values of *00 Past*, *15 Past*, *30 Past* and *45 Past*.

When you are done, click the <- *Add* button. A description of the time trigger setting appears as a line in the *Triggers for this Job* list. Create and add other time-based triggers if desired.

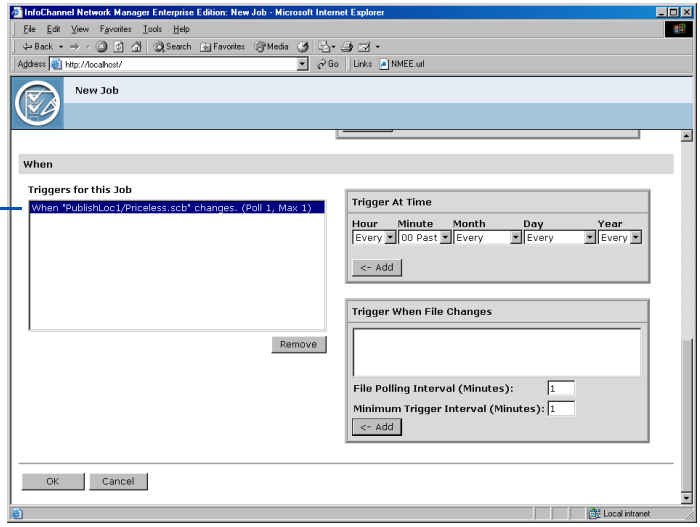
To create a file-based trigger:

In the *Trigger When File Changes* section, you can select a file, and specify how often Network Manager automatically checks it on its Publish Location for changes.

For example, you could check every five minutes to see if the script has changed; if it has been re-published, Network Manager would notice and could automatically trigger a *Send Content* job to update the Players.

a. Select the name of the file to check from those listed. (Typically this is a content file, but it could also be a file sent with *Install File* or *Install System File*.) To be listed here, the file must exist on a Publish Location and be named in a *Send Main Script*, *Send Content*, *Install File*, or *Install System File* task in this job.

file change job trigger



b. If desired, change the default *File Polling Interval (Minutes):* setting. This option determines how often the file is checked.

c. If desired, change the default *Minimum Trigger Interval (Minutes):* setting. This option determines how often a file—having been polled and found to have changed—may be transmitted. It lets you limit the maximum frequency that this job will be triggered even if the file changes more often.

When you are done, click the <- *Add* button. A description of the file trigger setting appears as a line in the *Triggers for this Job* list. Create and add other file-based triggers if desired.

8. Click the *OK* button at the bottom of the form.

9. Choose *SUBMIT CHANGES* to store your changes in the database.

The jobs you have created on the **New Job** form are listed on the **Jobs** page under the names you gave, with summary information in the *What*, *Where*, and *When* columns.

A job's automatic trigger scheduling is activated as soon as it has been submitted to the database. Any submitted jobs that were created with a schedule, either time-based or file-based, will automatically execute the next time the specified trigger occurs.

Job commands

Sending a Main Script

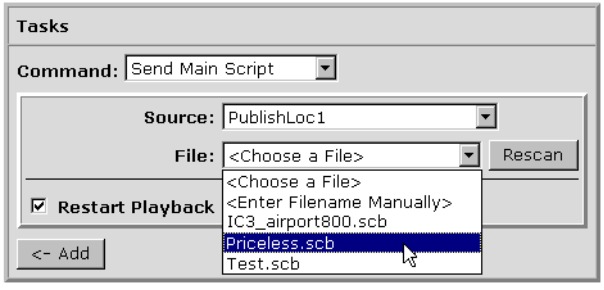
The *Send Main Script* command transfers scripts and their media files to the Content folder of one or more Players.

a. Choose the Publish Location from which to get the script using the *Source:* pop-up. It lists all the Publish Locations that you have already defined.

   After you choose a Publish Location, you see a *File:* pop-up. Network Manager scans the selected Publish Location, and lists in the pop-up all scripts it finds in the defined Publish Location folder.

   The *Rescan* button next to it lets you scan the Publish Location again, if you want to refresh the list to pick up the names of new scripts that have just arrived at the Publish Location. (Publish Locations listed in red are currently disabled, and

will not be accessed by this job until they are re-enabled on the **Publish Locations** page.)



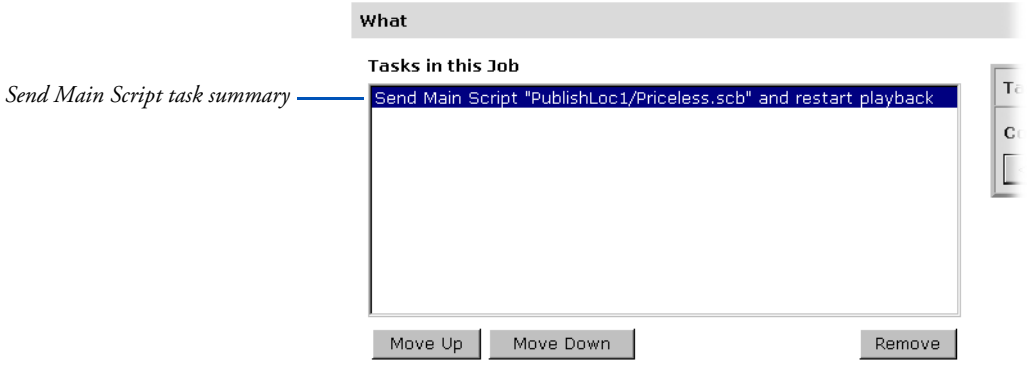
b. From the *File:* pop-up list, choose from the script files available on the Publish Location.

   Or, if the script does not currently exist on the Publish Location, but you expect it to at a later time and know its name, you can enter a name by choosing <*Enter Filename Manually*> from the pop-up. Then type the name into the *File Name:* field that appears.

c. If the change in content is urgent, or if the script does not regularly loop back to the beginning, make sure the *Restart Playback* option is on (✓). This causes the Main Script that is currently running on the Player to exit and the new script to start playback as soon as it is received.

   Leaving *Restart Playback* off allows the current Main Script to continue playing. The new Main Script is not swapped in until the old one has ended and is about to restart.

d. Click the <- *Add* button to add this task to the job. A summary of the task information appears as a line in the *Tasks in this Job* list.



Send Main Script task summary

e. Resume the procedure with step 5 in the "*Creating a job*" section on page 132.

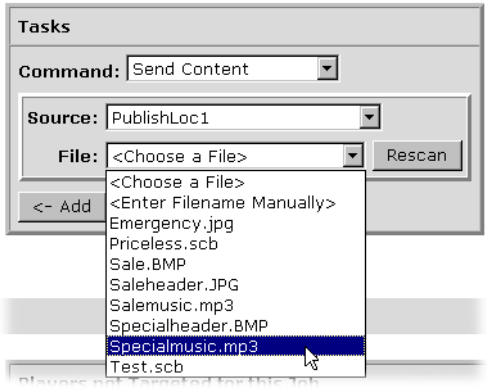
Sending Content

The *Send Content* command transfers content (media files and/or script files that are not intended as Main Scripts) to the Content folder of one or more Players.

a. Choose the Publish Location from which to get the content using the *Source:* pop-up. It lists all the Publish Locations that you have already defined.

After you choose a Publish Location, you see a *File:* pop-up. Network Manager scans the selected Publish Location for files, and lists in the pop-up everything it finds in the defined Publish Location folder.

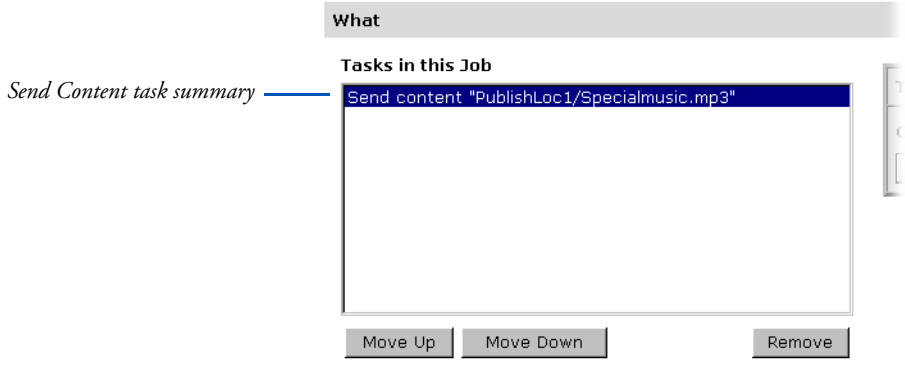
The *Rescan* button next to it lets you scan the Publish Location again, if you want to refresh the list to pick up the names of new files that have just arrived at the Publish Location. (Publish Locations listed in red are currently disabled, and will not be accessed by this job until they are re-enabled on the **Publish Locations** page.)



b. From the *File:* pop-up list, choose from the content files available on the Publish Location.

   Or, if the content file does not currently exist on the Publish Location, but you expect it to at a later time and know its name, you can enter a name into the *File Name:* field.

c. Click the <- *Add* button to add this task to the job. A summary of the task information appears as a line in the *Tasks in this Job* list.



Send Content task summary

d. Resume the procedure with step 5 in the "*Creating a job*" section on page 132.

Maintenance commands

Additional, maintenance-oriented commands are available from the *Command:* pop-up after you choose <*More Commands*>. The additional commands you see are:

- *Install File* – places a file other than a content file on the Player
- *Retrieve Content* – returns a specified content file from the Player to Network Manager
- *Retrieve Files* – returns specified non-content files from the Player to Network Manager
- *Install System File* – places a system file on the Player and reboots to ensure that the file is used by the system
- *Delete Files* – deletes specified files on the Player
- *Delete Unused Content* – deletes content files that are no longer being used by the Player's scripts
- *Run Command* – runs a command line on the Player, such as a batch file, to accomplish miscellaneous work
- *Reboot* – reboots the Player
- *Abort Jobs in Progress* – stops the execution of all jobs that are currently running on the Player
- *Install Software Update* – places a Scala Software Update file on the Player and automatically installs the software

The maintenance commands are discussed individually below. The way you make the *Where* and *When* settings for any of these commands is given in the "*Creating a job*" section on page 132.

Install File

The *Install File* command works much the same as *Send Content*. The primary difference is that Install File is for files other than content,

and therefore requires you to specify the destination path on the Player.

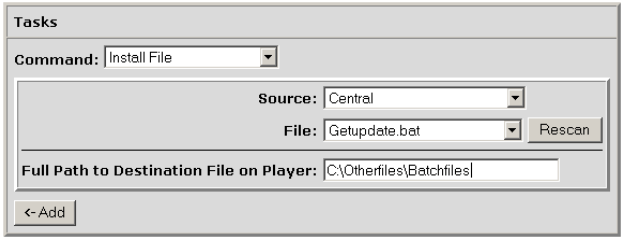
a. Choose a Publish Location from the *Source:* pop-up.

   Network Manager scans the Publish Location file server for files in its content folder just as for Send Content, and provides a list of what it found in the *File:* pop-up.

b. Choose one of the listed files, or choose <*Enter Filename Manually*> and type a filename in the *File Name:* field that appears.

   If you type in a filename that is not currently listed in the *File:* pop-up, that file must exist in the folder on the selected Publish Location at the time the job is run, or the job will fail.

c. Type the path to the location where the file should be installed on the Player in the *Full Path to Destination File on Player:* field. For example, `C:\Otherfiles\Batchfiles`.



d. Click the <- *Add* button to add this task to the job. A summary of the task information appears as a line in the *Tasks in this Job* list.

e. Resume the procedure with step 5 in the "*Creating a job*" section on page 132.

Retrieve Content

The *Retrieve Content* command gets a particular content file from a Player and returns it to the Network Manager server. This can be useful as a way of restoring a script or other content file that was accidentally deleted or corrupted at the authoring end, or to check what is

actually being shown on a Player when questionable content playback has been reported from the field.

a. In the *Content Name:* field, type the name of the content file that you wish to be returned to the Network Manager server. You must know the name of the file. The command looks in the Content folder on the Player so only the name is required, not a full path.

b. Click the <- *Add* button to add this task to the job. A summary of the task information appears as a line in the *Tasks in this Job* list.

c. Resume the procedure with step 5 in the "*Creating a job*" section on page 132.

Retrieved content files are placed in the following location within the Network Manager workspace folder:

`...\Receive\Content\<playername>`

Retrieve Files

The *Retrieve Files* command is similar to *Retrieve Content*, but it can get any file from a Player to return it to the Network Manager server, not just a content file. This command can be useful in verifying proper Player configuration (checking device driver versions, for example).

Retrieve Files supports the use of pattern-matching (the * and ? wildcards) to retrieve files.

a. In the *Full Path to Folder or File on Player:* field, type the path to the file that you wish to be returned to the Network Manager server. You must know the file's location and name. Entering a path to just a folder retrieves the contents of the folder.

b. If you have specified path to a folder, you can also retrieve the contents of the folders within it by turning on (✓) the *Retrieve File(s) in Subfolders* option.

c. Click the <- *Add* button to add this task to the job. A summary of the task information appears as a line in the *Tasks in this Job* list.

d. Resume the procedure with step 5 in the "*Creating a job*" section on page 132.

Retrieved files are placed in the following location within the Network Manager workspace folder:

`...\Receive\Files\<playername>`

Install System File

The *Install System File* command lets you send a file to the Player and then reboot the Player, in single operation. The intended use is for updating files, such as device drivers or other system files, that might be in continual use on the Player. Files that are in use ("locked") cannot be updated seamlessly—a reboot is required to stop and expunge the locked file, so that the newer file can be installed in its place and activated.

Using the command is identical to *Install File*:

a. Choose a Publish Location from the *Source:* pop-up.

   Network Manager scans the Publish Location file server for files in its content folder just as for Send Content, and provides a list of what it found in the *File:* pop-up.

b. Choose one of the listed files, or choose <*Enter Filename Manually*> and type a filename in the *File Name:* field that appears.

   If you type in a filename that is not currently listed in the *File:* pop-up, that file must exist in the content folder on the selected Publish Location at the time the job is run, or the job will fail.

c. Type the path to the location where the file should be installed on the Player in the *Full Path to Destination File on Player:* field. For example, `C:\Program Files\Windows Media Player\Mplayer2.exe`.

When the job runs, the system file is transferred to the Player, then the Player is rebooted. After the reboot, the new system file runs from the destination location you specified.

d. Click the <- *Add* button to add this task to the job. A summary of the task information appears as a line in the *Tasks in this Job* list.

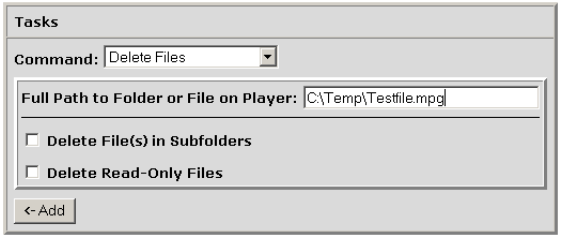
e. Resume the procedure with step 5 in the "*Creating a job*" section on page 132.

Delete Files

At times you may need to delete files on a Player. The *Delete Files* command allows you to do so. You can delete any non-locked file or folder on a Player with this command, provided that you know the full path to the item.

Note, however, that for the common Player maintenance task of deleting old content that is no longer needed, the *Delete Unused Content* command (discussed in the following section) is preferable, as it is both simpler to use and safer.

a. In the *Full Path to Folder or File on Player:* field, type the path to the item you want to delete, beginning with its drive letter. For example, `C:\Temp\Testfile.mpg`.



b. If the item is a folder and you want to also delete the contents of any subfolders, select the *Delete File(s) in Subfolders* option.

c. If you want the deletion to include files with the Read-Only attribute set, select the *Delete Read-Only Files* option.

d. Click the <- *Add* button to add this task to the job. A summary of the task information appears as a line in the *Tasks in this Job* list.

e. Resume the procedure with step 5 in the "*Creating a job*" section on page 132.

Delete Unused Content

As scripts on the Player are continually updated, scripts and their files that are no longer in use will accumulate. Unneeded files can fill the Player's hard drive, leaving insufficient room for further updates and general operation. This can happen quickly when much content is in the form of large digital video files.

The *Delete Unused Content* command provides a simple way to reclaim drive space from outdated files. It identifies any content in the Content folder that is no longer in use and deletes it from the Player. Scripts and media files are deleted only if the Main Script and its subscripts, if any, make no use of them.

a. The *Delete Unused Content* command has no options. Just choose it from the *Command:* pop-up.

b. Click the <- *Add* button to add this task to the job. The command appears as a line in the *Tasks in this Job* list.

c. Resume the procedure with step 5 in the "*Creating a job*" section on page 132.

Reboot

A Player that is not responding or not operating normally can sometimes be revived by rebooting it. Regular reboots of Players (generally weekly, at the least conspicuous time) are recommended as general maintenance practice to keep the machines functioning smoothly.

a. The *Reboot* command has no options. Just choose it from the *Command:* pop-up.

b. Click the <- *Add* button to add this task to the job. The command appears as a line in the *Tasks in this Job* list.

c. Resume the procedure with step 5 in the "*Creating a job*" section on page 132.

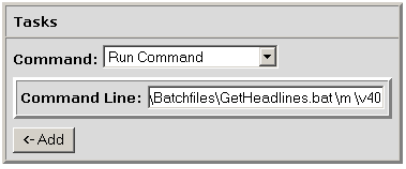
Run Command

Using the *Run Command* maintenance command, you can run almost any program on the Player that can be executed from a command line, provided that it is not something that interferes with normal Player operation. It is similar to using a Launch EX event within a script.

Typically, this command would be used to do something like run a batch file that fetches content from some source external to Network Manager Publish Locations. However, the range of possible applications for this command is limitless.

a. Type the command in the *Command Line:* field just as you would in a Windows Command Prompt window, with whatever paths and switches are appropriate. For example,

```
C:\Otherfiles\Batchfiles\GetHeadlines.bat \m \v40
```



To prevent the possibility of script playback being disrupted, the command you enter will automatically be forced to run minimized. The Player software is designed to block attempts by any other software to switch out the InfoChannel Player application.

b. Click the <- *Add* button to add this task to the job. A summary of the task information appears as a line in the *Tasks in this Job* list.

c. Resume the procedure with step 5 in the "*Creating a job*" section on page 132.

Abort Jobs in Progress

A Player that is executing a Network Manager job can have its job execution stopped by receiving the *Abort Jobs in Progress* command. This can be useful for a Player that is malfunctioning and is "stuck", or when you simply want to interrupt a problem job for some reason.

a. The *Abort Jobs in Progress* command has no options. Just choose it from the *Command:* pop-up.

b. Click the <- *Add* button to add this task to the job. The command appears as a line in the *Tasks in this Job* list.

c. Resume the procedure with step 5 in the "*Creating a job*" section on page 132.

Install Software Update

The *Install Software Update* command lets you send an ICPlayer software update to the Player and have it automatically installed.

Using the command is similar to the other *Install* commands, but it is not necessary to specify a destination path. The ICPlayer Software Update file must have previously been copied from the Scala Service Plan Software Release CD to a Publish Location. Also, you must have the username and password of an Administrator-level account on the Player.

a. Choose a Publish Location from the *Source:* pop-up.

   Network Manager scans the Publish Location file server for .CAB files in its content folder, and provides a list of what it found in the *File:* pop-up.

b. Choose the ICPlayer update .CAB file from the listed files, or choose <*Enter Filename Manually*> and type the filename in the *File Name:* field that appears.

   If you type in a filename that is not currently listed in the *File:* pop-up, that file must exist in the content folder on the selected Publish Location at the time the job is run, or the job will fail.

c. Software installation requires Administrator-level access to the destination machine. If the Player is already running under such an account, no further input is needed and you can skip to step e.

   However, if the Player is not running under an Administrator-level account, you must invoke one. Enter the username of an Administrator-level account on the Player in the *Optional User Name:* box.

d. Enter the password for the Administrator-level account in the *Optional Password:* and *Confirm Password:* boxes.

e. Click the <- *Add* button to add this task to the job. A summary of the task information appears as a line in the *Tasks in this Job* list.

   When the job runs, the update file is transferred to the Player, and an install process is run (under the specified account username if you gave one), installing the update. Then the Player is rebooted. After the reboot, the Player is running with updated ICPlayer software.

f. Resume the procedure with step 5 in the "*Creating a job*" section on page 132.

Editing a job

The job names in the *Name* column of the **Jobs** page are links that open the **Edit Job** form. This form is identical to the **New Job** form described in the preceding section.

To edit a job:

1. Click its link in the *Name* column on the **Jobs** page.

2. Make any changes necessary to the job settings on the **Edit Job** form.
3. Click *OK*.
4. Click *SUBMIT CHANGES*.

Your changes are reflected in the listing.

Running a job manually

In addition to automatically triggered execution, jobs can be run manually by the Network Manager operator whenever necessary.

Some jobs by their nature are not suited to be run on a scheduled basis, and would normally be run manually, only when needed. Even jobs that are scheduled may need to be run manually in certain circumstances. For example, if a script gets a very important update, you might manually run the scheduled Send Content job sooner than usual, so that the update is received as soon as possible.

To run a job manually:

1. Select it by clicking the checkbox next to its lightbulb icon.

2. Click the *Run Now* button at the bottom of the **Jobs** page.

   You see a confirmation dialog, and if you click *Yes*, you are automatically switched to the **Job Activity** page so that you can observe the progress of the job.

There is no need to submit changes, because running manually does not change anything in the Network Manager databases. If unsubmitted changes do exist, you see a dialog asking if you want to save them.

Running a job manually does not affect when it will run by any automatic triggers it may have.

Enabling and disabling jobs

Occasionally you may need to temporarily prevent scheduled jobs from running. If you know that a Player is malfunctioning or otherwise unable to communicate, for example, you can avoid repeated error messages in the activity logs by keeping its jobs from running.

Doing so is possible without having to delete and then re-create the jobs when you later need them by disabling them.

When you disable a job, its definition remains unchanged. It only stops responding to time based or file change triggers that would cause it to run.

A disabled job can still be run manually using the *Run Now* button.

To disable an enabled job:

1. Select it by clicking the checkbox next to its lightbulb icon.
2. Click the *Disable* button. You see its lightbulb darken.
3. Click *SUBMIT CHANGES*.

The job will no longer run when scheduled. It still can be run manually.

To enable a disabled job:

1. Select it by clicking the checkbox next to its darkened lightbulb icon.
2. Click the *Enable* button. You see its lightbulb light up.
3. Click *SUBMIT CHANGES*.

The job will resume its run schedule.

Deleting a job

If you are sure that you will never need an existing job again, you can delete it.

To delete a job:

1. Select it by clicking the checkbox next to its lightbulb icon.
2. Click the *Delete* button. You see a confirmation dialog.
3. Click *OK* in the dialog.
4. Click *SUBMIT CHANGES*.

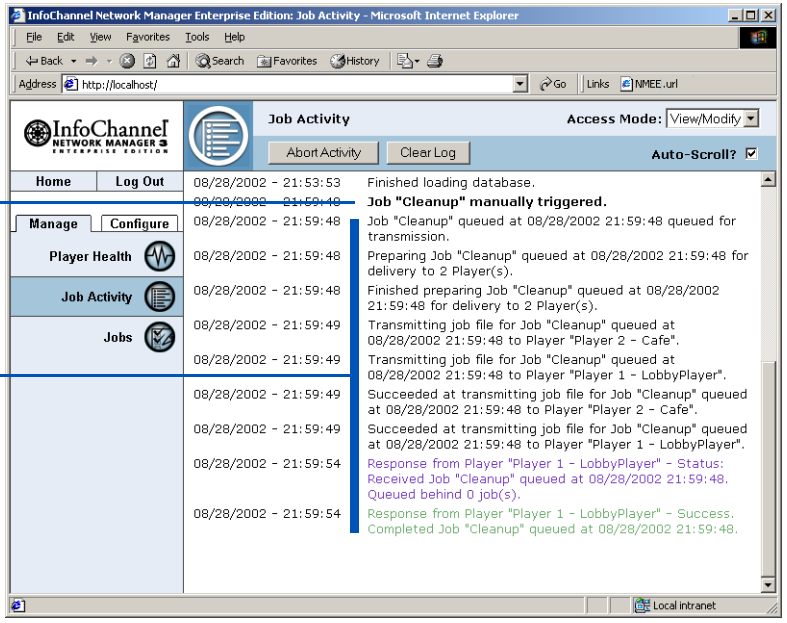
The job is deleted and no longer listed.

Monitoring job activity

The **Job Activity** page, accessible by clicking the *Job Activity* icon in the *Manage* panel of the control frame, lets you view messages that Network Manager outputs as it is performing job-related activity.

This is the same information that is recorded in the log files, and can be useful in tracking down problems with your installation, as well as helping Scala Technical Support identify and eliminate any problems in the software.

You are automatically jumped to this page when you trigger a job manually using the *Run Now* button.



a Run Now job, displayed in bold

typical activity messages for a successful job to one Player

All entries are timestamped, and the **Job Activity** page uses different colors to help you distinguish different types of entries:

- Black: Network Manager actions
- Purple: Job-received responses from Players
- Green: Job success responses from Players
- Amber: Job failure responses from Players
- Blue: FTP related messages (Direct FTP connections only)
- Red: Errors in communication or other Network Manager errors

If the messages on the **Job Activity** page indicate that a job is "stuck", for example continually retrying to send a job to a machine that is down, you can stop the retries by clicking the *Abort Activity* button.

Controlling the activity display

Job activity can be displayed with varying degrees of detail. The detail level can be changed using the *Activity Logging Detail:* control on the **System Settings** page. Lower levels of detail omit messages about less-significant steps in the job process; the Diagnostic level includes the most extensive and technical information.

To make the **Job Activity** page easier to read, you can clear the display of previous messages so that new activity messages start appearing from the top down. Click *Clear Log* to do this. *Clear Log* only clears the display; the activity log file is not affected.

Later messages appear below earlier messages. When the page has filled with activity messages, the display automatically scrolls the entire display upward so that the latest message is always visible at the bottom. To disable this feature if you need to focus on the details of a particular message for some time, turn off the *Auto-scroll?* option.

Working in InfoChannel Network Manager

10: Working in InfoChannel Network Manager

Chapter 9 of this User's Guide covered creating jobs, detailing the setup of jobs using the individual job commands.

This chapter discusses how you work in InfoChannel Network Manager from a task-oriented perspective. It will help you to understand how best to accomplish the various tasks that will take up the bulk of the time you spend in Network Manager.

In an operating InfoChannel Network, the work you do in InfoChannel Network Manager falls into two general categories:

- Content update tasks
- Maintenance tasks

Updating Player content

The most common Network Manager jobs are the *Send Main Script* and *Send Content* jobs, covered starting on page 137 of chapter 9.

The nature of InfoChannel Network applications is that content (scripts and/or their constituent media files) constantly need to be updated. You update content on Players by sending newer content files using a Send Content job.

There are three ways to update content:

- Sending a new script as the Main Script
- Sending a content file for use as linked content
- By a custom-programmed process external to Network Manager

Sending Main Scripts

When you send a script as a Main Script, it completely replaces the Main Script currently playing on the Player.

Restarting

One decision for you to make is whether the updated script replaces the current one immediately (interrupting the current script's playback) or waits until the current script comes to its natural end before being swapped in.

Turn on the *Restart Playback* option if the update is urgent (for example, late-breaking news, or a fix for an embarrassing script mistake). Another reason for using the Restart option is if the script contains an internal loop such that it never normally restarts from the beginning.

Atomic scripts

An ICDesigner script is published and transmitted "atomically", as a single file containing the script itself and all its media files. When a published script is received by a Player, it is unpacked into separate folders and files according to a special naming scheme and structure (see "*How content is stored on a Player*" on page 106 in chapter 7).

It is not possible to independently update constituent content files of a script unless those files were authored as "linked content" (see "*Sending linked content*" on page 158).

Storage of content on the Player

When new, updated content is sent to the Player, older versions of the same files with the same file names are automatically deleted. However, some content files that outlive their usefulness are not replaced, scripts simply no longer reference them. When this happens, the unused content files are not automatically deleted; they remain on the Player.

If scripts change frequently, and/or they contain large media files, such as MPEG digital video, the Player hard drive can start to fill with files that are no longer used. If the hard drive becomes too full with such accumulated files, system performance is impaired, and further script updates may not succeed.

This is the reason for the Network Manager *Delete Unused Content* command (see "*Deleting unused content*" on page 162).

Sending linked content

Linked content is the InfoChannel Network approach to allowing content files—sub-scripts or media files—to be independently updated. The benefits of using linked content are considerable:

- Transmission bandwidth savings—linked files can be updated without having to re-send the entire script
- Flexibility in scheduling updates—linked content can be updated more frequently or less frequently than the full script
- Smooth file replacement—even files that are locked (in use) can be transparently and efficiently replaced while the Player runs
- Worry-free updating—serial versionation means the latest version of a linked file is guaranteed to be used the next time it is displayed
- Flexibility in the source of the content—files do not necessarily have to be transmitted through Network Manager

A linked script is stored on the Player alongside the Main Script, in the same layout. All linked individual media files sent through Network Manager are placed in the Content folder at the same level as the Shared Files folder, and have their filenames versionated.

From Network Manager

Sending linked content using Network Manager is basically the same as sending any other content: just select it from the *File:* pop-up in the *Send Content* section of the **Edit Job** form. If it is a script, make sure you use a *Send Content* command, not *Send Main Script*. (Scripts sent as linked content are by definition sub-scripts and thus cannot be Main Scripts.)

To be available from the *File:* pop-up, individual files must be manually placed on a Publish Location machine in the same folder as the .scb files of published scripts.

From external sources

Sending or obtaining linked content from external sources takes more doing than using Network Manager, but it can be a very powerful way

to expand the range of content in your scripts. Some typical examples of how this approach could be used:

- a news headline MPEG file is uploaded hourly from a national news service Web site
- Financial data is parsed from a database, uploaded as text and streamed into a cued Text Crawl
- Local traffic information is downloaded by the Player

Doing this requires a third-party utility and/or custom programming that can access the desired data and perform the communication tasks involved. A detailed description of how to accomplish this is beyond the scope of this guide, but these tasks are not fundamentally difficult for someone with technical expertise.

The key to success is that at the Player end, the linked file must end up in the right place with the right name.

How linked content works

To manage and work with linked content, it is important to understand what it is and isn't.

Linked content is not a special type of content. Files designated as "linked" are ordinary script or media files, no different from what they were before they were linked, with one exception: when they reach the Player through Network Manager, their filenames have a semicolon (;) and a serial number inserted before the extension to "versionate" them. The number is a simple increasing serial number that represents the order in which files with the same name have been received.

The filename is the crucial factor in making linked content work. The name of the linked file on the Player must match the name that was used as the link in authoring the script. The versionation number in the name is ignored for matching purposes. For example:

Filename seen in authoring: **Headlines.mpg**

Filename as received on Player: **Headlines;3.mpg**

As long as a file by this base name exists in the Content or InstalledContent folders on the Player, then any script that was authored using linked content named "Headlines.mpg" would link to this file.

If there is more than one "Headlines;<*version*>.mpg" file in the Player's Content or InstalledContent folders, the one with the latest version number in the filename is the one linked to. If, while a linked file is in the process of playback, a newer version of that linked file arrives at the Player, the script is not interrupted. The next time the script needs to play back that file, the newest one is used.

Files become links during script authoring by being loaded into the script from the Linked Content folder, a special location defined on the InfoChannel Designer 3 authoring station.

Files loaded from the Linked Content folder look and feel no different from ordinary files to script authors. However, the files that the authors see function only as placeholders for preview positioning and timing purposes. When a script with linked content is published to the InfoChannel Network, the linked content files the authors saw are not included with the script—only references to their names.

Making sure linked content works

The InfoChannel Network administrator's responsibilities to ensure that linked content works properly include:

- Giving script authors appropriate files to use as placeholders

  Files placed in the Linked Content folder for authoring purposes should be representative in size, running time, etc., of the actual content files that will be linked to so that the scripts will appear as expected on playback. The ICDesigner Start menu has a shortcut to the Linked Content folder to make it easy to drop files there.

- Making sure script authors know where to use the Linked Content files

- Placing, in a separate step, the actual content files on the Players

  The names of the content files sent must match the names of the files used in authoring exactly. (The one exception: files that have

been previously published, then retrieved from a Player and are thus already versionated can be re-used as linked content like any file. The version characters are ignored for purposes of matching the file name, and are updated when the file is received on a Player.)

Linked content files can be sent with a Network Manager Send Content job, downloaded by a separate application, or copied to the Player machine's hard drive manually.

- Placing the content files in the proper place

  If you are sending linked content files via a Network Manager Send Content job, you do not need to worry about where files end up. That is managed for you automatically.

  Files placed on a Player by any means other than a Network Manager job should go in the InstalledContent folder. In order to be found by the Player software, files placed in InstalledContent must not be in subfolders; they must be at the "top" of the folder.

Performing Player maintenance

Aside from updating content, an InfoChannel Network administrator's other primary work within Network Manager is Player maintenance. Keeping up with maintenance tasks help ensure that the Network continues to function smoothly and reliably.

Maintenance can be divided into regular and occasional categories.

Regular maintenance tasks

There are three maintenance tasks that need to be done on a regular basis on any InfoChannel Network installation:

- Rebooting the Players
- Deleting unused content
- Reviewing Player status

Rebooting the Players

Scala recommends that all Players be rebooted weekly. In a world of bulletproof, bug-free device drivers and system software, this would not be necessary, but in the real world, it is only prudent. Planned reboots are far less disruptive than crashes due to memory leaks or corrupted files.

Set up a *Reboot* job with a time-based trigger for the least noticeable time, for example, Every Sunday at 10 minutes past 4 am.

Deleting unused content

As noted in chapter 7, unused content is not automatically deleted from a Player. Old content that is no longer used can build up, eventually filling the Player's hard drive and preventing it from working.

The solution to this problem is to schedule regular *Delete Unused Content* jobs for all Players. This command examines the Content folder on the Player. Any scripts or linked content that is not referenced directly or indirectly by the Main Script is deleted by this command.

How often you need to run a *Delete Unused Content* job will depend on the frequency of content updates, the degree of script changes in the updates, and the amount of free space on the Player's hard drive.

InfoChannel Note

Delete Unused Content does not affect the InstalledContent folder. Unused content files that accumulate there must be deleted explicitly using *Delete Files* jobs.

Reviewing Player status

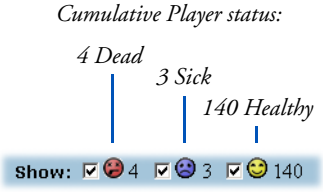
Part of an InfoChannel Network administrator's daily routine should be a review of both the Network Manager **Player Health** pages and the **Job Activity** page. They tell you what you need to know about what is currently going on in your InfoChannel Network, and how well your Players are operating.

Job Activity gives a real-time view of what Network Manager is doing at the moment. It also retains all the displayed messages about jobs that have run and their results, so that you have a cumulative history. Errors, listed in red, indicate problems that must be investigated.

The view offered by this page is good for getting immediate feedback on manually-run jobs, and for quickly looking through the history to determine when problems occurred.

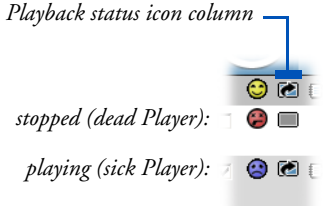
When you want to see at a glance which Players are functioning well and which are not, the **Job Activity** view is not ideal. Health monitoring is available for this purpose.

Player Health graphically shows you the status of all your Players, and allows you to examine the activity record in a per-Player format that lets you retrieve log files from those that are reporting errors. This makes it possible to determine the cause of the problems so you can decide how to fix them.



Players that have reported errors in communication and/or script playback but are still sending heartbeats show up in the Player Health listing as "sick". Players from which no heartbeats are being received are declared "dead".

Dead Players may not respond to any communication attempts, and thus can require a visit from a field technician. Sick Players, however, stand a good chance of being "cured" of software-related problems through appropriate Network Manager maintenance jobs.



The Player Health pages also have an icon column to draw attention to the playback status of your Players. It is possible for otherwise-healthy Players to not be performing their main function of script playback, for example if someone closed or minimized the playback window on the Player machine.

Using Player Health Monitoring is covered in detail in chapter 11.

Reviewing the IC.log file

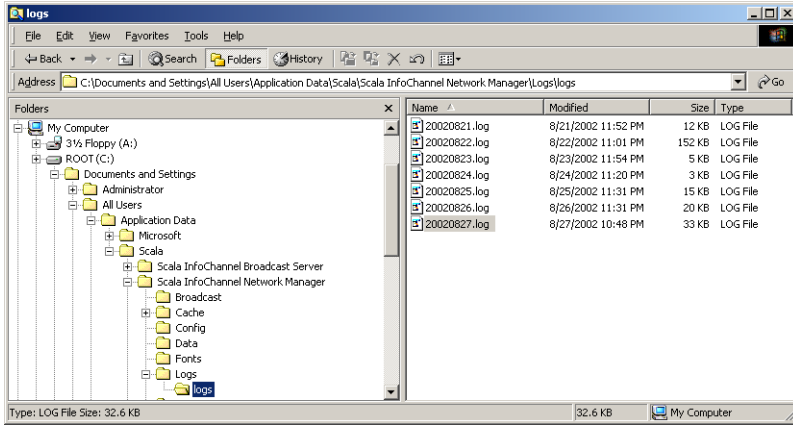
If you want to examine the activity record in more detail than simply scrolling through a list of messages, you can open the file Ic.log, which is a text file version of what appears in the **Job Activity** page. By opening Ic.log in a text editor, for example, you could use a text search to quick scan through all messages pertaining to a specific Player.

The Ic.log file for the Network Manager machine is typically located in:

```
<systemroot>:\Documents and Settings\All Users\Application
Data\Scala\Scala InfoChannel Network Manager\Logs
```

where *<systemroot>* is the drive letter where Windows is installed.

Ic.log contains the activity messages for the current day. At midnight each day (assuming the Network Manager Engine is running) the Ic.log file is renamed with a datestamp to "*<yyyymmdd>*.log" and placed in a folder named "logs" that is within the Logs folder named above, as illustrated here:



Then a new Ic.log is begun. A week of archived log files is retained in this folder. Every day the oldest file is deleted after the newest one is added.

Reviewing Player log files

Per-Player log files are maintained on each Player. If you are having problems with a particular Player and want to study its activity record in detail, you need to examine its log file. The usual way to do this is through the **Player Health: Log File Reader** page. But if for some reason you are unable to retrieve the log via that method, you can do so "manually".

ICPlayer Note

When you install the ICPlayer software, the installer creates a shortcut on the Windows Start menu to the Logs folder.

On a Player, log files are normally stored in the following location:

```
<systemroot>:\Documents and Settings\All Users\Application
Data\Scala\Scala InfoChannel Player\Logs
```

The log generation and archiving scheme on the Players is the same as on the Network Manager machine: an Ic.log file for the current day, and the previous week's datestamped .log files stored in the Logs\logs folder.

Use a *Retrieve Files* job to return a log file from a specific Player, or from several Players at once. Use the above path, substituting the correct drive letter for <*systemroot*> and appending "\Ic.log" or "\logs*.log".

Retrieved files are placed in the following location within the Network Manager workspace folder, which also has a Start menu shortcut:

```
...\Receive\Files\<playername>
```

Occasional maintenance tasks

Various other tasks that are periodically necessary to keep Players running smoothly can be performed remotely using Network Manager jobs.

Bear in mind that the *Install System Files*, *Install Files*, *Delete Files*, and *Run Command* job commands should be used with care, as they are potentially hazardous. A *Delete Files* command that uses pattern-matching (the * and ? wildcards) is especially high-risk.

If you overwrite, delete, or run a file on a remote computer, you cannot directly and immediately observe the results. Unexpected results could include freezing or crashing the machine. Beyond that point, Network Manager would not be of any use until the Player could be rebooted manually.

Installing files

To send files to a Player that are something other than script content, use an *Install File* job. The *Install File* command allows you to specify a full path, so you can put the file anywhere on the Player.

Use this kind of job to send batch files, software archives to be installed, and other types of files.

If a file by the same name already exists in the location given in the command, that file is overwritten by the file you send, so be careful.

Installing system files

At times you may need to install a new driver, restore a corrupted DLL, or replace some other system-level file on a Player. Since such files are normally in constant use, just overwriting the file is not enough. The Player must be rebooted for the new file to be activated.

An *Install System File* job is what you should use in such cases. This command is essentially the same as *Install File*, except that it reboots the Player after it installs the file. You can include as many *Install System File* tasks in a single job as you need to install multiple system files; the Player is rebooted only once, after all files have been installed.

If a file by the same name already exists in the location given in the command, that file is overwritten by the file you send, so be careful.

Installing Software Updates

Scala periodically distributes update releases (service packs) of its software that add performance enhancements, bug fixes, and new features to the InfoChannel software. You should install new software releases as soon as possible after they are available to keep your InfoChannel Networks up to date.

The *Install Software Update* command enables automated updating of the ICPlayer software on remote Players via a Network Manager job.

Note that this command was added as a new feature in Release 4 of the Network Manager/ICPlayer software. It can be used to install later releases of ICPlayer software on Players that already have Release 4 or above installed on them. **It cannot, however, be used to update Players *to* Release 4 or above—that must be done through a normal install from the Scala Software Release CD-ROM.**

Retrieving content

Generally, content flows from Network Manager to Players. However, it is sometimes useful to get content from Players. The most typical reasons:

- to get back a script or other media files mistakenly deleted from the Network Manager machine or authoring machine
- to check linked content that was sent to Players from an outside source, to be sure that the content is what it is supposed to be

Use a *Retrieve Content* job for this task. You only need to know the name of the script or linked file, not a full path, since all content files reside in a single folder on the Player.

A retrieved script remains in its published form—a relatively small <*scriptname*>.scb file accompanied by specially-named folders in Shared Files containing all the content. The retrieved script can be loaded back into ICDesigner by loading the .scb file, and can be edited, played back, and republished like any script. However, the script will no longer reference the original content files on the authoring station, as the published script now references the content in the Shared Files folder.

Retrieving files

A *Retrieve Files* job can have various uses:

- checking file versions
- getting a Player-specific batch file or Windows script file back for editing

If for any reason you need to get a file other than a content file from a Player, use a *Retrieve Files* job. *Retrieve Files* allows the use of standard wildcards (*, ?) in the name in the *Full Path* box. This lets you retrieve multiple files with one command, or retrieve a file having a name you do not know exactly.

So for example, you could use “Vidx??.dll” to retrieve Vidx03.dll, Vidx05.dll, Vidx9b.dll and so on, or “*.bat” to retrieve all .bat files in the folder.

Deleting files

Files on a Player other than those in Content occasionally need to be deleted. Use a *Delete Files* job for this. You need to know the exact path to the file.

Because the *Delete File* command can be particularly hazardous, it has options that allow you to decide whether to exclude sub-folder contents and read-only files from its action.

Delete Files allows the use of standard wildcards (*, ?) in the name in the *Full Path* box. This lets you delete multiple files with one command, or delete a file having a name you do not know exactly.

> ***CAUTION***
>
> A pattern-matching *Delete Files* command is very powerful. Improperly specifying a match pattern could be destructive to a Player system, especially if the option to include subfolders is enabled. Use such a command only when you are certain of its consequences.

Running commands

A *Run Command* job lets you execute an arbitrary command line on the Player. Thus you can run any program or batch file that does not require interactive input. Among many potential uses, some likely ones would be:

- running a batch file that downloaded linked content from an external site
- running a disk defragmenting utility
- unpacking and running a software installer

Stopping jobs

There might be occasions when you want to stop a Player from running jobs it is currently running:

- a malfunction of some kind has caused the Player to become "stuck"
- you realize that a job that the Player is running is the wrong job, or an incorrectly-specified job, which could be lengthy or dangerous to allow to run to completion
- you need to send a job to fix a problem, but the Player is caught in a series of retries that would be unnecessary and time-consuming to wait for

An *Abort Jobs in Progress* job is called for in such cases.

Using Health Monitoring

11: Using Health Monitoring

The Health Monitoring system in InfoChannel Network Manager gives you an easy way to keep track of the status of all the Players in your InfoChannel Network. It is your first line of defense against unscheduled Player outages and network malfunctions.

Player Health Monitoring allows you to:

- see the status of all Players at once
- see the status details of individual Players
- see problem Players grouped by errors that they have in common
- retrieve and read log files from particular Players, including Windows logs, to help you diagnose problems
- have automatic alert emails sent to a system administrator when a new problem occurs on a Player
- clear errors so that they no longer produce alerts or affect status

How it works

Health Monitoring works by having all Players send out a "heartbeat" at a regular interval. The heartbeat is a very brief status message that simply identifies the Player that sent it and notes whether there are any outstanding problems that have been logged for that Player.

Players that have outstanding problems are designated as "sick". A sick Player might still be functioning correctly, but logged a problem event that threatens its future operation. Even an error that results in disrupted or stopped playback is likely to leave the Player Engine running, and capable of reporting its status and responding to communication.

InfoChannel Note

Heartbeat status messages are independent of the messages that the Player normally sends back to Network Manager in the course of running jobs.

Network Manager expects to receive a heartbeat from every Player at the specified interval. If Network Manager hasn't

received a heartbeat from a given Player for too long, that Player is considered "dead".

Keep in mind that "dead" status is based on a lack of communication, and thus is a presumption, not a confirmed fact. A Player that is listed as dead might in fact still be functioning correctly, as there are various possible causes for the lack of a heartbeat other than a failed Player—a bad network connection, or misconfiguration, for example.

Enabling and disabling Health Monitoring

Health Monitoring can be enabled or disabled on the **System Settings** page.

By default, Health Monitoring is disabled when you first install the Network Manager software, because there are system-specific configuration steps that you must complete before it can operate properly.

The basic Health Monitoring configuration steps are described in chapter 4, starting on page 76.

When you have completed these steps, you can enable Health Monitoring. When you do so, the *Player Health* icon becomes available on the *Manage* panel of the control frame.

When to disable Health Monitoring

Scala strongly recommends that you enable Health Monitoring, in view of how much more easily you can notice and address problems in your network using the feedback it provides.

However, there are reasons you might want to disable the Health Monitoring system:

- If your Players do not have a back channel

  The operation of Health Monitoring depends on messages being sent back to Network Manager. This requires a "back channel" from the Players. Some network implementations—such as broadcast-only networks with no point-to-point connection—have no back channel, and thus cannot use Health Monitoring.

Health Monitoring should be disabled in such cases, so that Players do not attempt to send heartbeats.

- If you are using a Shared Folder based InfoChannel Network that uses an unsuitable type of LAN

  Health Monitoring depends on IP or domain-name style machine addressing in order to work. Non-TCP/IP LANs that do not support such addressing cannot use Health Monitoring. Health Monitoring should be disabled in such cases, so that Players do not attempt to send heartbeats.

- If network connections for heartbeat messages are costly

  A network in which Players connect to Network Manager via dial-up would require a separate phone call for each heartbeat. If each phone call to an ISP incurs a charge, this could quickly become expensive for all but the smallest networks. One way to avoid the cost is simply to disable Health Monitoring.

  An alternate approach to this problem would be to set a very long heartbeat interval. This would minimize the connection charges, while still allowing you to take advantage of Health Monitoring. The trade-off in that case would be in reducing how quickly you could notice and respond to network problems.

The Player Health pages

The **Player Health** pages are accessible from the *Manage* panel of the control frame when Health Monitoring has been enabled.

Several views of the Network are available from this location, to allow you to get the most useful picture of the state of Player Health:

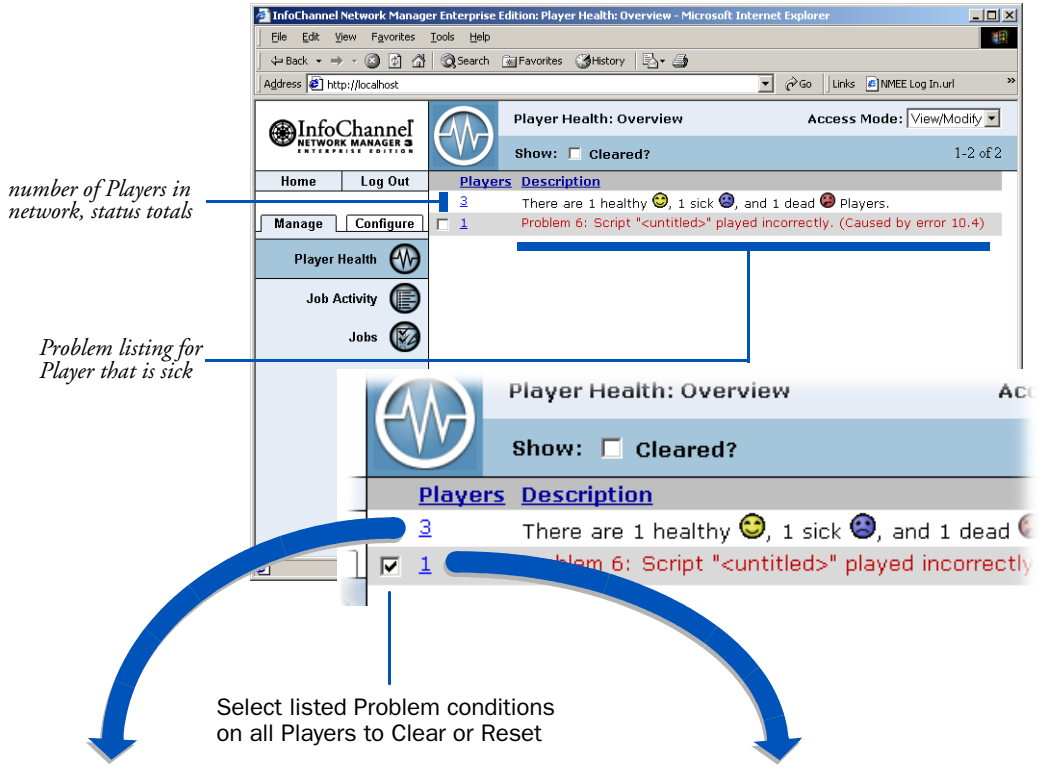
- Player Health: Overview
- Player Health: Whole Network
- Player Health: All Players with Selected Problem
- Player Health: Log File Reader

All of these views share the same basic rows and columns layout of other list pages in Network Manager. They can be set to automatically refresh their contents to reflect up-to-the-moment Player status, or have this capability disabled. All have *Show:* options to allow you to filter the information displayed in different ways.

So that you can see and compare the histories of several Players at a time, the Log File Reader opens in a separate window, one per Player.

Player Health: Overview

When you click the *Player Health* icon, you first see the **Player Health: Overview** screen. It provides the most concise and general view of network health.



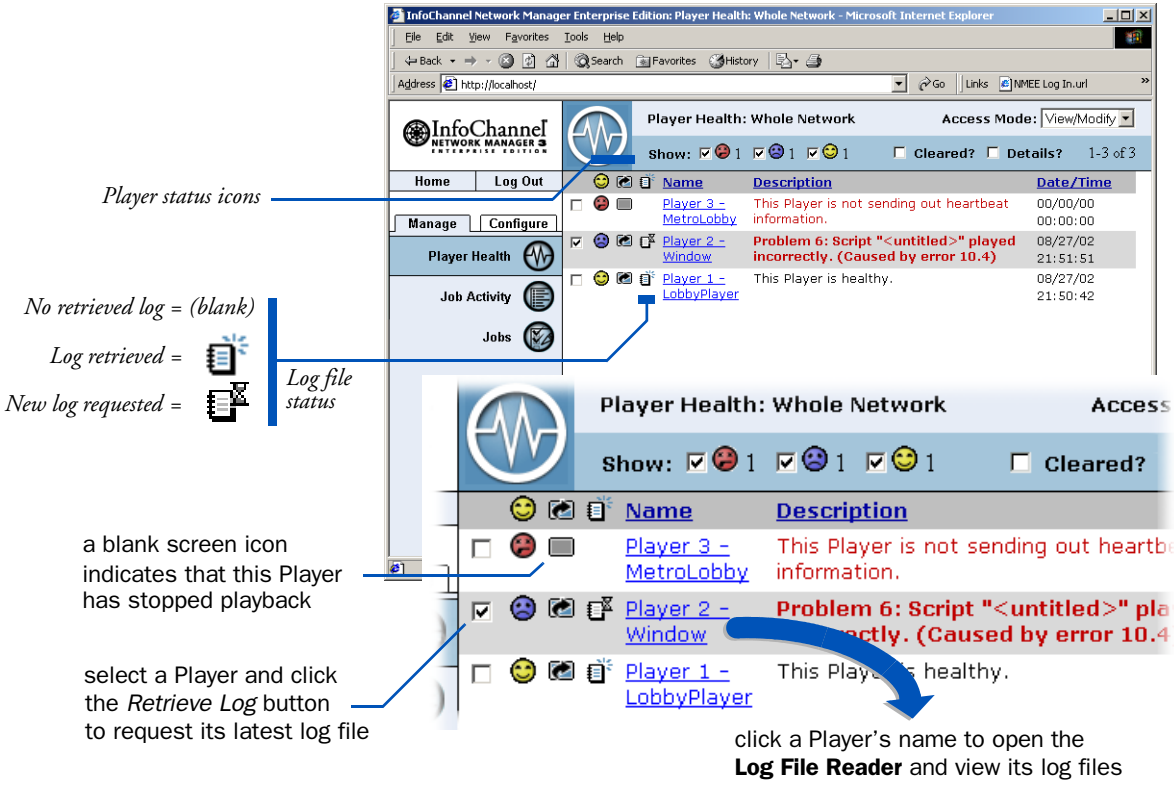
The top line of this view shows the total number of Players in this InfoChannel Network, then a breakdown into totals for healthy (), sick (), and dead () Players, using corresponding icons.

Below this, each existing uncleared Problem on the network, if any, is listed in red, with the number of Players suffering from the Problem given in the *Players* column.

Player Health: Whole Network

In the **Player Health: Whole Network** view, each Player is listed. Dead Players are normally listed first, healthy Players last.

Sick Players are shown with the most significant problem condition for each. The most significant condition is the *oldest* Error-level Problem that has not been cleared.



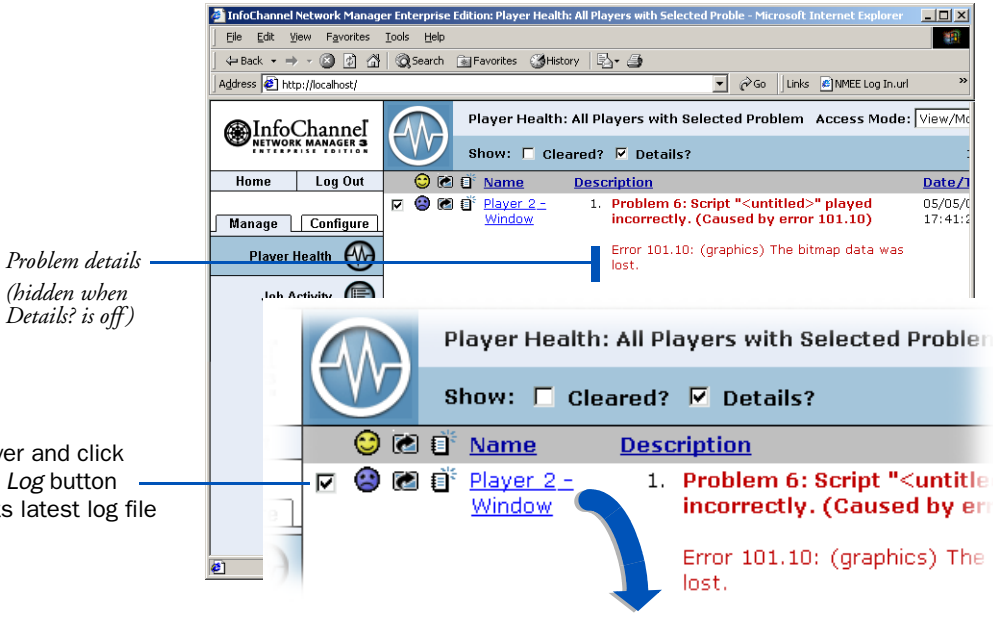
The *Show:* options at the top of this page allow you to decide which of the three Player status levels are visible (the number of Players at each level is shown next to its icon).

The column headed by the InfoChannel Player 3 logo icon is there to draw attention to the playback status of the Players, which is independent of their communication status. When the icon appears in the column, the Player's playback engine is operating, indicating that the Player is playing its script normally. A blank screen icon in this column indicates that the Player is not playing back.

Player Health: All Players with Selected Problem

In the **Player Health: All Players with Selected Problem** view, all the Players that are listed share the same Problem.

Here, the *Show:* options include *Details?*, which when selected gives additional information about the Problem to help in diagnosing what went wrong.



Player Health: Log File Reader

The **Player Health: Log File Reader** view is different from the other Player Health views. It opens in a separate window for a particular Player. It offers an easy and versatile way to view a Player's logs, for a truly detailed account of its operational history.

Each log entry is timestamped, and identified according to the type of message: information, warning, or error. Errors are shown in red, cleared errors in green.

Repeated error display

To prevent clutter in the log from repeated errors, when the same error occurs several times consecutively, there is a single listing for the error under the timestamp of its first occurrence. Such entries have a prominent notation of how many times the error has happened.

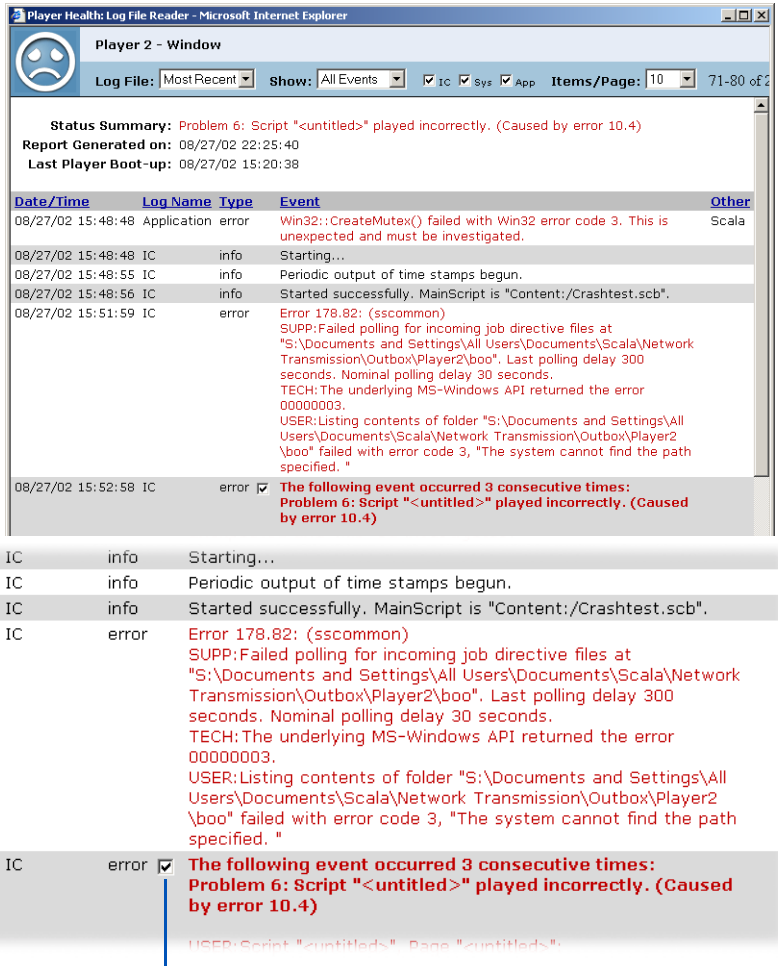
Windows logs

The reader shows not just InfoChannel (IC) logs, but messages in the Windows System and Application logs as well, to give a more complete picture.

Filtering the log file display

There are several *Show:* options to filter what appears in the Reader window. As with the other views, these options let you focus on what you need to find: you can limit the display to Warnings and Errors, or

just Errors, and you can choose which of the three logs (InfoChannel, Windows System, Windows Application) displays its messages.



In addition, you can choose which version of the log file you want to view—the default is the most recent log file, but previous days' log files, each of which is stored separately, are also kept available.

Reading log files

Some hints for reading through log files:

- When events are sorted by the *Date/Time* column (the default), the *oldest* events in the log are on page 1, the most recent events on the last page. Use the "Last page" link (>|) to jump to the most recent messages.
- To avoid having to move through the log page by page, choose *All* from the *Items/Page:* pop-up and use the scroll bar.
- The *Event* column expands as the browser window is widened. Widen the window to make long paths easier to read.
- In Player logs, the terms "upload" and "download" are used from the Player's perspective: content or other files coming to the Player are downloaded by the Player; files returned by the Player to Network Manager are uploaded.
- In IC log messages, "server" refers to Network Manager, "client" refers to the Player.

Problems and Errors

In an effort to help you evaluate the feedback in log files, Network Manager uses the terms "Problem" and "Error". Understanding the distinction is a helpful step in learning how to use Health Monitoring feedback to get your InfoChannel Network operating smoothly.

In Player log files, a Problem is a result; an Error is a cause.

An Error is the specific failure involved in the message, something like "File not Found", or "Connection Refused". A Problem is the effect of the failure, such as a script failing to play, or playing incorrectly.

A Problem, then, is an interpretation of an Error that tries to tell you what you need to know to evaluate how important the Error is, so that you can decide what to do about it.

There is not a one-to-one correspondence between Problems and Errors. For example, here are many different kinds of failure (Errors) that can result in the single Problem "Script did not play". Problem messages are more general than Error messages; in some cases, they cannot describe a specific effect.

Some Errors—failure to successfully send a heartbeat message, for example—do not have a specific Problem that they are sure to result in.

The "Problem" interpretation is available only for Errors within the InfoChannel logs; Errors in the Windows System or Application logs are presented without an attached Problem message.

Examining both the Problem and Error messages in a log event will often give you enough information to determine what happened, and decide what to do.

Clearing and resetting Conditions

The Health Monitoring system has the ability to "Clear" Conditions (Problems) as a way of letting you take Problems out of your way once they have been dealt with.

Clearing a Condition just changes the Health Monitoring system's interpretation of the Player's status. A Condition that has been Cleared no longer causes a Player to show up as Sick, or to email alerts for that Problem. Clearing does not delete anything from the log, or affect the Condition itself.

Resetting a Cleared Condition restores its normal alert-causing status.

The display uses red to indicate normal, uncleared Problems, and green for Cleared problems. The tooltip for an Error also indicates its state.

Using Clear Condition and Reset Condition

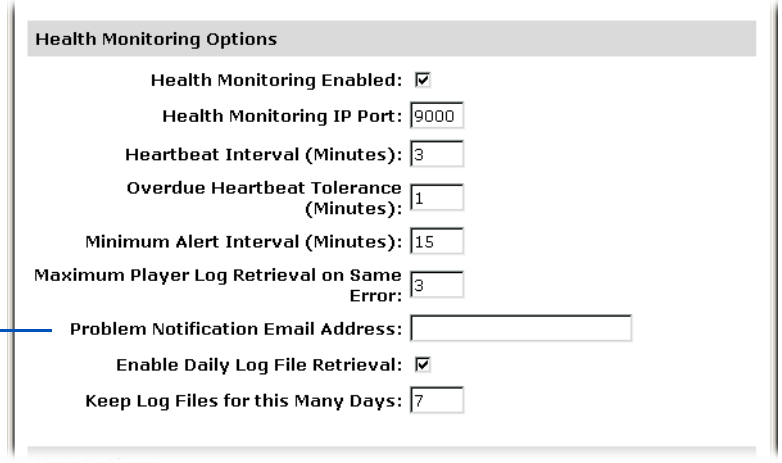
The **Overview** and **Log File Reader** pages provide a checkbox for all cleared and uncleared Problem events. When you select one or more Problems on these pages, the *Clear Condition* and *Reset Condition* buttons are enabled.

You should Clear an Error only when you know it to be harmless, or when you have taken action to fix it. If your fix did not work, the Error will recur. If the Error does recur, or if you otherwise realize that a fix did not or will not work as expected, you should Reset the Condition, so that it is not ignored.

> ***Important***
>
> Clearing is not the same as fixing! *Clear Condition* only stops the selected error from requiring your attention. Clearing without first fixing hides a Problem.

Health Monitoring configuration settings

The Health Monitoring system in Network Manager has several options on the **System Settings** page that allow you to tune its performance to suit your installation.



customer-specific option – default setting not possible

As described in chapter 4 (starting on page 76), you must set *Network Manager's Host Address:* to the Network Manager machine's IP address in order for Health Monitoring to function.

The other Health Monitoring settings do not need to be changed for Health Monitoring to work. However, you may find you want or need to make changes to some of these settings for your network.

Health Monitoring IP Port

Health Monitoring heartbeat messages must use a particular port to reach Network Manager. There is not a specific port number that must be used; the port specified in *Health Monitoring IP Port:* must simply be one that no other application or service on the system uses.

Heartbeat Interval

The *Heartbeat Interval (Minutes):* setting controls how often Players send their status messages back to Network Manager. Thus it specifies a maximum time that can elapse before a change in Player status can be communicated.

You might decrease the interval time if you need to monitor Player status especially closely, or increase it to reduce the network traffic of the heartbeat messages in a large network. A more likely reason to adjust the interval would be to increase it to reduce the number of connections made by dial-up FTP Players.

Overdue Heartbeat Tolerance

Network Manager considers a Player to be Dead when it does not receive a heartbeat from the Player after the expected interval. However, the Player is not declared Dead the moment that the Heartbeat Interval has passed without a status message being received. A certain "grace period" is allowed after the heartbeat interval has expired, to account for network latency and other unforeseeable timing variances. This grace period is specified by the *Overdue Heartbeat Tolerance (Minutes):* setting.

If you see Players being declared Dead when you know that they are working, the tolerance may be too low to cover the delays in your system. Try increasing the value of this setting.

Minimum Alert Interval

When a new, unique error occurs on a Player, the Player sends an alert email message (see "*Problem Notification Email Address*", below).

Since the same basic malfunction can in some cases cause a rapid series of identical errors, the *Minimum Alert Interval (Minutes):* setting provides a way to control the frequency that alerts can be sent. A given Player can send alert messages no closer together than the time set here. The default is 15 minutes. If you are receiving too many redundant alerts, increase this value.

Maximum Player Log Retrieval on Same Error

When Network Manager receives an error alert from a Player, it automatically retrieves the log file from the Player. Because some conditions cause the identical error to show up in many or all Players, this could result in excessive traffic in returned log files, when only a few are needed to ascertain the problem's cause.

Maximum Player Log Retrieval on Same Error: sets a limit on the number of different Players whose logs will be retrieved in response to the same error. If the default of 3 does not provide enough information to allow you to reliably diagnose errors, you can raise the number.

Problem Notification Email Address

As noted in chapter 4, the *Problem Notification Email Address:* box allows you to specify an email address to which automatic alert messages are sent. An alert email is sent to this address whenever a Problem appears on a Player in a previously all-healthy network.

Entering an address here is optional. If no address is given, notification emails are not sent.

Enable Daily Log File Retrieval

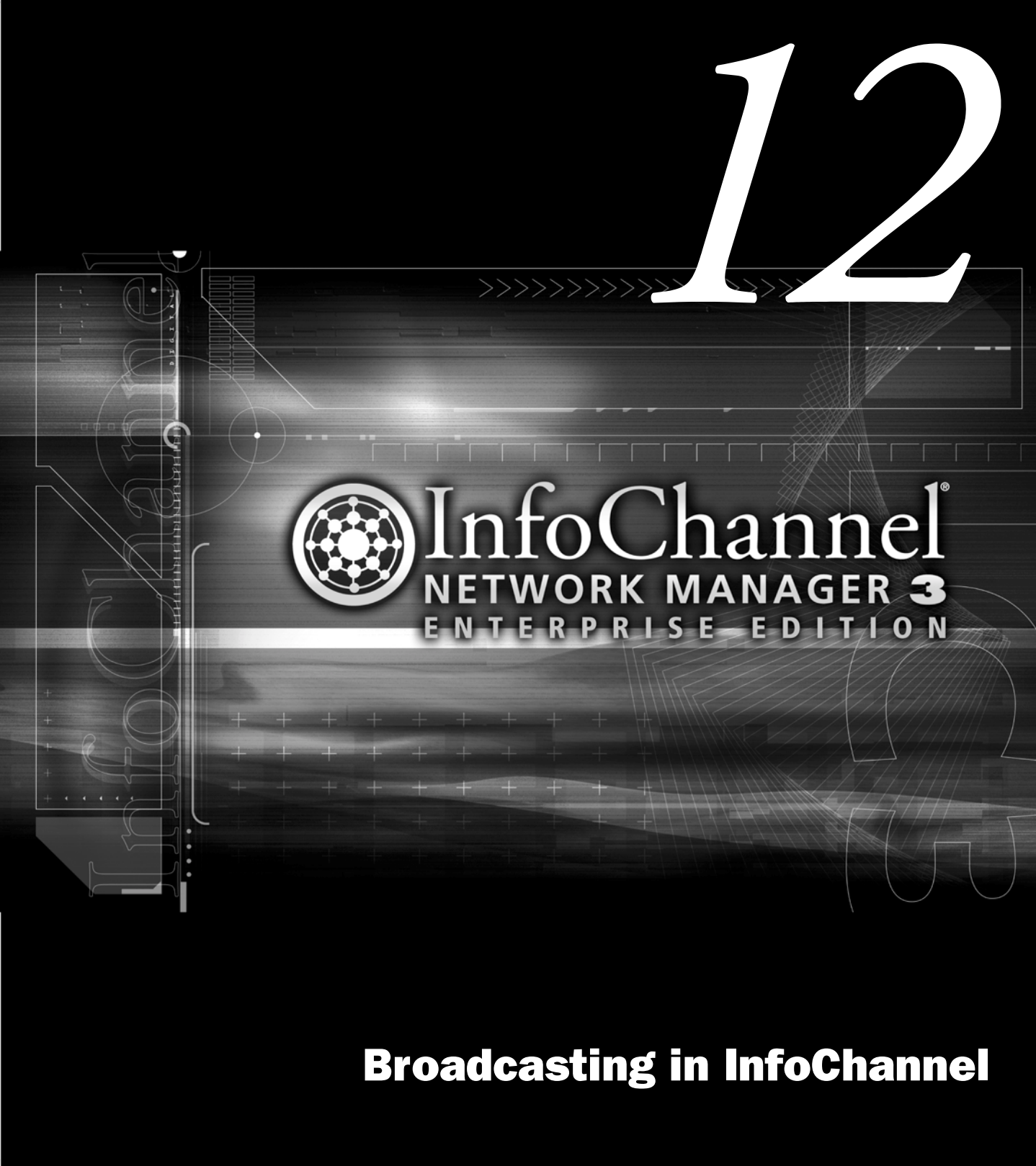
Standard practice is for every Player's log file to be retrieved and stored on Network Manager once a day, at approximately midnight. The content of the log file is cumulative, but separate files are maintained for each day.

It is recommended that you leave *Enable Daily Log File Retrieval* on (✓) so that you are assured a constant record of your Players' operation.

Keep Log Files for this Many Days

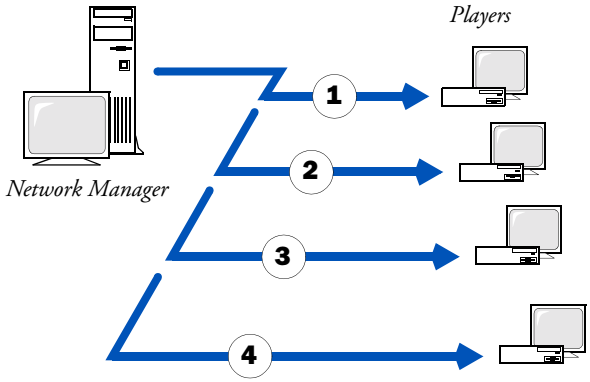
The separate log files retrieved each day are not kept indefinitely. After a set number of days, the oldest file is deleted. Set the number of days' worth of log files to keep on hand with *Keep Log Files for this Many Days:*.

If you have a large network, you might decrease the number of days to reduce disk space usage on Network Manager, provided you leave enough of a history to allow you to diagnose any problems that occur.


12
InfoChannel®
NETWORK MANAGER 3
ENTERPRISE EDITION
Broadcasting in InfoChannel

12: Broadcasting in InfoChannel

In small to medium sized InfoChannel Networks—those with up to a hundred or so Players—the standard point-to-point communication model works well. However, as installations grow larger, sending jobs to each Player individually becomes less and less practical. In a system with a thousand Players, for example, contacting each of them one after the other each time an update was required would obviously take far too much time.



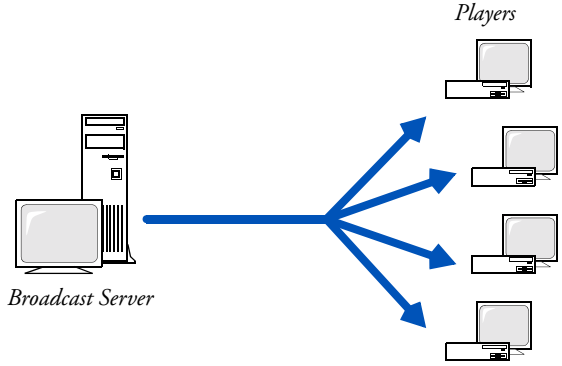
Point-to-point communication—Players are contacted sequentially

A broadcasting overview

To provide an efficient solution for larger InfoChannel Networks, Scala developed broadcast technology for Player communication. Using the broadcast approach, Network Manager can send out commands and update information to numerous Players at the same time. Players have unique identifying addresses such that, although information sent out reaches all Players physically accessible to the Network Manager machine that is transmitting, only those Players for which the information is intended actually accept it.

Thus it is still possible for Network Manager to target certain Players and Groups for updating, without needing to make an individual connection with each.

Sending a message once to many recipients such that they all receive it at essentially the same time is clearly far more expedient than sending the identical message multiple times to individual recipients. The time saved by the broadcast method increases with the total number of Players that must be reached.



Broadcast communication—Players are contacted simultaneously

The Broadcast Server

Using the InfoChannel broadcast approach requires an additional application developed specifically to manage the broadcast transmission process, the InfoChannel Broadcast Server 3.

The Broadcast Server software runs on a separate machine intermediate between Network Manager and broadcast Players. This machine is dedicated to broadcasting, and the term “Broadcast Server” may be used to refer either to the software or to the machine running it.

The Broadcast Server handles the processing overhead of converting the data stream normally produced by Network Manager into a format adapted for broadcast using a particular transmission technology (IP Multicast, for example.)

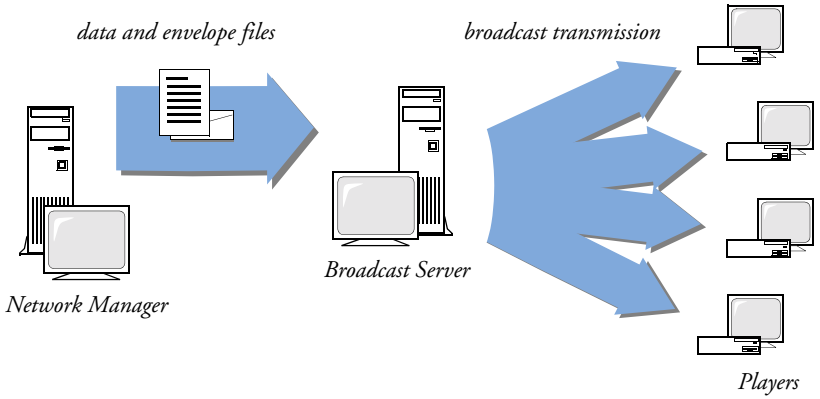
Data flow in broadcast connections

Broadcasting technology is quite different from point-to-point communication technology. The transmissions sent through a Broadcast connection go through processing steps that point-to-point transmissions do not, in order to safely negotiate the alternate technology of a broadcast transport layer.

However, the data flow in a broadcast connection is in fact more straightforward than the indirect approach Network Manager uses for point-to-point connections. In a broadcast transmission, Network Manager actually does send the data, not just a job file. The Players do not download their content from Network Manager; Network Manager delivers it directly to them.

The data, packaged as a single large data file and an accompanying "envelope" file, is sent from Network Manager to the Broadcast Server. The Broadcast Server processes the data into a format appropriate for the particular type of broadcast transport being used—a satellite system, for example—and then actually manages its transmission to the Players.

The following diagram illustrates the more direct data flow in broadcasting.

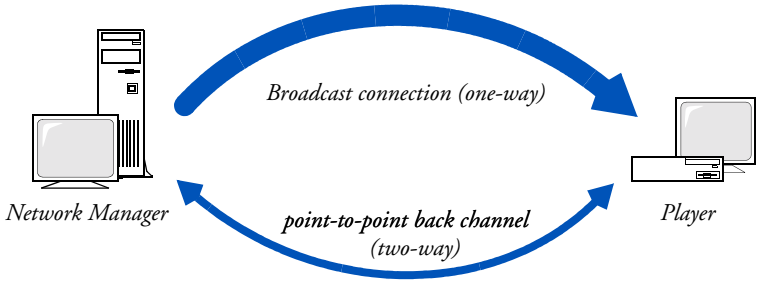


InfoChannel Network broadcast data flow

The fact that different approaches to actually transporting data to the Players are used in point-to-point and broadcast connections is entirely transparent from the point of view of a Network Manager operator. You can think about and work with broadcast Players in exactly the same way as other Players. How the data actually gets from point A to point B and back can be ignored.

One-way communication and back channels

The current state of generally-available broadcast communication is that connections are one-way. This means that in a pure broadcast environment there is no "back channel" by which a receiving Player can send data, Health Monitoring messages, etc. back to the Network Manager. With no back channel, there is no way of confirming transmissions, notifying Network Manager of errors in transmission, or of receiving files or collected data from Players.



Because such communication from Player back to Network Manager can be needed, many broadcast-based installations are not purely broadcast.

Network Manager allows you to define a Player with a point-to-point connection alone, a broadcast connection alone, or both a broadcast connection and a point-to-point connection.

For Players with both types of connection, the broadcast connection is primary for transmissions to the Player; the point-to-point connection is used as the back channel for Health Monitoring and other two-way communication with Players whenever it is necessary.

The point-to-point connection might be a modem or other lower-bandwidth channel than the broadcast connection, on the assumption that the back-channel communication will be of lower volume and less frequent than on the broadcast connection.

A broadcast Player that has no back-channel connection can still operate, however Health Monitoring, file retrieval, and other operations that require a back channel are not available. Such networks ultimately require some sort of direct human observation as a form of monitoring, to report Players that are not operating correctly.

Ensuring reliable broadcast communication

Data transmission errors are a fact of life. Network Manager's broadcast architecture has therefore been designed to be as robust as possible, in order to minimize the need for use of a back channel.

The simplest way to deal with transmission errors without constant use of a back channel is through redundancy: the data is broadcast multiple times. Doing so can fix random problems introduced by line noise and intermittent equipment failures without requiring Players to actually notify Network Manager of missed files. The Scala Broadcast Server software provides an option to choose how many times the broadcast information is automatically retransmitted.

Confirmed broadcasting

Confirmed broadcasting is a method of monitoring broadcast performance, available in InfoChannel Network broadcast installations that provide a back channel from the Players to the Broadcast Server. In confirmed broadcasting, individual Players report the success or failure of each transmission. If there is a failure, just the needed data can be re-sent to the appropriate destination, or technical personnel can be dispatched to the Player site if the problem is hardware-related.

Choosing confirmed broadcasting offers a way to increase reliability, while managing transmission bandwidth more efficiently than the non-confirmed approach. Without confirmation capability, redundant transmissions are made, to attempt to ensure that all Players have received all elements that were sent. Although this can be highly reliable, it still does not guarantee success, and failures may not be imme-

diately apparent. In addition, network bandwidth can be strained by the continual redundant transmission.

When confirmed broadcasting is enabled, data does not need to be resent unless there has been a failure, and failures are reported immediately. Because individual Players can communicate back to a central location, the nature and location of whatever problems do occur is known and can be dealt with quickly.

Confirmed broadcasting does not tie in to the Player Health Monitoring system at this time.

Pipe drivers

Scala's broadcast technology uses a "pipe" model for the actual transmission medium. The pipe can be any kind of hardware/software combination for which a pipe driver exists.

Scala supplies an IP multicast pipe and a satellite pipe, and can also supply custom pipe drivers for system-specific solutions.

Working with the Broadcast Server

The Scala Broadcast Server is a stand-alone application. It runs on a machine physically separate from the one used for Network Manager. The Broadcast Server runs at all times.

With a machine dedicated exclusively to transmitting broadcast data, the high processing and I/O load of broadcasting does not hinder your other applications. This machine is typically set up to run the Broadcast Server automatically when it boots.

The Broadcast Server works in concert with Network Manager. Once the broadcast installation has been fully configured and is working properly, there is little need to work directly with the Broadcast Server software. The only occasions would be if the network configuration changes significantly, or hardware troubleshooting must be done.

When the Broadcast Server is functioning normally, it is invisible to the Network Manager operator—working with broadcast Players appears to be no different from working with point-to-point Players.

The installation and operation of the Broadcast Server software is covered in the Scala *Broadcast Server User's Guide*.

Defining a Broadcast Player connection in Network Manager

Most of the configuration requirements of broadcasting are handled in the Scala Broadcast Server software. The process of setting up the Broadcast Server is covered in the User's Guide for that product.

The broadcast-related options within Network Manager are few. All you need to do in Network Manager to use broadcasting is:

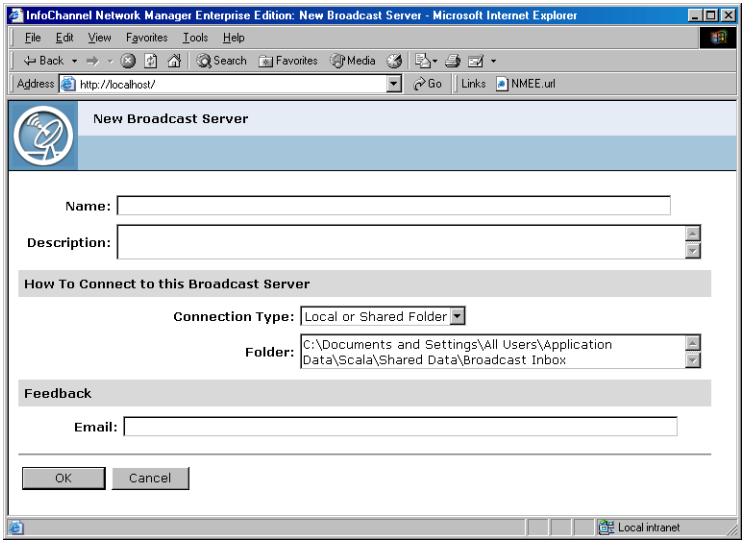
- Define a Broadcast Server connection
- In Player definitions, select a Broadcast Server connection, and enter an identification number for the Player

Defining a Broadcast Server

Defining a Broadcast Server is quite similar to defining a Player.

1. On the *Configure* control frame, click the *Broadcasting* icon. You see the **Broadcast Servers** page. Normally all Broadcast Servers that have been created for this system are listed here. Initially it is blank.

2. Click the *New Broadcast Server* button. You see the **New Broadcast Server** form:



3. Enter identifying information about the new Broadcast Server in the following fields:

   a. *Name:* – Enter a name for the Broadcast Server. It can be anything, as long as it is unique.

   b. *Description:* – Enter a brief description for the Broadcast Server (optional).

4. Using the *Connection Type:* pop-up, choose how Network Manager gets to the Broadcast Server's Broadcast Inbox folder, either *FTP* or *Local or Shared Folder*.

   Typically, you would choose FTP if the Broadcast Server is remotely located, or Local or Shared Folder if it is on the same LAN as the Network Manager machine.

5. Make settings specific to the connection type. Depending on which type you choose, a different set of options appears below in the form.

FTP connection

a. *URL:* – Enter the FTP location that Network Manager would use to access the Broadcast Server's Broadcast Inbox folder.

   For example:

   ```
   ftp://192.168.0.12/Broadcast Inbox
   ```

   or

   ```
   ftp://ICBserver.com/Broadcast Inbox
   ```

   This assumes that the Broadcast Server machine has been configured as an FTP server, with accounts, permissions, and the FTP root set to allow this connection.

b. *User Name:* – Enter the username to gain access to the FTP server.

c. *Password:* – Enter the password needed for the username. (Only asterisks appear.)

d. *Confirm Password:* – Enter the password again (to ensure you didn't type it wrong).

OR:

Local or Shared Folder connection

a. *Folder:* – Enter the drive letter or UNC path that Network Manager would use to access the Broadcast Server's Broadcast Inbox folder.

   For example:

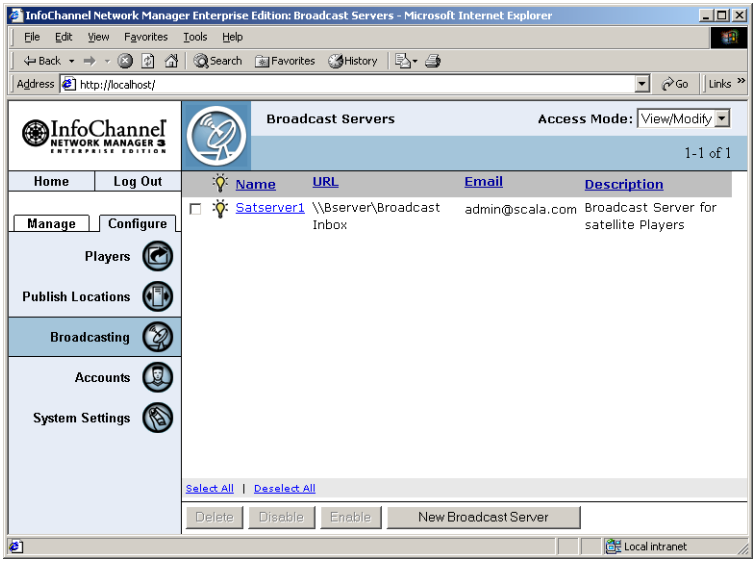
   ```
   \\ICBserver\Network\Broadcast Inbox
   ```

6. Optionally, enter a feedback email address.

   In the *Email:* text box, you can enter an email address to which status emails will be sent.

7. Click the *OK* button at the bottom of the form.
8. Choose *SUBMIT CHANGES* to store your changes in the database.

You see the Broadcast Server listed on the **Broadcast Servers** page.



Defining a broadcast Player

When a Broadcast Server connection has been defined, you can set up Players with broadcast connections.

Creating a broadcast Player is essentially the same as for creating a point-to-point Player, as described in chapter 7. Use the procedure starting on page 96, adding the broadcast-related settings described in here:

1. On the **New Player** or **Edit Player** form, choose a Broadcast Server from the *Use Broadcast Server:* pop-up.

2. Enter an identification number for the Player in the *Player ID:* box.

   This can be any number, as long as it is unique on your system. The Broadcast Server uses this number to find the Player. Note the number you use for this Player, because it will also need to be entered during configuration of the Player itself (page 122 in chapter 8).

3. Some broadcast systems also require the use of a secondary identification number. If your system requires it, enter the number in the *Custom ID:* box. Otherwise, leave the box empty.

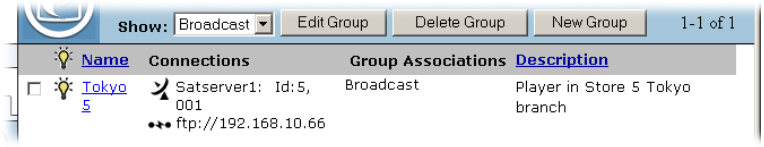
Grouping for broadcast Players

The preceding steps are the only additional tasks required within Network Manager related to defining a broadcast Player.

However, because broadcast Players are generally used in very large installations, it is very likely that you will also want to define broadcast-specific Groups, and associate your broadcast Players with these Groups. Grouping makes the management of large numbers of Players much simpler.

The procedures for creating and associating Groups is no different for broadcast Player than for point-to-point Players. See page 102 in chapter 7 for details on using Groups.

The illustration below shows how a broadcast Player listed on the **Players** page looks. This example Player has both a broadcast connection and a point-to-point (FTP) back channel, indicated by the icons in the *Connections* column. The Player has its Player ID of 5 and a Custom ID of 001 shown after the Broadcast Server name, and it is a member of a Group called “Broadcast”:



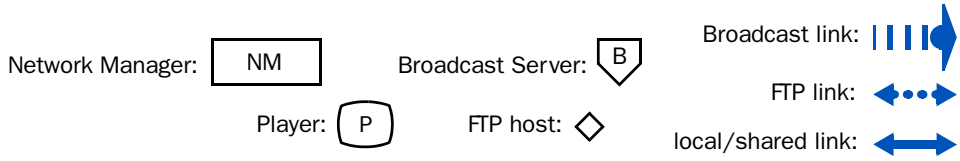
Broadcast topologies

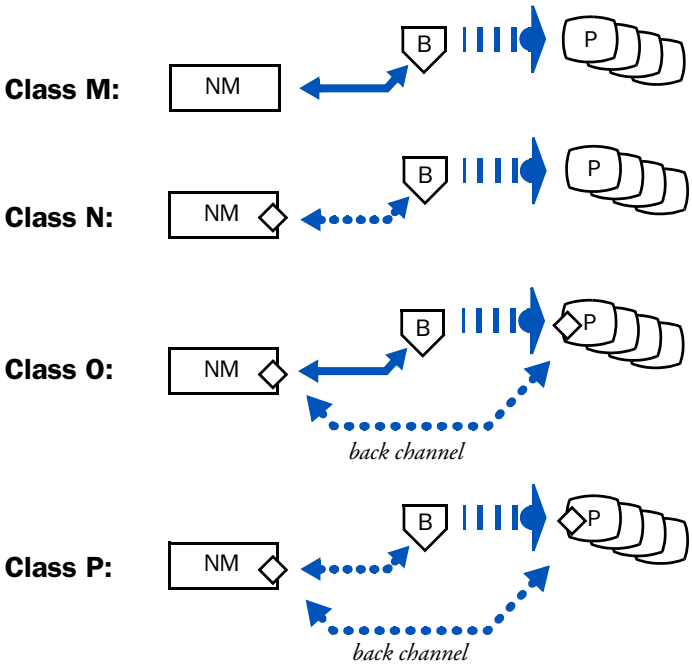
There are various possible broadcast topologies. The five topologies illustrated in the diagrams on the next page omit the ICDesigner and Publish Location components, for which the same possibilities exist as in point-to-point networks (see the diagrams on page 49 in chapter 3).

The topologies shown include both Shared Folder and FTP links to the Broadcast Server, and both broadcast-only Players and those with an FTP back channel. Finally, Class Q illustrates one way that the same network can use both broadcast and point-to-point Players.

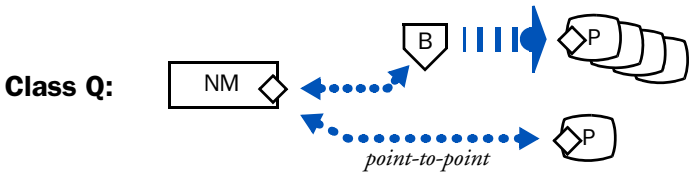
Still other variations using the same components and linking approaches are possible in this part of the connection chain. Any of these topologies can in turn be deployed with any of the four combi-

nations of ICDesigner/Publish Location connection in determining the final topology of the entire network.





InfoChannel Network basic broadcast topologies



InfoChannel Network mixed broadcast topology

Troubleshooting tips

13: Troubleshooting tips

General tips

If you are having trouble with Network Manager, the first thing to do is to double-check your installation of the software, starting with the Windows pieces.

- Did you deviate in some way from the instructions here?
- Or, if you followed the installation instructions faithfully, did you later modify the system in some way—install/reinstall a patch, driver, or update of some kind?
- Did you change your system configuration from what is specified here?

The surest way to begin with a working system is to follow the installation and configuration steps as closely as possible. If your particular system happened to require some special custom steps, chances are good that the problems are in some way related to them.

Assuming your software was installed and configured sufficiently correctly that you can run jobs, the next place to look is the **Job Activity** page in Network Manager. Running any job produces descriptive output on this page.

If you are having problems running jobs, make sure that the *Activity Logging Detail* option is set to *Diagnostic* on the **System Settings** page. Then run a problem job and look at the output on the **Job Activity** page. Every step of the job execution process is described. Errors are highlighted in red and describe the nature of the failure. The error messages should serve to point out the where the problem is occurring.

Also look at the Player log files in the **Player Health** pages. If the problem is on the Player end, it is likely that the messages there indicate the source of the difficulty.

Problem:	**Network Manager does not appear to function**
Reason and possible solutions:	Cgi-bin permissions may not be set correctly. 1. Right-click on the cgi-bin directory and choose *Properties*. 2. Choose the *Security* tab. 3. Make sure that for the listed users, that Read and Execute permissions are set. This is necessary for the Network Manager application. If this permission is not set, the application will not function. The installation process should set this property automatically.

Problem:	**Player is not responding**
Reasons and possible solutions:	There are many potential reasons that a Player might not be responding to jobs targeted at it. 1. The Player cannot reach its job folder. There are several possible causes: ❖ A job folder with the specified name does not exist in the FTP or shared location in the Player's definition. A folder of the correct name must be created in the correct location. ❖ The FTP or shared location for the job folder in the Player's definition in Network Manager does not match the location configured on the Player machine. The locations must be made to match by either using the Player Configuration utility on the Player or editing the Player definition on the Network Manager **Players** page. ❖ The Player cannot reach its shared job folder because the permissions set on the folder for the ICPlayer user are not sufficient. The ICPlayer user account on the Network Manager machine must have "Change" permission. ❖ The Player cannot reach its job folder via Shared because the folder is not a share. The folder must be made Shared.

Problem: (continued)	Player is not responding
Reasons and possible solutions: (continued)	❖ The Network Manager cannot reach the Player's job folder via FTP because the username and/or password configured on the job folder location do not match what the FTP account on the Network Manager machine specifies. The Computer Management tool must be run on the machine hosting the folder location and the FTP login information corrected. ❖ The Player can no longer reach a shared job folder (when previously it could) because an account password has expired. A new password must be entered for the account by which the Player accesses its job folder. (The *Password never expires* option should be turned on for the account at the same time to prevent this problem from happening again.) The new password must also be entered in the Player Configuration utility on each Player that uses that account. ❖ The Player cannot reach its job folder via FTP because the username and/or password configured on the Player do not match what the FTP account for Players on the Network Manager machine specifies. The Player Configuration utility must be run on the Player and the login information corrected. ❖ The Player cannot reach its job folder via FTP because the permissions set for the FTP account are not Read/Write/Modify. The Player FTP account permissions on the Network Manager machine must be made Read/Write/Modify. ❖ The Player cannot reach its job folder on Network Manager via Direct FTP because there is a conflict between the Direct FTP server's FTP port number and the IIS FTP port number. The IIS FTP server on Network Manager should be shut down if it is not needed, or the IIS *TCP Port* setting in its FTP Site Properties should be changed to something other than 21.

Problem: (continued)	Player is not responding
Reasons and possible solutions (continued):	2. The Network Manager cannot reach the Player's job folder ❖ The Network Manager cannot reach the Player's shared job folder because the permissions set on the folder for the Network Manager user are not sufficient. The NetManager user account on the machine hosting the folder location must have "Change" permission. ❖ The Network Manager cannot reach the Player's shared job folder because the folder is not a share. The folder must be made Shared. ❖ The Network Manager cannot reach the Player's shared job folder (when previously it could) because an account password has expired. A new password must be entered for the account by which Network Manager accesses the Player job folder. (The *Password never expires* option should be turned on for the account at the same time to prevent this problem from happening again.) ❖ The Network Manager cannot reach the Player's job folder via FTP because the permissions set for the FTP account are not Read/Write/Modify. The Network Manager's FTP account permissions on the machine hosting the folder location must be made Read/Write/Modify. ❖ The Network Manager cannot reach the Player's job folder via Direct FTP because there is a conflict between the Player-Direct FTP server's FTP port number and the IIS FTP port number. The IIS FTP server on the Player should be shut down if it is not needed, or the IIS *TCP Port* setting in its FTP Site Properties should be changed to something other than 21. 3. The Player is not actually targeted. Check the job definitions on the Network Manager **Jobs** page to make sure that all desired Players have been added to the *Players Targeted for this Job* list for each.

Problem: (continued)	Player is not responding
Reasons and possible solutions (continued):	4. Communications hardware failure. A network card, modem, cable, or other related hardware connecting the Player to the Network Manager machine is faulty. Hardware problems must be diagnosed and fixed. 5. The Player is disabled. Enable the Player on the Network Manager **Players** page. 6. Communications infrastructure failure. A phone company trunk line, Internet router, network server, ISP, or other intermediary device or service is down. Try to diagnose the location of the failure and determine whether the expected downtime warrants finding a workaround. 7. Player lockup from Windows Event Log overflow. It is possible for a PC to freeze if its Windows event logs fill up and no further events can be recorded. To prevent this from happening, the Windows System, Application, and Security logs on all Players should be set so that the oldest events are overwritten when the log becomes full. 8. Player software failure. If the Player has crashed, you may be able to revive it by sending a Reboot job. If the crash was so severe that the Player Engine is no longer functioning, rebooting the Player manually will be necessary. The cause of the crash (full hard disk, corrupted driver, virus infection, etc.) must be diagnosed and fixed. 9. Player hardware failure. The Player machine itself may have had a hardware failure, or had its power or communications inadvertently disconnected. A visit from a field technician will be necessary.

Problem:	Poor Player performance
Reasons and possible solutions:	1. The Player hard disk may be full. Run a *Delete Unused Content* job. 2. Shoddy device drivers or other third party software may be filling up free memory. Update the software with an *Install System File* job. If the problem software cannot be replaced, scheduling more frequent *Reboot* jobs may help. 3. The file system may be fragmented. Defragment the Player hard drive. Consider moving the FTP root location to a location other than the one on which Windows is installed to reduce the rate of fragmentation.

Problem:	Linked content not appearing as expected on Player
Reasons and possible solutions:	1. Linked content referenced by a script may not have been sent to the Player. Run a *Send Content* job to send the referenced content files, or execute some external process that accomplishes the same purpose (a batch file or custom program). 2. Linked content referenced by a script may be on the Player but not have the correct name. The base name of the linked content files on the Player must match the file names referenced in the script. 3. Linked content referenced by a script may not be on the Player in the correct location. All linked content files must be in either the Content or the InstalledContent folders, and must not be in subfolders of either of these folders. 4. Linked content files placed on a Player may not match, in appearance or duration, the placeholder files used to represent them during authoring. Care must be taken to ensure that updates of linked content are consistent with their placeholders, or that authoring techniques are adjusted to account for possible variations.

Problem:	**Tooltips flashing**
Reason and possible solution:	If you find that the tooltip help in Network Manager is difficult to read because the tooltip often flashes when the mouse pointer is over text, the problem may be the pointer scheme you are using. Some pointer schemes produce this effect. In the Windows Mouse Control Panel applet, try selecting a different pointer scheme.

Problem:	**Difficulty with the XML parser installation**
Reason and possible solution:	If you have trouble installing the XML parser, bear in mind that the XML parser installer requires permissions to the WINNT Installer folder.

Problem:	**Player Health monitoring heartbeats not being received**
Reasons and possible solutions:	1. System settings such as *Network Manager's Host Address*, *Health Monitoring IP Port*, or *Heartbeat Interval* have been changed in Network Manager, but one or more Players have not received a job to update them on these changes. Thus they are attempting to send back status messages but failing. If any changes have been made on the **System Settings** page, a job (any job) must be sent to all Players so that they are aware of the changes. 2. The *Network Manager's Host Address* or *Health Monitoring IP Port* settings are incorrect, preventing communication. *IP Address* must match the address of the Network Manager machine. The TCP/IP port number specified in *Server Port* must not be one used by any other network traffic, such as FTP or HTTP. 3. Communication is being blocked by a firewall. The firewall must be configured to allow access through the port number specified in *Health Monitoring IP Port*.

Problem:	Content is not being updated
Reasons and possible solutions:	1. The Publish Location specified in *Send Content* jobs is disabled. It must be re-enabled before content on it will be sent. 2. The Publish Location from which *Send Content* jobs are drawing is not the Publish Location to which updated scripts are being published. Either script authors must adjust the location to which they are publishing, or the defined path to the Publish Location in Network Manager must be changed to reflect the actual location where updated scripts are being published. 3. *Send Content* job is disabled. Re-enable the job on the **Jobs** page. 4. A time-based trigger for the *Send Content* job was not set up correctly. Review the scheduling on the **Jobs** page to be sure that it is triggering at the intended times. 5. The Player cannot retrieve content from Network Manager via Direct FTP because there is a conflict between the Direct FTP server's FTP port number and the IIS FTP port number. The IIS FTP server on Network Manager should be shut down if it is not needed, or the IIS *TCP Port* setting in its FTP Site Properties should be changed to something other than 21.

Problem:	Can't edit databases
Reason and possible solution:	If you do not see icons for certain Network Manager pages, or the controls that allow you to edit Network Manager items seem to be missing, the problem is that you do not currently have editing access. There are two possible reasons: 1. You are in *View Only* mode. With the *Access Mode:* pop-up, switch to *View/Modify* mode. 2. The Network Manager account you are logged in under does not have editing privileges. An Observer account has no editing privileges, and cannot be switched to *View/Modify* mode (the *Access Mode:* pop-up is not available). A Manager account cannot edit account or configuration settings, so the *Accounts* and *System Settings* icons are not in the control frame. Log in under an account with sufficient privileges if possible.

Appendix: Setup of Custom connections

Appendix: Setup of Custom connections

With Release 6 and beyond of the InfoChannel software, the preferred method of setting up an InfoChannel Network is to use “Direct FTP” for point-to-point connections. The Direct FTP scheme takes advantage of FTP servers that are now built into the Network Manager and ICPlayer software.

The use of Direct FTP has great advantages in ease of setup and maintenance of an InfoChannel Network. It is not necessarily suitable for every situation, however. You might need to use an alternative connection scheme if your installation has special requirements:

- It uses remote FTP hosting
- It is an existing InfoChannel Network, and you do not wish to reconfigure its current communication setup
- It must use particular FTP server software for administrative reasons
- It must use FTP, but the Players cannot be given static IP addresses
- It must use FTP, but the network administrator wants to keep Player job folders on the Network Manager machine
- FTP access is not possible

To accommodate such cases, InfoChannel lets you create “Custom” point-to-point connections. For those who need it, Custom connections allow all the flexibility that the InfoChannel software has always provided.

The capabilities and basic procedures associated with Custom connections match those of the FTP and UNC connections in earlier releases of Scala InfoChannel. InfoChannel Networks created under preceding InfoChannel releases are entirely compatible with the current release. Only some terminology has changed.

For certain installation types, it is even possible to mix the Custom and Direct FTP approaches to take advantage of the strengths of both. An example of a mixed approach can be found on page 244.

Using the information in this appendix

This appendix describes the basic requirements in setting up the various types of Custom connections that are available in an InfoChannel Network.

Using the information in this appendix presumes that you have read and understood the material in chapter 3 of this manual and performed the relevant configuration steps in chapter 4.

Expertise required

Network communication is a complex subject. The price of being able to make use of the complete flexibility offered by Custom connections is the need to understand the implications of the many possible network configuration choices.

This document cannot describe all of the innumerable potential system configurations and the steps to set them up. It can, however, tell you what you need to know to choose the optimum topology and to consider the relevant factors in setting up that type of InfoChannel Network.

It is assumed that anyone who opts to configure an InfoChannel Network with Custom connections has a reasonable level of competence in the basic networking concepts involved, and in working with the security issues in a modern Microsoft Windows-based environment.

Getting detailed information

Fortunately, all connections in InfoChannel use standard networking protocols and Windows practices. Any of the many standard sources of reference information on networking and using Windows can be consulted for step-by-step details on procedures such as creating user accounts, setting permissions, and sharing folders.

Using third-party software

Among the options afforded by Custom connections is the use of third-party FTP server software. If you will be using a third-party FTP server, you or an administrator in your organization must be familiar with that server's operation: installing it, enabling it, and setting up the usernames and passwords that it requires.

For customers who do not have the expertise in Windows and networking necessary to navigate the various choices, Scala recommends finding a way to use Direct FTP rather than Custom connections.

Training available from Scala

On the aspects of InfoChannel Network configuration that are specific to its software, Scala offers regular training classes. Anyone responsible for planning and setting up an InfoChannel solution—especially one using Custom connections—is strongly advised to take the relevant Scala training courses. They provide invaluable help in negotiating the many possible approaches to installation setup that are possible with InfoChannel.

You can request information on attending Scala's InfoChannel training courses by visiting our web site at http://www.scala.com.

Information included here

This appendix gives step-by-step instructions on the settings you need to make within Network Manager and the Player Configuration utility that are related to configuring Custom connections.

The setup of dial-up FTP connections in Windows, which requires some InfoChannel-specific knowledge to complete, is also covered in detail in this appendix.

Making settings and related procedures for enabling and configuring FTP server software is covered only in terms of general requirements; the server manufacturer's documentation must be consulted for server-specific details. Similarly, setting up Windows user accounts and their permissions is part of basic Windows operating procedures and only the basic requirements are specified here.

Deciding on FTP vs. Shared Folder

InfoChannel offers two basic types of Custom connection: *FTP* and *Shared Folder*. These are equivalent to earlier releases' "FTP" and "UNC" connections.

InfoChannel Networks most commonly use FTP for communication with Players, because Players are typically far enough from Network Manager that connecting them all by the local/LAN links that the Shared Folder approach requires would be impractical.

However, with the current InfoChannel release, using the Shared Folder approach is not necessarily preferable even on entirely LAN-based InfoChannel Networks. FTP can run over most LANs, so an InfoChannel Network based on Direct FTP is simpler to set up even on a LAN than one based on shared folders.

Thus with current InfoChannel software, using the Shared Folder approach is worthwhile only in certain situations:

- the InfoChannel Network is entirely LAN-based, but the LAN uses NetBEUI or some other non-TCP/IP networking protocol that does not support FTP

  Note that on a non-TCP/IP network the Health Monitoring feature is not available.

- the InfoChannel Network was set up using "UNC" connections (shared folders) under an earlier InfoChannel release, and reconfiguring to use Direct FTP is deemed not worthwhile

If your installation does not fit either of these scenarios, Scala recommends using Direct FTP if possible.

Basic considerations for using FTP connections

If you need to use FTP connections in your InfoChannel Network but choose not to use Scala's Direct FTP, any third-party FTP server software can be used for a Custom FTP connection.

InfoChannel software has been tested extensively with Microsoft's IIS FTP service. Other vendors' FTP servers, configured appropriately, can be expected to work correctly and may offer certain advantages. However, they have not been tested by Scala.

The most critical tasks you must attend to regardless of FTP server manufacturer are:

- Disabling Anonymous access to all FTP servers
- Creating password-protected accounts for access on the FTP server machines
- Making sure that accounts and folders have the necessary permissions—the folders used for FTP must be read/write/modify for the appropriate users

Setup common to all Custom connections

Certain tasks must be performed regardless of whether the Custom connections you use are of the FTP or Shared Folder type.

Chief among these tasks are:

- Creating job folders
- Assigning Network Manager's workspace locations
- Creating accounts and assigning account privileges

Creating Player job folders

Every Player needs its own unique job folder.

In InfoChannel Networks that use Direct FTP connections, job folders are created automatically. When you are using Custom connections, you need to create job folders for Players manually. (For Release 4 and beyond of InfoChannel Network Manager 3, one default Player folder is created for you on the Network Manager system during installation.)

To add any additional Players to a system that uses Custom connections, you must create their job folders yourself in Windows.

Job folder location

The job folders can be located anywhere that is accessible both to Network Manager and to the Players—on the Network Manager machine, on a separate file server, or on the Players themselves.

For simplicity and ease of administration, it is best to stay consistent in locating the job folders. Create all your Player job folders in the same location on the Network Manager side, or create each individual job folder in the same location on all Players.

It is recommended that for job folders on Network Manager, you create additional job folders in the same location in which the default Player job folder is placed during installation, namely:

```
<systemroot>:\Documents and Settings\All Users\Documents\Scala\Network Transmission\Outbox
```

For a job folder accessed by FTP, it is recommended that you put the job folder within the folder that is the FTP root for the Player machine. This location will vary depending on the FTP server you are using. For an IIS FTP system configured according to the default installation recommendations, that location is

```
<systemroot>:\Inetpub\Ftproot
```

A Player that will not use FTP does not need to have its job folder within the FTP root. The location of the job folder in this case is not as critical, but a good place is the Player's equivalent of the Network Manager default location shown above:

```
<systemroot>:\Documents and Settings\All Users\Documents\Scala\Network Transmission\Outbox
```

In either case, follow these steps:

1. In Windows Explorer, select the folder within which you wish to create the new job folder(s) (Outbox or Ftproot, if you are using the above examples).
2. From the Explorer **File** menu, choose *New* > *Folder*.
3. Give the new folder a meaningful name.

   For a job folder on Network Manager, use a name that clearly and uniquely identifies the particular Player, such as "Player1".

   If you are creating the job folder on the Player machine itself, a name like "Inbox" is sufficient because there is only one job folder in that location. (A Player job folder created like this can be seen in the folder structure illustration on page 107.)
4. Repeat steps 1–3 for each Player machine in your InfoChannel Network, giving each a name.

Assigning workspace locations

You need to make sure that Network Manager Workspace and Transmission Workspace folders are defined to point to the right places.

> ***InfoChannel Network Manager Note***
>
> The Network Manager Workspace folder is where all content and other data related to all connected Players will reside. For this reason, you must be sure that the folder is located on a large-capacity drive with plenty of empty space.

You may need to change one or both locations if you are using FTP. The Transmission Workspace location in most cases should be the same folder as the Network Manager Workspace folder AND should coincide with its machine's FTP root. Achieving this if you are using a third-party FTP server and must use its already-established FTP root folder requires adjusting the default folder locations. Using remote FTP hosting requires that you alter the Transmission Workspace loca-

tion to coincide with the remote FTP host's root folder. Additional detail is available in chapter 3 starting on page 59.

For Shared Folder use, the default locations are generally acceptable.

Detailed instructions for setting the Workspace folder locations are found in the setup procedures for FTP and Shared Folder that follow.

Creating accounts

In order for communication through the InfoChannel Network to be secure, the participants at either end must have their identities authenticated before a connection is established. FTP authentication is handled through username/password identities; for Shared Folder authentication by the creation of Windows user accounts with appropriate privileges. (In IIS, FTP usernames are also linked to Windows user accounts.)

Network Manager Note

The accounts discussed here are not related to the access-level accounts defined on Network Manager's **User Accounts** page.

The descriptions given here use "NetManager" as the username or account name to identify Network Manager, and "ICPlayer" as the username or account name to identify any Player. You do not need to use these particular names. The important thing is that they be descriptive, and that they match on both ends of the connection.

Network Manager should be running under its "NetManager" user account at all times. Players should be running under their "ICPlayer" user account at all times. These should be Administrator-level accounts for full InfoChannel functionality to be available.

Authentication needed using Custom FTP

The following table shows what needs to be set up for authentication on the Network Manager and Player ends of given types of Custom FTP accesses:

FTP Access	Needed on NM	Needed on Players
NM deposits jobs in job folders on Player	a "NetManager" username in Network Manager's Player definition	FTP server must allow user "NetManager" to log in and access the job folder
Players poll job folders on Network Manager	FTP server must allow user "ICPlayer" to log in and access the job folder	an "ICPlayer" username set up in Player Config utility FTP login dialog
Players retrieve or deposit files from NM	an "ICPlayer" username in Network Manager's **Edit System Settings** Custom FTP page	*no setup on Players required* (the username/password for Players to use is sent to them encrypted within job files)
Players retrieve or deposit files from remote FTP server	a username specified by remote FTP service provider entered in Network Manager's **Edit System Settings** Custom FTP page — also used by NM to log in to an offsite FTP server to transfer files to/from Transmission Workspace	*no setup on Players required* (the username/password for Players to use is sent to them encrypted within job files)
	(passwords that accompany matching usernames must match at both ends)	

Authentication needed using Custom Shared Folder

The following table shows what needs to be set up for authentication on the Network Manager and Player ends of given types of Custom Shared Folder accesses:

Share Access	Needed on NM	Needed on Players
NM deposits jobs in job folders on Player	a "NetManager" Windows user account	Job folder must be a share Windows must allow user "NetManager" read/write/modify access to the job folder
Players poll job folders on Network Manager	Job folder must be a share Windows must allow user "ICPlayer" read/write/modify access to the job folder	an "ICPlayer" Windows user account
Players retrieve or deposit files from NM	Network Transmission folder must be a share Windows must allow user "ICPlayer" read/write/modify access to the Network Transmission folder	an "ICPlayer" Windows user account
	(matching user accounts must exist at both ends)	

Choosing single or multiple Player accounts

Both FTP and Shared or Local Folder installations can use a single generic "ICPlayer" account. The above tables indicate the use of a generic ICPlayer account.

However, with a Shared or Local Folder installation, the per-folder permission capability of Windows' NTFS 5 lets you set up unique

accounts for each Player. This allows individualized access rules for each Player job folder for greater security and flexibility. To do this, you need to create multiple Windows user accounts on Network Manager, one for each Player, each with its own username and password. You would need to know the usernames and passwords to be used for each Player in order to create the accounts on Network Manager. Then you would configure each Player's job folder with the desired permissions.

If using multiple Player accounts, you may wish to wait to perform that process until after you have completed the setup on the Player machines, where you will also be creating the account for each.

Setting folder privileges

Setting the appropriate account privileges on the folders that InfoChannel uses for communication is a crucial step in allowing the InfoChannel Network to function. Running with incorrectly set privileges is a common source of operational problems and security risks.

Regardless of the type of connection you use, make sure of the following:

- the Network Manager Workspace folder grants read/write/modify access to the NetManager user and—assuming no remote FTP hosting—to the ICPlayer user
- (if remote FTP hosting is being used) the Transmission Workspace folder grants read/write/modify access to the NetManager and ICPlayer users
- the Players' job folders grant read/write/modify access to the NetManager user and the ICPlayer user

You typically set folder privileges for FTP connections by using the FTP server configuration software. (Under IIS, user-specific privileges are defined using Windows Explorer, in the *Security* panel of the Properties sheet for a given folder.)

Account privileges for Shared Folder connections are all defined using Windows Explorer, in the *Security* panel of the Properties sheet for a given folder.

Custom connection setup: FTP access

Important data you need to know before you start is the FTP login information: the root or home directory address of the FTP server you will be using, with its username and password.

The address is likely to be the FTP root address of the Network Manager machine. When you are using remote FTP hosting, it is the address of the remote host. Note that if you are using an offsite FTP hosting service, you will need to get this login information from them, and they may not allow you to choose custom usernames such as "NetManager" and "ICPlayer".

> ***InfoChannel Configuration Note***
>
> If you are planning to have the Player use FTP dial-up in either direction (from Network Manager to Player or from Player to Network Manager), you also need to consult the section "*Dial-up FTP access configuration*" on page 235.

FTP setup on Network Manager machine

The following steps outline the basic process needed to set up the Network Manager machine to be able to use Custom FTP connections.

Step 1: Enable FTP

Follow your FTP server software manufacturer's instructions to enable the server. Preferably, the FTP server should be enabled automatically when the Network Manager machine boots, so that it is guaranteed to be running.

Step 2: Disable Anonymous access

For the security of your network, it is crucial that you disable anonymous FTP access. If this step is omitted, an error message noting the fact is logged for the system at a regular interval until this vulnerability is corrected.

Step 3: Establish the FTP root

For FTP communication with Players (or Publish Locations), the Network Manager machine's FTP root ("FTP Home Directory" under IIS) needs to coincide with the Network Manager Workspace location.

The recommended procedure to do this is to change the default Workspace location within Network Manager to match the existing FTP root. If you will do so, there is no need to change the FTP root, and in this Step you only need to take note of what the FTP root location is, and to make sure that it can be written to.

Network Manager Note

If your InfoChannel Network will not be using the default Network Manager Workspace Location, changing the root location will need to be done after the final Workspace location has been established (Step 4), so that you can enter it.

Alternatively, you can choose to make the two locations coincide by changing the FTP root location to match the Network Manager Workspace location. This approach can work just as well as the reverse. The specifics of your InfoChannel Network layout and/or administrative concerns might make this approach preferable. If so, in this Step you actually change the FTP root location.

The default home directory for FTP under Windows 2000 is established by IIS at <*systemroot*>*Inetpub**Ftproot*, where <*systemroot*> is the letter of the drive in which Windows is installed. If you are using a different FTP server, its root location would be different. Follow the procedures laid out in its documentation for viewing/changing its FTP root or home directory.

Step 4: Set the Network Manager Workspace folder

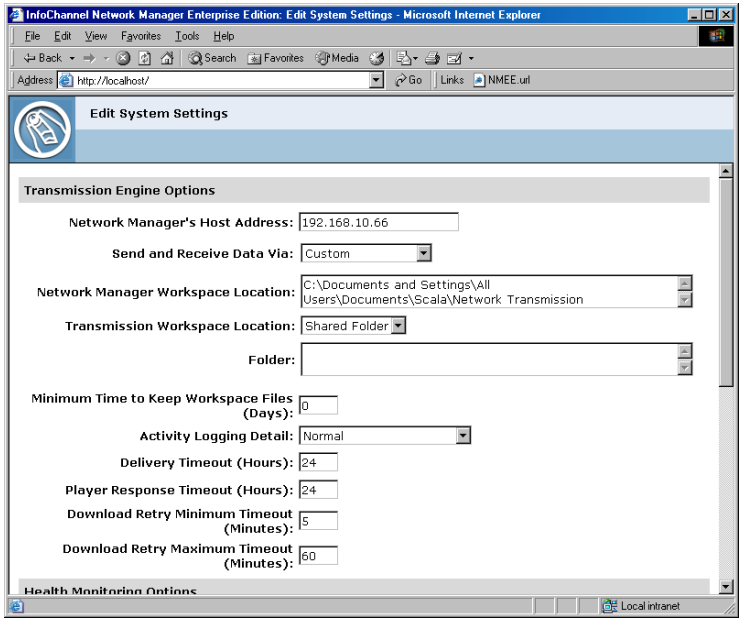
1. In Network Manager, click the *Configure* tab to display the icons in that panel of the control frame.
2. Click the *System Settings* icon.

You see the **System Settings** page, which displays the current settings of its options.

3. Click the *Edit Settings* button at the bottom of the page to open the **Edit System Settings** form.

4. Verify that the Network Manager's host address is correct. (See "*Step 4: Configure transmission options*" on page 73 of chapter 4 for instructions on checking and setting the address.)

5. Set the *Send and Receive Data Via:* pop-up to *Custom*.



6. In *Network Manager Workspace Location:*, you should see the path that was set up during installation. This defaults to

   `<systemroot>:\Documents and Settings\All Users\Documents\Scala\Network Transmission`

   where *<systemroot>* is the letter of the drive on which Windows is installed.

The preferred approach is to change this location to match the FTP root directory of your FTP server. You also might wish to change this location if you have special considerations:

- Your network uses a separate file server machine, external to the Network Manager machine
- You must use a machine that is running 24 hours a day every day, and the Network Manager machine is not always running
- You need to use a machine that has a different version of Windows—one with a higher number of licensed connections, for example

If you need to change the *Network Manager Workspace Location:* setting, use these steps:

a. Make sure that the location you choose allows read/write/modify access to any user account.

b. It is recommended, but not required, that you create a folder named "Network Transmission" in the desired location.

c. Then enter the full path to the location here in Network Manager.

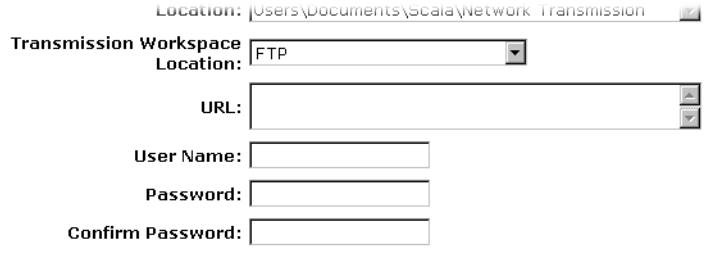
Step 5: Set access to the Transmission Workspace

1. Choose the *Transmission Workspace Location:* setting.

   This setting is what determines whether the Players communicate with Network Manager via the FTP or the Shared Folder approach. Depending on which access method you choose, a different set of options appears below on the page.

> ***InfoChannel Network Manager Note***
>
> All Players will use the Custom FTP point-to-point connection set here for sending and receiving data between themselves and Network Manager. (A Player can have a broadcast connection as well as, or instead of, this point-to-point connection.)

Choose *FTP* from the *Transmission Workspace Location:* pop-up list to display the FTP login options.



Note that if the associated *URL:* location that you give (see next step) is different from the *Network Manager Workspace Location:* setting, choosing *FTP* also specifies that Network Manager communicates between its Workspace and the Transmission Workspace via FTP. The diagram on page 59 in chapter 3 shows this graphically.

2. Enter the FTP login information for access to the Transmission Workspace. Network Manager includes the FTP login information encrypted in its job files to tell the Players where to retrieve content, send log files, etc. via FTP.

    a. *URL:* – Enter the FTP URL of the Transmission Workspace folder.

    Normally, the Transmission Workspace location is the same as the Network Manager Workspace location. The only reason it would need to be different is if you plan to use remote FTP hosting to communicate with your Players.

    If you are not using remote FTP hosting, enter the FTP address of the Network Manager machine. Assuming you plan to follow the instructions in "*Step 3: Establish the FTP root*" on page 224, the FTP root of this machine is identical

with the Network Manager location, and entering the FTP site address alone is sufficient:

`ftp://192.168.0.10`

OR

`ftp://ICNMserver.com`

If remote FTP hosting is being used, enter the site address and any further path needed to reach the folder.

For example:

`ftp://OffsiteServerCo.com/Customerftp/YourCo/Network Transmission`

b. *User Name:* – Enter the username to gain access to the FTP server. If you have set up the workspace on the Network Manager server and followed the account setup suggestions given previously (see page 220), this would be "ICPlayer".

c. *Password:* – Enter the password needed for the username. (Only asterisks appear.) Passwords are case-sensitive.

This is the password for the ICPlayer FTP account.

d. *Confirm Password:* – Enter the password again (to ensure you didn't type it wrong).

3. Click *OK* to accept your changes on the **Edit System Settings** form.

4. Finally, click *SUBMIT CHANGES* to store your changes in the database.

Step 6: Define the Player

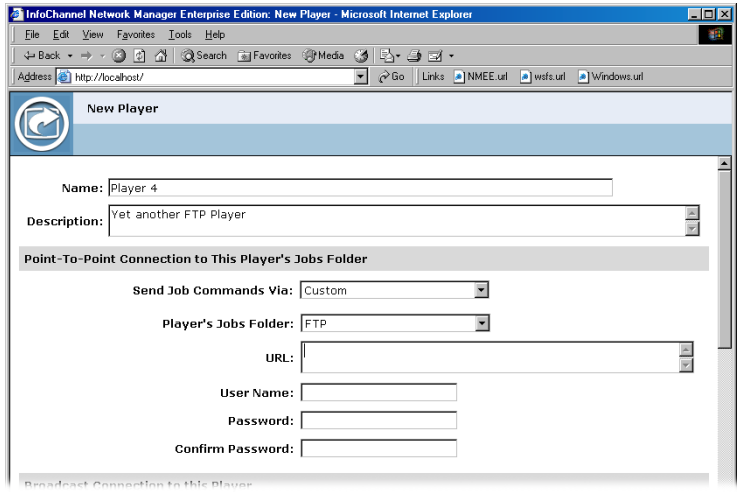
1. Click the *Players* icon in the Network Manager control frame to open the **Players** page.

2. Click the *New Player* button to open the **New Player** form.

3. Enter a Name and Description for the Player.

4. Choose *Custom* from the *Send Job Commands Via:* pop-up.
5. Specify how Network Manager delivers its job files. In most Custom FTP based installations, this is via FTP:

   Choose *FTP* from the *Player's Job Folder:* pop-up.



> There is a situation in which it is possible and in fact preferable **not** to choose FTP here when Players are connecting through Custom FTP: when the FTP host being used is onsite, accessible via LAN to Network Manager; AND the Player job folders are located on that host, rather than on the Players.
>
> In this case it is more efficient—especially with large numbers of Players—to deliver job files via Local or Shared Folder access directly to the job folders in the FTP server's root folder. Delivering to local job folders by FTP also works, but is much slower.

6. Make settings for the FTP connection to the Player's job folder. The following options appear below in the form:

   a. *URL:* – Enter the FTP location that the Network Manager machine would use to access the Player's job folder.

      Examples:

      `ftp://192.168.0.10/Outbox/LobbyPlayer`

      OR

      `ftp://ICNMserver.com/Outbox/LobbyPlayer`

      OR, if using offsite FTP hosting

      `ftp://OffsiteServerCo.com/Customerftp/YourCo/Network Transmission/Outbox/LobbyPlayer`

      > There are special ways to enter the URL if you need to use dial-up FTP to send jobs to job folders located on the Players themselves. See "*Special URL format*" on page 235.

   b. *User Name:* – Enter the username to gain access to the FTP server. Assuming you follow the account setup instructions given previously (see page 220), this would be "NetManager".

   c. *Password:* – Enter the password needed for the NetManager username. (Only asterisks appear.) Passwords are case-sensitive.

   d. *Confirm Password:* – Enter the password again (to ensure you didn't type it wrong).

7. If the Player will be a member of a Group, make the appropriate settings in the *Group Associations* section (see page 99 for details).

8. Click the *OK* button to close the **New Player** form.

9. If necessary, repeat the process to create additional Players.

When you have finished, click *SUBMIT CHANGES* to store the new Player(s) in the database.

FTP setup on each Player

The steps in this section must be done on each Player machine you intend to use with a Custom FTP connection.

Step 1: Enable FTP

Players that will poll remotely-located job folders by FTP need not function as FTP servers.

If your installation is configured with the Player's job folder on the Player machine itself, rather than located remotely, and the Network Manager will access the folder by FTP, then you do need to enable FTP on the Player and configure the machine as an FTP server.

Step 2: Disable Anonymous access

For the security of your network, it is crucial that you disable anonymous FTP access to the Player. If this step is omitted, an error message noting the fact is logged for the system at a regular interval until this vulnerability is corrected.

Step 3: Establish the FTP root

Setup tasks and general administration are simpler if you leave the FTP root at its default, and Scala recommends that you do so if you have no compelling reason to change it. If you will retain the default, just verify that the root folder can be written to.

However, if for example you want to have the FTP root on a drive different from the Windows drive, you need to change the root location.

Step 4: Edit accounts and permissions

1. Disable the Guest user account in Windows. This is necessary to prevent ignorant or malicious users from gaining access to the Player FTP server.

2. Create and configure the Player's user account on the Player. If you have followed the account setup suggestions given previously (see page 220), this would be "ICPlayer". For all job functions to be available, this should be an Administrator-level account. The

ICPlayer account is what the Player uses when it contacts Network Manager.

3. If the Player job folder is located on the Player, you must also create an account to allow Network Manager to log in to the Player. If you have followed the account setup suggestions given previously (see page 220), this would be "NetManager".
4. Add the ICPlayer user to the FTP root on this machine so that it has Read/Write and Modify access.
5. If the Player job folder is located on the Player, add the NetManager user to the FTP root on this machine so that it has Read/Write and Modify access.

Step 5: Point the Player to an FTP job folder

You need to use the InfoChannel Player Configuration utility to tell the Player how to reach its job folder.

(There is no need to explicitly tell the Player how to reach the Transmission Workspace—Network Manager includes that information within the job files as mentioned on page 227.)

1. Run the InfoChannel Player Configuration utility on the Player machine you are setting up.
2. In the *Network* panel of the utility, choose *Custom* from the *Receive Job Commands Via:* popup.
3. Choose how the Player gets to its job folder. The choice you make depends on whether the job folder is local or remote.
   - ❖ If the Player's job folder is remote—located on Network Manager or on a remote FTP host—choose *FTP* from the *Player's Job Folder:* pop-up list.

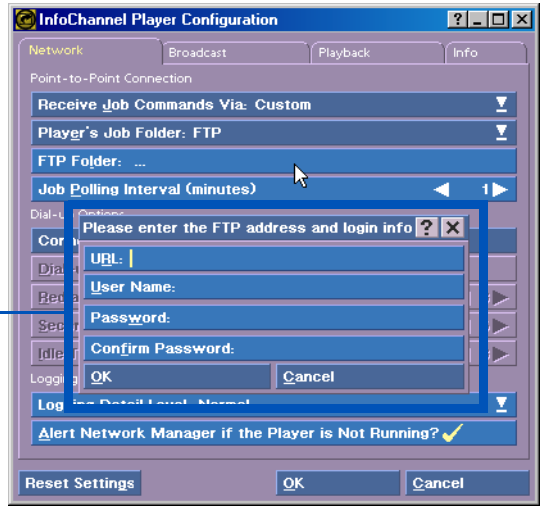
     You see the *FTP Folder:* button and the *Job Polling Interval* control below the pop-up.
   - ❖ If the Player's job folder is local—located on the Player or on another machine local to the Player—choose *Local or Shared Folder* from the *Player's Job Folder:* pop-up list.

You see the *Folder:* button below the pop-up.

> ***Important***
>
> Don't confuse this connection with other connections in the Custom FTP scheme.
>
> Choosing *Local or Shared Folder* here does not affect, or need to match, how the Player contacts the Transmission Workspace. That is set to be FTP on Network Manager's **System Settings** page.
>
> Nor does it need to match how Network Manager reaches the job folder—that is specified in Network Manager's Player definition.

In this Step, only FTP job folder access is covered. See the description for Shared Folder access starting on page 252 if the job folder is local.

4. Click the *FTP Folder:* button to open a dialog that lets you enter the FTP login information that this machine would use to access its job folder.



FTP login dialog

URL: – Enter the FTP address where the job folder is located. The address should include the FTP server address and the path to the job folder from the FTP root. (You need to have set the FTP root appropriately, as described in Step 2 on page 224.)

For example:

`ftp://192.168.0.10/Outbox/LobbyPlayer`

OR

`ftp://ICNMserver.com/Outbox/LobbyPlayer`

OR, if using offsite FTP hosting

`ftp://OffsiteServerCo.com/Customerftp/YourCo/Network Transmission/Outbox/LobbyPlayer`

User Name: – Enter the username needed to gain access to the FTP server. If you have followed the setup recommendations (see page 220), this would be "ICPlayer".

Password: – Enter the password needed for the username. (Only asterisks appear.) Passwords are case-sensitive.

This must match the password entered for the ICPlayer account that was created on the FTP server.

Confirm Password: – Enter the password again for confirmation.

5. Click *OK* to exit the FTP login dialog. The FTP address entered appears in the *FTP Folder:* button with the user name embedded in it like this:

   `ftp://ICPlayer@ICNMserver.com/Outbox/LobbyPlayer`

6. Set the polling interval using the *Job Polling Interval* control.

   The Player regularly polls (checks its job folder) for pending jobs. The *Job Polling Interval* control lets you specify how many minutes the Player waits between each check.

   You can adjust the interval value from the default if necessary to balance the timeliness of Players receiving their jobs against the

bandwidth/cost constraints of the network's FTP connection. An interval of 1-5 minutes is appropriate when the FTP connection is made via a direct connection to the Internet. For a dial-up connection, an interval of 30 minutes or more is recommended.

Note that using FTP dial-up requires important additional configuration tasks in Windows. See the following section for details.

Dial-up FTP access configuration

FTP communications in an InfoChannel Network can use modems rather than Ethernet cards, by taking advantage of the dial-up networking (RASdial) capabilities in the Windows operating system.

Using dial-up FTP requires the same basic setup steps as FTP via LAN/Internet—enabling the FTP server on the receiving end, creating user accounts and setting appropriate permissions—plus some additional steps.

The additional steps required to configure FTP dial-up are mainly a matter of creating connections in Windows Dial-up Networking. The steps you need to follow are different depending on whether the InfoChannel Network is configured with job folders on the Players themselves, or on the Network Manager machine.

Special URL format

If the Player's job folder is located on the Player itself and Network Manager will use FTP dial-up to access it, there is a special format to use for the FTP URL when defining the Player in the Network Manager **New Player** form. Network Manager uses variations in this format to allow for alternative approaches to FTP dial-up. (See below for details.)

The simplest approach uses the following format:

```
ftp://(phonenumber)/<path>
```

In the place of the IP address or server name in a normal URL, you substitute the Player's dial-up phone number **in parentheses** (). Follow

this with a forward slash and the path from the FTP root of the Player to the job folder. A typical dial-up FTP *URL:* entry of this type would be:

```
ftp://(6105556666)/Jobs
```

When Network Manager begins to transmit a job and sees a phone number in parentheses in the FTP URL instead of an IP address or domain, this is a signal that FTP dial-up is to be used. Network Manager extracts the phone number, looks for the dial-up connection named "InfoChannel Network Manager" and passes the number to that connection to dial.

Dial-up FTP with job folders on the Player

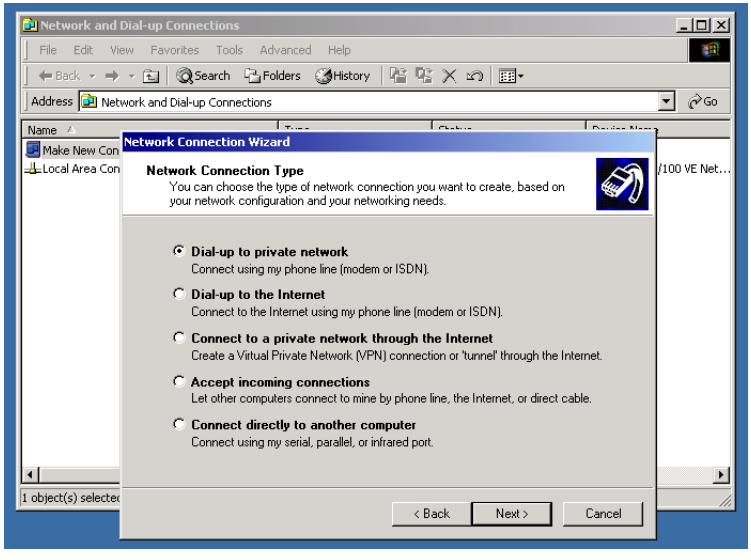
Follow the steps in this section if your InfoChannel Network is configured with job folders on the Players themselves. If Player job folders are located on the Network Manager machine, skip to "*Dial-up FTP with job folders on Network Manager*" on page 240.

Step 1: Create a connection on Network Manager

If Network Manager will be delivering job files to a job folder on the Player through a dial-up connection (RASdial) rather than through a direct Internet connection, you need to create a specially-named connection on the Network Manager to dial the Player.

1. From the Network Manager machine's Start menu, choose *Settings* > *Control Panel*.
2. Open *Network and Dial-up Connections*.
3. Double-click *Make New Connection* to open the Make New Connection Wizard and click *Next*.

4. For *Network Connection Type*, choose *Dial-up to private network* and click *Next*.



5. Select the modem that Network Manager will use to call the Player and click *Next*.

6. Enter a phone number. The number you enter here is only a placeholder, so it can be anything, such as 555-5555.

   You do not need to enter a real Player phone number in this connection because the real phone number is specified in the Player definition (see page 235). Network Manager ensures that the real phone number is passed to the connection and automatically substituted for the placeholder number when the call is made.

   Click *Next*.

7. Under *Connection Availability*, select *For all users* and click *Next*.

8. Finally, you must give the connection a name. In order for the phone number substitution to work, you must name the connection “InfoChannel Network Manager” (without quotes).

9. Click *Finish*.

Testing the connection
When you click *Finish*, you see a connection dialog that allows you to test the connection you have just created. You will not be able to successfully complete the connection test until you have completed all the necessary FTP, account, and connection configuration steps on a Player machine.

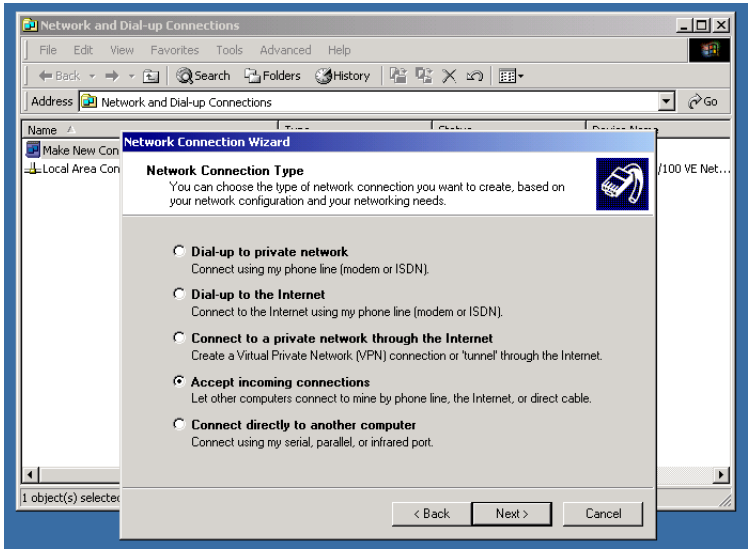
Once you have done so, you should test the InfoChannel Network Manager connection. Pick a Player to connect to, then use the "Net-Manager" user name and the password you configured on that Player, plus its real phone number.

Step 2: Create an Incoming connection on Player

Now you need to create an Incoming connection on the Player to accept Network Manager's communication.

1. From the Player's Start menu, choose *Settings* > *Control Panel*.
2. Open *Network and Dial-up Connections*.
3. Double-click *Make New Connection* to open the Make New Connection Wizard and click *Next*.

4. For *Network Connection Type*, choose *Accept incoming connections* and click *Next*.



5. Select the modem device that the Player uses for communication and click *Next*.

6. Under *Incoming Virtual Private Connections*, select the *Do not allow* option and click *Next*.

7. For *Allowed Users*, select the accounts to which you wish to give incoming connection access on the Player.

   One of these should be the “NetManager” account you created in step 3 on page 232. You may also wish to enable an Administrator account for maintenance purposes. Generally, the number of allowed users should be as few as needed, to reduce security vulnerability.

   Click *Next*.

8. Under *Networking Components*, be sure that at least *Internet Protocol (TCP/IP)* is turned on. *File and Printer Sharing for Microsoft Networks* is a security risk and should be left off.

If your Player is connected to a LAN, you should disallow incoming caller access to the network for security reasons.

a. Select *Internet Protocol* and click *Properties*.

b. In the Incoming TCP/IP Properties sheet, turn off *Allow callers to access by local area network*. The *DHCP* address assignment option should be selected.

c. Click *OK*.

d. Click *Next*.

9. Click *Finish*.

You see "Incoming Connections" listed as a connection in the Network and Dial-up Connections window.

Dial-up FTP with job folders on Network Manager

Use these steps if Player job folders are located on the Network Manager machine and Players access them via dial-up to an ISP.

> ***InfoChannel Configuration Note***
>
> This procedure assumes that you have a modem connected to your Player system and properly configured in Windows. You also must have an ISP account that offers dial-up service, with the dial-up phone number, account username, and password handy.

Step 1: Turn off auto-dial

You need to configure the Player's Internet properties to not use system-wide auto-dialing, since the Player handles the dialing.

1. Right-click on the Internet Explorer icon on the Player desktop, or choose *Tools* > *Internet Options* in Internet Explorer itself.

2. In the Internet Properties sheet, go to the *Connections* panel.

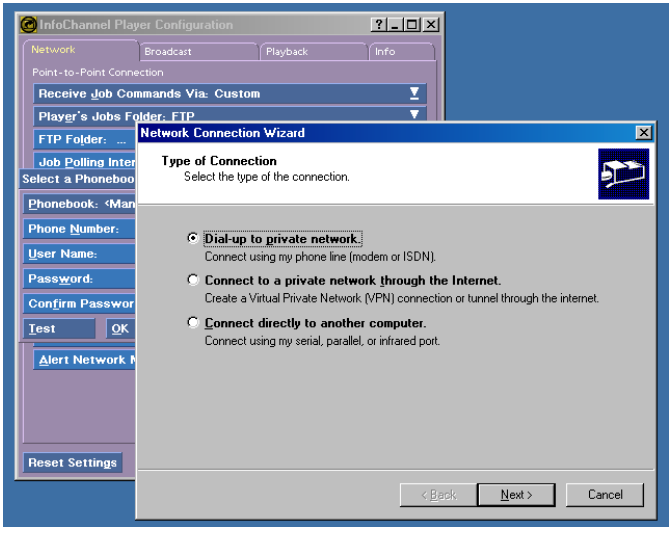
3. Select *Never dial a connection*.
4. Click *OK* exit the Internet Properties sheet.

Step 2: Create the dial-up connection on the Player

1. From the Start menu, go to *Programs* > *Scala InfoChannel Player 3* and choose *Configure InfoChannel Player*.
2. On the *Network* panel, turn on (✓) the *Connect Using Dial-up?* option.
3. Click the *Dial-up Connection:* button to open the Select a Phonebook entry dialog.
4. If a Windows Phonebook entry has already been set up to dial the Internet, select its name from the *Phonebook:* pop-up and skip to "*Step 3: Adjust connection options*".

   Assuming you have not already created a Windows Phonebook entry to dial the Internet, you have two choices: you can create a phonebook entry now using the Windows Wizard, or you can create a simple dialing connection right in this dialog.

   Phonebook entry – To create a phonebook entry, click *Add*. This opens the Windows Network Connection Wizard.



a. For *Type of Connection*, choose *Dial-up to private network* and click *Next*.

b. For *Phone Number to Dial*, enter your Internet service provider's dial-up access number.

c. Click *Next*.

d. For *Connection Availability*, select *Only for myself* and click *Next*.

e. In the final dialog, give the connection a name and click *Finish*.

f. Skip to "*Step 3: Adjust connection options*".

Simple dialing connection – To use a simple dialing connection:

a. Choose <*Manual*> in the *Phonebook:* pop-up. This enables the text boxes below.

b. Enter the number to dial for the Internet in the *Phone Number:* box.

c. Enter the Internet service provider's required login information in the *User Name:* and *Password:* boxes. Passwords are case-sensitive.

d. Enter the password again in the *Confirm Password:* box.

The Player should now be set up to dial the ISP that provides the Internet service for this Player.

The information entered in the *FTP Folder:* button dialog in the Player Config utility is used to connect to an account at the FTP host, from which the FTP connection to the Network Manager machine can be established.

Step 3: Adjust connection options

The *Redial Attempts*, *Seconds Between Attempts*, and *Idle Time Hang Up* options in the lower section of this panel have default values that should work well in most cases.

If you have reason to expect that the Player will have problems connecting or remaining connected, you may want to modify these values.

Step 4: Test the connection

The last thing to do is to test the dial-up connection.

1. Click the *Test* button.
2. This should cause the Player to dial the ISP, connect, and display a success dialog. If you see a dialog saying a connection could not be established instead, review your settings to try to diagnose the problem.

   You can adjust the settings of a phonebook connection by clicking the *Edit* button to open the Windows connection settings dialog.

Dial-up practicality

One factor to keep in mind if you are considering using FTP dial-up is that the connections take much more time than through direct Internet connection.

The process of modems dialing and establishing a connection is inherently slow—allow a minimum of roughly a minute to complete a job file transmission, as opposed to a few seconds for a direct connection.

This makes the dial-up approach less attractive for large networks. The process of just delivering job files to all the Players in a 500-Player network via dial-up would take many hours. Then there is the matter of downloading content at modem speeds. Updates that include multi-gigabyte media files would be impractical in a modem-based system.

Other FTP dial-up approaches

A number of alternative approaches to FTP dial-up job transmission might be used depending on the needs of a given InfoChannel Network.

The procedures given above cover the simplest approach, which uses a single “generic” connection on the Network Manager server for all Players.

FTP dial-up alternatives supported in Network Manager are:

- mixing Direct FTP with Custom connections
- individual connections for each Player
- accessing the Players through a dial-up router
- specifying a custom FTP port number

Mixed connection approach
Direct FTP and Custom connections are not mutually exclusive. In certain situations it is in fact possible to make use of all three connection types—Direct FTP, Custom FTP, and Shared Folder—in contacting Players.

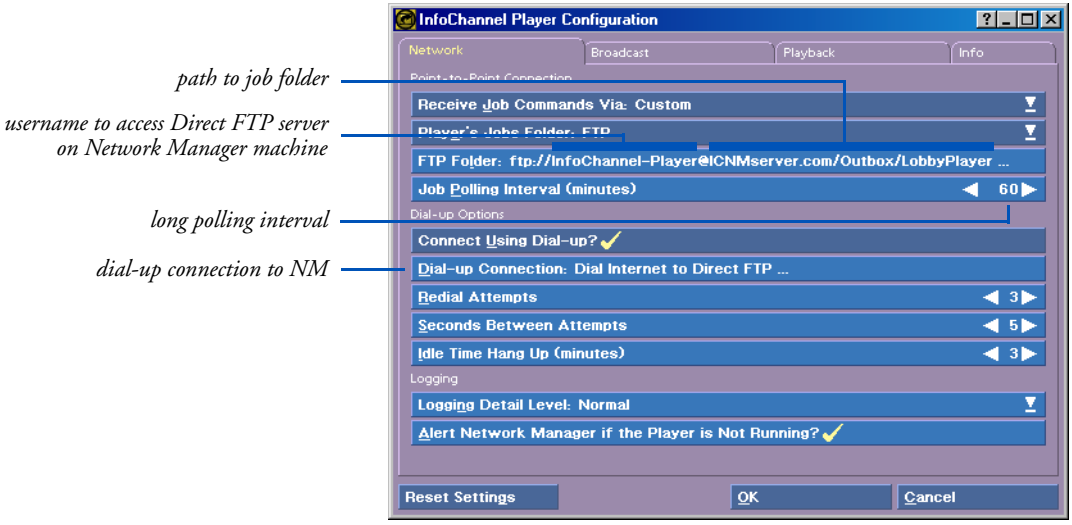
The prime scenario in which it is advantageous to use multiple connection types involves Players that cannot be set up as FTP servers—for example because they do not have static IP addresses. Network Manager cannot deliver jobs to the Players, so Players must poll job folders on Network Manager and download their files by dial-up Custom FTP. However, you can streamline the setup job considerably compared to a completely Custom FTP installation by using Server-Direct FTP at the Network Manager end.

You set it up like this (refer to the indicated sections for relevant procedures):

1. On the Network Manager **Edit System Settings** page, choose *Send and Receive Data Via: Server-Direct FTP*. Create a password and remember it (see page 73).
2. Create job folders for the Players in Network Manager's Network Transmission\Outbox folder (see page 216).
3. In each Player definition, choose *Local or Shared Folder* as the connection type and give the path to the folder you created for it in step 2 (see page 251).
4. On the Player, create a dial-up connection to the Internet called "Dial Internet to Direct FTP" (see page 240).

5. In Player Config, set the Player's job folder to be accessed by Custom FTP (see page 232).
6. Turn on *Connect Using Dial-up?* and choose the "Dial Internet to Direct FTP" connection (see page 241).
7. In the Player Config FTP login dialog, enter the "Dial Internet to Direct FTP" connection's phone number for the URL. Include the path to the Player's job folder as you gave it in step 3 (see page 233).
8. For the FTP username, you must enter "InfoChannel-Player" (case-sensitive) and use the password you gave with Server-Direct FTP in step 1 above (see page 234).
9. Set an appropriately long *Job Polling Interval* value, since the Players will be polling for their jobs via dial-up (see page 234).

You should end up with something like this in Player Config:



This approach is more complex than an all-Direct FTP solution. However, where that is not an option, the mixed approach still involves much less labor than setting up every Player as an FTP server, which would otherwise be necessary.

Using individual Player connections
Creating an individual connection for each Player is very labor-intensive if the system has many Players. However, it offers the advantages of allowing custom connection parameters per Player, and the additional security of a unique username/password for each Player.

To use this approach, you need to create dial-up connections on the Network Manager server for each Player in essentially the same way as described in creating the "InfoChannel Network Manager" connection (Step 1 on page 236). However, instead of a placeholder phone number, enter the actual Player phone number and give the connection a unique name.

Then, in the FTP URL field of the Player definition form, put the Player's unique connection name in the parentheses instead of its phone number:

```
ftp://(LobbyPlayer)/Jobs
```

To have a unique username and password for the Player, enter them in the **Edit Player** form, and change the "NetManager" account on that Player, giving it the name and password that you entered in the form.

Do this for each Player for which you want an individual connection.

It is possible to have individual connections for some Players and to let other Players use the generic connection. Any Players that have their phone number rather than a connection name between the parentheses in the FTP URL "fall through" and get the "InfoChannel Network Manager" connection.

Using a dial-up router
If Network Manager needs to go through a dial-up router to get to one of several Players at a site, that is easily accommodated. Create a connection to the dial-up router as you would for an individual Player (see preceding section). Put the connection name between the parentheses in the URL field. Then, immediately following the close parenthesis, put the IP address or machine name of the target Player. For example:

```
ftp://(MetroRASserver) 12.38.104.57/Jobs

ftp://(MetroRASserver) Lobby1/Jobs
```

Using custom FTP port numbers
If you need to use an FTP port number other than the default (21), you can do so for any of the dial-up FTP approaches. Precede the forward slash that begins the job folder path with a colon and an alternative port number. For example:

```
ftp://(6105556666):12345/Jobs

ftp://(LobbyPlayer):12345/Jobs

ftp://(MetroRASserver) 12.38.104.57:12345/Jobs

ftp://(MetroRASserver) Lobby1:12345/Jobs
```

Custom connection setup: Shared Folder access

The setup process for Local and Shared Folder access is less complex than for FTP access. Many of the same basic steps still need to be performed, however.

For the steps that are the same in both FTP and Shared Folder setup, consult the FTP setup section of this appendix. The procedures and incidental remarks that are no different are not repeated.

Note that if the LAN on which you are setting up this InfoChannel Network does not support TCP/IP-style addressing (through IP number or DNS hostname), then the Health Monitoring feature will not be available for the Network. Health Monitoring requires that type of addressing for its communication tasks.

Shared Folder setup on Network Manager machine

The following steps outline the basic process needed to set up the Network Manager machine to be able to use Custom Shared Folder connections.

Step 1: Share Workspace folders

Ensure that the folder(s) indicated in *Transmission Workspace Location:* and *Network Manager Workspace Location:* are Shared.

Step 2: Set Workspace folder permissions

Ensure that the NetManager and ICPlayer accounts have Read/Write and Modify access permissions to the Workspace folder(s).

Step 3: Set the Network Manager Workspace folder

1. In Network Manager, click the *Configure* tab to display the icons in that panel of the control frame.
2. Click the *System Settings* icon.

   You see the **System Settings** page, which displays the current settings of its options.
3. Click the *Edit Settings* button at the bottom of the page to open the **Edit System Settings** form.
4. Verify that the Network Manager's IP address is correct. (See "*Step 4: Configure transmission options*" on page 73 of chapter 4 for instructions on checking and setting the address.)
5. The *Send and Receive Data Via:* pop-up should be set to *Custom*.
6. In *Network Manager Workspace Location:*, you should see the path that was set up during installation. This defaults to

   `<systemroot>:\Documents and Settings\All Users\Documents\Scala\Network Transmission`

   where *<systemroot>* is the letter of the drive on which Windows is installed.

   You can change this location if you have special requirements:

   - Your network uses a separate file server machine, external to the Network Manager machine
   - You must use a machine that is always running, and the Network Manager machine is not running 24 hours a day every day
   - You need to use a machine that has a different version of Windows—one with a higher number of licensed connections, for example

In choosing a location that is different from the default, Scala recommends that you still locate the folder somewhere within the "Documents and Settings\All Users..." hierarchy shown above if possible.

If you need to change the *Network Manager Workspace Location:* setting, use these steps:

a. Make sure that the location you choose allows read/write/modify access to any user account.

b. It is recommended but not required that you create a folder named "Network Transmission" in the desired location.

c. Then enter the full path to the location here in Network Manager.

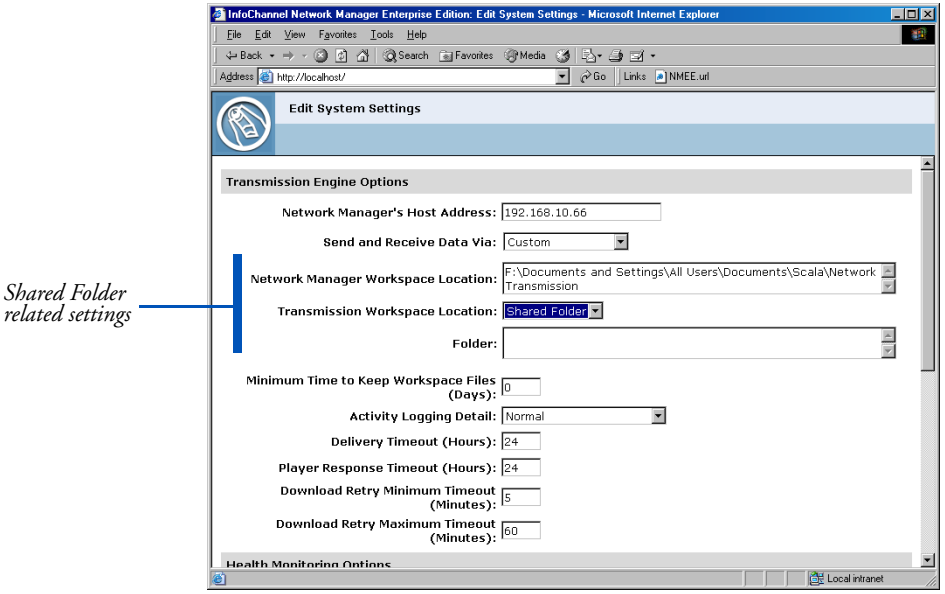
Step 4: Set access to the Transmission Workspace

1. Choose the *Transmission Workspace Location:* setting.

   This setting is what determines whether the Players communicate with Network Manager via the FTP or the Shared Folder approach. Depending on which access method you choose, a different set of options appears below on the page.

> ***InfoChannel Network Manager Note***
>
> All Players will use the Custom Shared Folder point-to-point connection set here for sending and receiving data between themselves and Network Manager. (A Player can have a broadcast connection as well as, or instead of, this point-to-point connection.)

Choose *Shared Folder* from the *Transmission Workspace Location:* pop-up. You see the *Folder:* box below the pop-up:



2. Compare the paths in the *Network Manager Workspace Location:* and *Folder:* boxes and determine whether the Folder setting needs to be changed.

   Normally, for best system performance, you should ensure that the two paths indicate the same location.

   If you need the Players to communicate using a Transmission Workspace location that is different from the Network Manager Workspace, enter the path to that location in the *Folder:* box.

   The path entered in the *Folder:* box needs to be a UNC path—starting with "\\<*computer name*>\<*share name*>\"—which requires that a share be set up. Depending on exactly how you defined the share, your Transmission Workspace *Folder:* setting would be something like this:

   `\\ICNMserver\Network Transmission`

3. Click *OK* to accept your changes on the **Edit System Settings** form.
4. Finally, click *SUBMIT CHANGES* to store your changes in the database.

Step 5: Define the Player

1. Click the *Players* icon in the control frame to open the **Players** page.
2. Click the *New Player* button to open the **New Player** form.
3. Enter a Name and Description for the Player.
4. Choose *Custom* from the *Send Job Commands Via:* pop-up.
5. Choose *Local or Shared Folder* from the *Player's Job Folder:* pop-up.
6. In the *Folder:* box, enter the path that this machine would use to access the Player's job folder, created previously (see "*Creating Player job folders*" on page 216).

   For example:

   ```
   C:\Documents and Settings\All Users\Documents\Scala\Network Transmission\Outbox\Player1
   ```

   A local drive-letter path works, without requiring a share to be set up. The path would need to be a UNC path only if the folder is a share that is not on the Network Manager machine.
7. If the Player will be a member of a Group, make the appropriate settings in the *Group Associations* section (see page 99 for details).
8. Click the *OK* button to close the **New Player** form.
9. If necessary, repeat the process to create additional Players.

When you have finished, click *SUBMIT CHANGES* to store the new Player(s) in the database.

Shared Folder setup on each Player

The tasks in this section must be done on each Player machine you intend to use with a Custom Shared Folder connection.

Step 1: Edit accounts and permissions

1. In order for the system to be secure, you need to disable the Guest user account in Windows. This is necessary to prevent ignorant or malicious users from gaining access to the Player.
2. Create and configure the ICPlayer user account on the Player. For all job functions to be available, this should be an administrator-level account. The ICPlayer account is what the Player uses when it contacts Network Manager. *The Player needs to be running under the ICPlayer account for access to the share on Network Manager.*
3. If the Player job folder is located on the Player, you must also create a NetManager account to allow Network Manager to access the Player. *Network Manager needs to be running under the NetManager account for access to the share on the Player.*
4. Add the ICPlayer user to the Network Transmission folder on this machine so that it has Read/Write and Modify access.
5. If the Player job folder is located on the Player, add the NetManager user to the Network Transmission folder on this machine so that it has Read/Write and Modify access.

Step 2: Point the Player to a shared job folder

You need to use the InfoChannel Player Configuration utility to tell the Player how to reach its job folder.

(There is no need to explicitly tell the Player how to reach the Transmission Workspace—Network Manager includes that information within the job files as mentioned on page 227.)

1. Run the InfoChannel Player Configuration utility on the Player machine you are setting up.
2. In the *Network* panel of the utility, choose *Custom* from the *Receive Job Commands Via:* popup.

3. From the *Player's Job Folder:* popup, choose *Local or Shared Folder*.

   With this setting, the Player polls its job folder directly over the network, using a path that you specify.

   This works with the job folder on the Network Manager machine if that folder is a network share (a Shared folder), or if the job folder is located on the Player itself (a Local folder).

   When you choose *Local or Shared Folder*, you see the *Folder:* button below the pop-up.

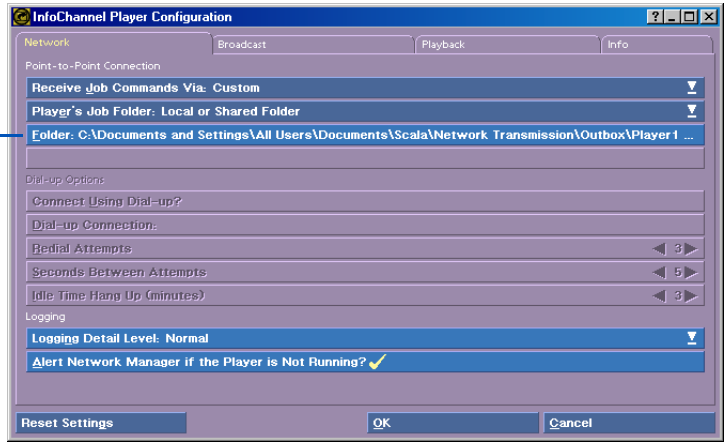
4. Click *Folder:* to open the File dialog, and navigate to the location that you defined in Network Manager for the Player job folder.

> ***Configuration Note***
>
> If you cannot access the job folder through Network Neighborhood in the File dialog, the folder needs to be made Shared.

5. Click *OK* to close the File dialog.

   You should see the path to the folder in either local or UNC format. (The Player Configuration window can be widened if necessary so that you can see all of a long path at once.)

local job folder path



For example, for a local job folder you created on the Player itself:

```
C:\Documents and Settings\All Users\Documents\Scala\Net-
work Transmission\Inbox
```

or a shared job folder you created on Network Manager in its Outbox folder:

```
\\ICNMserver\Network Transmission\Outbox\LobbyPlayer
```

Dial-up settings are used only with FTP connections, so the *Dial-Up Options* settings are disabled when *Local or Shared Folder* is selected.

Glossary

Glossary

A

access mode – in Network Manager Enterprise Edition, a setting that allows users to determine which of several logged-in users is the one permitted to modify settings within the program at that time.

account – in Network Manager Enterprise Edition, in Windows, or on an FTP server, a set of privileges associated with a particular user.

alert – in the Network Manager health monitoring system, a status message that is sent to report an error or some other unexpected condition. See also *heartbeat*.

authoring station – a machine running Scala ICDesigner software, used for authoring and publishing the scripts that are sent to Players.

B

back channel – a data pathway through which a Player can send information back to Network Manager.

broadcast – a type of ICDesigner connection in which Network Manager sends information to many Players all at once, rather than making a separate connection to each Player one at a time. Data that is broadcast reaches each Player, but only those Players to which it is addressed accept the data. Broadcasting can run over a LAN/WAN or the Internet, often using satellite technology. Used when large numbers of Players must be controlled. See also *point-to-point*.

Broadcast Server – a machine that prepares and transmits broadcast files received from a Network Manager machine. Also may refer to the Scala broadcasting software that runs on this machine, or the Network Manager definition of the machine's location.

broadcast folder – a folder on the Broadcast Server machine in which published files are received for subsequent broadcast transmission.

browser – software for viewing web sites, HTML files, and related content, such as Microsoft Internet Explorer.

C

choose – to put a menu option into effect, usually by clicking on a button. This is different from selecting, which highlights an object, file, etc. to work with, but does not actually perform the work.

confirmed broadcasting – broadcasting in which there is a back channel through which Players can respond to transmissions with confirmation or error messages. See also *back channel*.

connection – the type of networking technology used to communicate one computer to another.

content – any files that are played back as part of an InfoChannel script, including graphics files, sound files, video files, and Scala script files themselves.

Content folder – a folder on the Player machine in which all content files sent to the Player are stored. See also *InstalledContent folder*.

control frame – the frame on the left side of the Network Manager window, from which you choose which Network Manager screen to work in.

Custom connection – a type of highly flexible point-to-point connection between Network Manager and InfoChannel Players that does not use Direct FTP. Custom connections can use third-party FTP servers or shared folders. See also *Direct FTP*, *shared folder*.

D

database – in Network Manager, the collection of data on accounts, Players, jobs, etc. that collectively define an InfoChannel Network installation and its settings.

dial-up – access to the Internet that involves the computer using a modem to dial the phone number for another computer's modem, or for an ISP that provides the Internet access. See also *ISP*.

digital video – a video that has been digitized so that it can be controlled from a PC and displayed directly on a computer monitor.

Direct FTP – Scala's easy-to-configure point-to-point scheme for FTP communication between Network Manager and Players, which uses FTP server software built into InfoChannel. See also *Custom connection*.

DirectX – Microsoft's universal graphics driver software for Windows PCs. ICDesigner depends on DirectX for its graphics playback functions, thus DirectX must be present on any PC that plays back ICDesigner scripts.

E

event – an action in a script; virtually everything that happens in a script is an event, including text, sounds, wipes, animations, etc.

EX (extension) **module** – a software module, which may be available separately, to extend the functionality of ICDesigner; for example, enabling control of a new hardware device. If the function involves an activity that can be controlled by the ICDesigner user, a column is added to the Main menu and a new menu specific to the EX can be opened by clicking on the corresponding button.

F

FTP (File Transfer Protocol) – a standard protocol for transferring data over TCP/IP. To use FTP, FTP software must be set up on both sending and receiving ends of an FTP transmission, and the client (initiator) must have a username, password and a valid target address on the server (receiving) computer.

FTP server – a computer that can receive requests for an FTP link from a client machine, or the software on that machine that allows it to do so. IIS includes FTP server capability. Also called an FTP host. See also *IIS*.

G

Group – a collection of Players defined in Network Manager.

H

Health Monitoring – a facility in Network Manager that lets you continuously monitor Players on an InfoChannel Network. Players report

regularly on their operational status, and log files can be retrieved from individual Players to help diagnose problems.

heartbeat – a brief status message sent to the Network Manager machine at regular intervals by a running Player, for Health Monitoring purposes.

host, FTP – See *FTP server*.

I

ICDesigner – InfoChannel Designer 3.

ICPlayer software – the InfoChannel Player 3 software, which must be installed on InfoChannel Player machines to play back InfoChannel Designer 3 scripts. The ICPlayer software also handles communication with Network Manager.

IIS (Internet Information Services) – Microsoft's suite of Internet-related software included with the Windows 2000 and above operating system software. IIS provides both FTP server and web server capability.

InfoChannel Designer 3 (ICDesigner) – Scala's multimedia authoring software for InfoChannel Networks. Scripts are created in ICDesigner, then published to a location accessible to Network Manager for distribution to Player machines. Should not be confused with the original (Release 1) version of InfoChannel Designer (still available), which cannot publish to InfoChannel Networks.

InfoChannel Network – a network for multimedia content distribution and display, comprising an InfoChannel Network Manager 3 machine and at least one Player.

InstalledContent folder – a folder on the Player for content files that have been placed on the machine by some method other than being sent by Network Manager—being copied from a CD-ROM, or downloaded by a separate application, for example. See also *Content folder*.

interactive script – a script in which the viewer controls the direction of the production.

IP address – an address in four-part numerical format that uniquely identifies a computer accessible over a TCP/IP-based LAN or the Internet. For example, 127.0.0.10.

IP Multicast – a method for broadcasting that uses common IP protocols and transmission technologies.

ISP (Internet service provider) – a company that provides web hosting, FTP hosting, email and other Internet services.

J

job – a task or series of tasks generated in InfoChannel Network Manager, to perform maintenance tasks on one or more Players. Jobs typically involve uploading and downloading scripts, log files, and media files. See also *task*.

job file – a relatively small file that is created by Network Manager and placed in the job folder of each Player targeted by that job. The job file instructs the Player on job tasks it should execute, such as downloading an updated script, deleting a file, installing a software update, etc. Job files contain references to content files, but do not themselves contain content.

job folder – a folder, unique to each Player in an InfoChannel Network, into which Network Manager deposits job files for a Player to retrieve. Job folders can be located on the Network Manager machine, on the Player machines, or any other location that is accessible to both.

K

Key – See *Scala Key*.

kiosk – a small, freestanding, often interactive presentation station in a public place, for displaying information on products, events, locations, etc.

L

LAN (local area network) – a network of computers sharing a single server or servers in a single location, typically in an office or building. See also *WAN*.

linked content – in InfoChannel Network publishing, content that is referenced by a script, but is not sent as part of the script when that script is sent to Players. Linked content can be updated at a separate time from normal script content or from an independent source.

log file – a text file consisting of timestamped status and error messages, detailing the operational history of a given piece of software. InfoChannel Players keep individual log files. Windows also maintains its own log files.

login – a name or account under which someone gains a certain level of access to a computer.

M

Main Script – the script that an InfoChannel Player is currently running. This script runs continuously, in a loop, 24 hours a day. It can be updated or changed remotely from Network Manager.

modem (modulator/demodulator) – an electronic device that allows computers to communicate over ordinary telephone lines.

monitor – the device on which an ICDesigner presentation is displayed; for example, a computer monitor, television, video wall, etc.

MPEG (Motion Picture Experts Group) – a standard used for the compression of digital video and audio sequences. Also the file format used for MPEG-compressed information, or a file using this format.

MPG – the file-type extension for digital video files in the MPEG format.

multimedia – the combination of various presentation media such as text, sound, graphics, animation, and video.

N

Network Manager – InfoChannel Network Manager 3, Scala's application for distributing scripts published from InfoChannel Designer 3 to remote InfoChannel Player 3 machines. Available in standard and Enterprise Edition releases.

Network Manager Workspace folder – the folder on the Network Manager machine within which the other local folders used by Network Manager are located. Content and log files are also stored here. See also *Transmission Workspace folder*.

P

path – the sequence of folders leading from a drive to a target file or folder, such as `C:\Tmp\Tempfile.txt`.

pattern matching – use of wildcards * and ? as part of a filename specification, to select multiple files with similar names. For example, "*.txt" matches all files ending with .txt; "Car_0??.jpg" matches any of a series of JPEG image files starting with "Car_0". See also *wildcard*.

permissions – Attributes that may be associated with a folder to restrict the types of access that different users have to it.

pipe – a software/hardware construct that moves data from one location to another.

Player – a computer that runs InfoChannel Player 3 software, which allows it to receive and respond to communication from InfoChannel Network Manager 3, and play InfoChannel Designer 3 scripts. A Player is usually at a site remote from Network Manager, connected to it over the Internet or a LAN. The Player is always running an ICDesigner script, which generates the final display that viewers see.

Player ID – a number that uniquely identifies a Player for targeting of broadcast transmissions from Network Manager.

point-to-point – a type of network connection in which Network Manager sends and receives information one Player at a time, as distinguished from a broadcast connection. See also *broadcast*.

polling interval – the length of time that may elapse before a Player checks for a certain condition, such as whether a job has been delivered to its job folder, or whether its script has been updated.

port, IP – a numerically designated access point for messages of a particular type in TCP/IP network communications.

publish – to prepare an ICDesigner script for distribution. Scripts must be published to InfoChannel Network in order to be available for distribution to Players via Network Manager.

Publish Location – a folder to which ICDesigner scripts are published, where content and other files that may be sent to Players are stored. Publish Locations are defined within Network Manager, and need only be accessible to both the ICDesigner and Network Manager machines.

Q

query – a request for status information from the Broadcast Server software to Players.

R

RAS (remote access service) – a service provided by Windows Dial-Up Networking to establish a network connection with another computer via modem.

root – a particular folder chosen as the base reference point, relative to which all other paths within a web server or FTP server are defined.

S

SCA – the file-type extension used by ICDesigner to identify script files.

SCB – the file-type extension used by ICDesigner to identify script files that have been published.

Scala Key – a small hardware device or "dongle" that is inserted in the parallel or USB port of licensed ICDesigner, Network Manager and ICPlayer machines. A machine will not run Scala software without an appropriate Key installed.

ScalaNet – the name of the networking and maintenance application that was roughly equivalent to Network Manager in the IC200 level of Scala's InfoChannel software.

scheduling – the capability to specify a time or set of times at which an ICDesigner event or a Network Manager job runs. Scheduling of events and jobs are separate and independent.

script – the page-by-page definition of a presentation, which specifies image files, text, sound files, and all other elements of a page, as well as settings that control the way in which it is displayed.

select – to mark or highlight an item so that it will be affected by the next action. This is different from "choose" in that selecting does not actually perform an action, it identifies items you intend to work with.

shared folder – a folder that has been made Shared in Windows, so that it is accessible over a network by other machines. *Shared Folder* is a type of Custom connection available in InfoChannel networking that uses exchanges through shared folders via standard LAN protocols for its communication tasks. See also *Custom connection*.

T

task – a single component of a Network Manager job, consisting of a command and target set of Players, and optionally a set of automatic triggers. Jobs consist of one or more tasks.

TCP/IP – a networking protocol designed for flexible, high-speed communications, used for LANs and the Internet.

timeout – a time limit for an operation. If the timeout period expires before an expected event, some default or alternative action is taken.

topology – the physical and logical layout of a networked system, such as an InfoChannel Network. Possible topologies for InfoChannel use FTP or shared folder connections between different network components.

Transmission Workspace folder – the folder within which the other folders directly used during Player communications are located. This is the same folder as the Network Manager Workspace folder except when offsite FTP hosting is used. See also *Network Manager Workspace folder*.

trigger – an event that causes a Network Manager job to run. A trigger event can be either a scheduled time, the detection of a change in a particular file, or a button click.

U

UNC (Universal Naming Convention) – a type of path that identifies a location by using the computer name and share name as the beginning of the path, preceded by double backslashes. For example:

```
\\mycomputer\myshare\workfiles\work.txt
```

URL (Universal Resource Locator) – a type of path that identifies a location accessible via TCP/IP, such as a web page or FTP site. A URL may include an IP address as the root. For example:

FTP URLs:

```
ftp://127.0.0.10/Workspace
ftp://ICNMserver.com/Workspace
```

Web URL:

```
http://www.scala.com
```

user name – an assigned name that someone must enter, along with a password, in order to connect to an FTP server or to log in to Network Manager Enterprise Edition.

V

VAR (value-added reseller) – a person or company that sells, services, configures, and/or trains clients to use an advanced product. InfoChannel installations are often set up and maintained for their customers by VARs.

versionation – the process of inserting a serial number into a file name or folder name to indicate the order in which successively newer versions of a file with the same base name have been received on the Player. The ICPlayer software automatically versionates script content files as they are received from Network Manager. For example, successive updates of “News.mpg” would become “News;2.mpg”, “News;3.mpg”, and so on.

W

WAN (wide area network) – a network of computers sharing servers in multiple locations, such as the different offices of a large company. See also *LAN*.

web server – software that responds to HTTP requests for web pages (URLs). Also can refer to a machine running such software.

wildcard – a special character that can be used for pattern-matching in specifying the names of files to work with. The most common wildcards are the asterisk (*) to match any number of occurrences of any character, and the question mark (?) to match exactly one occurrence of any character.

workspace folder – a folder within which files for all Players reside, and through which all transmissions between Network Manager and Players pass. See also *Network Manager Workspace folder*, *Transmission Workspace folder*.

Index

E

F

G

H

I

M

N

O

P

R

S

T

U

V

W

X