Forward T Software

FDPostPlay

Configuration of Remote Access via Network



Revision as of April 14, 2010

Quick Start

© SoftLab-NSK

Notice

The information in this document is subject to change without prior notice in order to improve reliability, design, or function and does not represent a commitment on the part of this company.

In no event will we be liable for direct, indirect, special, incidental, or consequential damages arising out of the use or the inability to use the product or documentation, even if advised of the possibility of such damages.

Copyright © 1997 - 2010 SoftLab-NSK Ltd. All Rights Reserved.

No part of this reference manual may be reproduced or transmitted in any form or by any means without the prior written permission of this company.

Throughout this manual, we make reference to product names that are trademarks of other companies. We are using these names for identification purposes only, with no intention of infringement of the trademarks.

FCC Information

FCC ID:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Shielded cables and I/O cards must be used for this equipment to comply with the relevant FCC regulations. Changes or modifications not expressly approved in writing by SoftLab-NSK Ltd. may void the user's authority to operate this equipment.

Limited Warranty

Our company warrants this product against defects in materials and workmanship for a period of one year from the date of purchase. During the warranty period, products determined by us to be defective in form or function will be repaired or replaced at our option, at no charge. This warranty does not apply if the product has been damaged by accident, abuse, misuse, or as a result of service or modification other than by us.

This warranty is in lieu of any other warranty expressed or implied. In no event shall we be held liable for incidental or consequential damages, such as lost revenue or lost business opportunities arising from the purchase of this product.



Table of Contents

Configuration of Remote Access in the FDPostPlay System	3
1. General Information	3
2. Stop of Applications	4
3. Configuration of Network Connections	4
4. Configuration of Local Security Settings	5
5. Configuration of Windows Firewall Turning Off on Both PCs	6
6. Configuration of COM Security	9
7. User Permissions	11
8. Additional Information	17



Configuration of Remote Access in the FDPostPlay System

1. General Information

٢

Remote access via local network to the PostPlay system on another PC is necessary in the following cases:

- to input data into remote storage via the FDPostPlay VideoIn application;
- to create and view clips in remote storage via the FDPostPlay Preview application;
- to broadcast of clips on air from the remote storage via the FDOnAir application.

User that launches a client application must have permission to access the PostPlay system on a remote PC in any of these cases.

Let the user with the USER1 name and some password logged in the system on a client PC. Register a user with the same name (USER1) and password to connect to the PostPlay system on a remote PC for the client application (FDPostPlay VideoIn, FDPostPlay Preview or FDOnAir) launched by the user. It is better when this user is included either in the «Power users» or the «Administrators» groups on the remote PC. In other case he will not be authorized to launch PostPlay system services.

Tip: Apply either to administrator of the remote machine or to administrator of used network to register a user on remote PC and to include him into the group.

For more information on the FDPostPlay system, see the "FDPostPlay – Retransmitted signal delay server. User's Guide".



2. Stop of Applications

- 1. Close all active applications (FDPostPlay VideoIn, FDPostPlay Preview, OnAir) before configuration of remote access.
- 2. Stop the PostPlay server by activating the Advanced/Post-Play Service/Stop commands via the FDPostPlay Indicator application (see the P program icon in taskbar notification area). Confirm that you stop a work of the service.



3. Configuration of Network Connections

Check and configure network connections.

- 1. Be sure that network access among PCs works and PCs are in one workgroup.
- 2. Register the users («Administrators») with the same name and password on both machines. Log in using this name.
- **Important:** It is obligatory to request a password to log in the system.

Further configurations are implemented if the Windows XP SP 2 system is installed on PC.



4. Configuration of Local Security Settings

1. Open Local Security Settings Window via Start: Control Panel > Administrative Tools > Local Security Policy.



- 2. Open the Local Policies > Security Options folder in the Local Security Policy dialog window.
- 3. Select the Network access: Sharing and security model for local accounts policy in the list on the right.
- 4. Open the window with properties by double-clicking the policy.

Local Security Settings		- •	3
$\begin{array}{c c c c c c c c c c c c c c c c c c c $			
Security Settings Account Policies Local Policies Audit Policy Security Options Control Security Options Control Software Restriction Policies TP Security Policies on Loca	Policy A Network access: Let Everyone permissions apply t Network access: Named Pipes that can be accesse Network access: Remotely accessible registry paths Network access: Shares that can be accessed ano Network access: Shares that can be accessed ano Network access: Shares that can be accessed ano Network security: Do not store LAN Manager hash Network security: Force logoff when logon hours e Network security: LAN Manager authentication level Network security: LDAP client signing requirements Network security: Minimum session security for NT Recovery console: Allow automatic administrative I Shutdown: Allow system to be shut down without Shutdown: Clear virtual memory pagefile System cryptography: Use FIPS compliant algorith	Security Setting Disabled COMNAP,COMNOD System\CurrentCon COMCFG,DFS\$ Classic - local users Disabled Enabled Send LM & NTLM re Negotiate signing No minimum Disabled Disabled Disabled Disabled Disabled Disabled	- (
	Bystem objects: Default owner for objects created	Object creator	~

5. Select Classic - local users authenticate as themselves in the appeared window.



5. Turning Off Windows Firewall on Both PCs

1. Open the Start command: Control Panel > Windows Firewall.





- 2. Select Off (not recommended).
- 3. Then click OK.





- 4. Stop Windows Firewall in the Windows XP services window. Open the Start command: Control Panel > Administrative Tools> Services.
- 5. Select the Windows Firewall/Internet Connection Sharing (ICS) service in the list on the right.
- 6. Click Stop.



Important Firewall will be automatically loaded in the system and will be on when installing the SP2 updates for the Windows XP system. During subsequent system updates it will automatically be on.



6. Configuration of COM Security

1. Open Component Services either via the Start command: Control Panel> Administrative Tools > Component Services or the dcomcnfg command line.



- 2. Open the Component Services folder.
- 3. Open the Computers folder or click the Computers folder located on the right.





4. Open the Properties window by right-clicking My Computer.



- 5. Allow remote access in the appeared window by selecting the COM Security tab.
- 6. Click Edit Limits... in the Access Permissions group.

My Computer Properties	?×
General Options Default Properties Default Protocols MSDT 5 COM Securit	y
Access Permissions You may edit who is allowed default access to applications. You m also set limits on applications that determine their own permissions.	nay
6 — Edit Limits Edit Default	
Launch and Activation Permissions You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions.	
Edit Limits Edit <u>D</u> efault	
OK Cancel Ar	ply



7. Put the Remote Access mark in the appeared window for Anonymous Logon and Everyone users, the Allow parameter.

ACO	ess Permission		? 🛛
S	ecurity Limits		
	Group or user names:		
	ANONYMOUS LOGON		
	🕵 Everyone		
	Permissions for ANONYMOUS	A <u>d</u> d	<u>R</u> emove
·			
		Allow	Deny
	Local Access		
	Local Access Remote Access		
	LOGON Local Access Remote Access		
	Local Access Remote Access		
	Local Access Remote Access	Allow	
	Local Access Remote Access		

7. User Permissions

Users with the same name, password and administrative rights must be registered on both PCs.

Complete the following in the COM Security settings on PC with the PostPlay server if both registered users are not administrators:

1. Open the COM Security settings (see subsection 7 above, 1-6 points).



2. Click Edit Limits... in the Access Permissions group.

My Computer Properties	? ×				
General Options Default Properties					
Default Protocols MSDTC COM Security					
Access Permissions	I I				
You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.					
2 — Edit Limits Edit Default					
Launch and Activation Permissions You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions.					
Edit L <u>i</u> mits Edit <u>D</u> efault					
OK Cancel App	yly				

3. Add the user by clicking Add... in the Access Permissions dialog.

Access Permission		? 🛛
Security Limits		
Group or user names:		
MANONYMOUS LOGON		
🕵 Everyone		
(3)	A <u>d</u> d	<u>R</u> emove
Permissions for AND MOUS	Allow	Deny
Local Access	V	
Remote Access	✓	
	OK	Cancel I

- 4. Select remote user name.
- 5. Click OK.

	Select Users, Computers, or Groups	? ×
	<u>S</u> elect this object type: Users, Groups, or Built-in security principals	<u>O</u> bject Types
	Erom this location: sl.iae.nsk.su	Locations
(4)-	Enter the object names to select (<u>examples</u>): Testxp-home	<u>C</u> heck Names
0		1 (
	Advanced 5 — OK	Cancel

- 6. Allow remote and local accesses for the added user by setting the Local Access and Remote Access marks.
- 7. Click OK.

Access Permission ? ×
Security Limits
Group or user names:
🕵 АНОНИМНЫЙ ВХОД 🕵 Все
Testxp-home
Add <u>R</u> emove
Permissions for Bce Allow Deny
Local Access 6 — Z
7 OK Cancel

8. Open the COM Security settings (see above subsection 7, 1-6 items).

My Computer Proper	ties	? ×			
General Default Protocols	Options MSDTC	Default Properties COM Security			
Access Permissions You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.					
	Edit <u>L</u> imits	Edit Default			
Launch and Activation Permissions You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions.					
	Edit Limits	Edit <u>D</u> efault			
	ок	Cancel Apply			

9. Click Edit Defaults... in the Access Permissions group.

10. Add the user by clicking Add... in the Access Permissions dialog.

Access Permission		?	×
Default Security			
Group or user names:			
SELF			
SYSTEM			
(10)	Add	Remove	
Permissions for SELE			
	Allow	Deny	
Local Access			
Local Access Remote Access			
Local Access Remote Access			
Local Access Remote Access			
Local Access Remote Access			
Local Access Remote Access			
Local Access Remote Access			
Local Access Remote Access		Cancel	

- 11. Select remote user name.
- 12. Click OK.

	Select Users, Computers, or Groups	? ×
	<u>S</u> elect this object type: Users, Groups, or Built-in security principals	<u>O</u> bject Types
	<u>F</u> rom this location: sl.iae.nsk.su	Locations
(11)-	Enter the object names to select (<u>examples</u>): Testxp-home	Check Names
	<u>A</u> dvanced 0K	Cancel

- 13. Allow remote and local accesses for the added user by setting the Local Access and Remote Access marks.
- 14. Click $\mathsf{OK}.$

Access Permission			? :	×
Default Security				
<u>G</u> roup or user names:				
SELF				
Testxp-home			_	
		[- 1	
		<u>Add</u>	<u>R</u> emove	
Permissions for SELF		Allow	Deny	
Local Access Remote Access	(13)-	V		
I				
	14 -	ОК	Cancel	



- 15. Click Edit Limits... in the Launch and Activation Permissions group.
- 16. Add the user in the same way (3-5 items).
- 17. Allow remote and local accesses for the added user by setting the Local Launch, Local Activation and Remote Access marks.
- 18. Clik OK.

Launch Permission ?	×
Security Limits	
Group or user names:	
Administrators (Master\Administrators) Bce	
Testxp-home	
Add <u>R</u> emove	
Permissions for Administrators Allow Deny	
Local Launch Remote Launch Local Activation Remote Activation	
0K Cancel	

- 19. Click Edit Defaults in the Launch and Activation Permissions group.
- 20. Add the user in the same way (3-5 items).



- 21. Allow remote and local accesses for the added user by setting the Local Launch, Local Activation and Remote Access marks.
- 22. Click OK.

Launch Permission				?	×
Default Security					
Group or user names:					
Madministrators (Mask Mask Mathematics (Mask Mathematics (Mask Mathematics (Mask Mathematics (Mask))	ter\Admini E	istrators)			
Testxp-home					
		Add	<u>R</u> emove		
Permissions for Administr	ators	Allow	Deny		
Local Launch Remote Launch Local Activation Remote Activation	21)-	5 5 5 5			
(2	22)-	OK	Cano	el	

8. Additional Information

Reassign all calls to the PostPlay system to remote PC for the FDPostPlayVideoIn2 application to record data to remote storage. For this configure Distributed COM on client PC by indicating PC where server applications (PostPlay server) FragmentStorage and RPMServer work.

For Windows 2000.

- 1. Launch the Distributed COM application dcomcnfg via the Start command > Run in the Open field by typing dcomcnfg and pressing Enter.
- 2. Specify the FragmentStorage service location. Open the Application tab and select the RPMFragmentStorage2s application in the list by clicking Properties. Select Location in appeared window. The option is selected by default. Switch the Run application on this computer option off. Then switch the Run application on the following computer option on. Enter network PC name in text field or select PC from network by clicking Browse.
- 3. Specify location of the RPMServer. Repeat actions described in point 2 for the given application.



For Windows XP.

- Launch the Component Services application via the Start command: Control Panel > Administrative Tools > Component Services.
- 2. Open the list of all PC system services via the Component Services > Computers > My Computer > DCOM Config items.



- 3. Specify location of the FragmentStorage system. Find the RPMFragmentStorage2s component in the list.
- 4. Open Properties in the context menu.

Somponent Services	- 🗆 🗙
🐌 File Action View Window Help	
← → 🖻 📧 × 📽 🕅 😫 🎦 🏪 🖫 🏥 🏥 🏥 🕮	
RPMFragmentStorage2s 0 object(s)	
3 Image: Reprint Storage 2 Image: Reprint Storage 2 Reprint Storage 2 Image: Reprint Storage 2 Image: Reprint Storage 2<	
Opens property sheet for the current selection.	

- 5. The RPMFragmentStorage2s Properties window appears. Select the Location tab.
- 6. Switch the Run application on this computer option off.
- 7. Switch the Run application on the following computer option on. After this a field for entering PC local name and the Browse button will be available. The button is used to open the window of search/selection of PC in local network.
- 8. Identify necessary PC.



9. Click OK.

	RPMFragmentStorage2s Properties	? ×
	General Location Security Endpoints Identity	
	The following settings allow DCOM to locate the correct computer for application. If you make more than one selection, then DCOM uses the applicable one. Client applications may overide your selections.	his e first
	Run application on the computer where the <u>d</u> ata is located.	
6-	—— Run application on <u>t</u> his computer.	
(7)-	Run application on the <u>following</u> computer:	
(8	8 testxp-home Browse	
	9 — OK Cancel A	oply

 $10.\ {\rm Specify}\ {\rm location}\ {\rm of}\ {\rm the}\ {\rm RPMServer}\ {\rm in}\ {\rm the}\ {\rm same}\ {\rm way}.$

Useful Links

ForwardT Software set: description, download, documentation, solutions http://www.softlab-nsk.com/forward/index.html

Support

e-mail: forward@sl.iae.nsk.su forward@softlab-nsk.com

Forum

http://www.softlab-nsk.com/forum

Documentation for more information:

FDPostPlay – Retransmitted Signal Delay Server. User's Guide.

Translation from 1 December, 2010

 \bigcirc SoftLab-NSK

