

JP1 Version 12 for Windows Systems

**JP1/File Transmission Server/FTP Description,
Reference and Operator's Guide**

3021-3-D38(E)

Notices

■ Relevant program products

P-2A41-94CL JP1/File Transmission Server/FTP 12-00 (for Windows Server 2012, and Windows Server 2016)

■ Trademarks

HITACHI, JP1 are either trademarks or registered trademarks of Hitachi, Ltd. in Japan and other countries.

Microsoft and Visual Studio are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Microsoft is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Visual C++ is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

Windows is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

Windows Server is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

Other company and product names mentioned in this document may be the trademarks of their respective owners.

Throughout this document Hitachi has attempted to distinguish trademarks from descriptive terms by writing the name with the capitalization used by the manufacturer, or by writing the name with initial capital letters. Hitachi cannot attest to the accuracy of this information. Use of a trademark in this document should not be regarded as affecting the validity of the trademark.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

This product includes software developed by IAIK of Graz University of Technology.

This software and documentation is based in part on BSD Networking Software, Release 1 licensed from The Regents of the University of California. We acknowledge the role of the Computer Systems Research Group and the Electrical Engineering and Computer Sciences Department of the University of California at Berkeley in its development.

1. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)

2. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

3. This product includes software written by Tim Hudson (tjh@cryptsoft.com)

4. This product includes the OpenSSL Toolkit software used under OpenSSL License and Original SSLeay License. OpenSSL License and Original SSLeay License are as follow:

LICENSE ISSUES

=====

The OpenSSL toolkit stays under a double license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit.

See below for the actual license texts.

OpenSSL License

```

-----
/* =====
* Copyright (c) 1998-2018 The OpenSSL Project. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in
* the documentation and/or other materials provided with the
* distribution.
*
* 3. All advertising materials mentioning features or use of this
* software must display the following acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
* endorse or promote products derived from this software without
* prior written permission. For written permission, please contact
* openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
* nor may "OpenSSL" appear in their names without prior written
* permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
* acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;

```

```

* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* =====
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
Original SSLeay License
-----
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given
attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright

```

```

* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
* must display the following acknowledgement:
* "This product includes cryptographic software written by
* Eric Young (eay@cryptsoft.com)"
* The word 'cryptographic' can be left out if the routines from the library
* being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
* the apps directory (application code) you must include an acknowledgement:
* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/

```

HITACHI
Inspire the Next

©Hitachi, Ltd.



■ Microsoft product screen shots

Microsoft product screen shots reprinted with permission from Microsoft Corporation.

■ Microsoft product name abbreviations

This manual uses the following abbreviations for Microsoft product names.

Abbreviation			Full name or meaning
MSDN			MSDN ^(R)
Visual C			Visual C++ ^(R)
Visual Studio			Visual Studio ^(R)
Win32			Win32 ^(R)
Windows	Windows Server 2012	Windows Server 2012	Microsoft ^(R) Windows Server ^(R) 2012 Datacenter
			Microsoft ^(R) Windows Server ^(R) 2012 Standard
		Windows Server 2012 R2	Microsoft ^(R) Windows Server ^(R) 2012 R2 Datacenter
			Microsoft ^(R) Windows Server ^(R) 2012 R2 Standard
	Windows Server 2016		Microsoft ^(R) Windows Server ^(R) 2016 Datacenter
			Microsoft ^(R) Windows Server ^(R) 2016 Standard

■ Restrictions

Information in this document is subject to change without notice and does not represent a commitment on the part of Hitachi. The software described in this manual is furnished according to a license agreement with Hitachi. The license agreement contains all of the terms and conditions governing your use of the software and documentation, including all warranty rights, limitations of liability, and disclaimers of warranty.

Material contained in this document may describe Hitachi products not available or features not available in your country.

No part of this material may be reproduced in any form or by any means without permission in writing from the publisher.

■ Issued

Jan. 2019: 3021-3-D38(E)

■ Copyright

All Rights Reserved. Copyright (C) 2019, Hitachi, Ltd.

Summary of amendments

The following table lists changes in this manual (3021-3-D38(E)) and product changes related to this manual.

Changes	Location
The following OS was deleted from the supported OSs: <ul style="list-style-type: none">Windows Server 2008 R2	--
Files can now be transmitted via FTPS.	<i>1.1, 3.3.1(1), 3.4.1, 3.6.1, 3.16, 3.17, Chapter 6, Chapter 7, 9.3.2, Appendix A, Appendix D.2, Appendix E.1, Appendix I.3</i>
The following OSs are now supported: <ul style="list-style-type: none">Windows Server 2016	<i>2.1.1</i>
Event IDs 43, 45, 46, and 47 have been added to the messages displayed in Event Viewer.	<i>8.2</i>
Messages for <code>ftstran</code> command execution have been added.	<i>8.3.1</i>
Messages for <code>ftsregc</code> command execution have been added.	<i>8.3.2</i>

Legend:

--: Not applicable

In addition to the above changes, minor editorial corrections were made.

Preface

This manual describes the functions of and explains how to operate JP1/File Transmission Server/FTP.

In this manual, JP1/File Transmission Server/FTP is abbreviated as *JP1/FTP*.

■ Intended readers

This manual is intended for system administrators of systems that use JP1/FTP to transmit files, and the system operators who operate and maintain such systems. Note that this manual assumes that readers have the following knowledge:

- Knowledge about Windows
- Knowledge about TCP/IP
- Knowledge about FTP protocol
- Knowledge about FTPS protocol
- Knowledge about PKI

■ Conventions: Fonts and symbols

The following table explains the text formatting conventions used in this manual:

Text formatting	Convention
Bold	Bold characters indicate text in a window, other than the window title. Such text includes menus, menu options, buttons, radio box options, or explanatory labels. For example: <ul style="list-style-type: none">• From the File menu, choose Open.• Click the Cancel button.• In the Enter name entry box, type your name.
<i>Italic</i>	Italic characters indicate a placeholder for some actual text to be provided by the user or system. For example: <ul style="list-style-type: none">• Write the command as follows: <code>copy source-file target-file</code>• The following message appears: A file was not found. (file = <i>file-name</i>) Italic characters are also used for emphasis. For example: <ul style="list-style-type: none">• Do <i>not</i> delete the configuration file.
Monospace	Monospace characters indicate text that the user enters without change, or text (such as messages) output by the system. For example: <ul style="list-style-type: none">• At the prompt, enter <code>dir</code>.• Use the <code>send</code> command to send mail.• The following message is displayed: <code>The password is incorrect.</code>

The following table explains the symbols used in this manual:

Symbol	Convention
	In syntax explanations, a vertical bar separates multiple items, and has the meaning of OR. For example:

Symbol	Convention
	A B C means A, or B, or C.
{ }	In syntax explanations, curly brackets indicate that only one of the enclosed items is to be selected. For example: { A B C } means only one of A, or B, or C.
[]	In syntax explanations, square brackets indicate that the enclosed item or items are optional. For example: [A] means that you can specify A or nothing. [B C] means that you can specify B, or C, or nothing.
. . .	In coding, an ellipsis (. . .) indicates that one or more lines of coding have been omitted. In syntax explanations, an ellipsis indicates that the immediately preceding item can be repeated as many times as necessary. For example: A, B, B, . . . means that, after you specify A, B, you can specify B as many times as necessary.
()	Parentheses indicate the range of items to which the vertical bar () or ellipsis (. . .) is applicable.
(())	Double parentheses enclose the range of values that can be specified.
<< >>	Double angle brackets enclose the default value.

■ Conventions: Version numbers

The version numbers of Hitachi program products are usually written as two sets of two digits each, separated by a hyphen. For example:

- Version 1.00 (or 1.0) is written as 01-00.
- Version 2.05 is written as 02-05.
- Version 2.50 (or 2.5) is written as 02-50.
- Version 12.25 is written as 12-25.

The version number might be shown on the spine of a manual as *Ver. 2.00*, but the same version number would be written in the program as *02-00*.

Contents

Notices 2

Summary of amendments 7

Preface 8

1 Overview of JP1/FTP 15

- 1.1 Features 16
- 1.2 Functions 17
 - 1.2.1 File transmission function 17
 - 1.2.2 Operations-Manager function 18
 - 1.2.3 JP1 program linkage function 18
- 1.3 Flow of JP1/FTP operations 19
 - 1.3.1 Registering JP1/FTP definition information 19
 - 1.3.2 Transmitting a file 20
 - 1.3.3 Saving and recovering JP1/FTP settings 21
 - 1.3.4 Checking the JP1/FTP definition information for other hosts 22

2 Installation and Setup 24

- 2.1 JP1/FTP system configuration 25
 - 2.1.1 Supported OSs 25
 - 2.1.2 Basic system configuration 25
- 2.2 Installing and setting up 26
 - 2.2.1 Installing JP1/FTP 26
 - 2.2.2 Setting the language type 26
 - 2.2.3 Setting the port numbers 27
 - 2.2.4 Creating environments in which names can be resolved 28
 - 2.2.5 Uninstalling JP1/FTP 28
- 2.3 Starting and stopping services 29
 - 2.3.1 Types of services 29
 - 2.3.2 Starting services 29
 - 2.3.3 Stopping services 30

3 File Transmission by JP1/FTP 31

- 3.1 Defining an environment for JP1/FTP 32
 - 3.1.1 Defining an environment for JP1/FTP 32
 - 3.1.2 Using a definition file to define an environment for JP1/FTP 34
- 3.2 Registering the users who can log in to a JP1/FTP server 37
 - 3.2.1 Registering the login users 37

3.2.2	Changing login user information	38
3.2.3	Deleting login user information	39
3.3	Registering auto-start programs	40
3.3.1	Registering auto-start programs	40
3.3.2	Changing the auto-start programs	45
3.3.3	Deleting auto-start programs	45
3.3.4	Changing the information displayed in the Auto-Start Program Registration window	46
3.4	Registering transmission information	47
3.4.1	Registering transmission information onto a transmission card	47
3.4.2	Changing the information registered on a transmission card	52
3.4.3	Deleting transmission cards	54
3.4.4	Checking the contents of a transmission card	54
3.5	Transmitting files	56
3.5.1	Executing transmission by specifying a transmission card (Select Card method of file transmission)	56
3.5.2	Executing transmission by entering a transmission card (Enter Information method of file transmission)	58
3.6	Checking the transmission logs	60
3.6.1	Checking the details of transmission results and errors	60
3.6.2	Changing the information displayed in the Log Information window	62
3.6.3	Changing the log file that is displayed	64
3.6.4	Using the ftshistory command to display logs	64
3.7	Saving and recovering JP1/FTP settings	65
3.7.1	Saving definition information	65
3.7.2	Recovering definition information	66
3.8	Outputting definition information as text	69
3.8.1	Outputting definition information as text	69
3.9	File transmission in the PASV mode	71
3.9.1	Registering the host names	71
3.10	Function for controlling remote host connections	73
3.10.1	Registering host names	73
3.11	Using JP1/FTP in a multiple IP address environment	76
3.11.1	Creating a definition file	76
3.12	Collecting access logs	79
3.12.1	Settings for collecting access logs	79
3.12.2	Log output file	79
3.12.3	Messages that are output to the access logs	79
3.13	Function for using the access control function to change the root directory for absolute path names	81
3.13.1	Registering the absolute path name format	81
3.14	FTP connection response message control function	83
3.14.1	Registering the definition information	83
3.14.2	FTP connection response message that is displayed	84
3.15	Using JP1/FTP in an IPv6 environment	86

- 3.15.1 Registering the Internet protocol version 86
- 3.16 Using FTPS (at the FTP client) 88
 - 3.16.1 Certificate and CRL 88
 - 3.16.2 Notes about the certificate and the CRL 88
 - 3.16.3 Definition of transmission information 88
- 3.17 Using FTPS (at the FTP server) 89
 - 3.17.1 Private key and certificate 89
 - 3.17.2 Notes about the private key and the certificate 89
 - 3.17.3 Creating a definition file 89

4 JP1/FTP Operations Management 91

- 4.1 Setting up the Operations-Manager Console 92
 - 4.1.1 Adding managed hosts 93
 - 4.1.2 Deleting managed hosts 94
- 4.2 Organization and functions of the Operations-Manager Console windows 96
 - 4.2.1 Environment Definition window 96
 - 4.2.2 User-To-Login Registration window 97
 - 4.2.3 Auto-Start Program Registration window 97
 - 4.2.4 Transmission Registration window 98
 - 4.2.5 Log Information window 99
- 4.3 Examples of Operations-Manager Console menu operations 101
 - 4.3.1 Example of registering login user information 101
 - 4.3.2 Example of distributing (copying) transmission information 101
 - 4.3.3 Example of displaying log information 102
 - 4.3.4 Example of outputting multiple definition information items as text 103

5 Linkage with Other JP1 Programs 105

- 5.1 Linking to JP1/AJS3 106
 - 5.1.1 System configuration for linking to JP1/AJS3 106
 - 5.1.2 Specifying the settings for linking to JP1/AJS3 106
 - 5.1.3 Performing scheduled transmissions 108
- 5.2 Linking to JP1/IM 115
 - 5.2.1 System configuration for linking to JP1/IM 115
 - 5.2.2 Specifying the settings for linking to JP1/IM 115
 - 5.2.3 Starting the services 115
 - 5.2.4 Monitoring transmission results by JP1/IM 116

6 Commands 117

- List of commands 118
- Details of commands 119
 - ftstran - executes transmission 120
 - ftsregc - registers, changes, deletes, and displays transmission information 123
 - ftshistory - displays log information 126

ftssave - saves definition information 127
ftsload - recovers definition information 128

7 API Library 130

How to use the library 131
Example of library usage 139
List of functions 143
Details of functions 144
fts_ftp_open_ex() - establish connection with JP1/FTP 145
fts_ftp_syn_request_ex() - register transmission requests (synchronous) 147
fts_ftp_asyn_request_ex() - register transmission requests (asynchronous) 149
fts_ftp_event_ex() - obtain the transmission-end results 151
fts_ftp_cancel() - cancel transmission 153
fts_ftp_close() - release connection with JP1/FTP 155

8 Messages 156

8.1 Format of displayed messages 157
8.1.1 Message output formats 157
8.1.2 Formats of message explanations 158
8.2 Messages displayed in Event Viewer 159
8.3 Messages displayed during command execution 167
8.3.1 Messages displayed during execution of the ftstran command 167
8.3.2 Messages displayed during execution of the ftsregc command 169
8.3.3 Messages displayed during execution of the ftshistory command 172
8.3.4 Messages displayed during execution of the ftsload command 174
8.3.5 Messages displayed during execution of the ftssave command 174
8.4 Messages output to the access log 176

9 Troubleshooting 177

9.1 Error handling procedures 178
9.2 Types of log information 179
9.2.1 Common message log 179
9.2.2 Log by process 179
9.3 Data to collect when a problem occurs 180
9.3.1 Log information about the operating system (OS) 180
9.3.2 Information about JP1/FTP 180
9.3.3 List of JP1/FTP processes 181
9.3.4 Operation information 181
9.3.5 Error information on screen displays 182
9.3.6 How to collect data 182

Appendixes 184

A List of Files and Directories 185
B Port Numbers 189

B.1	List of port numbers	189
B.2	Firewall passage directions	189
B.3	Items to check when performing transmission via a firewall	190
C	List of Processes	191
D	JP1 Events	192
D.1	List of JP1 events	192
D.2	Attributes of JP1 events	192
E	Format Files Used for Output of Definition Information	201
E.1	Creating a format file	201
F	Tools	204
F.1	FTSTRANINIT.BAT and FTSMGRINIT.BAT - initialize results	204
F.2	FTSMGRHOST.BAT - change monitored host information	205
G	Notes about Operation	206
H	Changes in Each Version	210
H.1	Changes in 12-00	210
H.2	Changes in 11-00	210
H.3	Changes in 10-10	210
H.4	Changes in 10-00	211
H.5	Changes in 09-00	211
I	Reference Material for This Manual	213
I.1	Related publications	213
I.2	Conventions: Abbreviations	213
I.3	Conventions: Acronyms	213
I.4	Conventions: KB, MB, GB, and TB	214

Index 215

1

Overview of JP1/FTP

JP1/FTP is a program for transmitting files in LAN and WAN environments. This chapter describes the features and functions of JP1/FTP. It also uses an example to explain the flow of the file transmission operations.

1.1 Features

JP1/FTP is a file transmission program that is provided with an Operations-Manager function. It uses the FTP procedure, a standard protocol for file transmission. It also enables safe transmission of files by using FTPS. Compared with the OS's standard FTP functions, JP1/FTP provides functions that are especially useful when files are transmitted by standard applications.

- Automation of file transmission jobs
 - The job start function enables you to automate processing startup when file transmission is completed.
 - The API function enables you to send files to and receive files from user applications.
 - You can automate processing such as receiving data from a base server on a regular schedule throughout the day and then summing up the data at the end of the day.
- Management of execution status
 - By using the display and notification of file transmission status, you can take actions such as error handling.
 - You can manage the transmission status by collecting and displaying log information during file transmission.
- Scheduling transmissions

When linked to JP1/AJS3, JP1/FTP enables you to easily perform scheduled transmission for standard applications. Additionally, JP1/FTP's automated job startup enables you to automate job execution when file transmission is finished.
- Centralized monitoring by JP1/IM

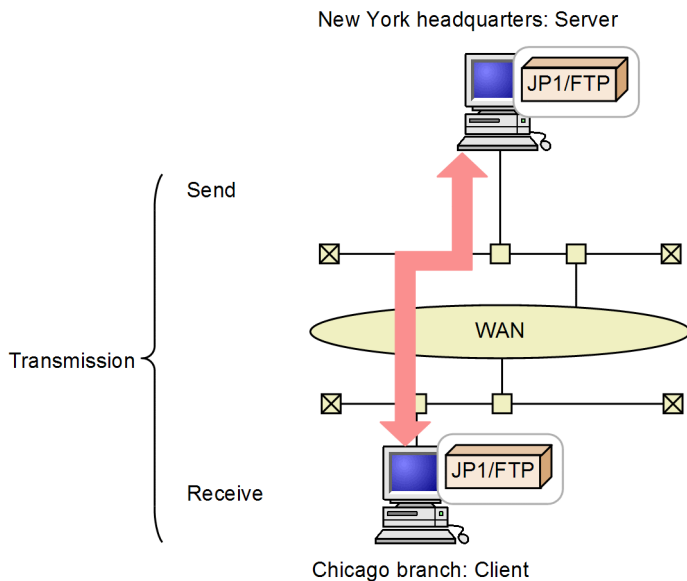
By using JP1/IM, you can achieve centralized monitoring of services starting and stopping and the termination status of transmissions (normal, warning, abnormal).
- Operations-Manager function

You can perform processing on multiple JP1/FTP hosts that are linked in a network, such as by displaying their file transmission histories and distributing and setting up various definition information.

1.2 Functions

The following figure presents an example of file transmission using JP1/FTP.

Figure 1–1: Example of file transmission (transmitting files between the Chicago branch and the New York headquarters)



Use of JP1/FTP to send and receive files between hosts is called *transmission*. The end that sends a file is called the *client*, while the end that receives the file is called the *server*. A host can function as both client and server.

JP1/FTP provides the following three functions:

- File transmission function
- Operations-Manager function
- JP1 program linkage function

The following subsections describe these functions.

1.2.1 File transmission function

(1) Using transmission cards to register and transmit transmission information

You use a *transmission card* to register the information to be transmitted. You can specify multiple transmission cards and transmit in batch mode. You can use a transmission card that has already been registered as a model by editing its contents and then transmitting the edited version.

JP1/FTP supports the following operations:

- Transmitting multiple files in the batch mode
You can use wildcards to specify multiple files that are to be transmitted. If you set standard file naming rules, you can achieve efficient transmission, for example when business report files of multiple groups are to be transmitted on a weekly basis.

- Checking the file size during transmission

You can check that the size of a file is the same at the sender and the receiver. If transmission terminates successfully, any damage to the file that occurs during transmission is not detected. However, if you check the file size, any change in the file size is detected as a transmission error. This helps you achieve reliable transmission.

You can check the file size only when transmission is between JP1/FTP instances or between JP1/FTP and uCosminexus Service Platform.

(2) Automatically starting a program after file transmission

You can specify a program to start automatically when file transmission is completed, thereby achieving automation of task execution. The following types of automated program startup are supported:

- Starting a specified program when file transmission is performed by a specified user
- Starting a specified program when a specified file is transmitted

(3) Checking file transmission logs

You can check transmission logs from either the server or the client. Supported operations include viewing transmission logs and checking for errors when transmission has terminated abnormally. You can also select the information to be included in the logs, such as displaying logs of abnormal termination information only.

(4) Using an API to link with user programs

You can use an API to link with user programs to perform file transmission. This feature enables you to achieve file transmission that is appropriate to the environment in use and to automate task execution after transmission.

(5) Saving and restoring definition information

You can save the JP1/FTP definition information items and distribute them to other hosts. You can also restore definition information from the saved items. By restoring the definition information of one host at multiple different hosts, you can simplify the setup procedure.

1.2.2 Operations-Manager function

The Operations-Manager function enables you to reference the logs of multiple JP1/FTP hosts that are linked in a network and check their definition information from a single host, thereby reducing the system administrator's workload.

1.2.3 JP1 program linkage function

(1) Linking to JP1/AJS3 to perform scheduling transmissions

You can link to JP1/AJS3 to execute jobs when transmission occurs. This function enables you to automate execution of a series of jobs.

(2) Linking to JP1/IM to check transmission results

You can link to JP1/IM to check the JP1/FTP service status and the results of file transmission. Normally, JP1/IM is used to monitor operations. In the event of an error, you can use the JP1/FTP logs to check the details.

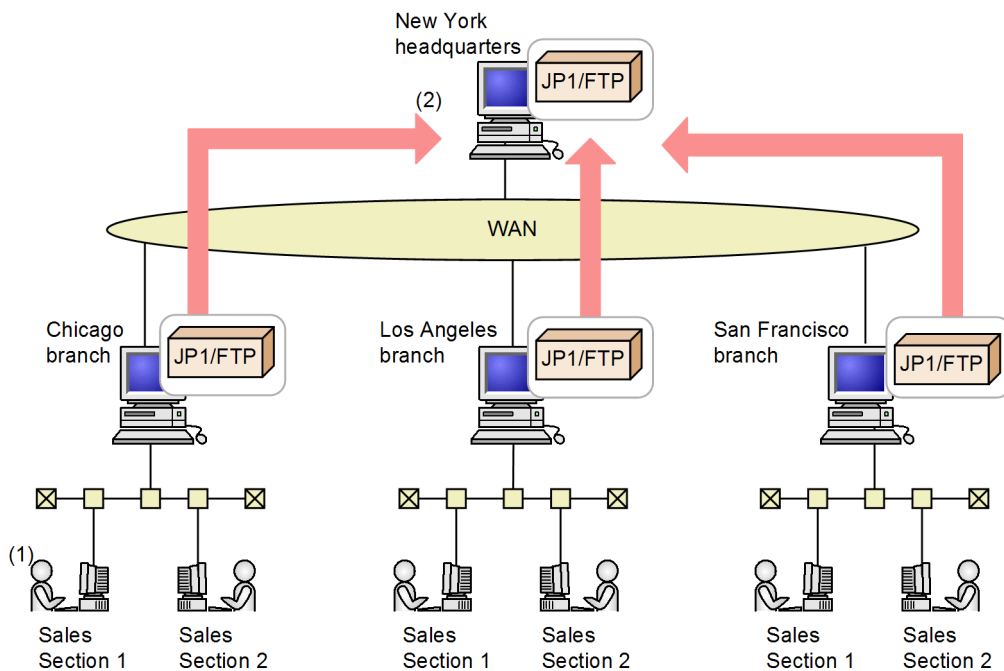
1.3 Flow of JP1/FTP operations

To start each function of JP1/FTP, from the **Start** menu, choose **Programs, JP1_File Transmission Server_FTP**, and then a function menu.

This section uses the following application example to describe the flow of the file transmission operations.

Figure 1–2: Example of application

- Example of application:
- (1) At each branch host, the sales report files are stored by Sales Sections 1 and 2.
 - (2) At each branch host, the sales report files are summed up and then JP1/FTP is used to transmit them to the New York headquarters.

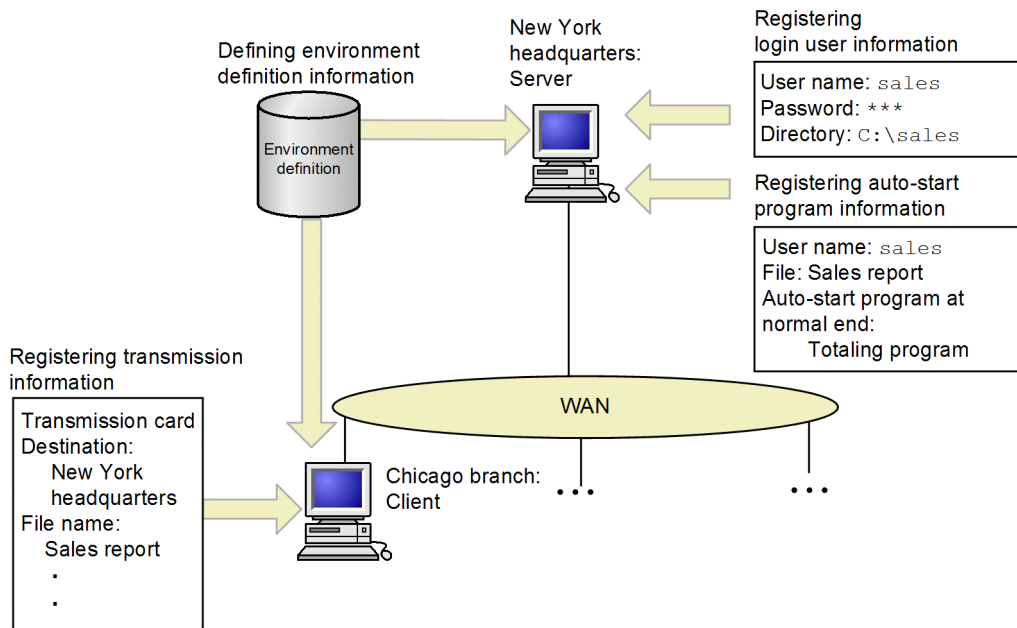


1.3.1 Registering JP1/FTP definition information

The following definition information must be registered:

- Environment definition information
- Transmission execution information (auto-start program information, transmission information, and login user information)

Figure 1–3: Example of registering definition information

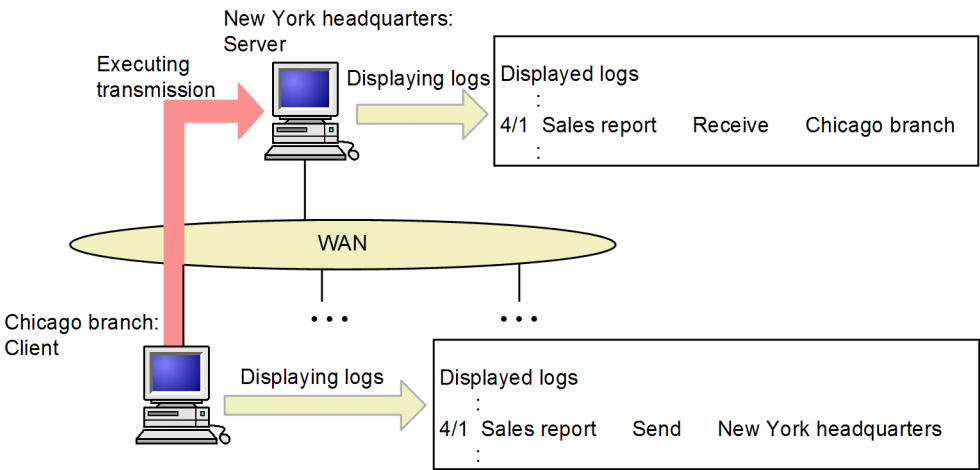


Type of information	Overview of operation	Executing host	Menu selection
Environment definition information	Defining environment definition information: Defines a JP1/FTP environment, such as the buffer size during transmission and the log file size.	Server/client	Environment Definition (see 3.1 Defining an environment for JP1/FTP)
Transmission execution information	Registering login user information: Registers the users who are permitted to log in to the server during file transmission. In the example, a user (<i>sales</i>) who logs in to the server at the New York headquarters from the Chicago branch is registered.	Server	User-To-Login Registration (see 3.2 Registering the users who can log in to a JP1/FTP server)
	Registering auto-start program information: Registers programs that are started automatically at the server when file transmission to the server is completed. The example registers into the server at the New York headquarters that the <i>Totaling program</i> is to be started when a <i>Sales report</i> file is received from <i>sales</i> .	Server	Auto-Start Program Registration (see 3.3 Registering auto-start programs)
	Registering transmission information: Registers in transmission cards the information to be transmitted (such as remote server names and transmission file names). A command can also be used to register transmission information. In this example, information about file transmission from the Chicago branch to the New York headquarters is registered.	Client	Transmission Regist. & Exe. (see 3.4 Registering transmission information)

1.3.2 Transmitting a file

You register transmission information onto a *transmission card* and then execute transmission. Logs can be used to check the transmission results.

Figure 1–4: Example of file transmission

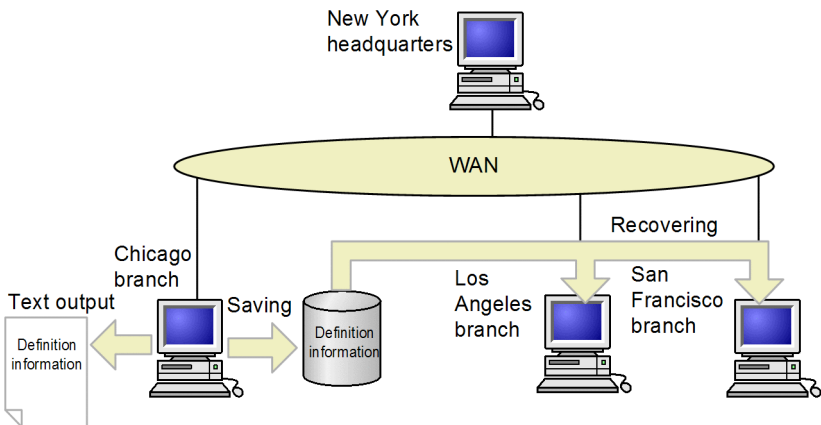


Overview of operation	Executing host	Menu selection
<p>Transmitting a file:</p> <p>Specifies a registered transmission card and then executes transmission. A command can also be used to execute transmission.</p> <p>This example transmits a file from the Chicago branch to the New York headquarters.</p>	Client	Transmission Regist. & Exe. (see 3.5 <i>Transmitting files</i>)
<p>Displaying logs:</p> <p>Displays logs to check the result of file transmission.</p> <p>In this example, reception logs can be checked at the New York headquarters and transmission logs can be checked at the Chicago branch.</p>	Server/client	Log Information (see 3.6 <i>Checking the transmission logs</i>)

1.3.3 Saving and recovering JP1/FTP settings

You can save and recover JP1/FTP settings and output them in text format.

Figure 1–5: Example of saving and recovering JP1/FTP settings

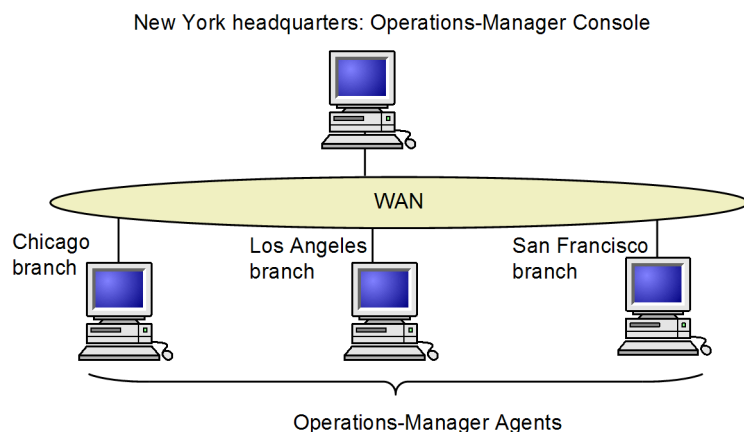


Overview of operation	Executing host	Menu selection
<p>Saving and recovering JP1/FTP settings: You can save the definition information created at one host and then recover it at other hosts.</p> <p>Definition information that can be saved and recovered:</p> <ul style="list-style-type: none"> • Environment settings • User-to-login settings • Auto-start program settings • Transmission settings <p>This example recovers definition information for the Chicago branch at the Los Angeles and San Francisco branches. This makes it easy to set up environments.</p>	Server/client where the information is registered	<p>Saving and Recovering Settings (see 3.7 <i>Saving and recovering JP1/FTP settings</i>)</p>
<p>Outputting definition information as text: You can output the registered information in text format. For the output format, use the provided sample.</p> <p>Definition information that can be output as text:</p> <ul style="list-style-type: none"> • User-to-login settings • Auto-start program settings • Transmission settings • Log information 	Server/client where the information is registered	<p><i>menu-item-for-type-of-information</i> (see 3.8 <i>Outputting definition information as text</i>)</p>

1.3.4 Checking the JP1/FTP definition information for other hosts

You can use the Operations-Manager Console to check and change other hosts' JP1/FTP definition information and to reference their logs.

Figure 1–6: Example of checking the JP1/FTP definition information for other hosts



Overview of operation	Executing host	Menu selection
<p>Operations-Manager Console: Enables you to check, register, change, and delete definition information for other hosts and to reference log information.</p> <p>The end that checks definition information is called the <i>Operations-Manager Console</i>, and the end whose definition information is checked is called the <i>Operations-Manager Agent</i>.</p>	Operations-Manager Console	<p>Manager Console (see 4. <i>JP1/FTP Operations Management</i>)</p>

Overview of operation	Executing host	Menu selection
In the above example, the New York headquarters can reference each branch's log information and check its definition information.	Operations-Manager Console	Manager Console (see 4. JP1/FTP Operations Management)

2

Installation and Setup

This chapter describes the setup of JP1/FTP and the procedures required before JP1/FTP can be used.

2.1 JP1/FTP system configuration

This section describes the JP1/FTP system configuration.

2.1.1 Supported OSs

The following OSs are supported:

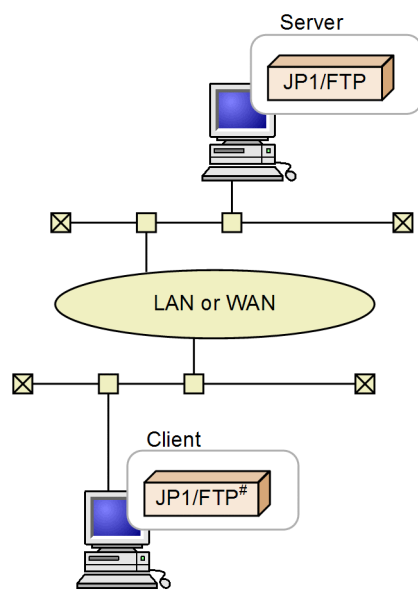
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

2.1.2 Basic system configuration

JP1/FTP must be installed at both the server and the client in order to transmit files. Files are transmitted from the client to the server.

When you have finished installing JP1/FTP, you assign the client and server functions to individual machines at the time that you start services. You can also start the services of both the client and the server on the same machine. For details about starting services, see [2.3 Starting and stopping services](#).

Figure 2–1: Example of a basic system configuration for using JP1/FTP to transmit files



#: Or the OS's default FTP

2.2 Installing and setting up

This section describes how to install and set up JP1/FTP.

2.2.1 Installing JP1/FTP

A distribution medium is provided for installing JP1/FTP, or you can use JP1/SD to perform remote installation.

To install JP1/FTP from the distribution medium:

1. Log in to the machine on which JP1/FTP is to be installed as an administrator.

2. Terminate the following programs:

- JP1/FTP programs (services, windows, etc.)
- Windows Event Viewer
- Windows services window

If installation is performed while the above programs are running, installation of JP1/FTP might fail.

For details on how to terminate services, see [2.3 Starting and stopping services](#).

3. Insert the distribution medium.

The installer starts. Perform installation by following the installer's instructions.

You will define the following information during installation:

- User information
Enter your user name and organization name.
- Installation target
Specify the directory in which JP1/FTP is to be installed.
The following default directories are used.

For the main product files:

OS-installation-drive: \Program Files (x86) \Hitachi \FTSFTP

For the API libraries for 64-bit:

OS-installation-drive: \Program Files \Hitachi \FTSFTP

Note:

Do not install the main product files under *OS-installation-drive*: \Program Files. Doing so may cause operational problems since the 64-bit module is located there.

2.2.2 Setting the language type

JP1/FTP can run in a Japanese or English environment.

To set the language type:

1. From the Windows **Start** menu, select **Programs, JP1_File Transmission Server_FTP**, and then **Language Selection**.

The dialog box for selecting the language to be used is displayed.

2. From the drop-down list box, select **Japanese** or **English**, and then click **OK**.

Note:

Terminate JP1/FTP programs (services, windows, etc.) before setting the language type.

2.2.3 Setting the port numbers

You must specify in the following file the port numbers to be used by JP1/FTP.

File used for setting the port numbers

```
OS-installation-directory\system32\drivers\etc\services
```

Settings

```
ftssdata  aaaaa-1/tcp  #Used by the server during data transmission
ftss      aaaaa/tcp   #Used by the server during reception
ftsc      bbbbbb/tcp   #Used by the client
ftsclog   ccccc/tcp   #Used by the client to obtain log information
ftsslog   ddddd/tcp   #Used by the server to obtain log information
ftsagent  eeeee/tcp   #Used by the Operations-Manager function (agent)
ftsagentdata fffff/tcp #Used by the Operations-Manager function (agent)
```

Legend:

aaaaa, *bbbbbb*, *cccccc*, *dddddd*, *eeeeee*, *ffffff*: Unique port numbers. Each must be different from any port numbers used by any other programs.

- *aaaaa-1* can be set automatically, but we recommend that you specify the number explicitly, as shown above.
- *ftsagentdata* can be omitted, in which case an unused port number assigned by the OS is used.
- If you specify a port number that is within the range of port numbers automatically assigned by the OS, it is assigned by the OS when JP1/FTP or another program is running. This may result in redundant assignment.
- If you plan to use the host only as a server or only as a client, specify one of the following sets of port numbers:
To use the host only as a server: *ftssdata*, *ftss*, *ftsslog*
To use the host only as a client: *ftsc*, *ftsclog*

Example of setting port numbers

```
ftssdata  20124/tcp  #Used by the server during data transmission
ftss      20125/tcp  #Used by the server during reception
ftsc      20126/tcp  #Used by the client
ftsclog   20127/tcp  #Used by the client to obtain log information
ftsslog   20128/tcp  #Used by the server to obtain log information
ftsagent  20252/tcp  #Used by the Operations-Manager function (agent)
ftsagentdata 20364/tcp #Used by the Operations-Manager function (agent)
```

A sample file is provided in *JP1/FTP-installation-directory\services.sample*.

Specification during transmission

To use JP1/FTP at the server, the client must specify the port number that was assigned to *ftss* during file transmission (in the above example, 20125).

When transmitting files from the OS's default FTP to JP1/FTP

If JP1/FTP is at the server and the OS's default FTP is used at the client to transmit files, the port specifications are as shown below.

Figure 2–2: Example of file transmission from the OS's default FTP to JP1/FTP

```
C:\>ftp
ftp> open hostname1 20125
      Name of remote host Port number specified for ftss
      :
      Omitted
      :
ftp> put localfile1 remotefile1
      File to be transmitted Name of remote file
      :
      Omitted
      :
```

2.2.4 Creating environments in which names can be resolved

JP1/FTP performs host name resolution of local and remote hosts (lookup), as well as IP address resolution (reverse lookup). Set up the OS environment so that the host name and IP address can be resolved uniquely.

In an environment where the host name and IP address cannot be resolved, file transmissions might result in an error, or performance might suffer.

2.2.5 Uninstalling JP1/FTP

To uninstall JP1/FTP:

1. Terminate the following programs:
 - JP1/FTP programs (services, windows, etc.)
 - Windows Event Viewer
 - Windows services window

If uninstallation is performed while the above programs are running, uninstallation of JP1/FTP might fail.
For details on how to terminate services, see [2.3 Starting and stopping services](#).

2. From the Windows **Start** menu, choose **Control Panel**, and then **Programs and Features**.
A dialog box for selecting the programs to be uninstalled is displayed.
3. While **Uninstall or change a program** is selected, select **JP1/File Transmission Server/FTP** from the list of currently installed programs, and then click the **Uninstall** button.
A dialog box for confirming the deletion request is displayed.
4. Click the **Yes** button.
The program is uninstalled.

2.3 Starting and stopping services

To use JP1/FTP, you must start its services.

2.3.1 Types of services

To use JP1/FTP, you must start the services for the desired functions. The types of services are as follows:

- **JP1/File Transmission Server/FTP Server**
Start this service to perform file transmission as the server.
- **JP1/File Transmission Server/FTP Client**
Start this service to perform file transmission as the client.
- **JP1/File Transmission Server/FTP Log**
Start this service to obtain log information.
- **JP1/File Transmission Server/FTP Agent**
Start this service to use the Operations-Manager function.

2.3.2 Starting services

Notes about starting services

- The JP1/FTP services are used with the account specified during logon. Permissions, such as file access permissions, depend on the account.
- Use the same account to start all the desired JP1/FTP services.
- The account of JP1/FTP services can be changed to only the user accounts below. If you change it to an account other than one of the accounts below, JP1/FTP processing might be affected or services might stop in the middle of processing.
 - If User Account Control (UAC) is enabled:
Administrator
 - If User Account Control (UAC) is disabled:
User who has Administrators permissions

Start the services to be used. You can also set services so that they will be started automatically when the system is started.

To start services:

1. From the Windows **Start** menu, choose **Control Panel**, **Administrative Tools**, and then **Services**.
The Services dialog box is displayed.
2. Right-click the name of a service to be started, and then from the displayed pop-up menu, choose **Start**.
The service starts. If an error is displayed when the service starts, check the event log that is displayed in Event Viewer. For details about the event log, see [8.2 Messages displayed in Event Viewer](#).

To start services automatically when the system starts:

In the Properties dialog box for the service to be started, on the **General** page, set **Startup type** to **Automatic**.
The service will start automatically whenever the system starts.

2.3.3 Stopping services

To stop services:

1. From the Windows **Start** menu, choose **Control Panel**, **Administrative Tools**, and then **Services**.
The Services dialog box is displayed.
2. Right-click the name of the service to be stopped, and then from the displayed pop-up menu, choose **Stop**.
The service stops. If any file is being transmitted, transmission processing is terminated forcibly, resulting in abnormal termination.

3

File Transmission by JP1/FTP

This chapter describes how to use JP1/FTP to transmit files.

3.1 Defining an environment for JP1/FTP

You must define an environment for JP1/FTP.

To define an environment, you choose **Environment Definition** at both the server and the client, and then use the Environment Definition dialog box.

How to display the Environment Definition dialog box

From the Windows **Start** menu, choose **Programs**, **JP1_File Transmission Server_FTP**, and then **Environment Definition**.

The following figure shows the Environment Definition dialog box.

Figure 3–1: Environment Definition dialog box

Environment Definition

No. of file transmissions to log: 2000 Items [Default]

Size of protocol trace file: 50 KBytes Size of Access log file: 0 MBytes

Size of module trace file: 50 KBytes Size of TCP/IP window: 32768 Bytes

When connecting to a host

No. of retries: 5 Time-limit waiting to send data: 60 Secs

Retry interval: 2 Secs Time-limit waiting to receive data: 60 Secs

Server

Size of sending buffer: 4096 Bytes

Size of receiving buffer: 4096 Bytes

Time-limit for idle connection: 900 Secs

Client

Size of sending buffer: 4096 Bytes

Size of receiving buffer: 4096 Bytes

Directory for log: C:\Program Files (x86)\HITACHI\FTSFTP\ [Browse...]

☐ Link with JP1/IM

☐ Output transmission result to NT event log ☐ Restrict access

[OK] [Cancel]

3.1.1 Defining an environment for JP1/FTP

The default values are set during installation. We recommend that you change these values only if necessary.

To use the Environment Definition dialog box to define an environment for JP1/FTP:

1. Change settings as desired in the Environment Definition dialog box, and then click **OK**.

After you have changed the settings, restart all services.

The following table lists and describes each item in the Environment Definition dialog box.

Table 3–1: Items in the Environment Definition dialog box

Item	Setting
No. of file transmissions to log ((0 to 100,000)) <<2,000>>	Specifies the number of log entries to retain. One file transmission is counted as one entry. When the number of files transmitted exceeds the number of entries being retained, the oldest information is overwritten. Because the size of one entry is 1,500 bytes, the required file size equals <i>number of retained entries</i> x 1,500 bytes.

Item	Setting
No. of file transmissions to log ((0 to 100,000)) <<2,000>>	Increasing the number of log entries to be retained: If you increase the number of log entries to be retained, it might take longer to display logs, depending on the CPU and hardware performance as well as on the amount of memory that is installed. If you want to retain log information over a long period of time, we recommend that you copy the log information file (<i>JP1/FTP-installation-directory\history</i>) and then store the copy.
Default	Clicking this button resets all environment definition settings to their default values.
Size of protocol trace file ((4 to 3,000 KB)) <<50 KB>>	Specifies the size of a file to be used to collect FTP protocol trace information. The protocol trace files enable you to check the operation of commands at the FTP level. When the amount of trace information for a file exceeds the specified file size, the oldest information is overwritten. You need 120 files, each of the specified size. You can use a text editor such as Notepad to view the trace files.
Size of module trace file ((4 to 3,000 KB)) <<50 KB>>	Specifies the size of a file to be used to collect module trace information. Module traces are collected as maintenance information. When the amount of trace information for a module trace file exceeds the specified file size, the oldest information is overwritten. You need 132 files, each of the specified size. The module trace files cannot be viewed.
Size of Access log file ((0 to 100 MB)) <<0 MB>>	Specifies the size of the file to be used to store access logs. When the amount of access log information exceeds the specified size, the old information is backed up and a new file is created. If there already is a backup file, that file is overwritten. You can use a text editor such as Notepad to view the access log file.
No. of retries (When connecting to a host) Retry interval (When connecting to a host)	Specifies the number of and interval for retries in the event connection for file transmission cannot be established (for a reason such as busy status). Retries are attempted whenever a connect system call results in one of the following error codes: When attempting to establish control connection: WSAECONNREFUSED (10061) When attempting to establish data connection: WSAEADDRINUSE (10048) <ul style="list-style-type: none"> • No. of retries (When connecting to a host) ((0 to 100,000)) <<5>> If you specify 0, no retries will be attempted. • Retry interval (When connecting to a host) ((0 to 86,400 seconds)) <<2 seconds>> If you specify 0, retries are attempted immediately (without any interval between retry attempts).
Size of TCP/IP window ((0 to 65,535 bytes)) <<32,768 bytes>>	Specifies the size of the socket buffer for sending and receiving (SO_SNDBUF and SO_RCVBUF). If the specified value is 0, the system's default value is used. This size is not the window size when transmissions are actually performed. Note that various factors affect transmission efficiency, such as the line speed, usage status, and CPU performance. Specify a value that is appropriate for the system being used.
Time-limit waiting to send data ((1 to 3,600 seconds)) <<60 seconds>>	Specifies the amount of time to wait for the sending buffer to become available after a package has been sent during data transmission. If the buffer is still not available when the specified amount of time elapses, the transmission terminates abnormally.
Time-limit waiting to receive data ((1 to 3,600 seconds)) <<60 seconds>>	Specifies the amount of time to wait for a packet to be received during data reception (a packet is transmitted by a remote target). If no data is received after the specified amount of time has elapsed, the transmission terminates abnormally.
Server/Client	<ul style="list-style-type: none"> • Size of sending buffer/Size of receiving buffer ((512 to 65,535 bytes)) <<4,096 bytes>> Specifies the size of the buffer (memory) for file transmission (sending) at both the server and the client. You might want to change this value if the amount of memory is limited or when you want to improve transmission efficiency. <i>Note that various factors affect transmission efficiency.</i>

Item	Setting
Server/Client	<p><i>such as the line speed, usage status, and CPU performance.</i> Specify a value that is appropriate for the system being used.</p> <p>The memory size that should be allocated for the transmission buffer equals <i>maximum number of concurrent transmissions</i> x <i>specified buffer size</i>. Buffers for sending and receiving are not allocated at the same time. Allocation occurs only during transmission.</p> <ul style="list-style-type: none"> • Time-limit for idle connection ((30 to 7,200 seconds)) <<900 seconds>> <p>If there is no request from the client for a specific period of time, the server releases the connection with the client. This item specifies the amount of time before the connection is to be released.</p>
Directory for log ((2 to 230-byte character string)) <<JP1/FTP installation directory>>	<p>Specifies the directory in which to create the log information files (<i>history</i>) and the trace information output directory (<i>trace</i>). The specified directory must be on the local drive.</p> <p>If you change this setting, the previous files and directory are retained. If you no longer need those files and directory, delete them.</p>
Link with JP1/IM	<p>Specifies that JP1 events are to be issued. If you select this item, JP1 events will be issued when the service status changes and when transmission ends. If you link to JP1/IM, you can monitor the status on JP1/IM. For details about linkage with JP1/IM, see 5.2 Linking to JP1/IM.</p> <p>The default is that this item is not selected.</p>
Output transmission result to NT event log	<p>Specifies whether to output file transmission results (normal or abnormal termination) and the start of file transmission to the event log.</p> <p>If you select this item, event IDs 33, 34, and from 24 to 27 are output. All other event IDs are always output to the event log, regardless of this setting.</p> <p>The default is that this item is not selected.</p>
Restrict access	<p>Specifies whether a user who logs in to the server is allowed to access only the home directory specified during user registration and the files under that home directory. Because the highest directory becomes the root directory of each drive, no access between drives is permitted. This setting applies to all users.</p> <p>When Restrict access is selected, the system's root directory becomes the root directory for the absolute path names of files and directories that are displayed and set. However, if you register the absolute path name format beforehand, you can change the root directory for absolute path names to the home directory. For details about how to change the root directory for absolute path names to the home directory, see 3.13 Function for using the access control function to change the root directory for absolute path names.</p> <p>The default is that this item is not selected.</p>

Note

If the value set in the Environment Definition dialog box in **No. of file transmissions to log**, **Size of protocol trace file**, and **Size of module trace file** is smaller than the current value for that item, the corresponding information files are deleted when the service is restarted. This means that the information existing before the restart will be deleted. The log information is backed up to the file *log-information-directory\FTSLOGSAVE*.

3.1.2 Using a definition file to define an environment for JP1/FTP

You can use a definition file to define some of the environment settings for JP1/FTP.

You create a definition file and specify the definition information as described below.

(1) Creating a definition file

Create a definition file with the following path name:

(2) Contents of the definition file

Specify the definition information in the format of a Windows initialization file (.ini), as shown below:

```
[ENV_INFO_VIEW]
GEN_USER=ON|OFF
[WELL_KNOWN_PORTS]
Enable=ON|OFF
[ANOTHER_ADDRESS]
Enable=ON|OFF
[MASK_CMD]
PORT=ON|OFF
```

The following table lists and describes the sections, keys, and values that can be specified.

Table 3–2: Contents of the definition file (ftsenv.ini)

Section	Key	Value	Description
[ENV_INFO_VIEW]	GEN_USER	ON OFF <<OFF>>	Specifies whether a non-Administrator user can reference the definition information. ^{#1} <ul style="list-style-type: none"> ON: Make the definition information referenceable. OFF: Do not display the definition information.
[WELL_KNOWN_PORTS]	Enable	ON OFF <<OFF>>	Specifies whether to permit connection when a well-known port (0 to 1023) is specified in the PORT command at the FTP server. ^{#2} <ul style="list-style-type: none"> ON: Permit connection. OFF: Reject connection.
[ANOTHER_ADDRESS]	Enable	ON OFF <<OFF>>	Specifies whether to permit connection when the IP address specified in the PORT command at the FTP server does not belong to the client that established the control connection. ^{#2} <ul style="list-style-type: none"> ON: Permit connection. OFF: Reject connection.
[MASK_CMD]	PORT	ON OFF <<OFF>>	Specifies whether to suppress reception of the PORT command at the FTP server. ^{#2, #3} <ul style="list-style-type: none"> ON: Suppress. OFF: Do not suppress.
	EPRT	ON OFF <<OFF>>	Specifies whether to suppress reception of the EPRT command at the FTP server. ^{#2, #3} <ul style="list-style-type: none"> ON: Suppress. OFF: Do not suppress.
[C_WELL_KNOWN_PORTS]	Enable	ON OFF <<OFF>>	At the FTP client, specifies whether to permit a connection when a well-known port (0 to 1023) is specified in the port number received from the FTP server after the PASV command is issued. ^{#4} <ul style="list-style-type: none"> ON: Permit connection.

Section	Key	Value	Description
[C_WELL_KNOWN_PORTS]	Enable	ON OFF <<OFF>>	<ul style="list-style-type: none"> • OFF: Reject connection.
[C_ANOTHER_ADDRESS]	Enable	ON OFF <<OFF>>	<p>Specifies whether to permit a connection when the IP address received from the FTP server after the PASV command is issued at the FTP client does not belong to the server that established the control connection.^{#4}</p> <ul style="list-style-type: none"> • ON: Permit connection. • OFF: Reject connection.

#1

In version 8 or earlier, a non-Administrator user cannot reference some of the definition information. If ON is specified, all the definition information becomes referenceable, including the information that was not referenceable in version 8 or earlier.

When the Operations-Manager Console is used to reference definition information, the user must be an administrator.

#2

This registration information takes effect the next time the JP1/File Transmission Server/FTP Server service starts.

#3

If ON is specified and the FTP server receives the corresponding command, the FTP server sends to the FTP client the response message 500 '*command-name*' : command not understood.

Note that Help for this command is not disabled.

#4

This registration information takes effect the next time the JP1/File Transmission Server/FTP Client service starts.

3.2 Registering the users who can log in to a JP1/FTP server

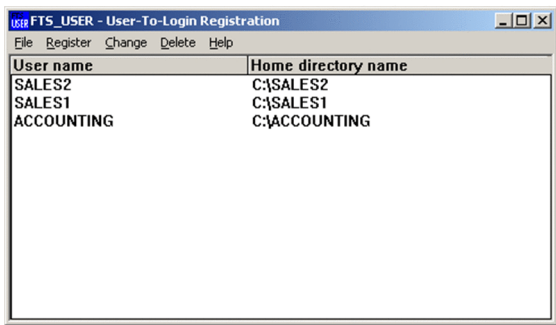
You must register all login users who will be logging in to the server during file transmission. The server will reject reception requests from any other users. To register login users, you choose **User-To-Login Registration** at the server and then register the users in the User-To-Login Registration window.

How to display the User-To-Login Registration window

From the Windows **Start** menu, choose **Programs, JP1_File Transmission Server_FTP**, and then **User-To-Login Registration**.

The following figure shows the User-To-Login Registration window.

Figure 3–2: User-To-Login Registration window



Note

The login users that you register here are not the same as the Windows login users.

3.2.1 Registering the login users

To register the login users:

1. In the User-To-Login Registration window, choose **Register**.
The Register User To Login dialog box is displayed.

Figure 3–3: Register User To Login dialog box



2. Specify each item and then click **Register**.
You can register multiple users one after another until you click **Close**.
3. After you have finished registering users, click **Close**.

The following table lists and describes each setting item in the Register User To Login dialog box.

Table 3–3: Setting items in the Register User To Login dialog box

Item	Description
User name ((1 to 50-byte character string))	Specifies the name of a user from whom the server can receive data. If Japanese characters (double-byte characters) are specified for this item, the FTP client at the transmission target might refuse access or the text might become garbled in some cases. This item is mandatory. None of the following characters can be used: \\, ", /, :, <, >, , *, ? (all single-byte characters) A user name cannot be a string that begins or ends with a single-byte space.
Password ((0 to 50-byte character string))	Specifies the password to be used by this user to log in to the server. If Japanese characters (double-byte characters) are specified for this item, the FTP client at the transmission target might refuse access or the text might become garbled in some cases. If entry of a password will not be required, enter nothing in this item, in which case password checking will not be performed during file reception.
Re-enter password	For confirmation purposes, this field is used to re-enter the password that was specified in Password . If you have not specified a password, do not enter anything in this item.
Home directory ((2 to 259-byte character string))	Specifies the directory to be used by this user to receive data during file transmission. If a file to be transmitted is specified by its relative path, the home directory specified here is assumed. You can also click Browse to find a directory in the system to use. This item is mandatory.

3.2.2 Changing login user information

You can change a user's password and home directory in login user information that has been registered.

To change login user information:

1. From the list in the User-To-Login Registration window, select a user and then choose **Change**.
The Change User Information dialog box is displayed.

Figure 3–4: Change User Information dialog box

2. Select an item you wish to change, and then enter the new information.
You can change a user's password and/or home directory.
3. Click **Change**.

3.2.3 Deleting login user information

You can delete a user's registered login user information from the User-To-Login Registration window. When you delete a user's login information, any auto-start programs that have been set for that user are also deleted.

To delete login user information:

1. From the list in the User-To-Login Registration window, select a user to delete.
To delete multiple users at the same time, select the users while holding down the **Shift** or **Ctrl** key.
2. Choose **Delete**.
A confirmation message is displayed.
3. Click **Yes**.

3.3 Registering auto-start programs

You can register a program to start at the server after file transmission is finished.

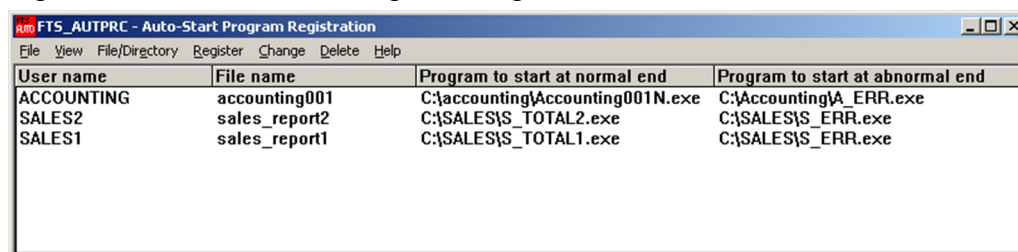
To register auto-start programs, you start **Auto-Start Program Registration** at the server and then register auto-start programs in the Auto-Start Program Registration window.

How to display the Auto-Start Program Registration window

From the Windows **Start** menu, choose **Programs**, **JP1_File Transmission Server_FTP**, and then **Auto-Start Program Registration**.

The Auto-Start Program Registration window is displayed. The following figure shows the Auto-Start Program Registration window.

Figure 3–5: Auto-Start Program Registration window



3.3.1 Registering auto-start programs

The following features characterize auto-start programs:

- You can register different programs to start in the event of normal termination and abnormal termination of transmission.
- The time at which a specified program starts depends on how the transmission file is specified:
 - file-name* is specified
The program starts when the specified file is transmitted.
 - directory-name* is specified
The program starts when a file is transmitted to the specified directory.
- An auto-start program is executed when transmission is completed for the registered user. To register an auto-start program for all users, specify `.default` in **User name**.
- You can either specify from scratch an auto-start program to start, or you can edit existing registration information to specify a different auto-start program.

To register auto-start programs:

1. In the Auto-Start Program Registration window, from the **Register** menu, choose **For File Trigger** or **For Directory Trigger**. Alternatively, select existing registration information, and then from the **Register** menu, choose **For File Trigger** or **For Directory Trigger**.

The Register Auto-Start Program dialog box appears.

Figure 3–6: Register Auto-Start Program dialog box (for files)

Register Auto-Start Program

User name: SALES1

File name: sales_report Browse...

Program to start when transmission ends normally: C:\SALES1S_TOTAL.exe Browse...

Program to start when transmission ends abnormally: C:\SALES1S_ERR.exe Browse...

Register Close

- 2. Specify the items and then click **Register**.
You can make entries for multiple auto-start programs one after another until you click **Close**.
- 3. After registering the programs, click **Close**.

The following table lists and describes each item in the Register Auto-Start Program dialog box.

Table 3–4: Items in the Register Auto-Start Program dialog box

Item	Setting
User name ((user displayed in the list))	<p>Specifies a user name for registering an auto-start program. This item is mandatory.</p> <p>The following users displayed in the drop-down list can register auto-start programs.</p> <ul style="list-style-type: none">• Users who have been registered as JP1/FTP login users• .default (default users): All users who have been registered as login users <p>When there is no registration information that corresponds to an individual user, JP1/FTP references the default user registration information. If such an item is found, JP1/FTP starts those programs automatically.</p> <p>When a user name is already set in User name:</p> <p>If a user has been specified in Info. For Specific User in the View menu, that user name is displayed here. From the View menu, choose Info. For All Users.</p>
File name/Directory name ((1 to 259-byte character string))	<p>Specifies the name of the file or directory that is to be subject to automatic start. This item is mandatory.</p> <p>If you specify a file, specify its full path or only the file name. If you specify a directory, specify its full path. For the directory delimiter, use \.</p>
Program to start when transmission ends normally Program to start when transmission ends abnormally ((2 to 259-byte character string))	<p>Specifies the program to start when transmission terminates normally and/or when transmission terminates abnormally.</p> <p>For the name of a program to start, specify its full path. When the program starts, transmission information can be passed as arguments. For details, see (1) <i>Parameter keywords</i>. Note that if the length of the expanded parameter keywords exceeds 2,047 bytes, start processing of the specified auto-start program will fail.</p> <p>When a program name contains a space:</p> <p>If the specified program name contains a space, enclose the entire program name in double-quotation marks (").</p> <p>Example: When specifying c:\aaaΔbbb\cccΔddd.exe as the name of an auto-start program:</p> <p>"c:\aaaΔbbb\cccΔddd.exe:" (Δ: Single-byte space)</p> <p>Note that in the case of a batch file, if you enclose both the program name and the arguments in double-quotation marks, the arguments will not be passed correctly.</p>

Item	Setting
Program to start when transmission ends normally Program to start when transmission ends abnormally ((2 to 259-byte character string))	About JP1EVENT specification Events cannot be issued by specifying JP1EVENT for program names supported in older versions. To issue an event, use the JP1/Base <code>jvsend.exe</code> command and specify a full path.

About the programs to start

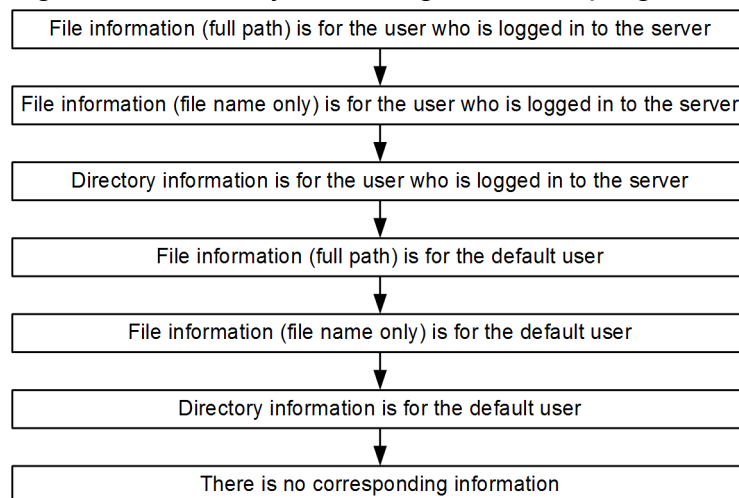
Because the specified programs are started from the JP1/File Transmission Server/FTP Server service, we recommend that you note the following:

- Make sure that the account (user) used to start the JP1/File Transmission Server/FTP Server service is authorized to execute the specified programs.
- Because automatic start of programs is executed in a service session that is independent of the user's logon session, some of the information might not be readable (such as the registry settings specified during the user's logon session).
- An auto-start program cannot have a graphical user interface. If you specify that a program with a graphical user interface is to start automatically, JP1/FTP processing might be affected adversely and the service might stop during operation.

Priority of program start

If multiple auto-start programs have been registered, the start condition (file name or directory name) might be applicable to more than one of the programs. In such a case, JP1/FTP searches the programs based on the priority order described below and starts only the first program that satisfies a priority condition. The following figure shows the priorities.

Figure 3–7: Priority of starting auto-start programs



How to start programs when multiple files are transmitted

If a wildcard is used to transmit multiple files, an auto-start program is started as many times as there are file transmissions. Information is inherited to the auto-start program separately for each transmission. The transmission information cannot be inherited to all instances of the auto-start program at once.

(1) Parameter keywords

You can pass all the transmission-end information items to the user program by specifying a keyword in the auto-start program. You can also use keywords to pass specific transmission-end information items. The following table lists and describes the keywords.

Table 3–5: List of parameter keywords

Parameter keyword	Information that is output	Client	Server
ALL	All the following items	Y	Y
TRNO	Transmission number	Y	Y
TCNO	Connection number	Y	Y
CARD	Card name	Y	--
HOST	Connection-target host name or IP address	Y	--
	Connecting client's IP address	--	Y
PORT	Connection-target host's port number	Y	--
USER	Login user name	Y	Y
TRTP	Transmission mode: 1: ASCII 2: Binary	Y	Y
TRCM	Transmission command: 1: Send 2: Receive 3: Append	Y	Y
COMP	Compression mode: 1: Stream 2: Compress	Y	Y
LCFN	Local file name	Y	Y
RMFN	Remote file name	Y	--
STTM	Transmission start time (return value of <code>time()</code>)	Y	Y
SPTM	Transmission end time (return value of <code>time()</code>)	Y	Y
TRSZ	Transmission data size (bytes)	Y	Y
CMNT	Comment	Y	--
TRST	Transmission end status: 1: Success 2: Failure	Y	Y
ERKD	Error type: 1: System call error 2: Logical error 3: Protocol error 5: SSL communication error	Y	Y
SYCN	System call name	Y	Y
SYKD	System call type: 1: Win32 API 2: C runtime 3: Winsock API	Y	Y
ERNO	Error number	Y	Y
PLMG	Protocol message	Y	--

Parameter keyword	Information that is output	Client	Server
SSLE	SSL communication error number	Y	Y

Legend:

Y: Enabled

--: Disabled

About keyword specification

- If any keyword other than the ones shown in the table above or an invalid keyword is specified, the specified keyword is passed to the user program.
- If arguments to be passed to an auto-start program contain any spaces, you must enclose the keywords in double-quotation marks.

Example: "ALL"

When keywords are enclosed in double-quotation marks, the arguments are passed differently between .exe and .bat files, as shown below:

Example: A.exe "PLMG" aargv[1]=aaa bbb
Example: A.bat "PLMG" a%1="aaa bbb"

Example of argument specification

The following shows an example of specifying arguments.

All transmission-end information:

C:\USERS\accounting\PROC ALL

Selected transmission-end information:

C:\USERS\accounting\PROC1 TRNO USER TRCM STTM SPTM
C:\USERS\accounting\PROC2 "PLMG"

Command line during execution

Example 1: Specifying keywords (without double-quotation marks):

Specification:

C:\USERS\accounting\PROC1 TRNO USER TRCM STTM SPTM

Execution command line:

C:\USERS\accounting\PROC1 12 accounting 1 12:45:35 12:45:45
(Transmission connection number: 12, login user name: accounting,
transmission command: send(1), transmission start time: 12:45:35,
transmission end time: 12:45:45)

Example 2: Specifying keywords (with double-quotation marks):

Specification:

C:\USERS\WAKA\PROC2 "PLMG"

Execution command line:

C:\USERS\WAKA\PROC2 "550 D:\temp\test.dat:The system cannot find the
path specified."

```
(Protocol message: 550 D:\temp\test.dat:The system cannot find the path specified.)
```

The user can obtain the entire command line character string by using the `GetCommandLine` function within the termination procedure. If the user program is a C runtime process, you can use the mechanism of `argc` and `argv`.

3.3.2 Changing the auto-start programs

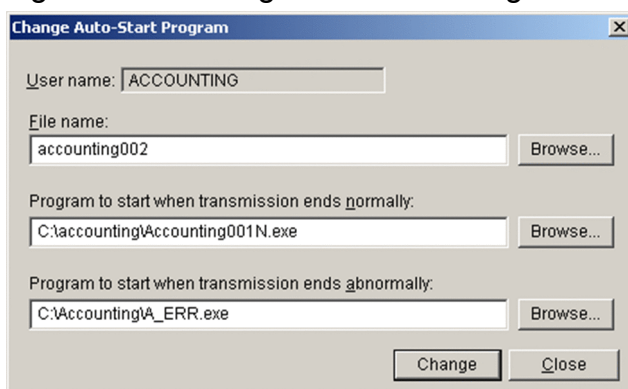
You can use the Auto-Start Program Registration window to change registered auto-start programs.

To change an auto-start program:

1. From the Auto-Start Program Registration window, select the information that you wish to change, and then click **Change**.

The Change Auto-Start Program dialog box appears.

Figure 3–8: Change Auto-Start Program dialog box



2. Enter the desired information in the applicable items.
3. Click **Change**.

3.3.3 Deleting auto-start programs

You can delete auto-start programs from the Auto-Start Program Registration window.

To delete auto-start programs:

1. From the Auto-Start Program Registration window, select the information that you wish to delete.
To select multiple items, select them while holding down the **Shift** or **Ctrl** key.
2. Choose **Delete**.
A configuration message is displayed.
3. Click **Yes**.

3.3.4 Changing the information displayed in the Auto-Start Program Registration window

You can change how information is displayed in the Auto-Start Program Registration window, as follows:

- Display by user who is registered for the auto-start programs (all users, specified user, or default user)
- Display by program start trigger target (file or directory)

(1) Displaying the auto-start programs by user

To display the auto-start programs by user:

1. From the **View** menu, choose **Info. For All Users**, **Info. For Specific User**, or **Info. For .default User**.

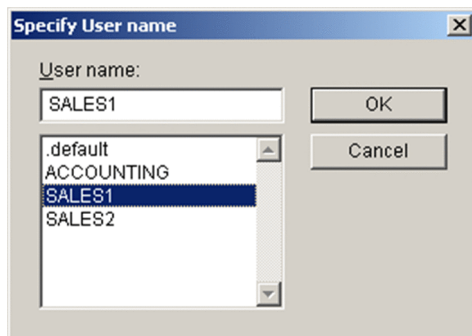
- **Info. For All Users**

Displays all the information that has been registered.

- **Info. For Specific User**

Specify a desired user in the Specify User name dialog box. The following figure shows the Specify User name dialog box.

Figure 3–9: Specify User name dialog box



- **Info. For .default User**

Displays only the information registered for the default user.

(2) Displaying the auto-start programs by program start trigger target (file or directory)

To display the auto-start programs by program start trigger target:

1. Select **File/Directory**, and then select either **Trigger Is File** or **Trigger Is Directory**.

- **Trigger Is File**

Displays only the information associated with files.

- **Trigger Is Directory**

Displays only the information associated with directories.

3.4 Registering transmission information

You register information about a transmission (such as the remote host name, remote user name, and transmission file) onto a *transmission card*. You can also specify a program to be started by the client when transmission finishes.

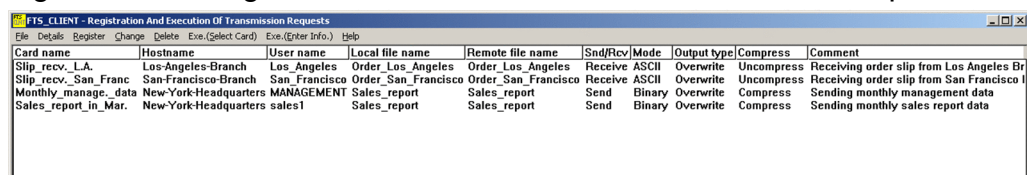
To register transmission information, you use **Transmission Regist. & Exe.** at the client to display the Registration And Execution Of Transmission Requests window. Alternatively, you can use a command.

How to display the Registration And Execution Of Transmission Requests window

From the Windows **Start** menu, choose **Programs**, **JP1_File Transmission Server_FTP**, and then **Registration And Execution Of Transmission Requests**.

The Registration And Execution Of Transmission Requests window is displayed. The following figure shows the Registration And Execution Of Transmission Requests window.

Figure 3–10: Registration And Execution Of Transmission Requests window



Card name	Hostname	User name	Local file name	Remote file name	Snd/Rcv	Mode	Output type	Compress	Comment
Slip_recv_LA	Los-Angeles-Branch	Los_Angeles	Order_Los_Angeles	Order_Los_Angeles	Receive	ASCII	Overwrite	Uncompress	Receiving order slip from Los Angeles Br
Slip_recv_San_Franc	San-Francisco-Branch	San_Francisco	Order_San_Francisco	Order_San_Francisco	Receive	ASCII	Overwrite	Uncompress	Receiving order slip from San Francisco B
Monthly_manage_data	New-York-Headquarters	MANAGEMENT	Sales_report	Sales_report	Send	Binary	Overwrite	Compress	Sending monthly management data
Sales_report_in_Mar	New-York-Headquarters	sales1	Sales_report	Sales_report	Send	Binary	Overwrite	Compress	Sending monthly sales report data

3.4.1 Registering transmission information onto a transmission card

You register transmission information onto a transmission card. This subsection describes two methods, one that uses the Registration And Execution Of Transmission Requests window and one that uses the command.

Alternatively, you can edit an existing transmission card and register it as a new transmission card.

(1) Using the Registration And Execution Of Transmission Requests window

To register transmission information onto a transmission card:

1. In the Registration And Execution Of Transmission Requests window, choose **Register**, or select an existing transmission card, and then choose **Register**.

The Register Transmission Information dialog box appears.

Figure 3–11: Register Transmission Information dialog box

- 2. Specify the items and then click **Register**.
You can register multiple sets of transmission information until you click **Close**.
- 3. After you have finished with the registration, click **Close**.

The following table lists and describes each item in the Transmission Information dialog box.

Table 3–6: Items in the Register Transmission Information dialog box

Item	Setting
Transmission card name ((1 to 20-byte character string))	Specifies a name for the transmission information. If you link to JP1/AJS3, make sure that the specified transmission card name does not contain any spaces. This item is mandatory.
Remote host name ((1 to 256-byte character string))	Specifies the name or IP address of the remote host. When you specify an IP address, you can specify an IPv4 or IPv6 address. This item is mandatory.
Port number ((1 to 65,535)) <<21>>	Specifies the port number of the remote host. If this item is omitted, 21 is assumed. <ul style="list-style-type: none">For transmitting to the JP1/FTP server: Specify the port number that was specified in <code>ftss</code> in the port number settings.For transmitting to the OS's default FTP server: Specify the default value (21).
Remote user name ((1 to 50-byte character string))	Specifies the name of the login user at the transmission target. This item is mandatory.
Password ((0 to 50-byte character string))	Specifies the password registered for the login user. If no password was specified during the registration process, leave this item blank.
Send/receive type	Specifies the transmission type: <ul style="list-style-type: none">SendReceive
Transmission mode	Specifies the transmission mode according to the file to be transmitted. <ul style="list-style-type: none">ASCII: In this transmission mode, the receiving end adjusts linefeed codes according to the local system. Use this mode to transmit text files.

Item	Setting
Transmission mode	<ul style="list-style-type: none"> • BINARY: This mode achieves transparent transmission without having to be aware of the data contents. Use this mode to transmit data files and executable files.
Output type	<p>Specifies how to output files after transmission:</p> <ul style="list-style-type: none"> • Append: If a file with the same name already exists, the transmitted data will be appended to that file. If there is no file with the same name, a new file will be created. This option is not available when the send/receive type is Receive. • Overwrite: If a file with the same name already exists, that file will be overwritten (in which case the file's existing contents will be destroyed). If there is no file with the same name, a new file will be created.
Compression mode	<p>Specifies whether to compress the transmitted files.</p> <p>About the compression specification:</p> <ul style="list-style-type: none"> • If the remote FTP host does not support the compression mode, data is not compressed during transmission even if you specify compression. • The run-length compression method defined in RFC 959 (FILE TRANSFER PROTOCOL) is used as the compression method.
Size check	<p>Specifies whether to check the size of a transmitted file at the sending and receiving ends for errors after file transmission. If a file's transmission data size does not match between the sending and receiving ends, a transmission error results.</p> <p>For the size check to be enabled, the remote FTP server must be JP1/FTP (version 06-00 or later) or uCosminexus Service Platform (version 08-53 or later).</p>
Single/Multiple-file transmission	<p>Specifies whether to transmit is to be of a single file or of multiple files.</p> <ul style="list-style-type: none"> • Auto: If the remote file name contains * or ?, JP1/FTP is to perform multiple-file transmission. If the file name does not contain * or ?, JP1/FTP is to perform single-file transmission. • Multiple: JP1/FTP is to perform multiple-file transmission exactly as dictated by the wildcard. • Single: JP1/FTP is to perform single-file transmission. If a wildcard is specified, JP1/FTP treats it as a character and transmits a single file.
Local file name	<p>Specification depends on the transmission type, as described below. This item is mandatory.</p> <ul style="list-style-type: none"> • Send transmission type ((1 to 259-byte character string)) <p>Specifies the name of the file to be sent from the local system. You can use wildcard characters to specify multiple files. If you use a wildcard character, the length of the expanded path name must not exceed 259 bytes.</p> <p>To specify multiple files: You can use the following wildcard characters to specify multiple files:</p> <p>*: Any number of any characters, including no characters</p> <p>?: Any single character</p> <p>If you send multiple files, specify a directory for the remote files. Files with the same names as local files will be created in the specified directory.</p> • Receive transmission type ((1 to 259-byte character string)) <p>Specifies the name of the file to be output at the local system after the file is received. If you have specified a wildcard in the remote file name, specify a directory name (other than the root directory). Note that the length of the expanded path name must not exceed 259 bytes.</p> <p>When specifying a relative path:</p> <p>If the specified directory and file exist under <i>JP1/FTP-installation-directory\temp</i>, the file is transmitted. If there is no such directory or file, the transmission terminates abnormally.</p> <p>Local file name:</p> <p>No shortcut can be specified for local file names.</p>
Remote file name	<p>Specification depends on the transmission type, as described below. This item is mandatory.</p> <ul style="list-style-type: none"> • Send transmission type ((1 to 259-byte character string)) <p>Specifies the name of the output file at the remote system. If you have used a wildcard character in the local file name, specify a directory name. Note that the length of the expanded path name must not exceed 259 bytes.</p> • Receive transmission type ((1 to 259-byte character string))

Item	Setting
Remote file name	<p>Specifies the name of the input file at the remote system.</p> <p>You can use wildcard characters (* and ?) to specify multiple files. Note that the length of the expanded path name must not exceed 259 bytes.</p> <p>If you receive multiple files, specify a directory for the local files. Files with the same names as the remote files will be created in the specified directory.</p> <p>How wildcard characters are interpreted:</p> <p>A wildcard is specified in the NLST command and then sent to the remote FTP server. The file that is transmitted is determined by the response from the FTP server. Therefore, interpretation of the wildcard depends on the remote FTP server.</p> <p>JP1/FTP supports only * and ? as wildcard characters. Wildcard characters cannot be used in directory names. If a directory name contains a wildcard, set Single/Multiple-file transmission to Single.</p> <p>When specifying a relative path:</p> <p>For both sending and receiving, the specified path is relative to the current directory.</p> <p>About the specification of remote files:</p> <ul style="list-style-type: none"> • Browse displays files as viewed from the local system. For the remote file name, specify a file name that is viewed from the remote system. • If Japanese characters (double-byte characters) are specified for the remote file name, the remote FTP server might refuse access or the text might become garbled in some cases.
Program to start at normal end ((0 to 259-byte character string))	<p>Specifies the full path name of a program to start automatically at the client when transmission terminates normally. You can also specify arguments to pass as transmission information to the program when the program starts. For details about the arguments, see 3.3.1(1) Parameter keywords.</p> <p>Note that if the length of the converted parameter keywords exceeds 2,047 bytes, the specified auto-start program will not start.</p>
Program to start at abnormal end ((0 to 259-byte character string))	<p>Specifies the full path name of a program to start automatically at the client when transmission terminates abnormally. You can also specify arguments to pass as transmission information to the program when the program starts. For details about the arguments, see 3.3.1(1) Parameter keywords.</p> <p>Note that if the length of the converted parameter keywords exceeds 2,047 bytes, the specified auto-start program will not start.</p>
FTP command ((0 to 300-byte character string))	<p>Specifies an FTP command to be executed prior to transmission after connection is established with the server. To specify multiple commands, separate them with the semicolon (;).</p> <p>Example: CWD C:\users\user1;SITE xxx</p> <p>You can specify only commands that do not establish a data connection. Whether the specified commands can be executed at the FTP server depends on the FTP server.</p> <p>When the FTP server is JP1/FTP:</p> <ul style="list-style-type: none"> • Major commands that can be specified: CDUP, CWD, DELE, HELP, MDTM, MKD, NOOP, PWD, RMD, SITE, SIZE, STAT, SYST, XCUP, XCWD, XMKD, XPWD, XRMD • Commands that can reference the result by means of a protocol trace: HELP, MDTM, SIZE, STAT, SYST <p>About the specification of FTP commands:</p> <ul style="list-style-type: none"> • Some commands require consecutive command transmission. Before using commands, check the FTP specifications. • If you use a command accompanied by an argument, note the following: If Japanese characters (double-byte characters) are specified for the argument, the remote FTP server might refuse access or the text might become garbled in some cases.
Comment ((0 to 80-byte character string))	<p>Specifies any comment. Because the comment is displayed in the log information, this option is useful for setting a memo about the transmission. A comment is not passed to the transmission target.</p>
FTPS enable	<p>Specifies whether to use FTPS.</p>

Item	Setting
FTPS enable	When FTPS is not used, the usual FTP is used.
Server certificate expiration check	Specifies whether to check the expiration date of the server certificate used with FTPS. If you enable the checking, the transmission of files with the expired server certificate ends in failure.
Path name of the CA certificate ((0 to 259-byte character string))	Specifies a full path to the file containing the CA certificate used with FTPS.
Path name of the CRL ((0 to 259-byte character string))	Specifies a full path to the file containing the CRL used with FTPS.

About the programs that are specified as auto-start programs

Because auto-start programs are started from the JP1/File Transmission Server/FTP Client service, we recommend that you note the following:

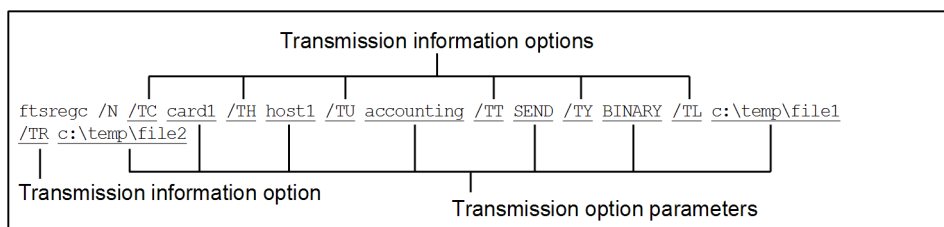
- Make sure that the account (user) used to start the JP1/File Transmission Server/FTP Server service is authorized to execute the specified programs.
- Because automatic start of programs is executed in a service session that is independent of the user's logon session, some of the information might not be readable (such as the registry settings specified during the user's logon session).
- An auto-start program cannot have a graphical user interface. If you specify that a program with a graphical user interface is to start automatically, JP1/FTP processing might be affected adversely and the service might stop during operation.

How to start programs when multiple files are transmitted

If a wildcard is used to transmit multiple files, an auto-start program is started as many times as there are file transmissions. Information is inherited to the auto-start program separately for each transmission. The transmission information cannot be inherited to all instances of the auto-start program at once.

(2) Using the ftsregc command

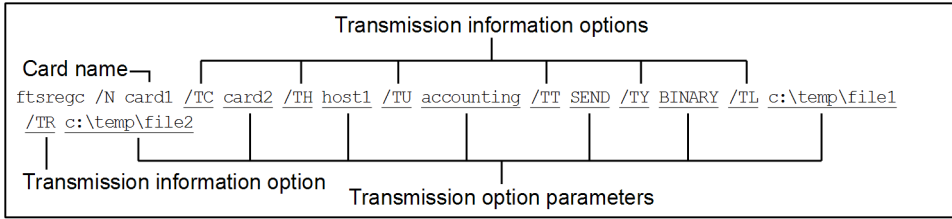
The following figure shows an example of using a command to register new transmission information:



This example registers the following information:

- `/TC`: The transmission card name is `card1`.
- `/TH`: The connection-target host name is `host1`.
- `/TU`: The login user name is `accounting`.
- `/TT`: The send/receive type is `SEND`.
- `/TY`: The transmission mode is `BINARY`.
- `/TL`: The local file name is `c:\temp\file1`.
- `/TR`: The remote file name is `c:\temp\file2`.

The following figure shows an example of a command that registers transmission information using an existing transmission card:



This example registers the following information:

- The name of the existing transmission card that is being used is `card1`.
- `/TC`: The name specified for the new transmission card is `card2`.
- `/TH`: The connection-target host name is `host1`.
- `/TU`: The login user name is `accounting`.
- `/TT`: The send/receive type is `SEND`.
- `/TY`: The transmission mode is `BINARY`.
- `/TL`: The local file name is `c:\temp\file1`.
- `/TR`: The remote file name is `c:\temp\file2`.

For details about the `ftsregc` command, see [ftsregc - registers, changes, deletes, and displays transmission information](#) in 6. Commands.

3.4.2 Changing the information registered on a transmission card

You can change the information registered on a transmission card. This subsection describes two methods, one that uses the Registration And Execution Of Transmission Requests window and one that uses a command.

(1) Using the Registration And Execution Of Transmission Requests window

To change the information registered on a transmission card:

1. In the Registration And Execution Of Transmission Requests window, select the transmission card to be edited, and then choose **Change**.
The Change Transmission Information dialog box appears.

Figure 3–12: Change Transmission Information dialog box

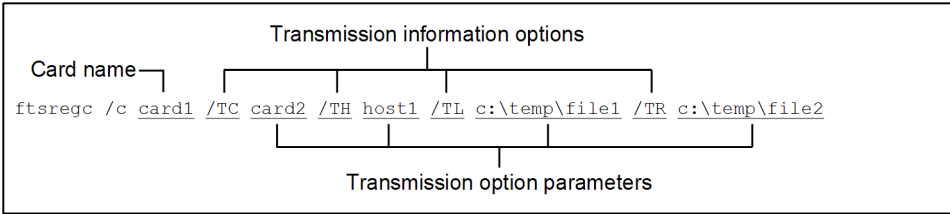
The dialog box is titled "Change Transmission Information". It contains the following fields and controls:

- Transmission card name:
- Remote host name:
- Remote user name:
- Port number:
- Password:
- Send/receive type:
- Transmission mode:
- Output type:
- Compression mode:
- Size Check: ☒
- Single/Multiple-file transmission:
- Local file name:
- Remote file name:
- Program to start at normal end:
- Program to start at abnormal end:
- FTP command:
- Comment:
- FTPS enable: ☐
- Server certificate expiration check: ☐
- Path name of the CA certificate:
- Path name of the CRL:
-

- 2. Enter new information in the applicable items.
- 3. Click **Change**.

(2) Using the `ftsregc` command

The following example changes information on a transmission card:



This example changes the following transmission information on `card1`:

- `/TC`: The card name is `card2`.
- `/TH`: The connection-target host name is `host1`.
- `/TL`: The local file name is `c:\temp\file1`.
- `/TR`: The remote file name is `c:\temp\file2`.

For details about the `ftsregc` command, see *ftsregc - registers, changes, deletes, and displays transmission information* in 6. Commands.

3.4.3 Deleting transmission cards

You can delete registered transmission cards from the Registration And Execution Of Transmission Requests window. This subsection describes two methods, one that uses the Registration And Execution Of Transmission Requests window and one that uses a command.

(1) Using the Registration And Execution Of Transmission Requests window

To delete transmission cards:

1. In the Registration And Execution Of Transmission Requests window, select a transmission card to be deleted.
To select multiple transmission cards, select them while holding down the **Shift** or **Ctrl** key.
2. Choose **Delete**.
A configuration message is displayed.
3. Click **Yes**.

(2) Using the `ftsregc` command

The following example deletes information on a transmission card:

```
ftsregc /D card1  
Card name
```

For details about the `ftsregc` command, see *ftsregc - registers, changes, deletes, and displays transmission information* in 6. *Commands*.

3.4.4 Checking the contents of a transmission card

You can check the contents of a transmission card before you start transmission. This subsection describes two methods, one that uses the Registration And Execution Of Transmission Requests window and one that uses a command.

(1) Using the Registration And Execution Of Transmission Requests window

To check the contents of a transmission card:

1. In the Registration And Execution Of Transmission Requests window, select a transmission card whose contents are to be displayed, and then choose **Details**.
The Transmission Card Details dialog box appears.
2. After checking the contents, click **OK**.

(2) Using the `ftsregc` command

The following example displays the contents of a transmission card:

```
ftsregc /L card1  
Transmission card name
```

For details about the `ftsregc` command, see *ftsregc - registers, changes, deletes, and displays transmission information* in 6. *Commands*.

3.5 Transmitting files

There are two ways to transmit files:


- Select Card method of file transmission
This method specifies a registered transmission card in the Registration And Execution Of Transmission Requests window and then executes transmission.
- Enter Information method of file transmission
For this method, you start **Transmission Regist. & Exe.** at the client to open the Registration And Execution Of Transmission Requests window. Alternatively, you can use a command.

How to display the Registration And Execution Of Transmission Requests window

From the Windows **Start** menu, choose **Programs, JP1_File Transmission Server_FTP**, and then choose **Registration And Execution Of Transmission Requests**.

The Registration And Execution Of Transmission Requests window appears. The following figure shows the Registration And Execution Of Transmission Requests window.

Figure 3–13: Registration And Execution Of Transmission Requests window



Card name	Hostname	User name	Local file name	Remote file name	Snd/Rcv	Mode	Output type	Compress	Comment
Slip_rcv_LA	Los-Angeles-Branch	Los_Angeles	Order_Los_Angeles	Order_Los_Angeles	Receive	ASCII	Overwrite	Uncompress	Receiving order slip from Los Angeles Br
Slip_rcv_San_Franc	San-Francisco-Branch	San_Francisco	Order_San_Francisco	Order_San_Francisco	Receive	ASCII	Overwrite	Uncompress	Receiving order slip from San Francisco I
Monthly_manage_data	New-York-Headquarters	MANAGEMENT	Sales_report	Sales_report	Send	Binary	Overwrite	Compress	Sending monthly management data
Sales_report_in_Mar	New-York-Headquarters	sales I	Sales_report	Sales_report	Send	Binary	Overwrite	Compress	Sending monthly sales report data

3.5.1 Executing transmission by specifying a transmission card (Select Card method of file transmission)

This method specifies a transmission card. You can specify multiple transmission cards.

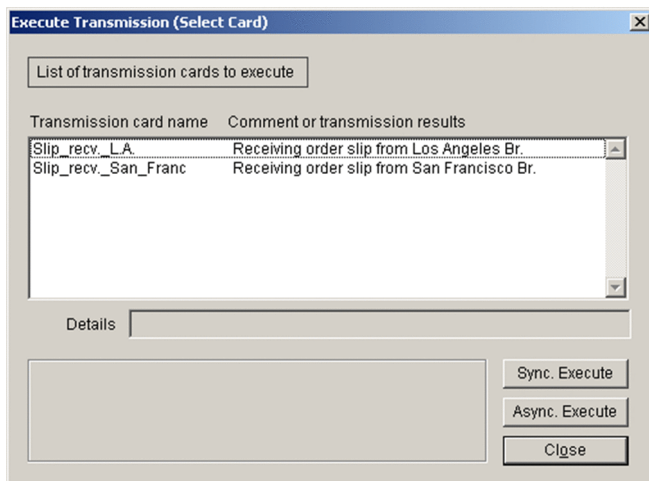
This subsection describes two methods, one that uses the Registration And Execution Of Transmission Requests window and one that uses a command.

(1) Using the Registration And Execution Of Transmission Requests window

To execute transmission:

1. In the Registration And Execution Of Transmission Requests window, select a transmission card to be transmitted.
2. Choose **Exe.(Select Card)**.
The Execute Transmission (Select Card) dialog box appears.

Figure 3–14: Execute Transmission (Select Card) dialog box



To change the sequence of transmission

The Select Card method of file transmission transmits sequentially in the order that the files are listed in the Execute Transmission (Select Card) dialog box. To change the sequence, double-click a desired transmission card. The double-clicked transmission card is moved to the top of the list and will be transferred first.

3. Click either **Sync. Execute** or **Async. Execute**.

- Synchronous execution

Transmission is executed sequentially for each card (each card name). Transmission of one file must be completed before the next file can be transmitted, thereby preventing line overloading.

The transmission result is displayed under the details in the Execute Transmission (Select Card) dialog box. The numbers in parentheses indicate the sequential transmission numbers of the file transmissions. If an error occurs before transmission, no transmission number is displayed.

- Asynchronous execution

All cards are transmitted in the batch mode. You can transmit a maximum of 60 files concurrently. If you select asynchronous execution, the message `Registration ended` is displayed, and no transmission results are displayed. You must check the logs for the results.

4. After executing transmission, click **Close**.

How to cancel file transmission

When you click **Sync. Execute** or **Async. Execute**, **Stop** or **Force Stop** is displayed.

- **Stop**

Synchronous execution: The request is canceled after the current file transmission is finished.

Asynchronous execution: The request is canceled after the current file transmission request is registered.

If connection is established with the JP1/File Transmission Server/FTP Client service, the request is canceled after the connection is released.

- **Force Stop**

Cancels the transmission immediately. When asynchronous execution is specified, transmissions that have already been registered are not canceled. Note that the file transmission log might not be output.

If possible, try to avoid using this option because the system might not be able to release the resources.

About the display of file transmission errors when a wildcard is used

Only the first error that occurred is displayed in **Comment or transmission results**.

(2) Using the ftstran command

The following figure shows an example of using a command to execute the Select Card method of file transmission:

```
ftstran card1
Card name
```

Transmission by the `ftstran` command is applicable only to synchronous execution. For details about the `ftstran` command, see *ftstran - executes transmission* in 6. *Commands*.

3.5.2 Executing transmission by entering a transmission card (Enter Information method of file transmission)

This method transmits the contents of a transmission card as is. You can enter a new transmission card or use an existing transmission card and edit its contents. The Enter Information method of file transmission does not register the transmission card.

This subsection describes two methods, one that uses the Registration And Execution Of Transmission Requests window and one that uses a command.

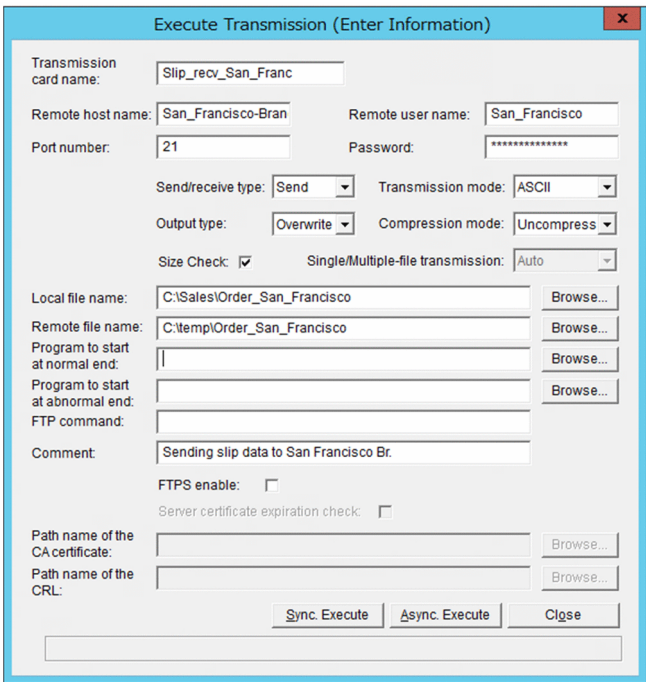
(1) Using the Registration And Execution Of Transmission Requests window

To execute transmission:

- 1. In the Registration And Execution Of Transmission Requests window, choose **Exe.(Enter Info.)**. Alternatively, in the Registration And Execution Of Transmission Requests window, specify the transmission card to use, and then choose **Exe.(Enter Info.)**.

The Execute Transmission (Enter Information) dialog box appears.

Figure 3–15: Execute Transmission (Enter Information) dialog box



2. Enter or edit the transmission contents.

For details about the settings of the items, see [3.4.1 Registering transmission information onto a transmission card](#).

3. Click either **Sync. Execute** or **Async. Execute**.

- Synchronous execution

Transmission is executed sequentially for each card (each card name). Transmission of one file must be completed before the next file can be transmitted, thereby preventing line overloading.

- Asynchronous execution

All cards are transmitted in the batch mode. You can transmit a maximum of 60 files concurrently. If you select asynchronous execution, the message `Registration ended` is displayed, and no transmission results are displayed. You must check the logs for the results.

4. After executing transmission, click **Close**.

How to cancel file transmission

When you click **Sync. Execute** or **Async. Execute**, the **Now executing** dialog box is displayed. Clicking **Force Stop** in this dialog box cancels the transmission immediately. Note that the file transmission log might not be output.

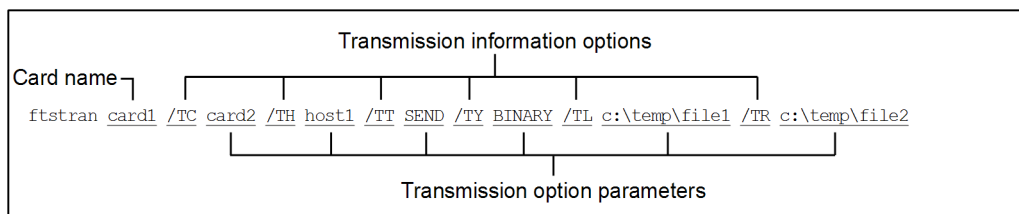
If you execute synchronous execution after forced cancellation, there might be a delay before transmission begins.

About the display of file transmission errors when a wildcard is used

Only the first error that occurred is displayed in the message that is displayed after transmission.

(2) Using the `ftstran` command

The following figure shows an example of using a command to execute the Enter Information method of file transmission:



This example changes the following transmission information on `card1` and then executes transmission:

- `/TC`: The card name is `card2`.
- `/TH`: The connection-target host name is `host1`.
- `/TT`: The send/receive type is `SEND`.
- `/TY`: The transmission mode is `BINARY`.
- `/TL`: The local file name is `c:\temp\file1`.
- `/TR`: The remote file name is `c:\temp\file2`.

Transmission by the `ftstran` command is applicable only to synchronous execution. For details about the `ftstran` command, see [ftstran - executes transmission](#) in [6. Commands](#).

3.6 Checking the transmission logs

You can check the logs of file transmissions (such as for the transmission times, the names of the transmitted files, the results and details of the transmissions, and the details of errors).

Logs can be displayed by both the server and the client. Start **Log Information** to display the Log Information window, or use the `ftshistory` command.

How to display the Log Information window

From the Windows **Start** menu, choose **Programs, JP1_File Transmission Server_FTP**, and then **Log Information**.

The Log Information window is displayed. The following figure shows the Log Information window.







Figure 3–16: Log Information window

FTS_HIST - Log Information

File View Details Help

Date	Start time-End time	Card	Trans. No./Snd/Rcv	Local file	Bytes	Remote host	Error type	Comment	
10/02/25	20:54:25-20:54:25	Slip_recv_L.A.	72	Received	Order_Los_Angeles	15058	Los-Angeles-Branch		Receiving order slip from Los Angeles Br.
10/02/25	20:53:29-20:53:29	Slip_recv_L.A.	71	Received	Order_Los_Angeles	0	Los-Angeles-Branch		Receiving order slip from Los Angeles Br.
10/02/25	20:52:55-20:52:55	Slip_recv_L.A.	70	Received	Order_Los_Angeles	0	Los-Angeles-Branch	System call error	Receiving order slip from Los Angeles Br.
10/02/25	20:52:16-20:52:16	Slip_recv_San_Franc	69	Received	Order_San_Francisco	12117	San-Francisco-Branch		Receiving order slip from San Francisco Br.
10/02/25	20:51:30-20:51:30	Slip_recv_San_Franc	68	Received	Order_San_Francisco	14311	San-Francisco-Branch		Receiving order slip from San Francisco Br.
10/02/25	20:49:30-20:49:30	Slip_recv_San_Franc	67	Received	Order_San_Francisco	13132	San-Francisco-Branch		Receiving order slip from San Francisco Br.
10/02/25	20:49:28-20:49:28	Slip_recv_L.A.	66	Received	Order_Los_Angeles	13095	Los-Angeles-Branch		Receiving order slip from Los Angeles Br.
10/02/25	20:48:30-20:48:31	Slip_recv_San_Franc	65	Received	Order_San_Francisco	24064	San-Francisco-Branch		Receiving order slip from San Francisco Br.
10/02/25	20:48:24-20:48:24	Slip_recv_L.A.	64	Received	Order_Los_Angeles	25088	Los-Angeles-Branch		Receiving order slip from Los Angeles Br.
10/02/25	20:45:22-20:45:22	Definition_info.	63	Sent	definition.inf	1495	San-Francisco-Branch		
10/02/25	20:44:57-20:44:57	Definition_info.	62	Sent	definition.inf	0	Los-Angeles-Branch	System call error	
10/02/25	20:44:41-20:44:41	accounting_test	61	Sent	testaccounting.bt	9	San-Francisco-Branch		
10/02/25	20:43:55-20:43:55		12	Received	testaccounting.bt	9	xxxx.xxxx.xxxx.xxxx		

Legend:

-  (Blue) : Transmission that terminated normally at the client
-  (Red) : Transmission that terminated abnormally at the client
-  (Green) : Program that cannot be started automatically at the client
-  (Blue) : Transmission that terminated normally at the server
-  (Red) : Transmission that terminated abnormally at the server
-  (Green) : Program that cannot be started automatically at the server

3.6.1 Checking the details of transmission results and errors

To display detailed information from the Log Information window:

1. From the Log Information window, select the log information whose details are to be displayed, and then choose **Details**.

The Log Details dialog box appears. If a protocol trace and errors have been output, you can check the details of the errors.

Figure 3–17: Log Details dialog box

Log Details

Transmission number : 70

Transmission card name: Slip_recv_LA

Transmission start-end : 10/02/25 20:52:55 - 10/02/25 20:52:55

Remote host name : Los-Angeles-Branch

Remote port number : 21

Logged-in user : Los_Angeles

Client or server : Client End status : Abnormal

Sent or received : Received Transmission period : 00:00:00

Output type : Overwrite Size transmitted : 0

Transmission mode : ASCII Connection number : 11

Compression mode : Uncompress

Local file name : C:\temp\Order_Los_Angeles

Remote file name : C:\temp\Order_Los_Angeles

Comment : Receiving order slip from Los Angeles Br.

Error type : System call error

Protocol Trace... Error Details... OK

2. Check the detailed information, and then click **OK**.

The following table lists and describes each item in the Log Details dialog box.

Table 3–7: Items in the Log Details dialog box

Item	Description
Transmission number	Displays the transmission number. This number is determined separately at the server and the client. Because this is a unique number assigned to each transmission, you can use it as an identifier when you view logs. The largest transmission number is 999,999 (if this value is exceeded, the counter is reset to 0).
Transmission card name	<ul style="list-style-type: none"> Client: Displays the name of the card that was transmitted. Server: Not displayed.
Transmission start-end	Displays the date and time transmission started and the date and time transmission ended.
Remote host name	Displays the remote host name that was specified in the transmission request. This is a host name or IP address defined in the system.
Remote port number	<ul style="list-style-type: none"> Client: Displays the remote port number that executed transmission. Server: Not displayed.
Logged-in user	<ul style="list-style-type: none"> Client: Displays the name of the remote login user that executed transmission. Server: Displays the name of the login user that received the transmission.
Client or server	<ul style="list-style-type: none"> Client: Displayed when file transmission was executed by the client. Server: Displayed when file transmission was executed by the server.
Sent or received	Displays the send/receive type (Send or Receive) that was specified during the transmission request.
Output type	Displays the output type (Append or Overwrite) that was specified in the transmission request.
Transmission mode	Displays the transmission mode (ASCII or BINARY) that was specified in the transmission request.

Item	Description
Compression mode	Displays the compression mode (Compress or Uncompress) that was specified in the transmission request.
End status	Displays the termination status of the file transmission (Normal or Abnormal). If automatic program start fails but file transmission itself was successful, Normal is displayed.
Transmission period	Displays the amount of time required for the file transmission. If this value is 24 hours or more, the number of days is not displayed.
Size transmitted	Displays the data size (in bytes) of the transmitted file.
Connection number	Displays a transmission identifier based on when JP1/FTP established connection with the remote system. This is a separate number for the server and the client in the range from 1 to 60 (the maximum value depends on the maximum number of connections). Because various traces (such as the protocol trace) are output for each connection number, you can use this number as a guide for viewing traces of the corresponding transmission. Example: When Connection number is 2: Client's protocol trace file: CSProtocolTrace2 Server's protocol trace file: SSProtocolTrace2
Local file name	<ul style="list-style-type: none"> For sending: Displays the name of the file sent from the local system. For receiving: Displays the name of the file received by the local system.
Remote file name	<ul style="list-style-type: none"> Client For sending: Displays the output file name at the remote system. For receiving: Displays the name of the input source file as is. Server: Not displayed.
Comment	<ul style="list-style-type: none"> Client: Displays the comment that was specified in the transmission request. Server: Not displayed.
Error type	When the transmission status is Abnormal, displays one of the errors listed below. To view the details of an error, click Error Details . <ul style="list-style-type: none"> System call error Protocol error Logical error SSL communication error
Protocol Trace	Displays internal processing from the start to the end of the transmission. A response code that is preceded by an asterisk (*) means that the response was generated internally by the JP1/FTP client, and that it is not an actual response received from the remote server. For the protocol traces output by version 07-50 or later, traces for the corresponding transmission are displayed. If there is no trace for the corresponding transmission, all traces are displayed.
Error Details	Displays error details, such as the error types and locations.

3.6.2 Changing the information displayed in the Log Information window

You can change the information that is displayed in the Log Information window, such as by refreshing the information or displaying only those logs that satisfy specified conditions.

To change the information:

1. In the Log Information window, from the **View** menu, choose the information that you wish to have displayed:

Entire Log or Specify Log Info.

Specifies either all logs or only those logs that satisfy specific conditions.

If you choose **Specify Log Info.**, the View Range dialog box is displayed.

Sort By End Time or Sort By Start Time

Specifies whether the logs are to be sorted by file transmission end time (starting with the most recent) or by file transmission start time (starting with the most recent).

Newest Log Info.

Refreshes the log information.

Figure 3–18: View Range dialog box

The screenshot shows the 'View Range' dialog box. It has a title bar with 'View Range' and a close button. The main area is divided into several sections. The 'Date/time range' section has a label 'For the log beginning time and log end time use the file transmission:' and two radio buttons: 'Start times' and 'End times' (which is selected). To the right of these are two date/time pickers: 'From:' (2010 / 6 / 1 20 : 41 : 1) and 'Until:' (2010 / 12 / 31 1 : 58 : 59). Above the 'Until' picker is a checkbox 'Display info. until the log end.' and below the 'From' picker is a checkbox 'Display info. from the log beginning.' The bottom section has three groups of radio buttons: 'Client or server' (Client, Server, Client and server - selected), 'Sent or received' (Sent, Received, Sent and received - selected), and 'Transmission end status' (Normal, Abnormal, Normal and abnormal - selected). On the right side of the dialog are four buttons: 'All Info.', 'Today's Info.', 'OK', and 'Cancel'.

The following table lists and describes each item in the View Range dialog box.

Table 3–8: Items in the View Range dialog box

Item	Setting
Date/time range	<p>Specifies the time period for which log information is to be displayed. The left column specifies whether the display is to be sorted based on start time or end time. The right column specifies the date/time range.</p> <ul style="list-style-type: none">• Left column (sort order) Specifies whether the log information is to be searched by start time or by end time.• Right column (time period) Specifies the beginning and ending dates and times of the period for which log information is to be displayed, using the following format: <i>YYYY/MM/DD HH:MM:SS</i>
All Info.	Sets the time period so that it is from the oldest log to the most recent log in the log file.
Today's Info.	Changes the time period settings to today's date.
Client or server	Specifies Client or Server as the log type to display. If there is no need to make this distinction, select Client and server .
Sent or received	Specifies Sent or Received as the log type to display. If there is no need to make this distinction, select Sent and received .
Transmission end status	Specifies Normal or Abnormal as the log type to display. If there is no need to make this distinction, select Normal and abnormal .

3.6.3 Changing the log file that is displayed

You can specify to have a different log file displayed in the event of a failure.

1. In the Log Information window, from the **File** menu, choose **Specify Log File**.

A dialog box for loading a log file is displayed.

2. Specify the log file to be loaded and then click **Open**.

The specified log file is loaded.

To return to the current log file, from the **File** menu, choose **Current Log File**.

3.6.4 Using the `ftshistory` command to display logs

The following example displays the details of all log information (default format):

```
ftshistory
```

For details about the `ftshistory` command, see [*ftshistory - displays log information*](#) in 6. *Commands*.

3.7 Saving and recovering JP1/FTP settings

Definition information can be saved and then restored in a different environment. You can achieve a standardized system environment by specifying definition information in one system and then distributing it to multiple systems. You can save and recover the following four types of definition information:

- Environment settings
- User-to-login settings
- Auto-start program settings
- Transmission settings

To save or recover definition information, you start **Saving and Recovering Settings** to display the Saving and Recovering Settings dialog box. Alternatively, you can use a command.

How to display the Saving and Recovering Settings dialog box

From the Windows **Start** menu, choose **Programs**, **JP1_File Transmission Server_FTP**, and then **Saving and Recovering Settings**.

The following figure shows the Saving and Recovering Settings dialog box.

Figure 3–19: Saving and Recovering Settings dialog box



3.7.1 Saving definition information

To save definition information, you can use the Saving and Recovering Settings dialog box or you can execute a command.

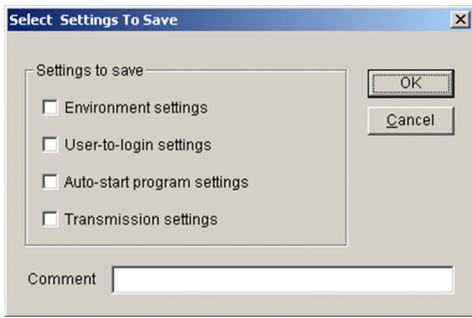
(1) Using the Saving and Recovering Settings dialog box

To save settings:

1. In the Saving and Recovering Settings dialog box, click **Save**.

The Select Settings To Save dialog box is displayed. The following figure shows the Select Settings To Save dialog box.

Figure 3–20: Select Settings To Save dialog box



2. Select the boxes for the types of settings that you wish to save. You can also enter a comment (a character string of up to 40 bytes).

This comment will be displayed when the settings are recovered. Entry of a comment is optional.

When nothing is specified in the settings that are selected

The settings are saved as is with no information specified and are recovered as is with nothing specified. You can specify applicable settings information during recovery processing.

3. Click **OK**.

A dialog box for specifying a file name is displayed.

4. Specify the storage location and a name for the settings file, and then click **Open**.

5. In the Saving and Recovering Settings dialog box, click **Close**.

(2) Using the `ftssave` command

The following figure shows an example of the command that saves definition information:

```
ftssave definition1
        File name
```

This example saves all definition information (environment settings, user-to-login settings, auto-start program settings, and transmission settings). You can also select the types of settings that are saved.

For details about the `ftssave` command, see [*ftssave - saves definition information*](#) in 6. *Commands*.

3.7.2 Recovering definition information

To recover saved definition information, you can use the Saving and Recovering Settings dialog box or you can execute a command.

You must select one of the following formats for recovering definition information:

- **Do not delete settings at destination**

This format recovers the definition file without deleting the existing settings at the destination.

- **Delete settings at destination**

This format deletes the existing settings at the destination and then recovers the definition file.

In the event of a failure during recovery processing

If a failure occurs during recovery processing, the definition information is not recovered. We recommend that you always save the existing settings before you perform recovery with **Delete settings at destination** specified.

About the log information directory during recovery of an environment definition

The log information directory specified in the environment definition is not created automatically. If you are using a non-default log information directory, use the Environment Definition utility to update the environment definition. Without this directory, you will not be able to start various JP1/FTP services.

(1) Using the Saving and Recovering Settings dialog box

To recover settings:

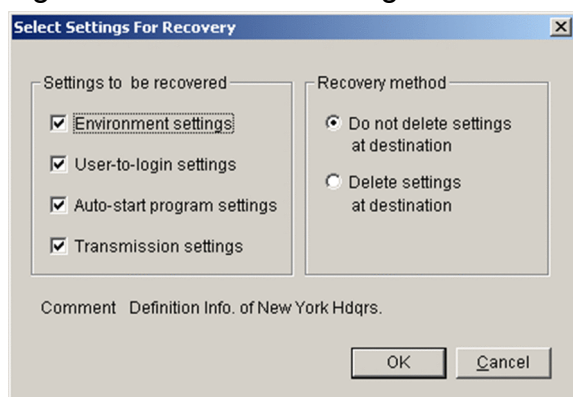
1. In the Saving and Recovering Settings dialog box, click **Recover**.

A dialog box for selecting the file to recover is displayed.

2. Specify the file to be recovered, and then click **Open**.

The Select Settings For Recovery dialog box is displayed.

Figure 3–21: Select Settings For Recovery dialog box



3. Select the boxes for the types of settings recover, and then select the radio button for the recovery method to use.

4. Click **OK**.

A message is displayed.

5. Click **OK**.

6. In the Saving and Recovering Settings dialog box, click **Close**.

The following table lists and describes each setting item in the Select Settings For Recovery dialog box.

Table 3–9: Setting items in the Select Settings For Recovery dialog box

Item	Setting
Settings to be recovered	Selects the types of settings to be recovered: <ul style="list-style-type: none">• Environment settings Recovers information that was set by the Environment Definition utility.• User-to-login settings Recovers information that was specified when login users were registered.• Auto-start program settings Recovers information that was specified when auto-start programs were registered.

Item	Setting
Settings to be recovered	<ul style="list-style-type: none"> • Transmission settings Recovers information that was registered when transmissions were registered and executed.
Recovery method	<p>Specifies whether to delete the existing settings.</p> <ul style="list-style-type: none"> • Do not delete settings at destination Recovers settings in the saved definition file without deleting the existing settings at the destination. If the destination contains key information identical to that given below, the settings at the destination are updated to those in the saved file. If the destination does not contain the same key information, the settings in the saved file are added. The keys are as follows: Environment settings: All environment settings become a single key. User-to-login settings: User name Auto-start program settings: File name, directory name Transmission settings: Card name • Delete settings at destination Deletes the settings at the destination and then recovers the information in the saved file. Because the information in the saved file becomes the settings, no unneeded settings information remains. The existing settings are deleted one at a time after being checked. Note that environment settings will not be deleted. When user information is deleted, any associated auto-start program settings are also deleted.
Comment	Displays the comment that was specified when the settings were saved.

(2) Using the ftsload command

The following figure shows an example of a command for recovering saved definition information:

```
ftsload definition1
      File name
```

This example recovers all definition information (environment settings, user-to-login settings, auto-start program settings, and transmission settings) without deleting the existing settings at the destination. You can also select specific types of settings to recover, and you can specify to delete the existing settings.

For details about the `ftsload` command, see [ftsload - recovers definition information](#) in 6. *Commands*.

3.8 Outputting definition information as text

You can output the following four types of definition information to a text file:

- Login user information
- Auto-start program information
- Transmission information
- Log information

When you output definition information, you can use a sample format file that was set up during installation. You can edit the format file to a desired format. For details about format files, see *E. Format Files Used for Output of Definition Information*.

3.8.1 Outputting definition information as text

To output definition information as text, you use the **File** menu in each registration window.

You can select one of the following text output formats:

Output text

This format outputs information to a specified file. If the specified file already exists, its contents are overwritten.

Append text

This format adds the information after the last line of the specified file.

To output definition information as text:

1. From the Windows **Start** menu, choose **JP1_File Transmission Server_FTP**, and then choose the registration window from which to output definition information as text.
2. From the **File** menu, choose **Output To Text File** or **Append To Text File**.
A dialog box for specifying the output destination file is displayed.
3. Specify the output destination file and then click **Open**.

The following figures show a format file for auto-start programs and an example of text output.

Figure 3–22: Format file

```
////////// Auto-Start Program Registrations ////////// No.$ICNT //////////  
User name: $USER  
Trigger key: $AKEY  
Type of key: $AFDK  
Auto-start program at normal end: $ANML  
Auto-start program at abnormal end: $AERR
```

Figure 3–23: Example of text output

```
////////// Auto-Start Program Registrations ////////// No.1 //////////  
User name: ACCOUNTING  
Trigger key: accounting001  
Type of key: file  
  Auto-start program at normal end: C:\accounting\Accounting001N.exe  
  Auto-start program at abnormal end: C:\Accounting\A_Err.exe  
  
////////// Auto-Start Program Registrations ////////// No.2 //////////  
User name: SALES1  
Trigger key: salesreport3  
Type of key: file  
  Auto-start program at normal end: JP1EVENT 1124 ALL  
  Auto-start program at abnormal end: JP1EVENT 1144 ALL
```

3.9 File transmission in the PASV mode

At the client, you can transmit files in the PASV mode.

File transmission in the PASV mode can be enabled separately for each host at the remote FTP server.

To transmit files in the PASV mode, you must register in advance the names of the hosts at the remote FTP server to which you wish to transfer files in the PASV mode.

This registration information takes effect the next time the client service starts.

3.9.1 Registering the host names

Create a definition file as shown below and then specify the host names.

(1) Creating a definition file

Create a definition file with the following path name:

JP1/FTP-installation-directory\FTPPASV.INI

(2) Contents of the definition file

Specify information in the format of a Windows initialization file (.ini), as shown below:

[PasvMode]
MaxInfoCount=*maximum-number-of-hosts* | ALL
HostName[1]=*host-name-1*
HostName[2]=*host-name-2*
:
HostName[X]=*host-name-X*

The following table lists and describes the section, keys, and values that can be specified.

Table 3–10: Contents of the definition file in the PASV mode

Section	Key	Value	Description
[PasvMode]	MaxInfoCount	<i>maximum-number-of-hosts</i> ALL	Specifies the number of remote FTP server hosts to which transmission of files in the PASV mode will be permitted: <ul style="list-style-type: none"><i>maximum-number-of-hosts</i>: Specifies a maximum value for <i>X</i> in the HostName[<i>X</i>] lines that follow this line.ALL: Specifies that file transmission in the PASV mode is to be permitted for all remote FTP server hosts. When ALL is specified, any HostName[<i>X</i>] lines are ignored.

Section	Key	Value	Description
[PasvMode]	HostName [<i>X</i>]	<i>host-name</i>	<p>Specifies the host name or IP address of the remote FTP server to which files will be transmitted in the PASV mode.</p> <p>When you specify an IP address, you can specify an IPv4 or IPv6 address. Use one line for each host to be registered.</p> <p>For a host name, specify the same remote host name as is used in the transmission information.</p> <ul style="list-style-type: none"> For <i>X</i>, specify a value of 1 or greater but no greater than the value of MaxInfoCount. If the specified value is greater than the value of MaxInfoCount, the specification is ignored. The <i>X</i> value on each line must be unique. The <i>X</i> values can be specified in any order.

Examples

Example 1: Enable transmission of files to HOST1 and HOST2 in the PASV mode:

```
; JP1/File Transmission Server/FTP
; PASV mode configuration file
;
[PasvMode]
MaxInfoCount=2
HostName[1]=HOST1
HostName[2]=HOST2
```

Example 2: Enable transmission of files to all hosts in the PASV mode:

```
; JP1/File Transmission Server/FTP
; PASV mode configuration file
;
[PasvMode]
MaxInfoCount=ALL
```


3.10 Function for controlling remote host connections

At the FTP server, you can limit the FTP clients that are permitted to establish connection.

When the IP addresses or host names of FTP clients whose connection is to be permitted are defined in a permission list, transmission can be performed only by those FTP clients. You can also control connection by defining in a rejection list the IP addresses or host names of FTP clients whose connection requests are to be rejected.

This function checks the definitions in effect when an FTP client attempts to establish connection with the FTP server. If the connection request is rejected, the control connection is lost and no control connection response message is sent.

Note that you can change definitions while the JP1/File Transmission Server/FTP Server service is running.

3.10.1 Registering host names

You create a definition file as shown below and then specify host names.

(1) Creating a definition file

Create a definition file with the following path name:

```
JP1/FTP-installation-directory\FTPHOSTACC.INF
```

(2) Contents of the definition file

Use a text editor to specify the definition file (FTPHOSTACC.INF) according to the following method:

```
# comment
definition-name
:
```

Begin by specifying a definition name, and then specify values on the following lines. If you specify multiple values, make sure that you specify only one value on each line. Any characters following a hash mark (#) through a linefeed are treated as a comment.

The following table lists and describes the definition names and values that can be specified.

Table 3–11: Definition names and values that can be specified in the definition file (FTPHOSTACC.INF)

Definition name	Description	Value
[allow_list]	Specifies hosts whose connection is to be permitted. In the case of an IP address, you can specify an IPv4 or IPv6 address.	IP address or host name
[deny_list]	Specifies hosts whose connection is to be rejected. In the case of an IP address, you can specify an IPv4 or IPv6 address.	IP address or host name

The following table shows the formats that can be used for specifying an IPv6 address.

Table 3–12: Formats that can be specified for an IPv6 address

No.	Address to be specified	Description	Definition
1	2001:0db8:0020:0003:1000:0100:0020:0003	All 128 bits specified	Valid
2	2001:db8::9abc	Partial omission	Valid
3	::1	Loopback address specification	Valid
4	2001:F123:2221:2312:3333:4444::/96	Mask specification	Valid
5	2001:128:222:333	Last value omission specification	Invalid
6	2001:F123:2221:2312:3333*:5555:6666	Multiple specifications	Invalid
7	2001:F123:2221:2312:3333:4444:5555:1111-FFFF	Multiple-range specification	Invalid

Example

[allow_list]	# Defines hosts whose connection is permitted.
192.168.10.2	# IP address. Connection is OK if the IP address matches exactly.
192.169.20.	# Multiple IP addresses. Connection is OK for any IP address that begins with the specified value.
192.169.20.0/255.255.255.0	# Same as above, but uses mask specification.
192.169.30.*	# Specifies multiple IP addresses.
192.169.30.0/255.255.255.0	# Same as above, but uses mask specification.
192.170.	# Multiple IP addresses. Connection OK for any IP address that begins with the specified value.
192.170.0.0/255.255.0.0	# Same as above, but uses mask specification.
192.171.17.68-71	# Specifies a range of IP addresses.
	# Permits 192.171.17.68 through 192.171.17.71.
192.171.17.68/255.255.255.252	# Same as above, but uses mask specification.
192.172.18-19.*	# Specifies a range of IP addresses.
	# Permits 192.172.18.1 through 192.172.18.255 and 192.172.19.1 through 192.172.19.255.
192.173.*.10	# Specifies a range of IP addresses.
	# Permits 192.173.1.10 through 192.173.255.10.
192.173.*.10/255.255.0.255	# Same as above, but uses mask specification.
host1.aname.com	# Specifies host names.
.sample.co.jp	# Specifies multiple host names. Connection is OK for any host name that ends with the specified value.
2001:0db8:0020:0003:1000:0100:0020:0003	# IPv6 address. Connection is OK when the complete IPv6 address matches.
2001:0db8:9abc::/48	# IPv6 address. Connection is OK when the first 48 bits of the IPv6 address match.
[deny_list]	# Defines hosts to be rejected (among the hosts that are permitted).
192.169.20.3	# 192.169.20.1 through 192.169.20.255 are permitted, except for 192.169.20.3.
192.170.10.	# 192.170.0.0 through 192.170.255.255 are permitted, except for 192.170.10.0 through 192.170.10.255.
www.sample.co.jp	# Hosts whose name ends with .sample.co.jp are permitted, except for www.sample.co.jp.
2001:db8::1234:0:0:9abc	# IPv6 address.
	Host is rejected when the complete IPv6 address matches.
2001:db8::9abc	# IPv6 address.
	Host is rejected when the complete IPv6 address matches.

(3) Notes

- If there is no definition file, connection is permitted from all hosts.

- If there is a definition file but it does not contain any valid definitions, connection requests from all hosts are rejected.
- A connection request from a host that is not specified in the definition file or a host that is specified in both `[allow_list]` and `[deny_list]` is rejected.
- Alias host names cannot be specified for host names.
- To permit or reject a loopback address, do not specify a host name (localhost), but specify an IP address (127.0.0.1).
- When specifying an IPv6 address, specify a mask value in the format *address-portion/xx* (where *xx* is a decimal number between 1 and 128).
- IPv6 address specifications that have a scope ID (with the % character specified) are invalid.

3.11 Using JP1/FTP in a multiple IP address environment

In an environment in which multiple IP addresses can be used, such as an environment that uses multiple NICs or a cluster environment, the following functions are available:

- Function that enables you to specify the local IP address of the FTP client
Setting the local address for the FTP client's source address is enabled by defining YES in the FTP client definition and specifying the logical host name in the API, in an argument of the `ftstran` command, or in the input field for the client host name in a custom job.
- Function for setting the FTP server host name in a response message sent by the FTP server to the address that accepted the connection
Specifying the connected IP address or the host name obtained by converting the connected IP address as the FTP server's host name in a response message that is sent from the FTP server is enabled by defining either YES or NO in the FTP server definition.
- Function for specifying the destination of JP1 events
Sending JP1 events to a specified host is enabled by defining the logical host name or logical IP address in the JP1 event definition.

These functions take effect after the definition file is created, and then each service is started.

3.11.1 Creating a definition file

Create a definition file as shown below.

(1) Creating a definition file

Create a definition file with the following path name:

```
JP1/FTP-installation-directory\HOSTINFO.INI
```

(2) Contents of the definition file

Specify information in the format of a Windows initialization file (`.ini`), as shown below:

```
[CSHOST]
CSHost=YES|NO
[RSPMSG]
Reverse=YES|NO|(omitted)
[JP1EVENT]
HostName=host-name|IP-address|(omitted)
AgentInSame=YES|NO
TransIsSame=YES|NO
```

The following table lists and describes the sections, keys, and values that can be specified.

Table 3–13: Contents of the definition file (HOSTINFO.INI)

Section	Key	Value	Description
[CSHOST]	CSTHost	YES NO <<NO>>	<p>At the FTP client, specifies whether the <code>ftstran</code> command's <code>/H</code> specification and the <code>fts_ftp_open_ex()</code> function's <code>hostname</code> specification are to be effective:</p> <ul style="list-style-type: none"> • YES: Set the FTP client's source address to the IP address of the host that is specified in <code>/H</code> in the <code>ftstran</code> command or in <code>hostname</code> in the <code>fts_ftp_open_ex()</code> function. • If you specify YES but <code>/H</code> is omitted in the <code>ftstran</code> command, the physical host name is assumed. Also, if you specify YES but NULL is specified in <code>hostname</code> in the <code>fts_ftp_open_ex()</code> function, the physical host name is assumed. • NO: Set the FTP client's source address to the value that is assigned automatically by the OS.
[RSPMSG]	Reverse	YES NO (omitted) <<omitted>>	<p>Specifies the output format for the FTP server's host name in a response message that is sent from the FTP server:</p> <ul style="list-style-type: none"> • YES: Output the host name obtained by converting the connected IP address. • NO: Output the connected IP address. • Omitted: Output the physical host name.
[JP1EVENT]	HostName	<i>host-name</i> <i>IP-address</i> (omitted) <<omitted>>	<p>Specifies the destination for output of JP1 events:</p> <ul style="list-style-type: none"> • <i>host-name</i> <i>IP-address</i>: Specifies the destination for JP1 events that report the start and stop of services (client, server, log, or agent). When you specify an IP address, you can specify an IPv4 or IPv6 address. The destination (logical or physical address) of a JP1 event that is generated during termination of a transmission is set to the host that executed the transmission. • Omitted: Send all JP1 events to the physical host.
	AgentIsSame	YES NO <<YES>>	<p>Specifies whether to set the destination of the JP1 events reporting the start and stop of the agent service to the host specified in <code>HostName</code>.</p> <ul style="list-style-type: none"> • YES: Set the destination of JP1 events to the host specified in <code>HostName</code>. • NO: Set the destination of JP1 events to the physical host.
	TransIsSame	YES NO <<NO>>	<p>Specifies whether to set the destination of the JP1 events reporting the end of transmission to the host specified in <code>HostName</code>.</p> <ul style="list-style-type: none"> • YES: Set the destination of JP1 events to the host specified in <code>HostName</code>. • NO: Set the destination of JP1 events to the host that executed the transmission.

The following table shows the destination of the JP1 events reporting the end of transmission, as determined on the basis of the combination of defined specification values.

Table 3–14: Destination of the JP1 events reporting the end of transmission, as determined on the basis of the combination of defined specification values

HostName	TransIsSame	Destination of the JP1 events reporting the end of transmission
Specified	YES	Host specified by HostName
	NO	Host that executed the transmission
Not specified	YES	Physical host
	NO	Physical host

Example

- This example enables the /H specification in the `ftstran` command and the `hostname` specification in `fts_ftp_open_ex()` function.
- This example sets the host name obtained by converting the connected IP address as the FTP server's host name in the FTP server's response message.
- This example sets the destination of JP1 events reporting the start and stop of services (client, server, log, or agent) or the end of transmission to `Host1` (logical host name = `Host1`).

```
;JP1/File Transmission Server/FTP
;For logical host configuration file
;
[CSHOST]
CSHost=YES
[RSPMSG]
Reverse=YES
[JP1EVENT]
HostName=Host1
AgentInSame=YES
TransIsSame=YES
```

(3) Note

If there is no definition file, these functions are disabled (they operate on the basis of the default values).

3.12 Collecting access logs

At the FTP server, you can log invalid or unsuccessful access attempts by an FTP client until it successfully logs in (achieves user authentication) after establishing a connection.

3.12.1 Settings for collecting access logs

To set JP1/FTP to collect access logs, you must specify a value of at least 1 megabyte in **Size of Access log file** in the Environment Definition dialog box. For details about the Environment Definition dialog box, see [3.1 Defining an environment for JP1/FTP](#).

3.12.2 Log output file

Access logs are output as text to the access log file. The following table shows the access log file and its backup file.

Table 3–15: Access log output file and backup file

Description	File name
Access log file	<i>directory-for-log-information\ftsaccess.log</i>
Backup file	<i>directory-for-log-information\ftsaccess.log.old</i>

The file size is from 0 bytes to the size specified in **Size of Access log file** in the Environment Definition dialog box. When the output exceeds the size specified in **Size of Access log file**, JP1/FTP saves the file into the backup file, initializes the file size to 0 bytes, and then writes data from the beginning of the file.

If the backup file already exists when a backup is needed, JP1/FTP overwrites the existing backup file.

3.12.3 Messages that are output to the access logs

The following table lists and describes the messages that are output to the access logs.

Table 3–16: Messages that are output to the access logs

Message	Description
<i>FTP-command</i> ^{#1} is invalid because it was sent by a user who was not logged in. [Remote host: <i>IP-address</i> ^{#2}] [Remote port: <i>port-number</i> ^{#3}] [Connection number: <i>connection-number</i> ^{#4}]	An FTP command that becomes executable after login was accepted before login.
Login of user <i>user-name</i> ^{#5} failed. [Remote host: <i>IP-address</i> ^{#2}] [Remote port: <i>port-number</i> ^{#3}] [Connection number: <i>connection-number</i> ^{#4}]	Login failed.
The max. number of FTP clients was reached. No more clients can use the service.	More connections were accepted than the maximum permissible number of concurrent transmissions.
The connection was closed without login. [Remote host: <i>IP-address</i> ^{#2}] [Remote port: <i>port-number</i> ^{#3}] [Connection number: <i>connection-number</i> ^{#4}]	The FTP client disconnected itself without logging in.

#1

FTP-command: Indicates the FTP command.

#2

IP-address: Indicates the IP address of the FTP client.

#3

port-number: Indicates the port number of the FTP client.

#4

connection-number: Indicates the connection number.

#5

user-name: Indicates the user name.

3.13 Function for using the access control function to change the root directory for absolute path names

When you use the access control function, you can change the root directory for the absolute path names of files and directories to the user's home directory.

This function enables you to hide the directory hierarchy above the user's home directory when the user views and sets files and directories.

To use this function, you must have already registered the absolute path name format.

The registered information takes effect the next time the JP1/File Transmission Server/FTP Server service starts.

3.13.1 Registering the absolute path name format

Create a definition file and specify the absolute path name format as described below.

(1) Creating a definition file

Create a definition file with the following path name:

```
JP1/FTP-installation-directory\AccessLimitation.ini
```

(2) Contents of the definition file

Specify information in the format of a Windows initialization file (.ini), as shown below:

```
[HomeDir]  
Display=Root|FullPath
```

The following table lists and describes the section, key, and values that can be specified.

Table 3–17: Contents of the definition file (AccessLimitation.ini)

Section	Key	Value	Description
[HomeDir]	Display	Root FullPath <<FullPath>>	Specifies the absolute path name format for files and directories: <ul style="list-style-type: none">• Root: Format in which the root directory is the home directory.• FullPath: Format in which the root directory is the system's root directory (full path format).

(3) Example of display and specification format

This subsection describes the display and specification formats using examples based on the following directory structure:

```

C:
└─ Dir01
   └─ Dir02 ← Home directory during login
      ├── File01
      └─ File02

```

Example 1

Response message that is displayed when the `pwd` command is entered at the standard FTP client when the current directory is the home directory (Dir02):

- When Root is set:
257 "\" is current directory.
- When FullPath is set:
257 "C:\Dir01\Dir02" is current directory.

Example 2

Specification for deleting File01 at the standard FTP client when the current directory is the home directory (Dir02):

- When Root is set:
delete \File01
- When FullPath is set:
delete C:\Dir01\Dir02\File01

(4) Notes

- If there is no definition file, the full path format is assumed.
- If you do not use the access control function, this definition file is ignored.
- Messages are always output to the event log in the full path format regardless of this definition.

3.14 FTP connection response message control function

Normally, the following response message is displayed at the time of an FTP connection:

220 HHH FTP server (JP1/File Transmission Server/FTP VV-RR-SS YYYY/MM/DD) ready.
Host name Product name Version information#

VV-RR-SS: Version (-SS might not be displayed.)
YYYY: Year
MM: Month
DD: Date

You can set that the response message is not to display the host name, product name, and version information. You can also set the response message to display any optional character string.

To change the FTP connection response message, you must have already registered the definition information.

The registered information takes effect the next time the JP1/File Transmission Server/FTP Server service starts.

3.14.1 Registering the definition information

Create a definition file and specify the definition information as described below.

(1) Creating a definition file

Create a definition file with the following path name:

JP1/FTP-installation-directory\FtsBanner.ini

(2) Contents of the definition file

Specify information in the format of a Windows initialization file (.ini), as shown below:

[BANNER]
Display=ON|OFF

The following table lists and describes the section, key, and values that can be specified.

Table 3–18: Contents of the definition file (FtsBanner.ini)

Section	Key	Value	Description
[BANNER]	Display	ON OFF <<ON>>	Specifies whether to display the host name, product name, and version information in the FTP connection response message: <ul style="list-style-type: none">ON: Display.OFF: Do not display.

(3) Creating an FTP connection response message file

To set a character string of your choosing for the FTP connection response message, first set `Display` to `OFF` in the definition file, and then create an FTP connection response message file with the following path name:

```
JP1/FTP-installation-directory\FtsBanner.txt
```

(4) Contents of the FTP connection response message file

Specify a text for the FTP connection response message as follows:

```
FTP-connection-response-message-text
```

Notes

- The FTP connection response message file must consist of at least one line.
- A maximum of 256 bytes of characters can be specified per line. Any additional characters are ignored.
- The maximum file size is 512 bytes. The file is ignored if it exceeds 512 bytes.
- A line consisting of a linefeed only is valid.
- You cannot specify a comment.
- If the file size is 0 bytes, the file is ignored.
- Depending on the connecting FTP client, some limitations might apply to the format of a response message. In the FTP connection response message file, make sure that you specify text that can be recognized by the connecting FTP client.

3.14.2 FTP connection response message that is displayed

This subsection shows and explains the FTP connection response message that is displayed.

If `Display` is set to `OFF` in the definition file (`FtsBanner.ini`), but there is no FTP connection response message file (`FtsBanner.txt`), the following FTP connection response message is displayed:

```
220 FTP server ready.
```

If there is an FTP connection response message file (`FtsBanner.txt`), the FTP connection response message is set as follows according to the FTP protocol specifications:

- If the file contains only one line of data, response code 220 is added at the beginning of the line.
- If the file contains multiple lines, 220- is added at the beginning of the first line, 220 is added at the beginning of the last line, and five single-byte spaces are added at the beginning of each of the intervening lines.

The following figures show an example of an FTP connection response message.

Contents of the FTP connection response message file (`FtsBanner.txt`)

```
Welcome to FTP server.  
Anonymous users cannot connect to this server.  
Please enter the username and password.
```

FTP connection response message

```
220- Welcome to FTP server.  
      Anonymous users cannot connect to this server.  
220 Please enter the username and password.
```

3.15 Using JP1/FTP in an IPv6 environment

You can transmit files using an IPv6 address.

To transmit files using an IPv6 address, you must first register the definition information.

3.15.1 Registering the Internet protocol version

Create a definition file as shown below and describe the definition information.

(1) Creating a definition file

Create a definition file with the following path name:

```
JP1/FTP-installation-directory\IPversion.ini
```

(2) Contents of the definition file

Specify information in the format of a Windows initialization file (.ini), as shown below:

```
[address_family_S]  
IPv4=ON|OFF  
IPv6=ON|OFF  
[address_family_C]  
Priority=IPv4|IPv6
```

The following table lists and describes the section, key, and values that can be specified.

Table 3–19: Contents of the definition file (IPversion.ini)

Section	Key	Value	Description
[address_family_S]	IPv4	ON OFF <<ON>>	Specifies whether to use IPv4 at the FTP server when accepting a connection from the FTP client. <ul style="list-style-type: none">• ON: Uses IPv4.• OFF: Does not use IPv4.
	IPv6	ON OFF <<OFF>>	Specifies whether to use IPv6 at the FTP server when accepting a connection from the FTP client. <ul style="list-style-type: none">• ON: Uses IPv6.• OFF: Does not use IPv6.
[address_family_C]	IPv4	ON OFF <<ON>>	Specifies whether to use IPv4 at the FTP client when connecting to the FTP server. <ul style="list-style-type: none">• ON: Uses IPv4.• OFF: Does not use IPv4.
	IPv6	ON OFF <<OFF>>	Specifies whether to use IPv6 at the FTP client when connecting to the FTP server. <ul style="list-style-type: none">• ON: Uses IPv6.• OFF: Does not use IPv6.
	Priority	IPv4 IPv6	Specifies the Internet protocol version preferred by the FTP client when connecting to the FTP server.

Section	Key	Value	Description
[address_family_C]	Priority	<<IPv4>>	<ul style="list-style-type: none"> IPv4: IPv4 is given priority. IPv6: IPv6 is given priority. <p>This definition is used for selecting the Internet protocol version to be used for connection in the following cases.</p> <p>When the FTP client's transmission source address is not specified:</p> <p>A host name is specified for the remote host name of the transmission card, and both IPv4 and IPv6 IP addresses are defined for that host name.</p> <p>When the FTP client's transmission source address is specified:</p> <p>A host name is specified in the /H option of the ftstran command, or in the client host name input field in a custom job, and both IPv4 and IPv6 IP addresses are defined for that host name.</p>
[address_family_L]	Use	IPv4 IPv6 <<IPv4>>	<p>Specifies the Internet protocol version to be used by the JP1/File Transmission Server/FTP Log service for connecting to the JP1/File Transmission Server/FTP Server service or the JP1/File Transmission Server/FTP Client service.</p> <ul style="list-style-type: none"> IPv4: Uses IPv4. IPv6: Uses IPv6.

(3) Notes

- If there is no definition file, the Internet protocol version selection is invalid. In this case, IPv4=ON and IPv6=OFF are assumed at both the FTP server and the FTP client.
- If IPv4=OFF and IPv6=OFF are defined at the FTP server, it is considered that there is no definition. In this case, IPv4=ON and IPv6=OFF are assumed.
- If IPv4=OFF and IPv6=OFF are defined at the FTP client, the definition is assumed not to exist. In this case, IPv4=ON and IPv6=OFF are assumed.
- When changing the definition, first stop the server service, client service, and log service.

3.16 Using FTPS (at the FTP client)

At the FTP client, files can be transmitted by using FTPS.

The following table describes the implemented features related to FTPS.

Table 3–20: Implemented features related to FTPS (at the FTP client)

Item	Implemented feature
Implicit mode	Not supported
Explicit mode	Supported
Automatic switching to the usual FTP when the FTP server does not support FTPS	Not supported
Version of SSL communication	TLS1.2
Client authentication method	Password authentication
Server certificate verification	<ul style="list-style-type: none">• Certificate chain• Expiration date of the certificate• Expiration status of the certificate
Server certificate expiration notification method	CRL
Data protection level for data connection	Private
SSL sessions for data connection	Reuse the control connection sessions
CCC command (Environment where NAT conversion is carried out)	Not supported

3.16.1 Certificate and CRL

Prepare a root certificate corresponding to the server certificate used by the destination FTP server.

You can use a CRL.

3.16.2 Notes about the certificate and the CRL

You can only use certificates and CRLs in X509 PEM format.

3.16.3 Definition of transmission information

Define transmission information.

For details about the transmission information to be defined, see [Table 3-6 Items in the Register Transmission Information dialog box](#).

3.17 Using FTPS (at the FTP server)

At the FTP server, files can be transmitted by using FTPS.

The following table describes the implemented features related to FTPS.

Table 3–21: Implemented features related to FTPS (at the FTP server)

Item	Implemented feature
Implicit mode	Not supported
Explicit mode	Supported
Version of SSL communication	TLS1.2
Client authentication method	Password authentication
Data protection level for data connection	<ul style="list-style-type: none">• Clear• Private
CCC command (Environment where NAT conversion is carried out)	Not supported

3.17.1 Private key and certificate

Prepare a server private key and the corresponding server certificate.

If the server certificate has been issued by an intermediate certificate authority, you should also prepare all intermediate certificates up to the root certificate. Put all certificates together, including the server certificate, the lower-ranking intermediate certificates, and the higher-ranking intermediate certificates, in that order, and store them in a single file.

3.17.2 Notes about the private key and the certificate

- You cannot use a private key with a passphrase. In other words, you have to cancel the passphrase before using the private key. Thus, it is important that appropriate access permissions be assigned so that the private key is not accessed by users other than those with administrator permissions.
- You can only use private keys and certificates in X509 PEM format.

3.17.3 Creating a definition file

Create a definition file by following the procedure described below, and then specify definition information.

(1) To create a definition file

Create a definition file with the following path name:

```
JP1/FTP-installation-directory\ftsftps.ini
```

(2) Information specified in the definition file

As shown below, information inside the file must be specified in Windows initialization file (.ini) format.

```
[FTPS_ServInfo]
PrivateKey=path-name
Certificate=path-name
FTPSModeOnly=YES|NO
```

The following table describes the sections, keys, and values you can specify.

Table 3–22: Information defined in the definition file (ftsftps.ini)

Section	Key	Value	Description
[FTPS_ServInfo]	PrivateKey	path-name	Specify a full path to the private key file of the server.
	Certificate	path-name	Specify a full path to the server certificate file.
	FTPSModeOnly	YES NO <<NO>>	Specify whether to use only FTPS. <ul style="list-style-type: none">• YES: Only FTPS is available. The usual FTP is not available. If you specify YES, the JP1/File Transmission Server/FTP Server service would not start unless a value is specified for either PrivateKey or Certificate.• NO: Not only FTPS but also the usual FTP is available.

(3) Note

The definition information becomes valid after the JP1/File Transmission Server/FTP Server service starts.

4

JP1/FTP Operations Management

The Operations-Manager Console enables you to check the definition information for other JP1/FTP and view transmission logs. This chapter describes how to use the Operations-Manager Console.

4.1 Setting up the Operations-Manager Console

To use the Operations-Manager function, you must run the program at both the managing host and the managed hosts. Note that only an administrator can start the Operations-Manager Console.

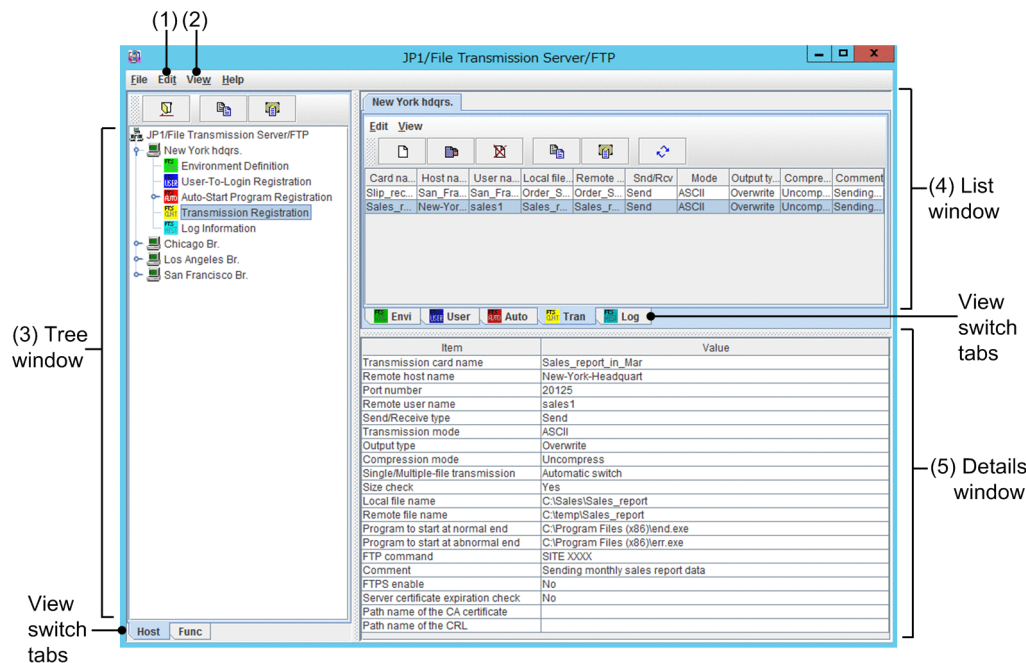
- Managing host: Start the Operations-Manager Console.

Start the Operations-Manager Console at the managing host. It enables you to view transmission logs of the remote and local JP1/FTP servers and to register, update, and view definition information items.

How to start the Operations-Manager Console

From the Windows **Start** menu, choose **Programs**, **JP1_File Transmission Server_FTP**, and then **Manager Console**.

Figure 4–1: Operations-Manager Console window



1. Choosing **Host List** from the **Edit** menu: See [4.1.1 Adding managed hosts](#).

2. Choosing **Display Log Count** from the **View** menu:

Set the number of logs to be displayed in the Log Information window. When the Display Log Count dialog box appears, specify the number of logs that you wish to display, in the range from 1 to 10,000.

3. Tree window:

This window displays a list of the managed hosts and corresponding information. The view switch tabs enable you to switch between displaying by hosts and displaying by functions.

If there are too many managed hosts to fit in the tree window, information about four hosts before and after the selected host is displayed.

4. List window:

This window provides a listing of the information selected in the tree window. You can use the view switch tabs to change the display for each function.

5. Details window:

This window displays details of the information selected in the list window. Note that nothing is displayed for the Environment Definition utility.

- Managed host: Start the Operations-Manager Agent.

Start the Operations-Manager Agent on each host where the Operations-Manager Agent is to be run.

How to start the Operations-Manager Agent

To start a manager agent that is to be managed by the Operations-Manager Console, start the JP1/File Transmission Server/FTP Agent service. For details about how to start the service, see [2.3 Starting and stopping services](#).

Notes

- If you use the Operations-Manager function, you can use only alphabetic characters, numbers, and hyphens for the host name.
- The Operations-Manager functions are supported even if the JP1/FTP versions for the Operations-Manager Console and the Operations-Manager Agent are different.
- In an environment in which IP address translation is performed between Operation-Manager Console and Operation-Manager Agent, the Operations-Manager function cannot be used.
- IPv6 cannot be used for connections between Operations-Manager Console and Operations-Manager Agent.
- You cannot use the Operations-Manager function to establish a connection between an environment using version 10-00 or earlier and a pre-10-00 version environment if the environments have different language settings (for example, a Japanese language environment and an English language environment).
- On the side of Operations-Manager Agent, the IP address of the physical host (the host returned by the hostname command) must be an IP address to which Operations-Manager Console can connect. In an environment where there are multiple IP addresses on the side of Operations-Manager Agent, the intended IP address might not be used. In such cases, by registering following definition information in advance (as described below), you can specify the IP address you want to use. The registered information will be applied to the JP1/File Transmission Server/FTP Agent service that starts after the settings are configured.

1. Create a definition file with the following path name:

JP1/FTP-installation-directory\manager\agent\jvmoptions.txt

2. Specify the following information:

-Djava.rmi.server.hostname=IP-address-on-the-side-of-JP1/File-Transmission-Server/FTP-Agent

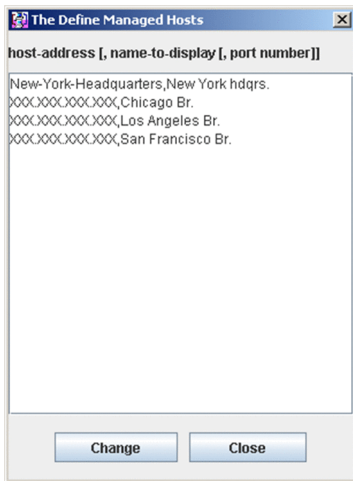
4.1.1 Adding managed hosts

You use the Operations-Manager Console to set the hosts that are to be managed.

To add managed hosts:

1. At the Operations-Manager Console, from the **Edit** menu, choose **Host List**.
The Define Managed Hosts dialog box appears.

Figure 4–2: The Define Managed Hosts dialog box



2. Specify the address and display name, separated by a comma, of a managed host that is to be added.

```
host-address[,name-to-display[,port-number]]
```

host-address

Specifies the host name or IP address of the managed host.

This item is mandatory.

name-to-display ((0 to 15-byte character string))

Specifies a name to be displayed for the managed host on the Operations-Manager Console window.

This item is optional. If it is omitted, the specified host address is displayed.

port-number

Specifies the port number of the managed host.

Specification of a port number is optional. If it is omitted, the port number of the local host in `ftsagent` is assumed.

When the host address or name to be displayed contains a comma (,) or double-quotation mark (")

Enclose the entire host address or name to be displayed in double-quotation marks (").

Example: Specifying `aaa,bbb` as the name to be displayed: `myhost,"aaa,bbb",20252`

Example: Specifying `aaa"bbb` as the name to be displayed: `myhost,"aaa"bbb",20252`

3. Repeat step 2 for each additional host that is to be registered.

4. Click **Change**.

The specified host names are displayed in the tree window.

4.1.2 Deleting managed hosts

To delete a managed host:

1. At the Operations-Manager Console, from the **Edit** menu, choose **Host List**.
The Define Managed Hosts dialog box appears.
2. Select the managed host that you want to delete, and then press the **Delete** key.

3. Click **Change**.

Other editing method

Information about the managed hosts is saved in the (comma-delimited) file *JP1/FTP-installation-directory* \manager\console\hostdef.csv. You can use a text editor such as Notepad to edit this file. To apply the edited information, you must restart the Operations-Manager Console.

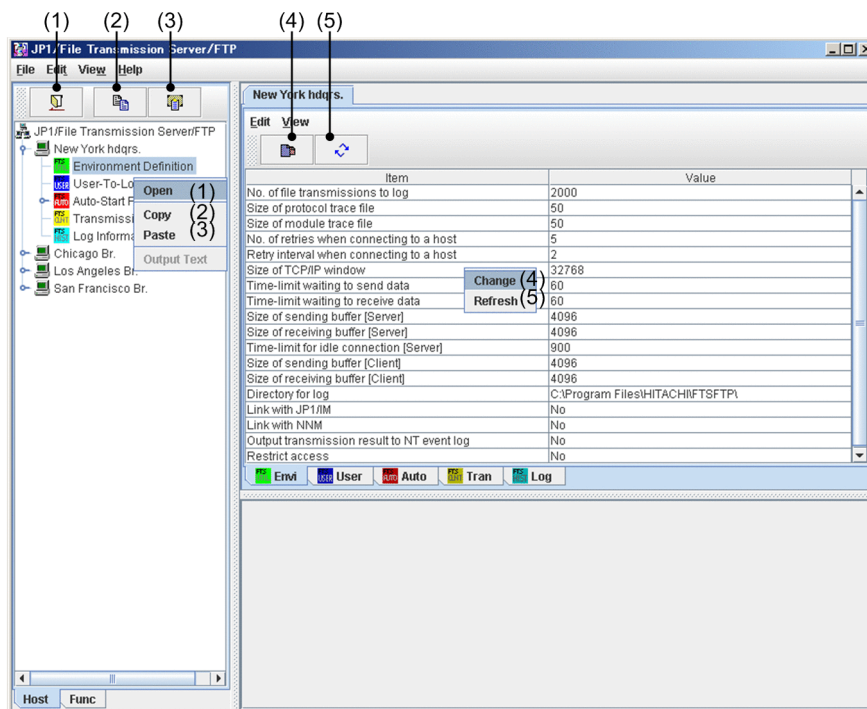
4.2 Organization and functions of the Operations-Manager Console windows






The Operations-Manager Console provides different windows for displaying various types of information. This section presents the windows of the Operations-Manager Console that are used to display information.

4.2.1 Environment Definition window

The figure below shows an example of the Environment Definition window for another host that is displayed in the Operations-Manager Console. This subsection describes the functions that you can use in the Environment Definition window.

Figure 4–3: Environment Definition window



1. Click , or right-click in the tree window: Opens host information.
2. Click , or right-click in the tree window: Copies host information.
3. Click , or right-click in the tree window: Pastes the copied information.
4. Click , or right-click in the list window: Changes the definition information.
5. Click , or right-click in the list window: Refreshes the information.

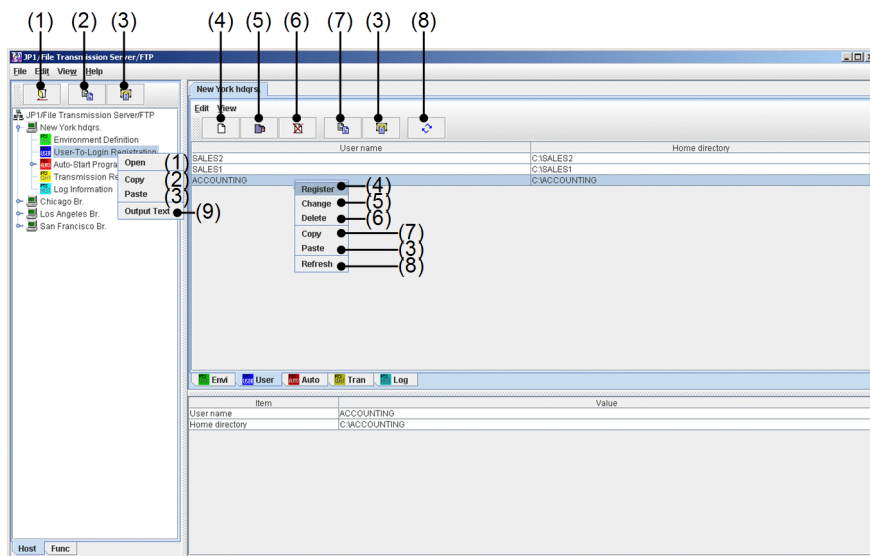
Notes









- Definition information cannot be copied between Windows hosts and UNIX hosts that have been set as managed hosts.
- If definition information is copied from a version earlier than 07-50 to version 07-50 or later, single-byte spaces can no longer be entered in the file path names.

4.2.2 User-To-Login Registration window

The figure below shows an example of another host's login user registration status that is displayed from the Operations-Manager Console. This subsection describes the functions that you can use in the User-To-Login Registration window.

Figure 4–4: User-To-Login Registration window



1. Click  , or right-click in the tree window: Opens host information.
2. Click  , or right-click in the tree window: Copies all login user definition information.
3. Click  , or right-click in the tree or list window: Pastes the copied login user information.
4. Click  , or right-click in the list window: Registers a new login user.
5. Click  , or right-click in the list window: Changes the information registered for the specified login user.
6. Click  , or right-click in the list window: Deletes the specified login user.
7. Click  , or right-click in the list window: Copies the specified login user information.
8. Click  , or right-click in the list window: Refreshes the information.
9. Right-click in the tree window: Outputs the login user information as text.

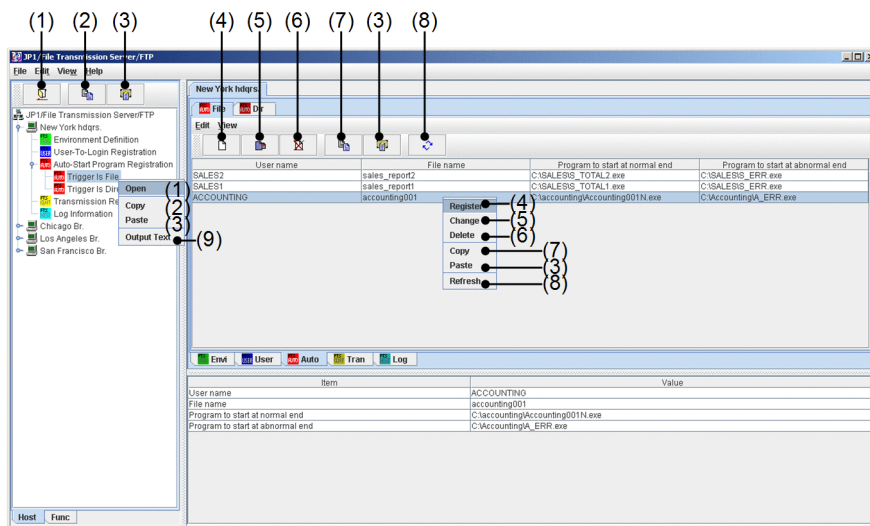
Notes









- When **Cancel** is clicked while **Register** or **Change** processing is underway, the message **Canceled** is displayed, but the registration or change processing might have already been completed.
- Login user information cannot be copied between Windows hosts and UNIX hosts that have been set as managed hosts.

4.2.3 Auto-Start Program Registration window

The figure below shows an example of an Auto-Start Program Registration window that displays from the Operations-Manager Console the registration status of the auto-start programs at another host. This subsection describes the functions that you can use in the Auto-Start Program Registration window.

Figure 4–5: Auto-Start Program Registration window (for files)



1. Click  , or right-click in the tree window: Opens host information.
2. Click  , or right-click in the tree window: Copies all auto-start program definition information.
3. Click  , or right-click in the tree or list window: Pastes the copied information.
4. Click  , or right-click in the list window: Registers new auto-start programs.
5. Click  , or right-click in the list window: Changes the registration details of auto-start programs.
6. Click  , or right-click in the list window: Deletes auto-start programs.
7. Click  , or right-click in the list window: Copies information about a specified auto-start program.
8. Click  , or right-click in the list window: Refreshes information.
9. Right-click in the tree window: Outputs information about auto-start programs as text.

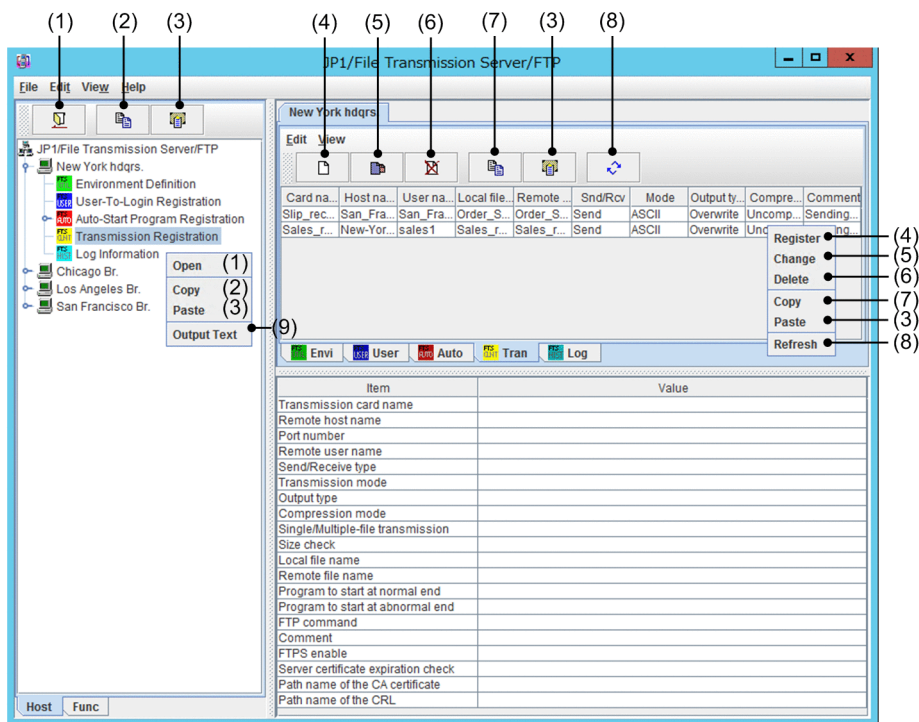
Notes









- When **Cancel** is clicked while **Register** or **Change** processing is underway, the message *Canceled* is displayed, but the registration or change processing might have already been completed.
- If the manager agent is UNIX, whether the login user name has been registered is not checked when auto-start programs are registered.
- Information about auto-start programs cannot be copied between Windows hosts and UNIX hosts that have been set as managed hosts.

4.2.4 Transmission Registration window

The figure below shows an example of a window that displays from the Operations-Manager Console the transmission information registration details at another host. This subsection describes the functions that you can use in the Transmission Registration window.

Figure 4–6: Transmission Registration window



1. Click , or right-click in the tree window: Opens host information.
2. Click , or right-click in the tree window: Copies all transmission definition information.
3. Click , or right-click in the tree or list window: Pastes the copied information.
4. Click , or right-click in the list window: Registers new transmission information.
5. Click , or right-click in the list window: Changes registered transmission information.
6. Click , or right-click in the list window: Deletes transmission information.
7. Click , or right-click in the list window: Copies the specified transmission information.
8. Click , or right-click in the list window: Refreshes information.
9. Right-click in the tree window: Outputs the transmission information as text.

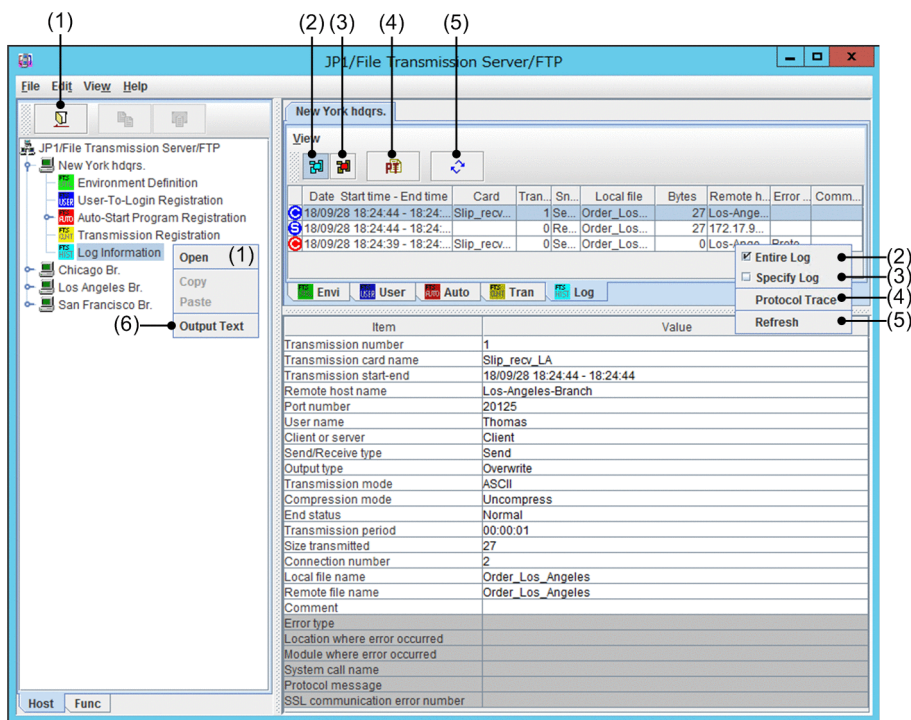
Notes






- When **Cancel** is clicked while **Register** or **Change** processing is underway, the message **Canceled** is displayed, but the registration or change processing might have already been completed.
- Transmission information cannot be copied between Windows hosts and UNIX hosts that have been set as managed hosts.
- Pre-10-00 versions of the Windows edition of Operations-Manager Agent have a limitation such that Operations-Manager Console can display only 5,000 items of transmission information from a host on which such an Operations-Manager Agent is running.

4.2.5 Log Information window

The figure below shows an example of a window that displays from the Operations-Manager Console another host's log information. This subsection describes the functions that can be used in the Log Information window.

Figure 4–7: Log Information window



1. Click , or right-click in the tree window: Opens host information.
2. Click , or right-click in the list window: Displays all log information.
3. Click , or right-click in the list window: Displays specific log information.
4. Click , or right-click in the list window: Displays protocol trace.
5. Click , or right-click in the list window: Refreshes information.
6. Right-click in the tree window: Outputs log information as text.

Notes

- If there are multiple logs with the same time, the order in which the information is displayed in the Operations-Manager Console's Log Information window might be different from the display order in the stand-alone Log Information window.
- The Log Information window displays all trace information, even if there is a trace of a transmission. This differs from when a protocol trace is displayed from the Windows **Start** menu by choosing **Programs, JP1_File Transmission Server_FTP**, and then **Log Information**.
- Operations-Manager Agent versions earlier than 10-00 do not support a transmission size of 4 gigabytes or greater. Consequently, if the Operations-Manager Console is connected to an Operations-Manager Agent earlier than version 10-00, and if an attempt is made to reference a transmission log whose transmission size is 4 gigabytes or greater, the displayed value will be smaller than the actual transmission size.

4.3 Examples of Operations-Manager Console menu operations

The operations when you use the Operations-Manager Console to register and edit information are the same in all windows. This section presents four examples of menu operations for reference purposes.

4.3.1 Example of registering login user information

This example registers login user information in the New York headquarters.

To register login user information:

1. In the tree window, double-click `New York headquarters`.

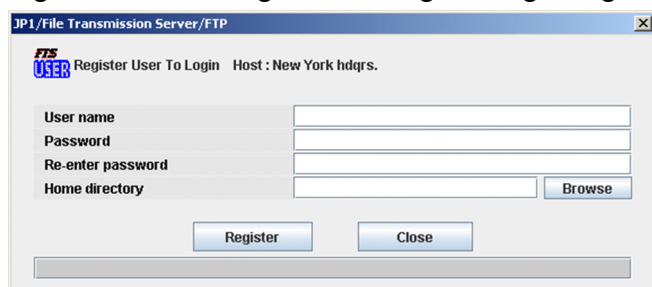
2. Under `New York headquarters`, select **User-To-Login Registration**, and then click .

The login user information that has been registered in the New York headquarters is displayed in the list window.

3. In the list window, click .

A dialog box for registering a login user is displayed. If login user information is selected in the list window, the selected login user information is displayed. You can also register new information by using the displayed information as a model.

Figure 4–8: Dialog box for registering a login user



4. Enter the login user information and then click **Register**.


For details about the information to be registered, see [3.2.1 Registering the login users](#).


You can register multiple sets of login user information one after another until you click **Close**.

5. Click **Close**.

Changing and deleting login user information

You can change and delete login user information in the same manner.



Changing: Specify the desired login user information and then click .

Deleting: Specify the desired login user information and then click .

4.3.2 Example of distributing (copying) transmission information

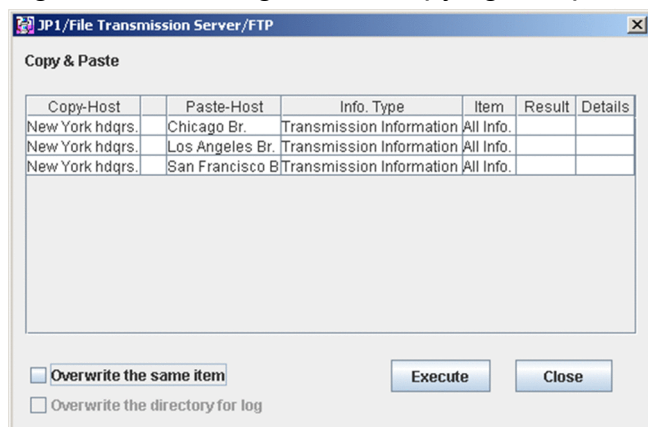
This example copies transmission information by distributing it from the New York headquarters to three branches (Chicago, Los Angeles, and San Francisco). If the same information already exists, it will be overwritten.

To copy information:

1. In the tree window, double-click New York headquarters.
2. Under New York headquarters, select **Transmission Registration**, and then click .
3. In the tree window, click Chicago, and then click Los Angeles and San Francisco while holding down the **Shift** or **Ctrl** key.
4. In the tree window or the list window, click .

A dialog box for copying and pasting information is displayed.

Figure 4–9: Dialog box for copying and pasting information



About Overwrite the directory for log


This option is enabled only when environment definition information is being copied. Select it only if you want to overwrite the existing log information directory.

5. Select **Overwrite the same item** and then click **Execute**.
When the copy and paste operation is finished, **Result** and **Details** are displayed. By clicking **Details**, you can view the copied information and error information.
6. Click **Close**.

4.3.3 Example of displaying log information

This example displays the log information for the New York headquarters.

To display log information:

1. In the tree window, click the **Func** tab at the bottom.
Information is displayed in the tree window by function.
 2. In the tree window, double-click **Log Information**.
 3. Select New York under the log information, and then click .
- Log information is displayed in the list window.

To display only specific log information:

In the list window, click . In the displayed dialog box, specify a condition for displaying information.

Figure 4–10: Dialog box for displaying specific information

JP1/File Transmission Server/FTP

View Range Host : New York Hdqrs.

Date/time range	From the log beginning
	Until the log end
	Sort by end time
Client or server	All
Send/Receive type	All
End status	All
Transmission card name	
Remote host name	
User name	
Local file name	
Remote file name	
Transmission number	-
Connection number	-
Size transmitted (Bytes)	-
Transmission period (Secs)	-
Transmission mode	All
Output type	All
Compression mode	All
Error type	All
Comment	

All Info. Today's Info. OK Cancel

4.3.4 Example of outputting multiple definition information items as text

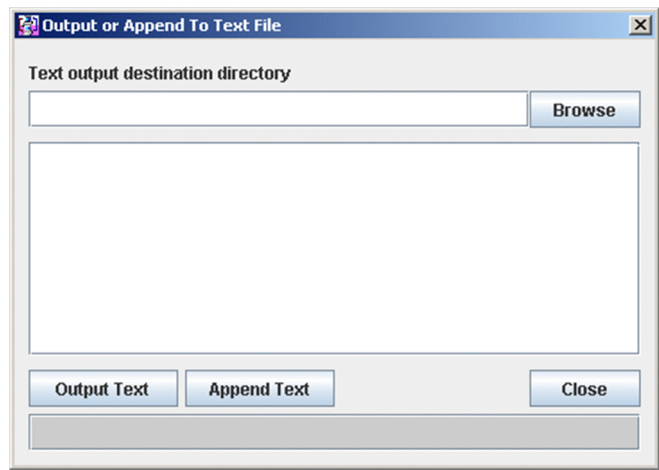
This example outputs definition information for the Chicago, Los Angeles, and San Francisco branches as text. You can select for the output method either **Output Text** or **Append Text**.

A sample format for text that is output is set up during installation. You can edit the format file to create a desired format. For details about how to edit the format file, see [E. Format Files Used for Output of Definition Information](#).

To output multiple definition information items as text:

1. In the tree window, click **Chicago** branch, and then click **Los Angeles** branch and **San Francisco** branch while holding down the **Shift** or **Ctrl** key.
2. From the right-click menu, choose **Output Text**.
The Output or Append To Text File dialog box appears.

Figure 4–11: Output or Append To Text File dialog box



3. Specify the directory to which the text is to be output, and then click either **Output Text** or **Append Text**.

Output Text

Outputs the registration information to the specified file. If the specified file already exists, its contents are overwritten.

Append Text

Outputs the definition information at the end of the specified file.

The text output status is displayed.

4. Click **Close**.

File name for the output text

The following table shows the name of the output file depending on the type of information.

Table 4–1: Names of output text files

Type of information	File name ^{#1}
User information ^{#2}	<i>host-name-to-be-displayed_user.txt</i>
Auto-start program information based on file	<i>host-name-to-be-displayed_autof.txt</i>
Auto-start program information based on directory	<i>host-name-to-be-displayed_autod.txt</i>
Transmission information	<i>host-name-to-be-displayed_tran.txt</i>
Log information	<i>host-name-to-be-displayed_hist.txt</i>

^{#1}
If the host name part of the file name to be displayed contains any illegal character for a file name ([\ / : ; , * ? < > |]), each such illegal character will be replaced with # to create the file name.

^{#2}
The information cannot be output when the target host is UNIX.

5

Linkage with Other JP1 Programs

This chapter describes the settings required for linking JP1/FTP to other JP1 programs and the respective operation methods.

5.1 Linking to JP1/AJS3

You can link JP1/FTP to JP1/AJS3 to perform scheduled file transmissions.

This section describes the settings for linking to JP1/AJS3 and the operation method.

5.1.1 System configuration for linking to JP1/AJS3

Required programs

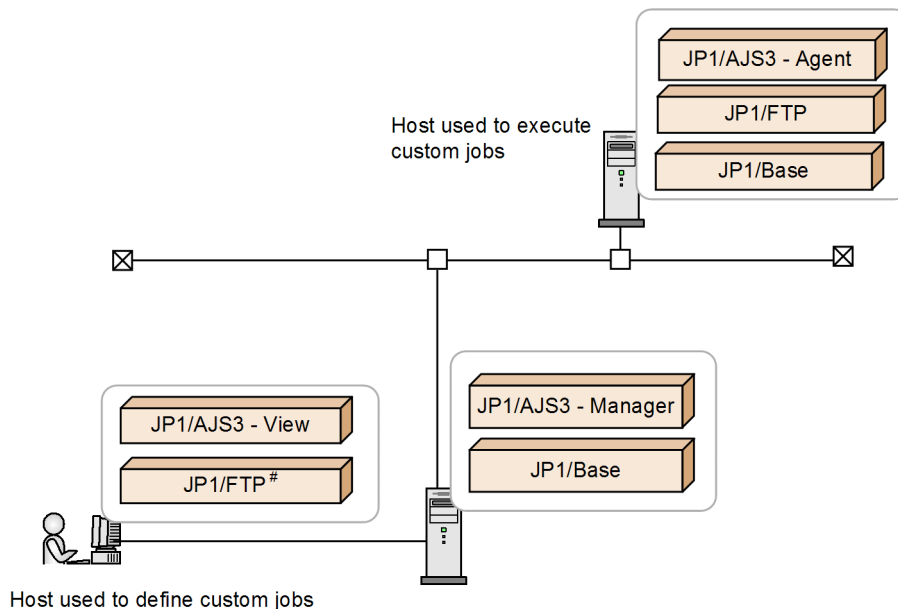
Install the following programs on the computer where JP1/FTP is installed:

- JP1/AJS3 - Manager or JP1/AJS3 - Agent
- JP1/AJS3 - View

When installing JP1/FTP and JP1/AJS3 - View on separate computers

JP1/FTP and JP1/AJS3 - View might be installed on separate computers. In such cases, you must copy the required files to the computer on which JP1/AJS3 - View is installed. For details, see [5.1.2 Specifying the settings for linking to JP1/AJS3](#).

Figure 5–1: Example of a system configuration for linking to JP1/AJS3



#: Instead of JP1/FTP, the definition program (`fts_card.exe`) can be copied and the copy can be used.

5.1.2 Specifying the settings for linking to JP1/AJS3

To link JP1/FTP to JP1/AJS3, you must specify the following settings in JP1/AJS3:

- Register JP1/FTP as a custom job
Register JP1/FTP into JP1/AJS3 as a custom job so that the job can be used in JP1/AJS3.
- Copy the transmission information for JP1/FTP
If the host used to define jobs differs from the host used to execute the jobs, copy the transmission information from the host used to execute jobs into the host used to define jobs.

(1) Registering JP1/FTP as a custom job

To register JP1/FTP into JP1/AJS3 as a custom job in order to link JP1/FTP to JP1/AJS3:

1. From the Windows **Start** menu, choose **Programs, JP1_Automatic Job Management System 3 - View**, and then **Register Custom Job**.

The Register Custom Job dialog box appears.

2. Click **Add**.

The Set Properties of Custom Job dialog box appears.

3. Set each item and then click **OK**.

The custom job is registered. The following shows the Set Properties of Custom Job dialog box and the settings.

Figure 5–2: Set Properties of Custom Job dialog box

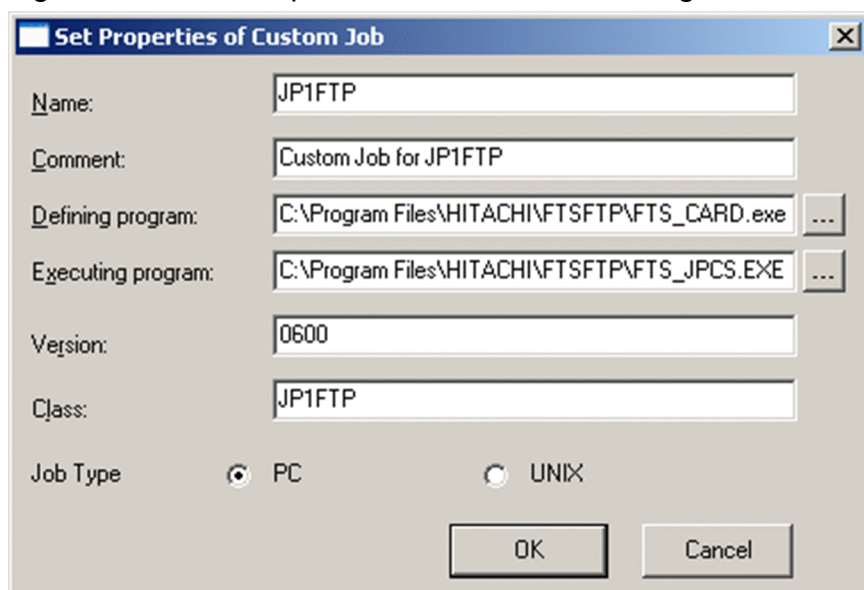


Table 5–1: Settings in the Set Properties of Custom Job dialog box

Item	Setting
Name ((1 to 8-byte character string)) <<blank>>	Specify any name for the custom job. This item is mandatory.
Comment ((0 to 40-byte character string)) <<blank>>	Specify any desired comment. The forward slash (/) and the space cannot be used in a comment.
Defining program	Specify the following definition program name: <i>JP1/FTP-installation-directory\FTS_CARD.EXE (fixed)</i> Specify the definition program on the host that is used to define jobs. If JP1/FTP is not installed on the host that is used to define jobs, copy the required files according to the description in (2) <i>Copying the definition program and configuring settings</i> .
Executing program	Specify the name of the following executable program: <i>JP1/FTP-installation-directory\FTS_JPCS.EXE (fixed)</i> This executable program must be located on the executing host. If the executable program exists in multiple JP1/AJS3 - Agents and their installation paths are different, specify \$xxx\$\name-of-executable-file (xxx: variable). In this case, you must register

Item	Setting
Executing program	(define) the variables at the JP1/AJS3 - Agent hosts. For details about the registration method, see the <i>JP1/Automatic Job Management System 3 Linkage Guide</i> . Note that the return value for the executable program is the same as that for the <code>ftstran</code> command. See the return value for this command.
Version	0600 (fixed)
Class	JP1FTP (fixed)
Job Type	PC

(2) Copying the definition program and configuring settings

If JP1/FTP is not installed on the host that is used to define jobs, perform the following steps:

1. Copy the following files to the machine on which JP1/AJS3 - View is installed.

The files must be copied to the following destinations:

- Copy destination for the definition program `FTS_CARD.EXE` and the DLL file `ftslang.dll`
The directory specified in **Defining program** in the Set Properties of Custom Job dialog box.
- Copy destination for the environment settings file `ftscard.ini`
`C:\Program Files\HITACHI\FTSFTP`
- Copy destination for the DLL files `Fts_card_*.dll` and `Fts_cmmsg_*.dll`
`C:\Program Files\HITACHI\FTSFTP\Lang`

2. In the environment setting file that was copied, configure the environment in which the definition program will run. The following table lists and describes the section, keys, and values that can be specified.

Table 5–2: Contents of the definition file (ftscard.ini)

Section	Key	Value	Description
[Language]	LangType	0x0409 0x0411 <<0x0411>>	Specifies the language to be used. <ul style="list-style-type: none"> • 0x0409: English. • 0x0411: Japanese.

5.1.3 Performing scheduled transmissions

To perform scheduled transmissions, you must first create a jobnet and then register the schedule in the jobnet.

(1) Creating a jobnet

To create a jobnet:

1. From the Windows **Start** menu, choose **Programs, JP1_Automatic Job Management System 3 - View, and Job System Management**, and then log in.
The JP1/AJS3 - View window is displayed.
2. From the **Edit** menu, choose **New**, and then **Jobnet** to create a jobnet.
3. Specify each setting and then click **OK**.

The following figure shows an example of the settings. For details, see the *JP1/Automatic Job Management System 3 Linkage Guide*.

Figure 5–3: Example of the settings in the Define Details - [Jobnet] dialog box

Define Details - [Jobnet]

Unit name: Data_Transmission

Comment:

Exec-agent:

Definition | Attributes

Concurrent exec. ☒ Disable ☐ Enable

No. logs to keep: 1

Priority: None

Time-out period: Use system settings

Schedule option ☒ Schedule skip ☐ Multi-schedule

Monitor jobnet ☐ Time-required-for-execution minutes

Exec. order control ☐ Yes ☒ No

Connection range ☒ Same service ☐ Other service

Connection host:

Connection service:

Jobnet connector:

Exec. order method ☐ Synchro ☒ Asynchro


OK Cancel Help

4. Double-click the created jobnet.

The Jobnet Editor window appears.

5. Select **Exclusive edit**.

6. From the icon list, drag the required job icon to the map area.

The JP1/FTP icon is the  icon on the **Custom Jobs** page.

The Define Details - [Custom Job] dialog box appears.

7. Specify each setting.

The figure below shows an example of the settings. For details, see the *JP1/Automatic Job Management System 3 Linkage Guide*.

Figure 5–4: Example of the settings in the Define Details - [Custom Job] dialog box

Define Details - [Custom Job]

Unit name

Data_Trans._Chicago_Branch

Comment

Exec-agent

Definition

Attributes

Priority

None

Standard output

Standard error

End judgment

Rule

Judgment by threshold

Warning

Abnormal

0

User name

Define detailed info.

Details...

OK

Cancel

Help

8. Click **Details**.

The Specify Transmission Card dialog box is displayed. This dialog box lists information about the transmission cards that have been registered in the Registration And Execution Of Transmission Requests dialog box or by the Operations-Manager Console.

9. Specify each setting and then click **OK**.

The following figure and table show an example of settings and the items in the Specify Transmission Card dialog box.

Figure 5–5: Example of the settings in the Specify Transmission Card dialog box

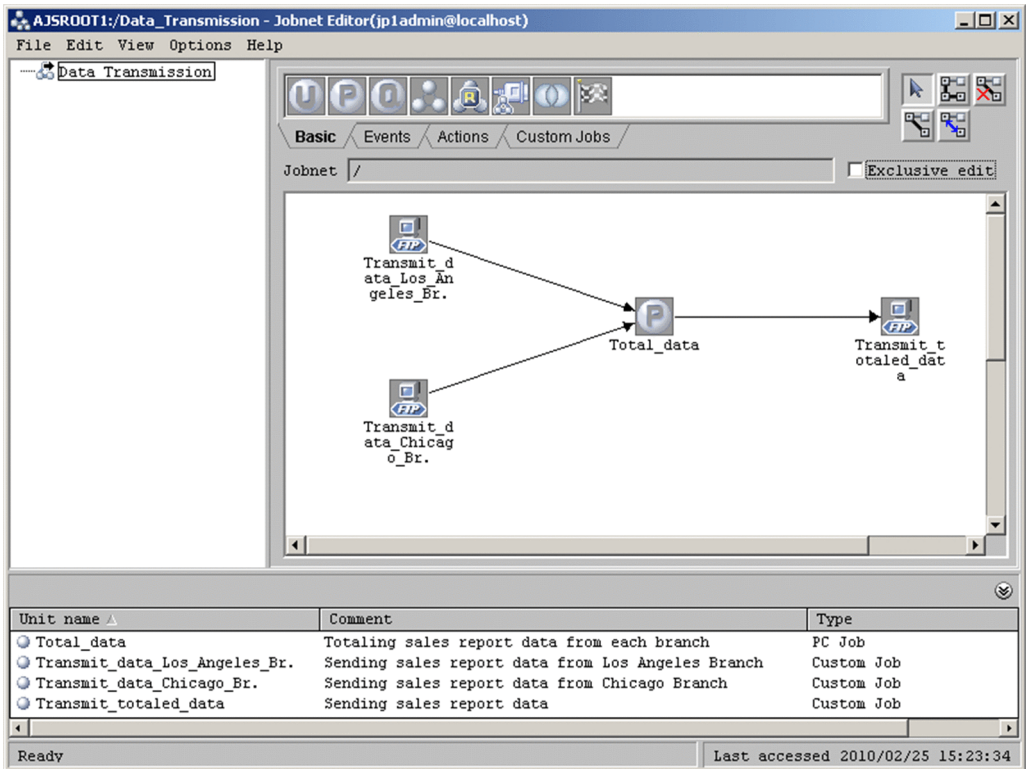
Table 5–3: Items in the Specify Transmission Card dialog box

Item	Description
Transmission card name	<p>Select a transmission card from the list and then click Select, or double-click the desired transmission card. A transmission card whose name contains a single-byte space cannot be specified.</p> <p>To check the contents of a transmission card, select the card and then click Details.</p> <p>The transmission cards displayed here are those set by JP1/FTP on the host that is used to define jobs. In the cases below, the list of applicable transmission cards will not be displayed. In such cases, enter a transmission card name.</p> <ul style="list-style-type: none"> The host used to define jobs differs from the host used to execute jobs. JP1/FTP is not installed.
Host name of client	<p>Specifies the host name (physical or logical host name) or IP address to be set as the FTP client's transmission source IP address.</p> <p>When you specify an IP address, you can specify an IPv4 or IPv6 address.</p> <p>If local IP address specification is enabled at the FTP client, the host name specified in this option becomes the FTP client's local IP address. If this option is omitted, the name of the FTP client's physical host is assumed.</p> <p>If local IP address specification is disabled at the FTP client, the address assigned automatically by the OS is used.</p> <p>For details about the definition for enabling local IP address specification at the FTP client, see 3.11 Using JP1/FTP in a multiple IP address environment.</p>
File to store transmission-end information ((0 to 259-byte character string))	<p>Specify the name of the file to which the transmission results are to be output. Express this file name as a full path. This item is optional.</p>
Output format	<p>Specify the format of the transmission results output file.</p> <p>If you specify binary, the serial data of the FTS_FTP_API_DATA_EX and FTS_FTP_API_RETDATA_EX structures is output.</p>

10. If necessary, set the job type as a PC job and associate the jobs.

The following figure shows an example of the settings.

Figure 5–6: Example of the jobnet settings



11. Close the Jobnet Editor window.

(2) Registering a schedule

To register a schedule:

1. From the list area of the JP1/AJS3 - View window, select the jobnet that is to be scheduled, and then from the **Edit** menu, choose **Schedule**.
The Schedule Settings dialog box is displayed.
2. Specify each setting and then click **OK**.
The figure below shows an example of the settings. For details, see the *JP1/Automatic Job Management System 3 Linkage Guide*.

Figure 5–7: Example of the settings in the Schedule Settings dialog box

Schedule Settings

Jobnet name: Data_Transmission

☐ Depends on upper-level jobnet Copy Upper

#	Linked	Type	Year/Month	Day
1	-	Absolute day ****/**		3 days before

Buttons: Add... Change... Copy... Delete

Valid term: ☐ Expiration date [] / [] / []

Options: ☐ Refer to a calendar of another job group
 Job group name: []
☐ Exclusive schedule
 Exclusive jobnet: []

Buttons: OK Cancel Help

- From the list area of the JP1/AJS3 - View window, select the jobnet to be registered for execution, and then from **Operations**, choose **Register for Execution**.
The Register for Execution dialog box is displayed.
- Specify each setting and then click **OK**.
The figure below shows an example of the settings. For details, see the *JP1/Automatic Job Management System 3 Linkage Guide*.

Figure 5–8: Example of the settings in the Register for Execution dialog box

Register for Execution

Jobnet name: Data_Transmission

Register method:

- ☒ Planned execution
- ☐ Fixed execution
- ☐ Immediate execution

Planned time passed when daemon starts:

- ☒ Execute immediately
- ☐ Execute from next time

Planned time passed when reg. for exe.:

- ☒ Execute immediately
- ☐ Execute from next time

OK Cancel Pass Info... Help

5.2 Linking to JP1/IM

You can link JP1/FTP to JP1/IM in order to use JP1/IM's Event Console window to perform centralized monitoring of the start and stop of the JP1/FTP service and the termination of transmissions (normal, warning, abnormal). It will also become possible to start JP1/FTP programs directly from JP1/IM's Tool Launcher window.

5.2.1 System configuration for linking to JP1/IM

Required programs

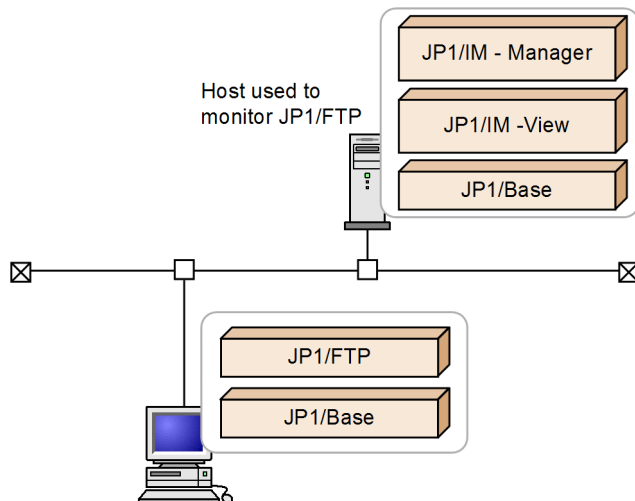
Install the following program on the computer where JP1/FTP is installed:

- JP1/Base

Additionally, install the following programs on the computer that is to be used to monitor JP1/FTP:

- JP1/IM - Manager
- JP1/IM - View
- JP1/Base

Figure 5–9: Example of a system configuration for linking to JP1/IM



5.2.2 Specifying the settings for linking to JP1/IM

To specify the settings for linking to JP1/IM:

1. In the Environment Definition dialog box, select **Link with JP1/IM**, and then click **OK**.
For details about the Environment Definition dialog box, see [3.1 Defining an environment for JP1/FTP](#).

5.2.3 Starting the services

Start the JP1/Base, JP1/IM, and JP1/FTP services. This subsection describes how to start services. If any JP1/FTP services are already running, stop and then restart them.

To start services:

1. From the Windows **Start** menu, choose **Control Panel, Administrative Tools**, and then **Services**.
2. Right-click the following services, and then from the displayed pop-up menu, choose **Start**:
 - JP1/Base event service: JP1/Base Event
 - JP1/IM service: JP1/IM-Manager
 - JP1/FTP service

The services start. Thereafter, JP1 events will be issued to report the status of the JP1/FTP service and the status of file transmissions.

When JP1 events cannot be issued

Issuance of JP1 events might fail depending on the status of the JP1/FTP service and the JP1/Base event service. If this happens, enter the following command at the command prompt to establish dependence:

```
ftsdpend.exe /D BASE
```

To release the dependence, enter the following command at the command prompt:

```
ftsdpend.exe /I BASE
```

5.2.4 Monitoring transmission results by JP1/IM

To monitor transmission results in the Event Console window of JP1/IM:

1. From the Windows **Start** menu, choose **Programs, JP1_Integrated Management - View**, and then **Integrated View**.
The Login window is displayed.
2. In the Login window, enter the user name, password, and name of the connected host.
3. Click **OK**.

The Event Console window is displayed.

For the list of JP1 events that are output by JP1/FTP and details about their attributes, see [D. JP1 Events](#).

6

Commands

This chapter describes the commands provided by JP1/FTP.

List of commands

The following table lists and describes the commands supported by JP1/FTP.

Table 6–1: Commands supported by JP1/FTP

Function	Command name
Executes transmission	<code>ftstran</code>
Registers, changes, deletes, and displays transmission information	<code>ftsregc</code>
Displays log information	<code>ftshistory</code>
Saves definition information	<code>ftssave</code>
Recovers definition information	<code>ftsload</code>

Details of commands

Storage location for commands:

```
JP1/FTP-installation-directory
```

The default is as follows:

```
OS-installation-drive:\Program Files(x86)\Hitachi\FTSFTP
```

ftstran - executes transmission

Format

```
ftstran transmission-card-name[/L file-name[/N file-name[/E file-name[/M  
[B|T]][/H host-name][transmission-information-option transmission-option-  
parameter]
```

Function

The `ftstran` command executes file transmission based on the information in a specified transmission card (Select Card method of file transmission) or by modifying information in a specified transmission card (Enter Information method of file transmission).

This command can be executed with the general user privilege.

Arguments

transmission-card-name ((1 to 20-byte character string))

Specifies the name of a transmission card that has been registered using **Transmission Regist. & Exe.**

/L file-name ((1 to 259-byte character string)) and ((1 to 255-character character string))

Specifies the name of the file to which the following log information is output when the `ftstran` command terminates:

Command termination time, return value, message, transmission card name, local file name, remote file name

Specify a file for which the user who executes the command has the write privilege. If this option is omitted, no log information is output.

If you specify a relative path for the file name, the command assumes the directory relative to the command execution directory.

If the size of the file exceeds 1 megabyte, *file-name* is renamed as *file-name_old*. If *file-name_old* already exists, the existing file is deleted before *file-name* is renamed as *file-name_old*.

The number of logs that can be stored in the file is as follows:

$1 \text{ MB} \div (\text{length of transmission card name} + \text{length of local file name} + \text{length of remote file name} + 122) + 1$

/N file-name ((1 to 259-byte character string))

Specifies the name of the file to which the results are output when the transmission terminates normally. Specify a file for which the user who executes the command has the write privilege. If this option is omitted, transmission results are not output when the transmission terminates normally.

If you specify a relative path for the file name, the command assumes the directory relative to the command execution directory.

If a file with the same name exists, it is overwritten.

/E file-name ((1 to 259-byte character string))

Specifies the name of the file to which the results are output when the transmission terminates abnormally. Specify a file for which the user who executes the command has the write privilege. If this option is omitted, transmission results are not output when the transmission terminates abnormally.

If you specify a relative path for the file name, the command assumes the directory relative to the command execution directory.

If a file with the same name exists, it is overwritten.

/M [B|T]

Specifies the output format.

- B: Binary format (data consisting of consecutive FTS_FTP_API_DATA_EX and FTS_FTP_API_RETDATA_EX structures)
- T: Text format

/H host-name ((1 to 256-byte character string))

Specifies the host name (physical or logical host name) or IP address to be set as the transmission source IP address of the FTP client. When you specify an IP address, you can specify an IPv4 or IPv6 address.

If you have enabled specification of the FTP client's local IP address, the value specified in this option becomes the FTP client's local IP address. If you omit this option, the address of the FTP client's physical host is assumed.

If you have disabled specification of the FTP client's local IP address, the address that is assigned automatically by the OS becomes the FTP client's local IP address.

For details about how to enable specification of the FTP client's local IP address, see [3.11 Using JPI/FTP in a multiple IP address environment](#).

transmission-information-option transmission-option-parameter

Specifies desired options in order to modify some of the transmission information on the specified transmission card (Enter Information method of file transmission). For details about the transmission information options, see [ftsregc - registers, changes, deletes, and displays transmission information](#) in this chapter. For details about the transmission option parameters for the transmission information options, see [3.4.1 Registering transmission information onto a transmission card](#).

Notes:

- As a transmission information option, you can specify a single-file or multiple-file transmission when receiving transmissions.
Specify AUTO when sending transmissions.

Return values (decimal number)

0	Normal termination.
10XXXXX	Normal termination with a warning due to an open error on the transmission-end information storage file. The CreateFile function's extended error information is set in XXXXX.
11XXXXX	Normal termination with a warning due to an output error on the transmission-end information storage file. The WriteFile function's extended error information is set in XXXXX.

12XXXXX	Normal termination with warning due to a JP1/FTP connection release error. The last byte of the <code>fts_ftp_close</code> function's extended error information is set in XXXXX.
1300000	Abnormal termination due to unacquired card information.
50XXXXX	Abnormal termination due to an error in <code>fts_ftp_open_ex()</code> . The last byte of the <code>fts_ftp_open_ex</code> function's extended error information is set in XXXXX.
51XXXXX	Abnormal termination due to an error in <code>fts_ftp_syn_request_ex()</code> . The last byte of the <code>fts_ftp_syn_request_ex</code> function's extended error information is set in XXXXX.
52XXXXX	Abnormal termination due to an error in <code>WSAStartup()</code> . The <code>WSAStartup</code> function's extended error information is set in XXXXX.
9000000	Abnormal termination of transmission.
9000001	Abnormal termination due to an argument specification error.
9900000	Abnormal termination (logical error).

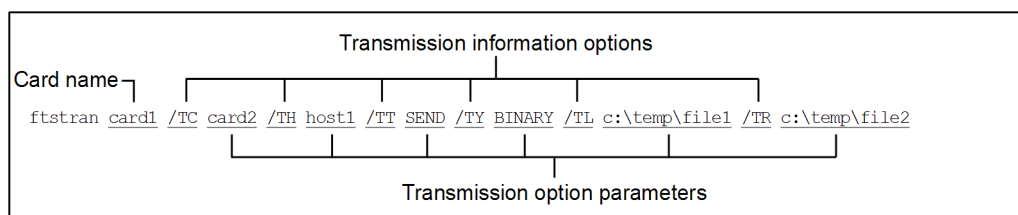
For details about the messages that are displayed, see [8.3.1 Messages displayed during execution of the `ftstran` command](#).

Usage examples

- Example of the Select Card method of file transmission:

```
ftstran card1
Card name
```

- Example of the Enter Information method of file transmission:



This example changes the following transmission information on `card1` and then executes transmission:

- `/TC`: The name for the new card is `card2`.
- `/TH`: The connection-target host name is `host1`.
- `/TT`: The send/receive type is `SEND`.
- `/TY`: The transmission mode is `BINARY`.
- `/TL`: The local file name is `c:\temp\file1`.
- `/TR`: The remote file name is `c:\temp\file2`.

ftsregc - registers, changes, deletes, and displays transmission information

Format

Registering:

```
ftsregc /N [transmission-card-name] [transmission-information-option  
transmission-option-parameter]
```

Changing:

```
ftsregc /C transmission-card-name [transmission-information-option  
transmission-option-parameter]
```

Deleting:

```
ftsregc /D transmission-card-name
```

Displaying:

```
ftsregc /L transmission-card-name
```

Function

The `ftsregc` command registers, changes, deletes, or displays transmission information.

Arguments

`/N [transmission-card-name] [transmission-information-option transmission-option-parameter]`

There are two ways to register transmission information. One is by registering new transmission information that has been set on a transmission card. The other is by using an existing transmission card as a model and editing its contents in order to register it as a separate transmission card.

- Registering new transmission information onto a transmission card
`ftsregc /N [transmission-information-option transmission-option-parameter]`
This method creates new transmission information based on the information specified with the transmission information options. Among the available transmission information options, you must always specify `/TC`, `/TH`, `/TU`, `/TT`, `/TY`, `/TL`, and `/TR`. You must use the `/TC` transmission information option to specify a name for the transmission card.
- Registering transmission information using an existing transmission card
`ftsregc /N [transmission-card-name] [transmission-information-option transmission-option-parameter]`
This method specifies the name of a transmission card to use as a model and then specifies transmission information options to change. You must specify in `/TC` a name for the new transmission card that you are registering.

The table below lists and describes the transmission information options.

Table 6–2: Transmission information options

Option name	Transmission option parameter	Value
<code>/TC</code>	Card name	((1 to 20 bytes))
<code>/TH</code>	Connection-target host name	((1 to 256 bytes))

Option name	Transmission option parameter	Value
/TP	Connection-target port number	((1 to 65,535))
/TU	Login user name	((1 to 50 bytes))
/TW	Login password	((1 to 50 bytes))
/TT	Send/receive type: <ul style="list-style-type: none"> SEND: Sends files (overwrite). RECV: Receives files. APPE: Sends files (append). 	SEND RECV APPE
/TY	Transmission mode: <ul style="list-style-type: none"> ASCII: Transmits files in the ASCII mode. BINARY: Transmits files in the binary mode. 	ASCII BINARY
/TM	Compression mode: <ul style="list-style-type: none"> STREAM: Transmits files without compressing them. COMPRESS: Compresses files during transmission. 	STREAM COMPRESS
/TK	Size check: <ul style="list-style-type: none"> CHECK: Checks the size. UNCHECK: Does not check the size. 	CHECK UNCHECK
/TL	Local file name	((1 to 259 bytes))
/TR	Remote file name	((1 to 259 bytes))
/TS	Name of the program to start when transmission ends normally	((1 to 259 bytes))
/TF	Name of the program to start when transmission ends abnormally	((1 to 256 bytes))
/TX	FTP command	((1 to 300 bytes))
/TO	Comment	((1 to 80 bytes))
/TA	Single-file or multiple-file transmission during reception: <ul style="list-style-type: none"> AUTO: Switches automatically between single-file transmission and multiple-file transmission. MULTIPLE: Transmits multiple files. SINGLE: Transmits a single file. 	AUTO MULTIPLE SINGLE
/TSS	Use FTPS <ul style="list-style-type: none"> CHECK: Uses FTPS. UNCHECK: Does not use FTPS. 	CHECK UNCHECK
/TSE	Check the expiration date of the server certificate <ul style="list-style-type: none"> CHECK: Checks the expiration date of the server certificate. UNCHECK: Does not check the expiration date of the server certificate. 	CHECK UNCHECK
/TSA	Path to the CA certificate	((1 to 259 bytes))
/TSR	Path to the CRL	((0 to 259 bytes))

For details about each transmission option parameter, see [3.4.1 Registering transmission information onto a transmission card](#).

/C card-name [transmission-information-option transmission-option-parameter]

Changes from the specified card the transmission information that is specified by the transmission information options.

/D *card-name*

Deletes the transmission information identified by the specified card name.

/L *card-name*

Displays the transmission information for the specified card.

Notes:

- As a transmission information option, you can specify a single-file or multiple-file transmission when receiving transmissions. Specify `AUTO` when sending transmissions.
- Do not execute the `ftsregc` command so that multiple instances are running at the same time. If you execute multiple instances of the command at the same time, an error will occur, and even if an error message is not output, you might not get the expected results. However, when displaying transmission information, multiple instances of the `ftsregc` command can be executed at the same time.

Return values

0	Normal termination
6100001	Omission of card name specification during registration
6100002	Omission of remote host name specification during registration
6100003	Omission of login user name specification during registration
6100004	Omission of send/receive type specification during registration
6100005	Omission of transmission mode specification during registration
6100006	Omission of local file name specification during registration
6100007	Omission of remote file name specification during registration
6100008	Abnormal termination when an existing card name is specified
6100009	Omission of card name specification during registration
6100010	Abnormal termination during registration of card information
6200001	Omission of card name specification during change
6200002	Abnormal termination during acquisition of card information before change
6200003	Abnormal termination during acquisition of card information after change
6200004	Abnormal termination during deletion of card information before change
6200005	Abnormal termination during change of card information
6300000	Abnormal termination when <code>ftsregc /D</code> is specified
6400000	Abnormal termination when <code>ftsregc /L</code> is specified
6900000	Command line syntax error
9000001	Abnormal termination common to <code>ftsregc</code>
9900001	Abnormal termination (not executed by the administrator)

For details about the messages that are displayed, see [8.3.2 Messages displayed during execution of the `ftsregc` command](#).

ftshistory - displays log information

Format

```
ftshistory
```

Function

The `ftshistory` command displays log information according to the output format defined by a format file.

This command uses the same format file as is used with the function for outputting displayed log information as text.

Return values (decimal number)

0	Normal termination
6400000	Log information display error
9000001	Abnormal termination due to an argument specification error
9900001	Abnormal termination (not executed by the administrator)

For the messages that are displayed, see [8.3.3 Messages displayed during execution of the `ftshistory` command](#).

ftssave - saves definition information

Format

```
ftssave file-name [/E] [/U] [/A] [/T]
```

Function

The `ftssave` command saves definition information to a specified file.

Arguments

file-name

Specifies a name for the file into which the information is saved. The permitted name is from 1 to 259 bytes of characters. If a relative path is specified, the location relative to the command execution path is assumed.

/E

Saves the environment settings.

/U

Saves the user-to-login settings.

/A

Saves the auto-start program settings.

/T

Saves the transmission settings.

Notes

- If `/E`, `/U`, `/A`, and `/T` are all omitted, all definition information is saved.
- This command does not support specification of a comment.
- If the specified file already exists, the command terminates abnormally.
- If the information to save cannot be found, the command terminates normally with a warning. If there is no information to save in the specified definition information, the command executes save processing with no definition information. In these cases, definition information can be specified for recovery, but nothing will be registered.
- Any message issued by this command is also output to the event log.

Return values

0	Normal termination
1	Normal termination with a warning
2	Abnormal termination

For the messages that are displayed, see [8.3.5 Messages displayed during execution of the `ftssave` command](#).

ftslload - recovers definition information

Format

```
ftslload file-name [/M[N|D]] [/E] [/U] [/A] [/T]
```

Function

The `ftslload` command recovers the saved definition information and defines an environment for JP1/FTP.

Arguments

file-name

Specifies the name of the file to recover. The permitted name is from 1 to 259 bytes of characters. If a relative path is specified, the location relative to the command execution path is assumed.

/M[N|D]

Specifies the recovery method:

- N: Do not delete the original information.
- D: Delete the original information.

/E

Recovers the environment settings.

/U

Recovers the user-to-login settings.

/A

Recovers the auto-start program settings.

/T

Recovers the transmission settings.

Notes:

- If `/E`, `/U`, `/A`, and `/T` are all omitted, all definition information is recovered.
- If the specified definition information is not in the specified file, the command recovers only the definition information contained in the file.
- If auto-start program registration information is to be recovered, but there is no corresponding user, the command terminates normally with a warning.
- If the specified file contains none of the specified definition information, the command terminates abnormally.
- Any message issued by this command is also output to the event log.

Return values

0	Normal termination
1	Normal termination with a warning

2	Abnormal termination
---	----------------------

For the messages that are displayed, see [8.3.4 Messages displayed during execution of the ftsload command](#).

7

API Library

This chapter explains how to use the JP1/FTP API library, which is used for linking JP1/FTP to user programs. It also provides library usage examples and details of functions.

How to use the library

You use the JP1/FTP API library when you use the file transmission function of JP1/FTP from a user program.

The JP1/FTP API library enables you to do the following:

- Register transmission requests from a single user program to multiple JP1/FTPs that are running on different hosts (or on the same host)
- Select the transmission type when you register transmission requests:
 - Synchronous type: Waits until a transmission is completed and the termination result is obtained.
 - Asynchronous type: Performs registration only and does not wait for the termination results (obtains the termination results later).

Prerequisites for using the functions

To use the functions provided by JP1/FTP, you need the following:

- JP1/FTP API library
- Compiler: Visual Studio

The following languages are supported for user programs:

- C
- C++

The JP1/FTP API library requires the following compilers:

Table 7–1: Compilers required by the JP1/FTP API library

Compiler	Type	Header file	Import library
Visual Studio 2012	32-bit	apihead.h	FTSFTP110.lib
	64-bit	apihead.h	FTSFTP110_x64.lib
Visual Studio 2013	32-bit	apihead.h	FTSFTP120.lib
	64-bit	apihead.h	FTSFTP120_x64.lib

For details on the storage locations of the header file and import library, see [A. List of Files and Directories](#). You can copy the header file and import libraries to the environment in which JP1/FTP is not installed to build a user program. The OSs under which Visual Studio itself can be installed depend on the Visual Studio specifications.

Setting up an environment

Setting services

Set the JP1/FTP client's service name as `ftsc`. For details, see [2.2.3 Setting the port numbers](#).

Setting hosts

Set the host name and IP address of the host on which the client's JP1/FTP program is running. Specify this host name in the connection information structure and the transmission information structure.

Add the following line to `OS-installation-directory\system32\drivers\etc\HOSTS`:

xxx.xxx.xxx.xxx

yyyyyy

Legend:

xxx.xxx.xxx.xxx: IP address

yyyyyy: Host name

Coding

Specifying information for establishing a connection with JP1/FTP

To establish a connection with the JP1/FTP Client service, specify the address of the connection information structure in the argument of `fts_ftp_open_ex()`.

- Connection information structure

```
typedef struct _FTS_FTP_API_CONN_DATA {
    char hostname[256+1]; /* Client host name */
    int priority;          /* IP version to be given priority */
    char reserve[1784];    /* Reserved area */
} FTS_FTP_API_CONN_DATA;
```

- Description of the connection information structure members

- `hostname`

Specify the host name or IP address of the host on which the JP1/FTP Client service is running. When you specify an IP address, you can specify an IPv4 or IPv6 address. If a null value is specified, the local host name (the physical host name returned by the OS's `hostname` command) is assumed.

If specification of a local IP address at the FTP client is enabled, the value specified in this argument becomes the local IP address of the FTP client.

If a null value is specified, the physical host of the FTP client is assumed.

If specification of a local IP address at the FTP client is disabled, the local IP address of the FTP client is automatically assigned by the OS. For details about the definition that enables specification of a local IP address at the FTP client, see *3.11 Using JP1/FTP in a multiple IP address environment*.

- `priority`

Specifies the Internet protocol version to be given priority.

`FTS_AF_INET`: IPv4 is given priority.

`FTS_AF_INET6`: IPv6 is given priority.

In all other cases, `FTS_AF_INET` is assumed.

- `reserve`

Reserved area. Initialize the area by specifying `\0`.

Note

Make sure that a `char`-type variable value ends with `\0`.

Specifying the transmission information

To register a file transmission request, you set the registered transmission card name and the address of the transmission information structure in the arguments of `fts_ftp_syn_request_ex()` and `fts_ftp_asyn_request_ex()`.

- Using the card name to register transmission requests:

You can register a transmission request by specifying a transmission card name registered using **Registration And Execution Of Transmission Requests**.

- Using the transmission information structure to specify transmission information:
You can register a transmission request by specifying the information needed for transmission.
- Transmission information structure

```
typedef struct _FTS_FTP_API_DATA_EX {
    char cardname[20+1]; /* Card name */
    char host[256+1]; /* Remote host name */
    unsigned int portnum; /* Port number */
    char username[50+1]; /* Remote user name */
    char password[50+1]; /* Password */
    int type; /* Transmission mode */
    int mode; /* Compression mode */
    int cmd; /* Send/receive type */
    char quote[300+1]; /* FTP command */
    char localname[260+1]; /* Local file name */
    char remotename[260+1]; /* Remote file name */
    char end_program[260+1]; /* Name of program to start at normal end */
    char abend_program[260+1]; /* Name of program to start at abnormal
end */
    char comment[80+1]; /* Comment */
    int fsize; /* Size check */
    int ftps; /* Use FTPS */
    int scertval; /* Check the expiration date of the server
certificate */
    char cacertpath[260+1]; /* Path to the CA certificate */
    char crlpath[260+1]; /* Path to the CRL */
    char reserve[708]; /* Reserved area */
} FTS_FTP_API_DATA_EX;
```

- Description of the transmission information structure members
 - cardname
Specifies the card name.
 - host
Specifies the FTP host name: ftp>open *aaaa*
 - portnum
Specifies the FTP port number: ftp>open *aaaa bbbb*
 - username
Specifies the login name: ftp>user *aaaa*
 - password
Specifies the password.
 - type
Specifies the transmission mode.
FTS_TYPE_A: Interprets data as being in ASCII code and then sends it (ftp>ascii).
FTS_TYPE_I: Interprets the data as an image and then sends it (ftp>binary).
 - mode
Specifies whether to use compressed transmission.

FTS_MODE_S: Does not use compressed transmission.

FTS_MODE_C: Uses compressed transmission.

- cmd

Specifies the type of transmission.

By using OR to specify single/multiple-file transmission, you can specify a combination of single-file transmission and multiple-file transmission. Note that this specification is applicable to reception only.

Transmission types:

FTS_CMD_SEND (send): ftp>put *aaaa bbbb*

FTS_CMD_RECV (receive): ftp>get *cccc dddd*

FTS_CMD_APPE (send with append): ftp>append *eeee ffff*

Single/multiple-file transmission:

FTS_MLT_AUTO: Switch automatically between single-file and multiple-file transmission. This is the default.

Specify FTS_MLT_AUTO when FTS_CMD_SEND or FTS_CMD_APPE is specified as the transmission type.

FTS_MLT_MULTIPLE: Perform multiple-file transmission.

FTS_MLT_SINGLE: Perform single-file transmission.

FTS_MLT_AUTO switches transmission automatically as follows:

When sending

The function checks whether * or ? is used in the local file name. If * or ? is used, multiple-file transmission is used. If neither of them is used, single-file transmission is used.

When receiving

The function checks whether * or ? is used in the remote file name. If * or ? is used, multiple-file transmission is used. If neither of them is used, single-file transmission is used.

Example

Receiving a single file:

```
cmd = FTS_CMD_RECV | FTS_MLT_SINGLE;
```

- mode

Specifies compressed transmission.

FTS_MODE_S: Does not perform compressed transmission.

FTS_MODE_C: Performs compressed transmission.

- quote

Specifies the FTP command to execute.

This structure member is a character string consisting of commands, such as CWD and SITE, delimited by semicolons (;) (the character string must end with \0).

Only commands that do not establish a data connection can be specified. Whether a command can be executed by the FTP server depends on the FTP server.

- localname

Specifies the local file name.

Examples

```
ftp>put aaaa bbbb
```

```
ftp>get cccc dddd
```

- remotename

Specifies the remote file name.

Examples

```
ftp>put aaaa bbbb
```

```
ftp>get cccc dddd
```

- `end_program`

Specifies the full path name of the program to start when transmission ends normally.

- `abend_program`

Specifies the full path name of the program to start when transmission ends abnormally.

- `comment`

Specifies any character string.

- `fsize`

Specifies whether to check the file size after transmission.

`FTS_FSIZE_TRUE`: Checks the size.

`FTS_FSIZE_FALSE`: Does not check the size.

- `ftps`

Specifies whether to use FTPS.

`FTS_FTPS_TRUE`: Uses FTPS.

`FTS_FTPS_FALSE`: Does not use FTPS.

- `scertval`

Specifies whether to check the expiration date of the server certificate.

`FTS_SCVAL_TRUE`: Checks the expiration date of the server certificate.

`FTS_SCVAL_FALSE`: Does not check the expiration date of the server certificate.

- `cacertpath`

Specifies a full path to the CA certificate file.

- `crlpath`

Specifies a full path to the CRL file.

- `reserve`

Reserved area. Initialize the area by specifying `\0`.

Note

Make sure that a `char`-type variable value ends with `\0`.

Obtaining transmission-end information

You can obtain the termination information for transmission requests registered by `fts_ftp_syn_request_ex()` and `fts_ftp_asyn_request_ex()`.

- When `fts_ftp_syn_request_ex()` is used to register requests:

Specify the address of the transmission-end information structure in the fourth argument of `fts_ftp_syn_request_ex()`.

- When `fts_ftp_asyn_request_ex()` is used to register requests:

Specify the address of the transmission-end information structure in the second argument of `fts_ftp_event_ex()`.

- Transmission-end information structure

```

typedef struct _FTS_FTP_API_RETDATA_EX {
    /* Data when transmission was successful */
    int trans_status;          /* Transmission end status:
                                success (TRANS_SUCCESS) */
                                /* Transmission end status:
                                failure (TRANS_FAILURE) */

    char cardname[20+1];       /* Card name */
    unsigned long trno;        /* Transmission number */
    unsigned long trcno;       /* Connection number */

    /* Data when transmission was successful */
#ifdef FTS_API_64BIT
    unsigned __int64 trans_size; /* Transmitted data size */
    unsigned __int64 trans_size_comp; /* Transmitted data size
                                        after compression */
#else
    unsigned long trans_size;    /* Transmitted data size */
    unsigned long trans_size_comp; /* Transmitted data size
                                    after compression */
#endif

    /* Data when transmission failed */
    int ab_kind;                /* System call error
                                (FTS_ERR_SYSTEM) */
                                /* Logical error
                                (FTS_ERR_LOGIC) */
                                /* Protocol error
                                (FTS_ERR_PROTOCOL) */
                                /* SSL communication error
                                (FTS_ERR_SSL) */

    char ab_place[8];          /* Location of error */
    char ab_func[32];          /* Name of module resulting
                                in error */

    char ab_system[32];        /* System call name */
    int ab_syskind;            /* System call type */
                                /* Win32 API (FTS_SYSKIND_WIN32) */
                                /* C runtime (FTS_SYSKIND_CRUNTIME) */
                                /* WinSock API (FTS_SYSKIND_WINSOCK) */

    unsigned long ab_errno;    /* Error number */
    char ab_promes[256];      /* Protocol message (error) */

#ifdef FTS_API_64BIT
    /* Data when transmission of more than 4 gigabytes of */
    /* data was successful */
    DWORD trans_size_Low;      /* Transmitted data size (value
                                of the trailing 32 bits). */
    LONG trans_size_High;      /* Transmitted data size (value
                                of the leading 32 bits). */
    DWORD trans_size_comp_Low; /* Transmitted data size
                                after compression (value
                                of the leading 32 bits). */
    LONG trans_size_comp_High; /* Transmitted data size
                                after compression (value
                                of the trailing 32 bits). */
#endif

    int ab_sslerno;            /* SSL communication error number */

```



```
char reserve[1664];      /* Reserved area */
} FTS_FTP_API_RETDATA_EX;
```

- Description of transmission-end information structure members

- trans_status

Returns one of the following values indicating the termination status of transmission:

TRANS_SUCCESS: Normal termination

TRANS_FAILURE: Abnormal termination

- cardname

Returns the transmission card name.

- trno

Returns the transmission number.

- trcno

Returns the connection number.

- trans_size (Applicable to normal termination only)

Transmitted data size

- trans_size_comp (Applicable to normal termination only)

Transmitted data size after compression

- ab_kind (Applicable to abnormal termination only)

Returns the error type:

FTS_ERR_SYSTEM: System call error

FTS_ERR_LOGIC: Logical error

FTS_ERR_PROTOCOL: Protocol error

FTS_ERR_SSL: SSL communication error

- ab_place (Applicable to abnormal termination only)

Returns the location of the error.

- ab_func (Applicable to abnormal termination only)

Returns the name of module resulting in the error.

- ab_system (Applicable to abnormal termination only)

Returns the system call name.

- ab_syskind (Applicable to abnormal termination only)

Returns the system call type:

FTS_SYSKIND_WIN32: Win32 API

FTS_SYSKIND_CRUNTIME: C runtime

FTS_SYSKIND_WINSOCK: WinSock API

- ab_errno (Applicable to abnormal termination only)

Returns the system call error number.

- ab_promes (Applicable to abnormal termination only)

Returns the protocol message sent from the FTP server.

- trans_size_Low (Applicable to normal termination only)

Returns the value of the trailing 32 bits of the transmitted data size.

- `trans_size_High` (Applicable to normal termination only)
Returns the value of the leading 32 bits of the transmitted data size.
- `trans_size_comp_Low` (Applicable to normal termination only)
Returns the value of the trailing 32 bits of the transmitted data size after compression.
- `trans_size_comp_High` (Applicable to normal termination only)
Returns the value of the leading 32 bits of the transmitted data size after compression.
- `ab_sslerno` (Applicable to abnormal termination only)
Returns the SSL communication error number.
- `reserve`
Reserved area.
- Notes about coding
Before and after you use the JP1/FTP API library functions, make sure that you call the following functions:

- Before calling

```
WSAStartup() : Winsock2 library
```

- After calling

```
WSACleanup() : Winsock2 library
```

If you do not call these functions, the library functions will not run correctly. For details about how to use these functions, see the MSDN documentation.

The two parameters `trans_size_Low` and `trans_size_High` are combined to form a single 64-bit value.

The two parameters `trans_size_comp_Low` and `trans_size_comp_High` are combined to form a single 64-bit value.

Compiling and linking

- If you are using the library for 64-bit, define `FTS_API_64BIT` in the definitions for the preprocessor.

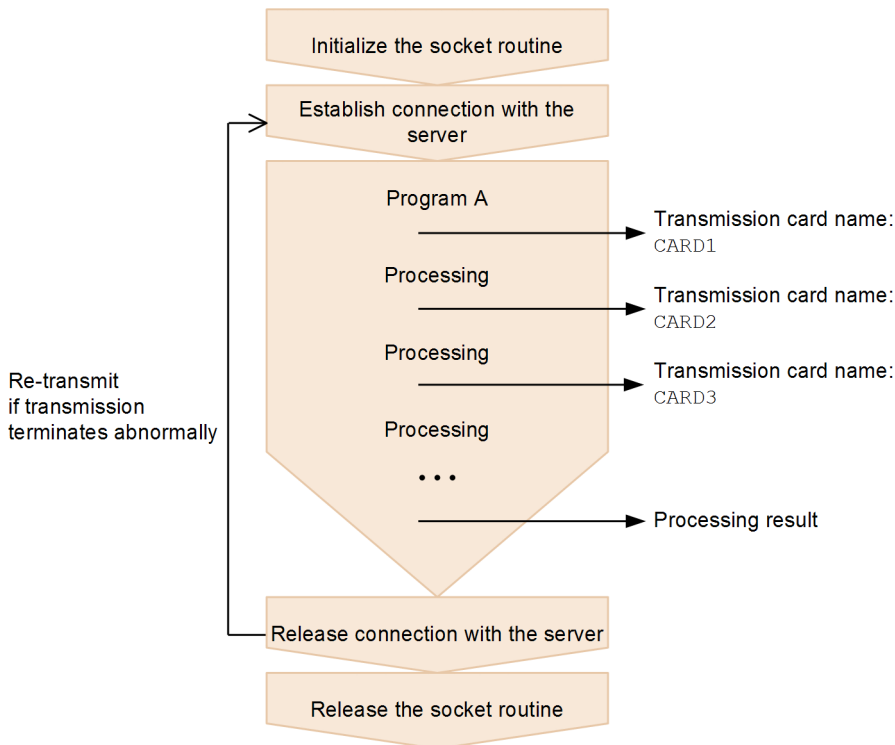
Notes about using libraries

- The following actions are not permitted:
 - Issuing multiple `fts_ftp_open_ex()` functions concurrently by multiple threads in a single process
 - Issuing multiple `fts_ftp_syn_request_ex()` or `fts_ftp_asyn_request_ex()` functions concurrently in a single `fts_ftp_open_ex()` function (issuing `fts_ftp_syn_request_ex()` or `fts_ftp_asyn_request_ex()` functions concurrently by multiple threads)
- If a wildcard character is specified, the transmission-end information that can be obtained is as follows:
When the wildcard transmission terminates normally: Transmission-end information for the last file transmitted
When the wildcard transmission terminates abnormally: Transmission-end information for the first file resulting in an error

Example of library usage

This sample program uses registered transmission cards (transmission card names: CARD1 through CARD3) to register asynchronous transmission requests and obtains the termination results.

Figure 7–1: Flowchart of sample program



```
/* **** */
/* Sample program: program to register an asynchronous */
/* transmission request and obtain the transmission */
/* termination results */
/* (This example uses a registered card) */
/* **** */
#include <apihead.h>
#include <windows.h>
#include <stdio.h>

#define CARD1 "card1"
#define CARD2 "card2"
#define CARD3 "card3"

#define FTS_EXECUTION 0
#define FTS_SUCCESS 1

#define FTS_MAX_RETRY 3

int main()
{
    FTS_FTP_API_DATA_EX data1, data2, data3;
    /* Transmission information structure */
    FTS_FTP_API_RETDATA_EX ret_data;
    /* End of transmission information structure */
    FTS_FTP_API_CONN_DATA con_data;
```

```

/* Connect information structure */

SOCKET sock;
WSADATA WSAData;
DWORD trno1, trno2, trno3;
DWORD status;
int flag1, flag2, flag3;
int err_num;
int i;

/*****
/* Initialize the socket routine
/* (This is required.)
*****/
status = WSASStartup( MAKEWORD(2,2), &WSAData );
if( status ) {
    /* Error */
    printf( "WSASStartup() error number = %d\n", status );
    return 1;
}

flag1 = FTS_EXECUTION;
flag2 = FTS_EXECUTION;
flag3 = FTS_EXECUTION;

for( i = 0; i <= FTS_MAX_RETRY; i++ ) {
    if( i == 0 ) {
        printf( "Transmission is executed. \n" );
    } else {
        printf( "Transmission is executed again.\n" );
    }

    memset( &data1, 0, sizeof(FTS_FTP_API_DATA_EX) );
    memset( &data2, 0, sizeof(FTS_FTP_API_DATA_EX) );
    memset( &data3, 0, sizeof(FTS_FTP_API_DATA_EX) );

    /*****
    /* Establish a connection with JP1/FTP
    *****/
    memset( &con_data, 0, sizeof(FTS_FTP_API_CONN_DATA) );
    con_data.priority = FTS_AF_INET;

    sock = fts_ftp_open_ex( &con_data );
    if( sock == INVALID_SOCKET ) {
        /* Error */
        err_num = WSAGetLastError();
        printf( "fts_ftp_open_ex() error!! error number = %d\n",
err_num );
        WSACleanup();
        return 1;
    }

    /*****
    /* Register the transmission request
    *****/
    if( flag1 == FTS_EXECUTION ) {
        if( !fts_ftp_asyn_request_ex( sock, CARD1, &data1, &trno1,
FTS_GET_RETURN ) ) {

```

```

        /* Error */
        err_num = WSAGetLastError();
        printf( "fts_ftp_request_ex(1) error!! error number = %d
\n", err_num );
    }
    if( flag2 == FTS_EXECUTION ) {
        if( !fts_ftp_asyn_request_ex( sock, CARD2, &data2, &trno2,
FTS_GET_RETURN ) ) {
            /* Error */
            err_num = WSAGetLastError();
            printf( "fts_ftp_request_ex(2) error!! error number = %d
\n", err_num );
        }
    }
    if( flag3 == FTS_EXECUTION ) {
        if( !fts_ftp_asyn_request_ex( sock, CARD3, &data3, &trno3,
FTS_GET_RETURN ) ) {
            /* Error */
            err_num = WSAGetLastError();
            printf( "fts_ftp_request_ex(3) error!! error number = %d
\n", err_num );
        }
    }

    /******
    /* Obtain the transmission termination results */
    /******
    while(1) {
        if( !fts_ftp_event_ex( sock, &ret_data ) ) {
            err_num = WSAGetLastError();
            if( err_num == FTS_API_ERROR_NODATA ) {
                /* Obtained all the transmission termination results */
                break;
            } else {
                /* Error */
                printf( "fts_ftp_event_ex error!! error number = %d\n",
err_num );

                fts_ftp_close( sock );
                WSACleanup();
                return 1;
            }
        }
        if( flag1 == FTS_EXECUTION ) {
            if( ret_data.trno == trno1 ) {
                /* Termination of CARD1 */
                if( ret_data.trans_status == TRANS_SUCCESS ) {
                    /* Transmission ends normally. */
                    printf( "CARD1 trnas success!!\n" );
                    flag1 = FTS_SUCCESS;
                } else {
                    /* Transmission ends abnormally. */
                    printf( "CARD1 trnas failure!!\n" );
                }
                continue;
            }
        }
        if( flag2 == FTS_EXECUTION ) {

```

```

        if( ret_data.trno == trno2 ) {
            /* Termination of CARD2 */
            if( ret_data.trans_status == TRANS_SUCCESS ) {
                /* Transmission ends normally. */
                printf( "CARD2 trnas success!!\n" );
                flag2 = FTS_SUCCESS;
            } else {
                /* Transmission ends abnormally. */
                printf( "CARD2 trnas failure!!\n" );
            }
            continue;
        }
    }
    if( flag3 == FTS_EXECUTION ) {
        if( ret_data.trno == trno3 ) {
            /* Termination of CARD3 */
            if( ret_data.trans_status == TRANS_SUCCESS ) {
                /* Transmission ends normally. */
                printf( "CARD3 trnas success!!\n" );
                flag3 = FTS_SUCCESS;
            } else {
                /* Transmission ends abnormally. */
                printf( "CARD3 trnas failure!!\n" );
            }
            continue;
        }
    }
}

/*****
/* Release the connection with JP1/FTP */
*****/
fts_ftp_close( sock );

    if( flag1 == FTS_SUCCESS && flag2 == FTS_SUCCESS && flag3 ==
FTS_SUCCESS ) {
        break;
    }
}
/*****
/* Release the socket routine. (Required) */
*****/
WSACleanup();

printf( "Transmission is ended. \n" );

return 0;
}

```

List of functions

The following table lists and describes the functions supported by the JP1/FTP API library.

Table 7–2: Functions supported by the JP1/FTP API library

Function	Function name
Establish connection with JP1/FTP	<code>fts_ftp_open_ex()</code>
Register transmission requests (synchronous)	<code>fts_ftp_syn_request_ex()</code>
Register transmission requests (asynchronous)	<code>fts_ftp_asyn_request_ex()</code>
Obtain the transmission-end results	<code>fts_ftp_event_ex()</code>
Cancel transmission	<code>fts_ftp_cancel()</code>
Release connection with JP1/FTP	<code>fts_ftp_close()</code>

Note

In addition to those listed above, the following functions are provided in order to maintain compatibility with earlier versions of JP1/FTP:

- `fts_ftp_open()`

Details of functions

Call the functions from a user program in the following order:

1. Establish connection with JP1/FTP by calling `fts_ftp_open_ex()`.
2. Set the transmission information in the transmission information structure and then call `fts_ftp_syn_request_ex()` (synchronous) or `fts_ftp_asyn_request_ex()` (asynchronous) to register transmissions. If you use `fts_ftp_syn_request_ex()`, you can obtain the result of each transmission upon termination of the function.
3. If you call `fts_ftp_asyn_request_ex()` in step 2, you can obtain transmission results by calling `fts_ftp_event_ex()`.
4. You can cancel the current transmission (server or client) by calling `fts_ftp_cancel()`. This does not require connection establishment with JP1/FTP.
5. Release connection with JP1/FTP by calling `fts_ftp_close()`.

The details of the functions provided in the following sections describe individual functions in the order they are called.

fts_ftp_open_ex() - establish connection with JP1/FTP

Format

```
#include <winsock2.h>
#include <apihead.h>

SOCKET fts_ftp_open_ex( FTS_FTP_API_CONN_DATA *condata )
```

Function

This function establishes connection with the JP1/File Transmission Server/FTP Client service.

Arguments

condata

Specifies the address of the connection information structure. JP1/FTP connects to the JP1/FTP Client service according to the connection information.

Notes

- Call this function before you call `fts_ftp_syn_request_ex()`, `fts_ftp_asyn_request_ex()`, and `fts_ftp_close()`.
- This function's return value is needed when you use other functions.
- If you wish to obtain the extended error information, do not call any function before you call the `WSAGetLastError` function. If you call another function before the `WSAGetLastError` function, the information might be lost.

Return values

Socket handler	Normal
INVALID_SOCKET	Abnormal

To obtain extended error information, call the `WSAGetLastError` function. The table below lists and describes the return values for the extended error information. For details about other errors, see the MSDN documentation.

Return value of extended error information (hexadecimal, decimal)	Description	Can be retrieved?
FTS_API_ERROR_NOTSTARTUP (0x2FFFFFF00, 805306112)	<code>WSAStartup()</code> has not been called.	No
FTS_API_ERROR_UNDEFFTHOST (0x2FFFFFF01, 805306113)	The specified host name is not defined in the <code>HOSTS</code> file.	No
FTS_API_ERROR_CONNREFUSED (0x2FFFFFF02, 805306114)	A connection request was rejected. The JP1/File Transmission Server/FTP Client service might not have been started.	No
FTS_API_ERROR_TIMEOUT (0x2FFFFFF03, 805306115)	A connection request to the JP1/File Transmission Server/FTP Client service resulted in a timeout. Connection processing in the JP1/File Transmission Server/FTP Client service might be taking too long or the system on which the JP1/File Transmission Server/FTP Client service is supposed to be running might be down.	Yes

Return value of extended error information (hexadecimal, decimal)	Description	Can be retried?
FTS_API_ERROR_UNREACH (0x2FFFFFF04, 805306116)	Routing to the host on which the JP1/File Transmission Server/FTP Client service is running might have failed.	No
FTS_API_ERROR_DISCONNECT (0x2FFFFFF05, 805306117)	A connection with the JP1/File Transmission Server/FTP Client service was released. If you want to register the transmission request again, you must start the process over from <code>fts_ftp_open_ex()</code> .	No
FTS_API_ERROR_MEMORY (0x2FFFFFF0B, 805306123)	Memory allocation failed.	No
FTS_API_ERROR_UNDEFTSSERV (0x2FFFFFF0C, 805306124)	The definition of the JP1/File Transmission Server/FTP Client (<code>ftsc</code>) is missing in the <code>SERVICES</code> file.	No
FTS_API_ERROR_MAXCONNECT (0x2FFFFFF0F, 805306127)	The permitted maximum number (64) of concurrent connections (issuances of <code>fts_ftp_open_ex()</code>) has been reached. No more connections can be established until another API releases connection (issues <code>fts_ftp_close()</code>).	Yes

fts_ftp_syn_request_ex() - register transmission requests (synchronous)

Format

```
#include <winsock2.h>
#include <apihead.h>

BOOL fts_ftp_syn_request_ex( SOCKET sock,
                           const char *cardname,
                           FTS_FTP_API_DATA_EX *data,
                           FTS_FTP_API_RETDATA_EX *retdata )
```

Function

This function registers a transmission request to JP1/FTP and returns the termination result when the transmission is terminated. You can specify the details for the transmission request by specifying a transmission information structure or the name of a registered transmission card. The termination result is returned to the transmission-end information structure. You can determine whether the transmission was successful by checking the `trans_status` member of the transmission-end information structure.

Arguments

sock

Specifies the return value of `fts_ftp_open_ex()`.

cardname

Specifies the name of a registered transmission card. The file transmission request is registered in accordance with the information on the transmission card.

data

Specifies the address of a transmission information structure.

If `NULL` is specified in *cardname*, the file transmission request is registered according to the information specified in *data*.

If the name of a registered transmission card is specified in *cardname*, the file transmission request is registered according to the information on the transmission card.

retdata

Specifies the address of a transmission-end information structure. It returns the termination result of transmission.

Notes

- Call this function after you have called `fts_ftp_open_ex()`.
- This function does not return control until the requested transmission is terminated.
- If you wish to obtain the extended error information, do not call any function before you call the `WSAGetLastError` function. If you call another function before the `WSAGetLastError` function, the information might be lost.

Return values

TRUE	Normal
FALSE	Abnormal. Registration of the transmission request or acquisition of the transmission termination result failed.

To obtain extended error information, call the `WSAGetLastError` function. The table below lists and describes the return values for the extended error information. For details about other errors, see the MSDN documentation.

Return value of extended error information (hexadecimal, decimal)	Description	Can be retried?
<code>FTS_API_ERROR_NOTSTARTUP</code> (0x2FFFFFF00, 805306112)	<code>WSAStartup()</code> has not been called.	No
<code>FTS_API_ERROR_DISCONNECT</code> (0x2FFFFFF05, 805306117)	A connection with the JP1/File Transmission Server/FTP Client service was released. To register the transmission request again, you must issue <code>fts_ftp_close()</code> and start the process over from <code>fts_ftp_open_ex()</code> .	No
<code>FTS_API_ERROR_NOTREADCARD</code> (0x2FFFFFF06, 805306118)	The specified card name cannot be referenced. The card might not have been registered correctly.	No
<code>FTS_API_ERROR_BADFORMAT</code> (0x2FFFFFF07, 805306119)	An address with an invalid data type was specified in an argument.	No
<code>FTS_API_ERROR_MAXPALTRANS</code> (0x2FFFFFF08, 805306120)	The maximum number of concurrent transmissions has been reached. Register the transmission request after another transmission is finished.	Yes
<code>FTS_API_ERROR_MEMORY</code> (0x2FFFFFF0B, 805306123)	Memory allocation failed.	No
<code>FTS_API_ERROR_NOTSOCK</code> (0x2FFFFFF0D, 805306125)	The return value of <code>fts_ftp_open_ex()</code> might not have been set in the first argument.	No
<code>FTS_API_ERROR_LOGIC</code> (0x2FFFFFF10, 805306128)	A logical conflict error occurred in API.	No

fts_ftp_asyn_request_ex() - register transmission requests (asynchronous)

Format

```
#include <winsock2.h>
#include <apihead.h>

BOOL fts_ftp_asyn_request_ex( SOCKET sock,
                             const char *cardname,
                             FTS_FTP_API_DATA_EX *data,
                             unsigned long *trno,
                             int get_return_flag )
```

Function

This function registers a transmission request to JP1/FTP, but does not wait for the transmission to terminate. You must use `fts_ftp_event_ex()` to obtain the termination result. You can define the transmission request by specifying a transmission information structure or the name of a registered transmission card. You can determine whether the transmission was successful by checking the `trans_status` member of the transmission-end information structure that is obtained by `fts_ftp_event_ex()`.

Arguments

sock

Specifies the return value of `fts_ftp_open_ex()`.

cardname

Specifies the name of a registered transmission card. The file transmission request is registered in accordance with the information on the transmission card.

data

Specifies the address of a transmission information structure.

If `NULL` is specified in *cardname*, the file transmission request is registered according to the information specified in *data*.

If the name of a registered transmission card is specified in *cardname*, the information on the transmission card is registered.

trno

Specifies the address at which the transmission number is stored.

This matches the transmission number in the transmission-end information that is obtained from log information or by `fts_ftp_event_ex()`.

get_return_flag

If you have specified `FTS_GET_RETURN`, you can obtain the transmission-end information by calling `fts_ftp_event_ex()`.

If you have specified `FTS_UNGET_RETURN`, the transmission-end information cannot be obtained.

Notes

- Call this function after you have called `fts_ftp_open_ex()`.
- If you want to obtain transmission-end information, call `fts_ftp_event_ex()` with `FTS_GET_RETURN` specified in the fifth argument. In this case, make sure that you issue `fts_ftp_event_ex()`. If `fts_ftp_event_ex()` is not issued, you might not be able to release the system resources (memory) because the transmission-end information remains in the process that issued the function or in JP1/FTP.
- If you do not want to obtain termination information, specify `FTS_UNGET_RETURN` in the fifth argument.

Return values

TRUE	Normal
FALSE	Abnormal. Registration of transmission request failed.

To obtain extended error information, call the `WSAGetLastError` function. The table below lists and describes the return values for the extended error information. For details about other errors, see the MSDN documentation.

Return value of extended error information (hexadecimal, decimal)	Description	Can be retrieved?
<code>FTS_API_ERROR_NOTSTARTUP</code> (0x2FFFFFF0, 805306112)	<code>WSAStartup()</code> has not been called.	No
<code>FTS_API_ERROR_DISCONNECT</code> (0x2FFFFFF5, 805306117)	A connection with the JP1/File Transmission Server/FTP Client service was released. To register the transmission request again, you must issue <code>fts_ftp_close()</code> and start the process over from <code>fts_ftp_open_ex()</code> .	No
<code>FTS_API_ERROR_NOTREADCARD</code> (0x2FFFFFF6, 805306118)	The specified card name cannot be referenced. The card might not have been registered correctly.	No
<code>FTS_API_ERROR_BADFORMAT</code> (0x2FFFFFF7, 805306119)	An address with an invalid data type was specified in an argument.	No
<code>FTS_API_ERROR_MAXPALTRANS</code> (0x2FFFFFF8, 805306120)	The maximum number of concurrent transmissions has been reached. Register the transmission request after another transmission is finished.	Yes
<code>FTS_API_ERROR_MEMORY</code> (0x2FFFFFFB, 805306123)	Memory allocation failed.	No
<code>FTS_API_ERROR_NOTSOCK</code> (0x2FFFFFFD, 805306125)	The return value of <code>fts_ftp_open_ex()</code> might not have been set in the first argument.	No
<code>FTS_API_ERROR_FTSMISS</code> (0x2FFFFFFE, 805306126)	An error occurred in the JP1/File Transmission Server/FTP Client service.	No
<code>FTS_API_ERROR_LOGIC</code> (0x2FFFFFF10, 805306128)	A logical conflict error occurred in API.	No

fts_ftp_event_ex() - obtain the transmission-end results

Format

```
#include <winsock2.h>
#include <apihead.h>

BOOL fts_ftp_event_ex( SOCKET sock, FTS_FTP_API_RETDATA_EX *retdata )
```

Function

This function obtains the termination results of a transmission that was registered by `fts_ftp_asyn_request_ex()`.

You can determine whether the transmission was successful by checking the `trans_status` member of the transmission-end information structure.

Arguments

sock

Specifies the return value of `fts_ftp_open_ex()`.

retdata

Specifies the address of a transmission-end information structure. It returns the termination result of transmission.

Notes

- Call this function after you have called `fts_ftp_open_ex()`.
- If transmission is not finished when this function is issued, the function waits until the transmission is finished.
- If you wish to obtain the extended error information, do not call any function before you call the `WSAGetLastError` function. If you call another function before the `WSAGetLastError` function, the information might be lost.

Return values

TRUE	Normal
FALSE	Abnormal. Acquisition of transmission-end information failed.

To obtain extended error information, call the `WSAGetLastError` function. The table below lists and describes the return values for the extended error information. For details about other errors, see the MSDN documentation.

Return value of extended error information (hexadecimal, decimal)	Description	Can be retried?
FTS_API_ERROR_NOTSTARTUP (0x2FFFFFF00, 8053306112)	<code>WSAStartup()</code> has not been called.	No
FTS_API_ERROR_DISCONNECT (0x2FFFFFF05, 8053306117)	A connection with the JP1/File Transmission Server/FTP Client service was released. To register the transmission request again, you must issue <code>fts_ftp_close()</code> and start the process over from <code>fts_ftp_open_ex()</code> .	No

Return value of extended error information (hexadecimal, decimal)	Description	Can be retrieved?
FTS_API_ERROR_BADFORMAT (0x2FFFFFF07, 8053306119)	An address with an invalid data type was specified in an argument.	No
FTS_API_ERROR_NODATA (0x2FFFFFF09, 8053306121)	There is no registered transmission request.	No
FTS_API_ERROR_NOTSOCK (0x2FFFFFF0D, 8053306125)	The return value of <code>fts_ftp_open_ex()</code> might not have been set in the first argument.	No
FTS_API_ERROR_LOGIC (0x2FFFFFF10, 8053306128)	A logical conflict error occurred in API.	No

fts_ftp_cancel() - cancel transmission

Format

```
#include <winsock2.h>
#include <apihead.h>

BOOL fts_ftp_cancel( int cs_flag, unsigned long trno )
```

Function

This function cancels the transmission (server or client) that is underway.

A canceled transmission terminates abnormally.

Arguments

cs_flag

Specifies the service type of the transmission that you wish to cancel.

If you specify FTS_CAN_SERVER, the function cancels the server's transmission.

If you specify FTS_CAN_CLIENT, the function cancels the client's transmission.

If you OR the two values, the function cancels both the server's and the client's transmissions.

trno

Specifies the transmission number of the transmission that you wish to cancel.

If you specify FTS_CAN_ALL, the function cancels all transmissions for the specified service.

Note

This function does not require connection establishment with JP1/FTP.

Return values

TRUE	Normal
FALSE	Abnormal. Cancellation of transmission failed.

To obtain extended error information, call the WSAGetLastError function. The table below lists and describes the return values for the extended error information. For details about other errors, see the MSDN documentation.

Return value of extended error information (hexadecimal, decimal)	Description	Can be retrieved?
FTS_API_ERROR_LOGIC (0x2FFFFFF10, 805306128)	A logical conflict error occurred in API.	No
FTS_API_ERROR_T_NOT_FOUND (0x2FFFFFF11, 805306129)	The specified transmission is not executing.	No

Return value of extended error information (hexadecimal, decimal)	Description	Can be retrieved?
FTS_API_ERROR_ARGUMENT (0x2FFFFFF12, 805306130)	An invalid argument value was specified.	No

fts_ftp_close() - release connection with JP1/FTP

Format

```
#include <winsock2.h>
#include <apihead.h>

BOOL fts_ftp_close( SOCKET sock )
```

Function

This function releases connection with JP1/FTP.

Arguments

sock

Return value of `fts_ftp_open_ex()`

Notes

- If `fts_ftp_open_ex()` has terminated normally, make sure that you call this function after all transmission registration processing is finished.
- If you wish to obtain the extended error information, do not call any function before you call the `WSAGetLastError` function. If you call another function before the `WSAGetLastError` function, the information might be lost.

Return values

TRUE	Normal
FALSE	Abnormal

To obtain extended error information, call the `WSAGetLastError` function. The table below lists and describes the return values for the extended error information. For details about other errors, see the MSDN documentation.

Return value of extended error information (hexadecimal, decimal)	Description	Can be retried?
FTS_API_ERROR_INVALIDSOCK (0x2FFFFFF0A, 805306122)	An invalid argument was specified. This might not be a return value of <code>fts_ftp_open_ex()</code> .	No
FTS_API_ERROR_LOGIC (0x2FFFFFF10, 805306128)	A logical conflict error occurred in API.	No

8

Messages

This chapter describes the messages that are issued by JP1/FTP.

8.1 Format of displayed messages

Some messages issued by JP1/FTP are displayed in Event Viewer, while others are displayed during command execution. This section describes the message formats and the formats of the message explanations in this chapter.

8.1.1 Message output formats

This subsection describes the messages for each output timing.

(1) Messages displayed in Event Viewer

To start Event Viewer, from the Windows **Start** menu, choose **Programs, Administrative Tools (Common)**, and then **Event Viewer**.

Type

The messages are of the following types:

- **Error:** Processing is canceled.
- **Warning:** Processing continues after the message is displayed.
- **Information:** Provides information about system processing results.

Category

This information is displayed in the format *XXX YYY*.

XXX:

Identifies one of the following as the message output targets:

- Agent
- Backup
- Client
- Server
- Log

YYY:

Identifies the type of message:

- **Error:** Error
- **Warning:** Warning
- **Info:** Information

(2) Messages displayed during command execution

Only the message text is displayed.

(3) Messages displayed in the access log

The date and time and the message text are output to the access log file.

8.1.2 Formats of message explanations

This subsection describes the formats of the message explanations in this chapter. Variable text is indicated by italic typeface.

(1) Messages displayed in Event Viewer

The messages are presented in table format in the order of the message IDs. The following table shows an example of the message explanations:

Event ID	Type	Category	Description	Notes
Event ID	Type of message	Output target and type of error	Message text	Notes

(2) Messages displayed during command execution

The following table shows an example of the message explanations:

Message that is displayed	Cause	Action
Message text	Cause of message output	Action to be taken when the message is displayed

(3) Messages displayed in the access log

The following table shows an example of the message explanations:

Message that is displayed	Cause
Message text	Cause of message output

8.2 Messages displayed in Event Viewer

The table below lists and describes the messages that can be displayed in Event Viewer.

Table 8–1: Messages displayed in Event Viewer

Event ID	Type	Category ^{#19}	Description	Notes
2	Error or Warning	Log Error (107) Log Warning (109) Agent Error (113) Agent Warning (115) Server Warning (106) Client Error (101) Client Warning (103)	System function error occurred. Function that caused error: ^{#1} Place where error occurred: ^{#2} Function name: ^{#3} Error message: ^{#4} Details: ^{#5}	Error and warning logs in the event of a system call error <ul style="list-style-type: none">Action: See Table 8-2.
3	Error	Server Error (104)	System function error occurred. Connection number: ^{#6} Function that caused error: ^{#1} Place where error occurred: ^{#2} Function name: ^{#3} Error message: ^{#4} User name: ^{#7} IP address: ^{#8} Details: ^{#5}	Error log in the event of a system call error
4	Error or Warning	Server Error (104) Server Warning (106)	System call error occurred. Connection number: ^{#6} Transmission number: ^{#9} Function that caused error: ^{#1} Place where error occurred: ^{#2} Function name: ^{#3} Error message: ^{#4} User name: ^{#7} IP address: ^{#8} Local file name: ^{#10} Details: ^{#5}	Error and warning logs in the event of a system call error during file transmission <ul style="list-style-type: none">Action: See Table 8-3.
5	Error	Client Error (101) Log Error (107) Server Error (104) Agent Error (113)	Logic error occurred. Function that caused error: ^{#1} Place where error occurred: ^{#2}	Error log in the event of a logical error
6	Warning	Client Warning (103)	Protocol error occurred. Function that caused error: ^{#1} Place where error occurred: ^{#2} Reply message: ^{#11} Connection number: ^{#6} Transmission number: ^{#9} Log-in user name: ^{#12} Log-in host name: ^{#13}	Error log in the event of a protocol error

Event ID	Type	Category ^{#19}	Description	Notes
6	Warning	Client Warning (103)	Transmission type: ^{#14} Local file name: ^{#15} Remote file name: ^{#16}	Error log in the event of a protocol error
7	Error or Warning	Client Error (101) Client Warning (103)	System call error occurred. Function that caused error: ^{#1} Place where error occurred: ^{#2} Function name: ^{#3} Error message: ^{#4} Connection number: ^{#6} Transmission number: ^{#9} Log-in user name: ^{#12} Log-in hostname: ^{#13} Transmission type: ^{#14} Local file name: ^{#15} Remote file name: ^{#16} Details: ^{#5}	Error log in the event of a system call error • Action: See Table 8-4 .
8	Error	Client Error (101)	Logic error occurred. Function that caused error: ^{#1} Place where error occurred: ^{#2} Connection number: ^{#6} Transmission number: ^{#9} Log-in user name: ^{#12} Log-in hostname: ^{#13} Transmission type: ^{#14} Local file name: ^{#15} Remote file name: ^{#16}	Error log in the event of a logical error
9	Error	Log Error (107)	File system is full, so cannot output log. Delete unnecessary files.	Error log when there was not enough disk space to write the log
10	Warning	Client Warning (103) Server Warning (106)	File system is full, so cannot output trace. Delete unnecessary files.	Warning log when there was not enough disk space to write the trace log
11	Information	Server Info (105)	JP1/File Transmission Server/FTP Server service started.	Information log when the server service started
12	Information	Server Info (105)	JP1/File Transmission Server/FTP Server service terminated.	Information log when the server service stopped
14	Information	Client Info (102)	JP1/File Transmission Server/FTP Client service started.	Information log when the client service started
15	Information	Client Info (102)	JP1/File Transmission Server/FTP Client service terminated.	Information log when the client service stopped
17	Warning	Client Warning (103) Server Warning (106)	Log server forced to disconnect connection.	Warning log when Log service forcibly terminated the connection

Event ID	Type	Category ^{#19}	Description	Notes
18	Warning	Server Warning (106)	Number of concurrent transmissions exceeds the maximum, so the request is rejected. <ul style="list-style-type: none"> IP address of requestor:^{#8} 	Warning log when the maximum number of connections was exceeded during server connection
19	Information	Log Info (108)	JP1/File Transmission Server/FTP Log service started.	Information log when the log service started
20	Information	Log Info (108)	JP1/File Transmission Server/FTP Log service terminated.	Information log when the log service stopped
21	Error	Client Error (101) Server Error (104) Log Error (107) Agent Error (113)	Port number is not defined in the Services file. [service name for which a port number is not defined]	Error log when the service started
24	Information	Server Info (105)	Transmission was finished normally. Connection number: ^{#6} Transmission number: ^{#9} User name: ^{#7} IP address: ^{#8} Local file name: ^{#10}	Information log when transmission terminated normally
25	Error	Server Error (104)	Transmission was finished abnormally. Connection number: ^{#6} Transmission number: ^{#9} User name: ^{#7} IP address: ^{#8} Local file name: ^{#10}	Error log when transmission terminated abnormally
26	Information	Client Info (102)	Transmission was finished normally. Connection number: ^{#6} Transmission number: ^{#9} Card name: ^{#17} Log-in user name: ^{#12} Log-in hostname or IP address: ^{#13} Local file name: ^{#15} Remote file name: ^{#16}	Information log when transmission terminated normally
27	Error	Client Error (101)	Transmission was finished abnormally. Connection number: ^{#6} Transmission number: ^{#9} Card name: ^{#17} Log-in user name: ^{#12} Log-in hostname or IP address: ^{#13} Local file name: ^{#15} Remote file name: ^{#16}	Information log when transmission terminated abnormally

Event ID	Type	Category ^{#19}	Description	Notes
28	Information	Agent Info (114)	JP1/File Transmission Server/FTP Agent service started.	Information log when the Operations-Manager Agent service started
29	Information	Agent Info (114)	JP1/File Transmission Server/FTP Agent service terminated.	Information log when the Operations-Manager Agent service ended
30	Information	Log Info (108)	The existing log information file (history) is being copied. (FTSLOGSAVE) (^{#18}) (Log information pointer)	Information log when the log information file was copied
31	Information	Log Info (108)	A new log information file (history) will now be created. (Log information pointer)	Information log when a new log information file was created
33	Information	Server Info (105)	Transmission was started. Connection number: ^{#6} Transmission number: ^{#9} User name: ^{#7} IP address: ^{#8} Local file name: ^{#10}	Information log when transmission started
34	Information	Client Info (102)	Transmission was started. Connection number: ^{#6} Transmission number: ^{#9} Card name: ^{#17} Log-in user name: ^{#12} Log-in hostname or IP address: ^{#13} Local file name: ^{#15} Remote file name: ^{#16}	Information log when transmission started
37	Warning	Client Warning (103) Server Warning (106)	An error occurred while a connection number or transmission number was being saved. Function that caused error: ^{#1} Place where error occurred: ^{#2} Function name: ^{#3} Error message: ^{#4} Details: ^{#5}	Warning log when writing of a connection number or transmission number failed
38	Error	Client Error (101)	Logic error occurred. Function that caused error: ^{#1} Place where error occurred: ^{#2} Details: ^{#5}	Error log in the event of a logical error
39	Information	Log Info (108)	The Log service and Client service were connected.	Information log when the log service connected to client service
40	Information	Log Info (108)	The Log service and Server service were connected.	Information log when the log service connected to server service

Event ID	Type	Category ^{#19}	Description	Notes
41	Information	Log Info (108)	The Log service and Client service were disconnected.	Information log when the log service disconnected to client service
42	Information	Log Info (108)	The Log service and Server service were disconnected.	Information log when the log service disconnected to server service
43	Error	Client Error (101)	An SSL error occurred. Function that caused error: ^{#1} Place where error occurred: ^{#2} Error message: ^{#4} Connection number: ^{#6} Transmission number: ^{#9} Log-in user name: ^{#12} Log-in host name: ^{#13} Transmission type: ^{#14} Local file name: ^{#15} Remote file name: ^{#16} Details: ^{#5}	Error log when the SSL communication error occurred
45	Error	Server Error (104)	An SSL communication error occurred. Connection number: ^{#6} Transmission number: ^{#9} Function that caused error: ^{#1} Place where error occurred: ^{#2} Error message: ^{#4} User name: ^{#7} IP address: ^{#8} Local file name: ^{#10} Details: ^{#5}	Error log when the SSL communication error occurred during file transmission
46	Error	Server Error (104)	An SSL communication error occurred. Connection number: ^{#6} Function that caused error: ^{#1} Place where error occurred: ^{#2} Error message: ^{#4} User name: ^{#7} IP address: ^{#8} Details: ^{#5}	Error log when the SSL communication error occurred
47	Warning	Client Warning (103) Server Warning (106)	File system is full, so cannot output log. Delete unnecessary files.	Warning log when there was not enough disk space to write the log
1001	Information Warning	Backup Info (110) Backup Warning (111)	Saved JP1/FTP settings.	Information and warning logs when the ftssave command was used

Event ID	Type	Category ^{#19}	Description	Notes
1002	Information or Warning	Backup Info (110) Backup Warning (111)	Recovered JP1/FTP settings.	Error log when the <code>ftsload</code> command was used
1003	Error	Backup Error (112)	Error occurred when saving JP1/FTP settings. ^{#4}	Error log when the <code>ftssave</code> command was used
1004	Error	Backup Error (112)	Error occurred when recovering JP1/FTP settings. ^{#4}	Error log when the <code>ftsload</code> command was used
1006	Error	Backup Error (112)	Incorrect parameter for <code>ftssave</code> command. ^{#4}	Error log when the <code>ftssave</code> command was used
1007	Error	Backup Error (112)	Incorrect parameter for <code>ftsload</code> command. ^{#4}	Error log when the <code>ftsload</code> command was used

#1

Name of the function that contains the process resulting in the error

#2

Location number in the function where the error was detected

#3

Name of the function resulting in the error

#4

Message indicating the nature of the error

#5

Details of the error (applicable to server and client services)

#6

Connection number managed by JP1/FTP

#7

Name of the connected user (when the server is used)

#8

IP address of the machine used by the connected user (when the server is used)

#9

Transmission number managed by JP1/FTP

#10

Name of the transmission file at the server (when the server is used)

#11

Response message from the connection-target server

#12

User name used for connection (when the client is used)

#13

Host name or IP address of the connection target (when the client is used)

#14

Send/receive type indicated as `send` (overwrite send), `append` (append send), or `recv` (receive)

#15

Name of the transmission file at the client (when the client is used)

#16

Name of the transmission file at the server (when the client is used)

#17

Transmission card name (when the client is used)

#18: One of the following:

- 1: The size of the log information has become smaller than the existing log information file.
- 2: The existing log information file has become smaller than the previous log information pointer.
- 3: The existing log information file is for an old version.

#19

The number in parentheses is displayed.

Table 8–2: Action to be taken when the event ID is 2

Function name	Error message	Action
IMEventLoad	The library was not found. (50)	Install JP1/Base.
IMEventOpenSender	Cannot connect to the event service. (40)	Start JP1/Base.

Table 8–3: Action to be taken when the event ID is 4

Name of function resulting in error	Function name	Error message	Action
--	IMEventLoad	The library was not found. (50)	Install JP1/Base.
--	IMEventOpenSender	Cannot connect to the event service. (40)	Start JP1/Base.
--	JpSeventOpen	Cannot connect to the event server. (11)	Check the status of the JP1/Base that is used as the event server.
fts_ss_callproc	SearchPath	The system cannot find the file specified. (2)	Check and, if necessary, revise Program to start when transmission ends normally (or Program to start when transmission ends abnormally) in the auto-start program settings.
fts_ss_callproc	CreateProcess	Access is denied. (5)	Check and, if necessary, revise Program to start when transmission ends normally (or Program to start when transmission ends abnormally) in the auto-start program settings.
retrieve	GetFileAttributes	The system cannot find the file specified. (2)	Check and, if necessary, revise the transmission file name at the server.
store	CreateFile	Access is denied. (5)	Check and, if necessary, revise the transmission file name at the server.

Legend:

--: There is no applicable function.

Table 8–4: Action to be taken when the event ID is 7

Name of function resulting in error	Function name	Error message	Action
--	IMEventLoad	The library was not found. (50)	Install JP1/Base.
--	IMEventOpenSender	Cannot connect to the event service. (40)	Start JP1/Base.
--	gethostbyname	Authoritative Answer Host not found. (11001)	Check and, if necessary, revise the host name in the transmission information.
fts_cs_callproc	SearchPath	The system cannot find the file specified. (2)	Check and, if necessary, revise Program to start at normal end (or Program to start at abnormal end) in the transmission settings.
fts_cs_callproc	CreateProcess	Access is denied. (5)	Check and, if necessary, revise Program to start at normal end (or Program to start at abnormal end) in the transmission settings.
sendrequest	GetFileAttributes	The system cannot find the file specified. (2)	Check and, if necessary, revise the transmission file name at the client.
fts_cs_recvrequest	CreateFile	Access is denied. (5)	Check and, if necessary, revise the transmission file name at the client.

Legend:

--: There is no applicable function.

8.3 Messages displayed during command execution

This section presents for each command the messages that can be output, their causes, and the actions to take.

8.3.1 Messages displayed during execution of the `ftstran` command

The table below lists and describes the messages that can be displayed when the `ftstran` command is executed.

Table 8–5: Messages displayed during execution of the `ftstran` command

Message that is displayed	Cause	Action
Specify CHECK or UNCHECK after the /TK switch.	Neither CHECK (do size checking) nor UNCHECK (do not do size checking) is specified after the /TK option.	Specify either CHECK (do size checking) or UNCHECK (do not do size checking).
Specify STREAM or COMPRESS after the /TM switch.	Neither STREAM (do not compress) nor COMPRESS (compress) is specified after the /TM option.	Specify either STREAM (do not compress) or COMPRESS (compress).
Specify SEND, RECV, or APPE after the /TT switch.	Neither SEND (overwrite send), nor RECV (receive), nor APPE (append send) is specified after the /TT option.	Specify one of SEND (overwrite send), RECV (receive), or APPE (append send).
Specify ASCII or BINARY after the /TY switch.	Neither ASCII nor BINARY is specified after the /TY option.	Specify either ASCII or BINARY.
Specify AUTO, MULTIPLE or SINGLE after the /TA switch.	Neither AUTO (switch automatically), nor MULTIPLE (transmit multiple files), nor SINGLE (transmit single file) is specified after the /TA option.	Specify one of AUTO (switch automatically), MULTIPLE (transmit multiple files), or SINGLE (transmit single file).
Specify CHECK or UNCHECK after the /TSS switch.	Neither CHECK (use FTPS) nor UNCHECK (do not use FTPS) is specified after the /TSS option.	Specify either CHECK (use FTPS) or UNCHECK (do not use FTPS).
Specify CHECK or UNCHECK after the /TSE switch.	Neither CHECK (check the expiration date of the server certificate) nor UNCHECK (do not check the expiration date of the server certificate) is specified after the /TSE option.	Specify either CHECK (check the expiration date of the server certificate) or UNCHECK (do not check the expiration date of the server certificate).
The FTP command is too long.	The FTP command exceeds the maximum length.	Specify the FTP command as no more than 300 bytes.
The name of the program that starts when file transmission ends abnormally is too long.	The name of the program that starts when transmission ends abnormally exceeds the maximum length.	Specify the name of the program to start when transmission ends abnormally as a string of 259 bytes or less.
In the name of the program that starts when file transmission ends abnormally you cannot specify the following characters: space < > " * ?	An invalid character is contained in the name of the program that starts when transmission ends abnormally.	Check and, if necessary, revise the name of the program to start when transmission ends abnormally.
The name of the program that starts when file transmission ends abnormally is specified incorrectly.	The name of the program that starts when transmission ends abnormally is invalid.	Check and, if necessary, revise the name of the program to start when transmission ends abnormally.

Message that is displayed	Cause	Action
Specify the name of the program that starts when file transmission ends abnormally with a full-path name.	The name of the program that starts when transmission ends abnormally is not specified as a full path.	Express as a full path the name of the program to start when transmission ends abnormally.
The card information is unacquirable. - func(error)	A system call error occurred during acquisition of card information.	Take appropriate action as indicated by the function's error code.
The card name is too long.	The specified card name exceeds the maximum length.	Specify the card name as a string of up to 20 bytes.
The command syntax is incorrect.	There is a syntax error in the command line.	Check and, if necessary, revise the command line entry.
The comment is too long.	The specified comment exceeds the maximum length.	Specify the comment as a string of up to 80 bytes.
Duplicated switch. - opt	A specified option is duplicated.	Do not specify the same option more than once.
Invalid switch. - option	The invalid switch <i>option</i> is specified.	Do not specify the invalid switch <i>option</i> .
The name of the program that starts when file transmission ends normally is too long.	The name of the program that starts when transmission ends normally exceeds the maximum length.	Specify the name of the program to start when transmission ends normally as a string of up to 259 bytes.
In the name of the program that starts when file transmission ends normally you cannot specify the following characters: space < > " * ?	An invalid character is contained in the name of the program that starts when transmission ends normally.	Check and, if necessary, revise the name of the program to start when transmission ends normally.
The name of the program that starts when file transmission ends normally is specified incorrectly.	The name of the program that starts when transmission ends normally is invalid.	Check and, if necessary, revise the name of the program to start when transmission ends normally.
Specify the name of the program that starts when file transmission ends normally with a full-path name.	The name of the program that starts when transmission ends normally is not specified as a full path.	Express as a full path the name of the program to start when transmission ends normally.
Transmission ended abnormally.	File transmission terminated abnormally.	Check the transmission log.
Transmission ended normally but with a warning.	(Normal termination with a warning)	Check the transmission log.
Transmission ended normally.	(Normal termination)	--
The password is too long.	The specified password exceeds the maximum length.	Specify the password as a string of up to 50 bytes.
The file name is too long.	The specified file name exceeds the maximum length.	Specify the file name as a string of up to 259 bytes.
The file name is specified incorrectly.	The specified file name is invalid.	Check and, if necessary, revise the file name.
Specify the port number in the range from 1 to 65535.	The port number is not an integer from 1 to 65,535.	Specify the port number as an integer from 1 to 65,535.
Specify the port number with an integer.	The specified port number contains a nonnumeric character.	Specify an integer.
The remote host name is too long.	The specified host name exceeds the maximum length.	Specify the host name as a string of up to 256 bytes.

Message that is displayed	Cause	Action
The remote host name is specified incorrectly.	The specified host name is invalid.	Check and, if necessary, revise the host name.
The name of a user to log in is too long.	The specified user name exceeds the maximum length.	Specify the user name as a string of up to 50 bytes.
The name of a user to log in is specified incorrectly.	The specified user name is invalid.	Check and, if necessary, revise the user name.
The remote file name is too long.	The specified remote file name exceeds the maximum length.	Specify the remote file name as a string of up to 259 bytes.
The remote file name is specified incorrectly.	The specified remote file name is invalid.	Check and, if necessary, revise the remote file name.
The local file name is too long.	The specified local file name exceeds the maximum length.	Specify the local file name as a string of up to 259 bytes.
In the local file name you cannot specify the following characters: space < > " * ?	The specified local file name contains an invalid character.	Check and, if necessary, revise the local file name.
The local file name is specified incorrectly.	The specified local file name is invalid.	Check and, if necessary, revise the local file name.
The path name of the CA certificate is too long.	The specified path to the CA certificate exceeds the maximum length.	Specify the path to the CA certificate as a string of up to 259 bytes.
Specify the path name of the CA certificate with a full-path name.	The specified path name is not the full path to the CA certificate.	Specify the full path name for the CA certificate.
The path name of the CA certificate cannot contain a tab.	Tab characters are used in the specified path to the CA certificate.	Check and, if necessary, revise the path name you have specified for the CA certificate.
In the path name of the CA certificate you cannot specify the following characters: < > " * ?	The specified path to the CA certificate contains invalid characters.	Check and, if necessary revise the path name you have specified for the CA certificate.
Specify the path name of the CA certificate.	The path to the CA certificate is not specified.	Specify the path to the CA certificate.
The path name of the CRL is too long.	The specified path to the CRL exceeds the maximum length.	Specify the path to the CRL as a string of up to 259 bytes.
Specify the path name of the CRL with a full-path name.	The specified path name is not the full path to the CRL.	Specify the full path name for the CRL.
The path name of the CRL cannot contain a tab.	Tab characters are used in the specified path to the CRL.	Check and, if necessary, revise the path name you have specified for the CRL.
In the path name of the CRL you cannot specify the following characters: < > " * ?	The specified path to the CRL contains invalid characters.	Check and, if necessary revise the path name you have specified for the CRL.

Legend:

--: There is no action that can be taken.

8.3.2 Messages displayed during execution of the `ftsregc` command

The table below lists and describes the messages that can be displayed when the `ftsregc` command is executed.

Table 8–6: Messages displayed during execution of the ftsregc command

Message that is displayed	Cause	Action
Specify CHECK or UNCHECK after the /TK switch.	Neither CHECK (do size checking) nor UNCHECK (do not do size checking) is specified after the /TK option.	Specify either CHECK (do size checking) or UNCHECK (do not do size checking).
Specify STREAM or COMPRESS after the /TM switch.	Neither STREAM (do not compress) nor COMPRESS (compress) is specified after the /TM option.	Specify either STREAM (do not compress) or COMPRESS (compress).
Specify SEND, RECV, or APPE after the /TT switch.	Neither SEND (overwrite send), nor RECV (receive), nor APPE (append send) is specified after the /TT option.	Specify one of SEND (overwrite send), RECV (receive), or APPE (append send).
Specify ASCII or BINARY after the /TY switch.	Neither ASCII nor BINARY is specified after the /TY option.	Specify either ASCII or BINARY.
Specify AUTO, MULTIPLE or SINGLE after the /TA switch.	Neither AUTO (switch automatically), nor MULTIPLE (transmit multiple files), nor SINGLE (transmit single file) is specified after the /TA option.	Specify one of AUTO (switch automatically), MULTIPLE (transmit multiple files), or SINGLE (transmit single file).
Specify CHECK or UNCHECK after the /TSS switch.	Neither CHECK (use FTPS) nor UNCHECK (do not use FTPS) is specified after the /TSS option.	Specify either CHECK (use FTPS) or UNCHECK (do not use FTPS).
Specify CHECK or UNCHECK after the /TSE switch.	Neither CHECK (check the expiration date of the server certificate) nor UNCHECK (do not check the expiration date of the server certificate) is specified after the /TSE option.	Specify either CHECK (check the expiration date of the server certificate) or UNCHECK (do not check the expiration date of the server certificate).
The FTP command is too long.	FTP command exceeds the maximum length.	Specify the FTP command as no more than 300 bytes.
The name of the program that starts when file transmission ends abnormally is too long.	The name of the program that starts when transmission ends abnormally exceeds the maximum length.	Specify the name of the program to start when transmission ends abnormally as a string of up to 259 bytes.
In the name of the program that starts when file transmission ends abnormally you cannot specify the following characters: < > * ?	An invalid character is contained in the name of the program that starts when transmission ends abnormally.	Check and, if necessary, revise the name of the program to start when transmission ends abnormally.
The name of the program that starts when file transmission ends abnormally is specified incorrectly.	The name of the program that starts when transmission ends abnormally is invalid.	Check and, if necessary, revise the name of the program to start when transmission ends abnormally.
Specify the name of the program that starts when file transmission ends abnormally with a full-path name.	The name of the program that starts when transmission ends abnormally is not specified as a full path.	Express as a full path the name of the program to start when transmission ends abnormally.
The card information is unacquirable. - func(error)	A system call error occurred during acquisition of card information.	Take appropriate action as indicated by the function's error code.
The card name is too long.	The specified card name exceeds the maximum length.	Specify the card name as a string of up to 20 bytes.
Specify the card name.	The card name is not specified.	Specify the card name.
The command syntax is incorrect.	There is a syntax error in the command line.	Check and, if necessary, revise the command line entry.

Message that is displayed	Cause	Action
The comment is too long.	The specified comment exceeds the maximum length.	Specify the comment as a string of up to 80 bytes.
The specified card (card) is already registered.	The specified card name already exists.	Change the card name.
The specified card (card) is not registered.	The specified card is not registered.	Specify a registered card name.
Duplicated switch. - opt	A specified option is duplicated.	Do not specify the same option more than once.
Invalid switch. - <i>option</i>	The invalid switch <i>option</i> is specified.	Do not specify the invalid switch <i>option</i> .
The name of the program that starts when file transmission ends normally is too long.	The name of the program that starts when transmission ends normally exceeds the maximum length.	Specify the name of the program to start when transmission ends normally as a string of up to 259 bytes.
In the name of the program that starts when file transmission ends normally you cannot specify the following characters: < > * ?	An invalid character is contained in the name of the program that starts when transmission ends normally.	Check and, if necessary, revise the name of the program to start when transmission ends normally.
The name of the program that starts when file transmission ends normally is specified incorrectly.	The name of the program that starts when transmission ends normally is invalid.	Check and, if necessary, revise the name of the program to start when transmission ends normally.
Specify the name of the program that starts when file transmission ends normally with a full-path name.	The name of the program that starts when transmission ends normally is not specified as a full path.	Express as a full path the name of the program to start when transmission ends normally.
Specify the name of the destination host to be connected.	The name of the connection-target host is missing.	Specify the name of the connection-target host.
Specify the send or reception type (/TT SEND RECV APPE) .	The send/receive type is not specified.	After /TT, specify SEND (overwrite send), RECV (receive), or APPE (append send) as the send/receive type.
Specify the transmission mode (/TY ASCII BINARY) .	The transmission mode is not specified.	After /TY, specify either ASCII or BINARY as the transmission mode.
The password is too long.	The specified password exceeds the maximum length.	Specify the password as a string of up to 50 bytes.
Specify the port number in the range from 1 to 65535.	The port number is not an integer from 1 to 65,535.	Specify the port number as an integer from 1 to 65,535.
Specify the port number with an integer.	The specified port number contains a nonnumeric character.	Specify an integer.
The remote host name is too long.	The specified host name exceeds the maximum length.	Specify the host name as a string of up to 256 bytes.
The remote host name is specified incorrectly.	The specified host name is invalid.	Check and, if necessary, revise the host name.
The name of a user to log in is too long.	The specified user name exceeds the maximum length.	Specify the user name as a string of up to 50 bytes.
The name of a user to log in is specified incorrectly.	The specified user name is invalid.	Check and, if necessary, revise the user name.
The remote file name is too long.	The specified remote file name exceeds the maximum length.	Specify the remote file name as a string of up to 259 bytes.

Message that is displayed	Cause	Action
The remote file name is specified incorrectly.	The specified remote file name is invalid.	Check and, if necessary, revise the remote file name.
Specify the remote file name.	The remote file name is not specified.	Check and, if necessary, revise the remote file name.
The local file name is too long.	The specified local file name exceeds the maximum length.	Specify the local file name as a string of up to 259 bytes.
In the local file name you cannot specify the following characters: space < > " * ?	The specified local file name contains an invalid character.	Check and, if necessary, revise the local file name.
The local file name is specified incorrectly.	The specified local file name is invalid.	Check and, if necessary, revise the local file name.
Specify the local file name.	The local file name is not specified.	Specify the local file name.
Specify the name of a user to log in.	The login user name is not specified.	Specify the login user name.
The path to the CA certificate is too long.	The specified path to the CA certificate exceeds the maximum length.	Specify the path to the CA certificate as a string of up to 259 bytes.
Specify the full path to the CA certificate.	The specified path name is not the full path to the CA certificate.	Specify the full path name for the CA certificate.
The specified path to the CA certificate must not contain tab characters.	Tab characters are used in the specified path to the CA certificate.	Check and, if necessary, revise the path name you have specified for the CA certificate.
You cannot specify the following characters in the path name for the CA certificate: < > " * ?	The specified path to the CA certificate contains invalid characters.	Check and, if necessary, revise the path name you have specified for the CA certificate.
Specify the path to the CA certificate.	The path to the CA certificate is not specified.	Specify the path to the CA certificate.
The path to the CRL is too long.	The specified path to the CRL exceeds the maximum length.	Specify the path to the CRL as a string of up to 259 bytes.
Specify the full path to the CRL.	The specified path name is not the full path to the CRL.	Specify the full path name for the CRL.
The specified path to the CRL must not contain tab characters.	Tab characters are used in the specified path to the CRL.	Check and, if necessary, revise the path name you have specified for the CRL.
You cannot specify the following characters in the path name for the CRL: < > " * ?	The specified path to the CRL contains invalid characters.	Check and, if necessary, revise the path name you have specified for the CRL.
Start the program as an administrator.	The user who started the command is not an administrator.	An administrator must start the command.

8.3.3 Messages displayed during execution of the ftshistory command

The table below lists and describes the messages that might be displayed when the `ftshistory` command is executed.

Table 8–7: Messages that might be displayed during execution of the ftshistory command

Message that is displayed	Cause	Action
The command syntax is incorrect.	There is a syntax error in the command line.	Check and, if necessary, revise the command line entry.
JP1/FTP cannot read the specified log file. or JP1/FTP cannot copy temporary file. <i>source-file</i> <i>destination-file</i> CopyFile code= <i>errno</i> <i>msg</i>	Copy operation on the temporary file failed.	Check the error message and take appropriate action.
There is no log-information.	There is no log information to view.	--
Error for access file. <i>function-name</i> code= <i>errno</i> <i>msg</i>	An error occurred while accessing the log file.	Check the error message and take appropriate action.
Error for access file. <i>function-name</i> code= <i>errno</i> POS= <i>pos</i> <i>msg</i>	An error occurred while accessing the log file. <i>pos</i> : Position of the erroneous log information in the log file (count)	Check the error message and take appropriate action.
Error for access file. <i>function-name</i> code= <i>errno</i> POS= <i>pos1, pos2</i> <i>msg</i>	An error occurred while accessing the log file. <i>pos1</i> : Position of processing (count) <i>pos2</i> : Position of the erroneous log information in the log file (count)	Check the error message and take appropriate action.
A part of the log file is corrupted. position = <i>pos</i>	A portion of the log file is corrupted. <i>pos</i> : Position of the erroneous log information in the log file (count)	Check and, if necessary, revise the log file.
This is not a JP1/FTP log file, or the file is corrupted.	This is not a JP1/FTP log file, or the log file is corrupted.	Check and, if necessary, revise the log file.
There is no form file.	There is no format file.	Check and, if necessary, revise the format file.
JP1/FTP cannot reference form file. <i>function-name</i> code= <i>errno</i> <i>msg</i>	An error occurred while accessing the format file.	Check the error message and take appropriate action.
There is no key in form.	There are no keys in the format file.	--
JP1/FTP cannot output to file. <i>function-name</i> code= <i>errno</i> <i>msg</i>	File output failed.	Check the error message and take appropriate action.
JP1/FTP cannot get the installation directory. <i>function-reg</i> code= <i>errno</i> <i>msg</i> Assumed C:\Program Files\Hitachi\FTSFTP.	An error occurred while obtaining the installation directory.	Check the error message and take appropriate action.
Could not acquire a data directory.	An error occurred while obtaining the directory for log information.	Check the error message and take appropriate action.

Message that is displayed	Cause	Action
<i>function-reg</i> code= <i>errno</i> <i>msg</i> Assumed C:\Program Files\Hitachi\FTSFTP.	An error occurred while obtaining the directory for log information.	Check the error message and take appropriate action.
A temporary directory cannot be acquired. GetTempPath code = <i>errno</i> <i>msg</i>	An error occurred while obtaining the temporary directory.	Check the error message and take appropriate action.
Start the program as an administrator.	The user who started the command is not an administrator.	An administrator must start the command.

Legend:

--: There is no action that can be taken.

8.3.4 Messages displayed during execution of the `ftsload` command

The table below lists and describes the messages that might be displayed when the `ftsload` command is executed.

Table 8–8: Messages that might be displayed during execution of the `ftsload` command

Message that is displayed	Cause	Action
JP1/FTP settings are recovered.	(Normal termination)	--
This is not a JP1/FTP settings storage file.	The specified file is not a JP1/FTP definition information file.	Check and, if necessary, revise the definition information file.
There is no corresponding user, so there is no auto-start program settings to be recovered.	(Normal termination with a warning)	--
The command syntax is incorrect.	There is a syntax error in the command line.	Check and, if necessary, revise the command line.
Duplicated switch - <i>opt</i> .	An option is duplicated.	Do not specify the same option more than once.
The file name is not specified.	The name of the file to be recovered is not specified.	Specify the name of the file to be recovered.
There are no settings to be recovered.	The definition information to be recovered is not in the file.	--
Invalid switch - <i>opt</i> .	The specified option is invalid.	Check and, if necessary, revise the option.
Start the program as an administrator.	The user who started the command is not an administrator.	An administrator must start the command.

Legend:

--: There is no action that can be taken.

8.3.5 Messages displayed during execution of the `ftssave` command

The table below lists and describes the messages that might be displayed when the `ftssave` command is executed.

Table 8–9: Messages that might be displayed during execution of the ftssave command

Message that is displayed	Cause	Action
JPl/FTP settings are saved.	(Normal termination)	--
The command syntax is incorrect.	There is a syntax error in the command line.	Check and, if necessary, revise the command line.
No auto-start program settings have been registered.	(Normal termination with a warning)	--
Duplicated switch - <i>opt</i> .	An option is duplicated.	Do not specify the same option more than once.
No transmission settings have been registered.	(Normal termination with a warning)	--
The file name is too long.	The specified file name exceeds the maximum length.	Specify the file name as a string of up to 259 bytes.
The file name is not specified.	The file name is not specified.	Specify the file name.
Invalid switch - <i>opt</i> .	The specified option is invalid.	Check and, if necessary, revise the option.
No user-to-login settings have been registered.	(Normal termination with a warning)	--
Start the program as an administrator.	The user who started the command is not an administrator.	An administrator must start the command.

Legend:

--: There is no action that can be taken.

8.4 Messages output to the access log

The following table lists and describes the messages that might be output to the access log.

Table 8–10: Messages that might be output to the access log

Message	Cause
<i>FTP-command</i> ^{#1} is invalid because it was sent by a user who was not logged in. [Remote host: <i>IP-address</i> ^{#2}] [Remote port: <i>port-number</i> ^{#3}] [Connection number: <i>connection-number</i> ^{#4}]	An FTP command that becomes executable after login was accepted before login.
Login of user <i>user-name</i> ^{#5} failed. [Remote host: <i>IP-address</i> ^{#2}] [Remote port: <i>port-number</i> ^{#3}] [Connection number: <i>connection-number</i> ^{#4}]	Login failed.
The max. number of FTP clients was reached. No more clients can use the service.	The number of connection requests has reached the maximum permissible number of concurrent transmissions.
The connection was closed without login. [Remote host: <i>IP-address</i> ^{#2}] [Remote port: <i>port-number</i> ^{#3}] [Connection number: <i>connection-number</i> ^{#4}]	The FTP client disconnected itself without logging in.

#1

FTP-command: Indicates the FTP command.

#2

IP-address: Indicates the IP address of the FTP client.

#3

port-number: Indicates the port number of the FTP client.

#4

connection-number: Indicates the connection number.

#5

user-name: Indicates the user name.

9

Troubleshooting

This chapter describes how to handle problems that can occur while you are using JP1/FTP.

9.1 Error handling procedures

This section describes the procedures for handling errors that might occur while you are using JP1/FTP.

1. Checking the processing event

Check the processing event that was underway when the error occurred. If a message has been output, check the details of the message (for the messages, see [8. Messages](#)). For details about the log information that is output by JP1/FTP, see [9.2 Types of log information](#).

2. Collecting data

Collect data to determine the cause of the error. For details about the data to collect, see [9.3 Data to collect when a problem occurs](#).

3. Checking the problem

Check the cause of the problem on the basis of the collected data. Also isolate the problem or the affected range.

9.2 Types of log information

The following two types of log information are output during operation of JP1/FTP:

- Common message log
- Log by process

This section describes these two types of log information.

9.2.1 Common message log

The common message log contains log information that reports system errors that have occurred and is intended for the system administrator. The common message log provides the minimum amount of error information that is required.

The common message log is output to the Windows event log.

9.2.2 Log by process

Log by process is the log information that is output by each function of JP1/FTP. The log by process is output to a separate log file for each function. For details about the log files, see [9.3.2 Information about JP1/FTP](#).

9.3 Data to collect when a problem occurs

This section describes the data that we recommend you collect in the event of an error on JP1/FTP and how to collect it.

9.3.1 Log information about the operating system (OS)

You need to collect the following log information about the OS:

- Windows event log
Use Windows Event Viewer to check the Windows event log. We recommend that you also output the log information to a file.

9.3.2 Information about JP1/FTP

The following table lists the information about JP1/FTP that needs to be collected.

Table 9–1: Information about JP1/FTP

File name	Directory name	Overview	Size	Management method
History [#]	<i>directory-for-log-information</i>	Results of file transmission	Number of log entries to be retained, as specified in the environment definition, x 1,500 bytes	Wraparound
CModuleTrace <i>n</i> <i>n</i> : Value from 1 to 64	<i>directory-for-log-information\trace</i>	Module trace for the client	Module trace file size specified in the environment definition	Wraparound
SModuleTrace <i>n</i> <i>n</i> : Value from 1 to 64		Module trace for the server	Same as the above	Wraparound
LModuleTrace <i>n</i> <i>n</i> : Value from 1 to 4		Module trace for the log service	Same as the above	Wraparound
CSProtocolTrace <i>n</i> <i>n</i> : Value from 1 to 60		Protocol trace for the client	Protocol trace file size specified in the environment definition	Wraparound
SProtocolTrace <i>n</i> <i>n</i> : Value from 1 to 60		Protocol trace for the server	Same as the above	Wraparound
ftsaccess.log[.old]	<i>directory-for-log-information</i>	Access log	Access log file size specified in the environment definition	2-file management
RegisterEventSource{1 2}.log	<i>directory-for-log-information</i>	Log files that JP1/FTP fails to output to the event log	1 megabyte	2-file management

File name	Directory name	Overview	Size	Management method
ReportEvent{1 2}.log	<i>directory-for-log-information</i>	Log files that JP1/FTP fails to output to the event log	1 megabyte	2-file management
DeregisterEventSource{1 2}.log				
ftstran_trace	OS installation drive:\ProgramData\Hitachi\FTSFTP\trace	Transmission command trace	2 megabytes	Wraparound
ftsagent{1 2}.log	<i>JP1/FTP-installation-directory\manager\trace</i>	Module trace for Operations-Manager Agent	1 megabyte	2-file management
ftsajnidll{1 2}.log		Module trace for Operations-Manager Agent	1 megabyte	2-file management
ftsconsole{1 2}.log		Module trace for Operations-Manager Console	1 megabyte	2-file management
service1{1 2}.log		Trace for the Operations-Manager Agent service	1 megabyte	2-file management
service2{1 2}.log		Trace for the Operations-Manager Agent service	1 megabyte	2-file management
service3{1 2}.log		Trace for the Operations-Manager Agent service	1 megabyte	2-file management
CSError	<i>directory-for-log-information\trace</i>	Error log for the client	100 kilobyte	Wraparound
SSError		Error log for the server	100 kilobyte	Wraparound

#

If you change the number of logs to be retained, the system might create a backup of the old log file. The backup file name is FTSLOGSAVE and the directory is the directory for log information.

9.3.3 List of JP1/FTP processes

You use the Windows Task Manager to check the operating status of processes. For details about the processes, see [C. List of Processes](#).

9.3.4 Operation information

You need the following information about the operation that was underway when the error occurred, so record this information:

- Details of the operation
- Time the error occurred
- Computer configuration (such as the version of each OS and the host names)

9.3.5 Error information on screen displays

When an error is displayed in a window, collect that information. Also make a hardcopy of the following information:

- Error dialog box
- If **Details** is displayed, make a copy of that information.

9.3.6 How to collect data

An information collection tool (the Extraction tool) is provided. The Extraction tool simplifies the collection procedure.

The extraction tool is described in detail below.

(1) Name

FTSLOGCLCT.BAT

(2) Storage directory

JP1/FTP installation directory

(3) Execution format

```
FTSLOGCLCT.BAT [Δ/DΔdirectory-for-log-information] Δtarget-directory
```

Δ: Single-byte space

(4) Function

This tool copies the following information to the specified target directory:

- Product information
- Definition information
- Information described in [9.3.2 Information about JP1/FTP](#)

(5) Arguments

directory-for-log-information

Specifies the directory for the log information.

If this argument is omitted, the directory for log information that is defined in the environment definition is assumed.

target-directory

Specifies the directory in which error information is to be collected.

If the specified directory does not exist, the tool creates a new directory.

If the specified directory already exists, the tool overwrites the data.

(6) Execution permissions

Administrator

(7) Note

To customize the Extraction tool, copy the tool to a directory of your choice before customizing it.

Appendixes

A. List of Files and Directories

The following table lists the names of the files and directories that are used by JP1/FTP. The default directories are as follows:

JP1/FTP installation directory:

For the main product files:

```
OS-installation-drive:\Program Files(x86)\Hitachi\FTSFTP
```

For the API libraries for 64-bit:

```
OS-installation-drive:\Program Files\Hitachi\FTSFTP
```

Directory for log information:

```
OS-installation-drive:\Program Files(x86)\Hitachi\FTSFTP
```

Table A–1: List of files and directories for JP1/FTP

Description		File and directory names
Commands	Executes transmission	<i>JP1/FTP-installation-directory\ftstran.exe</i>
	Registers, changes, deletes, and displays transmission information	<i>JP1/FTP-installation-directory\ftsregc.exe</i>
	Displays log information	<i>JP1/FTP-installation-directory\ftshistory.exe</i>
	Saves definition information	<i>JP1/FTP-installation-directory\ftssave.exe</i>
	Recovers definition information	<i>JP1/FTP-installation-directory\ftsload.exe</i>
Definition information files	Sample file for the port number settings	<i>JP1/FTP-installation-directory\services.sample</i>
	Environment definition file	<i>JP1/FTP-installation-directory\ftsenv.ini</i>
	Sample file for environment definition file	<i>JP1/FTP-installation-directory\ftsenv.ini.sample</i>
	PASV transmission definition file	<i>JP1/FTP-installation-directory\FTPPASV.INI</i>
	Sample file for PASV transmission definition file	<i>JP1/FTP-installation-directory\FTPPASV.INI.SAMPLE</i>
	Function for controlling remote host connections definition file	<i>JP1/FTP-installation-directory\FTPHOSTACC.INF</i>
	Sample file for function for controlling remote host connections definition file	<i>JP1/FTP-installation-directory\FTPHOSTACC.INF.sample</i>
	Multiple IP address environment definition file	<i>JP1/FTP-installation-directory\HOSTINFO.INI</i>
	Sample file for multiple IP address environment definition file	<i>JP1/FTP-installation-directory\HOSTINFO.INI.sample</i>

Description		File and directory names
Definition information files	Function for using the access control function to change the root directory of absolute path names definition file	<i>JP1/FTP-installation-directory\AccessLimitation.ini</i>
	Sample file for function for using the access control function to change the root directory of absolute path names definition file	<i>JP1/FTP-installation-directory\AccessLimitation.ini.sample</i>
	FTP connection response message control function definition file	<i>JP1/FTP-installation-directory\FtsBanner.ini</i>
	Sample file for FTP connection response message control function definition file	<i>JP1/FTP-installation-directory\FtsBanner.ini.sample</i>
	FTP connection response message file	<i>JP1/FTP-installation-directory\FtsBanner.txt</i>
	IPv6 environment definition file	<i>JP1/FTP-installation-directory\IPversion.ini</i>
	Sample file for IPv6 environment definition file	<i>JP1/FTP-installation-directory\IPversion.ini.sample</i>
	FTPS (for server) definition file	<i>JP1/FTP-installation-directory\ftsftps.ini</i>
	Sample of the FTPS (for server) definition file	<i>JP1/FTP-installation-directory\ftsftps.ini.sample</i>
Log information files	Log file	<i>directory-for-log-information\History</i>
	Backup of log file [#]	<i>directory-for-log-information\FTSLOGSAVE</i>
	Module trace for the client	<i>directory-for-log-information\trace\CSModuleTracen</i> <i>n: Value from 1 to 64</i>
	Module trace for the server	<i>directory-for-log-information\trace\SSModuleTracen</i> <i>n: Value from 1 to 64</i>
	Module trace for the log service	<i>directory-for-log-information\trace\LSModuleTracen</i> <i>n: Value from 1 to 4</i>
	Protocol trace for the client	<i>directory-for-log-information\trace\CSProtocolTracen</i> <i>n: Value from 1 to 60</i>
	Protocol trace for the server	<i>directory-for-log-information\trace\SSProtocolTracen</i> <i>n: Value from 1 to 60</i>
	Access log file	<i>directory-for-log-information\ftsaccess.log</i>
	Backup of the access log file	<i>directory-for-log-information\ftsaccess.log.old</i>
	Log files that JP1/FTP fails to output to the event log	<i>directory-for-log-information\RegisterEventSource{1 2}.log</i>
		<i>directory-for-log-information\ReportEvent{1 2}.log</i>
		<i>directory-for-log-information\DeregisterEventSource{1 2}.log</i>
	Error log for the client	<i>directory-for-log-information\trace\CSError</i>

Description		File and directory names
Log information files	Error log for the server	<i>directory-for-log-information\trace\SSError</i>
Transmission command trace		<i>OS-installation-drive:\ProgramData\Hitachi\FTSFTP\trace\ftstran_trace</i>
Format files for text output	Login user registration information	<i>JP1/FTP-installation-directory\Form\enUSFORM.TXT</i>
	Sample file for login user registration information	<i>JP1/FTP-installation-directory\Form\en \USFORM.TXT.sample</i>
	Auto-start program information	<i>JP1/FTP-installation-directory\Form\en \ATFORM.TXT</i>
	Sample file for auto-start program information	<i>JP1/FTP-installation-directory\Form\en \ATFORM.TXT.sample</i>
	Transmission request registration information	<i>JP1/FTP-installation-directory\Form\en \CLFORM.TXT</i>
	Sample file for transmission request registration information	<i>JP1/FTP-installation-directory\Form\en \CLFORM.TXT.sample</i>
	Log information	<i>JP1/FTP-installation-directory\Form\en \HSFORM.TXT</i>
	Sample file for log information	<i>JP1/FTP-installation-directory\Form\en \HSFORM.TXT.sample</i>
API library	Import library (for VS2012)	<i>JP1/FTP-installation-directory\FTSFTP110*.lib</i>
	Import library (for VS2013)	<i>JP1/FTP-installation-directory\FTSFTP120*.lib</i>
	Header file	<i>JP1/FTP-installation-directory\apihead.h</i>
	Sample program	<i>JP1/FTP-installation-directory\Sample.c</i>
Operations management	Managed host definition information	<i>JP1/FTP-installation-directory\manager\console\hostdef.csv</i>
	Operations-Manager Console module trace	<i>JP1/FTP-installation-directory\manager\trace\ftsconsole1.log or ftsconsole2.log</i>
	Operations-Manager Agent module trace	<i>JP1/FTP-installation-directory\manager\trace\ftsagent1 or ftsagent2</i>
		<i>JP1/FTP-installation-directory\manager\trace\ftsjsnidl11.log or ftsjsnidl12.log</i>
	Trace for the Operations-Manager Agent service	<i>JP1/FTP-installation-directory\manager\trace\service11.log or service12.log</i>
		<i>JP1/FTP-installation-directory\manager\trace\service21.log or service22.log</i>
		<i>JP1/FTP-installation-directory\manager\trace\service31.log or service32.log</i>
Utilities	Data collection tool	<i>JP1/FTP-installation-directory\FTSLOGCLCT.BAT</i>
	Transmission result initialization tool	<i>JP1/FTP-installation-directory\FTSTRANINIT.BAT</i>
	Operations management initialization tool	<i>JP1/FTP-installation-directory\manager\FTSMGRINIT.BAT</i>
	Managed host information changing tool	<i>JP1/FTP-installation-directory\manager\console\FTSMGRHOST.BAT</i>

Description		File and directory names
Correction patch information	Log file	<i>JP1/FTP-installation-directory</i> \PATCHLOG.TXT
	Backup directory	<i>JP1/FTP-installation-directory</i> \patch_backup_dir

#

If you change the number of logs to be retained, the system might create a backup of the old log file.

B. Port Numbers

This appendix describes the port numbers used by JP1/FTP and the firewall passage directions. The protocol to be used is TCP/IP.

B.1 List of port numbers

Each port number is set after JP1/FTP has been installed. You can set any port number. The table below shows an example of port number settings. For details about the settings, see [2.2.3 Setting the port numbers](#).

Table B–1: List of port numbers for JP1/FTP

Service name	Port number (example)	Usage
ftssdata	20124	Used for transferring data to be received (FTP data connection)
ftss	20125	Used as the server port (FTP control connection)
ftsc	20126	Used by the client service
ftsclog	20127	Used for JP1/FTP logging
ftsslog	20128	Used for JP1/FTP logging
ftsagent	20252	Used by the Operations-Manager function
ftsagentdata	20364	Used by the Operations-Manager function

B.2 Firewall passage directions

The following tables show the firewall passage directions.

Table B–2: Firewall passage directions (ACTV mode)

Connection type	Product at server	Port number (example)	Firewall passage direction	Product at client	Port number
Control connection	JP1/FTP	20125/tcp	<-	JP1/FTP [#]	ANY/tcp
Data connection	JP1/FTP	20124/tcp	->	JP1/FTP [#]	ANY/tcp

Table B–3: Firewall passage directions (PASV mode)

Connection type	Product at server	Port number (example)	Firewall passage direction	Product at client	Port number
Control connection	JP1/FTP	20125/tcp	<-	JP1/FTP [#]	ANY/tcp
Data connection	JP1/FTP	ANY/tcp	<-	JP1/FTP [#]	ANY/tcp

#

If the product at the client is not JP1/FTP, the port number depends on that product.

ANY means that an available port number assigned by the OS is to be used. If `ftsagentdata` is omitted, an unused port number assigned by the OS is used. In these cases, the range of available port numbers depends on the OS.

Table B–4: Firewall passage directions (Operations-Manager function)

Operations-Manager Agent		Firewall passage direction	Operations-Manager Console
Service name	Port number (example)		Port number
ftsagent	20252/tcp	<-	ANY/tcp
ftsagentdata	20364/tcp	<-	ANY/tcp

B.3 Items to check when performing transmission via a firewall

We recommend that you check the following when you perform file transmission via a firewall:

1. Check whether the firewall can pass the FTP protocol.
 - YES -> 2
 - NO -> Use a firewall that can pass the FTP protocol (evaluate this change).
2. Check whether the OS's default FTP is also to be used.
 - YES -> 3
 - NO -> Change `ftssdata` and `ftss` to the port numbers used for normal FTP:
`ftssdata: 20/TCP`
`ftss: 21/TCP`
3. Check whether the firewall settings allow addition of FTP ports.
 - YES -> Set the firewall in such a manner that `ftssdata` and `ftss` can be used as FTP ports.
 - NO -> If the default FTP is also used, JP1/FTP cannot be used.

Note

The Operations-Manager function cannot be used in an environment in which IP addresses are converted between Operations-Manager Console and Operations-Manager Agent.

C. List of Processes

The table below lists the processes of JP1/FTP. The value in parentheses is the maximum number of times the process can be executed concurrently.

You can check these processes on the **Processes** page in the Task Manager window.

Table C–1: List of JP1/FTP processes

Process name	Function
ftpd (1)	Server service
ftpcs (1)	Client service
ftpl (1)	Log service
ftsagent (1)	Agent service

D. JP1 Events

This appendix provides a list of the JP1 events that are issued by JP1/FTP, as well as lists of their attributes.

D.1 List of JP1 events

Table D–1: List of JP1 events

Event ID	Event	Message
00010D01	Start of the JP1/File Transmission Server/FTP Server service	FTP Server service started.
00010D02	Start of the JP1/File Transmission Server/FTP Client service	FTP Client service started.
00010D03	Start of the JP1/File Transmission Server/FTP Log service	FTP Log service started.
00010D0F	Start of the JP1/File Transmission Server/FTP Agent service	FTP Agent service started.
00010D04	Stop of the JP1/File Transmission Server/FTP Server service	FTP Server service ended.
00010D05	Stop of the JP1/File Transmission Server/FTP Client service	FTP Client service ended.
00010D06	Stop of the JP1/File Transmission Server/FTP Log service	FTP Log service ended.
00010D10	Stop of the JP1/File Transmission Server/FTP Agent service	FTP Agent service ended.
00010D0B	Normal termination of file transmission	FTP file transmission ended normally.
00010D0C	Abnormal termination of file transmission	FTP file transmission ended abnormally.
00010D0D	Termination of file transmission with a warning (auto-start program start failure)	FTP file transmission is terminated with a warning. Automatic start of a program failed.

D.2 Attributes of JP1 events

This section presents the details of the JP1 events for each event ID.

(1) Details of event ID: 00010D01

Attribute type	Item	Attribute name	Description
Basic attribute	Message	--	FTP Server service started.
Extended attributes (common information)	Severity	SEVERITY	Information
	User name	USER_NAME	User who started the service
	Product name	PRODUCT_NAME	/HITACHI/JP1/FTP
	Object type	OBJECT_TYPE	JOB
	Object name	OBJECT_NAME	SERVER
	Root object type	ROOT_OBJECT_TYPE	JOB

Attribute type	Item	Attribute name	Description
Extended attributes (common information)	Root object name	ROOT_OBJECT_NAME	JP1/FTP/SERVER
	Object ID	OBJECT_ID	SERVER
	Occurrence	OCCURRENCE	START
	Start time	START_TIME	Start time
	End time	END_TIME	--
	End code	RESULT_CODE	--

Legend:

--: There is no applicable information.

(2) Details of event ID: 00010D02

Attribute type	Item	Attribute name	Description
Basic attribute	Message	--	FTP Client service started.
Extended attributes (common information)	Severity	SEVERITY	Information
	User name	USER_NAME	User who started the service
	Product name	PRODUCT_NAME	/HITACHI/JP1/FTP
	Object type	OBJECT_TYPE	JOB
	Object name	OBJECT_NAME	CLIENT
	Root object type	ROOT_OBJECT_TYPE	JOB
	Root object name	ROOT_OBJECT_NAME	JP1/FTP/CLIENT
	Object ID	OBJECT_ID	CLIENT
	Occurrence	OCCURRENCE	START
	Start time	START_TIME	Start time
	End time	END_TIME	--
	End code	RESULT_CODE	--

Legend:

--: There is no applicable information.

(3) Details of event ID: 00010D03

Attribute type	Item	Attribute name	Description
Basic attribute	Message	--	FTP Log service started.
Extended attributes (common information)	Severity	SEVERITY	Information
	User name	USER_NAME	User who started the service
	Product name	PRODUCT_NAME	/HITACHI/JP1/FTP
	Object type	OBJECT_TYPE	JOB
	Object name	OBJECT_NAME	LOG
	Root object type	ROOT_OBJECT_TYPE	JOB

Attribute type	Item	Attribute name	Description
Extended attributes (common information)	Root object name	ROOT_OBJECT_NAME	JP1/FTP/LOG
	Object ID	OBJECT_ID	LOG
	Occurrence	OCCURRENCE	START
	Start time	START_TIME	Start time
	End time	END_TIME	--
	End code	RESULT_CODE	--

Legend:

--: There is no applicable information.

(4) Details of event ID: 00010D0F

Attribute type	Item	Attribute name	Description
Basic attribute	Message	--	FTP Agent service started.
Extended attributes (common information)	Severity	SEVERITY	Information
	User name	USER_NAME	User who started the service
	Product name	PRODUCT_NAME	/HITACHI/JP1/FTP
	Object type	OBJECT_TYPE	JOB
	Object name	OBJECT_NAME	AGENT
	Root object type	ROOT_OBJECT_TYPE	JOB
	Root object name	ROOT_OBJECT_NAME	JP1/FTP/AGENT
	Object ID	OBJECT_ID	AGENT
	Occurrence	OCCURRENCE	START
	Start time	START_TIME	Start time
	End time	END_TIME	--
	End code	RESULT_CODE	--

Legend:

--: There is no applicable information.

(5) Details of event ID: 00010D04

Attribute type	Item	Attribute name	Description
Basic attribute	Message	--	FTP Server service ended.
Extended attributes (common information)	Severity	SEVERITY	Information
	User name	USER_NAME	User who started the service
	Product name	PRODUCT_NAME	/HITACHI/JP1/FTP
	Object type	OBJECT_TYPE	JOB
	Object name	OBJECT_NAME	SERVER
	Root object type	ROOT_OBJECT_TYPE	JOB

Attribute type	Item	Attribute name	Description
Extended attributes (common information)	Root object name	ROOT_OBJECT_NAME	JP1/FTP/SERVER
	Object ID	OBJECT_ID	SERVER
	Occurrence	OCCURRENCE	END
	Start time	START_TIME	--
	End time	END_TIME	End time
	End code	RESULT_CODE	0

Legend:

--: There is no applicable information.

(6) Details of event ID: 00010D05

Attribute type	Item	Attribute name	Description
Basic attribute	Message	--	FTP Client service ended.
Extended attributes (common information)	Severity	SEVERITY	Information
	User name	USER_NAME	User who started the service
	Product name	PRODUCT_NAME	/HITACHI/JP1/FTP
	Object type	OBJECT_TYPE	JOB
	Object name	OBJECT_NAME	CLIENT
	Root object type	ROOT_OBJECT_TYPE	JOB
	Root object name	ROOT_OBJECT_NAME	JP1/FTP/CLIENT
	Object ID	OBJECT_ID	CLIENT
	Occurrence	OCCURRENCE	END
	Start time	START_TIME	--
	End time	END_TIME	End time
	End code	RESULT_CODE	0

Legend:

--: There is no applicable information.

(7) Details of event ID: 00010D06

Attribute type	Item	Attribute name	Description
Basic attribute	Message	--	FTP Log service ended.
Extended attributes (common information)	Severity	SEVERITY	Information
	User name	USER_NAME	User who started the service
	Product name	PRODUCT_NAME	/HITACHI/JP1/FTP
	Object type	OBJECT_TYPE	JOB
	Object name	OBJECT_NAME	LOG
	Root object type	ROOT_OBJECT_TYPE	JOB

Attribute type	Item	Attribute name	Description
Extended attributes (common information)	Root object name	ROOT_OBJECT_NAME	JP1/FTP/LOG
	Object ID	OBJECT_ID	LOG
	Occurrence	OCCURRENCE	END
	Start time	START_TIME	--
	End time	END_TIME	End time
	End code	RESULT_CODE	0

Legend:

--: There is no applicable information.

(8) Details of event ID: 00010D10

Attribute type	Item	Attribute name	Description
Basic attribute	Message	--	FTP Agent service ended.
Extended attributes (common information)	Severity	SEVERITY	Information
	User name	USER_NAME	User who started the service
	Product name	PRODUCT_NAME	/HITACHI/JP1/FTP
	Object type	OBJECT_TYPE	JOB
	Object name	OBJECT_NAME	AGENT
	Root object type	ROOT_OBJECT_TYPE	JOB
	Root object name	ROOT_OBJECT_NAME	JP1/FTP/AGENT
	Object ID	OBJECT_ID	AGENT
	Occurrence	OCCURRENCE	END
	Start time	START_TIME	--
	End time	END_TIME	End time
	End code	RESULT_CODE	0

Legend:

--: There is no applicable information.

(9) Details of event ID: 00010D0B

Attribute type	Item	Attribute name	Description
Basic attribute	Message	--	FTP file transmission ended normally.
Extended attributes (common information)	Severity	SEVERITY	Information
	User name	USER_NAME	FTP login user
	Product name	PRODUCT_NAME	/HITACHI/JP1/FTP
	Object type	OBJECT_TYPE	JOB
	Object name	OBJECT_NAME	For SERVER: Transmission number For CLIENT: Transmission card name

Attribute type	Item	Attribute name	Description
Extended attributes (common information)	Root object type	ROOT_OBJECT_TYPE	JOB
	Root object name	ROOT_OBJECT_NAME	JP1/FTP/SERVER or JP1/FTP/CLIENT
	Object ID	OBJECT_ID	SERVER or CLIENT
	Occurrence	OCCURRENCE	END
	End time	END_TIME	End time
	End code	RESULT_CODE	0
(program-specific information)	Transmission number	A0	Transmission number
	Connection number	A1	Connection number
	Card name	A2	Transmission card name (client only)
	Name of the host at the connection destination	A3	Name of the host at the connection destination
	Number of the port at the connection destination	A4	Number of the port at the connection destination (client only)
	User name	A5	FTP login user name
	Transmission mode	A6	ASCII or BINARY
	Transmission command	A7	Send (overwrite), send (append), receive (overwrite), or receive (append)
	Compression mode	A8	Compressed or uncompressed
	Local file name	A9	Local file name
	Remote file name	B0	Remote file name (client only)
	Transmission start time	B1	Transmission start time
	Transmission end time	B2	Transmission end time
	Size of the transmitted data	B3	Size of the transmitted data (bytes)
	Comment	B4	Comment (client only)
	Transmission end status	B5	Normal termination

Legend:

--: There is no applicable information.

(10) Details of event ID: 00010D0C

Attribute type	Item	Attribute name	Description
Basic attribute	Message	--	FTP file transmission ended abnormally.
Extended attributes (common information)	Severity	SEVERITY	Error
	User name	USER_NAME	FTP login user
	Product name	PRODUCT_NAME	/HITACHI/JP1/FTP
	Object type	OBJECT_TYPE	JOB

Attribute type	Item	Attribute name	Description
Extended attributes (common information)	Object name	OBJECT_NAME	For SERVER: Transmission number For CLIENT: Transmission card name
	Root object type	ROOT_OBJECT_TYPE	JOB
	Root object name	ROOT_OBJECT_NAME	JP1/FTP/SERVER or JP1/FTP/CLIENT
	Object ID	OBJECT_ID	SERVER or CLIENT
	Occurrence	OCCURRENCE	END
	End time	END_TIME	End time
	End code	RESULT_CODE	1
(program-specific information)	Transmission number	A0	Transmission number
	Connection number	A1	Connection number
	Card name	A2	Transmission card name (client only)
	Name of the host at the connection destination	A3	Name of the host at the connection destination
	Number of the port at the connection destination	A4	Number of the port at the connection destination (client only)
	User name	A5	FTP login user name
	Transmission mode	A6	ASCII or BINARY
	Transmission command	A7	Send (overwrite), send (append), receive (overwrite), or receive (append)
	Compression mode	A8	Compressed or uncompressed
	Local file name	A9	Local file name
	Remote file name	B0	Remote file name (client only)
	Transmission start time	B1	Transmission start time
	Transmission end time	B2	Transmission end time
	Size of the transmitted data	B3	Size of the transmitted data (bytes)
	Comment	B4	Comment (client only)
	Transmission end status	B5	Abnormal termination
	Module in which the error occurred	C0	Module in which the error occurred
	Location of the error	C1	Location of the error
	Error type	B6	System call error, logical error, protocol error, or SSL communication error
	Name of system call	B7	Name of the system call in which the error occurred (Error type: system call error)
	System call message	B8	System call error message (Error type: system call error)

Attribute type	Item	Attribute name	Description
(program-specific information)	Protocol message	B9	Protocol error message (Error type: protocol error)

Legend:

--: There is no applicable information.

(11) Details of event ID: 00010D0D

Attribute type	Item	Attribute name	Description
Basic attribute	Message	--	FTP file transmission is terminated with a warning. Automatic start of a program failed.
Extended attributes (common information)	Severity	SEVERITY	Warning
	User name	USER_NAME	FTP login user
	Product name	PRODUCT_NAME	/HITACHI/JP1/FTP
	Object type	OBJECT_TYPE	JOB
	Object name	OBJECT_NAME	For SERVER: Transmission number For CLIENT: Transmission card name
	Root object type	ROOT_OBJECT_TYPE	JOB
	Root object name	ROOT_OBJECT_NAME	JP1/FTP/SERVER or JP1/FTP/CLIENT
	Object ID	OBJECT_ID	SERVER or CLIENT
	Occurrence	OCCURRENCE	END
	End time	END_TIME	End time
	End code	RESULT_CODE	2
(program-specific information)	Transmission number	A0	Transmission number
	Connection number	A1	Connection number
	Card name	A2	Transmission card name (client only)
	Name of the host at the connection destination	A3	Name of the host at the connection destination
	Number of the port at the connection destination	A4	Number of the port at the connection destination (client only)
	User name	A5	FTP login user name
	Transmission mode	A6	ASCII or BINARY
	Transmission command	A7	Send (overwrite), send (append), receive (overwrite), or receive (append)
	Compression mode	A8	Compressed or uncompressed
	Local file name	A9	Local file name
	Remote file name	B0	Remote file name (client only)

Attribute type	Item	Attribute name	Description
(program-specific information)	Transmission start time	B1	Transmission start time
	Transmission end time	B2	Transmission end time
	Size of the transmitted data	B3	Size of the transmitted data (bytes)
	Comment	B4	Comment (client only)
	Transmission end status	B5	Normal termination
	Auto-start program name	C3	Auto-start program name

Legend:

--: There is no applicable information.

E. Format Files Used for Output of Definition Information

This appendix describes the format files that are used for output of definition information.

Sample format files are provided. For the storage locations and names of the sample format files, see [A. List of Files and Directories](#).

You can edit a format file for ease of use, such as by specifying the information you wish to have output.

E.1 Creating a format file

Keywords are used to specify the information that is to be output to a format file.

During output, information is embedded into the format file at the locations of the corresponding keywords. Any characters other than the keywords (including linefeed and control characters) are output as is to the text file.

Notes about creating a format file

- A format file must be created within a size limit of 2,048 bytes. If a created file exceeds 2,048 bytes, any excess information will be ignored.
- You can specify a maximum of 50 keywords in a format file. If you specify more than 50 keywords, the excess keywords will be ignored.

(1) Keywords that can be specified

This subsection lists the keywords that can be specified in each type of format file.

Table E–1: Keywords that can be specified for login user definition information

Keyword	Description
\$ICNT	Data count
\$USER	User name
\$CDIR	Current directory

Table E–2: Keywords that can be specified for auto-start programs

Keyword	Description
\$ICNT	Data count
\$USER	User name
\$AKEY	Trigger for auto-start
\$AFDK	Key type
\$ANML	Name of the program to start when transmission ends normally
\$AERR	Name of the program to start when transmission ends abnormally

Table E–3: Keywords that can be specified for transmission information

Keyword	Description
\$ICNT	Data count

Keyword	Description
\$USER	User name
\$PSWD	Password
\$CARD	Transmission card
\$LCAL	Local file name
\$RMTE	Remote file name
\$TRAN	Sending or receiving
\$MODE	Transmission mode
\$OUTK	Output type
\$COMP	Compression mode
\$FSIZ	Size check
\$HOST	Remote host name
\$PORT	Port number
\$ANML	Name of the program to start when transmission ends normally
\$AERR	Name of the program to start when transmission ends abnormally
\$CMND	FTP command
\$CMNT	Comment
\$MULT	Single-file or multiple-file transmission
\$FTPS	Use FTPS
\$SCVC	Check the expiration date of the server certificate
\$CACF	Path to the CA certificate
\$CRLF	Path to the CRL

Table E–4: Keywords that can be specified for log information

Keyword	Description
\$ICNT	Data count
\$USER	User name
\$CARD	Transmission card
\$LCAL	Local file name
\$RMTE	Remote file name
\$TRAN	Sending or receiving
\$MODE	Transmission mode
\$OUTK	Output type
\$COMP	Compression mode
\$HOST	Remote host name
\$PORT	Port number
\$CMNT	Comment

Keyword	Description
\$TRNO	Transmission number
\$SVCE	Client or server
\$STAT	End status
\$STIM	Start time
\$ETIM	End time
\$TIME	Transmission period
\$TSIZ	Size transmitted
\$CONO	Connection number
\$ETYP	Error type
\$EPOS	Location of the error
\$EMOD	Error module name
\$ESYS	Name of the system call
\$EMSG	Error message
\$EPRT	Protocol message
\$EMSC	SSL communication error message

F. Tools

The following table lists and describes the tools supported by JP1/FTP.

Table F–1: Tools supported by JP1/FTP

Function	Tool name
Initialize results	FTSTRANINIT.BAT FTSMGRINIT.BAT
Change monitored host information	FTSMGRHOST.BAT

F.1 FTSTRANINIT.BAT and FTSMGRINIT.BAT - initialize results

FTSTRANINIT.BAT initializes the transmission results (log information, trace information, transmission number, and connection number), and FTSMGRINIT.BAT initializes the operation results of the Operations-Manager function (trace information).

(1) Names

FTSTRANINIT.BAT

FTSMGRINIT.BAT

(2) Storage directories

FTSTRANINIT.BAT:

JP1/FTP-installation-directory

FTSMGRINIT.BAT:

JP1/FTP-installation-directory\manager

(3) Execution formats

FTSTRANINIT.BAT

FTSMGRINIT.BAT

(4) Functions

FTSTRANINIT.BAT:

Initializes the transmission results as follows:

- Deletes log information.
- Deletes protocol traces.
- Deletes module traces.
- Resets the transmission number to its initial value.
- Resets the connection number to its initial value.
- Initializes the access log file (becomes 0 bytes).

FTSMGRINIT.BAT:

Deletes the trace information for operations management.

(5) Arguments

None.

(6) Execution permissions

Administrator

(7) Notes

FTSTRANINIT.BAT:

Before you execute this tool, you must stop the client service, server service, and log service of JP1/FTP.

FTSMGRINIT.BAT:

Before you execute this tool, you must stop the agent service of JP1/FTP and close the Operations-Manager Console.

F.2 FTSMGRHOST.BAT - change monitored host information

FTSMGRHOST.BAT adds the local host to or deletes the local host from the monitored host information.

(1) Name

FTSMGRHOST.BAT

(2) Storage directory

JP1/FTP-installation-directory\manager\console

(3) Execution format

FTSMGRHOST.BAT /A|/D

(4) Function

FTSMGRHOST.BAT changes the information about the local host in the monitored host information.

(5) Arguments

1. /A

Specifies to add the information about the local host to the monitored host information.

2. /D

Specifies to delete the information about the local host from the monitored host information.

(6) Execution permissions

Administrator

G. Notes about Operation

1. You must start JP1/FTP commands, GUIs, and tools as administrator.
An administrator is a user who satisfies the following conditions:
 - If User Account Control (UAC) is enabled:
Administrator or a user who has been elevated to an administrator account
 - If User Account Control (UAC) is disabled:
User who has Administrators permissions
2. To start JP1/FTP from another linked product, the administrator must be executing that linked product. Otherwise, startup of JP1/FTP might fail.
3. Files are locked while they are engaged in file transmission (lock processing is performed). During send processing, such files can be read, but they are write-protected. During receive processing, the files are protected from both read and write operations.
4. If file transmission is interrupted, such as by forced termination of file receive processing or by a transmission error, an incomplete file might be created. If overwrite receive processing is interrupted, the original file cannot be restored.
5. JP1/FTP handles files on network drives as a single Windows file. Therefore, you can use files on a network drive only in an environment that supports them as Windows files and within the supported operation range.
Even if transmission processing is successful, the contents of a transmitted file might not be written correctly due to problems specific to network drives, their settings, and the environment configuration.
6. If you use a network relay device (such as a router or a firewall) that performs IP address translation (such as Network Address Translation (NAT) or IP masquerading), file transmission via the device might fail due to use of the FTP protocol. Make sure that the device in use supports the FTP protocol.

Note

The specifications of checking for the `PORT` command in 09-00 and the `PASV` command in 10-00 have been improved. These improvements can sometimes cause a problem to occur when an IP address is not properly translated. If this happens, revise the IP address translation settings so that it is properly translated, or change the specifications of checking for the `PORT` and `PASV` commands by referring to [Table 3-2](#) in the manual.

7. JP1/FTP uses the IP addresses shown in the table below.

Table G–1: IP addresses used by JP1/FTP

No.	Usage		IP address to be used
1	Client	IP address for control connection	IP address that is assigned automatically by the OS
2		IP address for data connection	IP address for control connection
3	Server	IP address for control connection	IP address that accepted the connection
4		IP address for data connection	IP address for control connection
5	IP address of the Operations-Manager Agent		Physical IP address (IP address corresponding to the host name that is returned by an OS command (such as <code>hostname</code>))
6	IP address of the Operations-Manager Console		IP address that is assigned automatically by the OS

8. Provided below are notes about using JP1/FTP in a cluster system configuration (in an HA configuration that supports system switching). For details about the definition of JP1/FTP in an environment where logical addresses are used, see [3.11 Using JP1/FTP in a multiple IP address environment](#). A cluster system is the same as what is referred to as a node switching system in the JP1 manuals.
 - Failover is not supported.

- Physical IP addresses must be enabled (IP addresses corresponding to the host names that are returned by an OS command, such as `hostname`).
- JP1/FTP services can be started and stopped by using cluster software.
- When JP1/FTP is run as the FTP server, file transmission is supported whether the FTP client specifies a local IP address or a physical IP address as the connection target.
- When JP1/FTP is run as the FTP client, re-transmission initiated by a method such as automatic retries of file transmission is not performed in the event of a failure.
- FTP custom jobs can be used to perform file transmission.

The following notes apply when the environment definition for a multiple IP address environment is not used:

- When JP1/FTP is run as the FTP client, the IP address for connection is usually a physical IP address because it is assigned automatically by the OS.
- JP1 events are sent to the physical IP address (IP address corresponding to the host name that is returned by an OS command, such as `hostname`).
- When JP1/FTP is run as the FTP server, the physical host name (host name returned by an OS command, such as `hostname`) is set in message 220, which is returned when control connection is established.

9. Class-3 and class-4 characters are not supported.

10. Before you change the system time, stop all JP1/FTP services and GUIs. To reset the system time, you must initialize the transmission logs.

The procedure for resetting the system time is as follows:

1. Stop all JP1/FTP services and GUIs.
2. Back up the log information file to a desired directory.
3. Change the system time.
4. Initialize the transmission results. For details about the initialization method, see [F.1 FTSTRANINIT.BAT and FTSMGRINIT.BAT - initialize results](#).
5. Start the JP1/FTP services and GUIs.

11. If only the drive name is specified in the specification of a root directory, operations might not execute correctly.

Example

(Incorrect) C :

(Correct) C : \

12. When the FTP client receives (get) a file from the FTP server and an error occurs in the FTP client after the FTP server sends the file normally, differences between the files in the FTP server and in the FTP client occur. Similar differences will occur during execution of operations with the size check option.

13. The maximum number of concurrent transmissions is 60. A connection request that causes the number of transmissions to exceed 64 is rejected.

14. There is no limit on the size of transmission files. The size of files that can be transmitted is dependent on the system limits.

15. On the JP1/FTP client, if you want to receive files by specifying wildcard characters, a local file name is generated from the list of file path names received in response to the `NLST` command. As a result, depending on the format of the list of file path names received from the destination FTP server, the file might not be able to be transmitted normally. The list of file path names supported by JP1/FTP is based on the RFC 959 (FILE TRANSFER PROTOCOL). In addition, of the file path names in the list, those that are supported by JP1/FTP must meet all of the following conditions:

- The format of the first part of the file path name must be the same as the format of the file path name specified for the remote file name. Alternatively, if the file path name specified for the remote file name is a relative path

and begins with either `"/` or `"\`, the format of the first part of the file path name must be the same as the format of the file path name (excluding `"/` or `"\`) specified for the remote file name.

- If the list of file path names includes blank lines, all file path names must be listed before the first blank line.

Examples are shown below.

In these examples, the configuration of directories on an FTP server is as shown below.

```
/
└─dir1
   ├──file11
   ├──file12
   ├──dir11
   │   └─file111
   ├──dir12
   │   └─file121
   └─dir13
       └─file131
```

Example 1

On the JP1/FTP client, the file path name specified for the remote file name is `"/dir1/*"` and the list of file path names is as follows:

```
/dir1/file11
file12
/dir1/dir11/file111

/dir1/dir12:
file121

/dir1/dir13:
file131
```

In this case, the supported file path names are `"/dir1/file11"` and `"/dir1/dir11/file111"` only.

Example 2

On the JP1/FTP client, if the file path name specified for the remote file name is `"/dir1/*"` or `"\dir1*"`, the following file path names in the list of file path names are supported:

```
./dir1/file11
.\dir1\file11
dir1/file11
dir1\file11
./dir1/dir11/file111
.\dir1\dir11\file111
```

Note

Depending on the FTP server, a list of file path names might include directory path names. In such cases, if the above conditions are met, the JP1/FTP client sends the `RETR` command with the path name as the parameter.

As a result, the FTP server usually returns an error response, and file transmission terminates abnormally.

16. If you stop the JP1/FTP Server or Client service during a file transmission or right after a file transmission, be sure to stop the JP1/FTP Log service as well. Not doing so might make it so that log information cannot be collected for subsequent file transmissions.
17. Files transmitted via an IPv6 address are not compatible with IPv4-mapped addresses.
18. The typical implementation of JP1/FTP is to create transmission information when setting up the environment, and then actually transmit files after operation is started. As a result, the `ftsregc` command is typically only used when setting up the environment, and not during normal operation.

Note the following:

- Do not transmit files and edit or delete transmission information at the same time. (This applies to GUI operations as well.)
 - The `ftsregc` command is resource-intensive.
 - If transmission information is fixed during operation, instead of executing the `ftsregc` command, we recommend using `ftstran` command arguments to specify the fixed transmission information.
19. Only one session is required to use Remote Desktop to remotely perform operations. (This is the same as when the console is used to perform operations.)
 20. The beginning of messages such as "System call error occurred." output to the Event log are displayed in Japanese when the OS language is Japanese, and in English for all other OS language settings. Note that the JP1/FTP language setting is not taken into account.
 21. The maximum path name size JP1/FTP can handle is 259 bytes.

H. Changes in Each Version

This appendix describes the changes that have been made in each version of JP1/FTP.

H.1 Changes in 12-00

- The following OS was deleted from the supported OSs:
 - Windows Server 2008 R2
- Files can now be transmitted via FTPS.
- The following OSs are now supported:
 - Windows Server 2016
- Event IDs 43, 45, 46, and 47 have been added to the messages displayed in Event Viewer.
- Messages for `ftstran` command execution have been added.
- Messages for `ftsregc` command execution have been added.

H.2 Changes in 11-00

- The Language Selection dialog box was added.
- The number of module trace files was changed.
- The function for linking to JP1/Cm2/NNM was removed.
- The display format of dates in FTP connection response messages was changed.
- A method for configuring the environment settings file of the definition program for custom jobs was added.
- The functions `fts_ftp_syn_request`, `fts_ftp_asyn_request`, and `fts_ftp_event` were removed.
- The format of the connection information structure was changed.
- Information about the compilers of the API libraries was changed.
- API libraries for 64-bit were added.
- The module trace of the Log service was added as information to be collected when a failure occurs.

H.3 Changes in 10-10

- You can now specify IPv6 addresses in `FTPHOSTACC.INF`.
- You can now specify the destination of a JP1 event to be sent when transmission ends.
- Information about the compilers of the API libraries was changed.
- General users can now execute the `ftstran` command.
- Event IDs 39, 40, 41, and 42 have been added to the messages displayed in Event Viewer.

H.4 Changes in 10-00

- Files can now be transmitted using IPv6 addresses.
- The default values and maximum values of the following settings have been changed:
 - Number of log entries that are retained
 - Protocol trace file size
 - Module trace file size
- The check specifications of the PASV command on the FTP client side have been modified.
- The 4-gigabyte restriction on the size of log information that can be displayed on Operations-Manager Console has been eliminated.
- The DLL file information required for registering custom jobs has been modified.
- The `fts_ftp_open_ex` function has been added.
- Notes have been added on using API libraries, previously used in versions earlier than 10-00, in version 10-00 or later.
- Information on the compilers assumed by the API libraries has been modified.
- Event IDs 37 and 38 have been added to the messages displayed in Event Viewer.

H.5 Changes in 09-00

- A non-administrator user or a user without administrator permissions can now reference the definition information.
- The PORT command checking specifications have been changed for the FTP server.
- The `ftstran` command's return value (9900001) has been added.
- The `ftsregc` command's return value (9900001) has been added.
- The `ftshistory` command's return value (9900001) has been added.
- The `fts_ftp_open` function's return value (0x2FFFFFF13) has been added.
- Messages for `ftstran` command execution have been added.
- Messages for `ftsregc` command execution have been added.
- Messages for `ftshistory` command execution have been added.
- Messages for `ftsload` command execution have been added.
- Messages for `ftssave` command execution have been added.
- Notes about using Windows Server 2008 have been added.
- The function for using the access control function to change the root directory of absolute path names has been added.
- The FTP connection response message control function has been added.
- Information has been added to the effect that when JP1/FTP is installed on multiple computers and JP1/AJS2 is linked, all installed JP1/FTPs in the system configuration must be the same version.
- Information about firewall passage directions has been added.
- The restriction on transmitting a file of more than 4 gigabytes has been removed (previously, transmission of a file of more than 4 gigabytes was supported only by the IPF version).

- The **Defining program** settings have been added to the Set Properties of Custom Job dialog box.

I. Reference Material for This Manual

This appendix provides reference information, including various conventions, for this manual.

I.1 Related publications

This manual is part of a related set of manuals. The manuals in the set are listed below (with the manual numbers):

- *JP1 Version 12 JP1/Base User's Guide* (3021-3-D65(E))
- *JP1 Version 12 JP1/Integrated Management 2 - Manager Configuration Guide* (3021-3-D52(E))
- *JP1 Version 12 JP1/Automatic Job Management System 3 Linkage Guide* (3021-3-D29(E))
- *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1* (3020-3-S81(E)), for Windows systems

I.2 Conventions: Abbreviations

This manual uses the following abbreviations for product names:

Abbreviation		Full name or meaning
JP1/AJS3	JP1/AJS - Manager	JP1/Automatic Job Management System 3 - Manager
	JP1/AJS - View	JP1/Automatic Job Management System 3 - View
JP1/FTP		JP1/File Transmission Server/FTP
JP1/IM	JP1/IM - Manager	JP1/Integrated Management - Manager
		JP1/Integrated Management 2 - Manager
	JP1/IM - View	JP1/Integrated Management - View
		JP1/Integrated Management 2 - View
JP1/SD		Job Management Partner 1/ Software Distribution

I.3 Conventions: Acronyms

This manual also uses the following abbreviations:

Abbreviation	Full name or meaning
API	Application Programming Interface
CA	Certificate Authority
CRL	Certificate Revocation List
DNS	Domain Name System
FTPS	File Transfer Protocol over SSL/TLS
LAN	Local Area Network

Abbreviation	Full name or meaning
NAT	Network Address Translation
NIC	Network Interface Card
PKI	Public Key Infrastructure
RFC	Request for Comments
TCP/IP	Transmission Control Protocol/Internet Protocol
WAN	Wide Area Network

I.4 Conventions: KB, MB, GB, and TB

This manual uses the following conventions:

- 1 KB (kilobyte) is 1,024 bytes.
- 1 MB (megabyte) is 1,024² bytes.
- 1 GB (gigabyte) is 1,024³ bytes.
- 1 TB (terabyte) is 1,024⁴ bytes.

Index

A

- abbreviations defined 213
- absolute path name
 - changing root directory of, using access control function 81
 - registering format of 81
- AccessLimitation.ini 81
- access log
 - collecting 79
 - setting for collecting 79
- access log output file 79
- acronyms 213
- API library 131
- append text 69
- asynchronous execution 57
- auto-start program
 - changing 45
 - deleting 45
 - registering 40
- Auto-Start Program Registration window 40, 98
 - changing information displayed in 46
 - displaying 40

C

- Change Auto-Start Program dialog box 45
- Change Transmission Information dialog box 53
- Change User Information dialog box 38
- client 17
- coding 132
 - notes about 138
- command
 - displaying log information 126
 - executing transmission 120
 - recovering definition information 128
 - registering, changing, deleting, and displaying transmission information 123
 - saving definition information 127
- commands, list of 118
- compiler 131
- Compiling and linking 138
- Contents of the definition file (ftserv.ini) 35
- conventions
 - abbreviations 213
 - acronyms 213

- fonts and symbols 8
- KB, MB, GB and TB 214
- version numbers 9

Creating environments in which names can be resolved 28

D

- data to collect when problem occurs 180
- definition information
 - example of outputting as text 103
 - outputting as text 69
 - registering 83
 - using ftload command to recover 68
 - using ftssave command to save 66

E

- Enter Information method of file transmission
 - using ftstran command 59
 - using Registration And Execution Of Transmission Requests window 58
- environment definition 32
- Environment Definition dialog box 32
 - displaying 32
 - items in 32
- Environment Definition window 96
- environment for JP1/FTP
 - defining 32
 - using definition file to define 34
- error handling procedures 178
- Execute Transmission (Enter Information) dialog box 58

F

- feature 16
- file transmission
 - canceling 57, 59
 - Enter Information method of 56
 - flow of 19
 - in PASV mode 71
 - Select Card method of 56
- file transmission function 17
- firewall
 - item to check when performing transmission via 190
 - passage direction 189

- font conventions 8
- format file
 - creating 201
 - keyword that can be specified in 201
- FTP connection response message control function 83
- FTP connection response message that is displayed 84
- FTPHOSTACC.INF 73
- FTPPASV.INI 71
- fts_ftp_asyn_request_ex() 149
- fts_ftp_cancel() 153
- fts_ftp_close() 155
- fts_ftp_event_ex() 151
- fts_ftp_open_ex() 145
- fts_ftp_syn_request_ex() 147
- FtsBanner.ini 83, 84
- FtsBanner.txt 84
- ftshistory (displaying log information) 126
- ftslload (recovering definition information) 128
- ftsregc (registering, changing, deleting, and displaying transmission information) 123
- ftssave (saving definition information) 127
- ftstran (executing transmission) 120
- function
 - canceling transmission 153
 - controlling remote host connection 73
 - establishing connection with JP1/FTP 145
 - obtaining transmission-end result 151
 - prerequisite for using 131
 - registering transmission request (asynchronous) 149
 - registering transmission request (synchronous) 147
 - releasing connection with JP1/FTP 155
 - using access control function to change root directory for absolute path name 81
- functions 17
 - details of 144
 - list of 143

G

GB meaning 214

H

HOSTINFO.INI 76

I

installing 26

Internet protocol version, registering 86

IPv6 environment, using JP1/FTP in 86

IPversion.ini 86

item

in Environment Definition dialog box 32

in Log Details dialog box 61

in Register Auto-Start Program dialog box 41

in Register Transmission Information dialog box 48

in View Range dialog box 63

J

JP1/AJS3, setting for linking to 106

JP1/FTP

in multiple IP address environment, using 76

list of files and directories for 185

overview of 15

JP1/IM

monitoring transmission result by 116

setting for linking to 115

JP1 events, list of 192

JP1 program linkage function 18

K

KB meaning 214

L

language type

setting 26

library

example of using 139

notes about using 138

setting up environment 131

using 131

linking

to JP1/AJS3 106

to JP1/IM 115

Log Details dialog box 61

items in 61

log file, loading 64

log information

example of displaying 102

using ftshistory command to display 64

Log Information window 60, 100

changing information displayed in 62

displaying 60

login user

changing information of 38

deleting information of 39
example of registering information of 101
registering 37

M

managed host
 adding 93
 deleting 94
MB meaning 214
message
 displayed during command execution 167
 displayed during execution of ftshistory command 172
 displayed during execution of ftsload command 174
 displayed during execution of ftsregc command 169
 displayed during execution of ftssave command 174
 displayed during execution of ftstran command 167
 displayed in Event Viewer 159
 output format of 157
multiple files, specifying 49
multiple IP address environment, using JP1/FTP in 76

O

operation, notes about 206
Operations-Manager Agent 92
Operations-Manager Console 92
Operations-Manager Console window 92
Operations-Manager function 18
OS, supported 25
Output or Append To Text File dialog box 104
output text 69
output text file, name of 104

P

parameter keyword 42
port numbers
 list of 189
 setting 27
processes, list of 191
program start
 priority of 42, 51
 when multiple files are transmitted 42

R

Register Auto-Start Program dialog box 41
 items in 41

Register Transmission Information dialog box 48
 items in 48

Register User To Login dialog box 37
 setting items in 38

Registration And Execution Of Transmission Requests window 47, 56
 displaying 47, 56

S

Saving and Recovering Settings dialog box 65
 displaying 65
 using, to recover setting 67
 using, to save setting 65
scheduled transmission (JP1/AJS3) 108
Select Card method of file transmission
 using ftstran command 58
 using Registration And Execution Of Transmission Requests window 56
Select Settings For Recovery dialog box 67
 setting items in 67
Select Settings To Save dialog box 66
server 17
service
 starting 29
 stopping 30
 type of 29
setting item
 in Register User To Login dialog box 37
 in Select Settings For Recovery dialog box 67
Specify User name dialog box 46
symbol conventions 8
synchronous execution 57
system configuration 25
 for linking to JP1/AJS3 106
 for linking to JP1/IM 115

T

TB meaning 214
transmission 17
transmission card
 using ftsregc command to change information on 53
 using ftsregc command to check content of 54
 using ftsregc command to delete 54
 using ftsregc command to register 51
 using Registration And Execution Of Transmission Requests window to change information on 52

using Registration And Execution Of Transmission
Requests window to check content of [54](#)

using Registration And Execution Of Transmission
Requests window to delete [54](#)

using Registration And Execution Of Transmission
Requests window to register [47](#)

transmission-end information, obtaining [135](#)

transmission information, example of distributing
(copying) [101](#)

Transmission Registration window [99](#)

transmission results and errors, checking details of [60](#)

U

uninstalling [28](#)

User-To-Login Registration window [37](#), [97](#)

displaying [37](#)

Using FTPS (at the FTP client) [88](#)

Using FTPS (at the FTP server) [89](#)

V

version, change in each [210](#)

version number conventions [9](#)

View Range dialog box [63](#)

items in [63](#)



6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100-8280 Japan
